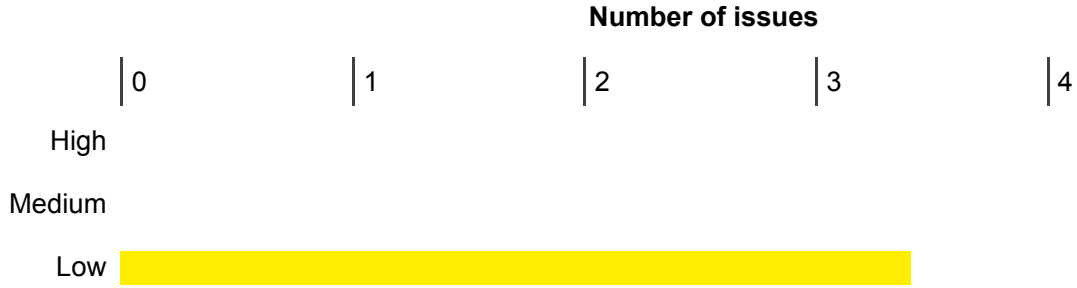
Burp Scanner Report

Summary

The table below shows the numbers of issues identified in different categories. Issues are classified according to severity as High, Medium, Low or Information. This reflects the likely impact of each issue for a typical organization. Issues are also classified according to confidence as Certain, Firm or Tentative. This reflects the inherent reliability of the technique that was used to identify the issue.

Severity	Confidence			
	Certain	Firm	Tentative	Total
High	0	0	0	0
Medium	0	0	0	0
Low	3	0	0	3
Information	3	21	1	25

The chart below shows the aggregated numbers of issues identified in each category. Solid colored bars represent issues with a confidence level of Certain, and the bars fade as the confidence level falls.



Contents

4. Email addresses disclosed

---

1. Strict transport security not enforced

There are 3 instances of this issue:

- https://192.168.1.193:7443/robots.txt
- https://192.168.1.193:7843/resources/css/google-font.css
- https://192.168.1.193:7843/robots.txt

Issue description

The application fails to prevent users from connecting to it over unencrypted connections. An attacker able to modify a legitimate user's network traffic could bypass the application's use of SSL/TLS encryption, and use the application as a platform for attacks against its users. This attack is performed by rewriting HTTPS links as HTTP, so that if a targeted user follows a link to the site from an HTTP page, their browser never attempts to use an encrypted connection. The sslstrip tool automates this process.

To exploit this vulnerability, an attacker must be suitably positioned to intercept and modify the victim's network traffic.This scenario typically occurs when a client communicates with the server over an insecure connection such as public Wi-Fi, or a corporate or home network that is shared with a compromised computer. Common defenses such as switched networks are not sufficient to prevent this. An attacker situated in the user's ISP or the application's hosting infrastructure could also perform this attack. Note that an advanced adversary could potentially target any connection made over the Internet's core infrastructure.

Issue remediation

The application should instruct web browsers to only access the application using HTTPS. To do this, enable HTTP Strict

Transport Security (HSTS) by adding a response header with the name 'Strict-Transport-Security' and the value 'max-age=expireTime', where expireTime is the time in seconds that browsers should remember that the site should only be accessed using HTTPS. Consider adding the 'includeSubDomains' flag if appropriate.

Note that because HSTS is a "trust on first use" (TOFU) protocol, a user who has never accessed the application will never have seen the HSTS header, and will therefore still be vulnerable to SSL stripping attacks. To mitigate this risk, you can optionally add the 'preload' flag to the HSTS header, and submit the domain for review by browser vendors.

References

- HTTP Strict Transport Security
- sslstrip
- HSTS Preload Form

Vulnerability classifications

- CWE-523: Unprotected Transport of Credentials

1.1. https://192.168.1.193:7443/robots.txt

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://192.168.1.193:7443**
Path:	**/robots.txt**

Request

```
GET /robots.txt HTTP/1.1
Host: 192.168.1.193:7443
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/69.0.3497.100 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response

```
HTTP/1.1 302 Found
Connection: close
Location: https://192.168.1.193:7443/adeptia/control/
```

1.2. https://192.168.1.193:7843/resources/css/google-font.css

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://192.168.1.193:7843**
Path:	**/resources/css/google-font.css**

Request

```
GET /resources/css/google-font.css HTTP/1.1
Host: 192.168.1.193:7843
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/69.0.3497.100 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: https://192.168.1.193:7843/
```

Response

```
HTTP/1.1 200
Strict-Transport-Security: max-age=0
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Accept-Ranges: bytes
ETag: W/"31244-1608185296000"
Last-Modified: Thu, 17 Dec 2020 06:08:16 GMT
Content-Security-Policy: script-src 'self' 'unsafe-inline' 'unsafe-eval'
vary: accept-encoding
Content-Type: text/css
Date: Mon, 21 Dec 2020 09:52:27 GMT
Connection: close
Server: Adeptia
Content-Length: 31244

/* latin-ext */
@font-face {
font-family: 'Raleway';
font-style: normal;
font-weight: 100;
src: local('Raleway Thin'), local('Raleway-Thin'), url(fonts/raleway/v14/1Ptsg8zYS_SKggPNwE44Q4F
...[SNIP]...
```

1.3. https://192.168.1.193:7843/robots.txt

Summary

Severity: **Low**

Confidence: **Certain**

Host: **https://192.168.1.193:7843**

Path: **/robots.txt**

Request

```
GET /robots.txt HTTP/1.1
Host: 192.168.1.193:7843
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/69.0.3497.100 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response

```
HTTP/1.1 404
Strict-Transport-Security: max-age=0
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Content-Security-Policy: script-src 'self' 'unsafe-inline' 'unsafe-eval'
vary: accept-encoding
Content-Type: text/html;charset=utf-8
Content-Language: en
Date: Mon, 21 Dec 2020 09:52:25 GMT
Connection: close
Server: Adeptia
Content-Length: 431

<!doctype html><html lang="en"><head><title>HTTP Status 404 ... Not Found</title><style type="text/css">body {font-
family:Tahoma,Arial,sans-serif;} h1, h2, h3, b {color:white;background-color:#525D76;
...[SNIP]...
```

---

2. Cross-site request forgery

Summary

Severity: **Information**

Confidence: **Tentative**

Host: **https://192.168.1.193:7443**

Path: **/adeptia/forgotpassword.jsp**

Issue detail

The request appears to be vulnerable to cross-site request forgery (CSRF) attacks against unauthenticated functionality. This is unlikely to constitute a security vulnerability in its own right, however it may facilitate exploitation of other vulnerabilities affecting application users.

Issue background

Cross-site request forgery (CSRF) vulnerabilities may arise when applications rely solely on HTTP cookies to identify the user that has issued a particular request. Because browsers automatically add cookies to requests regardless of their origin, it may be possible for an attacker to create a malicious web site that forges a cross-domain request to the vulnerable application. For a request to be vulnerable to CSRF, the following conditions must hold:

- The request can be issued cross-domain, for example using an HTML form. If the request contains non-standard headers or body content, then it may only be issuable from a page that originated on the same domain.
- The application relies solely on HTTP cookies or Basic Authentication to identify the user that issued the request. If the application places session-related tokens elsewhere within the request, then it may not be vulnerable.
- The request performs some privileged action within the application, which modifies the application's state based on the identity of the issuing user.
- The attacker can determine all the parameters required to construct a request that performs the action. If the request contains any values that the attacker cannot determine or predict, then it is not vulnerable.

Issue remediation

The most effective way to protect against CSRF vulnerabilities is to include within relevant requests an additional token that is not transmitted in a cookie: for example, a parameter in a hidden form field. This additional token should contain sufficient entropy, and be generated using a cryptographic random number generator, such that it is not feasible for an attacker to determine or predict the value of any token that was issued to another user. The token should be associated with the user's session, and the application should validate that the correct token is received before performing any action resulting from the request.

An alternative approach, which may be easier to implement, is to validate that Host and Referer headers in relevant requests are both present and contain the same domain name. However, this approach is somewhat less robust: historically, quirks in browsers and plugins have often enabled attackers to forge cross-domain requests that manipulate these headers to bypass such defenses.

References

- Using Burp to Test for Cross-Site Request Forgery
- The Deputies Are Still Confused

Vulnerability classifications

- CWE-352: Cross-Site Request Forgery (CSRF)

Request 1

```
POST /adeptia/forgotpassword.jsp HTTP/1.1
Host: 192.168.1.193:7443
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
```

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/69.0.3497.100 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: https://192.168.1.193:7443/adeptia/rememberPassword.jsp
Content-Type: application/x-www-form-urlencoded
Content-Length: 53
Cookie: JSESSIONID=node01asd5cuxdxlfo1xo574ead44g055

logonid=266802&submit=Get+New+Password&logonidHidden=
```

Response 1

```
HTTP/1.1 200 OK
Connection: close
Set-Cookie: JSESSIONID=node01asd5cuxdxlfo1xo574ead44g055;Path=/adeptia; HttpOnly;Secure
Expires: Thu, 01 Jan 1970 00:00:00 GMT
X-Frame-Options: SAMEORIGIN
Content-Type: text/html;charset=utf-8
Cache-Control: no-cache
Pragma: no-cache
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Security-Policy: script-src 'self' 'unsafe-inline' 'unsafe-eval';
Content-Length: 414


<html>
<title>Recover Password</title>
<head>
      <link rel="stylesheet" href=/adeptia/css/ui.css type="text/css" />
</head>
<body>
   <!--   <
...[SNIP]...
```

Request 2

```
POST /adeptia/forgotpassword.jsp HTTP/1.1
Host: 192.168.1.193:7443
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/69.0.3497.100 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: https://IzQaBaDvy.com:7443/adeptia/rememberPassword.jsp
Content-Type: application/x-www-form-urlencoded
Content-Length: 53
Cookie: JSESSIONID=node01gmxm3hhobml9agxz5p1qd9ss99

logonid=850271&submit=Get+New+Password&logonidHidden=
```

Response 2

```
HTTP/1.1 200 OK
Connection: close
Set-Cookie: JSESSIONID=node01gmxm3hhobml9agxz5p1qd9ss99;Path=/adeptia; HttpOnly;Secure
Expires: Thu, 01 Jan 1970 00:00:00 GMT
X-Frame-Options: SAMEORIGIN
Content-Type: text/html;charset=utf-8
Cache-Control: no-cache
Pragma: no-cache
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Security-Policy: script-src 'self' 'unsafe-inline' 'unsafe-eval';
Content-Length: 414


<html>
<title>Recover Password</title>
<head>
      <link rel="stylesheet" href=/adeptia/css/ui.css type="text/css" />
</head>
<body>
   <!--   <
...[SNIP]...
```

---

3. DOM data manipulation (DOM-based)

There are 21 instances of this issue:

- /adeptia/TransactionStatus.jsp
- /adeptia/TransactionStatus.jsp
- /adeptia/TransactionStatus.jsp
- /adeptia/control/datainterfaceslog.jsp
- /adeptia/control/datainterfaceslog.jsp
- /adeptia/control/datainterfaceslog.jsp
- /adeptia/control/eventMonitor.jsp
- /adeptia/control/eventMonitor.jsp
- /adeptia/control/eventMonitor.jsp
- /adeptia/control/monitorsPerformance.jsp
- /adeptia/control/monitorsPerformance.jsp
- /adeptia/control/monitorsPerformance.jsp
- /adeptia/control/reportUsageGUI.jsp
- /adeptia/control/reportUsageGUI.jsp
- /adeptia/control/reportUsageGUI.jsp
- /adeptia/js/beansupport.js
- /adeptia/js/beansupport.js
- /adeptia/js/beansupport.js
- /adeptia/rememberPassword.jsp
- /adeptia/rememberPassword.jsp
- /adeptia/rememberPassword.jsp

Issue background

DOM-based vulnerabilities arise when a client-side script reads data from a controllable part of the DOM (for example, the URL) and processes this data in an unsafe way.

DOM data manipulation arises when a script writes controllable data to a field within the DOM that is used within the visible UI or client-side application logic. An attacker may be able to use the vulnerability to construct a URL that, if visited by another application user, will modify the appearance or behavior of the client-side UI. An attacker may be able to leverage this to perform virtual defacement of the application, or possibly to induce the user to perform unintended actions.

Burp Suite automatically identifies this issue using static code analysis, which may lead to false positives that are not actually exploitable. The relevant code and execution paths should be reviewed to determine whether this vulnerability is indeed present, or whether mitigations are in place that would prevent exploitation.

Issue remediation

The most effective way to avoid DOM-based DOM data manipulation vulnerabilities is not to dynamically write to DOM data fields any data that originated from any untrusted source. If the desired functionality of the application means that this behavior is unavoidable, then defenses must be implemented within the client-side code to prevent malicious data from being stored. In general, this is best achieved by using a whitelist of permitted values.

Vulnerability classifications

- CWE-20: Improper Input Validation

3.1. https://192.168.1.193:7443/adeptia/TransactionStatus.jsp

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/TransactionStatus.jsp**

Issue detail

The application may be vulnerable to DOM-based DOM data manipulation. Data is read from **location** and passed to **the 'setAttribute()' function of a DOM element**.

Request 1

```
GET /adeptia/TransactionStatus.jsp HTTP/1.1
Host: 192.168.1.193:7443
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
```

```
Connection: close
X-Frame-Options: SAMEORIGIN
Content-Type: text/html;charset=utf-8
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: 0
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>

<link rel="stylesheet" href=/adeptia/css/ui.css type=
...[SNIP]...
</script>
<script type="text/javascript" src=/adeptia/js/beansupport.js></script>
...[SNIP]...
```

Request 2

```
GET /adeptia/js/beansupport.js HTTP/1.1
Host: 192.168.1.193:7443
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/69.0.3497.100 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: https://192.168.1.193:7443/adeptia/rememberPassword.jsp
Cookie: JSESSIONID=node0aiite2301smyc3n66dci78nv81
```

Response 2

```
HTTP/1.1 200 OK
Connection: close
Set-Cookie: JSESSIONID=node0aiite2301smyc3n66dci78nv81;Path=/adeptia; HttpOnly;Secure
Expires: Thu, 01 Jan 1970 00:00:00 GMT
X-Frame-Options: SAMEORIGIN
Last-Modified: Mon, 21 Dec 2020 07:53:28 GMT
Content-Type: application/javascript
Accept-Ranges: bytes
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Security-Policy: script-src 'self' 'unsafe-inline' 'unsafe-eval';


/*
* Bean editors support scripts
*/

var validationArray = new Array();
var permissionMask='711'
var userPermissionMask = 7;
```

```
var groupPermissionMask = 1;
var otherPermissionMask = 1;


...[SNIP]...
lue);

        if(location.indexOf('?') != -1) {
            location = location + '&' + tokenName + '=' + value;
        } else {
            location = location + '?' + tokenName + '=' + value;
        }

        try {
            element.setAttribute(attr, location);
        } catch (e) {
            // attempted to set/update unsupported attribute
        }
    }
  }
}
```

Static analysis

Data is read from **location** and passed to **the 'setAttribute()' function of a DOM element** via the following statement:

- `element.setAttribute(attr, location);`

3.2. https://192.168.1.193:7443/adeptia/TransactionStatus.jsp

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/TransactionStatus.jsp**

Issue detail

The application may be vulnerable to DOM-based DOM data manipulation. Data is read from **location** and passed to **the 'setAttribute()' function of a DOM element**.

Request 1

```
GET /adeptia/TransactionStatus.jsp HTTP/1.1
Host: 192.168.1.193:7443
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Connection: close
X-Frame-Options: SAMEORIGIN
Content-Type: text/html;charset=utf-8
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: 0
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>

<link rel="stylesheet" href=/adeptia/css/ui.css type=
...[SNIP]...
</script>
<script type="text/javascript" src=/adeptia/js/beansupport.js></script>
...[SNIP]...
```

Request 2

```
GET /adeptia/js/beansupport.js HTTP/1.1
Host: 192.168.1.193:7443
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/69.0.3497.100 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: https://192.168.1.193:7443/adeptia/rememberPassword.jsp
Cookie: JSESSIONID=node0aiite2301smyc3n66dci78nv81
```

Response 2

```
HTTP/1.1 200 OK
Connection: close
Set-Cookie: JSESSIONID=node0aiite2301smyc3n66dci78nv81;Path=/adeptia; HttpOnly;Secure
Expires: Thu, 01 Jan 1970 00:00:00 GMT
X-Frame-Options: SAMEORIGIN
Last-Modified: Mon, 21 Dec 2020 07:53:28 GMT
Content-Type: application/javascript
Accept-Ranges: bytes
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Security-Policy: script-src 'self' 'unsafe-inline' 'unsafe-eval';
```

```
/*
* Bean editors support scripts
*/

var validationArray = new Array();
var permissionMask='711'
var userPermissionMask = 7;
var groupPermissionMask = 1;
var otherPermissionMask = 1;


...[SNIP]...
ation);
        var value = (pageTokens[uri] != null ? pageTokens[uri] : tokenValue);

        if(location.indexOf('?') != -1) {
            location = location + '&' + tokenName + '=' + value;
        } else {
            location = location + '?' + tokenName + '=' + value;
        }

        try {
            element.setAttribute(attr, location);
        } catch (e) {
            // attempted to set/update unsupported attribute
        }
    }
  }
}
```

Static analysis

Data is read from **location** and passed to **the 'setAttribute()' function of a DOM element** via the following statements:

- `location = location + '?' + tokenName + '=' + value;`
- `element.setAttribute(attr, location);`

3.3. https://192.168.1.193:7443/adeptia/TransactionStatus.jsp

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/TransactionStatus.jsp**

Issue detail

The application may be vulnerable to DOM-based DOM data manipulation. Data is read from **location** and passed to **the 'setAttribute()' function of a DOM element**.

Request 1

```
GET /adeptia/TransactionStatus.jsp HTTP/1.1
Host: 192.168.1.193:7443
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Connection: close
X-Frame-Options: SAMEORIGIN
Content-Type: text/html;charset=utf-8
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: 0
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>

<link rel="stylesheet" href=/adeptia/css/ui.css type=
...[SNIP]...
</script>
<script type="text/javascript" src=/adeptia/js/beansupport.js></script>
...[SNIP]...
```

Request 2

```
GET /adeptia/js/beansupport.js HTTP/1.1
Host: 192.168.1.193:7443
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/69.0.3497.100 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: https://192.168.1.193:7443/adeptia/rememberPassword.jsp
Cookie: JSESSIONID=node0aiite2301smyc3n66dci78nv81
```

Response 2

```
HTTP/1.1 200 OK
Connection: close
Set-Cookie: JSESSIONID=node0aiite2301smyc3n66dci78nv81;Path=/adeptia; HttpOnly;Secure
Expires: Thu, 01 Jan 1970 00:00:00 GMT
X-Frame-Options: SAMEORIGIN
```

```
Last-Modified: Mon, 21 Dec 2020 07:53:28 GMT
Content-Type: application/javascript
Accept-Ranges: bytes
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Security-Policy: script-src 'self' 'unsafe-inline' 'unsafe-eval';


/*
* Bean editors support scripts
*/

var validationArray = new Array();
var permissionMask='711'
var userPermissionMask = 7;
var groupPermissionMask = 1;
var otherPermissionMask = 1;


...[SNIP]...
(location != null && isValidUrl(location)) {
        var uri = parseUri(location);
        var value = (pageTokens[uri] != null ? pageTokens[uri] : tokenValue);

        if(location.indexOf('?') != -1) {
            location = location + '&' + tokenName + '=' + value;
        } else {
            location = location + '?' + tokenName + '=' + value;
        }

        try {
            element.setAttribute(attr, location);
        } catch (e) {
            // attempted to set/update unsupported attribute
        }
    }
  }
}
```

Static analysis

Data is read from **location** and passed to **the 'setAttribute()' function of a DOM element** via the following statements:

- `location = location + '&' + tokenName + '=' + value;`
- `element.setAttribute(attr, location);`

3.4. https://192.168.1.193:7443/adeptia/control/datainterfaceslog.jsp

Summary

Severity:	**Information**
Confidence:	**Firm**

Host: **https://192.168.1.193:7443**

Path: **/adeptia/control/datainterfaceslog.jsp**

Issue detail

The application may be vulnerable to DOM-based DOM data manipulation. Data is read from **location** and passed to **the 'setAttribute()' function of a DOM element**.

Request 1

```
GET /adeptia/control/datainterfaceslog.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1.node0; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoV
C9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWl
l1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBwWQ0KdDVZUERkVWI
xd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktwe
WJuUQ0KbWU2dFFTdXVOZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsO
WRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2eWkrZ1AwL0wxRjNScTB5N1hndGNaQWt
mT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nT
GNXUE1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY2
1sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJScktySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRR
aE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBhbg0KQWpSR
WpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnR
WeDhuYzNTbQ0KVWxBaDZYWWpRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURN
NjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRmQ3bmV0cEF0cnptYnNBZTdmeGQv
Tys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEI1ZkwzZnNRQ
kVtNitGeHpGRGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0
x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuo
VilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6; lastService=CustomDashboard
```

Response 1

```
HTTP/1.1 200 OK
Connection: close
X-Frame-Options: SAMEORIGIN
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Content-Type: text/html;ISO-8859-1
Cache-Control: no-cache
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
```

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css" /
...[SNIP]...
</script>
<script type="text/javascript" src=/adeptia/js/beansupport.js></script>
...[SNIP]...
```

Request 2

```
GET /adeptia/js/beansupport.js HTTP/1.1
Host: 192.168.1.193:7443
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/69.0.3497.100 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: https://192.168.1.193:7443/adeptia/rememberPassword.jsp
Cookie: JSESSIONID=node0aiite2301smyc3n66dci78nv81
```

Response 2

```
HTTP/1.1 200 OK
Connection: close
Set-Cookie: JSESSIONID=node0aiite2301smyc3n66dci78nv81;Path=/adeptia; HttpOnly;Secure
Expires: Thu, 01 Jan 1970 00:00:00 GMT
X-Frame-Options: SAMEORIGIN
Last-Modified: Mon, 21 Dec 2020 07:53:28 GMT
Content-Type: application/javascript
Accept-Ranges: bytes
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Security-Policy: script-src 'self' 'unsafe-inline' 'unsafe-eval';


/*
* Bean editors support scripts
*/

var validationArray = new Array();
var permissionMask='711'
var userPermissionMask = 7;
var groupPermissionMask = 1;
var otherPermissionMask = 1;


...[SNIP]...
lue);

        if(location.indexOf('?') != -1) {
            location = location + '&' + tokenName + '=' + value;
        } else {
            location = location + '?' + tokenName + '=' + value;
```

```
        }

        try {
            element.setAttribute(attr, location);
        } catch (e) {
            // attempted to set/update unsupported attribute
        }
    }
  }
}
```

Static analysis

Data is read from **location** and passed to **the 'setAttribute()' function of a DOM element** via the following statement:

- `element.setAttribute(attr, location);`

3.5. https://192.168.1.193:7443/adeptia/control/datainterfaceslog.jsp

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/datainterfaceslog.jsp**

Issue detail

The application may be vulnerable to DOM-based DOM data manipulation. Data is read from **location** and passed to **the 'setAttribute()' function of a DOM element**.

Request 1

```
GET /adeptia/control/datainterfaceslog.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1.node0; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoV
C9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWl
l1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBwWQ0KdDVZUERkVWl
xd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktwe
```

```
WJuUQ0KbWU2dFFTdXVOZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsO
WRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2eWkrZ1AwL0wxRjNScTB5N1hndGNaQWt
mT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nT
GNXUE1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY2
1sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJScktySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRR
aE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBhbg0KQWpSR
WpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnR
WeDhuYzNTbQ0KVWxBaDZYWWpRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURN
NjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRmQ3bmV0cEF0cnptYnNBZTdmeGQv
Tys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEI1ZkwzZnNRQ
kVtNitGeHpGRGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0
x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuo
VilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6; lastService=CustomDashboard
```

Response 1

```
HTTP/1.1 200 OK
Connection: close
X-Frame-Options: SAMEORIGIN
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Content-Type: text/html;ISO-8859-1
Cache-Control: no-cache
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css" /
...[SNIP]...
</script>
<script type="text/javascript" src=/adeptia/js/beansupport.js></script>
...[SNIP]...
```

Request 2

```
GET /adeptia/js/beansupport.js HTTP/1.1
Host: 192.168.1.193:7443
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/69.0.3497.100 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: https://192.168.1.193:7443/adeptia/rememberPassword.jsp
Cookie: JSESSIONID=node0aiite2301smyc3n66dci78nv81
```

Response 2

```
HTTP/1.1 200 OK
```

```
Connection: close
Set-Cookie: JSESSIONID=node0aiite2301smyc3n66dci78nv81;Path=/adeptia; HttpOnly;Secure
Expires: Thu, 01 Jan 1970 00:00:00 GMT
X-Frame-Options: SAMEORIGIN
Last-Modified: Mon, 21 Dec 2020 07:53:28 GMT
Content-Type: application/javascript
Accept-Ranges: bytes
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Security-Policy: script-src 'self' 'unsafe-inline' 'unsafe-eval';


/*
* Bean editors support scripts
*/

var validationArray = new Array();
var permissionMask='711'
var userPermissionMask = 7;
var groupPermissionMask = 1;
var otherPermissionMask = 1;


...[SNIP]...
ation);
        var value = (pageTokens[uri] != null ? pageTokens[uri] : tokenValue);

        if(location.indexOf('?') != -1) {
            location = location + '&' + tokenName + '=' + value;
        } else {
            location = location + '?' + tokenName + '=' + value;
        }

        try {
            element.setAttribute(attr, location);
        } catch (e) {
            // attempted to set/update unsupported attribute
        }
    }
  }
}
```

Static analysis

Data is read from **location** and passed to **the 'setAttribute()' function of a DOM element** via the following statements:

- `location = location + '?' + tokenName + '=' + value;`
- `element.setAttribute(attr, location);`

3.6. https://192.168.1.193:7443/adeptia/control/datainterfaceslog.jsp

Summary

Severity: **Information**

Confidence: **Firm**

Host: **https://192.168.1.193:7443**

Path: **/adeptia/control/datainterfaceslog.jsp**

Issue detail

The application may be vulnerable to DOM-based DOM data manipulation. Data is read from **location** and passed to **the 'setAttribute()' function of a DOM element**.

Request 1

GET /adeptia/control/datainterfaceslog.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1.node0; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoV
C9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWl
l1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBwWQ0KdDVZUERkVWl
xd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktwe
WJuUQ0KbWU2dFFTdXVOZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsO
WRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2eWkrZ1AwL0wxRjNScTB5N1hndGNaQWt
mT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nT
GNXUE1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY2
1sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJScktySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRR
aE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBhbg0KQWpSR
WpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnR
WeDhuYzNTbQ0KVWxBaDZYWWpRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURN
NjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRmQ3bmV0cEF0cnptYnNBZTdmeGQv
Tys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEI1ZkwzZnNRQ
kVtNitGeHpGRGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0
x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuo
VilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6; lastService=CustomDashboard

Response 1

HTTP/1.1 200 OK
Connection: close
X-Frame-Options: SAMEORIGIN
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Content-Type: text/html;ISO-8859-1
Cache-Control: no-cache
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Strict-Transport-Security: max-age=31536000 ; includeSubDomains

```
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css" /
...[SNIP]...
</script>
<script type="text/javascript" src=/adeptia/js/beansupport.js></script>
...[SNIP]...
```

Request 2

```
GET /adeptia/js/beansupport.js HTTP/1.1
Host: 192.168.1.193:7443
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/69.0.3497.100 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: https://192.168.1.193:7443/adeptia/rememberPassword.jsp
Cookie: JSESSIONID=node0aiite2301smyc3n66dci78nv81
```

Response 2

```
HTTP/1.1 200 OK
Connection: close
Set-Cookie: JSESSIONID=node0aiite2301smyc3n66dci78nv81;Path=/adeptia; HttpOnly;Secure
Expires: Thu, 01 Jan 1970 00:00:00 GMT
X-Frame-Options: SAMEORIGIN
Last-Modified: Mon, 21 Dec 2020 07:53:28 GMT
Content-Type: application/javascript
Accept-Ranges: bytes
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Security-Policy: script-src 'self' 'unsafe-inline' 'unsafe-eval';


/*
* Bean editors support scripts
*/

var validationArray = new Array();
var permissionMask='711'
var userPermissionMask = 7;
var groupPermissionMask = 1;
var otherPermissionMask = 1;


...[SNIP]...
(location != null && isValidUrl(location)) {
        var uri = parseUri(location);
        var value = (pageTokens[uri] != null ? pageTokens[uri] : tokenValue);
```

```
        if(location.indexOf('?') != -1) {
            location = location + '&' + tokenName + '=' + value;
        } else {
            location = location + '?' + tokenName + '=' + value;
        }

        try {
            element.setAttribute(attr, location);
        } catch (e) {
            // attempted to set/update unsupported attribute
        }
    }
  }
}
```

Static analysis

Data is read from **location** and passed to **the 'setAttribute()' function of a DOM element** via the following statements:

- `location = location + '&' + tokenName + '=' + value;`
- `element.setAttribute(attr, location);`

3.7. https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/eventMonitor.jsp**

Issue detail

The application may be vulnerable to DOM-based DOM data manipulation. Data is read from **location** and passed to **the 'setAttribute()' function of a DOM element**.

Request 1

```
GET /adeptia/control/eventMonitor.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3
Sec-Fetch-Site: same-origin
```

```
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoV
C9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWl
l1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBwWQ0KdDVZUERkVWl
xd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktwe
WJuUQ0KbWU2dFFTdXVOZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsO
WRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2eWkrZ1AwL0wxRjNScTB5N1hndGNaQWt
mT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nT
GNXUE1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY2
1sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJScktySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRR
aE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBhbg0KQWpSR
WpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnR
WeDhuYzNTbQ0KVWxBaDZYWWpRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURN
NjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRmQ3bmV0cEF0cnptYnNBZTdmeGQv
Tys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEI1ZkwzZnNRQ
kVtNitGeHpGRGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0
x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuo
VilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6; lastService=datainterfaceslog.jsp
```

Response 1

```
HTTP/1.1 200 OK
Connection: close
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Expires: Thu, 01 Jan 1970 00:00:00 GMT
X-Frame-Options: SAMEORIGIN
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css" />
...[SNIP]...
</script>
<script type="text/javascript" src=/adeptia/js/beansupport.js></script>
...[SNIP]...
```

Request 2

```
GET /adeptia/js/beansupport.js HTTP/1.1
Host: 192.168.1.193:7443
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/69.0.3497.100 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: https://192.168.1.193:7443/adeptia/rememberPassword.jsp
```

```
Cookie: JSESSIONID=node0aiite2301smyc3n66dci78nv81
```

Response 2

```
HTTP/1.1 200 OK
Connection: close
Set-Cookie: JSESSIONID=node0aiite2301smyc3n66dci78nv81;Path=/adeptia; HttpOnly;Secure
Expires: Thu, 01 Jan 1970 00:00:00 GMT
X-Frame-Options: SAMEORIGIN
Last-Modified: Mon, 21 Dec 2020 07:53:28 GMT
Content-Type: application/javascript
Accept-Ranges: bytes
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Security-Policy: script-src 'self' 'unsafe-inline' 'unsafe-eval';


/*
* Bean editors support scripts
*/

var validationArray = new Array();
var permissionMask='711'
var userPermissionMask = 7;
var groupPermissionMask = 1;
var otherPermissionMask = 1;


...[SNIP]...
lue);

        if(location.indexOf('?') != -1) {
            location = location + '&' + tokenName + '=' + value;
        } else {
            location = location + '?' + tokenName + '=' + value;
        }

        try {
            element.setAttribute(attr, location);
        } catch (e) {
            // attempted to set/update unsupported attribute
        }
    }
  }
}
```

Static analysis

Data is read from **location** and passed to **the 'setAttribute()' function of a DOM element** via the following statement:

- `element.setAttribute(attr, location);`

3.8. https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/eventMonitor.jsp**

Issue detail

The application may be vulnerable to DOM-based DOM data manipulation. Data is read from **location** and passed to **the 'setAttribute()' function of a DOM element**.

Request 1

```
GET /adeptia/control/eventMonitor.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoV
C9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWl
l1bVRud2NvQXJ3c0plUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBwWQ0KdDVZUERkVWl
xd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktwe
WJuUQ0KbWU2dFFTdXVOZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsO
WRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2eWkrZ1AwL0wxRjNScTB5N1hndGNaQWt
mT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nT
GNXUE1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY2
1sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJScktySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRR
aE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBhbg0KQWpSR
WpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnR
WeDhuYzNTbQ0KVWxBaDZYWWpRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURN
NjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRmQ3bmV0cEF0cnptYnNBZTdmeGQv
Tys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEI1ZkwzZnNRQ
kVtNitGeHpGRGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0
x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuo
VilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6; lastService=datainterfaceslog.jsp
```

Response 1

```
HTTP/1.1 200 OK
Connection: close
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Expires: Thu, 01 Jan 1970 00:00:00 GMT
```

```
X-Frame-Options: SAMEORIGIN
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css" />
...[SNIP]...
</script>
<script type="text/javascript" src=/adeptia/js/beansupport.js></script>
...[SNIP]...
```

Request 2

```
GET /adeptia/js/beansupport.js HTTP/1.1
Host: 192.168.1.193:7443
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/69.0.3497.100 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: https://192.168.1.193:7443/adeptia/rememberPassword.jsp
Cookie: JSESSIONID=node0aiite2301smyc3n66dci78nv81
```

Response 2

```
HTTP/1.1 200 OK
Connection: close
Set-Cookie: JSESSIONID=node0aiite2301smyc3n66dci78nv81;Path=/adeptia; HttpOnly;Secure
Expires: Thu, 01 Jan 1970 00:00:00 GMT
X-Frame-Options: SAMEORIGIN
Last-Modified: Mon, 21 Dec 2020 07:53:28 GMT
Content-Type: application/javascript
Accept-Ranges: bytes
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Security-Policy: script-src 'self' 'unsafe-inline' 'unsafe-eval';


/*
* Bean editors support scripts
*/

var validationArray = new Array();
var permissionMask='711'
var userPermissionMask = 7;
var groupPermissionMask = 1;
var otherPermissionMask = 1;
```

```
...[SNIP]...
ation);
        var value = (pageTokens[uri] != null ? pageTokens[uri] : tokenValue);

        if(location.indexOf('?') != -1) {
            location = location + '&' + tokenName + '=' + value;
        } else {
            location = location + '?' + tokenName + '=' + value;
        }

        try {
            element.setAttribute(attr, location);
        } catch (e) {
            // attempted to set/update unsupported attribute
        }
    }
  }
}
```

Static analysis

Data is read from **location** and passed to **the 'setAttribute()' function of a DOM element** via the following statements:

- `location = location + '?' + tokenName + '=' + value;`
- `element.setAttribute(attr, location);`

3.9. https://192.168.1.193:7443/adeptia/control/eventMonitor.jsp

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/eventMonitor.jsp**

Issue detail

The application may be vulnerable to DOM-based DOM data manipulation. Data is read from **location** and passed to **the 'setAttribute()' function of a DOM element**.

Request 1

```
GET /adeptia/control/eventMonitor.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
```

```
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoV
C9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWl
l1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBwWQ0KdDVZUERkVWl
xd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktwe
WJuUQ0KbWU2dFFTdXVOZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsO
WRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2eWkrZ1AwL0wxRjNScTB5N1hndGNaQWt
mT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nT
GNXUE1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY2
1sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJScktySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRR
aE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBhbg0KQWpSR
WpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnR
WeDhuYzNTbQ0KVWxBaDZYWWpRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURN
NjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRmQ3bmV0cEF0cnptYnNBZTdmeGQv
Tys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEI1ZkwzZnNRQ
kVtNitGeHpGRGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0
x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuo
VilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6; lastService=datainterfaceslog.jsp
```

Response 1

```
HTTP/1.1 200 OK
Connection: close
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Expires: Thu, 01 Jan 1970 00:00:00 GMT
X-Frame-Options: SAMEORIGIN
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css" />
...[SNIP]...
</script>
<script type="text/javascript" src=/adeptia/js/beansupport.js></script>
...[SNIP]...
```

Request 2

```
GET /adeptia/js/beansupport.js HTTP/1.1
Host: 192.168.1.193:7443
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
```

```
Chrome/69.0.3497.100 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: https://192.168.1.193:7443/adeptia/rememberPassword.jsp
Cookie: JSESSIONID=node0aiite2301smyc3n66dci78nv81
```

Response 2

```
HTTP/1.1 200 OK
Connection: close
Set-Cookie: JSESSIONID=node0aiite2301smyc3n66dci78nv81;Path=/adeptia; HttpOnly;Secure
Expires: Thu, 01 Jan 1970 00:00:00 GMT
X-Frame-Options: SAMEORIGIN
Last-Modified: Mon, 21 Dec 2020 07:53:28 GMT
Content-Type: application/javascript
Accept-Ranges: bytes
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Security-Policy: script-src 'self' 'unsafe-inline' 'unsafe-eval';


/*
* Bean editors support scripts
*/

var validationArray = new Array();
var permissionMask='711'
var userPermissionMask = 7;
var groupPermissionMask = 1;
var otherPermissionMask = 1;


...[SNIP]...
(location != null && isValidUrl(location)) {
        var uri = parseUri(location);
        var value = (pageTokens[uri] != null ? pageTokens[uri] : tokenValue);

        if(location.indexOf('?') != -1) {
            location = location + '&' + tokenName + '=' + value;
        } else {
            location = location + '?' + tokenName + '=' + value;
        }

        try {
            element.setAttribute(attr, location);
        } catch (e) {
            // attempted to set/update unsupported attribute
        }
    }
  }
}
```

Static analysis

Data is read from **location** and passed to **the 'setAttribute()' function of a DOM element** via the following statements:

- `location = location + '&' + tokenName + '=' + value;`
- `element.setAttribute(attr, location);`

3.10. https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/monitorsPerformance.jsp**

Issue detail

The application may be vulnerable to DOM-based DOM data manipulation. Data is read from **location** and passed to **the 'setAttribute()' function of a DOM element**.

Request 1

GET /adeptia/control/monitorsPerformance.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1.node0; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoV
C9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWl
l1bVRud2NvQXJ3c0plUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBwWQ0KdDVZUERkVWI
xd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktwe
WJuUQ0KbWU2dFFTdXVOZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsO
WRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2eWkrZ1AwL0wxRjNScTB5N1hndGNaQWt
mT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nT
GNXUE1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY2
1sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJScktySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRR
aE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBhbg0KQWpSR
WpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnR
WeDhuYzNTbQ0KVWxBaDZYWWpRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURN
NjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRmQ3bmV0cEF0cnptYnNBZTdmeGQv
Tys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEI1ZkwzZnNRQ
kVtNitGeHpGRGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0
x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuo
VilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6; lastService=SolutionMonitor

Response 1

```
HTTP/1.1 200 OK
Connection: close
X-Frame-Options: SAMEORIGIN
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css" />
...[SNIP]...
</script>
<script type="text/javascript" src=/adeptia/js/beansupport.js></script>
...[SNIP]...
```

Request 2

```
GET /adeptia/js/beansupport.js HTTP/1.1
Host: 192.168.1.193:7443
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/69.0.3497.100 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: https://192.168.1.193:7443/adeptia/rememberPassword.jsp
Cookie: JSESSIONID=node0aiite2301smyc3n66dci78nv81
```

Response 2

```
HTTP/1.1 200 OK
Connection: close
Set-Cookie: JSESSIONID=node0aiite2301smyc3n66dci78nv81;Path=/adeptia; HttpOnly;Secure
Expires: Thu, 01 Jan 1970 00:00:00 GMT
X-Frame-Options: SAMEORIGIN
Last-Modified: Mon, 21 Dec 2020 07:53:28 GMT
Content-Type: application/javascript
Accept-Ranges: bytes
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Security-Policy: script-src 'self' 'unsafe-inline' 'unsafe-eval';


/*
* Bean editors support scripts
```

```
*/

var validationArray = new Array();
var permissionMask='711'
var userPermissionMask = 7;
var groupPermissionMask = 1;
var otherPermissionMask = 1;


...[SNIP]...
lue);

        if(location.indexOf('?') != -1) {
            location = location + '&' + tokenName + '=' + value;
        } else {
            location = location + '?' + tokenName + '=' + value;
        }

        try {
            element.setAttribute(attr, location);
        } catch (e) {
            // attempted to set/update unsupported attribute
        }
    }
  }
}
```

Static analysis

Data is read from **location** and passed to **the 'setAttribute()' function of a DOM element** via the following statement:

- `element.setAttribute(attr, location);`

3.11. https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/monitorsPerformance.jsp**

Issue detail

The application may be vulnerable to DOM-based DOM data manipulation. Data is read from **location** and passed to **the 'setAttribute()' function of a DOM element**.

Request 1

```
GET /adeptia/control/monitorsPerformance.jsp HTTP/1.1
Host: 192.168.1.193:7443
```

```
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1.node0; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoV
C9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWl
l1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBwWQ0KdDVZUERkVWl
xd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktwe
WJuUQ0KbWU2dFFTdXVOZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsO
WRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2eWkrZ1AwL0wxRjNScTB5N1hndGNaQWt
mT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nT
GNXUE1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY2
1sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJScktySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRR
aE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBhbg0KQWpSR
WpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnR
WeDhuYzNTbQ0KVWxBaDZYWWpRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURN
NjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRmQ3bmV0cEF0cnptYnNBZTdmeGQv
Tys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEI1ZkwzZnNRQ
kVtNitGeHpGRGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0
x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuo
VilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6; lastService=SolutionMonitor
```

Response 1

```
HTTP/1.1 200 OK
Connection: close
X-Frame-Options: SAMEORIGIN
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css" />
...[SNIP]...
</script>
<script type="text/javascript" src=/adeptia/js/beansupport.js></script>
...[SNIP]...
```

Request 2

```
GET /adeptia/js/beansupport.js HTTP/1.1
```

```
Host: 192.168.1.193:7443
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/69.0.3497.100 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: https://192.168.1.193:7443/adeptia/rememberPassword.jsp
Cookie: JSESSIONID=node0aiite2301smyc3n66dci78nv81
```

Response 2

```
HTTP/1.1 200 OK
Connection: close
Set-Cookie: JSESSIONID=node0aiite2301smyc3n66dci78nv81;Path=/adeptia; HttpOnly;Secure
Expires: Thu, 01 Jan 1970 00:00:00 GMT
X-Frame-Options: SAMEORIGIN
Last-Modified: Mon, 21 Dec 2020 07:53:28 GMT
Content-Type: application/javascript
Accept-Ranges: bytes
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Security-Policy: script-src 'self' 'unsafe-inline' 'unsafe-eval';


/*
* Bean editors support scripts
*/

var validationArray = new Array();
var permissionMask='711'
var userPermissionMask = 7;
var groupPermissionMask = 1;
var otherPermissionMask = 1;


...[SNIP]...
ation);
        var value = (pageTokens[uri] != null ? pageTokens[uri] : tokenValue);

        if(location.indexOf('?') != -1) {
            location = location + '&' + tokenName + '=' + value;
        } else {
            location = location + '?' + tokenName + '=' + value;
        }

        try {
            element.setAttribute(attr, location);
        } catch (e) {
            // attempted to set/update unsupported attribute
        }
    }
  }
}
```

Static analysis

Data is read from **location** and passed to **the 'setAttribute()' function of a DOM element** via the following statements:

- `location = location + '?' + tokenName + '=' + value;`
- `element.setAttribute(attr, location);`

3.12. https://192.168.1.193:7443/adeptia/control/monitorsPerformance.jsp

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/monitorsPerformance.jsp**

Issue detail

The application may be vulnerable to DOM-based DOM data manipulation. Data is read from **location** and passed to **the 'setAttribute()' function of a DOM element**.

Request 1

GET /adeptia/control/monitorsPerformance.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1.node0; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoV
C9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWl
l1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBwWQ0KdDVZUERkVWl
xd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktwe
WJuUQ0KbWU2dFFTdXVOZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsO
WRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2eWkrZ1AwL0wxRjNScTB5N1hndGNaQWt
mT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nT
GNXUE1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY2
1sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJScktySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRR
aE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBhbg0KQWpSR
WpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnR
WeDhuYzNTbQ0KVWxBaDZYWWpRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURN
NjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRmQ3bmV0cEF0cnptYnNBZTdmeGQv
Tys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEI1ZkwzZnNRQ

```
kVtNitGeHpGRGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0
x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuo
VilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6; lastService=SolutionMonitor
```

Response 1

```
HTTP/1.1 200 OK
Connection: close
X-Frame-Options: SAMEORIGIN
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css" />
...[SNIP]...
</script>
<script type="text/javascript" src=/adeptia/js/beansupport.js></script>
...[SNIP]...
```

Request 2

```
GET /adeptia/js/beansupport.js HTTP/1.1
Host: 192.168.1.193:7443
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/69.0.3497.100 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: https://192.168.1.193:7443/adeptia/rememberPassword.jsp
Cookie: JSESSIONID=node0aiite2301smyc3n66dci78nv81
```

Response 2

```
HTTP/1.1 200 OK
Connection: close
Set-Cookie: JSESSIONID=node0aiite2301smyc3n66dci78nv81;Path=/adeptia; HttpOnly;Secure
Expires: Thu, 01 Jan 1970 00:00:00 GMT
X-Frame-Options: SAMEORIGIN
Last-Modified: Mon, 21 Dec 2020 07:53:28 GMT
Content-Type: application/javascript
Accept-Ranges: bytes
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
```

```
Content-Security-Policy: script-src 'self' 'unsafe-inline' 'unsafe-eval';


/*
* Bean editors support scripts
*/

var validationArray = new Array();
var permissionMask='711'
var userPermissionMask = 7;
var groupPermissionMask = 1;
var otherPermissionMask = 1;


...[SNIP]...
(location != null && isValidUrl(location)) {
        var uri = parseUri(location);
        var value = (pageTokens[uri] != null ? pageTokens[uri] : tokenValue);

        if(location.indexOf('?') != -1) {
            location = location + '&' + tokenName + '=' + value;
        } else {
            location = location + '?' + tokenName + '=' + value;
        }

        try {
            element.setAttribute(attr, location);
        } catch (e) {
            // attempted to set/update unsupported attribute
        }
    }
  }
}
```

Static analysis

Data is read from **location** and passed to **the 'setAttribute()' function of a DOM element** via the following statements:

- `location = location + '&' + tokenName + '=' + value;`
- `element.setAttribute(attr, location);`

3.13. https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/reportUsageGUI.jsp**

Issue detail

The application may be vulnerable to DOM-based DOM data manipulation. Data is read from **location** and passed to **the 'setAttribute()' function of a DOM element**.

Request 1

```
GET /adeptia/control/reportUsageGUI.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1.node0; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoV
C9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWl
l1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBwWQ0KdDVZUERkVWl
xd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktwe
WJuUQ0KbWU2dFFTdXVOZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsO
WRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2eWkrZ1AwL0wxRjNScTB5N1hndGNaQWt
mT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nT
GNXUE1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY2
1sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJScktySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRR
aE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBhbg0KQWpSR
WpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnR
WeDhuYzNTbQ0KVWxBaDZYWWpRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURN
NjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRmQ3bmV0cEF0cnptYnNBZTdmeGQv
Tys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEI1ZkwzZnNRQ
kVtNitGeHpGRGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0
x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuo
VilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6; lastService=IndigoReportLimited
```

Response 1

```
HTTP/1.1 200 OK
Connection: close
X-Frame-Options: SAMEORIGIN
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
```

```
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css"
...[SNIP]...
</script>
<script type="text/javascript" src=/adeptia/js/beansupport.js></script>
...[SNIP]...
```

Request 2

```
GET /adeptia/js/beansupport.js HTTP/1.1
Host: 192.168.1.193:7443
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/69.0.3497.100 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: https://192.168.1.193:7443/adeptia/rememberPassword.jsp
Cookie: JSESSIONID=node0aiite2301smyc3n66dci78nv81
```

Response 2

```
HTTP/1.1 200 OK
Connection: close
Set-Cookie: JSESSIONID=node0aiite2301smyc3n66dci78nv81;Path=/adeptia; HttpOnly;Secure
Expires: Thu, 01 Jan 1970 00:00:00 GMT
X-Frame-Options: SAMEORIGIN
Last-Modified: Mon, 21 Dec 2020 07:53:28 GMT
Content-Type: application/javascript
Accept-Ranges: bytes
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Security-Policy: script-src 'self' 'unsafe-inline' 'unsafe-eval';


/*
* Bean editors support scripts
*/

var validationArray = new Array();
var permissionMask='711'
var userPermissionMask = 7;
var groupPermissionMask = 1;
var otherPermissionMask = 1;


...[SNIP]...
lue);

        if(location.indexOf('?') != -1) {
            location = location + '&' + tokenName + '=' + value;
        } else {
            location = location + '?' + tokenName + '=' + value;
        }

        try {
            element.setAttribute(attr, location);
```

```
        } catch (e) {
            // attempted to set/update unsupported attribute
        }
    }
  }
}
```

Static analysis

Data is read from **location** and passed to **the 'setAttribute()' function of a DOM element** via the following statement:

- `element.setAttribute(attr, location);`

3.14. https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/control/reportUsageGUI.jsp**

Issue detail

The application may be vulnerable to DOM-based DOM data manipulation. Data is read from **location** and passed to **the 'setAttribute()' function of a DOM element**.

Request 1

```
GET /adeptia/control/reportUsageGUI.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1.node0; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoV
C9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWl
l1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBwWQ0KdDVZUERkVWl
xd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktwe
WJuUQ0KbWU2dFFTdXVOZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsO
WRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2eWkrZ1AwL0wxRjNScTB5N1hndGNaQWt
mT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nT
```

GNXUE1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY2
1sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJScktySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRR
aE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBhbg0KQWpSR
WpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnR
WeDhuYzNTbQ0KVWxBaDZYWWpRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURN
NjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRmQ3bmV0cEF0cnptYnNBZTdmeGQv
Tys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEI1ZkwzZnNRQ
kVtNitGeHpGRGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0
x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuo
VilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6; lastService=IndigoReportLimited

Response 1

```
HTTP/1.1 200 OK
Connection: close
X-Frame-Options: SAMEORIGIN
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css"
...[SNIP]...
</script>
<script type="text/javascript" src=/adeptia/js/beansupport.js></script>
...[SNIP]...
```

Request 2

```
GET /adeptia/js/beansupport.js HTTP/1.1
Host: 192.168.1.193:7443
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/69.0.3497.100 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: https://192.168.1.193:7443/adeptia/rememberPassword.jsp
Cookie: JSESSIONID=node0aiite2301smyc3n66dci78nv81
```

Response 2

```
HTTP/1.1 200 OK
Connection: close
Set-Cookie: JSESSIONID=node0aiite2301smyc3n66dci78nv81;Path=/adeptia; HttpOnly;Secure
Expires: Thu, 01 Jan 1970 00:00:00 GMT
```

```
X-Frame-Options: SAMEORIGIN
Last-Modified: Mon, 21 Dec 2020 07:53:28 GMT
Content-Type: application/javascript
Accept-Ranges: bytes
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Security-Policy: script-src 'self' 'unsafe-inline' 'unsafe-eval';


/*
* Bean editors support scripts
*/

var validationArray = new Array();
var permissionMask='711'
var userPermissionMask = 7;
var groupPermissionMask = 1;
var otherPermissionMask = 1;


...[SNIP]...
ation);
        var value = (pageTokens[uri] != null ? pageTokens[uri] : tokenValue);

        if(location.indexOf('?') != -1) {
            location = location + '&' + tokenName + '=' + value;
        } else {
            location = location + '?' + tokenName + '=' + value;
        }

        try {
            element.setAttribute(attr, location);
        } catch (e) {
            // attempted to set/update unsupported attribute
        }
    }
  }
}
```

Static analysis

Data is read from **location** and passed to **the 'setAttribute()' function of a DOM element** via the following statements:

- `location = location + '?' + tokenName + '=' + value;`
- `element.setAttribute(attr, location);`

3.15. https://192.168.1.193:7443/adeptia/control/reportUsageGUI.jsp

Summary

Severity:	**Information**
Confidence:	**Firm**

Host: **https://192.168.1.193:7443**

Path: **/adeptia/control/reportUsageGUI.jsp**

Issue detail

The application may be vulnerable to DOM-based DOM data manipulation. Data is read from **location** and passed to **the 'setAttribute()' function of a DOM element**.

Request 1

```
GET /adeptia/control/reportUsageGUI.jsp HTTP/1.1
Host: 192.168.1.193:7443
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/76.0.3809.100 Safari/537.36
Sec-Fetch-Mode: nested-navigate
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3
Sec-Fetch-Site: same-origin
Referer: https://192.168.1.193:7443/adeptia/control
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1.node0; OLD_TOKEN=; ext-enterprise-viewport=o%3A;
ACCESS_TOKEN=eyJhbGciOiJIUzI1NiIsImVuYyI6IlNIQS0yNTYifQ.OWpXVzNvblBMOG5Db1hsbmVHbktpQXZlWVRoV
C9Vc2Q0RXlCSCtrWEtkMCtQU3hCanh6NkJNdkl2ZzJLVEt2U0tLT1FrYXpRcTEvaQ0KaXl5MjkyOWxLcUdsTWFnL2xoWl
l1bVRud2NvQXJ3c0pIUjVqVDRJaStuZHJUWi9FSTlZay9WVk9rZ28yS01TNS9xOUVwcE44UVBwWQ0KdDVZUERkVWl
xd0oweFB6UjNtQUJOUnBmQ3R6R1N2SS94T01YZzVWSFJVbUdzZFgvNmU3OW9jMXB2OU5vT2VLeStPWFpUUktwe
WJuUQ0KbWU2dFFTdXVOZGxodXNvUENhRXNiVnhGYWdTVVBGZy9TdE1vNE9pM1ArZk91WHNmOWRHbjA0b2VsO
WRFMzZnSTJaZ2NMNjlXZitkdw0KR1loMU44YUVaL0trOGVydXZxQVRSZzI2eWkrZ1AwL0wxRjNScTB5N1hndGNaQWt
mT0pVQ244YXd1Z29UZE9QWGF3cnhJRlJJTmVHcg0KbUJ3VDlqVW0rdkhvQzdlR1BWeHZjSnVIekNJYjJ3NTlMY29nT
GNXUE1YYVQ0bVFpS2tzcmpkRVVVZHFySlJ0THpOdlptblU0QkJZRQ0KWjBaTWVXU00xd29iWCt5dGFoMzhDRnREY2
1sM1NTc2Y2Q05GNFp2OW9UT2M1enk4Wlh3eGV2TnJScktySFoxbjYvY2RhVldSeUxJTQ0KVmJTM0U3V3FsRjlpQzRR
aE1jU0xxcnJyazdTcmlYdFhVSFZlY2Vlb3p3VGF6R2FQMU9jWDNCaE0vUjMvY2ZnWE1EVDJTcTZ1aXBhbg0KQWpSR
WpYaU1VK3RxMVdDNzh0WTJLdE05U2ptdVVVV2RMbWpudVNyK0JZa2o1NDlGdDVwbHdsTkdHSVRRMFVKT29oRnR
WeDhuYzNTbQ0KVWxBaDZYWWpRR05OK05RaWJFZlYrVUsyNnlXbUZTZjJOcFQ3UkZBa0RoS1NhNHNQZDdTaURN
NjZzc0MwT25lOFB4QktwSDlYcFoxRg0KcFlqM0tCUENaM01FVXJ2RHdWOXhpRmQ3bmV0cEF0cnptYnNBZTdmeGQv
Tys2dWNDOWp6SFRnNHBVZ3FTU3k1U3hvbEE1ODlXTDhhUw0KRkRONXBNL1RucUFNd1BmLzRKUEI1ZkwzZnNRQ
kVtNitGeHpGRGtvNEs4eEthL05XNTF6ZXlna0ZmV3ZKWEJZRXRpSHEwRzFTRGZtZQ0KY0lLb1h3MmkxYlVSSXN1M0
x1M1RCVHVIZ3k5VGlhQ21kVnBtM2N3aFdncWdzVGFIQmU1MERURjJNU0thTVBpTWRKM21Zdz09.rCpKzOpX4qKFuo
VilrWntJnUyYm-faAP97LIlFPCB3c; jwtid=FSpcFL9wM0Pnhb5dTlMaY6IV/VEJHIM6; lastService=IndigoReportLimited
```

Response 1

```
HTTP/1.1 200 OK
Connection: close
X-Frame-Options: SAMEORIGIN
Set-Cookie: JSESSIONID=node0949ckkou5nbfxdj1o3okv52c1;Path=/adeptia; HttpOnly;Secure
Content-Type: text/html;ISO-8859-1;charset=iso-8859-1
Cache-Control: no-cache
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
```

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css"
...[SNIP]...
</script>
<script type="text/javascript" src=/adeptia/js/beansupport.js></script>
...[SNIP]...
```

Request 2

```
GET /adeptia/js/beansupport.js HTTP/1.1
Host: 192.168.1.193:7443
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/69.0.3497.100 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: https://192.168.1.193:7443/adeptia/rememberPassword.jsp
Cookie: JSESSIONID=node0aiite2301smyc3n66dci78nv81
```

Response 2

```
HTTP/1.1 200 OK
Connection: close
Set-Cookie: JSESSIONID=node0aiite2301smyc3n66dci78nv81;Path=/adeptia; HttpOnly;Secure
Expires: Thu, 01 Jan 1970 00:00:00 GMT
X-Frame-Options: SAMEORIGIN
Last-Modified: Mon, 21 Dec 2020 07:53:28 GMT
Content-Type: application/javascript
Accept-Ranges: bytes
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Security-Policy: script-src 'self' 'unsafe-inline' 'unsafe-eval';


/*
* Bean editors support scripts
*/

var validationArray = new Array();
var permissionMask='711'
var userPermissionMask = 7;
var groupPermissionMask = 1;
var otherPermissionMask = 1;


...[SNIP]...
(location != null && isValidUrl(location)) {
        var uri = parseUri(location);
        var value = (pageTokens[uri] != null ? pageTokens[uri] : tokenValue);

        if(location.indexOf('?') != -1) {
```

```
            location = location + '&' + tokenName + '=' + value;
        } else {
            location = location + '?' + tokenName + '=' + value;
        }

        try {
            element.setAttribute(attr, location);
        } catch (e) {
            // attempted to set/update unsupported attribute
        }
    }
  }
}
```

Static analysis

Data is read from **location** and passed to **the 'setAttribute()' function of a DOM element** via the following statements:

- `location = location + '&' + tokenName + '=' + value;`
- `element.setAttribute(attr, location);`

3.16. https://192.168.1.193:7443/adeptia/js/beansupport.js

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/js/beansupport.js**

Issue detail

The application may be vulnerable to DOM-based DOM data manipulation. Data is read from **location** and passed to **the 'setAttribute()' function of a DOM element**.

Request 1

```
GET /adeptia/js/beansupport.js HTTP/1.1
Host: 192.168.1.193:7443
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/69.0.3497.100 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: https://192.168.1.193:7443/adeptia/rememberPassword.jsp
Cookie: JSESSIONID=node0aiite2301smyc3n66dci78nv81
```

Response 1

```
HTTP/1.1 200 OK
Connection: close
Set-Cookie: JSESSIONID=node0aiite2301smyc3n66dci78nv81;Path=/adeptia; HttpOnly;Secure
Expires: Thu, 01 Jan 1970 00:00:00 GMT
X-Frame-Options: SAMEORIGIN
Last-Modified: Mon, 21 Dec 2020 07:53:28 GMT
Content-Type: application/javascript
Accept-Ranges: bytes
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Security-Policy: script-src 'self' 'unsafe-inline' 'unsafe-eval';


/*
* Bean editors support scripts
*/

var validationArray = new Array();
var permissionMask='711'
var userPermissionMask = 7;
var groupPermissionMask = 1;
var otherPermissionMask = 1;


...[SNIP]...
lue);

        if(location.indexOf('?') != -1) {
            location = location + '&' + tokenName + '=' + value;
        } else {
            location = location + '?' + tokenName + '=' + value;
        }

        try {
            element.setAttribute(attr, location);
        } catch (e) {
            // attempted to set/update unsupported attribute
        }
    }
  }
}
```

Static analysis

Data is read from **location** and passed to **the 'setAttribute()' function of a DOM element** via the following statement:

- `element.setAttribute(attr, location);`

3.17. https://192.168.1.193:7443/adeptia/js/beansupport.js

Summary

Severity: **Information**

Confidence: **Firm**

Host: **https://192.168.1.193:7443**

Path: **/adeptia/js/beansupport.js**

Issue detail

The application may be vulnerable to DOM-based DOM data manipulation. Data is read from **location** and passed to **the 'setAttribute()' function of a DOM element**.

Request 1

```
GET /adeptia/js/beansupport.js HTTP/1.1
Host: 192.168.1.193:7443
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/69.0.3497.100 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: https://192.168.1.193:7443/adeptia/rememberPassword.jsp
Cookie: JSESSIONID=node0aiite2301smyc3n66dci78nv81
```

Response 1

```
HTTP/1.1 200 OK
Connection: close
Set-Cookie: JSESSIONID=node0aiite2301smyc3n66dci78nv81;Path=/adeptia; HttpOnly;Secure
Expires: Thu, 01 Jan 1970 00:00:00 GMT
X-Frame-Options: SAMEORIGIN
Last-Modified: Mon, 21 Dec 2020 07:53:28 GMT
Content-Type: application/javascript
Accept-Ranges: bytes
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Security-Policy: script-src 'self' 'unsafe-inline' 'unsafe-eval';


/*
* Bean editors support scripts
*/

var validationArray = new Array();
var permissionMask='711'
var userPermissionMask = 7;
var groupPermissionMask = 1;
var otherPermissionMask = 1;


...[SNIP]...
ation);
        var value = (pageTokens[uri] != null ? pageTokens[uri] : tokenValue);
```

```
        if(location.indexOf('?') != -1) {
            location = location + '&' + tokenName + '=' + value;
        } else {
            location = location + '?' + tokenName + '=' + value;
        }

        try {
            element.setAttribute(attr, location);
        } catch (e) {
            // attempted to set/update unsupported attribute
        }
    }
  }
}
```

Static analysis

Data is read from **location** and passed to **the 'setAttribute()' function of a DOM element** via the following statements:

- `location = location + '?' + tokenName + '=' + value;`
- `element.setAttribute(attr, location);`

3.18. https://192.168.1.193:7443/adeptia/js/beansupport.js

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/js/beansupport.js**

Issue detail

The application may be vulnerable to DOM-based DOM data manipulation. Data is read from **location** and passed to **the 'setAttribute()' function of a DOM element**.

Request 1

```
GET /adeptia/js/beansupport.js HTTP/1.1
Host: 192.168.1.193:7443
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/69.0.3497.100 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: https://192.168.1.193:7443/adeptia/rememberPassword.jsp
Cookie: JSESSIONID=node0aiite2301smyc3n66dci78nv81
```

Response 1

```
HTTP/1.1 200 OK
Connection: close
Set-Cookie: JSESSIONID=node0aiite2301smyc3n66dci78nv81;Path=/adeptia; HttpOnly;Secure
Expires: Thu, 01 Jan 1970 00:00:00 GMT
X-Frame-Options: SAMEORIGIN
Last-Modified: Mon, 21 Dec 2020 07:53:28 GMT
Content-Type: application/javascript
Accept-Ranges: bytes
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Security-Policy: script-src 'self' 'unsafe-inline' 'unsafe-eval';


/*
* Bean editors support scripts
*/

var validationArray = new Array();
var permissionMask='711'
var userPermissionMask = 7;
var groupPermissionMask = 1;
var otherPermissionMask = 1;


...[SNIP]...
(location != null && isValidUrl(location)) {
        var uri = parseUri(location);
        var value = (pageTokens[uri] != null ? pageTokens[uri] : tokenValue);

        if(location.indexOf('?') != -1) {
            location = location + '&' + tokenName + '=' + value;
        } else {
            location = location + '?' + tokenName + '=' + value;
        }

        try {
            element.setAttribute(attr, location);
        } catch (e) {
            // attempted to set/update unsupported attribute
        }
    }
  }
}
```

Static analysis

Data is read from **location** and passed to **the 'setAttribute()' function of a DOM element** via the following statements:

- `location = location + '&' + tokenName + '=' + value;`
- `element.setAttribute(attr, location);`

3.19. https://192.168.1.193:7443/adeptia/rememberPassword.jsp

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/rememberPassword.jsp**

Issue detail

The application may be vulnerable to DOM-based DOM data manipulation. Data is read from **location** and passed to **the 'setAttribute()' function of a DOM element**.

Request 1

```
GET /adeptia/rememberPassword.jsp HTTP/1.1
Host: 192.168.1.193:7443
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/69.0.3497.100 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: https://192.168.1.193:7443/adeptia/control/
Cookie: JSESSIONID=node01asd5cuxdxlfo1xo574ead44g055
```

Response 1

```
HTTP/1.1 200 OK
Connection: close
Set-Cookie: JSESSIONID=node01asd5cuxdxlfo1xo574ead44g055;Path=/adeptia; HttpOnly;Secure
Expires: Thu, 01 Jan 1970 00:00:00 GMT
X-Frame-Options: SAMEORIGIN
Content-Type: text/html;charset=utf-8
Cache-Control: no-cache
Pragma: no-cache
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Security-Policy: script-src 'self' 'unsafe-inline' 'unsafe-eval';
Content-Length: 1733


<title>Password Recovery</title>
<head>
    <link rel="stylesheet" href=/adeptia/css/ui.css type="text/css" />


    <meta http-equiv="Content-Type" content="text/html;">
```

```
    <
...[SNIP]...
</script>

    <script type="text/javascript" src=/adeptia/js/beansupport.js></script>
...[SNIP]...
```

Request 2

```
GET /adeptia/js/beansupport.js HTTP/1.1
Host: 192.168.1.193:7443
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/69.0.3497.100 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: https://192.168.1.193:7443/adeptia/rememberPassword.jsp
Cookie: JSESSIONID=node0aiite2301smyc3n66dci78nv81
```

Response 2

```
HTTP/1.1 200 OK
Connection: close
Set-Cookie: JSESSIONID=node0aiite2301smyc3n66dci78nv81;Path=/adeptia; HttpOnly;Secure
Expires: Thu, 01 Jan 1970 00:00:00 GMT
X-Frame-Options: SAMEORIGIN
Last-Modified: Mon, 21 Dec 2020 07:53:28 GMT
Content-Type: application/javascript
Accept-Ranges: bytes
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Security-Policy: script-src 'self' 'unsafe-inline' 'unsafe-eval';


/*
* Bean editors support scripts
*/

var validationArray = new Array();
var permissionMask='711'
var userPermissionMask = 7;
var groupPermissionMask = 1;
var otherPermissionMask = 1;


...[SNIP]...
lue);

        if(location.indexOf('?') != -1) {
            location = location + '&' + tokenName + '=' + value;
        } else {
            location = location + '?' + tokenName + '=' + value;
        }

        try {
```

```
            element.setAttribute(attr, location);
        } catch (e) {
            // attempted to set/update unsupported attribute
        }
    }
  }
}
```

Static analysis

Data is read from **location** and passed to **the 'setAttribute()' function of a DOM element** via the following statement:

- `element.setAttribute(attr, location);`

3.20. https://192.168.1.193:7443/adeptia/rememberPassword.jsp

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/rememberPassword.jsp**

Issue detail

The application may be vulnerable to DOM-based DOM data manipulation. Data is read from **location** and passed to **the 'setAttribute()' function of a DOM element**.

Request 1

```
GET /adeptia/rememberPassword.jsp HTTP/1.1
Host: 192.168.1.193:7443
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/69.0.3497.100 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: https://192.168.1.193:7443/adeptia/control/
Cookie: JSESSIONID=node01asd5cuxdxlfo1xo574ead44g055
```

Response 1

```
HTTP/1.1 200 OK
Connection: close
Set-Cookie: JSESSIONID=node01asd5cuxdxlfo1xo574ead44g055;Path=/adeptia; HttpOnly;Secure
Expires: Thu, 01 Jan 1970 00:00:00 GMT
X-Frame-Options: SAMEORIGIN
```

```
Content-Type: text/html;charset=utf-8
Cache-Control: no-cache
Pragma: no-cache
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Security-Policy: script-src 'self' 'unsafe-inline' 'unsafe-eval';
Content-Length: 1733


<title>Password Recovery</title>
<head>
	<link rel="stylesheet" href=/adeptia/css/ui.css type="text/css" />


	<meta http-equiv="Content-Type" content="text/html;">
	<
...[SNIP]...
</script>

	<script type="text/javascript" src=/adeptia/js/beansupport.js></script>
...[SNIP]...
```

Request 2

```
GET /adeptia/js/beansupport.js HTTP/1.1
Host: 192.168.1.193:7443
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/69.0.3497.100 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: https://192.168.1.193:7443/adeptia/rememberPassword.jsp
Cookie: JSESSIONID=node0aiite2301smyc3n66dci78nv81
```

Response 2

```
HTTP/1.1 200 OK
Connection: close
Set-Cookie: JSESSIONID=node0aiite2301smyc3n66dci78nv81;Path=/adeptia; HttpOnly;Secure
Expires: Thu, 01 Jan 1970 00:00:00 GMT
X-Frame-Options: SAMEORIGIN
Last-Modified: Mon, 21 Dec 2020 07:53:28 GMT
Content-Type: application/javascript
Accept-Ranges: bytes
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Security-Policy: script-src 'self' 'unsafe-inline' 'unsafe-eval';


/*
* Bean editors support scripts
*/

var validationArray = new Array();
```

```
var permissionMask='711'
var userPermissionMask = 7;
var groupPermissionMask = 1;
var otherPermissionMask = 1;


...[SNIP]...
ation);
        var value = (pageTokens[uri] != null ? pageTokens[uri] : tokenValue);

        if(location.indexOf('?') != -1) {
            location = location + '&' + tokenName + '=' + value;
        } else {
            location = location + '?' + tokenName + '=' + value;
        }

        try {
            element.setAttribute(attr, location);
        } catch (e) {
            // attempted to set/update unsupported attribute
        }
    }
  }
}
```

Static analysis

Data is read from **location** and passed to **the 'setAttribute()' function of a DOM element** via the following statements:

- `location = location + '?' + tokenName + '=' + value;`
- `element.setAttribute(attr, location);`

3.21. https://192.168.1.193:7443/adeptia/rememberPassword.jsp

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://192.168.1.193:7443**
Path:	**/adeptia/rememberPassword.jsp**

Issue detail

The application may be vulnerable to DOM-based DOM data manipulation. Data is read from **location** and passed to **the 'setAttribute()' function of a DOM element**.

Request 1

```
GET /adeptia/rememberPassword.jsp HTTP/1.1
Host: 192.168.1.193:7443
```

```
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/69.0.3497.100 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: https://192.168.1.193:7443/adeptia/control/
Cookie: JSESSIONID=node01asd5cuxdxlfo1xo574ead44g055
```

Response 1

```
HTTP/1.1 200 OK
Connection: close
Set-Cookie: JSESSIONID=node01asd5cuxdxlfo1xo574ead44g055;Path=/adeptia; HttpOnly;Secure
Expires: Thu, 01 Jan 1970 00:00:00 GMT
X-Frame-Options: SAMEORIGIN
Content-Type: text/html;charset=utf-8
Cache-Control: no-cache
Pragma: no-cache
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Security-Policy: script-src 'self' 'unsafe-inline' 'unsafe-eval';
Content-Length: 1733


<title>Password Recovery</title>
<head>
    <link rel="stylesheet" href=/adeptia/css/ui.css type="text/css" />


    <meta http-equiv="Content-Type" content="text/html;">
    <
...[SNIP]...
</script>

    <script type="text/javascript" src=/adeptia/js/beansupport.js></script>
...[SNIP]...
```

Request 2

```
GET /adeptia/js/beansupport.js HTTP/1.1
Host: 192.168.1.193:7443
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/69.0.3497.100 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: https://192.168.1.193:7443/adeptia/rememberPassword.jsp
Cookie: JSESSIONID=node0aiite2301smyc3n66dci78nv81
```

Response 2

```
HTTP/1.1 200 OK
Connection: close
Set-Cookie: JSESSIONID=node0aiite2301smyc3n66dci78nv81;Path=/adeptia; HttpOnly;Secure
Expires: Thu, 01 Jan 1970 00:00:00 GMT
X-Frame-Options: SAMEORIGIN
Last-Modified: Mon, 21 Dec 2020 07:53:28 GMT
Content-Type: application/javascript
Accept-Ranges: bytes
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Security-Policy: script-src 'self' 'unsafe-inline' 'unsafe-eval';


/*
* Bean editors support scripts
*/

var validationArray = new Array();
var permissionMask='711'
var userPermissionMask = 7;
var groupPermissionMask = 1;
var otherPermissionMask = 1;


...[SNIP]...
(location != null && isValidUrl(location)) {
        var uri = parseUri(location);
        var value = (pageTokens[uri] != null ? pageTokens[uri] : tokenValue);

        if(location.indexOf('?') != -1) {
            location = location + '&' + tokenName + '=' + value;
        } else {
            location = location + '?' + tokenName + '=' + value;
        }

        try {
            element.setAttribute(attr, location);
        } catch (e) {
            // attempted to set/update unsupported attribute
        }
    }
  }
}
```

Static analysis

Data is read from **location** and passed to **the 'setAttribute()' function of a DOM element** via the following statements:

- `location = location + '&' + tokenName + '=' + value;`
- `element.setAttribute(attr, location);`

---

4. Email addresses disclosed

There are 3 instances of this issue:

- /Mapper/rest/fetchproperties/serverconfigure
- /pd/rest/fetchproperties/serverconfigure
- /rest/fetchproperties/serverconfigure

Issue background

The presence of email addresses within application responses does not necessarily constitute a security vulnerability. Email addresses may appear intentionally within contact information, and many applications (such as web mail) include arbitrary third-party email addresses within their core content.

However, email addresses of developers and other individuals (whether appearing on-screen or hidden within page source) may disclose information that is useful to an attacker; for example, they may represent usernames that can be used at the application's login, and they may be used in social engineering attacks against the organization's personnel. Unnecessary or excessive disclosure of email addresses may also lead to an increase in the volume of spam email received.

Issue remediation

Consider removing any email addresses that are unnecessary, or replacing personal addresses with anonymous mailbox addresses (such as helpdesk@example.com).

To reduce the quantity of spam sent to anonymous mailbox addresses, consider hiding the email address and instead providing a form that generates the email server-side, protected by a CAPTCHA if necessary.

Vulnerability classifications

- CWE-200: Information Exposure

4.1. https://192.168.1.193:7843/Mapper/rest/fetchproperties/serverconfigure

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://192.168.1.193:7843**
Path:	**/Mapper/rest/fetchproperties/serverconfigure**

Issue detail

The following email address was disclosed in the response:

- help@adeptia.com

Request 1

```
GET /Mapper/rest/fetchproperties/serverconfigure HTTP/1.1
Host: 192.168.1.193:7843
```

```
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)
Connection: close
```

Response 1

```
HTTP/1.1 200
Connection: close
X-Frame-Options: SAMEORIGIN
X-Powered-By: Adeptia Connect
Cache-Control: no-cache
Expires: 0
Pragma: no-cache
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Security-Policy: script-src 'self' 'unsafe-inline' 'unsafe-eval';
vary: accept-encoding
Content-Type: text/plain
Date: Mon, 21 Dec 2020 10:40:58 GMT
Server: Adeptia

{"serverProperties":
{"isWSDL4jenabled":false,"cpuUsageThresHoldLimit":80,"isGACApplicable":true,"mapperFilterEmptyElements":false,"forc
edSAMLIDPLogoutEnabled":true,"characterSetEncoding":"UTF-
8","isWebMapperAutoSaveEnabled":true,"AIMapAdvancedMode":false,"contactMailForGUIErrorMessage":"help@adeptia
.com","productName":"Adeptia
Connect","SAMLSSORoleSwitchingAllowed":false,"isPlainFTPEnabled":true,"environmentName":"Development","isWebP
dAutoSaveEnabled":true,"acPortsJson":"{\\\"SoapServiceHttpPorts\\\"
...[SNIP]...
```

4.2. https://192.168.1.193:7843/pd/rest/fetchproperties/serverconfigure

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://192.168.1.193:7843**
Path:	**/pd/rest/fetchproperties/serverconfigure**

Issue detail

The following email address was disclosed in the response:

- help@adeptia.com

Request 1

```
GET /pd/rest/fetchproperties/serverconfigure HTTP/1.1
Host: 192.168.1.193:7843
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)
Connection: close
```

Response 1

```
HTTP/1.1 200
Connection: close
X-Frame-Options: SAMEORIGIN
X-Powered-By: Adeptia Connect
Cache-Control: no-cache
Expires: 0
Pragma: no-cache
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Security-Policy: script-src 'self' 'unsafe-inline' 'unsafe-eval';
vary: accept-encoding
Content-Type: text/plain
Date: Mon, 21 Dec 2020 10:40:58 GMT
Server: Adeptia

{"serverProperties":
{"isWSDL4jenabled":false,"cpuUsageThresHoldLimit":80,"isGACApplicable":true,"mapperFilterEmptyElements":false,"forc
edSAMLIDPLogoutEnabled":true,"characterSetEncoding":"UTF-
8","isWebMapperAutoSaveEnabled":true,"AIMapAdvancedMode":false,"contactMailForGUIErrorMessage":"help@adeptia
.com","productName":"Adeptia
Connect","SAMLSSORoleSwitchingAllowed":false,"isPlainFTPEnabled":true,"environmentName":"Development","isWebP
dAutoSaveEnabled":true,"acPortsJson":"{\\\"SoapServiceHttpPorts\\\"
...[SNIP]...
```

4.3. https://192.168.1.193:7843/rest/fetchproperties/serverconfigure

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://192.168.1.193:7843**
Path:	**/rest/fetchproperties/serverconfigure**

Issue detail

The following email address was disclosed in the response:

- help@adeptia.com

Request 1

```
GET /rest/fetchproperties/serverconfigure HTTP/1.1
Host: 192.168.1.193:7843
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)
Connection: close
```

Response 1

```
HTTP/1.1 200
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Cache-Control: no-cache
Content-Security-Policy: script-src 'self' 'unsafe-inline' 'unsafe-eval';
Connection: close
Expires: 0
Pragma: no-cache
X-Powered-By: Adeptia Connect
vary: accept-encoding
Content-Type: text/plain
Date: Mon, 21 Dec 2020 10:42:10 GMT
Server: Adeptia

{"serverProperties":
{"isWSDL4jenabled":false,"cpuUsageThresHoldLimit":80,"isGACApplicable":true,"mapperFilterEmptyElements":false,"forcedSAMLIDPLogoutEnabled":true,"characterSetEncoding":"UTF-8","isWebMapperAutoSaveEnabled":true,"AIMapAdvancedMode":false,"contactMailForGUIErrorMessage":"help@adeptia.com","productName":"Adeptia Connect","SAMLSSORoleSwitchingAllowed":false,"isPlainFTPEnabled":true,"environmentName":"Development","isWebPdAutoSaveEnabled":true,"acPortsJson":"{\\\"SoapServiceHttpPorts\\\"
...[SNIP]...
```

Report generated by Burp Suite web vulnerability scanner v2.1.01, at Thu Jan 14 17:56:04 IST 2021.