

# **ZAP Vulnerability Report**

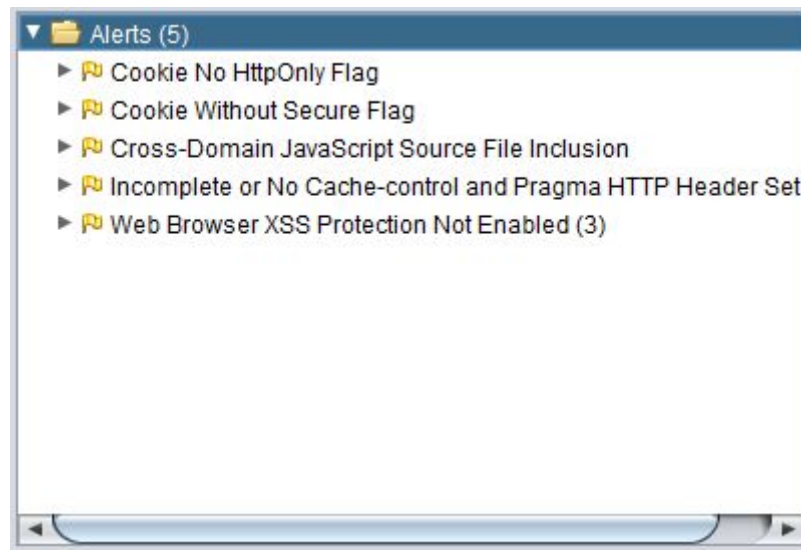
## **08/06/18**

Authors:

Chiranjeev RAMDIN

Konalsing PERMESSUR

# Vulnerabilities detected by Owasp ZAP:



## 1. Cookie No HttpOnly Flag



### Description:

A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then

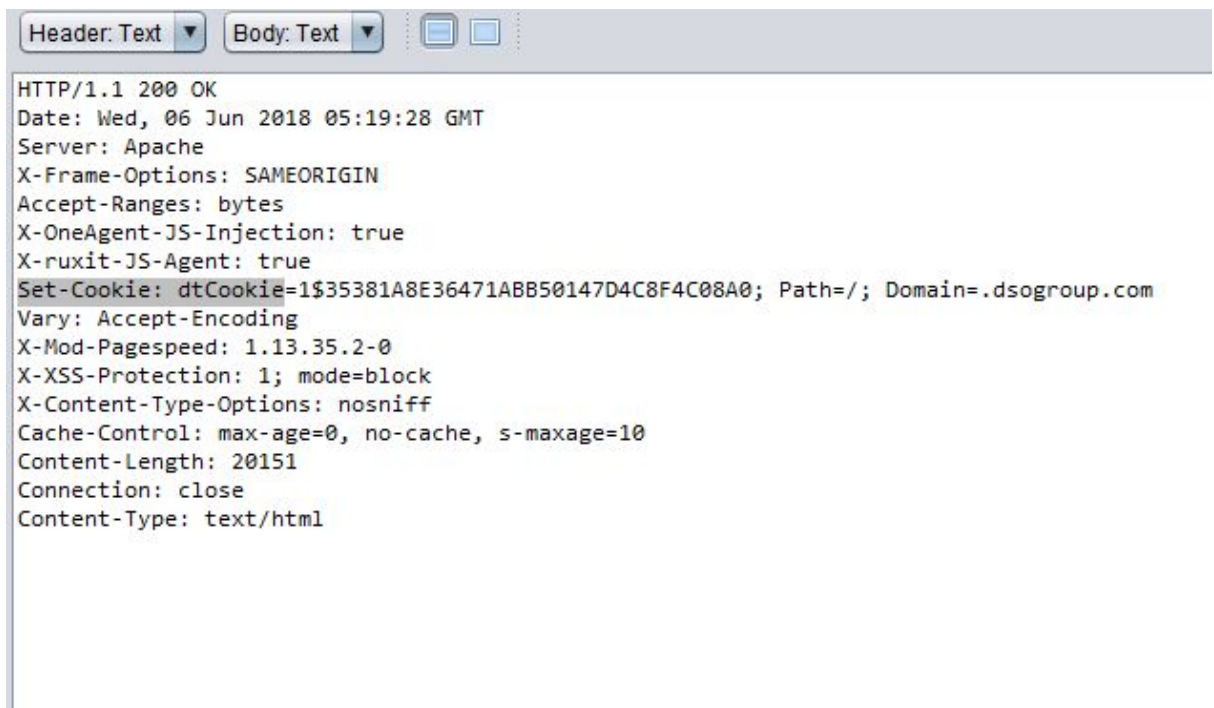
the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

## Request and Response



Header: Text ▼ Body: Text ▼

```
GET https://dso.mars-recette.dsogroup.com/ HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0;)
Pragma: no-cache
Cache-Control: no-cache
Content-Length: 0
Host: dso.mars-recette.dsogroup.com
```



Header: Text ▼ Body: Text ▼

```
HTTP/1.1 200 OK
Date: Wed, 06 Jun 2018 05:19:28 GMT
Server: Apache
X-Frame-Options: SAMEORIGIN
Accept-Ranges: bytes
X-OneAgent-JS-Injection: true
X-ruxit-JS-Agent: true
Set-Cookie: dtCookie=1$35381A8E36471ABB50147D4C8F4C08A0; Path=/; Domain=.dsogroup.com
Vary: Accept-Encoding
X-Mod-Pagespeed: 1.13.35.2-0
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Cache-Control: max-age=0, no-cache, s-maxage=10
Content-Length: 20151
Connection: close
Content-Type: text/html
```

## Solution:

Ensure that the HttpOnly flag is set for all cookies.

### Cookie no http-only flag (Low Risk)

If a cookie has no http-only flag its accessible from JavaScript. When the page has a cross site scripting (XSS) vulnerability the value of the cookie may be stolen and used to hijack the session if its a session cookie. Make sure that the http-only modifier is set on the cookie. There are [various ways](#) to do it. The easiest is when you have a Servlet API 3.0 container, there you can just declare it in the web.xml:

```
<session-config>
  <cookie-config>
    <http-only>true</http-only>
  </cookie-config>
</session-config>
```

## 2. Cookie Without Secure Flag

Edit Alert

Cookie Without Secure Flag

URL:

Risk:

Confidence:

Parameter:

Attack:

Evidence:

CWE ID:

WASC ID:

Description:

## Description:

A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

### Solution:

The purpose of the secure flag is to prevent cookies from being observed by unauthorized parties due to the transmission of a the cookie in clear text. If possible, ensure all communication occurs over an encrypted channel and add the 'secure' attribute to all session cookies or any cookies containing sensitive data.

In the <system.web> element, add the following element:

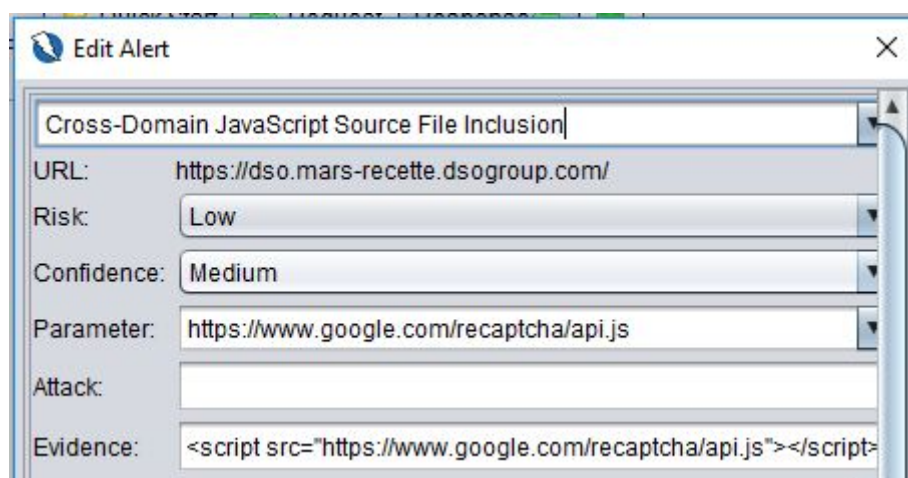
```
<httpCookies requireSSL="true" />
```

In that case, you need to add the requireSSL="true" attribute to the forms element as well.

So you will end up with:

```
<system.web>
<authentication mode="Forms">
<forms requireSSL="true">
/* forms content */ </forms>
</authentication>
</system.web>
```

## 3. Cross-Domain Javascript



```
<html>
<head>
  <meta http-equiv="X-UA-Compatible" content="IE=edge">
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no">
  <script type="text/javascript" src="/ruxitagentjs_25Vefhqr_10143180604090212.js" data-dtconfig=
"rid=RID_2418|rpId=-322580928|domain=dsogroup.com|reportUrl=/rb_c56cb57d-1d19-4946-92cb-ec2c74313a67|featureHash=25Vefhqr|md=3#a#component=1034|lastModification=1528262079706|dtVersion=10143180604090212|tp=500,50,0,1|agentUr
i=/ruxitagentjs_25Vefhqr_10143180604090212.js"></script><link rel="shortcut icon" href=".\\favicon.ico">
  <script src="https://www.google.com/recaptcha/api.js"></script>

  <script type="text/javascript">if(!window.console){console=(log:function(){});}</script>
</head>
<title>MARS</title>
```

## Request and Response

Header: Text Body: Text

```
GET https://dso.mars-recette.dsogroup.com/ HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0;)
Pragma: no-cache
Cache-Control: no-cache
Content-Length: 0
Host: dso.mars-recette.dsogroup.com
```

Header: Text Body: Text

```
HTTP/1.1 200 OK
Date: Wed, 06 Jun 2018 05:19:28 GMT
Server: Apache
X-Frame-Options: SAMEORIGIN
Accept-Ranges: bytes
X-OneAgent-JS-Injection: true
X-ruxit-JS-Agent: true
Set-Cookie: dtCookie=1$35381A8E36471ABB50147D4C8F4C08A0; Path=/; Domain=.dsogroup.com
Vary: Accept-Encoding
X-Mod-Pagespeed: 1.13.35.2-0
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Cache-Control: max-age=0, no-cache, s-maxage=10
Content-Length: 20151
Connection: close
Content-Type: text/html
```

## Description:

The page includes one or more script files from a third-party which is outside the control of this web application and as such may contain 'unexpected' functionality.

## Solution:

Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.

## 4. Incomplete or no Cache-Control and Pragma HTTP Header Set

Edit Alert

Incomplete or No Cache-control and Pragma HTTP Header Set

URL:

Risk:

Confidence:

Parameter:

Attack:

Evidence:

CWE ID:

WASC ID:

Description:

### Request and Response

```
GET https://dso.mars-recette.dsogroup.com/resources/css/lib/bootstrap.min.css HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0
Pragma: no-cache
Cache-Control: no-cache
Content-Length: 0
Referer: https://dso.mars-recette.dsogroup.com/
Host: dso.mars-recette.dsogroup.com
Cookie: dtCookie=1$EA475B26A7925954F09103BC4763A1A4
```



```
HTTP/1.1 200 OK
Date: Wed, 06 Jun 2018 05:19:35 GMT
Server: Apache
X-Frame-Options: SAMEORIGIN
Last-Modified: Tue, 22 May 2018 11:56:42 GMT
ETag: "18679-56cca1c90d280"
Accept-Ranges: bytes
Content-Length: 99961
Vary: Accept-Encoding
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Connection: close
Content-Type: text/css
```

---

```
GET https://dso.mars-recette.dsogroup.com/resources/css/lib/font-awesome.min.css HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0
Pragma: no-cache
Cache-Control: no-cache
Content-Length: 0
Referer: https://dso.mars-recette.dsogroup.com/
Host: dso.mars-recette.dsogroup.com
Cookie: dtCookie=1$EA475B26A7925954F09103BC4763A1A4
```

```
HTTP/1.1 200 OK
Date: Wed, 06 Jun 2018 05:19:32 GMT
Server: Apache
X-Frame-Options: SAMEORIGIN
Last-Modified: Tue, 22 May 2018 11:56:42 GMT
ETag: "6857-56cca1c90d280"
Accept-Ranges: bytes
Content-Length: 26711
Vary: Accept-Encoding
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Connection: close
Content-Type: text/css
```

---

```
GET https://dso.mars-recette.dsogroup.com/resources/css/lib/CancelButton.css HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0
Pragma: no-cache
Cache-Control: no-cache
Content-Length: 0
Referer: https://dso.mars-recette.dsogroup.com/
Host: dso.mars-recette.dsogroup.com
Cookie: dtCookie=1$EA475B26A7925954F09103BC4763A1A4
```



```
HTTP/1.1 200 OK
Date: Wed, 06 Jun 2018 05:19:34 GMT
Server: Apache
X-Frame-Options: SAMEORIGIN
Last-Modified: Tue, 22 May 2018 11:56:42 GMT
ETag: "5ae-56cca1c90d280"
Accept-Ranges: bytes
Content-Length: 1454
Vary: Accept-Encoding
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Connection: close
Content-Type: text/css
```

```
GET https://dso.mars-recette.dsogroup.com/resources/css/lib/converse.js/converse.min.css HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0
Pragma: no-cache
Cache-Control: no-cache
Content-Length: 0
Referer: https://dso.mars-recette.dsogroup.com/
Host: dso.mars-recette.dsogroup.com
Cookie: dtCookie=1$EA475B26A7925954F09103BC4763A1A4
```

```
HTTP/1.1 200 OK
Date: Wed, 06 Jun 2018 05:19:32 GMT
Server: Apache
X-Frame-Options: SAMEORIGIN
Last-Modified: Tue, 22 May 2018 11:56:42 GMT
ETag: "7cf0-56cca1c90d280"
Accept-Ranges: bytes
Content-Length: 31984
Vary: Accept-Encoding
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Connection: close
Content-Type: text/css
```

```
GET https://dso.mars-recette.dsogroup.com/resources/css/fonts.css HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0
Pragma: no-cache
Cache-Control: no-cache
Content-Length: 0
Referer: https://dso.mars-recette.dsogroup.com/
Host: dso.mars-recette.dsogroup.com
Cookie: dtCookie=1$EA475B26A7925954F09103BC4763A1A4
```

```
HTTP/1.1 200 OK
Date: Wed, 06 Jun 2018 05:19:35 GMT
Server: Apache
X-Frame-Options: SAMEORIGIN
Last-Modified: Tue, 22 May 2018 11:56:42 GMT
ETag: "24e-56cca1c90d280"
Accept-Ranges: bytes
Content-Length: 590
Vary: Accept-Encoding
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Connection: close
Content-Type: text/css
```

```
GET https://dso.mars-recette.dsogroup.com/resources/css/lib/jquery.Jcrop.min.css HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0
Pragma: no-cache
Cache-Control: no-cache
Content-Length: 0
Referer: https://dso.mars-recette.dsogroup.com/
Host: dso.mars-recette.dsogroup.com
Cookie: dtCookie=1$EA475B26A7925954F09103BC4763A1A4
```

```
HTTP/1.1 200 OK
Date: Wed, 06 Jun 2018 05:19:33 GMT
Server: Apache
X-Frame-Options: SAMEORIGIN
Last-Modified: Tue, 22 May 2018 11:56:42 GMT
ETag: "827-56cca1c90d280"
Accept-Ranges: bytes
Content-Length: 2087
Vary: Accept-Encoding
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Connection: close
Content-Type: text/css
```

```
GET https://dso.mars-recette.dsogroup.com/resources/css/main.css HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0
Pragma: no-cache
Cache-Control: no-cache
Content-Length: 0
Referer: https://dso.mars-recette.dsogroup.com/
Host: dso.mars-recette.dsogroup.com
Cookie: dtCookie=1$EA475B26A7925954F09103BC4763A1A4
```

---

```
HTTP/1.1 200 OK
Date: Wed, 06 Jun 2018 05:19:34 GMT
Server: Apache
X-Frame-Options: SAMEORIGIN
Last-Modified: Tue, 22 May 2018 11:56:42 GMT
ETag: "8ff-56cca1c90d280"
Accept-Ranges: bytes
Content-Length: 2303
Vary: Accept-Encoding
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Connection: close
Content-Type: text/css
```

---

```
GET https://dso.mars-recette.dsogroup.com/resources/css/jquery.percentageloader-0.1.css HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0
Pragma: no-cache
Cache-Control: no-cache
Content-Length: 0
Referer: https://dso.mars-recette.dsogroup.com/
Host: dso.mars-recette.dsogroup.com
Cookie: dtCookie=1$EA475B26A7925954F09103BC4763A1A4
```

---

```
HTTP/1.1 200 OK
Date: Wed, 06 Jun 2018 05:19:37 GMT
Server: Apache
X-Frame-Options: SAMEORIGIN
Last-Modified: Tue, 22 May 2018 11:56:42 GMT
ETag: "a2-56cca1c90d280"
Accept-Ranges: bytes
Content-Length: 162
Vary: Accept-Encoding
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Connection: close
Content-Type: text/css
```

---

```
GET https://dso.mars-recette.dsogroup.com/resources/select2/select2.min.css HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0
Pragma: no-cache
Cache-Control: no-cache
Content-Length: 0
Referer: https://dso.mars-recette.dsogroup.com/
Host: dso.mars-recette.dsogroup.com
Cookie: dtCookie=1$EA475B26A7925954F09103BC4763A1A4
```

```
HTTP/1.1 200 OK
Date: Wed, 06 Jun 2018 05:19:37 GMT
Server: Apache
X-Frame-Options: SAMEORIGIN
Last-Modified: Tue, 22 May 2018 11:56:42 GMT
ETag: "2278-56cca1c90d280"
Accept-Ranges: bytes
Content-Length: 8824
Vary: Accept-Encoding
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Connection: close
Content-Type: text/css
```

```
GET https://dso.mars-recette.dsogroup.com/resources/css/themes/theme-grey.css HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0
Pragma: no-cache
Cache-Control: no-cache
Content-Length: 0
Referer: https://dso.mars-recette.dsogroup.com/
Host: dso.mars-recette.dsogroup.com
Cookie: dtCookie=1$EA475B26A7925954F09103BC4763A1A4
```

```
HTTP/1.1 200 OK
Date: Wed, 06 Jun 2018 05:19:36 GMT
Server: Apache
X-Frame-Options: SAMEORIGIN
Last-Modified: Tue, 22 May 2018 11:56:42 GMT
ETag: "f2d-56cca1c90d280"
Accept-Ranges: bytes
Content-Length: 3885
Vary: Accept-Encoding
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Connection: close
Content-Type: text/css
```

---



```
GET https://dso.mars-recette.dsogroup.com/workflow/css/A.query-builder.css.pagespeed.cf.bVRQuQ4NF6.css HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0
Pragma: no-cache
Cache-Control: no-cache
Content-Length: 0
Referer: https://dso.mars-recette.dsogroup.com/
Host: dso.mars-recette.dsogroup.com
Cookie: dtCookie=1$EA475B26A7925954F09103BC4763A1A4
```



```
HTTP/1.1 200 OK
Date: Wed, 06 Jun 2018 05:19:33 GMT
Server: Apache
X-Frame-Options: SAMEORIGIN
Accept-Ranges: bytes
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Expires: Thu, 06 Jun 2019 05:16:51 GMT
Cache-Control: max-age=31536000
Etag: W/"0"
Last-Modified: Wed, 06 Jun 2018 05:16:51 GMT
X-Original-Content-Length: 5224
Vary: Accept-Encoding
Content-Length: 4042
Connection: close
Content-Type: text/css
```

Header: Text ▼ Body: Text ▼  

```
GET https://dso.mars-recette.dsogroup.com/ HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0;)
Pragma: no-cache
Cache-Control: no-cache
Content-Length: 0
Host: dso.mars-recette.dsogroup.com
```

Header: Text ▼ Body: Text ▼  

```
HTTP/1.1 200 OK
Date: Tue, 05 Jun 2018 07:27:21 GMT
Server: Apache
X-Frame-Options: SAMEORIGIN
Accept-Ranges: bytes
X-OneAgent-JS-Injection: true
X-ruxit-JS-Agent: true
Set-Cookie: dtCookie=1$617C6C4916A0518D092D13A7C8B4E3F6; Path=/; Domain=.dsogroup.com
Vary: Accept-Encoding
X-Mod-Pagespeed: 1.13.35.2-0
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Cache-Control: max-age=0, no-cache, s-maxage=10
Content-Length: 20151
Connection: close
Content-Type: text/html
```

## Description:

- The **cache-control** and **pragma** HTTP header have not been set properly or are missing allowing the browser and proxies to cache content.
- After a session has been closed, it might be possible to access the private or sensitive data exchanged within the session through the web browser cache.

## Solution:

- Whenever possible ensure the **cache-control** HTTP header is set with **no-cache, no-store, must-revalidate**; and that the **pragma** HTTP header is set with **no-cache**.

## How to set it?

Using PHP:

```
header("Cache-Control: no-cache, no-store, must-revalidate"); // HTTP 1.1.  
header("Pragma: no-cache"); // HTTP 1.0.  
header("Expires: 0"); // Proxies.
```

Using Java Servlet, or Node.js:

```
response.setHeader("Cache-Control", "no-cache, no-store, must-revalidate"); // HTTP 1.1.  
response.setHeader("Pragma", "no-cache"); // HTTP 1.0.  
response.setHeader("Expires", "0"); // Proxies.
```

Using ASP.NET-MVC

```
Response.Cache.SetCacheability(HttpCacheability.NoCache); // HTTP 1.1.  
Response.Cache.AppendCacheExtension("no-store, must-revalidate");  
Response.AppendHeader("Pragma", "no-cache"); // HTTP 1.0.  
Response.AppendHeader("Expires", "0"); // Proxies.
```

Using ASP.NET Web API:

```
// `response` is an instance of System.Net.Http.HttpResponseMessage  
response.Headers.CacheControl = new CacheControlHeaderValue  
{  
    NoCache = true,  
    NoStore = true,  
    MustRevalidate = true  
};  
response.Headers.Pragma.ParseAdd("no-cache");  
// We can't use `response.Content.Headers.Expires` directly  
// since it allows only `DateTimeOffset?` values.  
response.Content?.Headers.TryAddWithoutValidation("Expires", 0.ToString());
```



## 5. Web Browser XSS Protection Not Enabled

### Description:

- Web Browser XSS Protection is not enabled, or is disabled by the configuration of the 'X-XSS-Protection' HTTP response header on the web server.

### Request and Response

```
GET https://dso.mars-recette.dsogroup.com/.%5Cfavicon.ico HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0
Pragma: no-cache
Cache-Control: no-cache
Content-Length: 0
Referer: https://dso.mars-recette.dsogroup.com/
Host: dso.mars-recette.dsogroup.com
Cookie: dtCookie=1$EA475B26A7925954F09103BC4763A1A4
```

```
HTTP/1.1 404 Not Found
Date: Wed, 06 Jun 2018 05:19:31 GMT
Server: Apache
X-Frame-Options: SAMEORIGIN
Content-Length: 211
Connection: close
Content-Type: text/html; charset=iso-8859-1
```

---

```
GET https://dso.mars-recette.dsogroup.com/robots.txt HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0
Pragma: no-cache
Cache-Control: no-cache
Content-Length: 0
Host: dso.mars-recette.dsogroup.com
```

```
HTTP/1.1 404 Not Found
Date: Wed, 06 Jun 2018 05:19:29 GMT
Server: Apache
X-Frame-Options: SAMEORIGIN
Content-Length: 208
Connection: close
Content-Type: text/html; charset=iso-8859-1
```

```
GET https://dso.mars-recette.dsogroup.com/sitemap.xml HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0
Pragma: no-cache
Cache-Control: no-cache
Content-Length: 0
Host: dso.mars-recette.dsogroup.com
Cookie: dtCookie=1$EA475B26A7925954F09103BC4763A1A4
```

```
HTTP/1.1 404 Not Found
Date: Wed, 06 Jun 2018 05:19:30 GMT
Server: Apache
X-Frame-Options: SAMEORIGIN
Content-Length: 209
Connection: close
Content-Type: text/html; charset=iso-8859-1
```

## Solution:

`X-XSS-Protection: 1` : Force XSS protection (useful if XSS protection was disabled by the user)

`X-XSS-Protection: 0` : Disable XSS protection

The token `mode=block` will prevent browser (IE8+ and Webkit browsers) to render pages (instead of sanitizing) if a potential XSS reflection (= non-persistent) attack is detected.

Warning, `mode=block` creates a vulnerability in IE8

## Références:

Owasp.org. (2018). *HttpOnly - OWASP*. [online] Available at: <http://www.owasp.org/index.php/HttpOnly> [Accessed 6 Jun. 2018].

Inc, B. (2018). *Finding and Fixing Vulnerabilities in Web Application Cookies Lack Secure Flag , a Medium Risk Vulnerability*. [online] Beyondsecurity.com. Available at: [https://www.beyondsecurity.com/scan\\_pentest\\_network\\_vulnerabilities\\_web\\_application\\_cookies\\_lack\\_secure\\_flag](https://www.beyondsecurity.com/scan_pentest_network_vulnerabilities_web_application_cookies_lack_secure_flag) [Accessed 6 Jun. 2018].

Owasp.org. (2018). *Session Management Cheat Sheet - OWASP*. [online] Available at: [https://www.owasp.org/index.php/Session\\_Management\\_Cheat\\_Sheet#Web\\_Content\\_Caching](https://www.owasp.org/index.php/Session_Management_Cheat_Sheet#Web_Content_Caching) [Accessed 6 Jun. 2018].

How to control web page caching, a. (2018). *How to control web page caching, across all browsers?*. [online] Stack Overflow. Available at: <https://stackoverflow.com/questions/49547/how-to-control-web-page-caching-across-all-browsers> [Accessed 6 Jun. 2018].

Owasp.org. (2018). *XSS (Cross Site Scripting) Prevention Cheat Sheet - OWASP*. [online] Available at: [https://www.owasp.org/index.php/XSS\\_\(Cross\\_Site\\_Scripting\)\\_Prevention\\_Cheat\\_Sheet](https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet) [Accessed 6 Jun. 2018].

Veracode. (2018). *Guidelines for Setting Security Headers*. [online] Available at: <https://www.veracode.com/blog/2014/03/guidelines-for-setting-security-headers> [Accessed 6 Jun. 2018].

&ldquo;X-XSS-Protection&rdquo;?, W. (2018). *What is the http-header "X-XSS-Protection"?*. [online] Stack Overflow. Available at: <https://stackoverflow.com/questions/9090577/what-is-the-http-header-x-xss-protection> [Accessed 6 Jun. 2018].