



10/19/2020 12:48:44 PM (UTC+05:30)

Detailed Scan Report

<https://marketplace.uber.com/>

Scan Time : 10/19/2020 12:17:54 PM (UTC+05:30)
Scan Duration : 00:00:11:38
Total Requests : 9,733
Average Speed : 13.9r/s

Risk Level:
MEDIUM

17
IDENTIFIED

5
CONFIRMED

0
CRITICAL

0
HIGH

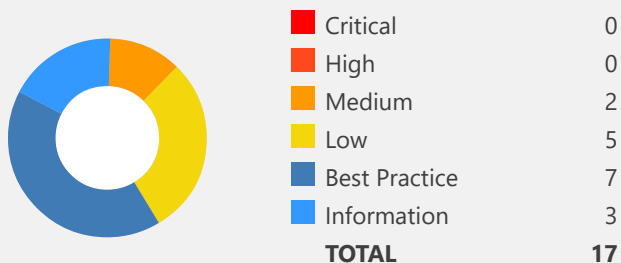
2
MEDIUM

5
LOW

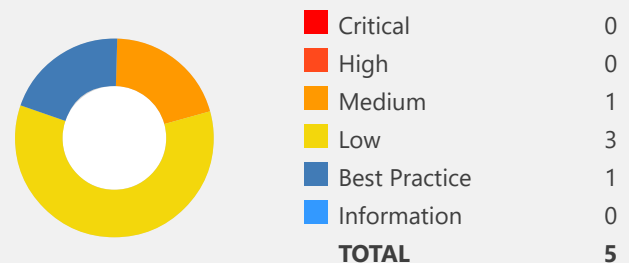
7
BEST PRACTICE

3
INFORMATION































Identified Vulnerabilities







Confirmed Vulnerabilities



Vulnerability Summary

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
 	HTTP Strict Transport Security (HSTS) Policy Not Enabled	GET	https://marketplace.uber.com/	
 	Weak Ciphers Enabled	GET	https://marketplace.uber.com/	
 	Missing X-Frame-Options Header	GET	https://marketplace.uber.com/	
 	Version Disclosure (Nginx)	GET	https://marketplace.uber.com/	
 	Cookie Not Marked as HttpOnly	GET	https://marketplace.uber.com/	
 	Cookie Not Marked as Secure	GET	https://marketplace.uber.com/	
 	Insecure Transportation Security Protocol Supported (TLS 1.0)	GET	https://marketplace.uber.com/	
 	Content Security Policy (CSP) Not Implemented	GET	https://marketplace.uber.com/	
 	Expect-CT Not Enabled	GET	https://marketplace.uber.com/	
 	Missing X-XSS-Protection Header	GET	https://marketplace.uber.com/	
 	Referrer-Policy Not Implemented	GET	https://marketplace.uber.com/	
 	SameSite Cookie Not Implemented	GET	https://marketplace.uber.com/	
 	Subresource Integrity (SRI) Not Implemented	GET	https://marketplace.uber.com/	
 	Insecure Transportation Security Protocol Supported (TLS 1.1)	GET	https://marketplace.uber.com/	
 	Email Address Disclosure	GET	https://marketplace.uber.com/principles	

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
 	Nginx Web Server Identified	GET	https://marketplace.uber.com/	
 	Out-of-date Version (Nginx)	GET	https://marketplace.uber.com/	

1. HTTP Strict Transport Security (HSTS) Policy Not Enabled

MEDIUM



1

Netsparker identified that HTTP Strict Transport Security (HSTS) policy is not enabled.

The target website is being served from not only HTTPS but also HTTP and it lacks of HSTS policy implementation.

HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure (HTTPS) connections. The HSTS Policy is communicated by the server to the user agent via a HTTP response header field named "Strict-Transport-Security". HSTS Policy specifies a period of time during which the user agent shall access the server in only secure fashion.

When a web application issues HSTS Policy to user agents, conformant user agents behave as follows:

- Automatically turn any insecure (HTTP) links referencing the web application into secure (HTTPS) links. (For instance, <http://example.com/some/page/> will be modified to <https://example.com/some/page/> before accessing the server.)
- If the security of the connection cannot be ensured (e.g. the server's TLS certificate is self-signed), user agents show an error message and do not allow the user to access the web application.

Vulnerabilities

1.1. <https://marketplace.uber.com/>

Certainty



Request

```
GET / HTTP/1.1
Host: marketplace.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 415.5454 Total Bytes Received : 70963 Body Length : 70684 Is Compressed : No

```
HTTP/1.1 200 OK
transfer-encoding: chunked
Server: nginx/1.14.1
X-Powered-By: Next.js
Vary: Accept-Encoding
Connection: keep-alive
Content-Type: text/html; charset=utf-8
Content-Encoding:
Date: Mon, 19 Oct 2020 06:48:30 GMT
ETag: "1141c-qLKWNeY7aNm3rSdIPMTEoQtJkjk"
```

```
<!DOCTYPE html><html class="no-js" lang="en"><head><meta charset="utf-8"/><meta http-equiv="x-ua-compatible" content="ie=edge"/><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"/><meta name="google-site-verification" content="yHvJ7x6qUkjrZRfaPzS05Iu42eP70uSS0Q88xPFBbSU"/><script src="https://polyfill.io/v2/polyfill.min.js?features=IntersectionObserver,Object.assign,Array.prototype.includes,Array.from,Array.prototype.find,Array.prototype.includes,String.prototype.startsWith,String.prototype.includes"></script><meta name="viewport" content="width=device-width"/><meta charset="utf-8"/><title>Marketplace | Uber</title><meta name="description" content="Learn about Uber's ridesharing marketplace and the principles that shape its design."/><meta property="og:title" content="Marketplace | Uber"/><meta property="og:description" content="Learn about Uber's ridesharing marketplace and the principles that shape its design."/><meta property="og:image" content="//images.ctfassets.net/kdwjnue2f64p/xjVlQoLAM88Qcgcg6m0Wy/a9bd5a146ce778b9cd379ec05e4d3aa9/share.png"/><meta property="og:image:width" content="1200"/><meta property="og:image:height" content="628"/><link rel="preload" href="//videos.ctfassets.net/kdwjnue2f64p/2CDUpWxmMM2qe8SAWGSycS/e0de83cfdc9f3c921c1ca30dd1a0c29f/forweb_loop_102318_under3mb.webmhd.webm" as="video" type="video/mp4"/><meta name="next-head-count" content="10"/><link rel="preload" href="/_next/static/css/styles.793d9c7f.chunk.css" as="style"/><link rel="stylesheet" href="/_next/static/css/styles.793d9c7f.chunk.css"/><link rel="preload" href="/_next/static/css/fa0d2a8633984918f0d634ef03f7b793f79d704a_CSS.5077fd2c.chunk.css" as="style"/><lin
...
```

Remedy

Configure your webserver to redirect HTTP requests to HTTPS.

i.e. for Apache, you should have modification in the httpd.conf. For more configurations, please refer to External References section.

```
# load module
LoadModule headers_module modules/mod_headers.so

# redirect all HTTP to HTTPS (optional)
<VirtualHost *:80>
    ServerAlias *
    RewriteEngine On
    RewriteRule ^(.*)$ https://%{HTTP_HOST}$1 [redirect=301]
```

```

</VirtualHost>

# HTTPS-Host-Configuration
<VirtualHost *:443>
    # Use HTTP Strict Transport Security to force client to use secure connections only
    Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains"

    # Further Configuration goes here
    [...]
</VirtualHost>

```

External References

- [Wikipedia - HTTP Strict Transport Security](#)
- [Configure HSTS \(HTTP Strict Transport Security\) for Apache/Nginx](#)
- [HTTP Strict Transport Security \(HSTS\) HTTP Header](#)
- [Mozilla SSL Configuration Generator](#)



CLASSIFICATION

OWASP 2013	A6
OWASP 2017	A3
SANS Top 25	523
CAPEC	217
WASC	4
ISO27001	A.14.1.2

2. Weak Ciphers Enabled

MEDIUM

1

CONFIRMED

1

Netsparker detected that weak ciphers are enabled during secure communication (SSL).
You should allow only strong ciphers on your web server to protect secure communication with your visitors.

Impact

Attackers might decrypt SSL traffic between your server and your visitors.

Vulnerabilities

2.1. <https://marketplace.uber.com/>

CONFIRMED

List of Supported Weak Ciphers

- TLS_RSA_WITH_AES_128_CBC_SHA (0x002F)
- TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC013)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014)
- TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003C)
- TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003D)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xC027)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xC028)

Request

[NETSPARKER] SSL Connection

Response

Response Time (ms) : 1 Total Bytes Received : 27 Body Length : 0 Is Compressed : No

[NETSPARKER] SSL Connection

Actions to Take

1. For Apache, you should modify the SSLCipherSuite directive in the httpd.conf.

```
SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4
```

2. Lighttpd:

```
ssl.honor-cipher-order = "enable"  
ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"
```

3. For Microsoft IIS, you should make some changes to the system registry. **Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.**

- a. Click Start, click Run, type regedt32 or type regedit, and then click OK.
- b. In Registry Editor, locate the following registry key: HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders
- c. Set "Enabled" DWORD to "0x0" for the following registry keys:

```
SCHANNEL\Ciphers\DES 56/56  
SCHANNEL\Ciphers\RC4 64/128  
SCHANNEL\Ciphers\RC4 40/128  
SCHANNEL\Ciphers\RC2 56/128  
SCHANNEL\Ciphers\RC2 40/128  
SCHANNEL\Ciphers\NULL  
SCHANNEL\Hashes\MD5
```

Remedy

Configure your web server to disallow using weak ciphers.

External References

- [OWASP - Insecure Configuration Management](#)
- [OWASP Top 10-2017 A3-Sensitive Data Exposure](#)
- [Zombie Poodle - Golden Doodle \(CBC\)](#)
- [Mozilla SSL Configuration Generator](#)
- [Strong Ciphers for Apache, Nginx and Lighttpd](#)



CLASSIFICATION

PCI DSS v3.2	6.5.4
OWASP 2013	A6
OWASP 2017	A3
SANS Top 25	327
CAPEC	217
WASC	4
ISO27001	A.14.1.3

CVSS 3.0 SCORE

Base	6.8 (Medium)
Temporal	6.8 (Medium)
Environmental	6.8 (Medium)

CVSS Vector String

CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

CVSS 3.1 SCORE

Base	6.8 (Medium)
Temporal	6.8 (Medium)
Environmental	6.8 (Medium)

CVSS Vector String

CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

3. Cookie Not Marked as HttpOnly

LOW



1

CONFIRMED



1

Netsparker identified a cookie not marked as HTTPOnly.

HTTPOnly cookies cannot be read by client-side scripts, therefore marking a cookie as HTTPOnly can provide an additional layer of protection against cross-site scripting attacks.

Impact

During a cross-site scripting attack, an attacker might easily access cookies and hijack the victim's session.

Vulnerabilities

3.1. <https://marketplace.uber.com/>

CONFIRMED

Identified Cookie(s)

- _ga
- _gid
- _gat

Cookie Source

- JavaScript

Request

```
GET / HTTP/1.1
Host: marketplace.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 1845.9581 Total Bytes Received : 70963 Body Length : 70684 Is Compressed : No

```
HTTP/1.1 200 OK
transfer-encoding: chunked
Server: nginx/1.14.1
X-Powered-By: Next.js
Vary: Accept-Encoding
Connection: keep-alive
Content-Type: text/html; charset=utf-8
Content-Encoding:
Date: Mon, 19 Oct 2020 06:47:59 GMT
ETag: "1141c-qLKWNeY7aNm3rSdIPMTEoQtJkjk"
```

```
<!DOCTYPE html><html class="no-js" lang="en"><head><meta charset="utf-8"/><meta http-equiv="x-ua-compatible" content="ie=edge"/><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"/><meta name="google-site-verification" content="yHvJ7x6qUkJrzRfaPzS05Iu42eP70uSS0Q88xPFBbSU"/><script src="https://polyfill.io/v2/polyfill.min.js?features=IntersectionObserver,Object.assign,Array.prototype.includes,Array.from,Array.prototype.find,Array.prototype.includes,String.prototype.startsWith,String.prototype.includes"></script><meta name="viewport" content="width=device-width"/><meta charset="utf-8"/><title>Marketplace | Uber</title><meta name="description" content="Learn about Uber's ridesharing marketplace and the principles that shape its design."/><meta property="og:title" content="Marketplace | Uber"/><meta property="og:description" content="Learn about Uber's ridesharing marketplace and the principles that shape its design."/><meta property="og:image" content="//images.ctfassets.net/kdwjnue2f64p/xjVlQoLAM88Qcgcg6m0Wy/a9bd5a146ce778b9cd379ec05e4d3aa9/share.png"/><meta property="og:image:width" content="1200"/><meta property="og:image:height" content="628"/><link rel="preload" href="//videos.ctfassets.net/kdwjnue2f64p/2CDUpWxmMM2qe8SAWGSycS/e0de83cfdc9f3c921c1ca30dd1a0c29f/forweb_loop_102318_under3mb.webmhd.webm" as="video" type="video/mp4"/><meta name="next-head-count" content="10"/><link rel="preload" href="/_next/static/css/styles.793d9c7f.chunk.css" as="style"/><link rel="stylesheet" href="/_next/static/css/styles.793d9c7f.chunk.css"/><link rel="preload" href="/_next/static/css/fa0d2a8633984918f0d634ef03f7b793f79d704a_CSS.5077fd2c.chunk.css" as="style"/><lin
...
```

Actions to Take

1. See the remedy for solution.
2. Consider marking all of the cookies used by the application as HTTPOnly. (After these changes javascript code will not be able to read cookies.)

Remedy

Mark the cookie as HTTPOnly. This will be an extra layer of defense against XSS. However this is not a silver bullet and will not protect the system against cross-site scripting attacks. An attacker can use a tool such as [XSS Tunnel](#) to bypass HTTPOnly protection.

External References

- [Netsparker - Security Cookies - HTTPOnly Flag](#)
- [OWASP HTTPOnly Cookies](#)
- [MSDN - ASP.NET HTTPOnly Cookies](#)



OWASP 2013	A5
OWASP 2017	A6
SANS Top 25	16
CAPEC	107
WASC	15
ISO27001	A.14.2.5

4. Cookie Not Marked as Secure

LOW



1

CONFIRMED



1

Netsparker identified a cookie not marked as secure, and transmitted over HTTPS.

This means the cookie could potentially be stolen by an attacker who can successfully intercept and decrypt the traffic, or following a successful man-in-the-middle attack.

Impact

This cookie will be transmitted over a HTTP connection, therefore if this cookie is important (*such as a session cookie*), an attacker might intercept it and hijack a victim's session. If the attacker can carry out a man-in-the-middle attack, he/she can force the victim to make an HTTP request to steal the cookie.

Vulnerabilities

4.1. <https://marketplace.uber.com/>

CONFIRMED

Identified Cookie(s)

- _ga
- _gid
- _gat

Cookie Source

- JavaScript

Request

```
GET / HTTP/1.1
Host: marketplace.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 1845.9581 Total Bytes Received : 70963 Body Length : 70684 Is Compressed : No

```
HTTP/1.1 200 OK
transfer-encoding: chunked
Server: nginx/1.14.1
X-Powered-By: Next.js
Vary: Accept-Encoding
Connection: keep-alive
Content-Type: text/html; charset=utf-8
Content-Encoding:
Date: Mon, 19 Oct 2020 06:47:59 GMT
ETag: "1141c-qLKWNeY7aNm3rSdIPMTEoQtJkjk"
```

```
<!DOCTYPE html><html class="no-js" lang="en"><head><meta charset="utf-8"/><meta http-equiv="x-ua-compatible" content="ie=edge"/><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"/><meta name="google-site-verification" content="yHvJ7x6qUkJrzRfaPzS05Iu42eP70uSS0Q88xPFBbSU"/><script src="https://polyfill.io/v2/polyfill.min.js?features=IntersectionObserver,Object.assign,Array.prototype.includes,Array.from,Array.prototype.find,Array.prototype.includes,String.prototype.startsWith,String.prototype.includes"></script><meta name="viewport" content="width=device-width"/><meta charset="utf-8"/><title>Marketplace | Uber</title><meta name="description" content="Learn about Uber's ridesharing marketplace and the principles that shape its design."/><meta property="og:title" content="Marketplace | Uber"/><meta property="og:description" content="Learn about Uber's ridesharing marketplace and the principles that shape its design."/><meta property="og:image" content="//images.ctfassets.net/kdwjnue2f64p/xjVlQoLAM88Qcgcg6m0Wy/a9bd5a146ce778b9cd379ec05e4d3aa9/share.png"/><meta property="og:image:width" content="1200"/><meta property="og:image:height" content="628"/><link rel="preload" href="//videos.ctfassets.net/kdwjnue2f64p/2CDUpWxmMM2qe8SAWGSycS/e0de83cfdc9f3c921c1ca30dd1a0c29f/forweb_loop_102318_under3mb.webmhd.webm" as="video" type="video/mp4"/><meta name="next-head-count" content="10"/><link rel="preload" href="/_next/static/css/styles.793d9c7f.chunk.css" as="style"/><link rel="stylesheet" href="/_next/static/css/styles.793d9c7f.chunk.css"/><link rel="preload" href="/_next/static/css/fa0d2a8633984918f0d634ef03f7b793f79d704a_CSS.5077fd2c.chunk.css" as="style"/><lin
...
```

Actions to Take

1. See the remedy for solution.
2. Mark all cookies used within the application as secure. *(If the cookie is not related to authentication or does not carry any personal information, you do not have to mark it as secure.)*

Remedy

Mark all cookies used within the application as secure.

Required Skills for Successful Exploitation

To exploit this issue, the attacker needs to be able to intercept traffic. This generally requires local access to the web server or to the victim's network. Attackers need to be understand layer 2, have physical access to systems either as waypoints for the traffic, or have locally gained access to to a system between the victim and the web server.

External References

- [Netsparker - Security Cookies - Secure Flag](#)
- [.NET Cookie.Secure Property](#)
- [How to Create Totally Secure Cookies](#)



CLASSIFICATION

PCI DSS v3.2	6.5.10
OWASP 2013	A6
OWASP 2017	A3
SANS Top 25	614
CAPEC	102
WASC	15
ISO27001	A.14.1.2

CVSS 3.0 SCORE

Base	2 (Low)
Temporal	2 (Low)
Environmental	2 (Low)

CVSS Vector String

CVSS:3.0/AV:P/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

CVSS 3.1 SCORE

Base	2 (Low)
Temporal	2 (Low)
Environmental	2 (Low)

CVSS Vector String

CVSS:3.1/AV:P/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

5. Insecure Transportation Security Protocol Supported (TLS 1.0)

LOW



1

CONFIRMED



1

Netsparker detected that insecure transportation security protocol (TLS 1.0) is supported by your web server.

TLS 1.0 has several flaws. An attacker can cause connection failures and they can trigger the use of TLS 1.0 to exploit vulnerabilities like BEAST (Browser Exploit Against SSL/TLS).

Websites using TLS 1.0 are considered non-compliant by PCI since 30 June 2018.

Impact

Attackers can perform man-in-the-middle attacks and observe the encryption traffic between your website and its visitors.

Vulnerabilities

5.1. <https://marketplace.uber.com/>
CONFIRMED

Request

[NETSPARKER] SSL Connection

Response

Response Time (ms) : 1 Total Bytes Received : 27 Body Length : 0 Is Compressed : No

[NETSPARKER] SSL Connection

Actions to Take

We recommended to disable TLS 1.0 and replace it with TLS 1.2 or higher. See Remedy section for more details.

Remedy

Configure your web server to disallow using weak ciphers. You need to restart the web server to enable changes.

- For Apache, adjust the SSLProtocol directive provided by the mod_ssl module. This directive can be set either at the server level or in a virtual host configuration.

```
SSLProtocol +TLSv1.2
```

- For Nginx, locate any use of the directive `ssl_protocols` in the `nginx.conf` file and remove TLSv1.

```
ssl_protocols TLSv1.2;
```

- For Microsoft IIS, you should make some changes on the system registry. **Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.**
 1. Click on Start and then Run, type `regedt32` or `regedit`, and then click OK.
 2. In Registry Editor, locate the following registry key or create if it does not exist:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\
```

3. Locate a key named `Server` or create if it doesn't exist.
 4. Under the `Server` key, locate a `DWORD` value named `Enabled` or create if it doesn't exist and set its value to "0".
- For `lighttpd`, put the following lines in your configuration file:

```
ssl.use-ssl2 = "disable"  
ssl.use-ssl3 = "disable"  
ssl.openssl.ssl-conf-cmd = ("Protocol" => "-TLSv1.1, -TLSv1, -SSLv3") # v1.4.48 or up  
ssl.ec-curve = "secp384r1"
```

External References

- [How to Disable TLS v1.0](#)
- [OWASP - Insecure Configuration Management](#)
- [OWASP Top 10 - 2017 A3 - Sensitive Data Exposure](#)
- [How to disable PCT 1.0, SSL 2.0, SSL 3.0, or TLS 1.0 in Internet Information Services](#)
- [IIS Crypto is a free tool that gives administrators the ability to enable or disable protocols, ciphers, hashes and key exchange algorithms on Windows Server 2003, 2008 and 2012](#)
- [Date Change for Migrating from SSL and Early TLS](#)
- [Browser Exploit Against SSL/TLS Attack \(BEAST\)](#)
- [Are You Ready for 30 June 2018? Saying Goodbye to SSL/early TLS](#)



CLASSIFICATION

PCI DSS v3.2	6.5.4
OWASP 2013	A6
OWASP 2017	A3
SANS Top 25	326
CAPEC	217
WASC	4
HIPAA	164.306
ISO27001	A.14.1.3

6. Missing X-Frame-Options Header

LOW



1

Netsparker detected a missing X-Frame-Options header which means that this website could be at risk of a clickjacking attack.

The X-Frame-Options HTTP header field indicates a policy that specifies whether the browser should render the transmitted resource within a frame or an iframe. Servers can declare this policy in the header of their HTTP responses to prevent clickjacking attacks, which ensures that their content is not embedded into other pages or frames.

Impact

Clickjacking is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on a framed page when they were intending to click on the top level page. Thus, the attacker is "hijacking" clicks meant for their page and routing them to other another page, most likely owned by another application, domain, or both.

Using a similar technique, keystrokes can also be hijacked. With a carefully crafted combination of stylesheets, iframes, and text boxes, a user can be led to believe they are typing in the password to their email or bank account, but are instead typing into an invisible frame controlled by the attacker.

Vulnerabilities

6.1. <https://marketplace.uber.com/>

Certainty



Request

```
GET / HTTP/1.1
Host: marketplace.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 1845.9581 Total Bytes Received : 70963 Body Length : 70684 Is Compressed : No

```
HTTP/1.1 200 OK
transfer-encoding: chunked
Server: nginx/1.14.1
X-Powered-By: Next.js
Vary: Accept-Encoding
Connection: keep-alive
Content-Type: text/html; charset=utf-8
Content-Encoding:
Date: Mon, 19 Oct 2020 06:47:59 GMT
ETag: "1141c-qLKWNeY7aNm3rSdIPMTEoQtJkjk"
```

```
<!DOCTYPE html><html class="no-js" lang="en"><head><meta charset="utf-8"/><meta http-equiv="x-ua-compatible" content="ie=edge"/><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"/><meta name="google-site-verification" content="yHvJ7x6qUkjrZRfaPzS05Iu42eP70uSS0Q88xPFBbSU"/><script src="https://polyfill.io/v2/polyfill.min.js?features=IntersectionObserver,Object.assign,Array.prototype.includes,Array.from,Array.prototype.find,Array.prototype.includes,String.prototype.startsWith,String.prototype.includes"></script><meta name="viewport" content="width=device-width"/><meta charset="utf-8"/><title>Marketplace | Uber</title><meta name="description" content="Learn about Uber's ridesharing marketplace and the principles that shape its design."/><meta property="og:title" content="Marketplace | Uber"/><meta property="og:description" content="Learn about Uber's ridesharing marketplace and the principles that shape its design."/><meta property="og:image" content="//images.ctfassets.net/kdwjnue2f64p/xjVlQoLAM88Qcgcg6m0Wy/a9bd5a146ce778b9cd379ec05e4d3aa9/share.png"/><meta property="og:image:width" content="1200"/><meta property="og:image:height" content="628"/><link rel="preload" href="//videos.ctfassets.net/kdwjnue2f64p/2CDUpWxmMM2qe8SAWGSycS/e0de83cfdc9f3c921c1ca30dd1a0c29f/forweb_loop_102318_under3mb.webmhd.webm" as="video" type="video/mp4"/><meta name="next-head-count" content="10"/><link rel="preload" href="/_next/static/css/styles.793d9c7f.chunk.css" as="style"/><link rel="stylesheet" href="/_next/static/css/styles.793d9c7f.chunk.css"/><link rel="preload" href="/_next/static/css/fa0d2a8633984918f0d634ef03f7b793f79d704a_CSS.5077fd2c.chunk.css" as="style"/><lin
...
```

Remedy

- Sending the proper X-Frame-Options in HTTP response headers that instruct the browser to not allow framing from other domains.
 - X-Frame-Options: DENYIt completely denies to be loaded in frame/iframe.
 - X-Frame-Options: SAMEORIGINIt allows only if the site which wants to load has a same origin.
 - X-Frame-Options: ALLOW-FROM URLIt grants a specific URL to load itself in a iframe. However please pay attention to that, not all browsers support this.
- Employing defensive code in the UI to ensure that the current frame is the most top level window.

External References

- [Clickjacking](#)
- [Can I Use X-Frame-Options](#)
- [X-Frame-Options HTTP Header](#)

Remedy References

- [Clickjacking Defense Cheat Sheet](#)



CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
SANS Top 25	693
CAPEC	103
ISO27001	A.14.2.5

7. Version Disclosure (Nginx)

LOW



1

Netsparker identified a version disclosure (Nginx) in the target web server's HTTP response.

This information might help an attacker gain a greater understanding of the systems in use and potentially develop further attacks targeted at the specific version of Nginx.

Impact

An attacker might use the disclosed information to harvest specific security vulnerabilities for the version identified.

Vulnerabilities

7.1. <https://marketplace.uber.com/>

Extracted Version

- 1.14.1

Certainty



Request

```
GET / HTTP/1.1
Host: marketplace.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 1845.9581 Total Bytes Received : 70963 Body Length : 70684 Is Compressed : No

```
HTTP/1.1 200 OK
transfer-encoding: chunked
Server: nginx/1.14.1
X-Powered-By: Next.js
Vary: Accept-Encoding
Connection: keep-alive
Content-Type: text/html; charset=utf-8
Content-Encoding:
Date: Mon, 19 Oct 2020 06:47:59 GMT
ETag: "1141c-qLKWNeY7aNm3rHTTP/1.1 200 OK
transfer-encoding: chunked
Server: nginx/1.14.1
X-Powered-By: Next.js
Vary: Accept-Encoding
Connection: keep-alive
Content-Type: text/html; charset=utf-8
Content-Encoding:
Date: Mon, 19 Oct 2020 06:47:59 GMT
ETag: "1141c-qLKWNeY7aNm3rSdIPM
...
```

Remedy

Add the following line to your nginx.conf file to prevent information leakage from the SERVERheader of its HTTP response:

```
server_tokens off
```



CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
SANS Top 25	205
CAPEC	170
WASC	45
HIPAA	164.306(A), 164.308(A)
ISO27001	A.18.1.3

8. Content Security Policy (CSP) Not Implemented

BEST PRACTICE

1

CSP is an added layer of security that helps to mitigate mainly Cross-site Scripting attacks.

CSP can be enabled instructing the browser with a Content-Security-Policy directive in a response header;

```
Content-Security-Policy: script-src 'self';
```

or in a meta tag;

```
<meta http-equiv="Content-Security-Policy" content="script-src 'self';">
```

In the above example, you can restrict script loading only to the same domain. It will also restrict inline script executions both in the element attributes and the event handlers. There are various directives which you can use by declaring CSP:

- **script-src**: Restricts the script loading resources to the ones you declared. By default, it disables inline script executions unless you permit to the evaluation functions and inline scripts by the `unsafe-eval` and `unsafe-inline` keywords.
- **base-uri**: Base element is used to resolve relative URL to absolute one. By using this CSP directive, you can define all possible URLs which could be assigned to `base-href` attribute of the document.
- **frame-ancestors**: It is very similar to `X-Frame-Options` HTTP header. It defines the URLs by which the page can be loaded in an `iframe`.
- **frame-src / child-src**: `frame-src` is the deprecated version of `child-src`. Both define the sources that can be loaded by `iframe` in the page. (Please note that `frame-src` was brought back in CSP 3)
- **object-src**: Defines the resources that can be loaded by embedding such as Flash files, Java Applets.
- **img-src**: As its name implies, it defines the resources where the images can be loaded from.
- **connect-src**: Defines the whitelisted targets for `XMLHttpRequest` and `WebSocket` objects.
- **default-src**: It is a fallback for the directives that mostly ends with `-src` suffix. When the directives below are not defined, the value set to `default-src` will be used instead:
 - `child-src`
 - `connect-src`
 - `font-src`
 - `img-src`
 - `manifest-src`
 - `media-src`
 - `object-src`
 - `script-src`
 - `style-src`

When setting the CSP directives, you can also use some CSP keywords:

- **none**: Denies loading resources from anywhere.
- **self**: Points to the document's URL (domain + port).
- **unsafe-inline**: Permits running inline scripts.
- **unsafe-eval**: Permits execution of evaluation functions such as `eval()`.

In addition to CSP keywords, you can also use wildcard or only a scheme when defining whitelist URLs for the points. Wildcard can be used for subdomain and port portions of the URLs:

```
Content-Security-Policy: script-src https://\*.example.com;
```

```
Content-Security-Policy: script-src https://example.com*;
```

```
Content-Security-Policy: script-src https;;
```

It is also possible to set a CSP in Report-Only mode instead of forcing it immediately in the migration period. Thus you can see the violations of the CSP policy in the current state of your web site while migrating to CSP:

```
Content-Security-Policy-Report-Only: script-src 'self'; report-uri: https://example.com;
```

Impact

There is no direct impact of not implementing CSP on your website. However, if your website is vulnerable to a Cross-site Scripting attack CSP can prevent successful exploitation of that vulnerability. By not implementing CSP you'll be missing out this extra layer of security.

Vulnerabilities

8.1. <https://marketplace.uber.com/>

Certainty



Request

GET / HTTP/1.1
Host: marketplace.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker

Response

Response Time (ms) : 1845.9581 Total Bytes Received : 70963 Body Length : 70684 Is Compressed : No

```
HTTP/1.1 200 OK
transfer-encoding: chunked
Server: nginx/1.14.1
X-Powered-By: Next.js
Vary: Accept-Encoding
Connection: keep-alive
Content-Type: text/html; charset=utf-8
Content-Encoding:
Date: Mon, 19 Oct 2020 06:47:59 GMT
ETag: "1141c-qLKWNeY7aNm3rSdIPMTEoQtJkjk"
```

```
<!DOCTYPE html><html class="no-js" lang="en"><head><meta charset="utf-8"/><meta http-equiv="x-ua-compatible" content="ie=edge"/><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"/><meta name="google-site-verification" content="yHvJ7x6qUkjrZRfaPzS05Iu42eP70uSS0Q88xPFBbSU"/><script src="https://polyfill.io/v2/polyfill.min.js?features=IntersectionObserver,Object.assign,Array.prototype.includes,Array.from,Array.prototype.find,Array.prototype.includes,String.prototype.startsWith,String.prototype.includes"></script><meta name="viewport" content="width=device-width"/><meta charset="utf-8"/><title>Marketplace | Uber</title><meta name="description" content="Learn about Uber&#x27;s ridesharing marketplace and the principles that shape its design."/><meta property="og:title" content="Marketplace | Uber"/><meta property="og:description" content="Learn about Uber&#x27;s ridesharing marketplace and the principles that shape its design."/><meta property="og:image" content="//images.ctfassets.net/kdwjnue2f64p/xjVlQoLAM88Qcgcg6m0Wy/a9bd5a146ce778b9cd379ec05e4d3aa9/share.png"/><meta property="og:image:width" content="1200"/><meta property="og:image:height" content="628"/><link rel="preload" href="//videos.ctfassets.net/kdwjnue2f64p/2CDUpWxmMM2qe8SAWGSycS/e0de83cfdc9f3c921c1ca30dd1a0c29f/forweb_loop_102318_under3mb.webmhd.webm" as="video" type="video/mp4"/><meta name="next-head-count" content="10"/><link rel="preload" href="/_next/static/css/styles.793d9c7f.chunk.css" as="style"/><link rel="stylesheet" href="/_next/static/css/styles.793d9c7f.chunk.css"/><link rel="preload" href="/_next/static/css/fa0d2a8633984918f0d634ef03f7b793f79d704a_CSS.5077fd2c.chunk.css" as="style"/><lin
...
```

Actions to Take

- Enable CSP on your website by sending the Content-Security-Policy in HTTP response headers that instruct the browser to apply the policies you specified.
- Apply the whitelist and policies as strict as possible.
- Rescan your application to see if Netsparker identifies any weaknesses in your policies.

Remedy

Enable CSP on your website by sending the Content-Security-Policy in HTTP response headers that instruct the browser to apply the policies you specified.

External References

- [An Introduction to Content Security Policy](#)
- [Content Security Policy \(CSP\) HTTP Header](#)

- [Content Security Policy \(CSP\)](#)



CLASSIFICATION

SANS Top 25	16
WASC	15
ISO27001	A.14.2.5

9. Expect-CT Not Enabled

BEST PRACTICE



1

Netsparker identified that Expect-CT is not enabled.

Certificate Transparency is a technology that makes impossible (or at least very difficult) for a CA to issue an SSL certificate for a domain without the certificate being visible to the owner of that domain.

Google announced that, starting with April 2018, if it runs into a certificate that is not seen in Certificate Transparency (CT) Log, it will consider that certificate invalid and reject the connection. Thus sites should serve certificate that takes place in CT Logs. While handshaking, sites should serve a valid Signed Certificate Timestamp (SCT) along with the certificate itself.

Expect-CT can also be used for detecting the compatibility of the certificates that are issued before the April 2018 deadline. For instance, a certificate that was signed before April 2018, for 10 years it will be still posing a risk and can be ignored by the certificate transparency policy of the browser. By setting Expect-CT header, you can prevent misissued certificates to be used.

Vulnerabilities

9.1. <https://marketplace.uber.com/>

Certainty



Request

```
GET / HTTP/1.1
Host: marketplace.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```


Response

Response Time (ms) : 1845.9581 Total Bytes Received : 70963 Body Length : 70684 Is Compressed : No

```
HTTP/1.1 200 OK
transfer-encoding: chunked
Server: nginx/1.14.1
X-Powered-By: Next.js
Vary: Accept-Encoding
Connection: keep-alive
Content-Type: text/html; charset=utf-8
Content-Encoding:
Date: Mon, 19 Oct 2020 06:47:59 GMT
ETag: "1141c-qLKWNeY7aNm3rSdIPMTEoQtJkjk"
```

```
<!DOCTYPE html><html class="no-js" lang="en"><head><meta charset="utf-8"/><meta http-equiv="x-ua-compatible" content="ie=edge"/><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"/><meta name="google-site-verification" content="yHvJ7x6qUkjrZRfaPzS05Iu42eP70uSS0Q88xPFBbSU"/><script src="https://polyfill.io/v2/polyfill.min.js?features=IntersectionObserver,Object.assign,Array.prototype.includes,Array.from,Array.prototype.find,Array.prototype.includes,String.prototype.startsWith,String.prototype.includes"></script><meta name="viewport" content="width=device-width"/><meta charset="utf-8"/><title>Marketplace | Uber</title><meta name="description" content="Learn about Uber's ridesharing marketplace and the principles that shape its design."/><meta property="og:title" content="Marketplace | Uber"/><meta property="og:description" content="Learn about Uber's ridesharing marketplace and the principles that shape its design."/><meta property="og:image" content="//images.ctfassets.net/kdwjnue2f64p/xjVlQoLAM88Qcgcg6m0Wy/a9bd5a146ce778b9cd379ec05e4d3aa9/share.png"/><meta property="og:image:width" content="1200"/><meta property="og:image:height" content="628"/><link rel="preload" href="//videos.ctfassets.net/kdwjnue2f64p/2CDUpWxmMM2qe8SAWGSycS/e0de83cfdc9f3c921c1ca30dd1a0c29f/forweb_loop_102318_under3mb.webmhd.webm" as="video" type="video/mp4"/><meta name="next-head-count" content="10"/><link rel="preload" href="/_next/static/css/styles.793d9c7f.chunk.css" as="style"/><link rel="stylesheet" href="/_next/static/css/styles.793d9c7f.chunk.css"/><link rel="preload" href="/_next/static/css/fa0d2a8633984918f0d634ef03f7b793f79d704a_CSS.5077fd2c.chunk.css" as="style"/><lin
...
```

Remedy

Configure your web server to respond with Expect-CT header.

```
Expect-CT: enforce, max-age=7776000, report-uri="https://ABSOLUTE\_REPORT\_URL"
```

Note: We strongly suggest you to use Expect-CT header in **report-only mode** first. If everything goes well and your certificate is ready, go with the Expect-CT enforce mode. To use **report-only mode** first, omit **enforce** flag and see the browser's behavior with your deployed certificate.

```
Expect-CT: max-age=7776000, report-uri="https://ABSOLUTE\_REPORT\_URL"
```

External References

- [Expect-CT Extension for HTTP](#)
- [Expect-CT HTTP Header](#)
- [Expect-CT Header](#)



CLASSIFICATION

SANS Top 25	16
WASC	15
ISO27001	A.14.1.2

10. Insecure Transportation Security Protocol Supported (TLS 1.1)

BEST PRACTICE

1

CONFIRMED

1

Netsparker detected that a deprecated, insecure transportation security protocol (TLS 1.1) is supported by your web server.

TLS 1.1 will be considered as deprecated by major web browsers (i.e. Chrome, Firefox, Safari, Edge, Internet Explorer) starting in 2020.

Impact

Your website will be inaccessible due to web browser deprecation.

Vulnerabilities

10.1. <https://marketplace.uber.com/>

CONFIRMED

Request

[NETSPARKER] SSL Connection

Response

Response Time (ms) : 1 Total Bytes Received : 27 Body Length : 0 Is Compressed : No

[NETSPARKER] SSL Connection

Actions to Take

We recommended to disable TLS 1.1 and replace it with TLS 1.2 or higher. See Remedy section for more details.

Remedy

Configure your web server to disallow using weak ciphers. You need to restart the web server to enable changes.

- For Apache, adjust the SSLProtocol directive provided by the mod_ssl module. This directive can be set either at the server level or in a virtual host configuration.

```
SSLProtocol +TLSv1.2
```

- For Nginx, locate any use of the directive ssl_protocols in the nginx.conf file and remove TLSv1.1.

```
ssl_protocols TLSv1.2;
```

- For Microsoft IIS, you should make some changes on the system registry. **Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.**
 1. Click on Start and then Run, type regedt32 or regedit, and then click OK.
 2. In Registry Editor, locate the following registry key or create it if it does not exist:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\
```

3. Locate a key named Server or create if it doesn't exist.
 4. Under the Server key, locate a DWORD value named Enabled or create if it doesn't exist and set its value to "0".
- For lighttpd, put the following lines in your configuration file:

```
ssl.use-ssl2 = "disable"  
ssl.use-ssl3 = "disable"  
ssl.openssl.ssl-conf-cmd = ("Protocol" => "-TLSv1.1, -TLSv1, -SSLv3") # v1.4.48 or up  
ssl.ec-curve = "secp384r1"
```

External References

- [Deprecating TLSv1.0 and TLSv1.1 draft-ietf-tls-oldversions-deprecate-00](#)
- [Google Security Blog: Modernizing Transport Security](#)
- [OWASP - Insecure Configuration Management](#)
- [OWASP Top 10 - 2017 A3 - Sensitive Data Exposure](#)
- [IIS Crypto is a free tool that gives administrators the ability to enable or disable protocols, ciphers, hashes and key exchange algorithms on Windows Server 2003, 2008 and 2012](#)
- [Date Change for Migrating from SSL and Early TLS](#)



CLASSIFICATION

PCI DSS v3.2	6.5.4
OWASP 2013	A6
OWASP 2017	A3
SANS Top 25	326
CAPEC	217
WASC	4
HIPAA	164.306
ISO27001	A.14.1.3

11. Missing X-XSS-Protection Header

BEST PRACTICE



1

Netsparker detected a missing X-XSS-Protectionheader which means that this website could be at risk of a Cross-site Scripting (XSS) attacks.

Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

Vulnerabilities

11.1. <https://marketplace.uber.com/>

Certainty



Request

```
GET / HTTP/1.1
Host: marketplace.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 1845.9581 Total Bytes Received : 70963 Body Length : 70684 Is Compressed : No

```
HTTP/1.1 200 OK
transfer-encoding: chunked
Server: nginx/1.14.1
X-Powered-By: Next.js
Vary: Accept-Encoding
Connection: keep-alive
Content-Type: text/html; charset=utf-8
Content-Encoding:
Date: Mon, 19 Oct 2020 06:47:59 GMT
ETag: "1141c-qLKWNeY7aNm3rSdIPMTEoQtJkjk"
```

```
<!DOCTYPE html><html class="no-js" lang="en"><head><meta charset="utf-8"/><meta http-equiv="x-ua-compatible" content="ie=edge"/><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"/><meta name="google-site-verification" content="yHvJ7x6qUkjrZRfaPzS05Iu42eP70uSS0Q88xPFBbSU"/><script src="https://polyfill.io/v2/polyfill.min.js?features=IntersectionObserver,Object.assign,Array.prototype.includes,Array.from,Array.prototype.find,Array.prototype.includes,String.prototype.startsWith,String.prototype.includes"></script><meta name="viewport" content="width=device-width"/><meta charset="utf-8"/><title>Marketplace | Uber</title><meta name="description" content="Learn about Uber's ridesharing marketplace and the principles that shape its design."/><meta property="og:title" content="Marketplace | Uber"/><meta property="og:description" content="Learn about Uber's ridesharing marketplace and the principles that shape its design."/><meta property="og:image" content="//images.ctfassets.net/kdwjnue2f64p/xjVlQoLAM88Qcgcg6m0Wy/a9bd5a146ce778b9cd379ec05e4d3aa9/share.png"/><meta property="og:image:width" content="1200"/><meta property="og:image:height" content="628"/><link rel="preload" href="//videos.ctfassets.net/kdwjnue2f64p/2CDUpWxmMM2qe8SAWGSycS/e0de83cfdc9f3c921c1ca30dd1a0c29f/forweb_loop_102318_under3mb.webmhd.webm" as="video" type="video/mp4"/><meta name="next-head-count" content="10"/><link rel="preload" href="/_next/static/css/styles.793d9c7f.chunk.css" as="style"/><link rel="stylesheet" href="/_next/static/css/styles.793d9c7f.chunk.css"/><link rel="preload" href="/_next/static/css/fa0d2a8633984918f0d634ef03f7b793f79d704a_CSS.5077fd2c.chunk.css" as="style"/><lin
...
```

Remedy

Add the X-XSS-Protection header with a value of "1; mode= block".

- X-XSS-Protection: 1; mode=block

External References

- [Internet Explorer 8 Security Features - MSDN](#)
- [X-XSS-Protection HTTP Header](#)
- [Internet Explorer 8 XSS Filter](#)



CLASSIFICATION

SANS Top 25	<u>16</u>
WASC	<u>15</u>
HIPAA	<u>164.308(A)</u>
ISO27001	<u>A.14.2.5</u>

12. Referrer-Policy Not Implemented

BEST PRACTICE



1

Netsparker detected that no Referrer-Policy header implemented.

Referrer-Policy is a security header designed to prevent cross-domain Referer leakage.

Impact

Referer header is a request header that indicates the site which the traffic originated from. If there is no adequate prevention in place, the URL itself, and even sensitive information contained in the URL will be leaked to the cross-site.

The lack of Referrer-Policy header might affect privacy of the users and site's itself

Vulnerabilities

12.1. <https://marketplace.uber.com/>

Certainty



Request

```
GET / HTTP/1.1
Host: marketplace.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 1845.9581 Total Bytes Received : 70963 Body Length : 70684 Is Compressed : No

```
HTTP/1.1 200 OK
transfer-encoding: chunked
Server: nginx/1.14.1
X-Powered-By: Next.js
Vary: Accept-Encoding
Connection: keep-alive
Content-Type: text/html; charset=utf-8
Content-Encoding:
Date: Mon, 19 Oct 2020 06:47:59 GMT
ETag: "1141c-qLKWNeY7aNm3rSdIPMTeoQtJkjk"
```

```
<!DOCTYPE html><html class="no-js" lang="en"><head><meta charset="utf-8"/><meta http-equiv="x-ua-compatible" content="ie=edge"/><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"/><meta name="google-site-verification" content="yHvJ7x6qUkJrzRfaPzS05Iu42eP70uSS0Q88xPFBbSU"/><script src="https://polyfill.io/v2/polyfill.min.js?features=IntersectionObserver,Object.assign,Array.prototype.includes,Array.from,Array.prototype.find,Array.prototype.includes,String.prototype.startsWith,String.prototype.includes"></script><meta name="viewport" content="width=device-width"/><meta charset="utf-8"/><title>Marketplace | Uber</title><meta name="description" content="Learn about Uber's ridesharing marketplace and the principles that shape its design."/><meta property="og:title" content="Marketplace | Uber"/><meta property="og:description" content="Learn about Uber's ridesharing marketplace and the principles that shape its design."/><meta property="og:image" content="//images.ctfassets.net/kdwjnue2f64p/xjVlQoLAM88Qcgcg6m0Wy/a9bd5a146ce778b9cd379ec05e4d3aa9/share.png"/><meta property="og:image:width" content="1200"/><meta property="og:image:height" content="628"/><link rel="preload" href="//videos.ctfassets.net/kdwjnue2f64p/2CDUpWxmMM2qe8SAWGSycS/e0de83cfdc9f3c921c1ca30dd1a0c29f/forweb_loop_102318_under3mb.webmhd.webm" as="video" type="video/mp4"/><meta name="next-head-count" content="10"/><link rel="preload" href="/_next/static/css/styles.793d9c7f.chunk.css" as="style"/><link rel="stylesheet" href="/_next/static/css/styles.793d9c7f.chunk.css"/><link rel="preload" href="/_next/static/css/fa0d2a8633984918f0d634ef03f7b793f79d704a_CSS.5077fd2c.chunk.css" as="style"/><lin
...
```

Actions to Take

In a response header:

```
Referrer-Policy: no-referrer | same-origin | origin | strict-origin | no-origin-when-downgrading
```

In a META tag

```
<meta name="Referrer-Policy" value="no-referrer | same-origin"/>
```

In an element attribute

```
<a href="http://crosssite.example.com" rel="noreferrer"></a>
```

or

```
<a href="http://crosssite.example.com" referrerpolicy="no-referrer | same-origin | origin | strict-origin | no-origin-when-downgrading"></a>
```

Remedy

Please implement a Referrer-Policy by using the Referrer-Policy response header or by declaring it in the meta tags. It’s also possible to control referrer information over an HTML-element by using the rel attribute.

External References

- [Referrer Policy](#)
- [Referrer Policy - MDN](#)
- [Referrer Policy HTTP Header](#)
- [A New Security Header: Referrer Policy](#)
- [Can I Use Referrer-Policy](#)



CLASSIFICATION

OWASP 2013	A6
OWASP 2017	A3
SANS Top 25	200
ISO27001	A.14.2.5

13. SameSite Cookie Not Implemented

BEST PRACTICE



1

Cookies are typically sent to third parties in cross origin requests. This can be abused to do CSRF attacks. Recently a new cookie attribute named *SameSite* was proposed to disable third-party usage for some cookies, to prevent CSRF attacks.

Same-site cookies allow servers to mitigate the risk of CSRF and information leakage attacks by asserting that a particular cookie should only be sent with requests initiated from the same registrable domain.

Vulnerabilities

13.1. <https://marketplace.uber.com/>

Identified Cookie(s)

- `_ga`
- `_gid`
- `_gat`

Cookie Source

- JavaScript

Certainty

Request

```
GET / HTTP/1.1
Host: marketplace.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 1845.9581 Total Bytes Received : 70963 Body Length : 70684 Is Compressed : No

```
HTTP/1.1 200 OK
transfer-encoding: chunked
Server: nginx/1.14.1
X-Powered-By: Next.js
Vary: Accept-Encoding
Connection: keep-alive
Content-Type: text/html; charset=utf-8
Content-Encoding:
Date: Mon, 19 Oct 2020 06:47:59 GMT
ETag: "1141c-qLKWNeY7aNm3rSdIPMTEoQtJkjk"
```

```
<!DOCTYPE html><html class="no-js" lang="en"><head><meta charset="utf-8"/><meta http-equiv="x-ua-compatible" content="ie=edge"/><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"/><meta name="google-site-verification" content="yHvJ7x6qUkjrZRfaPzS05Iu42eP70uSS0Q88xPFBbSU"/><script src="https://polyfill.io/v2/polyfill.min.js?features=IntersectionObserver,Object.assign,Array.prototype.includes,Array.from,Array.prototype.find,Array.prototype.includes,String.prototype.startsWith,String.prototype.includes"></script><meta name="viewport" content="width=device-width"/><meta charset="utf-8"/><title>Marketplace | Uber</title><meta name="description" content="Learn about Uber's ridesharing marketplace and the principles that shape its design."/><meta property="og:title" content="Marketplace | Uber"/><meta property="og:description" content="Learn about Uber's ridesharing marketplace and the principles that shape its design."/><meta property="og:image" content="//images.ctfassets.net/kdwjnue2f64p/xjVlQoLAM88Qcgcg6m0Wy/a9bd5a146ce778b9cd379ec05e4d3aa9/share.png"/><meta property="og:image:width" content="1200"/><meta property="og:image:height" content="628"/><link rel="preload" href="//videos.ctfassets.net/kdwjnue2f64p/2CDUpWxmMM2qe8SAWGSycS/e0de83cfdc9f3c921c1ca30dd1a0c29f/forweb_loop_102318_under3mb.webmhd.webm" as="video" type="video/mp4"/><meta name="next-head-count" content="10"/><link rel="preload" href="/_next/static/css/styles.793d9c7f.chunk.css" as="style"/><link rel="stylesheet" href="/_next/static/css/styles.793d9c7f.chunk.css"/><link rel="preload" href="/_next/static/css/fa0d2a8633984918f0d634ef03f7b793f79d704a_CSS.5077fd2c.chunk.css" as="style"/><lin
...
```

Remedy

The server can set a same-site cookie by adding the `SameSite=...` attribute to the `Set-Cookie` header. There are three possible values for the `SameSite` attribute:

- **Lax:** In this mode, the cookie will only be sent with a top-level get request.

```
Set-Cookie: key=value; SameSite=Lax
```

- **Strict:** In this mode, the cookie will not be sent with any cross-site usage even if the user follows a link to another website.

```
Set-Cookie: key=value; SameSite=Strict
```

- None: In this mode, the cookie will be sent with the cross-site requests. Cookies with SameSite=None must also specify the Secure attribute to transfer them via a secure context. Setting a SameSite=None cookie without the Secure attribute will be rejected by the browsers.

```
Set-Cookie: key=value; SameSite=None; Secure
```

External References

- [Security Cookies - SameSite Attribute - Netsparker](#)
- [Using the Same-Site Cookies Attribute to Prevent CSRF Attacks](#)
- [Same-site Cookies](#)
- [Preventing CSRF with the same-site cookie attribute](#)
- [SameSite cookies explained](#)
- [Get Ready for New SameSite=None; Secure Cookie Settings](#)



CLASSIFICATION

SANS Top 25	16
WASC	15
ISO27001	A.14.2.5

14. Subresource Integrity (SRI) Not Implemented

BEST PRACTICE



1

Subresource Integrity (SRI) provides a mechanism to check integrity of the resource hosted by third parties like Content Delivery Networks (CDNs) and verifies that the fetched resource has been delivered without unexpected manipulation.

SRI does this using hash comparison mechanism. In this way, hash value declared in HTML elements (for now only script and link elements are supported) will be compared with the hash value of the resource hosted by third party.

Use of SRI is recommended as a best-practice, whenever libraries are loaded from a third-party source.

Vulnerabilities

14.1. <https://marketplace.uber.com/>

Identified Sub Resource(s)

- <https://polyfill.io/v2/polyfill.min.js?features=IntersectionObserver,Object.assign,Array.prototype.includes,Array.from,Array.prototype.find,Array.prototype.includes,Strin>

Certainty

Request

```
GET / HTTP/1.1
Host: marketplace.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 1845.9581 Total Bytes Received : 70963 Body Length : 70684 Is Compressed : No

```
HTTP/1.1 200 OK
transfer-encoding: chunked
Server: nginx/1.14.1
X-Powered-By: Next.js
Vary: Accept-Encoding
Connection: keep-alive
Content-Type: text/html; charset=utf-8
Content-Encoding:
Date: Mon, 19 Oct 2020 06:47:59 GMT
ETag: "1141c-qLKWNeY7aNm3r
...
content="ie=edge"/><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=n
o"/><meta name="google-site-verification" content="yHvJ7x6qUkjrRfaPzS05Iu42eP70uSS0Q88xPFBbSU"/><scrip
t src="https://polyfill.io/v2/polyfill.min.js?features=IntersectionObserver,Object.assign,Array.prototy
pe.includes,Array.from,Array.prototype.find,Array.prototype.includes,String.prototype.startsWith,Strin
g.prototype.includes"></script><meta name="viewport" content="width=device-width"/><meta charSet="utf-
8"/><title>Marketplace | Uber</title><meta name="description" content="Learn about Uber&#x27;s rideshar
ing marketplace and the pr
...
```

Remedy

Using Subresource Integrity is simply to add *integrity* attribute to the *script* tag along with a base64 encoded cryptographic hash value.

```
<script src="https://code.jquery.com/jquery-2.1.4.min.js" integrity="sha384-
R4/ztc4ZlRqWjqIuvf6RX5yb/v90qNGx6fS48N0tRxiGkqveZETq72KgDVJCp2TC" crossorigin="anonymous"></script>
```

The hash algorithm must be one of **sha256**, **sha384** or **sha512**, followed by a '-' character.

External References

- [Subresource Integrity](#)
- [Do not let your CDN betray you: Use Subresource Integrity](#)
- [Web Application Security with Subresource Integrity](#)
- [SRI Hash Generator](#)



CLASSIFICATION

SANS Top 25	16
WASC	15
ISO27001	A.14.2.5

15. Email Address Disclosure

INFORMATION ⓘ

1

Netsparker identified an Email Address Disclosure.

Impact

Email addresses discovered within the application can be used by both spam email engines and also brute-force tools. Furthermore, valid email addresses may lead to social engineering attacks.

Vulnerabilities

15.1. <https://marketplace.uber.com/principles>

Email Address(es)

- whatmovesus@uber.com

Certainty



Request

```
GET /principles HTTP/1.1
Host: marketplace.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: _gat=1; _ga=GA1.2.1782103013.1603090086; _gid=GA1.2.1734872366.1603090086
Referer: https://marketplace.uber.com/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 604.0802 Total Bytes Received : 33832 Body Length : 33560 Is Compressed : No

```
HTTP/1.1 200 OK
Server: nginx/1.14.1
X-Powered-By: Next.js
Vary: Accept-Encoding
Content-Length: 7874
Connection: keep-alive
Content-Type: text/html; charset=utf-8
Content-Encoding:
Date: Mon, 19 Oct 2020 06:48:31 GMT
ETag: "8318-M36D+Gf1ZYIbU
```

```
...
___5bH5J _pBlock"><p>We are committed to an ongoing conversation. We understand that this site may not
answer every question about our ridesharing marketplace. Please reach out to us <a href="mailto:whatm
ovesus@uber.com" target="_blank" rel="noopener noreferrer">here</a> with additional questions and idea
s.</p></div><div class="reactMarkdown___s4eHa _mdImagelist description___5bH5J _pBlock"><p>We are commi
tted to ta
...
mitments","columnOne":"We are committed to an ongoing conversation. We understand that this site may no
t answer every question about our ridesharing marketplace. Please reach out to us [here](mailto:whatmo
vesus@uber.com\"here\") with additional questions and ideas.","columnTwo":"We are committed to taking a
ction. We will continue to incorporate these principles into our product development so that our market
place d
...

```

Remedy

Use generic email addresses such as contact@ or info@ for general communications and remove user/people-specific email addresses from the website; should this be required, use submission forms for this purpose.

External References

- [Wikipedia - Email Spam](#)



CLASSIFICATION

SANS Top 25	200
CAPEC	118
WASC	13
OWASP Proactive Controls	C7
ISO27001	A.9.4.1

CVSS 3.0 SCORE

Base	5.3 (Medium)
Temporal	5.3 (Medium)
Environmental	5.3 (Medium)

CVSS Vector String

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

CVSS 3.1 SCORE

Base	5.3 (Medium)
Temporal	5.3 (Medium)
Environmental	5.3 (Medium)

CVSS Vector String

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N



16. Nginx Web Server Identified

INFORMATION ⓘ

1

Netsparker identified a web server (Nginx) in the target web server's HTTP response.

Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

Vulnerabilities

16.1. <https://marketplace.uber.com/>

Certainty



Request

```
GET / HTTP/1.1
Host: marketplace.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 1845.9581 Total Bytes Received : 70963 Body Length : 70684 Is Compressed : No

```
HTTP/1.1 200 OK
transfer-encoding: chunked
Server: nginx/1.14.1
X-Powered-By: Next.js
Vary: Accept-Encoding
Connection: keep-alive
Content-Type: text/html; charset=utf-8
Content-Encoding:
Date: Mon, 19 Oct 2020 06:47:59 GMT
ETag: "1141c-qLKWNeY7aNm3rHTTP/1.1 200 OK
transfer-encoding: chunked
Server: nginx/1.14.1
X-Powered-By: Next.js
Vary: Accept-Encoding
Connection: keep-alive
Content-Type: text/html; charset=utf-8
Content-Encoding:
Date: Mon, 19 Oct 2020 06:47:59 GMT
ETag: "1141c-qLKWNeY7aNm
```

...



CLASSIFICATION

SANS Top 25	200
WASC	13
OWASP Proactive Controls	C7
ISO27001	A.18.1.3

CVSS 3.0 SCORE

Base	5.3 (Medium)
Temporal	5.1 (Medium)
Environmental	5.1 (Medium)

CVSS Vector String

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:H/RL:O/RC:C

CVSS 3.1 SCORE

Base	5.3 (Medium)
Temporal	5.1 (Medium)
Environmental	5.1 (Medium)

CVSS Vector String

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:H/RL:O/RC:C

17. Out-of-date Version (Nginx)

INFORMATION ⓘ

1

Netsparker identified you are using an out-of-date version of Nginx.

Impact

Since this is an old version of the software, it may be vulnerable to attacks.

Vulnerabilities

17.1. <https://marketplace.uber.com/>

Identified Version

- 1.14.1

Latest Version

- 1.17.8 (in this branch)

Vulnerability Database

- Result is based on 04/27/2020 17:30:00 vulnerability database content.

Certainty



Request

```
GET / HTTP/1.1
Host: marketplace.uber.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 1845.9581 Total Bytes Received : 70963 Body Length : 70684 Is Compressed : No

```
HTTP/1.1 200 OK
transfer-encoding: chunked
Server: nginx/1.14.1
X-Powered-By: Next.js
Vary: Accept-Encoding
Connection: keep-alive
Content-Type: text/html; charset=utf-8
Content-Encoding:
Date: Mon, 19 Oct 2020 06:47:59 GMT
ETag: "1141c-qLKWNeY7aNm3rHTTP/1.1 200 OK
transfer-encoding: chunked
Server: nginx/1.14.1
X-Powered-By: Next.js
Vary: Accept-Encoding
Connection: keep-alive
Content-Type: text/html; charset=utf-8
Content-Encoding:
Date: Mon, 19 Oct 2020 06:47:59 GMT
ETag: "1141c-qLKWNeY7aNm3rSdIPM
...
```

Remedy

Please upgrade your installation of Nginx to the latest stable version.

Remedy References

- [Downloading Nginx](#)



CLASSIFICATION

PCI DSS v3.2	6.2
OWASP 2013	A9
OWASP 2017	A9
SANS Top 25	829
CAPEC	310
WASC	13
HIPAA	164.308(A)(1)(I)
OWASP Proactive Controls	C1
ISO27001	A.14.1.2

Show Scan Detail

Enabled Security Checks

: Apache Struts S2-045 RCE,
Apache Struts S2-046 RCE,
BREACH Attack,
Code Evaluation,
Code Evaluation (Out of Band),
Command Injection,
Command Injection (Blind),
Content Security Policy,
Content-Type Sniffing,
Cookie,
Cross Frame Options Security,
Cross-Origin Resource Sharing (CORS),
Cross-Site Request Forgery,
Cross-site Scripting,
Cross-site Scripting (Blind),
Custom Script Checks (Active),
Custom Script Checks (Passive),
Custom Script Checks (Per Directory),
Custom Script Checks (Singular),
Drupal Remote Code Execution,

Expect Certificate Transparency (Expect-CT),
Expression Language Injection,
File Upload,
Header Analyzer,
Heartbleed,
HSTS,
HTML Content,
HTTP Header Injection,
HTTP Methods,
HTTP Status,
HTTP.sys (CVE-2015-1635),
IFrame Security,
Insecure JSONP Endpoint,
Insecure Reflected Content,
JavaScript Libraries,
Local File Inclusion,
Login Page Identifier,
Mixed Content,
Open Redirection,
Referrer Policy,
Reflected File Download,
Remote File Inclusion,
Remote File Inclusion (Out of Band),
Reverse Proxy Detection,
RoR Code Execution,
Server-Side Request Forgery (DNS),
Server-Side Request Forgery (Pattern Based),
Server-Side Template Injection,
Signatures,
SQL Injection (Blind),
SQL Injection (Boolean),
SQL Injection (Error Based),
SQL Injection (Out of Band),
SSL,
Static Resources (All Paths),
Static Resources (Only Root Path),
Unicode Transformation (Best-Fit Mapping),
WAF Identifier,
Web App Fingerprint,
Web Cache Deception,
WebDAV,
Windows Short Filename,
XML External Entity,
XML External Entity (Out of Band)

URL Rewrite Mode	: Heuristic
-------------------------	-------------

Detected URL Rewrite Rule(s)	: None
-------------------------------------	--------

Excluded URL Patterns	: (log sign)\-?(out off) exit endsession
------------------------------	--

gtm\js
WebResource\axd
ScriptResource\axd

Authentication : None

Scheduled : No

Additional Website(s) : None

This report created with 5.8.1.28119-master-bca4e4e
<https://www.netsparker.com>