# netsparker

# OWASP Top Ten 2013 Report

🔗 https://marketplace.uber.com/

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

## Explanation

This report is generated based on OWASP Top Ten 2013 classification.
There are 7 more vulnerabilities that are not shown below. Please take a look at the detailed scan report to see them.
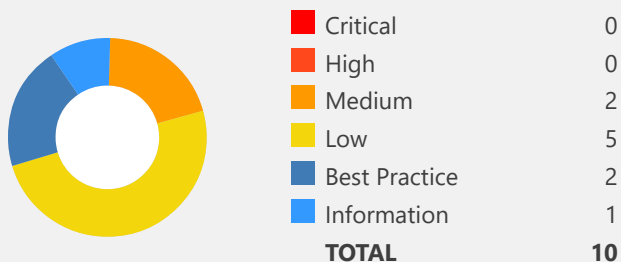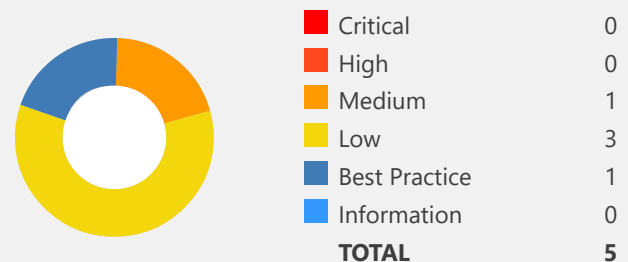
| 10 IDENTIFIED | 5 CONFIRMED | 0 ⊘ CRITICAL |
|---|---|---|

| 0 ⚑ HIGH | 2 ⚑ MEDIUM | 5 ⚑ LOW |
|---|---|---|
| | 2 💡 BEST PRACTICE | 1 ℹ INFORMATION |

## Identified Vulnerabilities

| | | |
|---|---|---|
| 🟥 | Critical | 0 |
| 🟧 | High | 0 |
| 🟧 | Medium | 2 |
| 🟨 | Low | 5 |
| 🟦 | Best Practice | 2 |
| 🟦 | Information | 1 |
| | **TOTAL** | **10** |

## Confirmed Vulnerabilities

| | | |
|---|---|---|
| 🟥 | Critical | 0 |
| 🟧 | High | 0 |
| 🟧 | Medium | 1 |
| 🟨 | Low | 3 |
| 🟦 | Best Practice | 1 |
| 🟦 | Information | 0 |
| | **TOTAL** | **5** |

# Vulnerabilities By OWASP 2013

| CONFIRM | VULNERABILITY | METHOD | URL | SEVERITY |
|---------|---------------|--------|-----|----------|

## A5 - SECURITY MISCONFIGURATION

| | Cookie Not Marked as HttpOnly | GET | https://marketplace.uber.com/ | LOW |
| | Missing X-Frame-Options Header | GET | https://marketplace.uber.com/ | LOW |
| | Version Disclosure (Nginx) | GET | https://marketplace.uber.com/ | LOW |

## A6 - SENSITIVE DATA EXPOSURE

| | Weak Ciphers Enabled | GET | https://marketplace.uber.com/ | MEDIUM |
| | HTTP Strict Transport Security (HSTS) Policy Not Enabled | GET | https://marketplace.uber.com/ | MEDIUM |
| | Cookie Not Marked as Secure | GET | https://marketplace.uber.com/ | LOW |
| | Insecure Transportation Security Protocol Supported (TLS 1.0) | GET | https://marketplace.uber.com/ | LOW |
| | Insecure Transportation Security Protocol Supported (TLS 1.1) | GET | https://marketplace.uber.com/ | BEST PRACTICE |
| | Referrer-Policy Not Implemented | GET | https://marketplace.uber.com/ | BEST PRACTICE |

## A9 - USING COMPONENTS WITH KNOWN VULNERABILITIES

| | Out-of-date Version (Nginx) | GET | https://marketplace.uber.com/ | INFORMATION |

# 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-compat
ible" content="ie=edge"/><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-
fit=no"/><meta name="google-site-verification" content="yHvJ7x6qUkjrzRfaPzSO5Iu42eP70uSS0Q88xPFBbSU"/><
script src="https://polyfill.io/v2/polyfill.min.js?features=IntersectionObserver,Object.assign,Array.pr
ototype.includes,Array.from,Array.prototype.find,Array.prototype.includes,String.prototype.startsWith,S
tring.prototype.includes"></script><meta name="viewport" content="width=device-width"/><meta charSet="u
tf-8"/><title>Marketplace | Uber</title><meta name="description" content="Learn about Uber&#x27;s rides
haring marketplace and the principles that shape its design."/><meta property="og:title" content="Marke
tplace | Uber"/><meta property="og:description" content="Learn about Uber&#x27;s ridesharing marketplac
e and the principles that shape its design."/><meta property="og:image" content="//images.ctfassets.ne
t/kdwjnue2f64p/xjVlQoLAM88Qcgcg6mOWy/a9bd5a146ce778b9cd379ec05e4d3aa9/share.png"/><meta property="og:im
age:width" content="1200"/><meta property="og:image:height" content="628"/><link rel="preload" href="//
videos.ctfassets.net/kdwjnue2f64p/2CDUpWxmMM2qe8SAWGSycS/e0de83cfdc9f3c921c1ca30dd1a0c29f/forweb_loop_1
02318_under3mb.webmhd.webm" as="video" type="video/mp4"/><meta name="next-head-count" content="10"/><li
nk 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/fa0d2a
8633984918f0d634ef03f7b793f79d704a_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](#) |

# 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

| | |
|---|---|
| OWASP 2013 | |

### 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. 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

### 3.1. 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\T
     LS 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-sslv2 = "disable"
ssl.use-sslv3 = "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**

OWASP 2013                                                                                                   A6

# 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-compat
ible" content="ie=edge"/><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-
fit=no"/><meta name="google-site-verification" content="yHvJ7x6qUkjrzRfaPzSO5Iu42eP70uSS0Q88xPFBbSU"/><
script src="https://polyfill.io/v2/polyfill.min.js?features=IntersectionObserver,Object.assign,Array.pr
ototype.includes,Array.from,Array.prototype.find,Array.prototype.includes,String.prototype.startsWith,S
tring.prototype.includes"></script><meta name="viewport" content="width=device-width"/><meta charSet="u
tf-8"/><title>Marketplace | Uber</title><meta name="description" content="Learn about Uber&#x27;s rides
haring marketplace and the principles that shape its design."/><meta property="og:title" content="Marke
tplace | Uber"/><meta property="og:description" content="Learn about Uber&#x27;s ridesharing marketplac
e and the principles that shape its design."/><meta property="og:image" content="//images.ctfassets.ne
t/kdwjnue2f64p/xjVlQoLAM88Qcgcg6mOWy/a9bd5a146ce778b9cd379ec05e4d3aa9/share.png"/><meta property="og:im
age:width" content="1200"/><meta property="og:image:height" content="628"/><link rel="preload" href="//
videos.ctfassets.net/kdwjnue2f64p/2CDUpWxmMM2qe8SAWGSycS/e0de83cfdc9f3c921c1ca30dd1a0c29f/forweb_loop_1
02318_under3mb.webmhd.webm" as="video" type="video/mp4"/><meta name="next-head-count" content="10"/><li
nk 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/fa0d2a
8633984918f0d634ef03f7b793f79d704a_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

| OWASP 2013 | A6 |
| --- | --- |

### 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. 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

### 5.1. 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-compat
ible" content="ie=edge"/><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-
fit=no"/><meta name="google-site-verification" content="yHvJ7x6qUkjrzRfaPzSO5Iu42eP70uSS0Q88xPFBbSU"/><
script src="https://polyfill.io/v2/polyfill.min.js?features=IntersectionObserver,Object.assign,Array.pr
ototype.includes,Array.from,Array.prototype.find,Array.prototype.includes,String.prototype.startsWith,S
tring.prototype.includes"></script><meta name="viewport" content="width=device-width"/><meta charSet="u
tf-8"/><title>Marketplace | Uber</title><meta name="description" content="Learn about Uber&#x27;s rides
haring marketplace and the principles that shape its design."/><meta property="og:title" content="Marke
tplace | Uber"/><meta property="og:description" content="Learn about Uber&#x27;s ridesharing marketplac
e and the principles that shape its design."/><meta property="og:image" content="//images.ctfassets.ne
t/kdwjnue2f64p/xjVlQoLAM88Qcgcg6mOWy/a9bd5a146ce778b9cd379ec05e4d3aa9/share.png"/><meta property="og:im
age:width" content="1200"/><meta property="og:image:height" content="628"/><link rel="preload" href="//
videos.ctfassets.net/kdwjnue2f64p/2CDUpWxmMM2qe8SAWGSycS/e0de83cfdc9f3c921c1ca30dd1a0c29f/forweb_loop_1
02318_under3mb.webmhd.webm" as="video" type="video/mp4"/><meta name="next-head-count" content="10"/><li
nk 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/fa0d2a
8633984918f0d634ef03f7b793f79d704a_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](#)

**CLASSIFICATION**

OWASP 2013                                                                A5

# 6. 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

### 6.1. 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

# 7. 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

### 7.1. 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-compat
ible" content="ie=edge"/><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-
fit=no"/><meta name="google-site-verification" content="yHvJ7x6qUkjrzRfaPzSO5Iu42eP70uSS0Q88xPFBbSU"/><
script src="https://polyfill.io/v2/polyfill.min.js?features=IntersectionObserver,Object.assign,Array.pr
ototype.includes,Array.from,Array.prototype.find,Array.prototype.includes,String.prototype.startsWith,S
tring.prototype.includes"></script><meta name="viewport" content="width=device-width"/><meta charSet="u
tf-8"/><title>Marketplace | Uber</title><meta name="description" content="Learn about Uber&#x27;s rides
haring marketplace and the principles that shape its design."/><meta property="og:title" content="Marke
tplace | Uber"/><meta property="og:description" content="Learn about Uber&#x27;s ridesharing marketplac
e and the principles that shape its design."/><meta property="og:image" content="//images.ctfassets.ne
t/kdwjnue2f64p/xjVlQoLAM88Qcgcg6mOWy/a9bd5a146ce778b9cd379ec05e4d3aa9/share.png"/><meta property="og:im
age:width" content="1200"/><meta property="og:image:height" content="628"/><link rel="preload" href="//
videos.ctfassets.net/kdwjnue2f64p/2CDUpWxmMM2qe8SAWGSycS/e0de83cfdc9f3c921c1ca30dd1a0c29f/forweb_loop_1
02318_under3mb.webmhd.webm" as="video" type="video/mp4"/><meta name="next-head-count" content="10"/><li
nk 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/fa0d2a
8633984918f0d634ef03f7b793f79d704a_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: DENY`It completely denies to be loaded in frame/iframe.
    - `X-Frame-Options: SAMEORIGIN`It allows only if the site which wants to load has a same origin.
    - `X-Frame-Options: ALLOW-FROM` *URL*It 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](#) |

---

# 8. 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

### 8.1. 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 if it does not exist:

        ```
        HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\T
        LS 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-sslv2 = "disable"
ssl.use-sslv3 = "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**

OWASP 2013                                                                                                    [A6](#)

---

# 9. 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

### 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-compat
ible" content="ie=edge"/><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-
fit=no"/><meta name="google-site-verification" content="yHvJ7x6qUkjrzRfaPzSO5Iu42eP70uSS0Q88xPFBbSU"/><
script src="https://polyfill.io/v2/polyfill.min.js?features=IntersectionObserver,Object.assign,Array.pr
ototype.includes,Array.from,Array.prototype.find,Array.prototype.includes,String.prototype.startsWith,S
tring.prototype.includes"></script><meta name="viewport" content="width=device-width"/><meta charSet="u
tf-8"/><title>Marketplace | Uber</title><meta name="description" content="Learn about Uber&#x27;s rides
haring marketplace and the principles that shape its design."/><meta property="og:title" content="Marke
tplace | Uber"/><meta property="og:description" content="Learn about Uber&#x27;s ridesharing marketplac
e and the principles that shape its design."/><meta property="og:image" content="//images.ctfassets.ne
t/kdwjnue2f64p/xjVlQoLAM88Qcgcg6mOWy/a9bd5a146ce778b9cd379ec05e4d3aa9/share.png"/><meta property="og:im
age:width" content="1200"/><meta property="og:image:height" content="628"/><link rel="preload" href="//
videos.ctfassets.net/kdwjnue2f64p/2CDUpWxmMM2qe8SAWGSycS/e0de83cfdc9f3c921c1ca30dd1a0c29f/forweb_loop_1
02318_under3mb.webmhd.webm" as="video" type="video/mp4"/><meta name="next-head-count" content="10"/><li
nk 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/fa0d2a
8633984918f0d634ef03f7b793f79d704a_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

---

# 10. 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

### 10.1. 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**

OWASP 2013                                                                                           A9

---

# Show Scan Detail ⌄

| | | |
|---|---|---|
| **Enabled Security Checks** | : | Apache Struts S2-045 RCE,<br>Apache Struts S2-046 RCE,<br>BREACH Attack,<br>Code Evaluation,<br>Code Evaluation (Out of Band),<br>Command Injection,<br>Command Injection (Blind),<br>Content Security Policy,<br>Content-Type Sniffing,<br>Cookie,<br>Cross Frame Options Security,<br>Cross-Origin Resource Sharing (CORS),<br>Cross-Site Request Forgery,<br>Cross-site Scripting,<br>Cross-site Scripting (Blind),<br>Custom Script Checks (Active),<br>Custom Script Checks (Passive),<br>Custom Script Checks (Per Directory),<br>Custom Script Checks (Singular),<br>Drupal Remote Code Execution,<br>Expect Certificate Transparency (Expect-CT),<br>Expression Language Injection,<br>File Upload,<br>Header Analyzer,<br>Heartbleed,<br>HSTS,<br>HTML Content,<br>HTTP Header Injection,<br>HTTP Methods,<br>HTTP Status,<br>HTTP.sys (CVE-2015-1635),<br>IFrame Security,<br>Insecure JSONP Endpoint,<br>Insecure Reflected Content,<br>JavaScript Libraries,<br>Local File Inclusion,<br>Login Page Identifier,<br>Mixed Content,<br>Open Redirection,<br>Referrer Policy,<br>Reflected File Download,<br>Remote File Inclusion,<br>Remote File Inclusion (Out of Band),<br>Reverse Proxy Detection,<br>RoR Code Execution,<br>Server-Side Request Forgery (DNS),<br>Server-Side Request Forgery (Pattern Based),<br>Server-Side Template Injection,<br>Signatures,<br>SQL Injection (Blind),<br>SQL Injection (Boolean),<br>SQL Injection (Error Based),<br>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)<br>exit<br>endsession<br>gtm\.js<br>WebResource\.axd<br>ScriptResource\.axd |
| **Authentication** | : None |
| **Scheduled** | : No |
| **Additional Website(s)** | : None |