Web Assessment Report

www.sitewall.net

Date: 6th December 2021

Prepared By: **pagEntra Infosec Pvt Ltd**

Introduction:

Purpose: The purpose of this assessment is to identify the current security posture of your website by scanning your website.

This assessment with help you in:

- Identify security weakness in your website which can be exploited by todays modern threat attackers.
- Minimize the damage by addressing the security gaps on your website.
- Reduce the risk of business impact by cyber-attacks on your website.

Scope: The scope of the assessment is limited to your website. We scan your websites using professional custom tools to identify the vulnerabilities and security gaps which can be exploited by the advance attackers.

Executive Summary:

Website	www.sitewall.net
Website Security Score	**"A"**
Backend Platform	PHP
Risk factor	**Low -** -
Others	-

Issue Identified:

		Confidence			
		Certain	Firm	Tentative	Total
Severity	High	0	**0**	**0**	**0**
	Medium	0	**2**	**0**	**2**
	Low	0	**2**	**2**	**4**
	Information	0	**0**	**0**	**0**

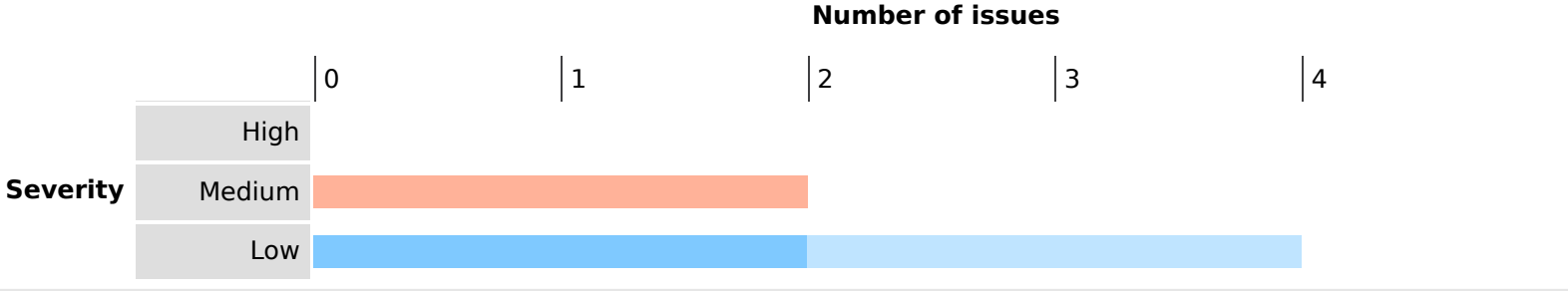
Sitewall Web Security Assessment Report

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	2	0	2
Low	0	2	2	4
Information	0	0	0	0

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

1. TLS cookie without secure flag set

There are 2 instances of this issue:

- /
- /

Issue background

If the secure flag is set on a cookie, then browsers will not submit the cookie in any requests that use an unencrypted HTTP connection, thereby preventing the cookie from being trivially intercepted by an attacker monitoring network traffic. If the secure flag is not set, then the cookie will be transmitted in clear-text if the user visits any HTTP URLs within the cookie's scope. An attacker may be able to induce this event by feeding a user suitable links, either directly or via another web site. Even if the domain that issued the cookie does not host any content that is accessed over HTTP, an attacker may be able to use links of the form http://example.com:443/ to perform the same attack.

To exploit this vulnerability, an attacker must be suitably positioned to eavesdrop on 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 secure flag should be set on all cookies that are used for transmitting sensitive data when accessing content over HTTPS. If cookies are used to transmit session tokens, then areas of the application that are accessed over HTTPS should employ their own session handling mechanism, and the session tokens used should never be transmitted over unencrypted communications.

Vulnerability classifications

- CWE-614: Sensitive Cookie in HTTPS Session Without 'Secure' Attribute

---

1.1. https://www.sitewall.net/

Summary

Severity:	**Medium**
Confidence:	**Firm**
Host:	**https://www.sitewall.net**
Path:	**/**

Issue detail

The following cookie was issued by the application and does not have the secure flag set:

- **SP.NET_SessionId**

The cookie appears to contain a session token, which may increase the risk associated with this issue. You should review the contents of the cookie to determine its function.This issue was found in multiple locations under the reported path.

Request 1

```
GET /web-assessment.php?name=lsLxnLNX&email=gHUWctAJ%40SiteWALLcollaborator.net HTTP/1.1
Host: www.sitewall.net
```

```
Cookie: PHPSESSID=d12d306394c66bda74fe70f07007b0e1; ASP.NET_SessionId=d12d306394c66bda74fe70f07007b0e1;
SP.NET_SessionId=d12d306394c66bda74fe70f07007b0e1
Upgrade-Insecure-Requests: 1
Referer: https://www.sitewall.net/web-assessment.php?name=XRyRPKVa&email=gKnKRJgi%40SiteWALLcollaborator.net
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/93.0.4577.82
Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 18 Nov 2021 15:12:47 GMT
Server: Apache
Set-Cookie: ASP.NET_SessionId=d12d306394c66bda74fe70f07007b0e1
Set-Cookie: SP.NET_SessionId=d12d306394c66bda74fe70f07007b0e1
Strict-Transport-Security: max-age=31536000
Content-Security-Policy: *.gstatic.com *.google.com*.googleapis.com *.jsdelivr.net
X-Content-Security-Policy: *.gstatic.com *.google.com*.googleapis.com *.jsdelivr.net
X-WebKit-CSP: *.gstatic.com *.google.com*.googleapis.com *.jsdelivr.net
X-XSS-Protection: 1
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 46603

<!DOCTYPE html>
<html lang="en">
<head><meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<!-- Required meta tags -->

<meta name="viewport" content="width=device-width
...[SNIP]...
```

Request 2

```
GET /web-assessment.php?
FirstName=HZcADHGv&LastName=UILIQOKK&email=IxmUpydV%40SiteWALLcollaborator.net&PhoneNumber=769-916-
4943&Company=331361&Job=585272&Country=&URL=http%3A%2F%2FSiteWALLcollaborator.net%2FPsqCfYFV&Comme
nts=713230&human=570345 HTTP/1.1
Host: www.sitewall.net
Cookie: PHPSESSID=d12d306394c66bda74fe70f07007b0e1; ASP.NET_SessionId=d12d306394c66bda74fe70f07007b0e1;
SP.NET_SessionId=d12d306394c66bda74fe70f07007b0e1
Upgrade-Insecure-Requests: 1
Referer: https://www.sitewall.net/web-assessment.php?name=JLxpfszQ&email=iCWlrJSo%40SiteWALLcollaborator.net
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/93.0.4577.82
Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 2

```
HTTP/1.1 200 OK
Date: Thu, 18 Nov 2021 15:11:50 GMT
Server: Apache
Set-Cookie: ASP.NET_SessionId=d12d306394c66bda74fe70f07007b0e1
Set-Cookie: SP.NET_SessionId=d12d306394c66bda74fe70f07007b0e1
Strict-Transport-Security: max-age=31536000
Content-Security-Policy: *.gstatic.com *.google.com*.googleapis.com *.jsdelivr.net
X-Content-Security-Policy: *.gstatic.com *.google.com*.googleapis.com *.jsdelivr.net
```

X-WebKit-CSP: *.gstatic.com *.google.com*.googleapis.com *.jsdelivr.net
X-XSS-Protection: 1
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 46603

<!DOCTYPE html>
<html lang="en">
<head><meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<!-- Required meta tags -->

<meta name="viewport" content="width=device-width
...[SNIP]...

Request 3

GET /web-assessment.php?
FirstName=oaJtpNjy&LastName=fzdOjqCw&email=bbZkfhiB%40SiteWALLcollaborator.net&PhoneNumber=125-521-3849&Company=134375&Job=578572&Country=&URL=http%3A%2F%2FSiteWALLcollaborator.net%2FcsRsfHfI&Comments=210255&human=677142 HTTP/1.1
Host: www.sitewall.net
Cookie: PHPSESSID=d12d306394c66bda74fe70f07007b0e1; ASP.NET_SessionId=d12d306394c66bda74fe70f07007b0e1; SP.NET_SessionId=d12d306394c66bda74fe70f07007b0e1
Upgrade-Insecure-Requests: 1
Referer: https://www.sitewall.net/web-assessment.php
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/93.0.4577.82 Safari/537.36
Connection: close
Cache-Control: max-age=0

Response 3

HTTP/1.1 200 OK
Date: Thu, 18 Nov 2021 15:04:29 GMT
Server: Apache
Set-Cookie: ASP.NET_SessionId=d12d306394c66bda74fe70f07007b0e1
Set-Cookie: SP.NET_SessionId=d12d306394c66bda74fe70f07007b0e1
Strict-Transport-Security: max-age=31536000
Content-Security-Policy: *.gstatic.com *.google.com*.googleapis.com *.jsdelivr.net
X-Content-Security-Policy: *.gstatic.com *.google.com*.googleapis.com *.jsdelivr.net
X-WebKit-CSP: *.gstatic.com *.google.com*.googleapis.com *.jsdelivr.net
X-XSS-Protection: 1
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 46603

<!DOCTYPE html>
<html lang="en">
<head><meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<!-- Required meta tags -->

<meta name="viewport" content="width=device-width
...[SNIP]...

1.2. https://www.sitewall.net/

Summary

	Severity:	**Medium**

Confidence:	**Firm**
Host:	**https://www.sitewall.net**
Path:	**/**

Issue detail

The following cookie was issued by the application and does not have the secure flag set:

- **ASP.NET_SessionId**

The cookie appears to contain a session token, which may increase the risk associated with this issue. You should review the contents of the cookie to determine its function.This issue was found in multiple locations under the reported path.

Request 1

```
GET /web-assessment.php?name=lsLxnLNX&email=gHUWctAJ%40SiteWALLcollaborator.net HTTP/1.1
Host: www.sitewall.net
Cookie: PHPSESSID=d12d306394c66bda74fe70f07007b0e1; ASP.NET_SessionId=d12d306394c66bda74fe70f07007b0e1;
SP.NET_SessionId=d12d306394c66bda74fe70f07007b0e1
Upgrade-Insecure-Requests: 1
Referer: https://www.sitewall.net/web-assessment.php?name=XRyRPKVa&email=gKnKRJgi%40SiteWALLcollaborator.net
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/93.0.4577.82
Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 18 Nov 2021 15:12:47 GMT
Server: Apache
Set-Cookie: ASP.NET_SessionId=d12d306394c66bda74fe70f07007b0e1
Set-Cookie: SP.NET_SessionId=d12d306394c66bda74fe70f07007b0e1
Strict-Transport-Security: max-age=31536000
Content-Security-Policy: *.gstatic.com *.google.com*.googleapis.com *.jsdelivr.net
X-Content-Security-Policy: *.gstatic.com *.google.com*.googleapis.com *.jsdelivr.net
X-WebKit-CSP: *.gstatic.com *.google.com*.googleapis.com *.jsdelivr.net
X-XSS-Protection: 1
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 46603

<!DOCTYPE html>
<html lang="en">
<head><meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<!-- Required meta tags -->

<meta name="viewport" content="width=device-width
...[SNIP]...
```

Request 2

```
GET /web-assessment.php?
FirstName=HZcADHGv&LastName=UILIQOKK&email=IxmUpydV%40SiteWALLcollaborator.net&PhoneNumber=769-916-
4943&Company=331361&Job=585272&Country=&URL=http%3A%2F%2FSiteWALLcollaborator.net%2FPsqCfYFV&Comme
nts=713230&human=570345 HTTP/1.1
Host: www.sitewall.net
Cookie: PHPSESSID=d12d306394c66bda74fe70f07007b0e1; ASP.NET_SessionId=d12d306394c66bda74fe70f07007b0e1;
SP.NET_SessionId=d12d306394c66bda74fe70f07007b0e1
Upgrade-Insecure-Requests: 1
Referer: https://www.sitewall.net/web-assessment.php?name=JLxpfszQ&email=iCWlrJSo%40SiteWALLcollaborator.net
```

```
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/93.0.4577.82
Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 2

```
HTTP/1.1 200 OK
Date: Thu, 18 Nov 2021 15:11:50 GMT
Server: Apache
Set-Cookie: ASP.NET_SessionId=d12d306394c66bda74fe70f07007b0e1
Set-Cookie: SP.NET_SessionId=d12d306394c66bda74fe70f07007b0e1
Strict-Transport-Security: max-age=31536000
Content-Security-Policy: *.gstatic.com *.google.com*.googleapis.com *.jsdelivr.net
X-Content-Security-Policy: *.gstatic.com *.google.com*.googleapis.com *.jsdelivr.net
X-WebKit-CSP: *.gstatic.com *.google.com*.googleapis.com *.jsdelivr.net
X-XSS-Protection: 1
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 46603

<!DOCTYPE html>
<html lang="en">
<head><meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<!-- Required meta tags -->

<meta name="viewport" content="width=device-width
...[SNIP]...
```

Request 3

```
GET /web-assessment.php?
FirstName=oaJtpNjy&LastName=fzdOjqCw&email=bbZkfhiB%40SiteWALLcollaborator.net&PhoneNumber=125-521-
3849&Company=134375&Job=578572&Country=&URL=http%3A%2F%2FSiteWALLcollaborator.net%2FcsRsfHfI&Commen
ts=210255&human=677142 HTTP/1.1
Host: www.sitewall.net
Cookie: PHPSESSID=d12d306394c66bda74fe70f07007b0e1; ASP.NET_SessionId=d12d306394c66bda74fe70f07007b0e1;
SP.NET_SessionId=d12d306394c66bda74fe70f07007b0e1
Upgrade-Insecure-Requests: 1
Referer: https://www.sitewall.net/web-assessment.php
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/93.0.4577.82
Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 3

```
HTTP/1.1 200 OK
Date: Thu, 18 Nov 2021 15:04:29 GMT
Server: Apache
Set-Cookie: ASP.NET_SessionId=d12d306394c66bda74fe70f07007b0e1
Set-Cookie: SP.NET_SessionId=d12d306394c66bda74fe70f07007b0e1
Strict-Transport-Security: max-age=31536000
Content-Security-Policy: *.gstatic.com *.google.com*.googleapis.com *.jsdelivr.net
X-Content-Security-Policy: *.gstatic.com *.google.com*.googleapis.com *.jsdelivr.net
X-WebKit-CSP: *.gstatic.com *.google.com*.googleapis.com *.jsdelivr.net
X-XSS-Protection: 1
Connection: close
Content-Type: text/html; charset=UTF-8
```

```
Content-Length: 46603

<!DOCTYPE html>
<html lang="en">
<head><meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<!-- Required meta tags -->

<meta name="viewport" content="width=device-width
...[SNIP]...
```

2. Vulnerable JavaScript dependency

There are 2 instances of this issue:

- /assets/js/jquery-min.js
- /lity/lity-master/vendor/jquery.js

Issue background

The use of third-party JavaScript libraries can introduce a range of DOM-based vulnerabilities, including some that can be used to hijack user accounts like DOM-XSS.

Common JavaScript libraries typically enjoy the benefit of being heavily audited. This may mean that bugs are quickly identified and patched upstream, resulting in a steady stream of security updates that need to be applied. Although it may be tempting to ignore updates, using a library with missing security patches can make your website exceptionally easy to exploit. Therefore, it's important to ensure that any available security updates are applied promptly.

Some library vulnerabilities expose every application that imports the library, but others only affect applications that use certain library features. Accurately identifying which library vulnerabilities apply to your website can be difficult, so we recommend applying all available security updates regardless.

Issue remediation

Develop a patch-management strategy to ensure that security updates are promptly applied to all third-party libraries in your application. Also, consider reducing your attack surface by removing any libraries that are no longer in use.

Vulnerability classifications

- CWE-1104: Use of Unmaintained Third Party Components
- A9: Using Components with Known Vulnerabilities

2.1. https://www.sitewall.net/assets/js/jquery-min.js

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://www.sitewall.net**
Path:	**/assets/js/jquery-min.js**

Issue detail

We observed a vulnerable JavaScript library.

We detected **jquery** version **2.1.4**, which has the following vulnerabilities:

- CVE-2015-9251: 3rd party CORS request may execute
- CVE-2015-9251: parseHTML() executes scripts in event handlers
- CVE-2019-11358: jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution
- CVE-2020-11022: Regex in its jQuery.htmlPrefilter sometimes may introduce XSS
- CVE-2020-11023: Regex in its jQuery.htmlPrefilter sometimes may introduce XSS

Request 1

```
GET /assets/js/jquery-min.js HTTP/1.1
Host: www.sitewall.net
Upgrade-Insecure-Requests: 1
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/93.0.4577.82
Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 18 Nov 2021 15:15:21 GMT
Server: Apache
Last-Modified: Tue, 19 Mar 2019 17:35:08 GMT
Accept-Ranges: bytes
Content-Length: 84345
Strict-Transport-Security: max-age=31536000
Content-Security-Policy: *.gstatic.com *.google.com*.googleapis.com *.jsdelivr.net
X-Content-Security-Policy: *.gstatic.com *.google.com*.googleapis.com *.jsdelivr.net
X-WebKit-CSP: *.gstatic.com *.google.com*.googleapis.com *.jsdelivr.net
X-XSS-Protection: 1
Connection: close
Content-Type: application/javascript

/*! jQuery v2.1.4 | (c) 2005, 2015 jQuery Foundation, Inc. | jquery.org/license */
!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?
b(a,!0):function(a){if(!a.document)th
...[SNIP]...
```

2.2. https://www.sitewall.net/lity/lity-master/vendor/jquery.js

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://www.sitewall.net**
Path:	**/lity/lity-master/vendor/jquery.js**

Issue detail

We observed a vulnerable JavaScript library.

We detected **jquery** version **1.11.2**, which has the following vulnerabilities:

- CVE-2015-9251: 3rd party CORS request may execute
- CVE-2015-9251: parseHTML() executes scripts in event handlers

- CVE-2019-11358: jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution
- CVE-2020-11022: Regex in its jQuery.htmlPrefilter sometimes may introduce XSS
- CVE-2020-11023: Regex in its jQuery.htmlPrefilter sometimes may introduce XSS

Request 1

```
GET /lity/lity-master/vendor/jquery.js HTTP/1.1
Host: www.sitewall.net
Upgrade-Insecure-Requests: 1
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/93.0.4577.82
Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 18 Nov 2021 15:14:54 GMT
Server: Apache
Last-Modified: Sun, 26 Apr 2020 08:53:09 GMT
Accept-Ranges: bytes
Content-Length: 399057
Strict-Transport-Security: max-age=31536000
Content-Security-Policy: *.gstatic.com *.google.com*.googleapis.com *.jsdelivr.net
X-Content-Security-Policy: *.gstatic.com *.google.com*.googleapis.com *.jsdelivr.net
X-WebKit-CSP: *.gstatic.com *.google.com*.googleapis.com *.jsdelivr.net
X-XSS-Protection: 1
Connection: close
Content-Type: application/javascript

/*!
* jQuery JavaScript Library v1.11.2
* http://jquery.com/
*
* Includes Sizzle.js
* http://sizzlejs.com/
*
* Copyright 2005, 2014 jQuery Foundation, Inc. and other contributors
* Released under the MIT license
* http://jquery.org/
...[SNIP]...
```

3. Cookie without HttpOnly flag set

There are 2 instances of this issue:

- /
- /

Issue background

If the HttpOnly attribute is set on a cookie, then the cookie's value cannot be read or set by client-side JavaScript. This measure makes certain client-side attacks, such as cross-site scripting, slightly harder to exploit by preventing them from trivially capturing the cookie's value via an injected script.

Issue remediation

There is usually no good reason not to set the HttpOnly flag on all cookies. Unless you specifically require legitimate client-side scripts within your application to read or set a cookie's value, you should set the HttpOnly flag by including this attribute within the relevant Set-cookie directive.

You should be aware that the restrictions imposed by the HttpOnly flag can potentially be circumvented in some circumstances, and that numerous other serious attacks can be delivered by client-side script injection, aside from simple cookie stealing.

References

- Web Security Academy: Exploiting XSS vulnerabilities
- HttpOnly effectiveness

Vulnerability classifications

- CWE-16: Configuration
- CAPEC-31: Accessing/Intercepting/Modifying HTTP Cookies

3.1. https://www.sitewall.net/

Summary

Severity:	**Low**
Confidence:	**Firm**
Host:	**https://www.sitewall.net**
Path:	**/**

Issue detail

The following cookie was issued by the application and does not have the HttpOnly flag set:

- **SP.NET_SessionId**

The cookie appears to contain a session token, which may increase the risk associated with this issue. You should review the contents of the cookie to determine its function.This issue was found in multiple locations under the reported path.

Request 1

```
GET /web-assessment.php?name=lsLxnLNX&email=gHUWctAJ%40SiteWALLcollaborator.net HTTP/1.1
Host: www.sitewall.net
Cookie: PHPSESSID=d12d306394c66bda74fe70f07007b0e1; ASP.NET_SessionId=d12d306394c66bda74fe70f07007b0e1;
SP.NET_SessionId=d12d306394c66bda74fe70f07007b0e1
Upgrade-Insecure-Requests: 1
Referer: https://www.sitewall.net/web-assessment.php?name=XRyRPKVa&email=gKnKRJgi%40SiteWALLcollaborator.net
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/93.0.4577.82
Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 18 Nov 2021 15:12:47 GMT
Server: Apache
```

Set-Cookie: ASP.NET_SessionId=d12d306394c66bda74fe70f07007b0e1
Set-Cookie: SP.NET_SessionId=d12d306394c66bda74fe70f07007b0e1
Strict-Transport-Security: max-age=31536000
Content-Security-Policy: *.gstatic.com *.google.com*.googleapis.com *.jsdelivr.net
X-Content-Security-Policy: *.gstatic.com *.google.com*.googleapis.com *.jsdelivr.net
X-WebKit-CSP: *.gstatic.com *.google.com*.googleapis.com *.jsdelivr.net
X-XSS-Protection: 1
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 46603

<!DOCTYPE html>
<html lang="en">
<head><meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<!-- Required meta tags -->

<meta name="viewport" content="width=device-width
...[SNIP]...

Request 2

GET /web-assessment.php?
FirstName=HZcADHGv&LastName=UILIQOKK&email=IxmUpydV%40SiteWALLcollaborator.net&PhoneNumber=769-916-4943&Company=331361&Job=585272&Country=&URL=http%3A%2F%2FSiteWALLcollaborator.net%2FPsqCfYFV&Comments=713230&human=570345 HTTP/1.1
Host: www.sitewall.net
Cookie: PHPSESSID=d12d306394c66bda74fe70f07007b0e1; ASP.NET_SessionId=d12d306394c66bda74fe70f07007b0e1; SP.NET_SessionId=d12d306394c66bda74fe70f07007b0e1
Upgrade-Insecure-Requests: 1
Referer: https://www.sitewall.net/web-assessment.php?name=JLxpfszQ&email=iCWlrJSo%40SiteWALLcollaborator.net
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/93.0.4577.82 Safari/537.36
Connection: close
Cache-Control: max-age=0

Response 2

HTTP/1.1 200 OK
Date: Thu, 18 Nov 2021 15:11:50 GMT
Server: Apache
Set-Cookie: ASP.NET_SessionId=d12d306394c66bda74fe70f07007b0e1
Set-Cookie: SP.NET_SessionId=d12d306394c66bda74fe70f07007b0e1
Strict-Transport-Security: max-age=31536000
Content-Security-Policy: *.gstatic.com *.google.com*.googleapis.com *.jsdelivr.net
X-Content-Security-Policy: *.gstatic.com *.google.com*.googleapis.com *.jsdelivr.net
X-WebKit-CSP: *.gstatic.com *.google.com*.googleapis.com *.jsdelivr.net
X-XSS-Protection: 1
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 46603

<!DOCTYPE html>
<html lang="en">
<head><meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<!-- Required meta tags -->

<meta name="viewport" content="width=device-width
...[SNIP]...

Request 3

GET /web-assessment.php?
FirstName=oaJtpNjy&LastName=fzdOjqCw&email=bbZkfhiB%40SiteWALLcollaborator.net&PhoneNumber=125-521-

```
3849&Company=134375&Job=578572&Country=&URL=http%3A%2F%2FSiteWALLcollaborator.net%2FcsRsfHfI&Commen
ts=210255&human=677142 HTTP/1.1
Host: www.sitewall.net
Cookie: PHPSESSID=d12d306394c66bda74fe70f07007b0e1; ASP.NET_SessionId=d12d306394c66bda74fe70f07007b0e1;
SP.NET_SessionId=d12d306394c66bda74fe70f07007b0e1
Upgrade-Insecure-Requests: 1
Referer: https://www.sitewall.net/web-assessment.php
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/93.0.4577.82
Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 3

```
HTTP/1.1 200 OK
Date: Thu, 18 Nov 2021 15:04:29 GMT
Server: Apache
Set-Cookie: ASP.NET_SessionId=d12d306394c66bda74fe70f07007b0e1
Set-Cookie: SP.NET_SessionId=d12d306394c66bda74fe70f07007b0e1
Strict-Transport-Security: max-age=31536000
Content-Security-Policy: *.gstatic.com *.google.com*.googleapis.com *.jsdelivr.net
X-Content-Security-Policy: *.gstatic.com *.google.com*.googleapis.com *.jsdelivr.net
X-WebKit-CSP: *.gstatic.com *.google.com*.googleapis.com *.jsdelivr.net
X-XSS-Protection: 1
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 46603

<!DOCTYPE html>
<html lang="en">
<head><meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<!-- Required meta tags -->

<meta name="viewport" content="width=device-width
...[SNIP]...
```

3.2. https://www.sitewall.net/

Summary

Severity:	**Low**
Confidence:	**Firm**
Host:	**https://www.sitewall.net**
Path:	**/**

Issue detail

The following cookie was issued by the application and does not have the HttpOnly flag set:

- **ASP.NET_SessionId**

The cookie appears to contain a session token, which may increase the risk associated with this issue. You should review the contents of the cookie to determine its function.This issue was found in multiple locations under the reported path.

Request 1

```
GET /web-assessment.php?name=lsLxnLNX&email=gHUWctAJ%40SiteWALLcollaborator.net HTTP/1.1
Host: www.sitewall.net
```

```
Cookie: PHPSESSID=d12d306394c66bda74fe70f07007b0e1; ASP.NET_SessionId=d12d306394c66bda74fe70f07007b0e1;
SP.NET_SessionId=d12d306394c66bda74fe70f07007b0e1
Upgrade-Insecure-Requests: 1
Referer: https://www.sitewall.net/web-assessment.php?name=XRyRPKVa&email=gKnKRJgi%40SiteWALLcollaborator.net
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/93.0.4577.82
Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 18 Nov 2021 15:12:47 GMT
Server: Apache
Set-Cookie: ASP.NET_SessionId=d12d306394c66bda74fe70f07007b0e1
Set-Cookie: SP.NET_SessionId=d12d306394c66bda74fe70f07007b0e1
Strict-Transport-Security: max-age=31536000
Content-Security-Policy: *.gstatic.com *.google.com*.googleapis.com *.jsdelivr.net
X-Content-Security-Policy: *.gstatic.com *.google.com*.googleapis.com *.jsdelivr.net
X-WebKit-CSP: *.gstatic.com *.google.com*.googleapis.com *.jsdelivr.net
X-XSS-Protection: 1
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 46603

<!DOCTYPE html>
<html lang="en">
<head><meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<!-- Required meta tags -->

<meta name="viewport" content="width=device-width
...[SNIP]...
```

Request 2

```
GET /web-assessment.php?
FirstName=HZcADHGv&LastName=UILIQOKK&email=IxmUpydV%40SiteWALLcollaborator.net&PhoneNumber=769-916-
4943&Company=331361&Job=585272&Country=&URL=http%3A%2F%2FSiteWALLcollaborator.net%2FPsqCfYFV&Comme
nts=713230&human=570345 HTTP/1.1
Host: www.sitewall.net
Cookie: PHPSESSID=d12d306394c66bda74fe70f07007b0e1; ASP.NET_SessionId=d12d306394c66bda74fe70f07007b0e1;
SP.NET_SessionId=d12d306394c66bda74fe70f07007b0e1
Upgrade-Insecure-Requests: 1
Referer: https://www.sitewall.net/web-assessment.php?name=JLxpfszQ&email=iCWlrJSo%40SiteWALLcollaborator.net
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/93.0.4577.82
Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 2

```
HTTP/1.1 200 OK
Date: Thu, 18 Nov 2021 15:11:50 GMT
Server: Apache
Set-Cookie: ASP.NET_SessionId=d12d306394c66bda74fe70f07007b0e1
Set-Cookie: SP.NET_SessionId=d12d306394c66bda74fe70f07007b0e1
Strict-Transport-Security: max-age=31536000
Content-Security-Policy: *.gstatic.com *.google.com*.googleapis.com *.jsdelivr.net
X-Content-Security-Policy: *.gstatic.com *.google.com*.googleapis.com *.jsdelivr.net
```

X-WebKit-CSP: *.gstatic.com *.google.com*.googleapis.com *.jsdelivr.net
X-XSS-Protection: 1
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 46603

<!DOCTYPE html>
<html lang="en">
<head><meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<!-- Required meta tags -->

<meta name="viewport" content="width=device-width
...[SNIP]...

Request 3

GET /web-assessment.php?
FirstName=oaJtpNjy&LastName=fzdOjqCw&email=bbZkfhiB%40SiteWALLcollaborator.net&PhoneNumber=125-521-3849&Company=134375&Job=578572&Country=&URL=http%3A%2F%2FSiteWALLcollaborator.net%2FcsRsfHfl&Comments=210255&human=677142 HTTP/1.1
Host: www.sitewall.net
Cookie: PHPSESSID=d12d306394c66bda74fe70f07007b0e1; ASP.NET_SessionId=d12d306394c66bda74fe70f07007b0e1; SP.NET_SessionId=d12d306394c66bda74fe70f07007b0e1
Upgrade-Insecure-Requests: 1
Referer: https://www.sitewall.net/web-assessment.php
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/93.0.4577.82 Safari/537.36
Connection: close
Cache-Control: max-age=0

Response 3

HTTP/1.1 200 OK
Date: Thu, 18 Nov 2021 15:04:29 GMT
Server: Apache
Set-Cookie: ASP.NET_SessionId=d12d306394c66bda74fe70f07007b0e1
Set-Cookie: SP.NET_SessionId=d12d306394c66bda74fe70f07007b0e1
Strict-Transport-Security: max-age=31536000
Content-Security-Policy: *.gstatic.com *.google.com*.googleapis.com *.jsdelivr.net
X-Content-Security-Policy: *.gstatic.com *.google.com*.googleapis.com *.jsdelivr.net
X-WebKit-CSP: *.gstatic.com *.google.com*.googleapis.com *.jsdelivr.net
X-XSS-Protection: 1
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 46603

<!DOCTYPE html>
<html lang="en">
<head><meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<!-- Required meta tags -->

<meta name="viewport" content="width=device-width
...[SNIP]...
