Web Application Scanning Detailed Scan Export: Web app scan Juice Shop & bWAAP

November 19, 2024 at 13:44 (UTC)

servicedesk@hst.com.br-20129cec

Confidential: The following report contains sensitive security information about the organization’s IT infrastructure. Refer to your company’s policy regarding data classification and handling of sensitive information.

Table of Contents

Scan Summary

Vulnerability Breakdown

26 CRITICAL	12 HIGH	41 MEDIUM	128 LOW

Scan Details

NAME	Web app scan Juice Shop & bWAAP
STATUS	Completed
CREATE TIME	11/19/2024 at 12:08 AM UTC
START TIME	11/19/2024 at 12:10 AM UTC
END TIME	11/19/2024 at 09:46 AM UTC
TEMPLATE	Scan
SCANNER	Cloud
TARGET	https://juice-shop-388277804329.us-west1.run.app/#/
DESCRIPTION	

Scan Notes

Severity	Scan Notes	
Medium	Request Redirect Limit Reached	URL https://juice-shop-388277804329.us-west1.run.app/portal.php/?x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=& was not able to be fully audited due to reaching request redirect limit of 20
Info	Maximum number of results published	Maximum number of instances to be reported for plugin ID 98050 has been reached. Scanner will not publish any other results
Info	Authentication Detected	The scanner has identified an authentication mechanism which could prevent it from accessing application pages.
Info	Debug Mode Enabled	This scan has been configured with debug mode enabled. In this mode, the scanner provides extra information in plugin outpu

Scan Results

Vulnerabilities

Severity	Plugin Id	Name	Family	Instances
Critical	98230	PHP Unsupported Version	Component Vulnerability	14
Critical	98912	Apache 2.4.x < 2.4.27 Multiple Vulnerabilities	Component Vulnerability	1
Critical	113545	Apache 2.4.x < 2.4.55 Multiple Vulnerabilities	Component Vulnerability	1
Critical	113254	Apache 2.4.x < 2.4.54 Multiple Vulnerabilities	Component Vulnerability	1
Critical	113194	Apache 2.4.x < 2.4.53 Multiple Vulnerabilities	Component Vulnerability	1
Critical	113079	Apache 2.4.x < 2.4.52 Multiple Vulnerabilities	Component Vulnerability	1
Critical	98911	Apache 2.4.x < 2.4.26 Multiple Vulnerabilities	Component Vulnerability	1
Critical	114360	Apache 2.4.x < 2.4.60 Multiple Vulnerabilities	Component Vulnerability	1
Critical	113673	Apache 2.4.x < 2.4.56 Multiple Vulnerabilities	Component Vulnerability	1
Critical	112981	Apache 2.4.x < 2.4.49 Multiple Vulnerabilities	Component Vulnerability	1
Critical	112806	Apache 2.4.x < 2.4.48 Multiple Vulnerabilities	Component Vulnerability	1
Critical	98669	Apache 2.4.x < 2.4.41 Multiple Vulnerabilities	Component Vulnerability	1
Critical	98914	Apache 2.4.x < 2.4.33 Multiple Vulnerabilities	Component Vulnerability	1
High	114090	Apache 2.4.x < 2.4.58 Multiple Vulnerabilities	Component Vulnerability	1
High	98530	Apache 2.4.x < 2.4.39 Multiple Vulnerabilities	Component Vulnerability	1
High	98537	Apache 2.4.x < 2.4.38 Multiple Vulnerabilities	Component Vulnerability	1
High	98905	Apache 2.4.x < 2.4.9 Multiple Vulnerabilities	Component Vulnerability	1
High	98906	Apache 2.4.x < 2.4.10 Multiple Vulnerabilities	Component Vulnerability	1
High	98907	Apache 2.4.x < 2.4.12 Multiple Vulnerabilities	Component Vulnerability	1
High	98908	Apache 2.4.x < 2.4.16 Multiple Vulnerabilities	Component Vulnerability	1
High	98910	Apache 2.4.x < 2.4.25 Multiple Vulnerabilities (httpoxy)	Component Vulnerability	1
High	98913	Apache 2.4.x < 2.4.28 HTTP Vulnerability (OptionsBleed)	Component Vulnerability	1
High	98915	Apache 2.4.x < 2.4.34 Multiple Vulnerabilities	Component Vulnerability	1
High	114249	Apache 2.4.x < 2.4.59 Multiple Vulnerabilities	Component Vulnerability	1
High	114385	Apache 2.4.x < 2.4.62 Multiple Vulnerabilities	Component Vulnerability	1
Medium	98056	Missing HTTP Strict Transport Security Policy	HTTP Security Header	25
Medium	98084	Directory Listing	Web Servers	8
Medium	98779	Source Code Passive Disclosure	Data Exposure	2
Medium	98916	Apache 2.4.x < 2.4.35 Denial of Service	Component Vulnerability	1
Medium	114195	Web Server Configuration File Detected	Data Exposure	1
Medium	98998	Apache 2.4.x < 2.4.43 Multiple Vulnerabilities	Component Vulnerability	1
Medium	98617	SSL/TLS Forward Secrecy Cipher Suites Not Supported	SSL/TLS	1
Medium	98594	Web.config File Information Disclosure	Data Exposure	1
Medium	98223	PHPinfo Information Disclosure	Web Applications	1
Low	98060	Missing 'X-Frame-Options' Header	HTTP Security Header	25
Low	112529	Missing 'X-Content-Type-Options' Header	HTTP Security Header	25
Low	112553	Missing 'Cache-Control' Header	HTTP Security Header	25
Low	98618	HTTP Header Information Disclosure	HTTP Security Header	25
Low	112551	Missing Content Security Policy	HTTP Security Header	22

Severity	Plugin Id	Name	Family	Instances
Low	113332	Login Form Cross-Site Request Forgery	Cross Site Request Forgery	1
Low	98081	Password Field With Auto-Complete	Authentication & Session	1
Low	98063	Cookie Without HttpOnly Flag Detected	HTTP Security Header	1
Low	115540	Cookie Without SameSite Flag Detected	HTTP Security Header	1
Low	112539	SSL/TLS Weak Cipher Suites Supported	SSL/TLS	1
Low	98064	Cookie Without Secure Flag Detected	HTTP Security Header	1

PHP Unsupported Version

VULNERABILITY CRITICAL PLUGIN ID 98230

Description

The installation of PHP detected on the remote host is no longer supported. Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

Solution

Upgrade to a supported version of PHP.

See Also

http://php.net/supported-versions.php

Plugin Details

PUBLICATION DATE	2018-08-09T00:00:00+00:00
MODIFICATION DATE	2024-01-11T00:00:00+00:00
FAMILY	Component Vulnerability
SEVERITY	Critical
PLUGIN ID	98230

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	10.0
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
CVSS BASE SCORE	10.0
CVSS VECTOR	CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Reference Information

CWE	16
WASC	Application Misconfiguration
OWASP	2021-A5, 2013-A5, 2013-A9, 2017-A9, 2017-A6, 2021-A6, 2010-A6, 2023-API8, 2019-API7
CVE	-
BID	-

PHP Unsupported Version Instances (14)

VULNERABILITY CRITICAL PLUGIN ID 98230

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/#/

Identification

OUTPUT

```
Technology PHP version 5.5.9 has been detected. Upgrade to the last supported version of PHP: 8.1
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/info_install.php

Identification

OUTPUT

```
Technology PHP version 5.5.9 has been detected. Upgrade to the last supported version of PHP: 8.1
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/soap/nusoap.php

Identification

OUTPUT

```
Technology PHP version 5.5.9 has been detected. Upgrade to the last supported version of PHP: 8.1
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/user_new.php

Identification

OUTPUT

```
Technology PHP version 5.5.9 has been detected. Upgrade to the last supported version of PHP: 8.1
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/phpinfo.php

Identification

OUTPUT

```
Technology PHP version 5.5.9 has been detected. Upgrade to the last supported version of PHP: 8.1
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/soap/class.wsdlcache.php

Identification

OUTPUT

```
Technology PHP version 5.5.9 has been detected. Upgrade to the last supported version of PHP: 8.1
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/portal.php

Identification

OUTPUT

```
Technology PHP version 5.5.9 has been detected. Upgrade to the last supported version of PHP: 8.1
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/install.php

Identification

OUTPUT

```
Technology PHP version 5.5.9 has been detected. Upgrade to the last supported version of PHP: 8.1
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/soap/class.nusoap_base.php

Identification

OUTPUT

```
Technology PHP version 5.5.9 has been detected. Upgrade to the last supported version of PHP: 8.1
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/soap/class.soap_fault.php

Identification

OUTPUT

```
Technology PHP version 5.5.9 has been detected. Upgrade to the last supported version of PHP: 8.1
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/info.php

Identification

OUTPUT

```
Technology PHP version 5.5.9 has been detected. Upgrade to the last supported version of PHP: 8.1
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/login.php

Identification

OUTPUT

```
Technology PHP version 5.5.9 has been detected. Upgrade to the last supported version of PHP: 8.1
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/training_install.php

Identification

OUTPUT

```
Technology PHP version 5.5.9 has been detected. Upgrade to the last supported version of PHP: 8.1
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/training.php

Identification

OUTPUT

```
Technology PHP version 5.5.9 has been detected. Upgrade to the last supported version of PHP: 8.1
```

Apache 2.4.x < 2.4.41 Multiple Vulnerabilities

VULNERABILITY CRITICAL PLUGIN ID 98669

Description

According to its banner, the version of Apache running on the remote host is 2.4.x prior to 2.4.41. It is, therefore, affected by multiple vulnerabilities:

- A cross-site scripting (XSS) vulnerability exists in mod_proxy when proxying is enabled and Proxy Error page is displayed. (CVE-2019-10092)

- An open redirect vulnerability exists in mod_rewrite when using self-referential redirects. (CVE-2019-10098)

- A read-after-free vulnerability exists in mod_http2 during connection shutdown. (CVE-2019-10082)

- A memory corruption vulnerability exists in mod_http2 on early pushes. (CVE-2019-10081)

- A denial of service (DoS) vulnerability exists in mod_http2 by exhausting h2 workers. (CVE-2019-9517)

- A stack buffer overflow and NULL pointer dereference vulnerabilities exist in mod_remoteip when using a specially crafted PROXY header. (CVE-2019-10097)

Note that the scanner has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Apache version 2.4.41 or later.

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.4.41
https://httpd.apache.org/security/vulnerabilities_24.html#2.4.41

Plugin Details

PUBLICATION DATE	2019-08-20T00:00:00+00:00
MODIFICATION DATE	2023-03-14T00:00:00+00:00
FAMILY	Component Vulnerability
SEVERITY	Critical
PLUGIN ID	98669

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	9.1
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H
CVSS BASE SCORE	7.8

CVSS VECTOR	CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:C

Reference Information

CWE	125, 476, 601, 787, 770, 416, 79, 400
WASC	Buffer Overflow, Cross-Site Scripting, Denial of Service, URL Redirector Abuse
OWASP	2021-A3, 2021-A6, 2010-A2, 2021-A1, 2010-A10, 2013-A9, 2017-A7, 2017-A9, 2013-A10, 2013-A3, 2019-API7, 2023-API8
CVE	CVE-2019-10082, CVE-2019-10098, CVE-2019-9517, CVE-2019-10092, CVE-2019-10081, CVE-2019-10097
BID	-

Apache 2.4.x < 2.4.41 Multiple Vulnerabilities Instances (1)

VULNERABILITY CRITICAL PLUGIN ID 98669

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/apps/

Identification

OUTPUT

```
Current Version: 2.4.7
Fixed Version: 2.4.41
Detected technology URL: https://juice-shop-388277804329.us-west1.run.app/apps/
```

Apache 2.4.x < 2.4.26 Multiple Vulnerabilities

VULNERABILITY CRITICAL PLUGIN ID 98911

Description

According to its banner, the version of Apache running on the remote host is 2.4.x prior to 2.4.26. It is, therefore, affected by the following vulnerabilities :

- An authentication bypass vulnerability exists due to third-party modules using the ap_get_basic_auth_pw() function outside of the authentication phase. An unauthenticated, remote attacker can exploit this to bypass authentication requirements. (CVE-2017-3167)

- A NULL pointer dereference flaw exists due to third-party module calls to the mod_ssl ap_hook_process_connection() function during an HTTP request to an HTTPS port. An unauthenticated, remote attacker can exploit this to cause a denial of service condition. (CVE-2017-3169)

- A NULL pointer dereference flaw exists in mod_http2 that is triggered when handling a specially crafted HTTP/2 request. An unauthenticated, remote attacker can exploit this to cause a denial of service condition. Note that this vulnerability does not affect 2.2.x. (CVE-2017-7659)

- An out-of-bounds read error exists in the ap_find_token() function due to improper handling of header sequences. An unauthenticated, remote attacker can exploit this, via a specially crafted header sequence, to cause a denial of service condition. (CVE-2017-7668)

- An out-of-bounds read error exists in mod_mime due to improper handling of Content-Type response headers. An unauthenticated, remote attacker can exploit this, via a specially crafted Content-Type response header, to cause a denial of service condition or the disclosure of sensitive information. (CVE-2017-7679)

Note that the scanner has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Apache version 2.4.26 or later.

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.4.26

https://httpd.apache.org/security/vulnerabilities_24.html#2.4.26

Plugin Details

PUBLICATION DATE	2019-01-09T00:00:00+00:00
MODIFICATION DATE	2023-03-14T00:00:00+00:00
FAMILY	Component Vulnerability
SEVERITY	Critical
PLUGIN ID	98911

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	9.8
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVSS BASE SCORE	7.5
CVSS VECTOR	CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P

Reference Information

CWE	125, 20, 476, 126, 122, 119, 287
WASC	Buffer Overflow, Improper Input Handling, Insufficient Authentication
OWASP	2010-A4, 2021-A3, 2013-A4, 2010-A3, 2021-A7, 2017-A9, 2017-A5, 2013-A2, 2021-A6, 2017-A2, 2013-A9, 2019-API7, 2023-API8
CVE	CVE-2017-7679, CVE-2017-7668, CVE-2017-7659, CVE-2017-3169, CVE-2017-3167
BID	99132, 99135, 99137, 99134, 99170

Apache 2.4.x < 2.4.26 Multiple Vulnerabilities Instances (1)

VULNERABILITY CRITICAL PLUGIN ID 98911

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/apps/

Identification

OUTPUT

```
Current Version: 2.4.7
Fixed Version: 2.4.26
Detected technology URL: https://juice-shop-388277804329.us-west1.run.app/apps/
```

Apache 2.4.x < 2.4.27 Multiple Vulnerabilities

VULNERABILITY CRITICAL PLUGIN ID 98912

Description

According to its banner, the version of Apache running on the remote host is 2.4.x prior to 2.4.27. It is, therefore, affected by the following vulnerabilities :

- A denial of service vulnerability exists in httpd due to a failure to initialize or reset the value placeholder in [Proxy-] Authorization headers of type 'Digest' before or between successive key=value assignments by mod_auth_digest. An unauthenticated, remote attacker can exploit this, by providing an initial key with no '=' assignment, to disclose sensitive information or cause a denial of service condition. (CVE-2017-9788)

- A read-after-free error exists in httpd that is triggered when closing a large number of connections. An unauthenticated, remote attacker can exploit this to have an unspecified impact. (CVE-2017-9789)

Note that the scanner has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Apache version 2.4.27 or later.

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.4.27

https://httpd.apache.org/security/vulnerabilities_24.html#2.4.27

Plugin Details

PUBLICATION DATE	2019-01-09T00:00:00+00:00
MODIFICATION DATE	2023-03-14T00:00:00+00:00
FAMILY	Component Vulnerability
SEVERITY	Critical
PLUGIN ID	98912

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	9.1
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H
CVSS BASE SCORE	6.4
CVSS VECTOR	CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:P

Reference Information

CWE	20, 200, 416, 456

WASC	Improper Input Handling, Information Leakage
OWASP	2010-A4, 2021-A3, 2021-A1, 2013-A5, 2013-A9, 2013-A4, 2017-A9, 2017-A5, 2017-A6, 2021-A6, 2010-A6, 2023-API8, 2019-API7
CVE	CVE-2017-9788, CVE-2017-9789
BID	99569, 99568

Apache 2.4.x < 2.4.27 Multiple Vulnerabilities Instances (1)

VULNERABILITY CRITICAL PLUGIN ID 98912

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/apps/

Identification

OUTPUT

```
Current Version: 2.4.7
Fixed Version: 2.4.27
Detected technology URL: https://juice-shop-388277804329.us-west1.run.app/apps/
```

Apache 2.4.x < 2.4.33 Multiple Vulnerabilities

VULNERABILITY CRITICAL PLUGIN ID 98914

Description

According to its banner, the version of Apache running on the remote host is 2.4.x prior to 2.4.33. It is, therefore, affected by the following vulnerabilities:

- An out-of-bounds write flaw exists within the derive_codepage_from_lang() function of the modules/aaa/mod_authnz_ldap.c script due to improper handling of 'Accept-Language' header values that are less than two-bytes. A remote attacker, with a specially crafted request, could potentially crash the process. (CVE-2017-15710)

- A ACL bypass flaw exists within the ap_rgetline_core() function of the server/protocol.c script due to improper handling of <FilesMatch> expressions. A remote attacker could potentially bypass restrictions an upload a file. (CVE-2017-15715)

- A data tampering flaw exists in the session_fixups() function of the modules/session/mod_session.c script when forwarding mod_session data to CGI applications. A remote attacker, with a specially crafted request, could potentially tamper with the mod_session data of the CGI application. (CVE-2018-1283)

- An out-of-bound read flaw exists when hitting a size limit while handling HTTP headers. A remote attacker, with a specially crafted request, could crash the process. (CVE-2018-1301)

- A use-after-free flaw exists when handling the HTTP/2 stream shutdown. A remote attacker could potentially write to already freed memory and crash the process. (CVE-2018-1302)

- An out-of-bounds read flaw exists in the read_table() function of the modules/cache/mod_cache_socache.c script when handling empty headers. A remote attacker, with a specially crafted request, could potentially crash the process. (CVE-2018-1303)

- A flaw exists within the modules/aaa/mod_auth_digest.c script due to improperly generating nonce when sending HTTP Digest Authentication challenges. A remote attacker could potentially conduct replay attacks against the server. (CVE-2018-1312)

Note that the scanner has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Apache version 2.4.33 or later.

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.4.33
https://httpd.apache.org/security/vulnerabilities_24.html#2.4.33

Plugin Details

PUBLICATION DATE	2019-01-09T00:00:00+00:00
MODIFICATION DATE	2023-03-14T00:00:00+00:00
FAMILY	Component Vulnerability
SEVERITY	Critical

PLUGIN ID	98914

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	9.8
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVSS BASE SCORE	6.8
CVSS VECTOR	CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P

Reference Information

CWE	125, 20, 476, 787, 305, 119, 287
WASC	Buffer Overflow, Improper Input Handling, Insufficient Authentication
OWASP	2010-A4, 2021-A3, 2013-A4, 2010-A3, 2021-A7, 2017-A9, 2017-A5, 2013-A2, 2021-A6, 2017-A2, 2013-A9, 2019-API7, 2023-API8
CVE	CVE-2017-15715, CVE-2018-1303, CVE-2018-1302, CVE-2018-1301, CVE-2018-1312, CVE-2017-15710, CVE-2018-1283
BID	103525, 103515, 103524, 103528, 103520, 103522, 103512

Apache 2.4.x < 2.4.33 Multiple Vulnerabilities Instances (1)

VULNERABILITY CRITICAL PLUGIN ID 98914

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/apps/

Identification

OUTPUT

```
Current Version: 2.4.7
Fixed Version: 2.4.33
Detected technology URL: https://juice-shop-388277804329.us-west1.run.app/apps/
```

Apache 2.4.x < 2.4.48 Multiple Vulnerabilities

VULNERABILITY CRITICAL PLUGIN ID 112806

Description

According to its banner, the version of Apache running on the remote host is 2.4.x prior to 2.4.48. It is, therefore, affected by multiple vulnerabilities:

- Unexpected <Location> section matching with 'MergeSlashes OFF'. (CVE-2021-30641)

- mod_auth_digest: possible stack overflow by one nul byte while validating the Digest nonce. (CVE-2020-35452)

- mod_session: Fix possible crash due to NULL pointer dereference, which could be used to cause a Denial of Service with a malicious backend server and SessionHeader. (CVE-2021-26691)

- mod_session: Fix possible crash due to NULL pointer dereference, which could be used to cause a Denial of Service. (CVE-2021-26690)

- mod_proxy_http: Fix possible crash due to NULL pointer dereference, which could be used to cause a Denial of Service. (CVE-2020-13950)

- Windows: Prevent local users from stopping the httpd process (CVE-2020-13938)

- mod_proxy_wstunnel, mod_proxy_http: Handle Upgradable protocols end-to-end negotiation. (CVE-2019-17567)

- mod_http2: Fix a potential NULL pointer dereference. (CVE-2021-31618)

Note that the scanner has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Apache version 2.4.48 or later.

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.4.48
https://httpd.apache.org/security/vulnerabilities_24.html#2.4.48

Plugin Details

PUBLICATION DATE	2021-06-15T00:00:00+00:00
MODIFICATION DATE	2023-03-14T00:00:00+00:00
FAMILY	Component Vulnerability
SEVERITY	Critical
PLUGIN ID	112806

Risk Information

CVSSV4 BASE SCORE	-

CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	9.8
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVSS BASE SCORE	7.5
CVSS VECTOR	CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P

Reference Information

CWE	120, 20, 862, 476, 444, 787, 122, 119, 287
WASC	Insufficient Authentication, Buffer Overflow, HTTP Request Smuggling, Improper Input Handling, Insufficient Authorization
OWASP	2013-A7, 2010-A4, 2021-A3, 2021-A1, 2021-A4, 2013-A4, 2010-A3, 2021-A7, 2017-A9, 2017-A5, 2013-A2, 2021-A6, 2017-A2, 2013-A9, 2010-A8, 2019-API7, 2023-API8
CVE	CVE-2021-30641, CVE-2021-26690, CVE-2021-31618, CVE-2019-17567, CVE-2021-26691, CVE-2020-35452, CVE-2020-13950, CVE-2020-13938
BID	-

Apache 2.4.x < 2.4.48 Multiple Vulnerabilities Instances (1)

VULNERABILITY CRITICAL PLUGIN ID 112806

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/apps/

Identification

OUTPUT

```
Current Version: 2.4.7
Fixed Version: 2.4.48
Detected technology URL: https://juice-shop-388277804329.us-west1.run.app/apps/
```

Apache 2.4.x < 2.4.49 Multiple Vulnerabilities

VULNERABILITY CRITICAL PLUGIN ID 112981

Description

According to its banner, the version of Apache running on the remote host is 2.4.x prior to 2.4.49. It is, therefore, affected by multiple vulnerabilities:

- A crafted method sent through HTTP/2 will bypass validation and be forwarded by mod_proxy, which can lead to request splitting or cache poisoning. (CVE-2021-33193)

- Malformed requests may cause the server to dereference a NULL pointer. (CVE-2021-34798)

- A carefully crafted request uri-path can cause mod_proxy_uwsgi to read above the allocated memory and crash (DoS). (CVE-2021-36160)

- ap_escape_quotes() may write beyond the end of a buffer when given malicious input. (CVE-2021-39275)

- A crafted request uri-path can cause mod_proxy to forward the request to an origin server choosen by the remote user. (CVE-2021-40438)

Note that the scanner has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Apache version 2.4.49 or later.

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.4.49
https://httpd.apache.org/security/vulnerabilities_24.html#2.4.49

Plugin Details

PUBLICATION DATE	2021-09-17T00:00:00+00:00
MODIFICATION DATE	2023-03-14T00:00:00+00:00
FAMILY	Component Vulnerability
SEVERITY	Critical
PLUGIN ID	112981

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	9.8
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVSS BASE SCORE	7.5
CVSS VECTOR	CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P

Reference Information

CWE	125, 476, 444, 787, 119, 918
WASC	Application Misconfiguration, Buffer Overflow, HTTP Request Smuggling
OWASP	2021-A4, 2021-A10, 2013-A5, 2013-A9, 2017-A9, 2017-A6, 2021-A6, 2010-A6, 2023-API7, 2023-API8, 2019-API7
CVE	CVE-2021-33193, CVE-2021-40438, CVE-2021-39275, CVE-2021-36160, CVE-2021-34798
BID	-

Apache 2.4.x < 2.4.49 Multiple Vulnerabilities Instances (1)

VULNERABILITY CRITICAL PLUGIN ID 112981

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/apps/

Identification

OUTPUT

```
Current Version: 2.4.7
Fixed Version: 2.4.49
Detected technology URL: https://juice-shop-388277804329.us-west1.run.app/apps/
```

Apache 2.4.x < 2.4.52 Multiple Vulnerabilities

VULNERABILITY CRITICAL PLUGIN ID 113079

Description

The version of Apache httpd installed on the remote host is prior to 2.4.52. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.52 advisory.

- A crafted URI sent to httpd configured as a forward proxy (ProxyRequests on) can cause a crash (NULL pointer dereference) or, for configurations mixing forward and reverse proxy declarations, can allow for requests to be directed to a declared Unix Domain Socket endpoint (Server Side Request Forgery). This issue affects Apache HTTP Server 2.4.7 up to 2.4.51 (included). (CVE-2021-44224)

- A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerabilty though it might be possible to craft one. This issue affects Apache HTTP Server 2.4.51 and earlier. (CVE-2021-44790)

Note that the scanner has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Apache version 2.4.52 or later.

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.4.52
https://httpd.apache.org/security/vulnerabilities_24.html#2.4.52

Plugin Details

PUBLICATION DATE	2021-12-21T00:00:00+00:00
MODIFICATION DATE	2023-03-14T00:00:00+00:00
FAMILY	Component Vulnerability
SEVERITY	Critical
PLUGIN ID	113079

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	9.8
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVSS BASE SCORE	7.5
CVSS VECTOR	CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P

Reference Information

CWE	476, 787, 918
WASC	Application Misconfiguration, Buffer Overflow
OWASP	2021-A10, 2013-A5, 2013-A9, 2017-A9, 2017-A6, 2021-A6, 2010-A6, 2023-API7, 2023-API8, 2019-API7
CVE	CVE-2021-44224, CVE-2021-44790
BID	-

Apache 2.4.x < 2.4.52 Multiple Vulnerabilities Instances (1)

VULNERABILITY CRITICAL PLUGIN ID 113079

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/apps/

Identification

OUTPUT

```
Current Version: 2.4.7
Fixed Version: 2.4.52
Detected technology URL: https://juice-shop-388277804329.us-west1.run.app/apps/
```

Apache 2.4.x < 2.4.53 Multiple Vulnerabilities

VULNERABILITY CRITICAL PLUGIN ID 113194

Description

According to its banner, the version of Apache running on the remote host is 2.4.x prior to 2.4.53. It is, therefore, affected by multiple vulnerabilities:

- A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. (CVE-2022-22719)

- A HTTP Request Smuggling vulnerability exists due earlier fails to close inbound connection when errors are encountered discarding the request body. (CVE-2022-22720)

- If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. (CVE-2022-22721)

- An out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. (CVE-2022-23943)

Note that the scanner has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Apache version 2.4.53 or later.

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.4.53

https://httpd.apache.org/security/vulnerabilities_24.html#2.4.53

Plugin Details

PUBLICATION DATE	2022-03-14T00:00:00+00:00
MODIFICATION DATE	2023-03-14T00:00:00+00:00
FAMILY	Component Vulnerability
SEVERITY	Critical
PLUGIN ID	113194

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	9.8
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVSS BASE SCORE	7.5
CVSS VECTOR	CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P

Reference Information

CWE	125, 665, 444, 787, 190, 908
WASC	Buffer Overflow, HTTP Request Smuggling, Integer Overflows
OWASP	2021-A6, 2021-A4, 2013-A9, 2017-A9, 2019-API7, 2023-API8
CVE	CVE-2022-22719, CVE-2022-22720, CVE-2022-22721, CVE-2022-23943
BID	-

Apache 2.4.x < 2.4.53 Multiple Vulnerabilities Instances (1)

VULNERABILITY CRITICAL PLUGIN ID 113194

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/apps/

Identification

OUTPUT

```
Current Version: 2.4.7
Fixed Version: 2.4.53
Detected technology URL: https://juice-shop-388277804329.us-west1.run.app/apps/
```

Apache 2.4.x < 2.4.54 Multiple Vulnerabilities

VULNERABILITY CRITICAL PLUGIN ID 113254

Description

According to its banner, the version of Apache running on the remote host is 2.4.x prior to 2.4.54. It is, therefore, affected by multiple vulnerabilities:

- Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. (CVE-2022-26377)

- Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module. (CVE-2022-28330)

- The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function. (CVE-2022-28614)

- Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected. (CVE-2022-28615)

- In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size. (CVE-2022-29404)

- If Apache HTTP Server 2.4.53 is configured to do transformations with mod_sed in contexts where the input to mod_sed may be very large, mod_sed may make excessively large memory allocations and trigger an abort. (CVE-2022-30522)

- Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer. (CVE-2022-30556)

- Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server /application. (CVE-2022-31813)

Note that the scanner has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Apache version 2.4.54 or later.

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.4.54
https://httpd.apache.org/security/vulnerabilities_24.html#2.4.54

Plugin Details

PUBLICATION DATE	2022-06-13T00:00:00+00:00
MODIFICATION DATE	2023-03-14T00:00:00+00:00
FAMILY	Component Vulnerability

SEVERITY	Critical
PLUGIN ID	113254

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	9.8
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVSS BASE SCORE	7.5
CVSS VECTOR	CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P

Reference Information

CWE	125, 770, 444, 345, 190, 200, 789, 348
WASC	Insufficient Authentication, Integer Overflows, Information Leakage, Denial of Service, HTTP Request Smuggling
OWASP	2010-A3, 2021-A1, 2021-A4, 2017-A9, 2013-A2, 2017-A6, 2021-A6, 2010-A6, 2013-A5, 2021-A8, 2017-A2, 2013-A9, 2023-API8, 2019-API7
CVE	CVE-2022-30522, CVE-2022-28614, CVE-2022-31813, CVE-2022-29404, CVE-2022-26377, CVE-2022-30556, CVE-2022-28330, CVE-2022-28615
BID	-

Apache 2.4.x < 2.4.54 Multiple Vulnerabilities Instances (1)

VULNERABILITY CRITICAL PLUGIN ID 113254

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/apps/

Identification

OUTPUT

```
Current Version: 2.4.7
Fixed Version: 2.4.54
Detected technology URL: https://juice-shop-388277804329.us-west1.run.app/apps/
```

Apache 2.4.x < 2.4.55 Multiple Vulnerabilities

VULNERABILITY CRITICAL PLUGIN ID 113545

Description

According to its banner, the version of Apache running on the remote host is 2.4.x prior to 2.4.55. It is, therefore, affected by multiple vulnerabilities:

- A crafted If: request header can cause a memory read, or write of a single zero byte, in a pool heap memory location beyond the header value sent. This could cause the process to crash. (CVE-2006-20001)

- HTTP Request Smuggling vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. (CVE-2022-36760)

- A malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client. (CVE-2022-26377)

Note that the scanner has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Apache version 2.4.55 or later.

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.4.55
https://httpd.apache.org/security/vulnerabilities_24.html#2.4.55

Plugin Details

PUBLICATION DATE	2023-01-18T00:00:00+00:00
MODIFICATION DATE	2024-01-03T00:00:00+00:00
FAMILY	Component Vulnerability
SEVERITY	Critical
PLUGIN ID	113545

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	9.0
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H
CVSS BASE SCORE	7.8
CVSS VECTOR	CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:C

Reference Information

CWE	444, 787
WASC	Buffer Overflow, HTTP Request Smuggling
OWASP	2021-A6, 2021-A4, 2013-A9, 2017-A9, 2019-API7, 2023-API8
CVE	CVE-2006-20001, CVE-2022-26377, CVE-2022-36760
BID	-

Apache 2.4.x < 2.4.55 Multiple Vulnerabilities Instances (1)

VULNERABILITY CRITICAL PLUGIN ID 113545

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/apps/

Identification

OUTPUT

```
Current Version: 2.4.7
Fixed Version: 2.4.55
Detected technology URL: https://juice-shop-388277804329.us-west1.run.app/apps/
```

Apache 2.4.x < 2.4.56 Multiple Vulnerabilities

VULNERABILITY CRITICAL PLUGIN ID 113673

Description

According to its banner, the version of Apache running on the remote host is 2.4.x prior to 2.4.56. It is, therefore, affected by multiple vulnerabilities:

- Some mod_proxy configurations allow a HTTP Request Smuggling attack. (CVE-2023-25690)

- HTTP Response Smuggling vulnerability via mod_proxy_uwsgi. (CVE-2023-27522)

Note that the scanner has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Apache version 2.4.56 or later.

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.4.56
https://httpd.apache.org/security/vulnerabilities_24.html#2.4.56

Plugin Details

PUBLICATION DATE	2023-03-08T00:00:00+00:00
MODIFICATION DATE	2023-03-16T00:00:00+00:00
FAMILY	Component Vulnerability
SEVERITY	Critical
PLUGIN ID	113673

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	9.8
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVSS BASE SCORE	10.0
CVSS VECTOR	CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Reference Information

CWE	113, 444
WASC	HTTP Request Smuggling, HTTP Response Splitting
OWASP	2013-A1, 2021-A3, 2021-A6, 2021-A4, 2017-A1, 2013-A9, 2017-A9, 2010-A1, 2019-API8, 2023-API8, 2019-API7
CVE	CVE-2023-25690, CVE-2023-27522
BID	-

Apache 2.4.x < 2.4.56 Multiple Vulnerabilities Instances (1)

VULNERABILITY CRITICAL PLUGIN ID 113673

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/apps/

Identification

OUTPUT

```
Current Version: 2.4.7
Fixed Version: 2.4.56
Detected technology URL: https://juice-shop-388277804329.us-west1.run.app/apps/
```

Apache 2.4.x < 2.4.60 Multiple Vulnerabilities

VULNERABILITY CRITICAL PLUGIN ID 114360

Description

According to its banner, the version of Apache running on the remote host is 2.4.x prior to 2.4.60. It is, therefore, affected by multiple vulnerabilities:

- Serving WebSocket protocol upgrades over a HTTP/2 connection could result in a Null Pointer dereference, leading to a crash of the server process, degrading performance. (CVE-2024-36387)

- SSRF in Apache HTTP Server on Windows allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests or content. (CVE-2024-38472)

- Encoding problem in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows request URLs with incorrect encoding to be sent to backend services, potentially bypassing authentication via crafted requests. (CVE-2024-38473)

- Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts in directories permitted by the configuration but not directly reachable by any URL or source disclosure of scripts meant to only to be executed as CGI. (CVE-2024-38474)

- Improper escaping of output in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows an attacker to map URLs to filesystem locations that are permitted to be served by the server but are not intentionally/directly reachable by any URL, resulting in code execution or source code disclosure. (CVE-2024-38475)

- Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution via backend applications whose response headers are malicious or exploitable. (CVE-2024-38476)

- Null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows an attacker to crash the server via a malicious request. (CVE-2024-38477)

- Potential SSRF in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows an attacker to cause unsafe RewriteRules to unexpectedly setup URL's to be handled by mod_proxy. (CVE-2024-39573)

Note that the scanner has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Apache version 2.4.60 or later.

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.4.60
https://httpd.apache.org/security/vulnerabilities_24.html#2.4.60

Plugin Details

PUBLICATION DATE	2024-07-03T00:00:00+00:00
MODIFICATION DATE	2024-07-22T00:00:00+00:00
FAMILY	Component Vulnerability

SEVERITY	Critical
PLUGIN ID	114360

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	9.8
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVSS BASE SCORE	10.0
CVSS VECTOR	CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Reference Information

CWE	829, 20, 116, 476, 918
WASC	Application Misconfiguration, Improper Input Handling, Improper Output Handling
OWASP	2010-A4, 2021-A3, 2013-A9, 2013-A4, 2017-A9, 2017-A5, 2017-A6, 2021-A6, 2010-A6, 2021-A10, 2013-A5, 2021-A8, 2023-API7, 2023-API8, 2019-API7, 2019-API8
CVE	CVE-2024-38473, CVE-2024-38476, CVE-2024-38475, CVE-2024-39573, CVE-2024-36387, CVE-2024-38474, CVE-2024-38472, CVE-2024-38477
BID	-

Apache 2.4.x < 2.4.60 Multiple Vulnerabilities Instances (1)

VULNERABILITY CRITICAL PLUGIN ID 114360

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/apps/

Identification

OUTPUT

```
Current Version: 2.4.7
Fixed Version: 2.4.60
Detected technology URL: https://juice-shop-388277804329.us-west1.run.app/apps/
```

Apache 2.4.x < 2.4.39 Multiple Vulnerabilities

VULNERABILITY HIGH PLUGIN ID 98530

Description

According to its banner, the version of Apache running on the remote host is 2.4.x prior to 2.4.39. It is, therefore, affected by multiple vulnerabilities:

- A privilege escalation vulnerability exists in module scripts due to an ability to execute arbitrary code as the parent process by manipulating the scoreboard. (CVE-2019-0211)

- An access control bypass vulnerability exists in mod_auth_digest due to a race condition when running in a threaded server. An attacker with valid credentials could authenticate using another username. (CVE-2019-0217)

- An access control bypass vulnerability exists in mod_ssl when using per-location client certificate verification with TLSv1.3. (CVE-2019-0215)

In addition, Apache httpd is also affected by several additional vulnerabilities including a denial of service, read-after-free and URL path normalization inconsistencies.

Note that the scanner has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Apache version 2.4.39 or later.

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.4.39
https://httpd.apache.org/security/vulnerabilities_24.html#2.4.39

Plugin Details

PUBLICATION DATE	2019-04-08T00:00:00+00:00
MODIFICATION DATE	2023-03-14T00:00:00+00:00
FAMILY	Component Vulnerability
SEVERITY	High
PLUGIN ID	98530

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	7.8
CVSSV3 VECTOR	CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS BASE SCORE	7.2
CVSS VECTOR	CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C

Reference Information

CWE	706, 41, 362, 250, 400, 284, 416, 264, 444
WASC	Application Misconfiguration, Denial of Service, HTTP Request Smuggling, Improper Input Handling, Insufficient Authorization
OWASP	2010-A8, 2013-A7, 2021-A1, 2021-A4, 2013-A5, 2013-A9, 2013-A4, 2010-A4, 2021-A5, 2017-A9, 2017-A5, 2017-A6, 2021-A6, 2010-A6, 2023-API8, 2019-API7
CVE	CVE-2019-0215, CVE-2019-0220, CVE-2019-0197, CVE-2019-0217, CVE-2019-0196, CVE-2019-0211
BID	107666, 107669, 107667, 107670, 107668, 107665

Apache 2.4.x < 2.4.39 Multiple Vulnerabilities Instances (1)

VULNERABILITY HIGH PLUGIN ID 98530

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/apps/

Identification

OUTPUT

```
Current Version: 2.4.7
Fixed Version: 2.4.39
Detected technology URL: https://juice-shop-388277804329.us-west1.run.app/apps/
```

Apache 2.4.x < 2.4.38 Multiple Vulnerabilities

VULNERABILITY HIGH PLUGIN ID 98537

Description

According to its banner, the version of Apache running on the remote host is 2.4.x prior to 2.4.38. It is, therefore, affected by multiple vulnerabilities:

- A denial of service (DoS) vulnerability exists in HTTP/2 steam handling. An unauthenticated, remote attacker can exploit this issue, via sending request bodies in a slow loris way to plain resources, to occupy a server thread. (CVE-2018-17189)

- A vulnerability exists in mod_sesion_cookie, as it does not properly check the expiry time of cookies. (CVE-2018-17199)

- A denial of service (DoS) vulnerability exists in mod_ssl when used with OpenSSL 1.1.1 due to an interaction in changes to handling of renegotiation attempts. An unauthenticated, remote attacker can exploit this issue to cause mod_ssl to stop responding. (CVE-2019-0190)

Note that the scanner has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Apache version 2.4.38 or later.

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.4.38

https://httpd.apache.org/security/vulnerabilities_24.html#2.4.38

Plugin Details

PUBLICATION DATE	2019-04-12T00:00:00+00:00
MODIFICATION DATE	2023-03-14T00:00:00+00:00
FAMILY	Component Vulnerability
SEVERITY	High
PLUGIN ID	98537

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	7.5
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N
CVSS BASE SCORE	5.0
CVSS VECTOR	CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P

Reference Information

CWE	384, 400, 613
WASC	Denial of Service, Insufficient Session Expiration, Session Fixation
OWASP	2010-A3, 2021-A7, 2017-A9, 2013-A2, 2021-A6, 2017-A2, 2013-A9, 2023-API2, 2019-API2, 2019-API7, 2023-API8
CVE	CVE-2018-17189, CVE-2018-17199, CVE-2019-0190
BID	106685, 106742, 106743

Apache 2.4.x < 2.4.38 Multiple Vulnerabilities Instances (1)

VULNERABILITY HIGH PLUGIN ID 98537

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/apps/

Identification

OUTPUT

```
Current Version: 2.4.7
Fixed Version: 2.4.38
Detected technology URL: https://juice-shop-388277804329.us-west1.run.app/apps/
```

Apache 2.4.x < 2.4.9 Multiple Vulnerabilities

VULNERABILITY HIGH PLUGIN ID 98905

Description

According to its banner, the version of Apache 2.4.x running on the remote host is a version prior to 2.4.9. It is, therefore, affected by the following vulnerabilities :

- A flaw exists with the 'mod_dav' module that is caused when tracking the length of CDATA that has leading white space. A remote attacker with a specially crafted DAV WRITE request can cause the service to stop responding. (CVE-2013-6438)

- A flaw exists in 'mod_log_config' module that is caused when logging a cookie that has an unassigned value. A remote attacker with a specially crafted request can cause the service to crash. (CVE-2014-0098)

Note that the scanner did not actually test for these issues, but instead has relied on the version in the server's banner.

Solution

Upgrade to Apache version 2.4.9 or later. Alternatively, ensure that the affected modules are not in use.

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.4.9
https://httpd.apache.org/security/vulnerabilities_24.html#2.4.9

Plugin Details

PUBLICATION DATE	2019-01-09T00:00:00+00:00
MODIFICATION DATE	2023-03-14T00:00:00+00:00
FAMILY	Component Vulnerability
SEVERITY	High
PLUGIN ID	98905

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	7.5
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CVSS BASE SCORE	5.0
CVSS VECTOR	CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P

Reference Information

CWE	119, 125, 20
WASC	Buffer Overflow, Improper Input Handling
OWASP	2010-A4, 2021-A3, 2021-A6, 2013-A9, 2013-A4, 2017-A9, 2017-A5, 2019-API7, 2023-API8
CVE	CVE-2013-6438, CVE-2014-0098

BID	66303

Apache 2.4.x < 2.4.9 Multiple Vulnerabilities Instances (1)

VULNERABILITY HIGH PLUGIN ID 98905

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/apps/

Identification

OUTPUT

```
Current Version: 2.4.7
Fixed Version: 2.4.9
Detected technology URL: https://juice-shop-388277804329.us-west1.run.app/apps/
```

Apache 2.4.x < 2.4.10 Multiple Vulnerabilities

VULNERABILITY HIGH PLUGIN ID 98906

Description

According to its banner, the version of Apache 2.4.x running on the remote host is prior to 2.4.10. It is, therefore, affected by the following vulnerabilities :

- A flaw exists in the 'mod_proxy' module that may allow an attacker to send a specially crafted request to a server configured as a reverse proxy that may cause the child process to crash. This could potentially lead to a denial of service attack. (CVE-2014-0117)

- A flaw exists in the 'mod_deflate' module when request body decompression is configured. This could allow a remote attacker to cause the server to consume significant resources. (CVE-2014-0118)

- A flaw exists in the 'mod_status' module when a publicly accessible server status page is in place. This could allow an attacker to send a specially crafted request designed to cause a heap buffer overflow. (CVE-2014-0226)

- A flaw exists in the 'mod_cgid' module in which CGI scripts that did not consume standard input may be manipulated in order to cause child processes to hang. A remote attacker may be able to abuse this in order to cause a denial of service. (CVE-2014-0231)

- A flaw exists in WinNT MPM versions 2.4.1 to 2.4.9 when using the default AcceptFilter. An attacker may be able to specially craft requests that create a memory leak in the application and may eventually lead to a denial of service attack. (CVE-2014-3523)

Note that the scanner has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Apache version 2.4.10 or later. Alternatively, ensure that the affected modules are not in use.

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.4.10

https://httpd.apache.org/security/vulnerabilities_24.html#2.4.10

Plugin Details

PUBLICATION DATE	2019-01-09T00:00:00+00:00
MODIFICATION DATE	2023-03-14T00:00:00+00:00
FAMILY	Component Vulnerability
SEVERITY	High
PLUGIN ID	98906

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-

CVSSV3 BASE SCORE	7.5
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CVSS BASE SCORE	6.8
CVSS VECTOR	CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P

Reference Information

CWE	20, 362, 399, 400, 122
WASC	Buffer Overflow, Denial of Service, Improper Input Handling
OWASP	2010-A4, 2021-A3, 2021-A6, 2013-A9, 2013-A4, 2017-A9, 2017-A5, 2019-API7, 2023-API8
CVE	CVE-2014-0226, CVE-2014-3523, CVE-2014-0118, CVE-2014-0117, CVE-2014-0231
BID	68747, 68678, 68742, 68745, 68740

Apache 2.4.x < 2.4.10 Multiple Vulnerabilities Instances (1)

VULNERABILITY HIGH PLUGIN ID 98906

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/apps/

Identification

OUTPUT

```
Current Version: 2.4.7
Fixed Version: 2.4.10
Detected technology URL: https://juice-shop-388277804329.us-west1.run.app/apps/
```

Apache 2.4.x < 2.4.12 Multiple Vulnerabilities

VULNERABILITY HIGH PLUGIN ID 98907

Description

According to its banner, the version of Apache 2.4.x running on the remote host is prior to 2.4.12. It is, therefore, affected by the following vulnerabilities :

- A flaw exists in module mod_headers that can allow HTTP trailers to replace HTTP headers late during request processing, which a remote attacker can exploit to inject arbitrary headers. This can also cause some modules to function incorrectly or appear to function incorrectly. (CVE-2013-5704)

- A NULL pointer dereference flaw exists in module mod_cache. A remote attacker, using an empty HTTP Content-Type header, can exploit this vulnerability to crash a caching forward proxy configuration, resulting in a denial of service if using a threaded MPM. (CVE-2014-3581)

- A out-of-bounds memory read flaw exists in module mod_proxy_fcgi. An attacker, using a remote FastCGI server to send long response headers, can exploit this vulnerability to cause a denial of service by causing a buffer over-read. (CVE-2014-3583)

- A flaw exists in module mod_lua when handling a LuaAuthzProvider used in multiple Require directives with different arguments. An attacker can exploit this vulnerability to bypass intended access restrictions. (CVE-2014-8109)

Note that the scanner has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Apache version 2.4.12 or later. Alternatively, ensure that the affected modules are not in use.

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.4.12

https://httpd.apache.org/security/vulnerabilities_24.html#2.4.12

Plugin Details

PUBLICATION DATE	2019-01-09T00:00:00+00:00
MODIFICATION DATE	2023-03-14T00:00:00+00:00
FAMILY	Component Vulnerability
SEVERITY	High
PLUGIN ID	98907

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	7.5
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CVSS BASE SCORE	5.0

CVSS VECTOR	CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N

Reference Information

CWE	125, 476, 264, 863, 399, 119, 287
WASC	Buffer Overflow, Insufficient Authentication, Insufficient Authorization
OWASP	2010-A8, 2013-A7, 2021-A1, 2010-A3, 2021-A7, 2017-A9, 2017-A5, 2013-A2, 2021-A6, 2017-A2, 2013-A9, 2019-API7, 2023-API8
CVE	CVE-2013-5704, CVE-2014-3581, CVE-2014-3583, CVE-2014-8109
BID	66550, 71656, 71657, 73040

Apache 2.4.x < 2.4.12 Multiple Vulnerabilities Instances (1)

VULNERABILITY HIGH PLUGIN ID 98907

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/apps/

Identification

OUTPUT

```
Current Version: 2.4.7
Fixed Version: 2.4.12
Detected technology URL: https://juice-shop-388277804329.us-west1.run.app/apps/
```

Apache 2.4.x < 2.4.16 Multiple Vulnerabilities

VULNERABILITY HIGH PLUGIN ID 98908

Description

According to its banner, the version of Apache 2.4.x installed on the remote host is prior to 2.4.16. It is, therefore, affected by the following vulnerabilities :

- A flaw exists in the lua_websocket_read() function in the 'mod_lua' module due to incorrect handling of WebSocket PING frames. A remote attacker can exploit this, by sending a crafted WebSocket PING frame after a Lua script has called the wsupgrade() function, to crash a child process, resulting in a denial of service condition. (CVE-2015-0228)

- A NULL pointer dereference flaw exists in the read_request_line() function due to a failure to initialize the protocol structure member. A remote attacker can exploit this flaw, on installations that enable the INCLUDES filter and has an ErrorDocument 400 directive specifying a local URI, by sending a request that lacks a method, to cause a denial of service condition. (CVE-2015-0253)

- A flaw exists in the chunked transfer coding implementation due to a failure to properly parse chunk headers. A remote attacker can exploit this to conduct HTTP request smuggling attacks. (CVE-2015-3183)

- A flaw exists in the ap_some_auth_required() function due to a failure to consider that a Require directive may be associated with an authorization setting rather than an authentication setting. A remote attacker can exploit this, if a module that relies on the 2.2 API behavior exists, to bypass intended access restrictions. (CVE-2015-3185)

- A flaw exists in the RC4 algorithm due to an initial double-byte bias in the keystream generation. An attacker can exploit this, via Bayesian analysis that combines an a priori plaintext distribution with keystream distribution statistics, to conduct a plaintext recovery of the ciphertext. Note that RC4 cipher suites are prohibited per RFC 7465. This issue was fixed in Apache version 2.4.13; however, 2.4.13, 2.4.14, and 2.4.15 were never publicly released.

Note that the scanner has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Apache version 2.4.16 or later. Alternatively, ensure that the affected modules are not in use.

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.4.16

https://httpd.apache.org/security/vulnerabilities_24.html#2.4.16

Plugin Details

PUBLICATION DATE	2019-01-09T00:00:00+00:00
MODIFICATION DATE	2023-03-14T00:00:00+00:00
FAMILY	Component Vulnerability
SEVERITY	High
PLUGIN ID	98908

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	7.5
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CVSS BASE SCORE	5.0
CVSS VECTOR	CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P

Reference Information

CWE	20, 476, 264, 172, 287
WASC	Improper Input Handling, Improper Output Handling, Insufficient Authentication, Insufficient Authorization
OWASP	2010-A8, 2013-A7, 2010-A4, 2021-A3, 2021-A1, 2013-A4, 2010-A3, 2021-A7, 2017-A9, 2017-A5, 2013-A2, 2021-A6, 2017-A2, 2013-A9, 2019-API7, 2019-API8, 2023-API8
CVE	CVE-2015-0228, CVE-2015-0253, CVE-2015-3183, CVE-2015-3185
BID	73041, 75963, 75964, 75965

Apache 2.4.x < 2.4.16 Multiple Vulnerabilities Instances (1)

VULNERABILITY HIGH PLUGIN ID 98908

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/apps/

Identification

OUTPUT

```
Current Version: 2.4.7
Fixed Version: 2.4.16
Detected technology URL: https://juice-shop-388277804329.us-west1.run.app/apps/
```

Apache 2.4.x < 2.4.25 Multiple Vulnerabilities (httpoxy)

VULNERABILITY HIGH PLUGIN ID 98910

Description

According to its banner, the version of Apache running on the remote host is 2.4.x prior to 2.4.25. It is, therefore, affected by the following vulnerabilities :

- A flaw exists in the mod_session_crypto module due to encryption for data and cookies using the configured ciphers with possibly either CBC or ECB modes of operation (AES256-CBC by default). An unauthenticated, remote attacker can exploit this, via a padding oracle attack, to decrypt information without knowledge of the encryption key, resulting in the disclosure of potentially sensitive information. (CVE-2016-0736)

- A denial of service vulnerability exists in the mod_auth_digest module during client entry allocation. An unauthenticated, remote attacker can exploit this, via specially crafted input, to exhaust shared memory resources, resulting in a server crash. (CVE-2016-2161)

- The Apache HTTP Server is affected by a man-in-the-middle vulnerability known as 'httpoxy' due to a failure to properly resolve namespace conflicts in accordance with RFC 3875 section 4.1.18. The HTTP_PROXY environment variable is set based on untrusted user data in the 'Proxy' header of HTTP requests. The HTTP_PROXY environment variable is used by some web client libraries to specify a remote proxy server. An unauthenticated, remote attacker can exploit this, via a crafted 'Proxy' header in an HTTP request, to redirect an application's internal HTTP traffic to an arbitrary proxy server where it may be observed or manipulated. (CVE-2016-5387)

- A denial of service vulnerability exists in the mod_http2 module due to improper handling of the LimitRequestFields directive. An unauthenticated, remote attacker can exploit this, via specially crafted CONTINUATION frames in an HTTP/2 request, to inject unlimited request headers into the server, resulting in the exhaustion of memory resources. (CVE-2016-8740)

- A flaw exists due to improper handling of whitespace patterns in user-agent headers. An unauthenticated, remote attacker can exploit this, via a specially crafted user-agent header, to cause the program to incorrectly process sequences of requests, resulting in interpreting responses incorrectly, polluting the cache, or disclosing the content from one request to a second downstream user-agent. (CVE-2016-8743)

- A CRLF vulnerability exists in the mod_userdir module. An unauthenticated, remote attacker can exploit this, allowing HTTP response splitting attacks. (CVE-2016-4975)

Note that the scanner has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Apache version 2.4.25 or later. Note that the 'httpoxy' vulnerability can be mitigated by applying the workarounds or patches as referenced in the vendor advisory asf-httpoxy-response.txt. Furthermore, to mitigate the other vulnerabilities, ensure that the affected modules (mod_session_crypto, mod_auth_digest, and mod_http2) are not in use.

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.4.25

https://httpd.apache.org/security/vulnerabilities_24.html#2.4.25

https://httpoxy.org

https://www.apache.org/security/asf-httpoxy-response.txt

Plugin Details

PUBLICATION DATE	2019-01-09T00:00:00+00:00
MODIFICATION DATE	2023-03-14T00:00:00+00:00
FAMILY	Component Vulnerability
SEVERITY	High
PLUGIN ID	98910

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	8.1
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
CVSS BASE SCORE	6.8
CVSS VECTOR	CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P

Reference Information

CWE	113, 399, 823, 310, 287, 19, 20, 93, 284, 770
WASC	Insufficient Authentication, Denial of Service, HTTP Response Splitting, Improper Input Handling, Insufficient Authorization
OWASP	2013-A7, 2010-A4, 2021-A3, 2021-A1, 2017-A1, 2021-A2, 2013-A4, 2010-A8, 2013-A1, 2010-A3, 2021-A7, 2017-A9, 2017-A5, 2013-A2, 2021-A6, 2010-A1, 2017-A2, 2013-A9, 2019-API8, 2023-API8, 2019-API7
CVE	CVE-2016-5387, CVE-2016-2161, CVE-2016-0736, CVE-2016-8740, CVE-2016-4975, CVE-2016-8743
BID	94650, 95076, 105093, 95078, 91816, 95077

Apache 2.4.x < 2.4.25 Multiple Vulnerabilities (httpoxy) Instances (1)

VULNERABILITY HIGH PLUGIN ID 98910

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/apps/

Identification

OUTPUT

```
Current Version: 2.4.7
Fixed Version: 2.4.25
Detected technology URL: https://juice-shop-388277804329.us-west1.run.app/apps/
```

Apache 2.4.x < 2.4.28 HTTP Vulnerability (OptionsBleed)

VULNERABILITY HIGH PLUGIN ID 98913

Description

According to its banner, the version of Apache running on the remote host is 2.4.x prior to 2.4.28. It is, therefore, affected by an HTTP vulnerability related to the <Limit {method}> directive in an .htaccess file.

Note that the scanner has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Apache version 2.4.28 or later.

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.4.28
https://httpd.apache.org/security/vulnerabilities_24.html#2.4.28

Plugin Details

PUBLICATION DATE	2019-01-09T00:00:00+00:00
MODIFICATION DATE	2023-03-14T00:00:00+00:00
FAMILY	Component Vulnerability
SEVERITY	High
PLUGIN ID	98913

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	7.5
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
CVSS BASE SCORE	5.0
CVSS VECTOR	CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N

Reference Information

CWE	416
WASC	-
OWASP	2021-A6, 2013-A9, 2017-A9, 2019-API7, 2023-API8
CVE	CVE-2017-9798
BID	100872, 105598

Apache 2.4.x < 2.4.28 HTTP Vulnerability (OptionsBleed) Instances (1)

VULNERABILITY HIGH PLUGIN ID 98913

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/apps/

Identification

OUTPUT

```
Current Version: 2.4.7
Fixed Version: 2.4.28
Detected technology URL: https://juice-shop-388277804329.us-west1.run.app/apps/
```

Apache 2.4.x < 2.4.34 Multiple Vulnerabilities

VULNERABILITY HIGH PLUGIN ID 98915

Description

According to its banner, the version of Apache running on the remote host is 2.4.x prior to 2.4.34. It is, therefore, affected by the following vulnerabilities:

- By specially crafting HTTP/2 requests, workers would be allocated 60 seconds longer than necessary, leading to worker exhaustion and a denial of service. (CVE-2018-1333)

- By specially crafting HTTP requests, the mod_md challenge handler would dereference a NULL pointer and cause the child process to segfault. This could be used to DoS the server. (CVE-2018-8011)

Note that the scanner has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Apache version 2.4.34 or later.

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.4.34
https://httpd.apache.org/security/vulnerabilities_24.html#2.4.34

Plugin Details

PUBLICATION DATE	2019-01-31T00:00:00+00:00
MODIFICATION DATE	2023-03-14T00:00:00+00:00
FAMILY	Component Vulnerability
SEVERITY	High
PLUGIN ID	98915

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	7.5
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CVSS BASE SCORE	5.0
CVSS VECTOR	CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P

Reference Information

CWE	400, 476
WASC	Denial of Service
OWASP	2021-A6, 2013-A9, 2017-A9, 2019-API7, 2023-API8

CVE	CVE-2018-1333, CVE-2018-8011
BID	-

Apache 2.4.x < 2.4.34 Multiple Vulnerabilities Instances (1)

VULNERABILITY HIGH PLUGIN ID 98915

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/apps/

Identification

OUTPUT

```
Current Version: 2.4.7
Fixed Version: 2.4.34
Detected technology URL: https://juice-shop-388277804329.us-west1.run.app/apps/
```

Apache 2.4.x < 2.4.58 Multiple Vulnerabilities

VULNERABILITY HIGH PLUGIN ID 114090

Description

According to its banner, the version of Apache running on the remote host is 2.4.x prior to 2.4.58. It is, therefore, affected by multiple vulnerabilities:

- Out-of-bounds read vulnerability in mod_macro of Apache HTTP Server. (CVE-2023-31122)

- An attacker, opening a HTTP/2 connection with an initial window size of 0, was able to block handling of that connection indefinitely in Apache HTTP Server. This could be used to exhaust worker resources in the server, similar to the well known slow loris attack pattern. (CVE-2023-43622)

- A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that. (CVE-2023-45802) Note that the scanner has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Apache version 2.4.58 or later.

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.4.58
https://httpd.apache.org/security/vulnerabilities_24.html#2.4.58

Plugin Details

PUBLICATION DATE	2023-10-20T00:00:00+00:00
MODIFICATION DATE	2023-11-15T00:00:00+00:00
FAMILY	Component Vulnerability
SEVERITY	High
PLUGIN ID	114090

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	7.5
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CVSS BASE SCORE	7.8
CVSS VECTOR	CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:C

Reference Information

CWE	125, 400

WASC	Denial of Service
OWASP	2021-A6, 2013-A9, 2017-A9, 2019-API7, 2023-API8
CVE	CVE-2023-31122, CVE-2023-43622, CVE-2023-45802
BID	-

Apache 2.4.x < 2.4.58 Multiple Vulnerabilities Instances (1)

VULNERABILITY HIGH PLUGIN ID 114090

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/apps/

Identification

OUTPUT

```
Current Version: 2.4.7
Fixed Version: 2.4.58
Detected technology URL: https://juice-shop-388277804329.us-west1.run.app/apps/
```

Apache 2.4.x < 2.4.59 Multiple Vulnerabilities

VULNERABILITY HIGH PLUGIN ID 114249

Description

According to its banner, the version of Apache running on the remote host is 2.4.x prior to 2.4.59. It is, therefore, affected by multiple vulnerabilities:

- Faulty input validation in the core of Apache allows malicious or exploitable backend/content generators to split HTTP responses. (CVE-2023-38709)

- HTTP Response splitting in multiple modules in Apache HTTP Server allows an attacker that can inject malicious response headers into backend applications to cause an HTTP desynchronization attack. (CVE-2024-24795)

- HTTP/2 incoming headers exceeding the limit are temporarily buffered in nghttp2 in order to generate an informative HTTP 413 response. If a client does not stop sending headers, this leads to memory exhaustion. (CVE-2024-27316)

Note that the scanner has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Apache version 2.4.59 or later.

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.4.59

https://httpd.apache.org/security/vulnerabilities_24.html#2.4.59

Plugin Details

PUBLICATION DATE	2024-04-09T00:00:00+00:00
MODIFICATION DATE	2024-04-09T00:00:00+00:00
FAMILY	Component Vulnerability
SEVERITY	High
PLUGIN ID	114249

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	7.5
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CVSS BASE SCORE	7.8
CVSS VECTOR	CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:C

Reference Information

CWE	113, 400, 770
WASC	Denial of Service, HTTP Response Splitting
OWASP	2013-A1, 2021-A3, 2021-A6, 2017-A1, 2013-A9, 2017-A9, 2010-A1, 2019-API8, 2023-API8, 2019-API7
CVE	CVE-2023-38709, CVE-2024-24795, CVE-2024-27316
BID	-

Apache 2.4.x < 2.4.59 Multiple Vulnerabilities Instances (1)

VULNERABILITY HIGH PLUGIN ID 114249

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/apps/

Identification

OUTPUT

```
Current Version: 2.4.7
Fixed Version: 2.4.59
Detected technology URL: https://juice-shop-388277804329.us-west1.run.app/apps/
```

Apache 2.4.x < 2.4.62 Multiple Vulnerabilities

VULNERABILITY HIGH PLUGIN ID 114385

Description

According to its banner, the version of Apache running on the remote host is 2.4.x prior to 2.4.62. It is, therefore, affected by multiple vulnerabilities:

- A partial fix for CVE-2024-39884 in the core of Apache HTTP Server 2.4.61 ignores some use of the legacy content-type based configuration of handlers. "AddType" and similar configuration, under some circumstances where files are requested indirectly, result in source code disclosure of local content. For example, PHP scripts may be served instead of interpreted. (CVE-2024-40725)

- SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTLM hashes to a malicious server via SSRF and malicious requests. (CVE-2024-40898) Note that the scanner has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Apache version 2.4.62 or later.

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.4.62
https://httpd.apache.org/security/vulnerabilities_24.html#2.4.62

Plugin Details

PUBLICATION DATE	2024-07-22T00:00:00+00:00
MODIFICATION DATE	2024-07-22T00:00:00+00:00
FAMILY	Component Vulnerability
SEVERITY	High
PLUGIN ID	114385

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	7.5
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
CVSS BASE SCORE	7.8
CVSS VECTOR	CVSS2#AV:N/AC:L/Au:N/C:C/I:N/A:N

Reference Information

CWE	668, 918
WASC	Application Misconfiguration, Insufficient Authorization
OWASP	2010-A8, 2013-A7, 2021-A1, 2021-A10, 2013-A5, 2013-A9, 2017-A9, 2017-A5, 2017-A6, 2021-A6, 2010-A6, 2023-API7,

	2023-API8, 2019-API7
CVE	CVE-2024-40725, CVE-2024-40898
BID	-

Apache 2.4.x < 2.4.62 Multiple Vulnerabilities Instances (1)

VULNERABILITY HIGH PLUGIN ID 114385

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/apps/

Identification

OUTPUT

```
Current Version: 2.4.7
Fixed Version: 2.4.62
Detected technology URL: https://juice-shop-388277804329.us-west1.run.app/apps/
```

Missing HTTP Strict Transport Security Policy

VULNERABILITY MEDIUM PLUGIN ID 98056

Description

The HTTP protocol by itself is clear text, meaning that any data that is transmitted via HTTP can be captured and the contents viewed. To keep data private and prevent it from being intercepted, HTTP is often tunnelled through either Secure Sockets Layer (SSL) or Transport Layer Security (TLS). When either of these encryption standards are used, it is referred to as HTTPS.

HTTP Strict Transport Security (HSTS) is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. This will be enforced by the browser even if the user requests a HTTP resource on the same server.

Cyber-criminals will often attempt to compromise sensitive information passed from the client to the server using HTTP. This can be conducted via various Man-in-The-Middle (MiTM) attacks or through network packet captures.

Scanner discovered that the affected application is using HTTPS however does not use the HSTS header.

Solution

Depending on the framework being used the implementation methods will vary, however it is advised that the `Strict-Transport-Security` header be configured on the server.
One of the options for this header is `max-age`, which is a representation (in milliseconds) determining the time in which the client's browser will adhere to the header policy.
Depending on the environment and the application this time period could be from as low as minutes to as long as days.

See Also
https://hstspreload.org/
https://tools.ietf.org/html/rfc6797
https://www.chromium.org/hsts
https://www.owasp.org/index.php/HTTP_Strict_Transport_Security_Cheat_Sheet

Plugin Details

PUBLICATION DATE	2017-03-31T00:00:00+00:00
MODIFICATION DATE	2024-03-18T00:00:00+00:00
FAMILY	HTTP Security Header
SEVERITY	Medium
PLUGIN ID	98056

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	6.5
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N
CVSS BASE SCORE	5.8
CVSS VECTOR	CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N

Reference Information

CWE	319, 523
WASC	Insufficient Transport Layer Protection
OWASP	2010-A9, 2013-A6, 2017-A3, 2021-A2, 2023-API8, 2019-API7
CVE	-
BID	-

Missing HTTP Strict Transport Security Policy Instances (25)

VULNERABILITY MEDIUM PLUGIN ID 98056

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/apps/

Identification

OUTPUT

```
The scanner did not find any Strict-Transport-Security header in the response returned by the target when querying URL
https://juice-shop-388277804329.us-west1.run.app/apps/.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/apps/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 00:30:17 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=b57b66949c25563ad77a69e4a354af47
Content-Length=1782
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/stylesheets/

Identification

OUTPUT

```
The scanner did not find any Strict-Transport-Security header in the response returned by the target when querying URL
https://juice-shop-388277804329.us-west1.run.app/stylesheets/.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/stylesheets/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 01:34:22 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=91660b485a30bbed64793dbe904193d3
Content-Length=2275
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/documents/

Identification

OUTPUT

```
The scanner did not find any Strict-Transport-Security header in the response returned by the target when querying URL
https://juice-shop-388277804329.us-west1.run.app/documents/.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/documents/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 00:48:33 GMT
Server=Google Frontend
```

```
Vary=Accept-Encoding
X-Cloud-Trace-Context=8659790f61386a0d355111f26ee2a386
Content-Length=3149
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/passwords/web.config.bak

Identification

OUTPUT

```
The scanner did not find any Strict-Transport-Security header in the response returned by the target when querying URL
https://juice-shop-388277804329.us-west1.run.app/passwords/web.config.bak.
```

HTTP Info

REQUEST MADE

```
GET /passwords/web.config.bak HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 200
last-modified: Wed, 13 Nov 2024 02:15:28 GMT
etag: "1d84-626c1e84a7000"
accept-ranges: bytes
content-type: application/x-trash
x-cloud-trace-context: dd8a0753fe21b8d0d381c2313f0202d5
date: Tue, 19 Nov 2024 06:08:24 GMT
server: Google Frontend
content-length: 7556
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/soap/nusoap.php

Identification

OUTPUT

```
The scanner did not find any Strict-Transport-Security header in the response returned by the target when querying URL
https://juice-shop-388277804329.us-west1.run.app/soap/nusoap.php.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/soap/nusoap.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
```

```
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type=text/html
Date=Tue, 19 Nov 2024 07:07:36 GMT
Server=Google Frontend
X-Cloud-Trace-Context=9b95efa061e2e33130bff09373a821c4
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=811
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/images/

Identification

OUTPUT

```
The scanner did not find any Strict-Transport-Security header in the response returned by the target when querying URL
https://juice-shop-388277804329.us-west1.run.app/images/.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/images/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 00:57:42 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=fc3fee9e75c9304bb77fd657cb75393d
Content-Length=5991
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/phpinfo.php

Identification

OUTPUT

```
The scanner did not find any Strict-Transport-Security header in the response returned by the target when querying URL
https://juice-shop-388277804329.us-west1.run.app/phpinfo.php.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/phpinfo.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 01:43:29 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=036c4d5909306dec6b8d0193b59d617a
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=85702
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/db/bwapp.sqlite

Identification

OUTPUT

```
The scanner did not find any Strict-Transport-Security header in the response returned by the target when querying URL
https://juice-shop-388277804329.us-west1.run.app/db/bwapp.sqlite.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/db/bwapp.sqlite
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
```

```
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Accept-Ranges=bytes
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type=text/html
Date=Tue, 19 Nov 2024 03:57:01 GMT
Etag="3000-626c1e84a7000"
Last-Modified=Wed, 13 Nov 2024 02:15:28 GMT
Server=Google Frontend
X-Cloud-Trace-Context=2a74d2d814c14512fd8fac93e4bfc679
Content-Length=12288
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/js/

Identification

OUTPUT

```
The scanner did not find any Strict-Transport-Security header in the response returned by the target when querying URL
https://juice-shop-388277804329.us-west1.run.app/js/.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/js/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 01:06:45 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=92dbc4630193c57aa70de731a23c4521
Content-Length=2393
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/soap/class.soap_fault.php

Identification

OUTPUT

```
The scanner did not find any Strict-Transport-Security header in the response returned by the target when querying URL
https://juice-shop-388277804329.us-west1.run.app/soap/class.soap_fault.php.
```

HTTP Info

REQUEST MADE

```
GET /soap/class.soap_fault.php HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 500
x-powered-by: PHP/5.5.9-1ubuntu4.14
content-type: text/html
x-cloud-trace-context: 85c8d444051c598a5636d47e2436b1d1
date: Tue, 19 Nov 2024 06:54:58 GMT
server: Google Frontend
content-length: 0
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/

Identification

OUTPUT

```
The scanner did not find any Strict-Transport-Security header in the response returned by the target when querying URL
https://juice-shop-388277804329.us-west1.run.app/.
```

HTTP Info

REQUEST MADE

```
GET / HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 302
x-powered-by: PHP/5.5.9-1ubuntu4.14
location: portal.php
content-type: text/html
x-cloud-trace-context: 007e090dd352049025be74deb6b4d016
date: Tue, 19 Nov 2024 03:14:32 GMT
```

```
server: Google Frontend
content-length: 0
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/login.php

Identification

OUTPUT

```
The scanner did not find any Strict-Transport-Security header in the response returned by the target when querying URL
https://juice-shop-388277804329.us-west1.run.app/login.php.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/login.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control=no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 01:51:06 GMT
Expires=Thu, 19 Nov 1981 08:52:00 GMT
Pragma=no-cache
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=97249a7d3363c12f26d1d625a5fdf4df
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4826
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/training_install.php

Identification

OUTPUT

```
The scanner did not find any Strict-Transport-Security header in the response returned by the target when querying URL
https://juice-shop-388277804329.us-west1.run.app/training_install.php.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/training_install.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 02:31:16 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=dc248926d66de31d4ae1d4212ab637d0
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4629
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/soap/

Identification

OUTPUT

```
The scanner did not find any Strict-Transport-Security header in the response returned by the target when querying URL
https://juice-shop-388277804329.us-west1.run.app/soap/.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/soap/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 01:24:49 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=00c8cab83d92eca2ba95785b966a73c5
Content-Length=4201
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/db/

Identification

OUTPUT

```
The scanner did not find any Strict-Transport-Security header in the response returned by the target when querying URL
https://juice-shop-388277804329.us-west1.run.app/db/.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/db/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 00:39:25 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=7330f8397d6d6ed7b0975d370f2d06ee
Content-Length=1778
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/passwords/

Identification

OUTPUT

```
The scanner did not find any Strict-Transport-Security header in the response returned by the target when querying URL
https://juice-shop-388277804329.us-west1.run.app/passwords/.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/passwords/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 01:15:47 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=23cbd446a1bfac87a66163e22db42b14
Content-Length=2204
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/soap/class.nusoap_base.php

Identification

OUTPUT

```
The scanner did not find any Strict-Transport-Security header in the response returned by the target when querying URL
https://juice-shop-388277804329.us-west1.run.app/soap/class.nusoap_base.php.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/soap/class.nusoap_base.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type=text/html
Date=Tue, 19 Nov 2024 06:46:36 GMT
Server=Google Frontend
X-Cloud-Trace-Context=c53cd0b0ef8c298766ed3c1bd61168b7
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=811
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/soap/class.wsdlcache.php

Identification

OUTPUT

```
The scanner did not find any Strict-Transport-Security header in the response returned by the target when querying URL
https://juice-shop-388277804329.us-west1.run.app/soap/class.wsdlcache.php.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/soap/class.wsdlcache.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type=text/html
Date=Tue, 19 Nov 2024 06:59:07 GMT
Server=Google Frontend
X-Cloud-Trace-Context=7cb98e8601bf9fb1d2977a54ea93f5f7
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=811
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/install.php

Identification

OUTPUT

```
The scanner did not find any Strict-Transport-Security header in the response returned by the target when querying URL
https://juice-shop-388277804329.us-west1.run.app/install.php.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/install.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Arch=""
Sec-Ch-Ua-Bitness=""
Sec-Ch-Ua-Full-Version-List="Chromium", "HeadlessChrome", "Not-A.Brand";v="99.0.0.0"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Model=""
Sec-Ch-Ua-Platform="Linux"
Sec-Ch-Ua-Platform-Version=""
Sec-Ch-Ua-Wow64=?0
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 00:19:04 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=793633ff205741c27021c36f1f4362a8
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=3083
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/passwords/wp-config.bak

Identification

OUTPUT

```
The scanner did not find any Strict-Transport-Security header in the response returned by the target when querying URL
https://juice-shop-388277804329.us-west1.run.app/passwords/wp-config.bak.
```

HTTP Info

REQUEST MADE

```
GET /passwords/wp-config.bak HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 200
last-modified: Wed, 13 Nov 2024 02:15:28 GMT
etag: "603-626c1e84a7000"
accept-ranges: bytes
content-type: application/x-trash
x-cloud-trace-context: bccbdb7c061d2d5009d67b2ae3eb5bac
date: Tue, 19 Nov 2024 06:12:37 GMT
server: Google Frontend
content-length: 1539
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/passwords/heroes.xml

Identification

OUTPUT

```
The scanner did not find any Strict-Transport-Security header in the response returned by the target when querying URL
https://juice-shop-388277804329.us-west1.run.app/passwords/heroes.xml.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/passwords/heroes.xml
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
H3 200
Accept-Ranges=bytes
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=application/xml
Date=Tue, 19 Nov 2024 06:00:20 GMT
Etag="4b8-626c1e84a7000-gzip"
Last-Modified=Wed, 13 Nov 2024 02:15:28 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=d0db3cb698fff35d3398f6d368ed869f
Content-Length=433
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/info_install.php

Identification

OUTPUT

```
The scanner did not find any Strict-Transport-Security header in the response returned by the target when querying URL
https://juice-shop-388277804329.us-west1.run.app/info_install.php.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/info_install.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Arch=""
Sec-Ch-Ua-Bitness=""
Sec-Ch-Ua-Full-Version-List="Chromium", "HeadlessChrome", "Not-A.Brand";v="99.0.0.0"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Model=""
Sec-Ch-Ua-Platform="Linux"
Sec-Ch-Ua-Platform-Version=""
Sec-Ch-Ua-Wow64=?0
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 02:21:07 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=3305fabc85563bee1adce5fca1986cef
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4188
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/#/

Identification

OUTPUT

```
The scanner did not find any Strict-Transport-Security header in the response returned by the target when querying URL
https://juice-shop-388277804329.us-west1.run.app/#/.
```

HTTP Info

REQUEST MADE

```
GET / HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
```

RESPONSE HEADERS

```
HTTP/2 302
x-powered-by: PHP/5.5.9-1ubuntu4.14
location: portal.php
content-type: text/html
x-cloud-trace-context: bd03eeb04ea4d0db88d2fb3b7cc89f58
date: Tue, 19 Nov 2024 00:10:35 GMT
server: Google Frontend
content-length: 0
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/portal.php

Identification

OUTPUT

```
The scanner did not find any Strict-Transport-Security header in the response returned by the target when querying URL
https://juice-shop-388277804329.us-west1.run.app/portal.php.
```

HTTP Info

REQUEST MADE

```
GET /portal.php HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 302
x-powered-by: PHP/5.5.9-1ubuntu4.14
expires: Thu, 19 Nov 1981 08:52:00 GMT
cache-control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
pragma: no-cache
location: login.php
content-type: text/html
x-cloud-trace-context: c1d67e5b82826b69f35bf8378f780dc6
date: Tue, 19 Nov 2024 00:15:26 GMT
server: Google Frontend
content-length: 0
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/apps/movie_search

Identification

OUTPUT

```
The scanner did not find any Strict-Transport-Security header in the response returned by the target when querying URL
https://juice-shop-388277804329.us-west1.run.app/apps/movie_search.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/apps/movie_search
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Arch=""
Sec-Ch-Ua-Bitness=""
Sec-Ch-Ua-Full-Version-List="Chromium", "HeadlessChrome", "Not-A.Brand";v="99.0.0.0"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Model=""
Sec-Ch-Ua-Platform="Linux"
Sec-Ch-Ua-Platform-Version=""
Sec-Ch-Ua-Wow64=?0
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Accept-Ranges=bytes
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type=text/html
Date=Tue, 19 Nov 2024 03:18:44 GMT
Etag="d9a7-626c1e84a7000"
Last-Modified=Wed, 13 Nov 2024 02:15:28 GMT
Server=Google Frontend
X-Cloud-Trace-Context=4a149f49b940643dfb9c9bcafe0604bb
Content-Length=55719
```

Directory Listing

VULNERABILITY MEDIUM PLUGIN ID 98084

Description

Web servers permitting directory listing are typically used for sharing files.

Directory listing allows the client to view a simple list of all the files and folders hosted on the web server. The client is then able to traverse each directory and download the files.

Cyber-criminals will utilise the presence of directory listing to discover sensitive files, download protected content, or even just learn how the web application is strurctured.

Scanner discovered that the affected page permits directory listing.

Solution

Unless the web server is being utilised to share static and non-sensitive files, enabling directory listing is considered a poor security practice
This can typically be done with a simple configuration change on the server. The steps to disable the directory listing will differ depending on the type of server being used (IIS, Apache, etc.). If directory listing is required, and permitted, then steps should be taken to ensure that the risk of such a configuration is reduced.
These can include:
1. Requiring authentication to access affected pages. 2. Adding the affected path to the `robots.txt` file to prevent the directory contents being searchable via search engines. 3. Ensuring that sensitive files are not stored within the web or document root. 4. Removing any files that are not required for the application to function.

See Also
https://www.owasp.org/index.php/OWASP_Periodic_Table_of_Vulnerabilities_-_Directory_Indexing

Plugin Details

PUBLICATION DATE	2019-02-04T00:00:00+00:00
MODIFICATION DATE	2024-08-12T00:00:00+00:00
FAMILY	Web Servers
SEVERITY	Medium
PLUGIN ID	98084

Risk Information

CVSSV4 BASE SCORE	6.9
CVSSV4 VECTOR	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N
CVSSV3 BASE SCORE	5.3
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
CVSS BASE SCORE	5.0
CVSS VECTOR	CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N

Reference Information

CWE	548
WASC	Directory Indexing
OWASP	2017-A6, 2021-A1, 2013-A5, 2010-A6, 2023-API8, 2019-API7
CVE	-
BID	-

Directory Listing Instances (8)

VULNERABILITY MEDIUM PLUGIN ID 98084

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/passwords/

Identification

OUTPUT

```
WAS Scanner has enumerated the following Directory Listings:

- https://juice-shop-388277804329.us-west1.run.app/passwords/
```

HTTP Info

REQUEST MADE

```
GET /passwords/ HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 200
vary: Accept-Encoding
content-type: text/html;charset=UTF-8
content-encoding: gzip
x-cloud-trace-context: cd3f9259fd82e950213bc4599d9dcb6e
date: Tue, 19 Nov 2024 01:21:21 GMT
server: Google Frontend
content-length: 518
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/documents/

Identification

OUTPUT

```
WAS Scanner has enumerated the following Directory Listings:

- https://juice-shop-388277804329.us-west1.run.app/documents/
```

HTTP Info

REQUEST MADE

```
GET /documents/ HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
```

```
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 200
vary: Accept-Encoding
content-type: text/html;charset=UTF-8
content-encoding: gzip
x-cloud-trace-context: 1873fa39a8b9382d83c4888155213b31
date: Tue, 19 Nov 2024 00:54:04 GMT
server: Google Frontend
content-length: 628
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/db/

Identification

OUTPUT

```
WAS Scanner has enumerated the following Directory Listings:

- https://juice-shop-388277804329.us-west1.run.app/db/
```

HTTP Info

REQUEST MADE

```
GET /db/ HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 200
vary: Accept-Encoding
content-type: text/html;charset=UTF-8
content-encoding: gzip
x-cloud-trace-context: 891eb0ffb664c618f1876b678be424a3
date: Tue, 19 Nov 2024 00:44:55 GMT
server: Google Frontend
content-length: 477
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/stylesheets/

Identification

OUTPUT

```
WAS Scanner has enumerated the following Directory Listings:

- https://juice-shop-388277804329.us-west1.run.app/stylesheets/
```

HTTP Info

REQUEST MADE

```
GET /stylesheets/ HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 200
vary: Accept-Encoding
content-type: text/html;charset=UTF-8
content-encoding: gzip
x-cloud-trace-context: a3c4e778db1f606c8341fcda67c48745
date: Tue, 19 Nov 2024 01:39:58 GMT
server: Google Frontend
content-length: 514
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/js/

Identification

OUTPUT

```
WAS Scanner has enumerated the following Directory Listings:

- https://juice-shop-388277804329.us-west1.run.app/js/
```

HTTP Info

REQUEST MADE

```
GET /js/ HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 200
vary: Accept-Encoding
content-type: text/html;charset=UTF-8
content-encoding: gzip
x-cloud-trace-context: d269e02571af679889bd62bd85b4e48a
date: Tue, 19 Nov 2024 01:12:19 GMT
server: Google Frontend
content-length: 532
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/soap/

Identification

OUTPUT

```
WAS Scanner has enumerated the following Directory Listings:

- https://juice-shop-388277804329.us-west1.run.app/soap/
```

HTTP Info

REQUEST MADE

```
GET /soap/ HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 200
vary: Accept-Encoding
content-type: text/html;charset=UTF-8
content-encoding: gzip
x-cloud-trace-context: 0f7345238c4d74fb5acb36bbb17a8516
date: Tue, 19 Nov 2024 01:30:25 GMT
server: Google Frontend
content-length: 649
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/images/

Identification

OUTPUT

```
WAS Scanner has enumerated the following Directory Listings:

- https://juice-shop-388277804329.us-west1.run.app/images/
```

HTTP Info

REQUEST MADE

```
GET /images/ HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 200
vary: Accept-Encoding
content-type: text/html;charset=UTF-8
content-encoding: gzip
x-cloud-trace-context: 62a5baa5c9f0d1fad2d940efbf109366;o=1
date: Tue, 19 Nov 2024 01:03:16 GMT
```

```
server: Google Frontend
content-length: 769
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/apps/

Identification

OUTPUT

```
WAS Scanner has enumerated the following Directory Listings:

- https://juice-shop-388277804329.us-west1.run.app/apps/
```

HTTP Info

REQUEST MADE

```
GET /apps/ HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 200
vary: Accept-Encoding
content-type: text/html;charset=UTF-8
content-encoding: gzip
x-cloud-trace-context: e04193ff70c470fdd8143563f51794f7;o=1
date: Tue, 19 Nov 2024 00:35:47 GMT
server: Google Frontend
content-length: 479
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

PHPinfo Information Disclosure

VULNERABILITY MEDIUM PLUGIN ID 98223

Description

Many PHP installation tutorials instruct the user to create a PHP file that calls the PHP function 'phpinfo()' for debugging purposes, and various PHP applications may also include such a file by default. By accessing it, a remote attacker can discover a large amount of information about the remote web server configuration to help conduct further attacks, including :
- Versions of the web server, operating system and PHP components
- Details of the PHP configuration
- Loaded PHP extensions with their configurations
- Server environment variables.

Solution

Remove the affected file(s).

See Also
http://php.net/manual/en/function.phpinfo.php

Plugin Details

PUBLICATION DATE	2018-06-27T00:00:00+00:00
MODIFICATION DATE	2022-06-28T00:00:00+00:00
FAMILY	Web Applications
SEVERITY	Medium
PLUGIN ID	98223

Risk Information

CVSSV4 BASE SCORE	6.9
CVSSV4 VECTOR	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N
CVSSV3 BASE SCORE	5.8
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N
CVSS BASE SCORE	5.0
CVSS VECTOR	CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N

Reference Information

CWE	200
WASC	Information Leakage
OWASP	2017-A6, 2021-A1, 2013-A5, 2010-A6, 2023-API8, 2019-API7
CVE	-
BID	-

PHPinfo Information Disclosure Instances (1)

VULNERABILITY MEDIUM PLUGIN ID 98223

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/phpinfo.php

Identification

PROOF

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml"><head>
<style type="text/css">
body {background-color: #ffffff; color: #000000;}
```

OUTPUT

```
The scanner detected the presence of the `phpinfo.php` file on https://juice-shop-388277804329.us-west1.run.app/phpinfo.
php
```

HTTP Info

REQUEST MADE

```
GET /phpinfo.php HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
```

RESPONSE HEADERS

```
HTTP/2 200
x-powered-by: PHP/5.5.9-1ubuntu4.14
vary: Accept-Encoding
content-type: text/html
content-encoding: gzip
x-cloud-trace-context: 033460d4c241a6aca82daeef78772f13
date: Tue, 19 Nov 2024 00:11:32 GMT
server: Google Frontend
content-length: 18936
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

Web.config File Information Disclosure

VULNERABILITY MEDIUM PLUGIN ID 98594

Description

An information disclosure vulnerability exists in the remote web server due to the disclosure of the web.config file. An unauthenticated, remote attacker can exploit this, via a simple GET request, to disclose potentially sensitive configuration information.

Solution

Ensure proper restrictions are in place, or remove the file if the file is not required.

See Also

Plugin Details

PUBLICATION DATE	2019-05-14T00:00:00+00:00
MODIFICATION DATE	2022-05-16T00:00:00+00:00
FAMILY	Data Exposure
SEVERITY	Medium
PLUGIN ID	98594

Risk Information

CVSSV4 BASE SCORE	6.9
CVSSV4 VECTOR	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N
CVSSV3 BASE SCORE	5.3
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
CVSS BASE SCORE	5.0
CVSS VECTOR	CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N

Reference Information

CWE	425
WASC	Predictable Resource Location
OWASP	2010-A4, 2021-A1, 2013-A4, 2017-A5, 2019-API7, 2023-API3, 2019-API3, 2023-API8
CVE	-
BID	-

Web.config File Information Disclosure Instances (1)

VULNERABILITY MEDIUM PLUGIN ID 98594

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/passwords/web.config

Identification

PROOF

```
<?xml version="1.0"?>
<configuration>
<configSections>
<sectionGroup name="system.web.extensions" type="System.Web.Configuration.SystemWebExtensionsSectionGroup, System.Web.Extensions, Version=3.5.0.0, Culture=neutral, PublicKeyToken=31BF3856AD364E35">
```

OUTPUT

```
The scanner detected the presence of the `web.config` file on https://juice-shop-388277804329.us-west1.run.app/passwords/web.config
```

HTTP Info

REQUEST MADE

```
GET /passwords/web.config HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 200
content-location: web.config.bak
vary: negotiate
tcn: choice
last-modified: Wed, 13 Nov 2024 02:15:28 GMT
etag: "1d84-626c1e84a7000;626c1e84a7000"
accept-ranges: bytes
content-type: application/x-trash
x-cloud-trace-context: 2d90a8fe0d402ca031593f36b106beeb
date: Tue, 19 Nov 2024 01:16:14 GMT
server: Google Frontend
content-length: 7556
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

SSL/TLS Forward Secrecy Cipher Suites Not Supported

VULNERABILITY MEDIUM PLUGIN ID 98617

Description

The remote host use at least one SSL/TLS ciphers that does not offer forward secrecy (FS) also known as perfect forward secrecy (PFS). It's a feature that provides assurances the session keys will not be compromised even if the server's private key is compromised.

Solution

Reconfigure the server to disable cipher suites without forward secrecy and retain only cipher suites that provide forward secrecy (ECDHE or DHE based cipher suites).

See Also

https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml

Plugin Details

PUBLICATION DATE	2019-06-12T00:00:00+00:00
MODIFICATION DATE	2022-11-10T00:00:00+00:00
FAMILY	SSL/TLS
SEVERITY	Medium
PLUGIN ID	98617

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	6.5
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N
CVSS BASE SCORE	5.8
CVSS VECTOR	CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N

Reference Information

CWE	327
WASC	Insufficient Transport Layer Protection
OWASP	2010-A9, 2013-A6, 2017-A3, 2021-A2, 2023-API8, 2019-API7
CVE	-
BID	-

SSL/TLS Forward Secrecy Cipher Suites Not Supported Instances (1)

VULNERABILITY MEDIUM PLUGIN ID 98617

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/#/

Identification

OUTPUT

```
Protocol Cipher Suite Name (RFC) Key Exchange Strength
--------------------------------------------------------------------
TLS1.2 TLS_RSA_WITH_AES_128_GCM_SHA256 RSA 4096
TLS1.2 TLS_RSA_WITH_AES_256_GCM_SHA384 RSA 4096
TLS1.2 TLS_RSA_WITH_AES_128_CBC_SHA RSA 4096
TLS1.2 TLS_RSA_WITH_AES_256_CBC_SHA RSA 4096
```

Source Code Passive Disclosure

VULNERABILITY MEDIUM PLUGIN ID 98779

Description

Scanner has detected server-side source code within the server's response.

A modern web application will be reliant on several different programming languages. These languages can be broken up in two flavours. These are client-side languages (such as those that run in the browser -- like JavaScript) and server-side languages (which are executed by the server -- like ASP, PHP, JSP, etc.) to form the dynamic pages (client-side code) that are then sent to the client.

Because all server side code should be executed by the server, it should never be seen by the client, however in some scenarios it is possible that the server has a misconfiguration or the server side code has syntax errors, and therefore is not executed by the server but is instead sent to the client. As the server-side source code often contains sensitive information, such as database connection strings or details into the application workflow, this can be extremely risky.

Cyber-criminals will attempt to discover pages that either accidentally or forcefully allow the server-side source code to be disclosed, to assist in discovering further vulnerabilities or sensitive information.

Solution

It is important that the server does not deliver server side code to the client, and the server misconfiguration or server code should be changed to prevent this.

See Also

Plugin Details

PUBLICATION DATE	2019-12-19T00:00:00+00:00
MODIFICATION DATE	2024-01-03T00:00:00+00:00
FAMILY	Data Exposure
SEVERITY	Medium
PLUGIN ID	98779

Risk Information

CVSSV4 BASE SCORE	6.9
CVSSV4 VECTOR	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N
CVSSV3 BASE SCORE	5.3
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
CVSS BASE SCORE	5.0
CVSS VECTOR	CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N

Reference Information

CWE	540
WASC	Information Leakage

OWASP	2017-A6, 2021-A1, 2010-A6, 2013-A5, 2023-API3, 2019-API3
CVE	-
BID	-

Source Code Passive Disclosure Instances (2)

VULNERABILITY MEDIUM PLUGIN ID 98779

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/passwords/wp-config.bak

Identification

PROOF

```
The following patterns were detected in the HTTP response body :
- <?php
```

OUTPUT

```
The scanner detected the presence of a 'PHP' source code in the web application response.
```

HTTP Info

REQUEST MADE

```
GET /passwords/wp-config.bak HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 200
last-modified: Wed, 13 Nov 2024 02:15:28 GMT
etag: "603-626c1e84a7000"
accept-ranges: bytes
content-type: application/x-trash
x-cloud-trace-context: b51b044286083ea892339be8a5c6cd23
date: Tue, 19 Nov 2024 06:12:36 GMT
server: Google Frontend
content-length: 1539
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/db/bwapp.sqlite

Identification

PROOF

```
The following patterns were detected in the HTTP response body :
- <?
```

OUTPUT

```
The scanner detected the presence of a 'PHP' source code in the web application response.
```

HTTP Info

REQUEST MADE

```
GET /db/bwapp.sqlite HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 200
last-modified: Wed, 13 Nov 2024 02:15:28 GMT
etag: "3000-626c1e84a7000"
accept-ranges: bytes
x-cloud-trace-context: 3b1f04fc2625b48a3ce0ea58d5a10a7e
date: Tue, 19 Nov 2024 03:57:00 GMT
content-type: text/html
server: Google Frontend
content-length: 12288
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

Apache 2.4.x < 2.4.35 Denial of Service

VULNERABILITY MEDIUM PLUGIN ID 98916

Description

According to its banner, the version of Apache running on the remote host is 2.4.x prior to 2.4.35. By sending continuous SETTINGS frames of maximum size an ongoing HTTP/2 connection could be kept busy and would never time out. This can be abused for a DoS on the server. This only affect a server that has enabled the h2 protocol.

Note that the scanner has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Apache version 2.4.35 or later.

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.4.35
https://httpd.apache.org/security/vulnerabilities_24.html#2.4.35

Plugin Details

PUBLICATION DATE	2019-01-31T00:00:00+00:00
MODIFICATION DATE	2023-03-14T00:00:00+00:00
FAMILY	Component Vulnerability
SEVERITY	Medium
PLUGIN ID	98916

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	5.9
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H
CVSS BASE SCORE	4.3
CVSS VECTOR	CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:P

Reference Information

CWE	20, 400
WASC	Denial of Service, Improper Input Handling
OWASP	2010-A4, 2021-A3, 2021-A6, 2013-A9, 2013-A4, 2017-A9, 2017-A5, 2019-API7, 2023-API8
CVE	CVE-2018-11763
BID	105414

Apache 2.4.x < 2.4.35 Denial of Service Instances (1)

VULNERABILITY MEDIUM PLUGIN ID 98916

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/apps/

Identification

OUTPUT

```
Current Version: 2.4.7
Fixed Version: 2.4.35
Detected technology URL: https://juice-shop-388277804329.us-west1.run.app/apps/
```

Apache 2.4.x < 2.4.43 Multiple Vulnerabilities

VULNERABILITY MEDIUM PLUGIN ID 98998

Description

According to its banner, the version of Apache running on the remote host is 2.4.x prior to 2.4.43. It is, therefore, affected by multiple vulnerabilities:

- An uninitialized value vulnerability exists in mod_proxy_ftp. (CVE-2020-1934)

- An open redirect vulnerability exists in mod_rewrite. (CVE-2020-1927)

Note that the scanner has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Apache version 2.4.43 or later.

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.4.43
https://httpd.apache.org/security/vulnerabilities_24.html#2.4.42

Plugin Details

PUBLICATION DATE	2020-04-10T00:00:00+00:00
MODIFICATION DATE	2023-03-14T00:00:00+00:00
FAMILY	Component Vulnerability
SEVERITY	Medium
PLUGIN ID	98998

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	6.1
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
CVSS BASE SCORE	5.8
CVSS VECTOR	CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N

Reference Information

CWE	456, 601, 908
WASC	URL Redirector Abuse
OWASP	2021-A6, 2021-A1, 2013-A10, 2010-A10, 2013-A9, 2017-A9, 2019-API7, 2023-API8
CVE	CVE-2020-1927, CVE-2020-1934
BID	-

Apache 2.4.x < 2.4.43 Multiple Vulnerabilities Instances (1)

VULNERABILITY MEDIUM PLUGIN ID 98998

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/apps/

Identification

OUTPUT

```
Current Version: 2.4.7
Fixed Version: 2.4.43
Detected technology URL: https://juice-shop-388277804329.us-west1.run.app/apps/
```

Web Server Configuration File Detected

VULNERABILITY MEDIUM PLUGIN ID 114195

Description

A web server configuration file has been detected on the target host. This may expose privileged information or configurations to a malicious actor.

Solution

Restrict access to the web server file or remove it.

See Also

Plugin Details

PUBLICATION DATE	2024-02-02T00:00:00+00:00
MODIFICATION DATE	2024-02-02T00:00:00+00:00
FAMILY	Data Exposure
SEVERITY	Medium
PLUGIN ID	114195

Risk Information

CVSSV4 BASE SCORE	6.9
CVSSV4 VECTOR	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N
CVSSV3 BASE SCORE	5.3
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
CVSS BASE SCORE	5.0
CVSS VECTOR	CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N

Reference Information

CWE	538
WASC	Predictable Resource Location
OWASP	2017-A6, 2021-A1, 2013-A5, 2010-A6, 2023-API8, 2023-API3, 2019-API3, 2019-API7
CVE	-
BID	-

Web Server Configuration File Detected Instances (1)

VULNERABILITY MEDIUM PLUGIN ID 114195

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/passwords/web.config

Identification

PROOF

```
<?xml version="1.0"?>
<configuration>
<configSections>
<sectionGroup name="system.web.extensions" type="System.Web.Configuration.SystemWebExtensionsSectionGroup, System.Web.
Extensions, Version=3.5.0.0, Culture=neutral, PublicKeyToken=31BF3856AD364E35">
```

OUTPUT

```
The scanner detected the presence of the `web.config` file on https://juice-shop-388277804329.us-west1.run.app/passwords
/web.config
```

HTTP Info

REQUEST MADE

```
GET /passwords/web.config HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 200
content-location: web.config.bak
vary: negotiate
tcn: choice
last-modified: Wed, 13 Nov 2024 02:15:28 GMT
etag: "1d84-626c1e84a7000;626c1e84a7000"
accept-ranges: bytes
content-type: application/x-trash
x-cloud-trace-context: f39315f1cbdcab2503fb7e87c5d5fc51
date: Tue, 19 Nov 2024 01:16:15 GMT
server: Google Frontend
content-length: 7556
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

Missing 'X-Frame-Options' Header

VULNERABILITY LOW PLUGIN ID 98060

Description

Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.

The server didn't return an `X-Frame-Options` header which means that this website could be at risk of a clickjacking attack.

The `X-Frame-Options` HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites.

Solution

Configure your web server to include an `X-Frame-Options` header.

See Also

http://tools.ietf.org/html/rfc7034
https://developer.mozilla.org/en-US/docs/Web/HTTP/X-Frame-Options
https://www.owasp.org/index.php/Clickjacking

Plugin Details

PUBLICATION DATE	2017-03-31T00:00:00+00:00
MODIFICATION DATE	2024-03-25T00:00:00+00:00
FAMILY	HTTP Security Header
SEVERITY	Low
PLUGIN ID	98060

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	3.1
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N
CVSS BASE SCORE	2.6
CVSS VECTOR	CVSS2#AV:N/AC:H/Au:N/C:N/I:P/A:N

Reference Information

CWE	1021, 346
WASC	Application Misconfiguration
OWASP	2021-A7, 2017-A6, 2021-A4, 2013-A5, 2010-A6, 2023-API8, 2019-API7
CVE	-

BID	-

Missing 'X-Frame-Options' Header Instances (25)

VULNERABILITY LOW PLUGIN ID 98060

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/stylesheets/

Identification

OUTPUT

```
Page https://juice-shop-388277804329.us-west1.run.app/stylesheets/ has no X-Frame-Options header defined
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/stylesheets/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 01:34:22 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=91660b485a30bbed64793dbe904193d3
Content-Length=2275
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/passwords/

Identification

OUTPUT

```
Page https://juice-shop-388277804329.us-west1.run.app/passwords/ has no X-Frame-Options header defined
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/passwords/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 01:15:47 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=23cbd446a1bfac87a66163e22db42b14
Content-Length=2204
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/passwords/wp-config.bak

Identification

OUTPUT

```
Page https://juice-shop-388277804329.us-west1.run.app/passwords/wp-config.bak has no X-Frame-Options header defined
```

HTTP Info

REQUEST MADE

```
GET /passwords/wp-config.bak HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 200
last-modified: Wed, 13 Nov 2024 02:15:28 GMT
etag: "603-626c1e84a7000"
accept-ranges: bytes
content-type: application/x-trash
x-cloud-trace-context: bccbdb7c061d2d5009d67b2ae3eb5bac
date: Tue, 19 Nov 2024 06:12:37 GMT
server: Google Frontend
content-length: 1539
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/passwords/web.config.bak

Identification

OUTPUT

```
Page https://juice-shop-388277804329.us-west1.run.app/passwords/web.config.bak has no X-Frame-Options header defined
```

HTTP Info

REQUEST MADE

```
GET /passwords/web.config.bak HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 200
last-modified: Wed, 13 Nov 2024 02:15:28 GMT
etag: "1d84-626c1e84a7000"
accept-ranges: bytes
content-type: application/x-trash
x-cloud-trace-context: dd8a0753fe21b8d0d381c2313f0202d5
date: Tue, 19 Nov 2024 06:08:24 GMT
server: Google Frontend
content-length: 7556
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/soap/nusoap.php

Identification

OUTPUT

```
Page https://juice-shop-388277804329.us-west1.run.app/soap/nusoap.php has no X-Frame-Options header defined
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/soap/nusoap.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type=text/html
Date=Tue, 19 Nov 2024 07:07:36 GMT
Server=Google Frontend
X-Cloud-Trace-Context=9b95efa061e2e33130bff09373a821c4
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=811
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/images/

Identification

OUTPUT

```
Page https://juice-shop-388277804329.us-west1.run.app/images/ has no X-Frame-Options header defined
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/images/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 00:57:42 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=fc3fee9e75c9304bb77fd657cb75393d
Content-Length=5991
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/install.php

Identification

OUTPUT

```
Page https://juice-shop-388277804329.us-west1.run.app/install.php has no X-Frame-Options header defined
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/install.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Arch=""
Sec-Ch-Ua-Bitness=""
Sec-Ch-Ua-Full-Version-List="Chromium", "HeadlessChrome", "Not-A.Brand";v="99.0.0.0"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Model=""
Sec-Ch-Ua-Platform="Linux"
Sec-Ch-Ua-Platform-Version=""
Sec-Ch-Ua-Wow64=?0
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 00:19:04 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=793633ff205741c27021c36f1f4362a8
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=3083
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/db/

Identification

OUTPUT

```
Page https://juice-shop-388277804329.us-west1.run.app/db/ has no X-Frame-Options header defined
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/db/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
```

```
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 00:39:25 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=7330f8397d6d6ed7b0975d370f2d06ee
Content-Length=1778
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/js/

Identification

OUTPUT

```
Page https://juice-shop-388277804329.us-west1.run.app/js/ has no X-Frame-Options header defined
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/js/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 01:06:45 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=92dbc4630193c57aa70de731a23c4521
Content-Length=2393
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/info_install.php

Identification

OUTPUT

```
Page https://juice-shop-388277804329.us-west1.run.app/info_install.php has no X-Frame-Options header defined
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/info_install.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Arch=""
Sec-Ch-Ua-Bitness=""
Sec-Ch-Ua-Full-Version-List="Chromium", "HeadlessChrome", "Not-A.Brand";v="99.0.0.0"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Model=""
Sec-Ch-Ua-Platform="Linux"
Sec-Ch-Ua-Platform-Version=""
Sec-Ch-Ua-Wow64=?0
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 02:21:07 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=3305fabc85563bee1adce5fca1986cef
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4188
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/user_new.php

Identification

OUTPUT

```
Page https://juice-shop-388277804329.us-west1.run.app/user_new.php has no X-Frame-Options header defined
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/user_new.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
```

```
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 07:45:52 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=1de28a3c31c89c397b35ab9cf352eeaf
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4224
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/db/bwapp.sqlite

Identification

OUTPUT

```
Page https://juice-shop-388277804329.us-west1.run.app/db/bwapp.sqlite has no X-Frame-Options header defined
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/db/bwapp.sqlite
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Accept-Ranges=bytes
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type=text/html
Date=Tue, 19 Nov 2024 03:57:01 GMT
Etag="3000-626c1e84a7000"
Last-Modified=Wed, 13 Nov 2024 02:15:28 GMT
Server=Google Frontend
X-Cloud-Trace-Context=2a74d2d814c14512fd8fac93e4bfc679
Content-Length=12288
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/training_install.php

Identification

OUTPUT

```
Page https://juice-shop-388277804329.us-west1.run.app/training_install.php has no X-Frame-Options header defined
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/training_install.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 02:31:16 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=dc248926d66de31d4ae1d4212ab637d0
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4629
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/info.php

Identification

OUTPUT

```
Page https://juice-shop-388277804329.us-west1.run.app/info.php has no X-Frame-Options header defined
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/info.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
```

```
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 08:28:20 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=d1dec854dbe62de69a7b5ea639baba79
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4239
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/soap/class.soap_fault.php

Identification

OUTPUT

```
Page https://juice-shop-388277804329.us-west1.run.app/soap/class.soap_fault.php has no X-Frame-Options header defined
```

HTTP Info

REQUEST MADE

```
GET /soap/class.soap_fault.php HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 500
x-powered-by: PHP/5.5.9-1ubuntu4.14
content-type: text/html
x-cloud-trace-context: 85c8d444051c598a5636d47e2436b1d1
date: Tue, 19 Nov 2024 06:54:58 GMT
server: Google Frontend
content-length: 0
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/apps/movie_search

Identification

OUTPUT

```
Page https://juice-shop-388277804329.us-west1.run.app/apps/movie_search has no X-Frame-Options header defined
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/apps/movie_search
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Arch=""
Sec-Ch-Ua-Bitness=""
Sec-Ch-Ua-Full-Version-List="Chromium", "HeadlessChrome", "Not-A.Brand";v="99.0.0.0"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Model=""
Sec-Ch-Ua-Platform="Linux"
Sec-Ch-Ua-Platform-Version=""
Sec-Ch-Ua-Wow64=?0
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Accept-Ranges=bytes
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type=text/html
Date=Tue, 19 Nov 2024 03:18:44 GMT
Etag="d9a7-626c1e84a7000"
Last-Modified=Wed, 13 Nov 2024 02:15:28 GMT
Server=Google Frontend
X-Cloud-Trace-Context=4a149f49b940643dfb9c9bcafe0604bb
Content-Length=55719
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/soap/

Identification

OUTPUT

```
Page https://juice-shop-388277804329.us-west1.run.app/soap/ has no X-Frame-Options header defined
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/soap/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
```

```
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 01:24:49 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=00c8cab83d92eca2ba95785b966a73c5
Content-Length=4201
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/phpinfo.php

Identification

OUTPUT

```
Page https://juice-shop-388277804329.us-west1.run.app/phpinfo.php has no X-Frame-Options header defined
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/phpinfo.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 01:43:29 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=036c4d5909306dec6b8d0193b59d617a
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=85702
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/training.php

Identification

OUTPUT

```
Page https://juice-shop-388277804329.us-west1.run.app/training.php has no X-Frame-Options header defined
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/training.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 08:36:37 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=beee281846f3b9b9397b531ce1a92fef
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4656
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/passwords/heroes.xml

Identification

OUTPUT

```
Page https://juice-shop-388277804329.us-west1.run.app/passwords/heroes.xml has no X-Frame-Options header defined
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/passwords/heroes.xml
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
```

```
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
H3 200
Accept-Ranges=bytes
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=application/xml
Date=Tue, 19 Nov 2024 06:00:20 GMT
Etag="4b8-626c1e84a7000-gzip"
Last-Modified=Wed, 13 Nov 2024 02:15:28 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=d0db3cb698fff35d3398f6d368ed869f
Content-Length=433
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/login.php

Identification

OUTPUT

```
Page https://juice-shop-388277804329.us-west1.run.app/login.php has no X-Frame-Options header defined
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/login.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control=no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 01:51:06 GMT
Expires=Thu, 19 Nov 1981 08:52:00 GMT
Pragma=no-cache
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=97249a7d3363c12f26d1d625a5fdf4df
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4826
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/soap/class.nusoap_base.php

Identification

OUTPUT

```
Page https://juice-shop-388277804329.us-west1.run.app/soap/class.nusoap_base.php has no X-Frame-Options header defined
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/soap/class.nusoap_base.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type=text/html
Date=Tue, 19 Nov 2024 06:46:36 GMT
Server=Google Frontend
X-Cloud-Trace-Context=c53cd0b0ef8c298766ed3c1bd61168b7
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=811
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/soap/class.wsdlcache.php

Identification

OUTPUT

```
Page https://juice-shop-388277804329.us-west1.run.app/soap/class.wsdlcache.php has no X-Frame-Options header defined
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/soap/class.wsdlcache.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
```

```
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type=text/html
Date=Tue, 19 Nov 2024 06:59:07 GMT
Server=Google Frontend
X-Cloud-Trace-Context=7cb98e8601bf9fb1d2977a54ea93f5f7
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=811
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/documents/

Identification

OUTPUT

```
Page https://juice-shop-388277804329.us-west1.run.app/documents/ has no X-Frame-Options header defined
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/documents/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 00:48:33 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=8659790f61386a0d355111f26ee2a386
Content-Length=3149
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/apps/

Identification

OUTPUT

```
Page https://juice-shop-388277804329.us-west1.run.app/apps/ has no X-Frame-Options header defined
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/apps/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 00:30:17 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=b57b66949c25563ad77a69e4a354af47
Content-Length=1782
```

Cookie Without HttpOnly Flag Detected

VULNERABILITY LOW PLUGIN ID 98063

Description

The HttpOnly flag assists in the prevention of client side-scripts (such as JavaScript) from accessing and using the cookie.

This can help prevent XSS attacks from targeting the cookies holding the client's session token (setting the HttpOnly flag does not prevent, nor safeguard against XSS vulnerabilities themselves).

Solution

The initial step to remedy this would be to determine whether any client-side scripts (such as JavaScript) need to access the cookie and if not, set the HttpOnly flag.
It should be noted that some older browsers are not compatible with the HttpOnly flag; therefore, setting this flag will not protect those clients against this form of attack.

See Also

https://www.owasp.org/index.php/HttpOnly

Plugin Details

PUBLICATION DATE	2017-03-31T00:00:00+00:00
MODIFICATION DATE	2023-12-11T00:00:00+00:00
FAMILY	HTTP Security Header
SEVERITY	Low
PLUGIN ID	98063

Risk Information

CVSSV4 BASE SCORE	2.1
CVSSV4 VECTOR	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:A/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N
CVSSV3 BASE SCORE	3.1
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N
CVSS BASE SCORE	2.6
CVSS VECTOR	CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N

Reference Information

CWE	1004
WASC	Application Misconfiguration
OWASP	2010-A9, 2013-A6, 2017-A3, 2021-A5
CVE	-
BID	-

Cookie Without HttpOnly Flag Detected Instances (1)

VULNERABILITY LOW PLUGIN ID 98063

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/

INPUT TYPE	cookie
INPUT NAME	PHPSESSID

Identification

PROOF

```
PHPSESSID=711vt1tpgrucudl1kaq9t074f5; Path=/
```

OUTPUT

```
The scanner detected a cookie named 'PHPSESSID' set with JavaScript which prevents the HTTPOnly attribute from being
used.

If the cookie is set to handle sensitive information (for example session-based information), it should be set via the
HTTP method.
```

HTTP Info

REQUEST MADE

```
GET /portal.php HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 302
x-powered-by: PHP/5.5.9-1ubuntu4.14
expires: Thu, 19 Nov 1981 08:52:00 GMT
cache-control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
pragma: no-cache
location: login.php
content-type: text/html
x-cloud-trace-context: c1d67e5b82826b69f35bf8378f780dc6
date: Tue, 19 Nov 2024 00:15:26 GMT
server: Google Frontend
content-length: 0
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

Cookie Without Secure Flag Detected

VULNERABILITY LOW PLUGIN ID 98064

Description

When the `secure` flag is set on a cookie, the browser will prevent it from being sent over a clear text channel (HTTP) and only allow it to be sent when an encrypted channel is used (HTTPS).

The scanner discovered that a cookie was set by the server without the secure flag being set. Although the initial setting of this cookie was via an HTTPS connection, any HTTP link to the same server will result in the cookie being sent in clear text.

Note that if the cookie does not contain sensitive information, the risk of this vulnerability is mitigated.

Solution

If the cookie contains sensitive information, then the server should ensure that the cookie has the `secure` flag set.

See Also

https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#secure-attribute

Plugin Details

PUBLICATION DATE	2017-03-31T00:00:00+00:00
MODIFICATION DATE	2023-12-11T00:00:00+00:00
FAMILY	HTTP Security Header
SEVERITY	Low
PLUGIN ID	98064

Risk Information

CVSSV4 BASE SCORE	2.1
CVSSV4 VECTOR	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:A/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N
CVSSV3 BASE SCORE	3.1
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N
CVSS BASE SCORE	2.6
CVSS VECTOR	CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N

Reference Information

CWE	614
WASC	Insufficient Transport Layer Protection
OWASP	2010-A9, 2013-A6, 2017-A3, 2021-A5
CVE	-
BID	-

Cookie Without Secure Flag Detected Instances (1)

VULNERABILITY LOW PLUGIN ID 98064

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/

INPUT TYPE	cookie
INPUT NAME	PHPSESSID

Identification

PROOF

```
PHPSESSID=711vt1tpgrucudl1kaq9t074f5; Path=/
```

OUTPUT

```
The scanner detected a cookie named 'PHPSESSID' set with JavaScript without the Secure flag set.
```

HTTP Info

REQUEST MADE

```
GET /portal.php HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 302
x-powered-by: PHP/5.5.9-1ubuntu4.14
expires: Thu, 19 Nov 1981 08:52:00 GMT
cache-control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
pragma: no-cache
location: login.php
content-type: text/html
x-cloud-trace-context: c1d67e5b82826b69f35bf8378f780dc6
date: Tue, 19 Nov 2024 00:15:26 GMT
server: Google Frontend
content-length: 0
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

Password Field With Auto-Complete

VULNERABILITY LOW PLUGIN ID 98081

Description

In typical form-based web applications, it is common practice for developers to allow `autocomplete` within the HTML form to improve the usability of the page. With `autocomplete` enabled (default), the browser is allowed to cache previously entered form values.

For legitimate purposes, this allows the user to quickly re-enter the same data when completing the form multiple times.

When `autocomplete` is enabled on either/both the username and password fields, this could allow a cyber-criminal with access to the victim's computer the ability to have the victim's credentials automatically entered as the cyber-criminal visits the affected page.

Scanner has discovered that the affected page contains a form containing a password field that has not disabled `autocomplete`.

Solution

The `autocomplete` value can be configured in two different locations.
The first and most secure location is to disable the `autocomplete` attribute on the `<form>` HTML tag. This will disable `autocomplete` for all inputs within that form. An example of disabling `autocomplete` within the form tag is `<form autocomplete=off>`.
The second slightly less desirable option is to disable the `autocomplete` attribute for a specific `<input>` HTML tag. While this may be the less desired solution from a security perspective, it may be preferred method for usability reasons, depending on size of the form. An example of disabling the `autocomplete` attribute within a password input tag is `<input type=password autocomplete=off>`.

See Also

https://www.owasp.org/index.php/Testing_for_Vulnerable_Remember_Password_(OTG-AUTHN-005)

Plugin Details

PUBLICATION DATE	2017-03-31T00:00:00+00:00
MODIFICATION DATE	2022-03-03T00:00:00+00:00
FAMILY	Authentication & Session
SEVERITY	Low
PLUGIN ID	98081

Risk Information

CVSSV4 BASE SCORE	2.3
CVSSV4 VECTOR	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:L/SA:N
CVSSV3 BASE SCORE	3.1
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N
CVSS BASE SCORE	2.6
CVSS VECTOR	CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N

Reference Information

CWE	16
WASC	Application Misconfiguration
OWASP	2021-A5, 2017-A6, 2013-A5, 2010-A6, 2023-API8, 2019-API7
CVE	-
BID	-

Password Field With Auto-Complete Instances (1)

VULNERABILITY LOW PLUGIN ID 98081

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/user_new.php

INPUT TYPE	form
INPUT NAME	combined:post::https://juice-shop-388277804329.us-west1.run.app/user_new.php

Identification

OUTPUT

```
The following form has been found to have not restricted 'password auto complete' attribute :

<form action="/user_new.php" method="POST">
<input type="text" id="login" name="login">
</input>
<input type="text" id="email" name="email" size="30">
</input>
<input type="password" id="password" name="password">
</input>
<input type="password" id="password_conf" name="password_conf">
</input>
<input type="text" id="secret" name="secret" size="40">
</input>
<input type="checkbox" id="mail_activation" name="mail_activation" value="">
</input>
<button type="submit" name="action" value="create">
Create
</button>
</form>
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/user_new.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 07:45:52 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=1de28a3c31c89c397b35ab9cf352eeaf
```

```
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4224
```

HTTP Header Information Disclosure

VULNERABILITY LOW PLUGIN ID 98618

Description

The HTTP headers sent by the remote web server disclose information that can aid an attacker, such as the server version and technologies used by the web server.

Solution

Modify the HTTP headers of the web server to not disclose detailed information about the underlying web server.

See Also

http://projects.webappsec.org/w/page/13246925/Fingerprinting
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers

Plugin Details

PUBLICATION DATE	2019-06-12T00:00:00+00:00
MODIFICATION DATE	2024-03-25T00:00:00+00:00
FAMILY	HTTP Security Header
SEVERITY	Low
PLUGIN ID	98618

Risk Information

CVSSV4 BASE SCORE	2.1
CVSSV4 VECTOR	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:A/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N
CVSSV3 BASE SCORE	3.1
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N
CVSS BASE SCORE	2.6
CVSS VECTOR	CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N

Reference Information

CWE	200
WASC	Information Leakage
OWASP	2017-A6, 2021-A1, 2013-A5, 2010-A6, 2023-API8, 2019-API7
CVE	-
BID	-

HTTP Header Information Disclosure Instances (25)

VULNERABILITY LOW PLUGIN ID 98618

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/stylesheets/

Identification

OUTPUT

```
The following header information disclosures have been detected on https://juice-shop-388277804329.us-west1.run.app
/stylesheets/:

- Server: Google Frontend
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/stylesheets/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 01:34:22 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=91660b485a30bbed64793dbe904193d3
Content-Length=2275
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/apps/movie_search

Identification

OUTPUT

```
The following header information disclosures have been detected on https://juice-shop-388277804329.us-west1.run.app/apps
/movie_search:

- Server: Google Frontend
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/apps/movie_search
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Arch=""
Sec-Ch-Ua-Bitness=""
Sec-Ch-Ua-Full-Version-List="Chromium", "HeadlessChrome", "Not-A.Brand";v="99.0.0.0"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Model=""
Sec-Ch-Ua-Platform="Linux"
Sec-Ch-Ua-Platform-Version=""
Sec-Ch-Ua-Wow64=?0
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Accept-Ranges=bytes
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type=text/html
Date=Tue, 19 Nov 2024 03:18:44 GMT
Etag="d9a7-626c1e84a7000"
Last-Modified=Wed, 13 Nov 2024 02:15:28 GMT
Server=Google Frontend
X-Cloud-Trace-Context=4a149f49b940643dfb9c9bcafe0604bb
Content-Length=55719
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/soap/class.nusoap_base.php

Identification

OUTPUT

```
The following header information disclosures have been detected on https://juice-shop-388277804329.us-west1.run.app/soap
/class.nusoap_base.php:

- X-Powered-By: PHP/5.5.9-1ubuntu4.14
- Server: Google Frontend
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/soap/class.nusoap_base.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
```

```
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type=text/html
Date=Tue, 19 Nov 2024 06:46:36 GMT
Server=Google Frontend
X-Cloud-Trace-Context=c53cd0b0ef8c298766ed3c1bd61168b7
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=811
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/passwords/web.config.bak

Identification

OUTPUT

```
The following header information disclosures have been detected on https://juice-shop-388277804329.us-west1.run.app
/passwords/web.config.bak:

- Server: Google Frontend
```

HTTP Info

REQUEST MADE

```
GET /passwords/web.config.bak HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 200
last-modified: Wed, 13 Nov 2024 02:15:28 GMT
etag: "1d84-626c1e84a7000"
accept-ranges: bytes
content-type: application/x-trash
x-cloud-trace-context: dd8a0753fe21b8d0d381c2313f0202d5
date: Tue, 19 Nov 2024 06:08:24 GMT
server: Google Frontend
content-length: 7556
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/soap/class.soap_fault.php

Identification

OUTPUT

```
The following header information disclosures have been detected on https://juice-shop-388277804329.us-west1.run.app/soap
/class.soap_fault.php:

- X-Powered-By: PHP/5.5.9-1ubuntu4.14
- Server: Google Frontend
```

HTTP Info

REQUEST MADE

```
GET /soap/class.soap_fault.php HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 500
x-powered-by: PHP/5.5.9-1ubuntu4.14
content-type: text/html
x-cloud-trace-context: 85c8d444051c598a5636d47e2436b1d1
date: Tue, 19 Nov 2024 06:54:58 GMT
server: Google Frontend
content-length: 0
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/db/

Identification

OUTPUT

```
The following header information disclosures have been detected on https://juice-shop-388277804329.us-west1.run.app/db/:

- Server: Google Frontend
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/db/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

```
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 00:39:25 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=7330f8397d6d6ed7b0975d370f2d06ee
Content-Length=1778
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/install.php

Identification

OUTPUT

```
The following header information disclosures have been detected on https://juice-shop-388277804329.us-west1.run.app
/install.php:

- X-Powered-By: PHP/5.5.9-1ubuntu4.14
- Server: Google Frontend
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/install.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Arch=""
Sec-Ch-Ua-Bitness=""
Sec-Ch-Ua-Full-Version-List="Chromium", "HeadlessChrome", "Not-A.Brand";v="99.0.0.0"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Model=""
Sec-Ch-Ua-Platform="Linux"
Sec-Ch-Ua-Platform-Version=""
Sec-Ch-Ua-Wow64=?0
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 00:19:04 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=793633ff205741c27021c36f1f4362a8
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=3083
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/images/

Identification

OUTPUT

```
The following header information disclosures have been detected on https://juice-shop-388277804329.us-west1.run.app
/images/:

- Server: Google Frontend
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/images/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 00:57:42 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=fc3fee9e75c9304bb77fd657cb75393d
Content-Length=5991
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/#/

Identification

OUTPUT

```
The following header information disclosures have been detected on https://juice-shop-388277804329.us-west1.run.app/#/:

- X-Powered-By: PHP/5.5.9-1ubuntu4.14
- Server: Google Frontend
```

HTTP Info

REQUEST MADE

```
GET / HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
```

RESPONSE HEADERS

```
HTTP/2 302
x-powered-by: PHP/5.5.9-1ubuntu4.14
location: portal.php
content-type: text/html
x-cloud-trace-context: bd03eeb04ea4d0db88d2fb3b7cc89f58
date: Tue, 19 Nov 2024 00:10:35 GMT
server: Google Frontend
content-length: 0
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/info_install.php

Identification

OUTPUT

```
The following header information disclosures have been detected on https://juice-shop-388277804329.us-west1.run.app
/info_install.php:

- X-Powered-By: PHP/5.5.9-1ubuntu4.14
- Server: Google Frontend
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/info_install.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Arch=""
Sec-Ch-Ua-Bitness=""
Sec-Ch-Ua-Full-Version-List="Chromium", "HeadlessChrome", "Not-A.Brand";v="99.0.0.0"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Model=""
Sec-Ch-Ua-Platform="Linux"
Sec-Ch-Ua-Platform-Version=""
Sec-Ch-Ua-Wow64=?0
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 02:21:07 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=3305fabc85563bee1adce5fca1986cef
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4188
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/phpinfo.php

Identification

OUTPUT

```
The following header information disclosures have been detected on https://juice-shop-388277804329.us-west1.run.app
/phpinfo.php:

- X-Powered-By: PHP/5.5.9-1ubuntu4.14
- Server: Google Frontend
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/phpinfo.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 01:43:29 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=036c4d5909306dec6b8d0193b59d617a
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=85702
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/portal.php

Identification

OUTPUT

```
The following header information disclosures have been detected on https://juice-shop-388277804329.us-west1.run.app
/portal.php:

- X-Powered-By: PHP/5.5.9-1ubuntu4.14
- Server: Google Frontend
```

HTTP Info

REQUEST MADE

```
GET /portal.php HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 302
x-powered-by: PHP/5.5.9-1ubuntu4.14
expires: Thu, 19 Nov 1981 08:52:00 GMT
cache-control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
pragma: no-cache
location: login.php
content-type: text/html
x-cloud-trace-context: c1d67e5b82826b69f35bf8378f780dc6
date: Tue, 19 Nov 2024 00:15:26 GMT
server: Google Frontend
content-length: 0
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/documents/

Identification

OUTPUT

```
The following header information disclosures have been detected on https://juice-shop-388277804329.us-west1.run.app
/documents/:

- Server: Google Frontend
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/documents/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 00:48:33 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=8659790f61386a0d355111f26ee2a386
```

```
Content-Length=3149
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/soap/

Identification

OUTPUT

```
The following header information disclosures have been detected on https://juice-shop-388277804329.us-west1.run.app
/soap/:

- Server: Google Frontend
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/soap/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 01:24:49 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=00c8cab83d92eca2ba95785b966a73c5
Content-Length=4201
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/soap/nusoap.php

Identification

OUTPUT

```
The following header information disclosures have been detected on https://juice-shop-388277804329.us-west1.run.app/soap
/nusoap.php:

- X-Powered-By: PHP/5.5.9-1ubuntu4.14
- Server: Google Frontend
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/soap/nusoap.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type=text/html
Date=Tue, 19 Nov 2024 07:07:36 GMT
Server=Google Frontend
X-Cloud-Trace-Context=9b95efa061e2e33130bff09373a821c4
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=811
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/apps/

Identification

OUTPUT

```
The following header information disclosures have been detected on https://juice-shop-388277804329.us-west1.run.app
/apps/:

- Server: Google Frontend
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/apps/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

```
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 00:30:17 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=b57b66949c25563ad77a69e4a354af47
Content-Length=1782
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/training_install.php

Identification

OUTPUT

```
The following header information disclosures have been detected on https://juice-shop-388277804329.us-west1.run.app
/training_install.php:

- X-Powered-By: PHP/5.5.9-1ubuntu4.14
- Server: Google Frontend
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/training_install.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 02:31:16 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=dc248926d66de31d4ae1d4212ab637d0
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4629
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/

Identification

OUTPUT

```
The following header information disclosures have been detected on https://juice-shop-388277804329.us-west1.run.app/:
```

```
- X-Powered-By: PHP/5.5.9-1ubuntu4.14
- Server: Google Frontend
```

HTTP Info

REQUEST MADE

```
GET / HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 302
x-powered-by: PHP/5.5.9-1ubuntu4.14
location: portal.php
content-type: text/html
x-cloud-trace-context: 007e090dd352049025be74deb6b4d016
date: Tue, 19 Nov 2024 03:14:32 GMT
server: Google Frontend
content-length: 0
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/soap/class.wsdlcache.php

Identification

OUTPUT

```
The following header information disclosures have been detected on https://juice-shop-388277804329.us-west1.run.app/soap
/class.wsdlcache.php:

- X-Powered-By: PHP/5.5.9-1ubuntu4.14
- Server: Google Frontend
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/soap/class.wsdlcache.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type=text/html
Date=Tue, 19 Nov 2024 06:59:07 GMT
Server=Google Frontend
X-Cloud-Trace-Context=7cb98e8601bf9fb1d2977a54ea93f5f7
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=811
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/passwords/heroes.xml

Identification

OUTPUT

```
The following header information disclosures have been detected on https://juice-shop-388277804329.us-west1.run.app
/passwords/heroes.xml:

- Server: Google Frontend
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/passwords/heroes.xml
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
H3 200
Accept-Ranges=bytes
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=application/xml
Date=Tue, 19 Nov 2024 06:00:20 GMT
Etag="4b8-626c1e84a7000-gzip"
Last-Modified=Wed, 13 Nov 2024 02:15:28 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=d0db3cb698fff35d3398f6d368ed869f
Content-Length=433
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/db/bwapp.sqlite

Identification

OUTPUT

```
The following header information disclosures have been detected on https://juice-shop-388277804329.us-west1.run.app/db
/bwapp.sqlite:

- Server: Google Frontend
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/db/bwapp.sqlite
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Accept-Ranges=bytes
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type=text/html
Date=Tue, 19 Nov 2024 03:57:01 GMT
Etag="3000-626c1e84a7000"
Last-Modified=Wed, 13 Nov 2024 02:15:28 GMT
Server=Google Frontend
X-Cloud-Trace-Context=2a74d2d814c14512fd8fac93e4bfc679
Content-Length=12288
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/js/

Identification

OUTPUT

```
The following header information disclosures have been detected on https://juice-shop-388277804329.us-west1.run.app/js/:

- Server: Google Frontend
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/js/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
```

```
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 01:06:45 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=92dbc4630193c57aa70de731a23c4521
Content-Length=2393
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/passwords/

Identification

OUTPUT

```
The following header information disclosures have been detected on https://juice-shop-388277804329.us-west1.run.app
/passwords/:

- Server: Google Frontend
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/passwords/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 01:15:47 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=23cbd446a1bfac87a66163e22db42b14
Content-Length=2204
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/login.php

Identification

OUTPUT

```
The following header information disclosures have been detected on https://juice-shop-388277804329.us-west1.run.app
/login.php:

- X-Powered-By: PHP/5.5.9-1ubuntu4.14
- Server: Google Frontend
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/login.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control=no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 01:51:06 GMT
Expires=Thu, 19 Nov 1981 08:52:00 GMT
Pragma=no-cache
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=97249a7d3363c12f26d1d625a5fdf4df
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4826
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/passwords/wp-config.bak

Identification

OUTPUT

```
The following header information disclosures have been detected on https://juice-shop-388277804329.us-west1.run.app
/passwords/wp-config.bak:

- Server: Google Frontend
```

HTTP Info

REQUEST MADE

```
GET /passwords/wp-config.bak HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 200
last-modified: Wed, 13 Nov 2024 02:15:28 GMT
etag: "603-626c1e84a7000"
accept-ranges: bytes
content-type: application/x-trash
x-cloud-trace-context: bccbdb7c061d2d5009d67b2ae3eb5bac
date: Tue, 19 Nov 2024 06:12:37 GMT
server: Google Frontend
content-length: 1539
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

Missing 'X-Content-Type-Options' Header

VULNERABILITY LOW PLUGIN ID 112529

Description

The HTTP 'X-Content-Type-Options' response header prevents the browser from MIME-sniffing a response away from the declared content-type.

The server did not return a correct 'X-Content-Type-Options' header, which means that this website could be at risk of a Cross-Site Scripting (XSS) attack.

Solution

Configure your web server to include an 'X-Content-Type-Options' header with a value of 'nosniff'.

See Also

https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options
https://www.owasp.org/index.php/OWASP_Secure_Headers_Project#xcto

Plugin Details

PUBLICATION DATE	2018-11-28T00:00:00+00:00
MODIFICATION DATE	2024-03-25T00:00:00+00:00
FAMILY	HTTP Security Header
SEVERITY	Low
PLUGIN ID	112529

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	3.1
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N
CVSS BASE SCORE	2.6
CVSS VECTOR	CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N

Reference Information

CWE	693
WASC	Application Misconfiguration
OWASP	2017-A6, 2013-A5, 2010-A6, 2023-API8, 2019-API7
CVE	-
BID	-

Missing 'X-Content-Type-Options' Header Instances (25)

VULNERABILITY LOW PLUGIN ID 112529

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/training_install.php

Identification

OUTPUT

```
The scanner detected the lack of a correct X-Content-Type-Options header configuration in the target application
response
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/training_install.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 02:31:16 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=dc248926d66de31d4ae1d4212ab637d0
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4629
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/images/

Identification

OUTPUT

```
The scanner detected the lack of a correct X-Content-Type-Options header configuration in the target application
response
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/images/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 00:57:42 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=fc3fee9e75c9304bb77fd657cb75393d
Content-Length=5991
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/passwords/

Identification

OUTPUT

```
The scanner detected the lack of a correct X-Content-Type-Options header configuration in the target application
response
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/passwords/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
```

```
Date=Tue, 19 Nov 2024 01:15:47 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=23cbd446a1bfac87a66163e22db42b14
Content-Length=2204
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/info.php

Identification

OUTPUT

```
The scanner detected the lack of a correct X-Content-Type-Options header configuration in the target application
response
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/info.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 08:28:20 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=d1dec854dbe62de69a7b5ea639baba79
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4239
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/documents/

Identification

OUTPUT

```
The scanner detected the lack of a correct X-Content-Type-Options header configuration in the target application
response
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/documents/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 00:48:33 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=8659790f61386a0d355111f26ee2a386
Content-Length=3149
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/info_install.php

Identification

OUTPUT

```
The scanner detected the lack of a correct X-Content-Type-Options header configuration in the target application
response
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/info_install.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Arch=""
Sec-Ch-Ua-Bitness=""
Sec-Ch-Ua-Full-Version-List="Chromium", "HeadlessChrome", "Not-A.Brand";v="99.0.0.0"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Model=""
Sec-Ch-Ua-Platform="Linux"
Sec-Ch-Ua-Platform-Version=""
Sec-Ch-Ua-Wow64=?0
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
```

```
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 02:21:07 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=3305fabc85563bee1adce5fca1986cef
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4188
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/login.php

Identification

OUTPUT

```
The scanner detected the lack of a correct X-Content-Type-Options header configuration in the target application
response
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/login.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control=no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 01:51:06 GMT
Expires=Thu, 19 Nov 1981 08:52:00 GMT
Pragma=no-cache
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=97249a7d3363c12f26d1d625a5fdf4df
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4826
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/phpinfo.php

Identification

OUTPUT

```
The scanner detected the lack of a correct X-Content-Type-Options header configuration in the target application
response
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/phpinfo.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 01:43:29 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=036c4d5909306dec6b8d0193b59d617a
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=85702
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/apps/movie_search

Identification

OUTPUT

```
The scanner detected the lack of a correct X-Content-Type-Options header configuration in the target application
response
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/apps/movie_search
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
```

```
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Arch=""
Sec-Ch-Ua-Bitness=""
Sec-Ch-Ua-Full-Version-List="Chromium", "HeadlessChrome", "Not-A.Brand";v="99.0.0.0"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Model=""
Sec-Ch-Ua-Platform="Linux"
Sec-Ch-Ua-Platform-Version=""
Sec-Ch-Ua-Wow64=?0
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Accept-Ranges=bytes
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type=text/html
Date=Tue, 19 Nov 2024 03:18:44 GMT
Etag="d9a7-626c1e84a7000"
Last-Modified=Wed, 13 Nov 2024 02:15:28 GMT
Server=Google Frontend
X-Cloud-Trace-Context=4a149f49b940643dfb9c9bcafe0604bb
Content-Length=55719
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/soap/class.nusoap_base.php

Identification

OUTPUT

```
The scanner detected the lack of a correct X-Content-Type-Options header configuration in the target application
response
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/soap/class.nusoap_base.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type=text/html
Date=Tue, 19 Nov 2024 06:46:36 GMT
Server=Google Frontend
```

```
X-Cloud-Trace-Context=c53cd0b0ef8c298766ed3c1bd61168b7
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=811
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/soap/class.wsdlcache.php

Identification

OUTPUT

```
The scanner detected the lack of a correct X-Content-Type-Options header configuration in the target application
response
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/soap/class.wsdlcache.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type=text/html
Date=Tue, 19 Nov 2024 06:59:07 GMT
Server=Google Frontend
X-Cloud-Trace-Context=7cb98e8601bf9fb1d2977a54ea93f5f7
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=811
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/stylesheets/

Identification

OUTPUT

```
The scanner detected the lack of a correct X-Content-Type-Options header configuration in the target application
response
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/stylesheets/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 01:34:22 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=91660b485a30bbed64793dbe904193d3
Content-Length=2275
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/db/bwapp.sqlite

Identification

OUTPUT

```
The scanner detected the lack of a correct X-Content-Type-Options header configuration in the target application
response
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/db/bwapp.sqlite
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Accept-Ranges=bytes
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type=text/html
Date=Tue, 19 Nov 2024 03:57:01 GMT
Etag="3000-626c1e84a7000"
```

```
Last-Modified=Wed, 13 Nov 2024 02:15:28 GMT
Server=Google Frontend
X-Cloud-Trace-Context=2a74d2d814c14512fd8fac93e4bfc679
Content-Length=12288
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/apps/

Identification

OUTPUT

```
The scanner detected the lack of a correct X-Content-Type-Options header configuration in the target application
response
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/apps/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 00:30:17 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=b57b66949c25563ad77a69e4a354af47
Content-Length=1782
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/training.php

Identification

OUTPUT

```
The scanner detected the lack of a correct X-Content-Type-Options header configuration in the target application
response
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/training.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 08:36:37 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=beee281846f3b9b9397b531ce1a92fef
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4656
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/soap/

Identification

OUTPUT

```
The scanner detected the lack of a correct X-Content-Type-Options header configuration in the target application
response
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/soap/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 01:24:49 GMT
```

```
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=00c8cab83d92eca2ba95785b966a73c5
Content-Length=4201
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/soap/class.soap_fault.php

Identification

OUTPUT

```
The scanner detected the lack of a correct X-Content-Type-Options header configuration in the target application
response
```

HTTP Info

REQUEST MADE

```
GET /soap/class.soap_fault.php HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 500
x-powered-by: PHP/5.5.9-1ubuntu4.14
content-type: text/html
x-cloud-trace-context: 85c8d444051c598a5636d47e2436b1d1
date: Tue, 19 Nov 2024 06:54:58 GMT
server: Google Frontend
content-length: 0
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/passwords/wp-config.bak

Identification

OUTPUT

```
The scanner detected the lack of a correct X-Content-Type-Options header configuration in the target application
response
```

HTTP Info

REQUEST MADE

```
GET /passwords/wp-config.bak HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 200
last-modified: Wed, 13 Nov 2024 02:15:28 GMT
etag: "603-626c1e84a7000"
accept-ranges: bytes
content-type: application/x-trash
x-cloud-trace-context: bccbdb7c061d2d5009d67b2ae3eb5bac
date: Tue, 19 Nov 2024 06:12:37 GMT
server: Google Frontend
content-length: 1539
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/soap/nusoap.php

Identification

OUTPUT

```
The scanner detected the lack of a correct X-Content-Type-Options header configuration in the target application
response
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/soap/nusoap.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type=text/html
Date=Tue, 19 Nov 2024 07:07:36 GMT
Server=Google Frontend
X-Cloud-Trace-Context=9b95efa061e2e33130bff09373a821c4
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=811
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/db/

Identification

OUTPUT

```
The scanner detected the lack of a correct X-Content-Type-Options header configuration in the target application
response
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/db/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 00:39:25 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=7330f8397d6d6ed7b0975d370f2d06ee
Content-Length=1778
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/install.php

Identification

OUTPUT

```
The scanner detected the lack of a correct X-Content-Type-Options header configuration in the target application
response
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/install.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Arch=""
Sec-Ch-Ua-Bitness=""
Sec-Ch-Ua-Full-Version-List="Chromium", "HeadlessChrome", "Not-A.Brand";v="99.0.0.0"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Model=""
Sec-Ch-Ua-Platform="Linux"
Sec-Ch-Ua-Platform-Version=""
Sec-Ch-Ua-Wow64=?0
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
```

```
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 00:19:04 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=793633ff205741c27021c36f1f4362a8
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=3083
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/passwords/web.config.bak

Identification

OUTPUT

```
The scanner detected the lack of a correct X-Content-Type-Options header configuration in the target application
response
```

HTTP Info

REQUEST MADE

```
GET /passwords/web.config.bak HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 200
last-modified: Wed, 13 Nov 2024 02:15:28 GMT
etag: "1d84-626c1e84a7000"
accept-ranges: bytes
content-type: application/x-trash
x-cloud-trace-context: dd8a0753fe21b8d0d381c2313f0202d5
date: Tue, 19 Nov 2024 06:08:24 GMT
server: Google Frontend
content-length: 7556
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/user_new.php

Identification

OUTPUT

```
The scanner detected the lack of a correct X-Content-Type-Options header configuration in the target application
response
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/user_new.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 07:45:52 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=1de28a3c31c89c397b35ab9cf352eeaf
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4224
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/passwords/heroes.xml

Identification

OUTPUT

```
The scanner detected the lack of a correct X-Content-Type-Options header configuration in the target application
response
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/passwords/heroes.xml
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
H3 200
Accept-Ranges=bytes
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=application/xml
Date=Tue, 19 Nov 2024 06:00:20 GMT
Etag="4b8-626c1e84a7000-gzip"
Last-Modified=Wed, 13 Nov 2024 02:15:28 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=d0db3cb698fff35d3398f6d368ed869f
Content-Length=433
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/js/

Identification

OUTPUT

```
The scanner detected the lack of a correct X-Content-Type-Options header configuration in the target application
response
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/js/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 01:06:45 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=92dbc4630193c57aa70de731a23c4521
Content-Length=2393
```

SSL/TLS Weak Cipher Suites Supported

VULNERABILITY LOW PLUGIN ID 112539

Description

The remote host supports the use of SSL/TLS ciphers that offer weak encryption (including RC4 and 3DES encryption).

Solution

Reconfigure the affected application, if possible to avoid the use of weak ciphers.

See Also

https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml

Plugin Details

PUBLICATION DATE	2019-01-21T00:00:00+00:00
MODIFICATION DATE	2022-10-07T00:00:00+00:00
FAMILY	SSL/TLS
SEVERITY	Low
PLUGIN ID	112539

Risk Information

CVSSV4 BASE SCORE	2.3
CVSSV4 VECTOR	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N
CVSSV3 BASE SCORE	3.7
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N
CVSS BASE SCORE	2.6
CVSS VECTOR	CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N

Reference Information

CWE	326
WASC	Application Misconfiguration
OWASP	2010-A7, 2013-A6, 2017-A3, 2021-A2, 2023-API8, 2019-API7
CVE	-
BID	-

SSL/TLS Weak Cipher Suites Supported Instances (1)

VULNERABILITY LOW PLUGIN ID 112539

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/#/

Identification

OUTPUT

```
Protocol Cipher Suite Name (RFC) Key Exchange Strength
--------------------------------------------------------------------------
TLS1.2 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA x25519 256
TLS1.2 TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA x25519 256
TLS1.2 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA x25519 256
TLS1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA x25519 256
TLS1.2 TLS_RSA_WITH_AES_128_GCM_SHA256 RSA 4096
TLS1.2 TLS_RSA_WITH_AES_256_GCM_SHA384 RSA 4096
TLS1.2 TLS_RSA_WITH_AES_128_CBC_SHA RSA 4096
TLS1.2 TLS_RSA_WITH_AES_256_CBC_SHA RSA 4096
```

Missing Content Security Policy

VULNERABILITY LOW PLUGIN ID 112551

Description

Content Security Policy (CSP) is a web security standard that helps to mitigate attacks like cross-site scripting (XSS), clickjacking or mixed content issues. CSP provides mechanisms to websites to restrict content that browsers will be allowed to load.

No CSP header has been detected on this host. This URL is flagged as a specific example.

Solution

Configure Content Security Policy on your website by adding 'Content-Security-Policy' HTTP header or meta tag http-equiv='Content-Security-Policy'.

See Also

https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP
https://csp-evaluator.withgoogle.com/
https://content-security-policy.com/
https://developers.google.com/web/fundamentals/security/csp/
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy

Plugin Details

PUBLICATION DATE	2019-02-14T00:00:00+00:00
MODIFICATION DATE	2024-03-25T00:00:00+00:00
FAMILY	HTTP Security Header
SEVERITY	Low
PLUGIN ID	112551

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	3.1
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N
CVSS BASE SCORE	2.6
CVSS VECTOR	CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N

Reference Information

CWE	1021
WASC	Application Misconfiguration
OWASP	2017-A6, 2021-A4, 2013-A5, 2010-A6, 2023-API8, 2019-API7
CVE	-

BID	-

Missing Content Security Policy Instances (22)

VULNERABILITY LOW PLUGIN ID 112551

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/info.php

Identification

OUTPUT

```
https://juice-shop-388277804329.us-west1.run.app/info.php has no Content Security Policy defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/info.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 08:28:20 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=d1dec854dbe62de69a7b5ea639baba79
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4239
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/passwords/

Identification

OUTPUT

```
https://juice-shop-388277804329.us-west1.run.app/passwords/ has no Content Security Policy defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/passwords/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 01:15:47 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=23cbd446a1bfac87a66163e22db42b14
Content-Length=2204
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/phpinfo.php

Identification

OUTPUT

```
https://juice-shop-388277804329.us-west1.run.app/phpinfo.php has no Content Security Policy defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/phpinfo.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 01:43:29 GMT
Server=Google Frontend
Vary=Accept-Encoding
```

```
X-Cloud-Trace-Context=036c4d5909306dec6b8d0193b59d617a
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=85702
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/stylesheets/

Identification

OUTPUT

```
https://juice-shop-388277804329.us-west1.run.app/stylesheets/ has no Content Security Policy defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/stylesheets/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 01:34:22 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=91660b485a30bbed64793dbe904193d3
Content-Length=2275
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/db/bwapp.sqlite

Identification

OUTPUT

```
https://juice-shop-388277804329.us-west1.run.app/db/bwapp.sqlite has no Content Security Policy defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/db/bwapp.sqlite
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Accept-Ranges=bytes
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type=text/html
Date=Tue, 19 Nov 2024 03:57:01 GMT
Etag="3000-626c1e84a7000"
Last-Modified=Wed, 13 Nov 2024 02:15:28 GMT
Server=Google Frontend
X-Cloud-Trace-Context=2a74d2d814c14512fd8fac93e4bfc679
Content-Length=12288
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/images/

Identification

OUTPUT

```
https://juice-shop-388277804329.us-west1.run.app/images/ has no Content Security Policy defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/images/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 00:57:42 GMT
Server=Google Frontend
Vary=Accept-Encoding
```

```
X-Cloud-Trace-Context=fc3fee9e75c9304bb77fd657cb75393d
Content-Length=5991
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/soap/class.nusoap_base.php

Identification

OUTPUT

```
https://juice-shop-388277804329.us-west1.run.app/soap/class.nusoap_base.php has no Content Security Policy defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/soap/class.nusoap_base.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type=text/html
Date=Tue, 19 Nov 2024 06:46:36 GMT
Server=Google Frontend
X-Cloud-Trace-Context=c53cd0b0ef8c298766ed3c1bd61168b7
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=811
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/soap/class.soap_fault.php

Identification

OUTPUT

```
https://juice-shop-388277804329.us-west1.run.app/soap/class.soap_fault.php has no Content Security Policy defined.
```

HTTP Info

REQUEST MADE

```
GET /soap/class.soap_fault.php HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
```

```
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 500
x-powered-by: PHP/5.5.9-1ubuntu4.14
content-type: text/html
x-cloud-trace-context: 85c8d444051c598a5636d47e2436b1d1
date: Tue, 19 Nov 2024 06:54:58 GMT
server: Google Frontend
content-length: 0
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/apps/

Identification

OUTPUT

```
https://juice-shop-388277804329.us-west1.run.app/apps/ has no Content Security Policy defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/apps/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 00:30:17 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=b57b66949c25563ad77a69e4a354af47
Content-Length=1782
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/user_new.php

Identification

OUTPUT

```
https://juice-shop-388277804329.us-west1.run.app/user_new.php has no Content Security Policy defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/user_new.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 07:45:52 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=1de28a3c31c89c397b35ab9cf352eeaf
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4224
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/install.php

Identification

OUTPUT

```
https://juice-shop-388277804329.us-west1.run.app/install.php has no Content Security Policy defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/install.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Arch=""
Sec-Ch-Ua-Bitness=""
Sec-Ch-Ua-Full-Version-List="Chromium", "HeadlessChrome", "Not-A.Brand";v="99.0.0.0"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Model=""
Sec-Ch-Ua-Platform="Linux"
```

```
Sec-Ch-Ua-Platform-Version=""
Sec-Ch-Ua-Wow64=?0
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 00:19:04 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=793633ff205741c27021c36f1f4362a8
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=3083
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/documents/

Identification

OUTPUT

```
https://juice-shop-388277804329.us-west1.run.app/documents/ has no Content Security Policy defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/documents/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 00:48:33 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=8659790f61386a0d355111f26ee2a386
Content-Length=3149
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/login.php

Identification

OUTPUT

```
https://juice-shop-388277804329.us-west1.run.app/login.php has no Content Security Policy defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/login.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control=no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 01:51:06 GMT
Expires=Thu, 19 Nov 1981 08:52:00 GMT
Pragma=no-cache
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=97249a7d3363c12f26d1d625a5fdf4df
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4826
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/soap/

Identification

OUTPUT

```
https://juice-shop-388277804329.us-west1.run.app/soap/ has no Content Security Policy defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/soap/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

```
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 01:24:49 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=00c8cab83d92eca2ba95785b966a73c5
Content-Length=4201
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/soap/nusoap.php

Identification

OUTPUT

```
https://juice-shop-388277804329.us-west1.run.app/soap/nusoap.php has no Content Security Policy defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/soap/nusoap.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type=text/html
Date=Tue, 19 Nov 2024 07:07:36 GMT
Server=Google Frontend
X-Cloud-Trace-Context=9b95efa061e2e33130bff09373a821c4
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=811
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/js/

Identification

OUTPUT

```
https://juice-shop-388277804329.us-west1.run.app/js/ has no Content Security Policy defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/js/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 01:06:45 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=92dbc4630193c57aa70de731a23c4521
Content-Length=2393
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/apps/movie_search

Identification

OUTPUT

```
https://juice-shop-388277804329.us-west1.run.app/apps/movie_search has no Content Security Policy defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/apps/movie_search
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Arch=""
Sec-Ch-Ua-Bitness=""
```

```
Sec-Ch-Ua-Full-Version-List="Chromium", "HeadlessChrome", "Not-A.Brand";v="99.0.0.0"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Model=""
Sec-Ch-Ua-Platform="Linux"
Sec-Ch-Ua-Platform-Version=""
Sec-Ch-Ua-Wow64=?0
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Accept-Ranges=bytes
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type=text/html
Date=Tue, 19 Nov 2024 03:18:44 GMT
Etag="d9a7-626c1e84a7000"
Last-Modified=Wed, 13 Nov 2024 02:15:28 GMT
Server=Google Frontend
X-Cloud-Trace-Context=4a149f49b940643dfb9c9bcafe0604bb
Content-Length=55719
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/db/

Identification

OUTPUT

```
https://juice-shop-388277804329.us-west1.run.app/db/ has no Content Security Policy defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/db/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 00:39:25 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=7330f8397d6d6ed7b0975d370f2d06ee
```

```
Content-Length=1778
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/soap/class.wsdlcache.php

Identification

OUTPUT

```
https://juice-shop-388277804329.us-west1.run.app/soap/class.wsdlcache.php has no Content Security Policy defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/soap/class.wsdlcache.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type=text/html
Date=Tue, 19 Nov 2024 06:59:07 GMT
Server=Google Frontend
X-Cloud-Trace-Context=7cb98e8601bf9fb1d2977a54ea93f5f7
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=811
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/training.php

Identification

OUTPUT

```
https://juice-shop-388277804329.us-west1.run.app/training.php has no Content Security Policy defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/training.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
```

```
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 08:36:37 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=beee281846f3b9b9397b531ce1a92fef
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4656
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/info_install.php

Identification

OUTPUT

```
https://juice-shop-388277804329.us-west1.run.app/info_install.php has no Content Security Policy defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/info_install.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Arch=""
Sec-Ch-Ua-Bitness=""
Sec-Ch-Ua-Full-Version-List="Chromium", "HeadlessChrome", "Not-A.Brand";v="99.0.0.0"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Model=""
Sec-Ch-Ua-Platform="Linux"
Sec-Ch-Ua-Platform-Version=""
Sec-Ch-Ua-Wow64=?0
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
```

```
Date=Tue, 19 Nov 2024 02:21:07 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=3305fabc85563bee1adce5fca1986cef
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4188
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/training_install.php

Identification

OUTPUT

```
https://juice-shop-388277804329.us-west1.run.app/training_install.php has no Content Security Policy defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/training_install.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 02:31:16 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=dc248926d66de31d4ae1d4212ab637d0
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4629
```

Missing 'Cache-Control' Header

VULNERABILITY LOW PLUGIN ID 112553

Description

The HTTP 'Cache-Control' header is used to specify directives for caching mechanisms.

The server did not return or returned an invalid 'Cache-Control' header which means page containing sensitive information (password, credit card, personal data, social security number, etc) could be stored on client side disk and then be exposed to unauthorised persons. This URL is flagged as a specific example.

Solution

Configure your web server to include a 'Cache-Control' header with appropriate directives. If page contains sensitive information 'Cache-Control' value should be 'no-store' and 'Pragma' header value should be 'no-cache'.

See Also

https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control

https://www.owasp.org/index.php/Testing_for_Browser_cache_weakness_(OTG-AUTHN-006)

Plugin Details

PUBLICATION DATE	2019-02-15T00:00:00+00:00
MODIFICATION DATE	2024-03-25T00:00:00+00:00
FAMILY	HTTP Security Header
SEVERITY	Low
PLUGIN ID	112553

Risk Information

CVSSV4 BASE SCORE	2.1
CVSSV4 VECTOR	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:A/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N
CVSSV3 BASE SCORE	3.7
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N
CVSS BASE SCORE	2.6
CVSS VECTOR	CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N

Reference Information

CWE	525
WASC	Application Misconfiguration
OWASP	2017-A6, 2021-A4, 2013-A5, 2010-A6, 2023-API8, 2019-API7
CVE	-
BID	-

Missing 'Cache-Control' Header Instances (25)

VULNERABILITY LOW PLUGIN ID 112553

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/apps/

Identification

OUTPUT

```
https://juice-shop-388277804329.us-west1.run.app/apps/ has no Cache Control header defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/apps/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 00:30:17 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=b57b66949c25563ad77a69e4a354af47
Content-Length=1782
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/passwords/heroes.xml

Identification

OUTPUT

```
https://juice-shop-388277804329.us-west1.run.app/passwords/heroes.xml has no Cache Control header defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/passwords/heroes.xml
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
H3 200
Accept-Ranges=bytes
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=application/xml
Date=Tue, 19 Nov 2024 06:00:20 GMT
Etag="4b8-626c1e84a7000-gzip"
Last-Modified=Wed, 13 Nov 2024 02:15:28 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=d0db3cb698fff35d3398f6d368ed869f
Content-Length=433
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/login.php

Identification

OUTPUT

```
https://juice-shop-388277804329.us-west1.run.app/login.php has invalid directive found :
- post-check=0
https://juice-shop-388277804329.us-west1.run.app/login.php has invalid directive found :
- pre-check=0
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/login.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

```
Cache-Control=no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 01:51:06 GMT
Expires=Thu, 19 Nov 1981 08:52:00 GMT
Pragma=no-cache
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=97249a7d3363c12f26d1d625a5fdf4df
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4826
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/soap/

Identification

OUTPUT

```
https://juice-shop-388277804329.us-west1.run.app/soap/ has no Cache Control header defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/soap/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 01:24:49 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=00c8cab83d92eca2ba95785b966a73c5
Content-Length=4201
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/passwords/web.config.bak

Identification

OUTPUT

```
https://juice-shop-388277804329.us-west1.run.app/passwords/web.config.bak has no Cache Control header defined.
```

HTTP Info

REQUEST MADE

```
GET /passwords/web.config.bak HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 200
last-modified: Wed, 13 Nov 2024 02:15:28 GMT
etag: "1d84-626c1e84a7000"
accept-ranges: bytes
content-type: application/x-trash
x-cloud-trace-context: dd8a0753fe21b8d0d381c2313f0202d5
date: Tue, 19 Nov 2024 06:08:24 GMT
server: Google Frontend
content-length: 7556
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/db/bwapp.sqlite

Identification

OUTPUT

```
https://juice-shop-388277804329.us-west1.run.app/db/bwapp.sqlite has no Cache Control header defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/db/bwapp.sqlite
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Accept-Ranges=bytes
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type=text/html
Date=Tue, 19 Nov 2024 03:57:01 GMT
Etag="3000-626c1e84a7000"
Last-Modified=Wed, 13 Nov 2024 02:15:28 GMT
Server=Google Frontend
```

```
X-Cloud-Trace-Context=2a74d2d814c14512fd8fac93e4bfc679
Content-Length=12288
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/soap/nusoap.php

Identification

OUTPUT

```
https://juice-shop-388277804329.us-west1.run.app/soap/nusoap.php has no Cache Control header defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/soap/nusoap.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type=text/html
Date=Tue, 19 Nov 2024 07:07:36 GMT
Server=Google Frontend
X-Cloud-Trace-Context=9b95efa061e2e33130bff09373a821c4
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=811
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/documents/

Identification

OUTPUT

```
https://juice-shop-388277804329.us-west1.run.app/documents/ has no Cache Control header defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/documents/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
```

```
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 00:48:33 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=8659790f61386a0d355111f26ee2a386
Content-Length=3149
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/install.php

Identification

OUTPUT

```
https://juice-shop-388277804329.us-west1.run.app/install.php has no Cache Control header defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/install.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Arch=""
Sec-Ch-Ua-Bitness=""
Sec-Ch-Ua-Full-Version-List="Chromium", "HeadlessChrome", "Not-A.Brand";v="99.0.0.0"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Model=""
Sec-Ch-Ua-Platform="Linux"
Sec-Ch-Ua-Platform-Version=""
Sec-Ch-Ua-Wow64=?0
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
```

```
Date=Tue, 19 Nov 2024 00:19:04 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=793633ff205741c27021c36f1f4362a8
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=3083
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/soap/class.nusoap_base.php

Identification

OUTPUT

```
https://juice-shop-388277804329.us-west1.run.app/soap/class.nusoap_base.php has no Cache Control header defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/soap/class.nusoap_base.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type=text/html
Date=Tue, 19 Nov 2024 06:46:36 GMT
Server=Google Frontend
X-Cloud-Trace-Context=c53cd0b0ef8c298766ed3c1bd61168b7
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=811
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/images/

Identification

OUTPUT

```
https://juice-shop-388277804329.us-west1.run.app/images/ has no Cache Control header defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/images/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 00:57:42 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=fc3fee9e75c9304bb77fd657cb75393d
Content-Length=5991
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/passwords/

Identification

OUTPUT

```
https://juice-shop-388277804329.us-west1.run.app/passwords/ has no Cache Control header defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/passwords/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 01:15:47 GMT
Server=Google Frontend
Vary=Accept-Encoding
```

```
X-Cloud-Trace-Context=23cbd446a1bfac87a66163e22db42b14
Content-Length=2204
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/info.php

Identification

OUTPUT

```
https://juice-shop-388277804329.us-west1.run.app/info.php has no Cache Control header defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/info.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 08:28:20 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=d1dec854dbe62de69a7b5ea639baba79
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4239
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/training_install.php

Identification

OUTPUT

```
https://juice-shop-388277804329.us-west1.run.app/training_install.php has no Cache Control header defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/training_install.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 02:31:16 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=dc248926d66de31d4ae1d4212ab637d0
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4629
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/phpinfo.php

Identification

OUTPUT

```
https://juice-shop-388277804329.us-west1.run.app/phpinfo.php has no Cache Control header defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/phpinfo.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 01:43:29 GMT
Server=Google Frontend
Vary=Accept-Encoding
```

```
X-Cloud-Trace-Context=036c4d5909306dec6b8d0193b59d617a
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=85702
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/user_new.php

Identification

OUTPUT

```
https://juice-shop-388277804329.us-west1.run.app/user_new.php has no Cache Control header defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/user_new.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 07:45:52 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=1de28a3c31c89c397b35ab9cf352eeaf
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4224
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/apps/movie_search

Identification

OUTPUT

```
https://juice-shop-388277804329.us-west1.run.app/apps/movie_search has no Cache Control header defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/apps/movie_search
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Arch=""
Sec-Ch-Ua-Bitness=""
Sec-Ch-Ua-Full-Version-List="Chromium", "HeadlessChrome", "Not-A.Brand";v="99.0.0.0"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Model=""
Sec-Ch-Ua-Platform="Linux"
Sec-Ch-Ua-Platform-Version=""
Sec-Ch-Ua-Wow64=?0
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Accept-Ranges=bytes
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type=text/html
Date=Tue, 19 Nov 2024 03:18:44 GMT
Etag="d9a7-626c1e84a7000"
Last-Modified=Wed, 13 Nov 2024 02:15:28 GMT
Server=Google Frontend
X-Cloud-Trace-Context=4a149f49b940643dfb9c9bcafe0604bb
Content-Length=55719
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/js/

Identification

OUTPUT

```
https://juice-shop-388277804329.us-west1.run.app/js/ has no Cache Control header defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/js/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 01:06:45 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=92dbc4630193c57aa70de731a23c4521
Content-Length=2393
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/soap/class.soap_fault.php

Identification

OUTPUT

```
https://juice-shop-388277804329.us-west1.run.app/soap/class.soap_fault.php has no Cache Control header defined.
```

HTTP Info

REQUEST MADE

```
GET /soap/class.soap_fault.php HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 500
x-powered-by: PHP/5.5.9-1ubuntu4.14
content-type: text/html
x-cloud-trace-context: 85c8d444051c598a5636d47e2436b1d1
date: Tue, 19 Nov 2024 06:54:58 GMT
server: Google Frontend
content-length: 0
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/stylesheets/

Identification

OUTPUT

```
https://juice-shop-388277804329.us-west1.run.app/stylesheets/ has no Cache Control header defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/stylesheets/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
```

```
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 01:34:22 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=91660b485a30bbed64793dbe904193d3
Content-Length=2275
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/db/

Identification

OUTPUT

```
https://juice-shop-388277804329.us-west1.run.app/db/ has no Cache Control header defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/db/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 00:39:25 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=7330f8397d6d6ed7b0975d370f2d06ee
Content-Length=1778
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/info_install.php

Identification

OUTPUT

```
https://juice-shop-388277804329.us-west1.run.app/info_install.php has no Cache Control header defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/info_install.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Arch=""
Sec-Ch-Ua-Bitness=""
Sec-Ch-Ua-Full-Version-List="Chromium", "HeadlessChrome", "Not-A.Brand";v="99.0.0.0"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Model=""
Sec-Ch-Ua-Platform="Linux"
Sec-Ch-Ua-Platform-Version=""
Sec-Ch-Ua-Wow64=?0
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 02:21:07 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=3305fabc85563bee1adce5fca1986cef
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4188
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/passwords/wp-config.bak

Identification

OUTPUT

```
https://juice-shop-388277804329.us-west1.run.app/passwords/wp-config.bak has no Cache Control header defined.
```

HTTP Info

REQUEST MADE

```
GET /passwords/wp-config.bak HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 200
last-modified: Wed, 13 Nov 2024 02:15:28 GMT
etag: "603-626c1e84a7000"
accept-ranges: bytes
content-type: application/x-trash
x-cloud-trace-context: bccbdb7c061d2d5009d67b2ae3eb5bac
date: Tue, 19 Nov 2024 06:12:37 GMT
server: Google Frontend
content-length: 1539
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/training.php

Identification

OUTPUT

```
https://juice-shop-388277804329.us-west1.run.app/training.php has no Cache Control header defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/training.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 08:36:37 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=beee281846f3b9b9397b531ce1a92fef
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4656
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/soap/class.wsdlcache.php

Identification

OUTPUT

```
https://juice-shop-388277804329.us-west1.run.app/soap/class.wsdlcache.php has no Cache Control header defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/soap/class.wsdlcache.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type=text/html
Date=Tue, 19 Nov 2024 06:59:07 GMT
Server=Google Frontend
X-Cloud-Trace-Context=7cb98e8601bf9fb1d2977a54ea93f5f7
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=811
```

Login Form Cross-Site Request Forgery

VULNERABILITY LOW PLUGIN ID 113332

Description

Cross Site Request Forgery (CSRF) occurs when an user is tricked into clicking on a link which would automatically submit a request without the user's consent.

This can be made possible when the request does not include an anti-CSRF token, generated each time the request is visited and passed when the request is submitted, and which can be used by the web application backend to verify that the request originates from a legitimate user.

Exploiting requests vulnerable to Cross-Site Request Forgery requires different factors:

- The request must perform a sensitive action.

- The attacker must make the victim click on a link to send the request without their consent.

The exploitation of this vulnerability will in most cases have a very limited impact. However, it is possible to create complex scenarios in case the application is also vulnerable to Cross-Site Scripting.

Solution

Update the application by adding support of anti-CSRF tokens on this login form.
Most web frameworks provide either built-in solutions or have plugins that can be used to easily add these tokens to any form.
Check the references for possible solutions provided for the most known frameworks.

See Also

https://codex.wordpress.org/WordPress_Nonces
https://www.nccgroup.trust/globalassets/our-research/us/whitepapers/csrf_paper.pdf
https://www.drupal.org/docs/7/security/writing-secure-code/create-forms-in-a-safe-way-to-avoid-cross-site-request-forgeries
https://symfony.com/doc/current/form/csrf_protection.html
http://en.wikipedia.org/wiki/Cross-site_request_forgery
https://docs.djangoproject.com/en/1.11/ref/csrf/
http://www.cgisecurity.com/csrf-faq.html
https://www.owasp.org/index.php/Testing_for_CSRF_(OTG-SESS-005)
https://docs.joomla.org/How_to_add_CSRF_anti-spoofing_to_forms
https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)

Plugin Details

PUBLICATION DATE	2022-08-08T00:00:00+00:00
MODIFICATION DATE	2023-01-17T00:00:00+00:00
FAMILY	Cross Site Request Forgery
SEVERITY	Low
PLUGIN ID	113332

Risk Information

CVSSV4 BASE SCORE	2.1
CVSSV4 VECTOR	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:A/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N
CVSSV3 BASE SCORE	3.1
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N
CVSS BASE SCORE	2.6
CVSS VECTOR	CVSS2#AV:N/AC:H/Au:N/C:N/I:P/A:N

Reference Information

CWE	352
WASC	Cross-Site Request Forgery
OWASP	2013-A8, 2010-A5, 2021-A1, 2023-API8, 2019-API7
CVE	-
BID	-

Login Form Cross-Site Request Forgery Instances (1)

VULNERABILITY LOW PLUGIN ID 113332

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/login.php

Identification

PROOF

```
<form action="/login.php" method="POST">
<input type="text" id="login" name="login" size="20" autocomplete="off">
</input>
<input type="password" id="password" name="password" size="20" autocomplete="off">
</input>
<select name="security_level">
<option value="0">
low
</option>
<option value="1">
medium
</option>
<option value="2">
high
</option>
</select>
<button type="submit" name="form" value="submit">
Login
</button>
</form>
```

OUTPUT

```
No anti-CSRF token could have been found in the login form attached in proof.

By requesting it several times, the scanner could not find any dynamic input field that would generate a token used by
the application to confirm the user intention to submit this form.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/login.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control=no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Content-Encoding=gzip
Content-Type=text/html
```

```
Date=Tue, 19 Nov 2024 01:51:06 GMT
Expires=Thu, 19 Nov 1981 08:52:00 GMT
Pragma=no-cache
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=97249a7d3363c12f26d1d625a5fdf4df
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4826
```

Cookie Without SameSite Flag Detected

VULNERABILITY LOW PLUGIN ID 115540

Description

SameSite is an attribute which can be set on a cookie to instruct the web browser if this cookie can be sent along with cross-site requests to help prevent Cross-Site Request Forgery (CSRF) attacks.

The attribute has three possible values :

- Strict : the cookie will only be sent in a first-party context, thus preventing cross-site requests initiated from third-party websites to include it.

- Lax : the cookie is allowed to be sent in GET cross-site requests initiated by the top-level navigation from third-party websites. For example, following an hypertext link from the external website will make the request include the cookie.

- None : the cookie is explicitly set to be sent by the browser in any context.

The scanner identified the lack of SameSite attribute on cookies set by the application or a misconfiguration.

Solution

Web browsers default behavior may differ when processing cookies in a cross-site context, making the final decision to send the cookie in this context unpredictable. The SameSite attribute should be set in every cookie to enforce the expected result by developers. When using the 'None' attribute value, ensure that the cookie is also set with the 'Secure' flag.

See Also

https://blog.chromium.org/2019/10/developers-get-ready-for-new.html
https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html#samesite-cookie-attribute
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie/SameSite
https://web.dev/samesite-cookies-explained

Plugin Details

PUBLICATION DATE	2018-12-14T00:00:00+00:00
MODIFICATION DATE	2023-12-11T00:00:00+00:00
FAMILY	HTTP Security Header
SEVERITY	Low
PLUGIN ID	115540

Risk Information

CVSSV4 BASE SCORE	2.1
CVSSV4 VECTOR	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:A/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N
CVSSV3 BASE SCORE	3.1
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N
CVSS BASE SCORE	2.6

CVSS VECTOR	CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N

Reference Information

CWE	352
WASC	Cross-Site Request Forgery
OWASP	2013-A8, 2010-A5, 2021-A1, 2023-API8, 2019-API7
CVE	-
BID	-

Cookie Without SameSite Flag Detected Instances (1)

VULNERABILITY LOW PLUGIN ID 115540

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/

INPUT TYPE	cookie
INPUT NAME	PHPSESSID

Identification

PROOF

```
PHPSESSID=711vt1tpgrucudl1kaq9t074f5; Path=/
```

OUTPUT

```
The scanner detected a cookie named 'PHPSESSID' set with JavaScript which does not have the 'SameSite' attribute set.
```

Scan Information

VULNERABILITY INFO PLUGIN ID 98000

Description

Provides scan information and statistics of plugins run.

Solution

-

See Also

Plugin Details

PUBLICATION DATE	2017-03-31T00:00:00+00:00
MODIFICATION DATE	2023-11-17T00:00:00+00:00
FAMILY	General
SEVERITY	Info
PLUGIN ID	98000

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

Scan Information Instances (1)

VULNERABILITY INFO PLUGIN ID 98000

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/#/

Identification

OUTPUT

```
Engine Version 2.26.10-1603
Plugins Version 202411140727
Scan ID 45c6aad7-0097-4f4e-a4bc-4623af2d119b

Start Time 2024-11-19 00:10:32 +0000
Duration 09:35:35

Requests 706972
Crawler Requests 92
Requests/s 24.7968
Mean Response Time 0.1317s

Bandwidth Usage
- Data to Target 274 MB
- Data from Target 2.24 GB

Timeouts Encountered
Network Timeouts 7
Browser Timeouts 0

Browser Respawns 0

HTTP Protocols Detected
- HTTPs


Authentication Identified
- None


Plugins
- 729 have been included per scan policy
- 792 have been started based on target information collected

List of plugins is available in 'plugins.csv' attachment.


Settings used to conduct this scan are available in 'configuration.csv' attachment.
```

Web Application Sitemap

VULNERABILITY INFO PLUGIN ID 98009

Description

Publishes the sitemap of the web application as seen by the scan.

The list of all URLs that have been detected during the scan are available as an attachment. For each URL in the sitemap, the following information is provided:

- The first time the URL is detected - The logic used to detect the URL. This information may be found by: crawling rendering the page by a specific plugin - The parent URL requested to detect the URL - If the URL has been requested at least once, information about the response - Whether or not the URL has been queued for audit - If the URL has not been queued for audit, the reason why the URL does not need an audit - Whether or not the URL has been effectively audited - If the URL has not been effectively audited, the reason that the scanner was unable to audit the URL

Reasons for not adding a URL to the audit queue are as follows:

- not_in_domain: The domain of the URL does not match main target URL - scope_configuration: The URL does not match scope include list scan settings - directory_depth: The number of directories in the URL path exceeds the scan configuration setting - exclude_file_extension: The URL file extension matched one entry of the file extension blacklist setting - exclude_path_patterns: The URL matched one entry of the URL exclusion blacklist setting - redundant_path: The number of URLs to be audited with the same path and query string parameters has been reached - request_redirect_limit: The number of HTTP redirects allowed per scan configuration setting has been reached - queue_full: The number of URLs to audit has been reached

If a scan fails to audit a URL that has been queued for audit, reasons for the failure are as follows:

- timeout: The request timed out when trying to retrieve URL contents - filesize_exceeded: URL response exceeded file size limit defined in the scan configuration - scan_timelimit_reached: The URL couldn't be audited before the scan time limit - user_abort: The user stopped the scan before the URL could be audited

Solution

-

See Also

Plugin Details

PUBLICATION DATE	2017-03-31T00:00:00+00:00
MODIFICATION DATE	2023-11-17T00:00:00+00:00
FAMILY	General
SEVERITY	Info
PLUGIN ID	98009

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

Web Application Sitemap Instances (1)

VULNERABILITY INFO PLUGIN ID 98009

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/#/

Identification

OUTPUT

```
The scan has discovered 173 distinct URLs.

The following is a breakdown of which URLs were audited:

- 69 effectively audited
- 8 not audited due to the page was too similar to another page already audited
- 42 not queued due to file extension exclusions
- 29 not queued due to the URL not being in the target domain
- 24 not queued due to the URL being considered redundant with other processed URLs
- 1 not queued due to the URL containing a fragment which is a feature of browsers and not included in HTTP requests.
The page being referred to by the fragment shall still be audited by the scanner.

For URLs we received responses for, here is a distribution of the content type headers:

- 1 application/javascript
- 2 application/x-trash
- 1 application/xml
- 7 image/gif
- 4 image/jpeg
- 11 image/png
- 1 text/css
- 26 text/html
- 48 text/html;charset=utf-8

Response times ranged between 0.020808s and 0.281579s.

You can access the complete list of URLs with the information collected by the scan as an attachment to this plugin.
```

Network Timeout Encountered

VULNERABILITY INFO PLUGIN ID 98019

Description

Provides a report of network timeouts encountered during the scan, showing URLs and the number of timeouts for each URL.

Note that assessment will stop on any URLs in timeout state, and timeouts may increase significantly the overall duration of the scan.

Solution

Check your web application logs and verify that it is functioning as expected and can handle significant amounts of traffic generated by the scanner.
Additionally, the scan policy may be edited to optimize the performance settings.

See Also

Plugin Details

PUBLICATION DATE	2017-09-25T00:00:00+00:00
MODIFICATION DATE	2023-11-17T00:00:00+00:00
FAMILY	General
SEVERITY	Info
PLUGIN ID	98019

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

Network Timeout Encountered Instances (1)

VULNERABILITY INFO PLUGIN ID 98019

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/#/

Identification

OUTPUT

```
The scanner encountered 7 network timeouts during the scan. See the attachment for more details
```

Login Form Detected

VULNERABILITY INFO PLUGIN ID 98033

Description

This is an informational notice that the scanner identified a potential login form that could be used by the scanner to authenticate and have access to additional pages for extending its coverage.

Solution

Edit scan policy and add login form authentication credentials to allow scanner to authenticate to the web application.

See Also

Plugin Details

PUBLICATION DATE	2018-02-08T00:00:00+00:00
MODIFICATION DATE	2018-02-08T00:00:00+00:00
FAMILY	Authentication & Session
SEVERITY	Info
PLUGIN ID	98033

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

Login Form Detected Instances (1)

VULNERABILITY INFO PLUGIN ID 98033

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/login.php

INPUT TYPE	form
INPUT NAME	combined:post::https://juice-shop-388277804329.us-west1.run.app/login.php

Identification

OUTPUT

```
Potential login form has been identified in URL 'https://juice-shop-388277804329.us-west1.run.app/login.php' with
following fields:
- login (TEXT)
- password (PASSWORD)
- No name or id (SELECT)
- form (SUBMIT)
To perform authenticated scan, configure your scan and add 'Login Form' authentication, with the URL associated to this
plugin and as login parameters values for the above non-hidden fields.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/login.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control=no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 01:51:06 GMT
Expires=Thu, 19 Nov 1981 08:52:00 GMT
Pragma=no-cache
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=97249a7d3363c12f26d1d625a5fdf4df
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4826
```

Allowed HTTP Methods

VULNERABILITY INFO PLUGIN ID 98047

Description

There are a number of HTTP methods that can be used on a webserver (`OPTIONS`, `HEAD`, `GET`, `POST`, `PUT`, `DELETE` etc.). Each of these methods perform a different function and each have an associated level of risk when their use is permitted on the webserver.

By sending an HTTP OPTIONS request and a direct HTTP request for each method, the scanner discovered the methods that are allowed by the server.

Solution

It is recommended that a whitelisting approach be taken to explicitly permit only the HTTP methods required by the application and block all others.

See Also

http://httpd.apache.org/docs/2.2/mod/core.html#limitexcept

Plugin Details

PUBLICATION DATE	2017-03-31T00:00:00+00:00
MODIFICATION DATE	2024-02-27T00:00:00+00:00
FAMILY	Web Applications
SEVERITY	Info
PLUGIN ID	98047

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

Allowed HTTP Methods Instances (1)

VULNERABILITY INFO PLUGIN ID 98047

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/#/

Identification

OUTPUT

```
The scanner was able to identify several HTTP methods that can be used for one or several URLs. The results are
available as attachments.
```

Interesting Response

VULNERABILITY INFO PLUGIN ID 98050

Description

The scanner identified some responses with a status code other than the usual 200 (OK), 301 (Moved Permanently), 302 (Found) and 404 (Not Found) codes. These codes can provide useful insights into the behavior of the web application and identify any unexpected responses to be addressed.

Solution

-

See Also

http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html

https://en.wikipedia.org/wiki/List_of_HTTP_status_codes

Plugin Details

PUBLICATION DATE	2017-03-31T00:00:00+00:00
MODIFICATION DATE	2021-06-14T00:00:00+00:00
FAMILY	Web Applications
SEVERITY	Info
PLUGIN ID	98050

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

Interesting Response Instances (25)

VULNERABILITY INFO PLUGIN ID 98050

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/passwords/.htaccess

Identification

PROOF

```
HTTP/2 403
```

OUTPUT

```
A response has been received with a response code '403' which may require further investigation to verify if this
response is due to an abnormal behavior of the target.

The response has been triggered by an HTTP GET request made on the URL 'https://juice-shop-388277804329.us-west1.run.app
/passwords/.htaccess'.
```

HTTP Info

REQUEST MADE

```
GET /passwords/.htaccess HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 403
content-type: text/html; charset=iso-8859-1
x-cloud-trace-context: 97fa1398a1575190b59c247660f91cf8
date: Tue, 19 Nov 2024 01:23:11 GMT
server: Google Frontend
content-length: 326
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/js/.htaccess

Identification

PROOF

```
HTTP/2 403
```

OUTPUT

```
A response has been received with a response code '403' which may require further investigation to verify if this
response is due to an abnormal behavior of the target.

The response has been triggered by an HTTP GET request made on the URL 'https://juice-shop-388277804329.us-west1.run.app
/js/.htaccess'.
```

HTTP Info

REQUEST MADE

```
GET /js/.htaccess HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 403
content-type: text/html; charset=iso-8859-1
x-cloud-trace-context: db7087aec6c9bf70fa45ff01dea3de87
date: Tue, 19 Nov 2024 01:14:09 GMT
server: Google Frontend
content-length: 319
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https%3A%2F%2Fjuice-shop-388277804329.us-west1.run.app%2Fapps%2Fsetup%2Fsetup-s%2F%25u002e%25u002e%2F%25u002e%25u002e%2Flog.jsp

Identification

PROOF

```
HTTP/2 400
```

OUTPUT

```
A response has been received with a response code '400' which may require further investigation to verify if this
response is due to an abnormal behavior of the target.

The response has been triggered by an HTTP GET request made on the URL 'https://juice-shop-388277804329.us-west1.run.app
/apps/setup/setup-s/%u002e%u002e/%u002e%u002e/log.jsp'.
```

HTTP Info

REQUEST MADE

```
GET /apps/setup/setup-s/%u002e%u002e/%u002e%u002e/log.jsp HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 400
content-type: text/html; charset=iso-8859-1
x-cloud-trace-context: faa05836554e60e828b617206200884c
date: Tue, 19 Nov 2024 00:30:20 GMT
server: Google Frontend
content-length: 331
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/#/

Identification

PROOF

```
HTTP/2 405
```

OUTPUT

```
A response has been received with a response code '405' which may require further investigation to verify if this
response is due to an abnormal behavior of the target.

The response has been triggered by an HTTP TRACE request made on the URL 'https://juice-shop-388277804329.us-west1.run.
app/#/'.
```

HTTP Info

REQUEST MADE

```
TRACE / HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
X-Tenable-Wasscan-Trace: 1
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 405
content-type: text/html; charset=UTF-8
referrer-policy: no-referrer
content-length: 1590
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/passwords/.htpasswd

Identification

PROOF

```
HTTP/2 403
```

OUTPUT

```
A response has been received with a response code '403' which may require further investigation to verify if this
response is due to an abnormal behavior of the target.

The response has been triggered by an HTTP GET request made on the URL 'https://juice-shop-388277804329.us-west1.run.app
/passwords/.htpasswd'.
```

HTTP Info

REQUEST MADE

```
GET /passwords/.htpasswd HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
```

```
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 403
content-type: text/html; charset=iso-8859-1
x-cloud-trace-context: c6d6e9274c431e8ae1fb714c8885be83
date: Tue, 19 Nov 2024 01:23:11 GMT
server: Google Frontend
content-length: 326
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/db/.htpasswd

Identification

PROOF

```
HTTP/2 403
```

OUTPUT

```
A response has been received with a response code '403' which may require further investigation to verify if this
response is due to an abnormal behavior of the target.

The response has been triggered by an HTTP GET request made on the URL 'https://juice-shop-388277804329.us-west1.run.app
/db/.htpasswd'.
```

HTTP Info

REQUEST MADE

```
GET /db/.htpasswd HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 403
content-type: text/html; charset=iso-8859-1
x-cloud-trace-context: f66a0c07676f4c04044439dd2f76e4b0
date: Tue, 19 Nov 2024 00:46:45 GMT
server: Google Frontend
content-length: 319
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/stylesheets/.htpasswd

Identification

PROOF

```
HTTP/2 403
```

OUTPUT

```
A response has been received with a response code '403' which may require further investigation to verify if this
response is due to an abnormal behavior of the target.

The response has been triggered by an HTTP GET request made on the URL 'https://juice-shop-388277804329.us-west1.run.app
/stylesheets/.htpasswd'.
```

HTTP Info

REQUEST MADE

```
GET /stylesheets/.htpasswd HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 403
content-type: text/html; charset=iso-8859-1
x-cloud-trace-context: 4531364c214c79e3af5f0a0804d76b5d
date: Tue, 19 Nov 2024 01:41:48 GMT
server: Google Frontend
content-length: 328
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/passwords/heroes

Identification

PROOF

```
HTTP/2 406
```

OUTPUT

```
A response has been received with a response code '406' which may require further investigation to verify if this
response is due to an abnormal behavior of the target.

The response has been triggered by an HTTP GET request made on the URL 'https://juice-shop-388277804329.us-west1.run.app
/passwords/heroes'.
```

HTTP Info

REQUEST MADE

```
GET /passwords/heroes HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: application/WAS; q=1.0
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 406
alternates: {"heroes.xml" 1 {type application/xml} {length 1208}}
vary: negotiate
tcn: list
content-type: text/html; charset=iso-8859-1
```

```
x-cloud-trace-context: b2adab0da22417dc8f8052dfcb2e923c
date: Tue, 19 Nov 2024 06:07:01 GMT
server: Google Frontend
content-length: 471
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/images/.htaccess

Identification

PROOF

```
HTTP/2 403
```

OUTPUT

```
A response has been received with a response code '403' which may require further investigation to verify if this
response is due to an abnormal behavior of the target.

The response has been triggered by an HTTP GET request made on the URL 'https://juice-shop-388277804329.us-west1.run.app
/images/.htaccess'.
```

HTTP Info

REQUEST MADE

```
GET /images/.htaccess HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 403
content-type: text/html; charset=iso-8859-1
x-cloud-trace-context: fe4cd1c7ab0b5c6b2677830a511cbd8f
date: Tue, 19 Nov 2024 01:05:07 GMT
server: Google Frontend
content-length: 323
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/soap/.htpasswd

Identification

PROOF

```
HTTP/2 403
```

OUTPUT

```
A response has been received with a response code '403' which may require further investigation to verify if this
response is due to an abnormal behavior of the target.

The response has been triggered by an HTTP GET request made on the URL 'https://juice-shop-388277804329.us-west1.run.app
/soap/.htpasswd'.
```

HTTP Info

REQUEST MADE

```
GET /soap/.htpasswd HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 403
content-type: text/html; charset=iso-8859-1
x-cloud-trace-context: 7e1bd6a2d97c8db2caab5217d70b7e90
date: Tue, 19 Nov 2024 01:32:22 GMT
server: Google Frontend
content-length: 321
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/documents/.htaccess

Identification

PROOF

```
HTTP/2 403
```

OUTPUT

```
A response has been received with a response code '403' which may require further investigation to verify if this
response is due to an abnormal behavior of the target.

The response has been triggered by an HTTP GET request made on the URL 'https://juice-shop-388277804329.us-west1.run.app
/documents/.htaccess'.
```

HTTP Info

REQUEST MADE

```
GET /documents/.htaccess HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 403
content-type: text/html; charset=iso-8859-1
x-cloud-trace-context: 3e479eed9071098a919a468da56623ce
date: Tue, 19 Nov 2024 00:55:55 GMT
server: Google Frontend
content-length: 326
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/apps/.htaccess

Identification

PROOF

```
HTTP/2 403
```

OUTPUT

```
A response has been received with a response code '403' which may require further investigation to verify if this
response is due to an abnormal behavior of the target.

The response has been triggered by an HTTP GET request made on the URL 'https://juice-shop-388277804329.us-west1.run.app
/apps/.htaccess'.
```

HTTP Info

REQUEST MADE

```
GET /apps/.htaccess HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 403
content-type: text/html; charset=iso-8859-1
x-cloud-trace-context: 66f748b7a587adcd454d918c9ca0edd6
date: Tue, 19 Nov 2024 00:37:37 GMT
server: Google Frontend
content-length: 321
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/apps/was-tnb.aspx

Identification

PROOF

```
HTTP/2 502
```

OUTPUT

```
A response has been received with a response code '502' which may require further investigation to verify if this
response is due to an abnormal behavior of the target.

The response has been triggered by an HTTP DEBUG request made on the URL 'https://juice-shop-388277804329.us-west1.run.
app/apps/was-tnb.aspx'.
```

HTTP Info

REQUEST MADE

```
DEBUG /apps/was-tnb.aspx HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

```
Accept: */*
Accept-Language: en-US,en;q=0.5
Command: stop-debug
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 502
content-type: text/html; charset=UTF-8
referrer-policy: no-referrer
content-length: 332
date: Tue, 19 Nov 2024 00:30:45 GMT
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/documents/.htpasswd

Identification

PROOF

```
HTTP/2 403
```

OUTPUT

```
A response has been received with a response code '403' which may require further investigation to verify if this
response is due to an abnormal behavior of the target.

The response has been triggered by an HTTP GET request made on the URL 'https://juice-shop-388277804329.us-west1.run.app
/documents/.htpasswd'.
```

HTTP Info

REQUEST MADE

```
GET /documents/.htpasswd HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 403
content-type: text/html; charset=iso-8859-1
x-cloud-trace-context: 76c206ba1455906541c2019987e41f43
date: Tue, 19 Nov 2024 00:55:55 GMT
server: Google Frontend
content-length: 326
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/.htaccess

Identification

PROOF

```
HTTP/2 403
```

OUTPUT

```
A response has been received with a response code '403' which may require further investigation to verify if this
response is due to an abnormal behavior of the target.

The response has been triggered by an HTTP GET request made on the URL 'https://juice-shop-388277804329.us-west1.run.
app/.htaccess'.
```

HTTP Info

REQUEST MADE

```
GET /.htaccess HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=vpagqnepcomj0eh55jfm27g335
```

RESPONSE HEADERS

```
HTTP/2 403
content-type: text/html; charset=iso-8859-1
x-cloud-trace-context: ad61b23217fd8f917f4da178495d19fe
date: Tue, 19 Nov 2024 00:14:56 GMT
server: Google Frontend
content-length: 316
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/stylesheets/.htaccess

Identification

PROOF

```
HTTP/2 403
```

OUTPUT

```
A response has been received with a response code '403' which may require further investigation to verify if this
response is due to an abnormal behavior of the target.

The response has been triggered by an HTTP GET request made on the URL 'https://juice-shop-388277804329.us-west1.run.app
/stylesheets/.htaccess'.
```

HTTP Info

REQUEST MADE

```
GET /stylesheets/.htaccess HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 403
content-type: text/html; charset=iso-8859-1
x-cloud-trace-context: 083f6b4ea2bd06c6696801ecc2b90d81
date: Tue, 19 Nov 2024 01:41:48 GMT
server: Google Frontend
```

```
content-length: 328
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/passwords/web.config

Identification

PROOF

```
HTTP/2 406
```

OUTPUT

```
A response has been received with a response code '406' which may require further investigation to verify if this
response is due to an abnormal behavior of the target.

The response has been triggered by an HTTP GET request made on the URL 'https://juice-shop-388277804329.us-west1.run.app
/passwords/web.config'.
```

HTTP Info

REQUEST MADE

```
GET /passwords/web.config HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: application/WAS; q=1.0
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 406
alternates: {"web.config.bak" 1 {type application/x-trash} {length 7556}}
vary: negotiate
tcn: list
content-type: text/html; charset=iso-8859-1
x-cloud-trace-context: 83c24212c96ac336035c2e21a3e7ad45
date: Tue, 19 Nov 2024 06:11:54 GMT
server: Google Frontend
content-length: 487
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/apps/.htpasswd

Identification

PROOF

```
HTTP/2 403
```

OUTPUT

```
A response has been received with a response code '403' which may require further investigation to verify if this
response is due to an abnormal behavior of the target.

The response has been triggered by an HTTP GET request made on the URL 'https://juice-shop-388277804329.us-west1.run.app
/apps/.htpasswd'.
```

HTTP Info

REQUEST MADE

```
GET /apps/.htpasswd HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 403
content-type: text/html; charset=iso-8859-1
x-cloud-trace-context: c33acaceb3b181aed32ea50187633139
date: Tue, 19 Nov 2024 00:37:37 GMT
server: Google Frontend
content-length: 321
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/images/.htpasswd

Identification

PROOF

```
HTTP/2 403
```

OUTPUT

```
A response has been received with a response code '403' which may require further investigation to verify if this
response is due to an abnormal behavior of the target.

The response has been triggered by an HTTP GET request made on the URL 'https://juice-shop-388277804329.us-west1.run.app
/images/.htpasswd'.
```

HTTP Info

REQUEST MADE

```
GET /images/.htpasswd HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 403
content-type: text/html; charset=iso-8859-1
x-cloud-trace-context: 09ef83ab7d0dc4ac834837815686bddc
date: Tue, 19 Nov 2024 01:05:07 GMT
server: Google Frontend
content-length: 323
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/soap/.htaccess

Identification

PROOF

```
HTTP/2 403
```

OUTPUT

```
A response has been received with a response code '403' which may require further investigation to verify if this
response is due to an abnormal behavior of the target.

The response has been triggered by an HTTP GET request made on the URL 'https://juice-shop-388277804329.us-west1.run.app
/soap/.htaccess'.
```

HTTP Info

REQUEST MADE

```
GET /soap/.htaccess HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 403
content-type: text/html; charset=iso-8859-1
x-cloud-trace-context: 398ccd0243aa897ed5a68b842664c8ba
date: Tue, 19 Nov 2024 01:32:22 GMT
server: Google Frontend
content-length: 321
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/js/.htpasswd

Identification

PROOF

```
HTTP/2 403
```

OUTPUT

```
A response has been received with a response code '403' which may require further investigation to verify if this
response is due to an abnormal behavior of the target.

The response has been triggered by an HTTP GET request made on the URL 'https://juice-shop-388277804329.us-west1.run.app
/js/.htpasswd'.
```

HTTP Info

REQUEST MADE

```
GET /js/.htpasswd HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

```
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 403
content-type: text/html; charset=iso-8859-1
x-cloud-trace-context: c8b8bdb1017d1747ff0b9ab32fae7d77
date: Tue, 19 Nov 2024 01:14:09 GMT
server: Google Frontend
content-length: 319
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/db/.htaccess

Identification

PROOF

```
HTTP/2 403
```

OUTPUT

```
A response has been received with a response code '403' which may require further investigation to verify if this
response is due to an abnormal behavior of the target.

The response has been triggered by an HTTP GET request made on the URL 'https://juice-shop-388277804329.us-west1.run.app
/db/.htaccess'.
```

HTTP Info

REQUEST MADE

```
GET /db/.htaccess HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 403
content-type: text/html; charset=iso-8859-1
x-cloud-trace-context: dddbb706207299c69c0a37931cfa1bfa
date: Tue, 19 Nov 2024 00:46:45 GMT
server: Google Frontend
content-length: 319
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/server-status

Identification

PROOF

```
HTTP/2 403
```

OUTPUT

```
A response has been received with a response code '403' which may require further investigation to verify if this
response is due to an abnormal behavior of the target.

The response has been triggered by an HTTP GET request made on the URL 'https://juice-shop-388277804329.us-west1.run.app
/server-status'.
```

HTTP Info

REQUEST MADE

```
GET /server-status HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 403
content-type: text/html; charset=iso-8859-1
x-cloud-trace-context: 89c7998c1e85f549d9047da3347454bc
date: Tue, 19 Nov 2024 00:14:52 GMT
server: Google Frontend
content-length: 320
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/.htpasswd

Identification

PROOF

```
HTTP/2 403
```

OUTPUT

```
A response has been received with a response code '403' which may require further investigation to verify if this
response is due to an abnormal behavior of the target.

The response has been triggered by an HTTP GET request made on the URL 'https://juice-shop-388277804329.us-west1.run.
app/.htpasswd'.
```

HTTP Info

REQUEST MADE

```
GET /.htpasswd HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=vpagqnepcomj0eh55jfm27g335
```

RESPONSE HEADERS

```
HTTP/2 403
content-type: text/html; charset=iso-8859-1
x-cloud-trace-context: 35fc857088e1a73267f73d042d726abb
date: Tue, 19 Nov 2024 00:14:56 GMT
server: Google Frontend
```

```
content-length: 316
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/install.php?cb=was_302_ebiu

Identification

PROOF

```
HTTP/2 400
```

OUTPUT

```
A response has been received with a response code '400' which may require further investigation to verify if this
response is due to an abnormal behavior of the target.

The response has been triggered by an HTTP GET request made on the URL 'https://juice-shop-388277804329.us-west1.run.app
/install.php'.
```

HTTP Info

REQUEST MADE

```
GET /install.php?cb=was_302_ebiu HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
X-Oversized-Header:
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 400
content-type: text/html; charset=iso-8859-1
x-cloud-trace-context: 33f0ae26724415da7b393b70e8eb377d
date: Tue, 19 Nov 2024 00:25:50 GMT
server: Google Frontend
content-length: 391
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

Technologies Detected

VULNERABILITY INFO PLUGIN ID 98059

Description

This is an informational plugin to inform the user what technologies the framework has detected on the target application, which can then be examined and checked for known vulnerable software versions

Solution

Only use components that do not have known vulnerabilities, only use components that when combined to not introduce a security vulnerability, and ensure that a misconfiguration does not cause any vulnerabilities

See Also

Plugin Details

PUBLICATION DATE	2017-12-06T00:00:00+00:00
MODIFICATION DATE	2023-11-17T00:00:00+00:00
FAMILY	Web Applications
SEVERITY	Info
PLUGIN ID	98059

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

Technologies Detected Instances (1)

VULNERABILITY INFO PLUGIN ID 98059

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/#/

Identification

OUTPUT

```
The framework has detected the following technologies in the target application:

- PHP (v5.5.9)
- Apache (v2.4.7)
```

Cookies Collected

VULNERABILITY INFO PLUGIN ID 98061

Description

The scanner collected the cookies returned by the application during the scan. The list includes the following information for each cookie:
- Name: name of the cookie
- Value: value of the cookie
- Domain: hosts to which the cookie will be sent
- Path: URL path which must exist in the requested resource before sending the cookie
- Expires: maximum lifetime of the cookie as an HTTP-date timestamp
- Max-Age: number of seconds until the cookie expires
- HttpOnly: cookie is set to be not accessible via JavaScript, XMLHttpRequest and Request APIs
- Secure: cookie will be sent to the server only when a request is made using HTTPS
- SameSite: cookie will be sent along with cross-site request according the defined policy
- URL: first URL discovered which set the cookie in its response
- Set-Method: method used by the application to set the cookie (Set-Cookie or JavaScript)
- Audited: cookie will be audited by plugins during the scan
- Reason Not Audited: reason given for the cookie not being audited during the scan

Solution

-

See Also

https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
https://en.wikipedia.org/wiki/HTTP_cookie
https://tools.ietf.org/html/rfc6265

Plugin Details

PUBLICATION DATE	2020-09-01T00:00:00+00:00
MODIFICATION DATE	2023-11-17T00:00:00+00:00
FAMILY	Web Applications
SEVERITY	Info
PLUGIN ID	98061

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

Cookies Collected Instances (1)

VULNERABILITY INFO PLUGIN ID 98061

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/#/

Identification

OUTPUT

```
The following cookies have been collected during the scan of the target:
- 0 cookie(s) specified via Set-Cookie
- 1 cookie(s) set via JavaScript code
The complete list of the cookies is available in attachment.
```

Common Files Detection

VULNERABILITY INFO PLUGIN ID 98071

Description

Scanner has detected common sensitive files on the remote web server.

Web applications are often made up of multiple files and directories. It is possible that over time some files may become unreferenced (unused) by the web application and forgotten about by the administrator or developer. Because web applications are built using common frameworks, they contain common files that can be discovered (independent of server).

During the initial reconnaissance stages of an attack, cyber-criminals will attempt to locate unreferenced files in the hope that the file will assist in further compromise of the web application. To achieve this, they will make thousands of requests using word lists containing common filenames. The response headers from the server will then indicate if the file exists.

Solution

If files are unreferenced, then they should be removed from the web root and/or the application directory.
Preventing access without authentication may also be an option and can stop a client from being able to view the contents of a file; however, it is still likely that the directory structure will be able to be discovered.
Using obscure file names is implementing 'security through obscurity' and is not a recommended option.

See Also

http://httpd.apache.org/docs/2.0/mod/mod_access.html
http://projects.webappsec.org/w/page/13246953/Predictable%20Resource%20Location
http://nginx.org/en/docs/http/ngx_http_access_module.html
https://www.nginx.com/resources/admin-guide/restricting-access-auth-basic/
https://www.owasp.org/index.php/Forced_browsing

Plugin Details

PUBLICATION DATE	2017-03-31T00:00:00+00:00
MODIFICATION DATE	2024-01-08T00:00:00+00:00
FAMILY	Web Servers
SEVERITY	Info
PLUGIN ID	98071

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

Common Files Detection Instances (1)

VULNERABILITY INFO PLUGIN ID 98071

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/install.php

Identification

OUTPUT

```
The common file 'install.php' was identified by the scanner.
```

HTTP Info

REQUEST MADE

```
GET /install.php HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
```

RESPONSE HEADERS

```
HTTP/2 200
x-powered-by: PHP/5.5.9-1ubuntu4.14
vary: Accept-Encoding
content-type: text/html
content-encoding: gzip
x-cloud-trace-context: 41976c367965e580e30e07c8e906a798
date: Tue, 19 Nov 2024 00:10:36 GMT
server: Google Frontend
content-length: 945
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

Common Directories Detection

VULNERABILITY INFO PLUGIN ID 98072

Description

Scanner has detected a common directory on the remote web server.

Web applications are often made up of multiple files and directories. It is possible that over time some directories may become unreferenced (unused) by the web application and forgotten about by the administrator or developer. Because web applications are built using common frameworks, they contain common directories that can be discovered (independent of server).

During the initial reconnaissance stages of an attack, cyber-criminals will attempt to locate unreferenced directories in the hope that the directory will assist in further compromise of the web application. To achieve this, they will make thousands of requests using word lists containing common names. The response headers from the server will then indicate if the directory exists.

Solution

If directories are unreferenced, then they should be removed from the web root and/or the application directory.
Preventing access without authentication may also be an option and can stop a client from being able to view the contents of a file; however, it is still likely that the directory structure will be able to be discovered.
Using obscure directory names is implementing 'security through obscurity' and is not a recommended option.

See Also

http://httpd.apache.org/docs/2.0/mod/mod_access.html
http://projects.webappsec.org/w/page/13246953/Predictable%20Resource%20Location
https://www.nginx.com/resources/admin-guide/restricting-access-auth-basic/
https://www.owasp.org/index.php/Forced_browsing

Plugin Details

PUBLICATION DATE	2017-03-31T00:00:00+00:00
MODIFICATION DATE	2024-01-03T00:00:00+00:00
FAMILY	Web Servers
SEVERITY	Info
PLUGIN ID	98072

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

Common Directories Detection Instances (8)

VULNERABILITY INFO PLUGIN ID 98072

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/db/

Identification

OUTPUT

```
The common directory 'db' was identified by the scanner.
```

HTTP Info

REQUEST MADE

```
GET /db/ HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
```

RESPONSE HEADERS

```
HTTP/2 200
vary: Accept-Encoding
content-type: text/html;charset=UTF-8
content-encoding: gzip
x-cloud-trace-context: 677b6f23aa804fa8754954086e8d57f7
date: Tue, 19 Nov 2024 00:10:54 GMT
server: Google Frontend
content-length: 477
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/documents/

Identification

OUTPUT

```
The common directory 'documents' was identified by the scanner.
```

HTTP Info

REQUEST MADE

```
GET /documents/ HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
```

RESPONSE HEADERS

```
HTTP/2 200
vary: Accept-Encoding
content-type: text/html;charset=UTF-8
content-encoding: gzip
x-cloud-trace-context: fee639dea548ad7ac4ad936e768b2c9b
date: Tue, 19 Nov 2024 00:10:55 GMT
server: Google Frontend
content-length: 628
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/images/

Identification

OUTPUT

```
The common directory 'images' was identified by the scanner.
```

HTTP Info

REQUEST MADE

```
GET /images/ HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
```

RESPONSE HEADERS

```
HTTP/2 200
vary: Accept-Encoding
content-type: text/html;charset=UTF-8
content-encoding: gzip
x-cloud-trace-context: 9b9a8c0f1bc5d6220c6b5a796143bd6e
date: Tue, 19 Nov 2024 00:11:00 GMT
server: Google Frontend
content-length: 769
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/stylesheets/

Identification

OUTPUT

```
The common directory 'stylesheets' was identified by the scanner.
```

HTTP Info

REQUEST MADE

```
GET /stylesheets/ HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

```
Accept: */*
Accept-Language: en-US,en;q=0.5
```

RESPONSE HEADERS

```
HTTP/2 200
vary: Accept-Encoding
content-type: text/html;charset=UTF-8
content-encoding: gzip
x-cloud-trace-context: a2e0f8a3d50572a6157c21fe674426e3
date: Tue, 19 Nov 2024 00:11:16 GMT
server: Google Frontend
content-length: 514
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/apps/

Identification

OUTPUT

```
The common directory 'apps' was identified by the scanner.
```

HTTP Info

REQUEST MADE

```
GET /apps/ HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
```

RESPONSE HEADERS

```
HTTP/2 200
vary: Accept-Encoding
content-type: text/html;charset=UTF-8
content-encoding: gzip
x-cloud-trace-context: 4d37b4d71f7f55c9509839b5eb30d29a
date: Tue, 19 Nov 2024 00:10:48 GMT
server: Google Frontend
content-length: 479
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/soap/

Identification

OUTPUT

```
The common directory 'soap' was identified by the scanner.
```

HTTP Info

REQUEST MADE

```
GET /soap/ HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
```

RESPONSE HEADERS

```
HTTP/2 200
vary: Accept-Encoding
content-type: text/html;charset=UTF-8
content-encoding: gzip
x-cloud-trace-context: 1ac74ee01d8d1853ce48d966d1f645f2
date: Tue, 19 Nov 2024 00:11:14 GMT
server: Google Frontend
content-length: 649
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/js/

Identification

OUTPUT

```
The common directory 'js' was identified by the scanner.
```

HTTP Info

REQUEST MADE

```
GET /js/ HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
```

RESPONSE HEADERS

```
HTTP/2 200
vary: Accept-Encoding
content-type: text/html;charset=UTF-8
content-encoding: gzip
x-cloud-trace-context: 206e37e022bbdeecbb30381149aae6f7
date: Tue, 19 Nov 2024 00:11:02 GMT
server: Google Frontend
content-length: 532
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/passwords/

Identification

OUTPUT

```
The common directory 'passwords' was identified by the scanner.
```

HTTP Info

REQUEST MADE

```
GET /passwords/ HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
```

RESPONSE HEADERS

```
HTTP/2 200
vary: Accept-Encoding
content-type: text/html;charset=UTF-8
content-encoding: gzip
x-cloud-trace-context: 46ff539c7fd7244ae8c44bfdd7e9c0a0
date: Tue, 19 Nov 2024 00:11:07 GMT
server: Google Frontend
content-length: 518
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

Private IP Address Disclosure

VULNERABILITY INFO PLUGIN ID 98077

Description

Private, or non-routable, IP addresses are generally used within a home or company network and are typically unknown to anyone outside of that network.

Cyber-criminals will attempt to identify the private IP address range being used by their victim, to aid in collecting further information that could then lead to a possible compromise.

Scanner discovered that the affected page returned a RFC 1918 compliant private IP address and therefore could be revealing sensitive information.

This finding typically requires manual verification to ensure the context is correct, as any private IP address within the HTML body will trigger it.

Solution

Identifying the context in which the affected page displays a Private IP address is necessary.
If the page is publicly accessible and displays the Private IP of the affected server (or supporting infrastructure), then measures should be put in place to ensure that the IP address is removed from any response.

See Also

http://projects.webappsec.org/w/page/13246936/Information%20Leakage

Plugin Details

PUBLICATION DATE	2017-03-31T00:00:00+00:00
MODIFICATION DATE	2023-11-17T00:00:00+00:00
FAMILY	Data Exposure
SEVERITY	Info
PLUGIN ID	98077

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-

OWASP	-
CVE	-
BID	-

Private IP Address Disclosure Instances (1)

VULNERABILITY INFO PLUGIN ID 98077

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/#/

Identification

OUTPUT

```
Number of Private IP Addresses Collected: 3

Listed below are each private ip address:
169.254.169.1 found on 1 URL
169.254.169.126 found on 1 URL
127.0.0.1 found on 1 URL
```

E-mail Address Disclosure

VULNERABILITY INFO PLUGIN ID 98078

Description

Email addresses are typically found on "Contact us" pages, however, they can also be found within scripts or code comments of the application. They are used to provide a legitimate means of contacting an organisation.

As one of the initial steps in information gathering, cyber-criminals will spider a website and using automated methods collect as many email addresses as possible, that they may then use in a social engineering attack.

Using the same automated methods, scanner was able to detect one or more email addresses that were stored within the affected page.

Solution

E-mail addresses should be presented in such a way that it is hard to process them automatically.

See Also

Plugin Details

PUBLICATION DATE	2017-03-31T00:00:00+00:00
MODIFICATION DATE	2023-11-17T00:00:00+00:00
FAMILY	Data Exposure
SEVERITY	Info
PLUGIN ID	98078

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

E-mail Address Disclosure Instances (1)

VULNERABILITY INFO PLUGIN ID 98078

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/#/

Identification

OUTPUT

```
Number of Email Addresses Collected: 3
Listed below are each email address and the number of URLs where the email address has been found:
license@php.net found on 1 URL
bee6885858486f31043e5839c735d99457f045affd0bwapp-bee@mailinator.comA found on 1 URL
A.I.M.6885858486f31043e5839c735d99457f045affd0bwapp-aim@mailinator.comA found on 1 URL
```

Target Information

VULNERABILITY INFO PLUGIN ID 98136

Description

Publishes the target information of the starting url as evaluated by the scan.

Solution

-

See Also

Plugin Details

PUBLICATION DATE	2017-07-27T00:00:00+00:00
MODIFICATION DATE	2024-04-26T00:00:00+00:00
FAMILY	General
SEVERITY	Info
PLUGIN ID	98136

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

Target Information Instances (1)

VULNERABILITY INFO PLUGIN ID 98136

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/#/

Identification

OUTPUT

```
Access to URL 'https://juice-shop-388277804329.us-west1.run.app/#/' has been confirmed.


Target Information
------------------------

Domain Name : juice-shop-388277804329.us-west1.run.app
IP Address : 216.239.32.53


Response Information
---------------------------

Status Code : 302
Return Code : ok
Return Message: No error
Response Time : 0.078037s
Response Size : 294 bytes
Content-Type : text/html


DEBUG INFORMATION
-----------------------

HTTP Network Timeout : 30s
```

HTTP Info

REQUEST MADE

```
GET / HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
```

RESPONSE HEADERS

```
HTTP/2 302
x-powered-by: PHP/5.5.9-1ubuntu4.14
location: portal.php
content-type: text/html
x-cloud-trace-context: 1af46a284798e67769151ba2877d7ea6
date: Tue, 19 Nov 2024 00:10:34 GMT
server: Google Frontend
content-length: 0
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

Screenshot

VULNERABILITY INFO PLUGIN ID 98138

Description

Screenshot of the target web page, see attached image. This screenshot should show you the target page we are launching the scan against. If the image is not of the intended target page, please check the provided url in the scan configuration.

Solution

-

See Also

Plugin Details

PUBLICATION DATE	2018-01-23T00:00:00+00:00
MODIFICATION DATE	2018-02-14T00:00:00+00:00
FAMILY	General
SEVERITY	Info
PLUGIN ID	98138

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

Screenshot Instances (1)

VULNERABILITY INFO PLUGIN ID 98138

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/#/

Identification

OUTPUT

```
WAS Scanner has taken a screenshot of the page at url 'https://juice-shop-388277804329.us-west1.run.app/#/' with
dimensions 1600x1200.

Please see the attachment for the screenshot image.
```

Form Detected

VULNERABILITY INFO PLUGIN ID 98148

Description

The scanner has detected the presence of a form during the crawling of the target web application. Details about the form are provided in the plugin output.

Solution

-

See Also

Plugin Details

PUBLICATION DATE	2021-10-21T00:00:00+00:00
MODIFICATION DATE	2021-10-21T00:00:00+00:00
FAMILY	Web Applications
SEVERITY	Info
PLUGIN ID	98148

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

Form Detected Instances (2)

VULNERABILITY INFO PLUGIN ID 98148

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/login.php

INPUT TYPE	form
INPUT NAME	combined:post::https://juice-shop-388277804329.us-west1.run.app/login.php

Identification

OUTPUT

```
A form with no identifier has been detected on the following URL https://juice-shop-388277804329.us-west1.run.app/login.
php with input fields :
- login (text)
- password (password)
- No name or id (select)
- form (submit)

This form is submitted by using the following action : https://juice-shop-388277804329.us-west1.run.app/login.php
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/login.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control=no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 01:51:06 GMT
Expires=Thu, 19 Nov 1981 08:52:00 GMT
Pragma=no-cache
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=97249a7d3363c12f26d1d625a5fdf4df
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4826
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/user_new.php

INPUT TYPE	form
INPUT NAME	combined:post::https://juice-shop-388277804329.us-west1.run.app/user_new.php

Identification

OUTPUT

```
A form with no identifier has been detected on the following URL https://juice-shop-388277804329.us-west1.run.app
/user_new.php with input fields :
- login (text)
- email (text)
- password (password)
- password_conf (password)
- secret (text)
- mail_activation (checkbox)
- action (submit)

This form is submitted by using the following action : https://juice-shop-388277804329.us-west1.run.app/user_new.php
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/user_new.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 07:45:52 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=1de28a3c31c89c397b35ab9cf352eeaf
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4224
```

External URLs

VULNERABILITY INFO PLUGIN ID 98154

Description

An external URL is an URL for which the Fully Qualified Domain Name (FQDN) is not the same as the web target URL one. The scanner detected the presence of external URLs on the target web application and have listed them based on two types : URLs with a domain name in common with the web target URL and all the other external URLs.

Solution

-

See Also

Plugin Details

PUBLICATION DATE	2022-11-30T00:00:00+00:00
MODIFICATION DATE	2022-12-12T00:00:00+00:00
FAMILY	General
SEVERITY	Info
PLUGIN ID	98154

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

External URLs Instances (1)

VULNERABILITY INFO PLUGIN ID 98154

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/#/

Identification

OUTPUT

```
The scanner detected the presence of 24 URLs on the target application:

- 0 URLs which use a hostname related to the target hostname
- 24 URLs which use a third party hostname

The list of the detected URLs is provided in attachment.
```

Missing Permissions Policy

VULNERABILITY INFO PLUGIN ID 98526

Description

Permissions Policy provides mechanisms to websites to restrict the use of browser features in its own frame and in iframes that it embeds.

Solution

Configure Permissions Policy on your website by adding 'Permissions-Policy' HTTP header.

See Also

https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy
https://scotthelme.co.uk/goodbye-feature-policy-and-hello-permissions-policy/

Plugin Details

PUBLICATION DATE	2019-03-27T00:00:00+00:00
MODIFICATION DATE	2024-03-25T00:00:00+00:00
FAMILY	HTTP Security Header
SEVERITY	Info
PLUGIN ID	98526

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

Missing Permissions Policy Instances (25)

VULNERABILITY INFO PLUGIN ID 98526

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/soap/class.nusoap_base.php

Identification

OUTPUT

```
No Permissions-Policy headers were found on https://juice-shop-388277804329.us-west1.run.app/soap/class.nusoap_base.php
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/soap/class.nusoap_base.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type=text/html
Date=Tue, 19 Nov 2024 06:46:36 GMT
Server=Google Frontend
X-Cloud-Trace-Context=c53cd0b0ef8c298766ed3c1bd61168b7
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=811
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/info_install.php

Identification

OUTPUT

```
No Permissions-Policy headers were found on https://juice-shop-388277804329.us-west1.run.app/info_install.php
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/info_install.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Arch=""
Sec-Ch-Ua-Bitness=""
Sec-Ch-Ua-Full-Version-List="Chromium", "HeadlessChrome", "Not-A.Brand";v="99.0.0.0"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Model=""
Sec-Ch-Ua-Platform="Linux"
Sec-Ch-Ua-Platform-Version=""
Sec-Ch-Ua-Wow64=?0
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 02:21:07 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=3305fabc85563bee1adce5fca1986cef
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4188
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/db/

Identification

OUTPUT

```
No Permissions-Policy headers were found on https://juice-shop-388277804329.us-west1.run.app/db/
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/db/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 00:39:25 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=7330f8397d6d6ed7b0975d370f2d06ee
Content-Length=1778
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/documents/

Identification

OUTPUT

```
No Permissions-Policy headers were found on https://juice-shop-388277804329.us-west1.run.app/documents/
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/documents/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 00:48:33 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=8659790f61386a0d355111f26ee2a386
Content-Length=3149
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/js/

Identification

OUTPUT

```
No Permissions-Policy headers were found on https://juice-shop-388277804329.us-west1.run.app/js/
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/js/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 01:06:45 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=92dbc4630193c57aa70de731a23c4521
Content-Length=2393
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/training_install.php

Identification

OUTPUT

```
No Permissions-Policy headers were found on https://juice-shop-388277804329.us-west1.run.app/training_install.php
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/training_install.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 02:31:16 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=dc248926d66de31d4ae1d4212ab637d0
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4629
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/install.php

Identification

OUTPUT

```
No Permissions-Policy headers were found on https://juice-shop-388277804329.us-west1.run.app/install.php
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/install.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Arch=""
Sec-Ch-Ua-Bitness=""
Sec-Ch-Ua-Full-Version-List="Chromium", "HeadlessChrome", "Not-A.Brand";v="99.0.0.0"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Model=""
Sec-Ch-Ua-Platform="Linux"
Sec-Ch-Ua-Platform-Version=""
Sec-Ch-Ua-Wow64=?0
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 00:19:04 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=793633ff205741c27021c36f1f4362a8
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=3083
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/stylesheets/

Identification

OUTPUT

```
No Permissions-Policy headers were found on https://juice-shop-388277804329.us-west1.run.app/stylesheets/
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/stylesheets/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 01:34:22 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=91660b485a30bbed64793dbe904193d3
Content-Length=2275
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/info.php

Identification

OUTPUT

```
No Permissions-Policy headers were found on https://juice-shop-388277804329.us-west1.run.app/info.php
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/info.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
```

```
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 08:28:20 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=d1dec854dbe62de69a7b5ea639baba79
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4239
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/images/

Identification

OUTPUT

```
No Permissions-Policy headers were found on https://juice-shop-388277804329.us-west1.run.app/images/
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/images/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 00:57:42 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=fc3fee9e75c9304bb77fd657cb75393d
Content-Length=5991
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/soap/

Identification

OUTPUT

```
No Permissions-Policy headers were found on https://juice-shop-388277804329.us-west1.run.app/soap/
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/soap/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 01:24:49 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=00c8cab83d92eca2ba95785b966a73c5
Content-Length=4201
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/passwords/

Identification

OUTPUT

```
No Permissions-Policy headers were found on https://juice-shop-388277804329.us-west1.run.app/passwords/
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/passwords/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
```

```
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 01:15:47 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=23cbd446a1bfac87a66163e22db42b14
Content-Length=2204
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/soap/class.wsdlcache.php

Identification

OUTPUT

```
No Permissions-Policy headers were found on https://juice-shop-388277804329.us-west1.run.app/soap/class.wsdlcache.php
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/soap/class.wsdlcache.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type=text/html
Date=Tue, 19 Nov 2024 06:59:07 GMT
Server=Google Frontend
X-Cloud-Trace-Context=7cb98e8601bf9fb1d2977a54ea93f5f7
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=811
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/passwords/wp-config.bak

Identification

OUTPUT

```
No Permissions-Policy headers were found on https://juice-shop-388277804329.us-west1.run.app/passwords/wp-config.bak
```

HTTP Info

REQUEST MADE

```
GET /passwords/wp-config.bak HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 200
last-modified: Wed, 13 Nov 2024 02:15:28 GMT
etag: "603-626c1e84a7000"
accept-ranges: bytes
content-type: application/x-trash
x-cloud-trace-context: bccbdb7c061d2d5009d67b2ae3eb5bac
date: Tue, 19 Nov 2024 06:12:37 GMT
server: Google Frontend
content-length: 1539
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/soap/class.soap_fault.php

Identification

OUTPUT

```
No Permissions-Policy headers were found on https://juice-shop-388277804329.us-west1.run.app/soap/class.soap_fault.php
```

HTTP Info

REQUEST MADE

```
GET /soap/class.soap_fault.php HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 500
x-powered-by: PHP/5.5.9-1ubuntu4.14
content-type: text/html
x-cloud-trace-context: 85c8d444051c598a5636d47e2436b1d1
date: Tue, 19 Nov 2024 06:54:58 GMT
server: Google Frontend
content-length: 0
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/phpinfo.php

Identification

OUTPUT

```
No Permissions-Policy headers were found on https://juice-shop-388277804329.us-west1.run.app/phpinfo.php
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/phpinfo.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 01:43:29 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=036c4d5909306dec6b8d0193b59d617a
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=85702
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/apps/movie_search

Identification

OUTPUT

```
No Permissions-Policy headers were found on https://juice-shop-388277804329.us-west1.run.app/apps/movie_search
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/apps/movie_search
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Arch=""
```

```
Sec-Ch-Ua-Bitness=""
Sec-Ch-Ua-Full-Version-List="Chromium", "HeadlessChrome", "Not-A.Brand";v="99.0.0.0"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Model=""
Sec-Ch-Ua-Platform="Linux"
Sec-Ch-Ua-Platform-Version=""
Sec-Ch-Ua-Wow64=?0
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Accept-Ranges=bytes
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type=text/html
Date=Tue, 19 Nov 2024 03:18:44 GMT
Etag="d9a7-626c1e84a7000"
Last-Modified=Wed, 13 Nov 2024 02:15:28 GMT
Server=Google Frontend
X-Cloud-Trace-Context=4a149f49b940643dfb9c9bcafe0604bb
Content-Length=55719
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/db/bwapp.sqlite

Identification

OUTPUT

```
No Permissions-Policy headers were found on https://juice-shop-388277804329.us-west1.run.app/db/bwapp.sqlite
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/db/bwapp.sqlite
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Accept-Ranges=bytes
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type=text/html
Date=Tue, 19 Nov 2024 03:57:01 GMT
Etag="3000-626c1e84a7000"
Last-Modified=Wed, 13 Nov 2024 02:15:28 GMT
Server=Google Frontend
```

```
X-Cloud-Trace-Context=2a74d2d814c14512fd8fac93e4bfc679
Content-Length=12288
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/passwords/heroes.xml

Identification

OUTPUT

```
No Permissions-Policy headers were found on https://juice-shop-388277804329.us-west1.run.app/passwords/heroes.xml
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/passwords/heroes.xml
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
H3 200
Accept-Ranges=bytes
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=application/xml
Date=Tue, 19 Nov 2024 06:00:20 GMT
Etag="4b8-626c1e84a7000-gzip"
Last-Modified=Wed, 13 Nov 2024 02:15:28 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=d0db3cb698fff35d3398f6d368ed869f
Content-Length=433
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/soap/nusoap.php

Identification

OUTPUT

```
No Permissions-Policy headers were found on https://juice-shop-388277804329.us-west1.run.app/soap/nusoap.php
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/soap/nusoap.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type=text/html
Date=Tue, 19 Nov 2024 07:07:36 GMT
Server=Google Frontend
X-Cloud-Trace-Context=9b95efa061e2e33130bff09373a821c4
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=811
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/apps/

Identification

OUTPUT

```
No Permissions-Policy headers were found on https://juice-shop-388277804329.us-west1.run.app/apps/
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/apps/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 00:30:17 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=b57b66949c25563ad77a69e4a354af47
```

```
Content-Length=1782
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/login.php

Identification

OUTPUT

```
No Permissions-Policy headers were found on https://juice-shop-388277804329.us-west1.run.app/login.php
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/login.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control=no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 01:51:06 GMT
Expires=Thu, 19 Nov 1981 08:52:00 GMT
Pragma=no-cache
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=97249a7d3363c12f26d1d625a5fdf4df
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4826
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/user_new.php

Identification

OUTPUT

```
No Permissions-Policy headers were found on https://juice-shop-388277804329.us-west1.run.app/user_new.php
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/user_new.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 07:45:52 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=1de28a3c31c89c397b35ab9cf352eeaf
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4224
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/passwords/web.config.bak

Identification

OUTPUT

```
No Permissions-Policy headers were found on https://juice-shop-388277804329.us-west1.run.app/passwords/web.config.bak
```

HTTP Info

REQUEST MADE

```
GET /passwords/web.config.bak HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 200
last-modified: Wed, 13 Nov 2024 02:15:28 GMT
etag: "1d84-626c1e84a7000"
accept-ranges: bytes
content-type: application/x-trash
x-cloud-trace-context: dd8a0753fe21b8d0d381c2313f0202d5
date: Tue, 19 Nov 2024 06:08:24 GMT
server: Google Frontend
content-length: 7556
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/training.php

Identification

OUTPUT

```
No Permissions-Policy headers were found on https://juice-shop-388277804329.us-west1.run.app/training.php
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/training.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 08:36:37 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=beee281846f3b9b9397b531ce1a92fef
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4656
```

Missing Referrer Policy

VULNERABILITY INFO PLUGIN ID 98527

Description

Referrer Policy provides mechanisms to websites to restrict referrer information (sent in the referer header) that browsers will be allowed to add.

No Referrer Policy header or metatag configuration has been detected.

Solution

Configure Referrer Policy on your website by adding 'Referrer-Policy' HTTP header or meta tag referrer in HTML.

See Also

https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy

Plugin Details

PUBLICATION DATE	2019-04-02T00:00:00+00:00
MODIFICATION DATE	2024-03-25T00:00:00+00:00
FAMILY	HTTP Security Header
SEVERITY	Info
PLUGIN ID	98527

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

Missing Referrer Policy Instances (25)

VULNERABILITY INFO PLUGIN ID 98527

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/passwords/wp-config.bak

Identification

OUTPUT

```
No Referrer-Policy headers or body meta tags were found on https://juice-shop-388277804329.us-west1.run.app/passwords
/wp-config.bak
```

HTTP Info

REQUEST MADE

```
GET /passwords/wp-config.bak HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 200
last-modified: Wed, 13 Nov 2024 02:15:28 GMT
etag: "603-626c1e84a7000"
accept-ranges: bytes
content-type: application/x-trash
x-cloud-trace-context: bccbdb7c061d2d5009d67b2ae3eb5bac
date: Tue, 19 Nov 2024 06:12:37 GMT
server: Google Frontend
content-length: 1539
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/user_new.php

Identification

OUTPUT

```
No Referrer-Policy headers or body meta tags were found on https://juice-shop-388277804329.us-west1.run.app/user_new.php
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/user_new.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
```

```
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 07:45:52 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=1de28a3c31c89c397b35ab9cf352eeaf
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4224
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/soap/class.nusoap_base.php

Identification

OUTPUT

```
No Referrer-Policy headers or body meta tags were found on https://juice-shop-388277804329.us-west1.run.app/soap/class.
nusoap_base.php
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/soap/class.nusoap_base.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type=text/html
Date=Tue, 19 Nov 2024 06:46:36 GMT
Server=Google Frontend
X-Cloud-Trace-Context=c53cd0b0ef8c298766ed3c1bd61168b7
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=811
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/soap/class.wsdlcache.php

Identification

OUTPUT

```
No Referrer-Policy headers or body meta tags were found on https://juice-shop-388277804329.us-west1.run.app/soap/class.
wsdlcache.php
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/soap/class.wsdlcache.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type=text/html
Date=Tue, 19 Nov 2024 06:59:07 GMT
Server=Google Frontend
X-Cloud-Trace-Context=7cb98e8601bf9fb1d2977a54ea93f5f7
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=811
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/passwords/web.config.bak

Identification

OUTPUT

```
No Referrer-Policy headers or body meta tags were found on https://juice-shop-388277804329.us-west1.run.app/passwords
/web.config.bak
```

HTTP Info

REQUEST MADE

```
GET /passwords/web.config.bak HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 200
last-modified: Wed, 13 Nov 2024 02:15:28 GMT
etag: "1d84-626c1e84a7000"
accept-ranges: bytes
content-type: application/x-trash
x-cloud-trace-context: dd8a0753fe21b8d0d381c2313f0202d5
date: Tue, 19 Nov 2024 06:08:24 GMT
server: Google Frontend
content-length: 7556
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/soap/

Identification

OUTPUT

```
No Referrer-Policy headers or body meta tags were found on https://juice-shop-388277804329.us-west1.run.app/soap/
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/soap/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 01:24:49 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=00c8cab83d92eca2ba95785b966a73c5
Content-Length=4201
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/passwords/

Identification

OUTPUT

```
No Referrer-Policy headers or body meta tags were found on https://juice-shop-388277804329.us-west1.run.app/passwords/
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/passwords/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 01:15:47 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=23cbd446a1bfac87a66163e22db42b14
Content-Length=2204
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/db/

Identification

OUTPUT

```
No Referrer-Policy headers or body meta tags were found on https://juice-shop-388277804329.us-west1.run.app/db/
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/db/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 00:39:25 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=7330f8397d6d6ed7b0975d370f2d06ee
Content-Length=1778
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/info_install.php

Identification

OUTPUT

```
No Referrer-Policy headers or body meta tags were found on https://juice-shop-388277804329.us-west1.run.app
/info_install.php
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/info_install.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Arch=""
Sec-Ch-Ua-Bitness=""
Sec-Ch-Ua-Full-Version-List="Chromium", "HeadlessChrome", "Not-A.Brand";v="99.0.0.0"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Model=""
Sec-Ch-Ua-Platform="Linux"
Sec-Ch-Ua-Platform-Version=""
Sec-Ch-Ua-Wow64=?0
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 02:21:07 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=3305fabc85563bee1adce5fca1986cef
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4188
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/soap/class.soap_fault.php

Identification

OUTPUT

```
No Referrer-Policy headers or body meta tags were found on https://juice-shop-388277804329.us-west1.run.app/soap/class.
soap_fault.php
```

HTTP Info

REQUEST MADE

```
GET /soap/class.soap_fault.php HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 500
x-powered-by: PHP/5.5.9-1ubuntu4.14
content-type: text/html
x-cloud-trace-context: 85c8d444051c598a5636d47e2436b1d1
date: Tue, 19 Nov 2024 06:54:58 GMT
server: Google Frontend
content-length: 0
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/training_install.php

Identification

OUTPUT

```
No Referrer-Policy headers or body meta tags were found on https://juice-shop-388277804329.us-west1.run.app
/training_install.php
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/training_install.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 02:31:16 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=dc248926d66de31d4ae1d4212ab637d0
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4629
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/soap/nusoap.php

Identification

OUTPUT

```
No Referrer-Policy headers or body meta tags were found on https://juice-shop-388277804329.us-west1.run.app/soap/nusoap.
php
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/soap/nusoap.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type=text/html
Date=Tue, 19 Nov 2024 07:07:36 GMT
Server=Google Frontend
X-Cloud-Trace-Context=9b95efa061e2e33130bff09373a821c4
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=811
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/passwords/heroes.xml

Identification

OUTPUT

```
No Referrer-Policy headers or body meta tags were found on https://juice-shop-388277804329.us-west1.run.app/passwords
/heroes.xml
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/passwords/heroes.xml
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
H3 200
Accept-Ranges=bytes
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=application/xml
Date=Tue, 19 Nov 2024 06:00:20 GMT
Etag="4b8-626c1e84a7000-gzip"
Last-Modified=Wed, 13 Nov 2024 02:15:28 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=d0db3cb698fff35d3398f6d368ed869f
Content-Length=433
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/images/

Identification

OUTPUT

```
No Referrer-Policy headers or body meta tags were found on https://juice-shop-388277804329.us-west1.run.app/images/
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/images/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 00:57:42 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=fc3fee9e75c9304bb77fd657cb75393d
Content-Length=5991
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/login.php

Identification

OUTPUT

```
No Referrer-Policy headers or body meta tags were found on https://juice-shop-388277804329.us-west1.run.app/login.php
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/login.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control=no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 01:51:06 GMT
Expires=Thu, 19 Nov 1981 08:52:00 GMT
Pragma=no-cache
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=97249a7d3363c12f26d1d625a5fdf4df
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4826
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/training.php

Identification

OUTPUT

```
No Referrer-Policy headers or body meta tags were found on https://juice-shop-388277804329.us-west1.run.app/training.php
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/training.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 08:36:37 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=beee281846f3b9b9397b531ce1a92fef
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4656
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/js/

Identification

OUTPUT

```
No Referrer-Policy headers or body meta tags were found on https://juice-shop-388277804329.us-west1.run.app/js/
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/js/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
```

```
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 01:06:45 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=92dbc4630193c57aa70de731a23c4521
Content-Length=2393
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/info.php

Identification

OUTPUT

```
No Referrer-Policy headers or body meta tags were found on https://juice-shop-388277804329.us-west1.run.app/info.php
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/info.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 08:28:20 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=d1dec854dbe62de69a7b5ea639baba79
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4239
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/phpinfo.php

Identification

OUTPUT

```
No Referrer-Policy headers or body meta tags were found on https://juice-shop-388277804329.us-west1.run.app/phpinfo.php
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/phpinfo.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 01:43:29 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=036c4d5909306dec6b8d0193b59d617a
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=85702
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/db/bwapp.sqlite

Identification

OUTPUT

```
No Referrer-Policy headers or body meta tags were found on https://juice-shop-388277804329.us-west1.run.app/db/bwapp.
sqlite
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/db/bwapp.sqlite
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
```

```
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Accept-Ranges=bytes
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type=text/html
Date=Tue, 19 Nov 2024 03:57:01 GMT
Etag="3000-626c1e84a7000"
Last-Modified=Wed, 13 Nov 2024 02:15:28 GMT
Server=Google Frontend
X-Cloud-Trace-Context=2a74d2d814c14512fd8fac93e4bfc679
Content-Length=12288
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/documents/

Identification

OUTPUT

```
No Referrer-Policy headers or body meta tags were found on https://juice-shop-388277804329.us-west1.run.app/documents/
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/documents/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 00:48:33 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=8659790f61386a0d355111f26ee2a386
Content-Length=3149
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/apps/

Identification

OUTPUT

```
No Referrer-Policy headers or body meta tags were found on https://juice-shop-388277804329.us-west1.run.app/apps/
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/apps/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 00:30:17 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=b57b66949c25563ad77a69e4a354af47
Content-Length=1782
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/install.php

Identification

OUTPUT

```
No Referrer-Policy headers or body meta tags were found on https://juice-shop-388277804329.us-west1.run.app/install.php
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/install.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Arch=""
Sec-Ch-Ua-Bitness=""
Sec-Ch-Ua-Full-Version-List="Chromium", "HeadlessChrome", "Not-A.Brand";v="99.0.0.0"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Model=""
```

```
Sec-Ch-Ua-Platform="Linux"
Sec-Ch-Ua-Platform-Version=""
Sec-Ch-Ua-Wow64=?0
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 00:19:04 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=793633ff205741c27021c36f1f4362a8
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=3083
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/apps/movie_search

Identification

OUTPUT

```
No Referrer-Policy headers or body meta tags were found on https://juice-shop-388277804329.us-west1.run.app/apps
/movie_search
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/apps/movie_search
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Arch=""
Sec-Ch-Ua-Bitness=""
Sec-Ch-Ua-Full-Version-List="Chromium", "HeadlessChrome", "Not-A.Brand";v="99.0.0.0"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Model=""
Sec-Ch-Ua-Platform="Linux"
Sec-Ch-Ua-Platform-Version=""
Sec-Ch-Ua-Wow64=?0
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Accept-Ranges=bytes
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type=text/html
Date=Tue, 19 Nov 2024 03:18:44 GMT
```

```
Etag="d9a7-626c1e84a7000"
Last-Modified=Wed, 13 Nov 2024 02:15:28 GMT
Server=Google Frontend
X-Cloud-Trace-Context=4a149f49b940643dfb9c9bcafe0604bb
Content-Length=55719
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/stylesheets/

Identification

OUTPUT

```
No Referrer-Policy headers or body meta tags were found on https://juice-shop-388277804329.us-west1.run.app/stylesheets/
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/stylesheets/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 01:34:22 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=91660b485a30bbed64793dbe904193d3
Content-Length=2275
```

Robots.txt File Detected

VULNERABILITY INFO PLUGIN ID 98705

Description

The remote host contains a file named 'robots.txt' that is intended to prevent web 'robots' from visiting certain directories in a website for maintenance or indexing purposes. A malicious user may also be able to use the contents of this file to learn of sensitive documents or directories on the affected site and either retrieve them directly or target them for other attacks.

Solution

Review the contents of the site's robots.txt file, use Robots META tags instead of entries in the robots.txt file, and/or adjust the web server's access controls to limit access to sensitive material.

See Also

https://www.robotstxt.org

Plugin Details

PUBLICATION DATE	2019-09-19T00:00:00+00:00
MODIFICATION DATE	2020-12-17T00:00:00+00:00
FAMILY	Web Servers
SEVERITY	Info
PLUGIN ID	98705

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

Robots.txt File Detected Instances (1)

VULNERABILITY INFO PLUGIN ID 98705

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/robots.txt

Identification

OUTPUT

```
A robots.txt file was detected at 'https://juice-shop-388277804329.us-west1.run.app/robots.txt'.
```

HTTP Info

REQUEST MADE

```
GET /robots.txt HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
```

RESPONSE HEADERS

```
HTTP/2 200
last-modified: Wed, 13 Nov 2024 02:15:28 GMT
etag: "a7-626c1e84a7000-gzip"
accept-ranges: bytes
vary: Accept-Encoding
content-type: text/plain
content-encoding: gzip
x-cloud-trace-context: 254908cf9b3dd329fb06f688b5d60e42
date: Tue, 19 Nov 2024 00:11:23 GMT
server: Google Frontend
content-length: 102
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

SSL/TLS Certificate Information

VULNERABILITY INFO PLUGIN ID 112491

Description

This plugin displays information about the X.509 certificate extracted from the HTTPS connection.

Solution

-

See Also

Plugin Details

PUBLICATION DATE	2018-10-03T00:00:00+00:00
MODIFICATION DATE	2023-05-05T00:00:00+00:00
FAMILY	SSL/TLS
SEVERITY	Info
PLUGIN ID	112491

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

SSL/TLS Certificate Information Instances (1)

VULNERABILITY INFO PLUGIN ID 112491

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/#/

Identification

OUTPUT

```
Certificate 1
--------------
Common Name: *.a.run.app
Alternative Names: *.a.run.app run.app *.africa-south1.run.app *.asia-east1.run.app *.asia-east2.run.app *.asia-
northeast1.run.app *.asia-northeast2.run.app *.asia-northeast3.run.app *.asia-south1.run.app *.asia-south2.run.app *.
asia-southeast1.run.app *.asia-southeast2.run.app *.australia-southeast1.run.app *.australia-southeast2.run.app *.
europe-central2.run.app *.europe-north1.run.app *.europe-north2.run.app *.europe-southwest1.run.app *.europe-west1.run.
app *.europe-west10.run.app *.europe-west12.run.app *.europe-west2.run.app *.europe-west3.run.app *.europe-west4.run.
app *.europe-west5.run.app *.europe-west6.run.app *.europe-west8.run.app *.europe-west9.run.app *.me-central1.run.app *.
me-central2.run.app *.me-west1.run.app *.northamerica-northeast1.run.app *.northamerica-northeast2.run.app *.
northamerica-south1.run.app *.southamerica-east1.run.app *.southamerica-west1.run.app *.us-central1.run.app *.us-
central2.run.app *.us-east1.run.app *.us-east4.run.app *.us-east5.run.app *.us-east7.run.app *.us-south1.run.app *.us-
west1.run.app *.us-west2.run.app *.us-west3.run.app *.us-west4.run.app *.us-west8.run.app
Issuer: Google Trust Services
Valid from: 2024-10-21 08:36:39 UTC
Valid until: 2025-01-13 08:36:38 UTC (expires in 1 month, 3 weeks, 3 days)
Validity Period: 83 days
Key: RSA 256-bit
Signature: sha256WithRSAEncryption

Certificate 2
--------------
Common Name: wr
Issuer: Google Trust Services LLC
Valid from: 2023-12-13 09:00:00 UTC
Valid until: 2029-02-20 14:00:00 UTC (expires in 4 years, 3 months, 2 days)
Validity Period: 1896 days
Key: RSA 2048-bit
Signature: sha256WithRSAEncryption

Certificate 3
--------------
Common Name: gts root r
Issuer: GlobalSign nv
Valid from: 2020-06-19 00:00:42 UTC
Valid until: 2028-01-28 00:00:42 UTC (expires in 3 years, 2 months, 1 week, 1 day)
Validity Period: 2779 days
Key: RSA 4096-bit
Signature: sha256WithRSAEncryption
```

Missing 'X-XSS-Protection' Header

VULNERABILITY INFO PLUGIN ID 112526

Description

The HTTP 'X-XSS-Protection' response header is a feature of old browsers that allows websites to control their XSS auditors. \n\nThe server is not configured to return a 'X-XSS-Protection' header which means that any pages on this website could be at risk of a Cross-Site Scripting (XSS) attack. This URL is flagged as a specific example.\n\nHowever, this header is deprecated by modern browsers, if legacy browsers support is not needed, it is recommended to use Content-Security-Policy without allowing unsafe-inline scripts instead.

Solution

Configure your web server to include an 'X-XSS-Protection' header with a value of '1; mode=block' on all pages.

See Also

https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-XSS-Protection
https://www.owasp.org/index.php/OWASP_Secure_Headers_Project#xxxsp

Plugin Details

PUBLICATION DATE	2018-11-27T00:00:00+00:00
MODIFICATION DATE	2024-03-25T00:00:00+00:00
FAMILY	HTTP Security Header
SEVERITY	Info
PLUGIN ID	112526

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

Missing 'X-XSS-Protection' Header Instances (25)

VULNERABILITY INFO PLUGIN ID 112526

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/documents/

Identification

OUTPUT

```
The scanner detected the lack of X-XSS-Protection header in the target application response.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/documents/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 00:48:33 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=8659790f61386a0d355111f26ee2a386
Content-Length=3149
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/phpinfo.php

Identification

OUTPUT

```
The scanner detected the lack of X-XSS-Protection header in the target application response.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/phpinfo.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 01:43:29 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=036c4d5909306dec6b8d0193b59d617a
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=85702
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/soap/class.soap_fault.php

Identification

OUTPUT

```
The scanner detected the lack of X-XSS-Protection header in the target application response.
```

HTTP Info

REQUEST MADE

```
GET /soap/class.soap_fault.php HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 500
x-powered-by: PHP/5.5.9-1ubuntu4.14
content-type: text/html
x-cloud-trace-context: 85c8d444051c598a5636d47e2436b1d1
date: Tue, 19 Nov 2024 06:54:58 GMT
server: Google Frontend
content-length: 0
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/soap/class.wsdlcache.php

Identification

OUTPUT

```
The scanner detected the lack of X-XSS-Protection header in the target application response.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/soap/class.wsdlcache.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type=text/html
Date=Tue, 19 Nov 2024 06:59:07 GMT
Server=Google Frontend
X-Cloud-Trace-Context=7cb98e8601bf9fb1d2977a54ea93f5f7
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=811
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/images/

Identification

OUTPUT

```
The scanner detected the lack of X-XSS-Protection header in the target application response.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/images/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
```

```
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 00:57:42 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=fc3fee9e75c9304bb77fd657cb75393d
Content-Length=5991
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/passwords/wp-config.bak

Identification

OUTPUT

```
The scanner detected the lack of X-XSS-Protection header in the target application response.
```

HTTP Info

REQUEST MADE

```
GET /passwords/wp-config.bak HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 200
last-modified: Wed, 13 Nov 2024 02:15:28 GMT
etag: "603-626c1e84a7000"
accept-ranges: bytes
content-type: application/x-trash
x-cloud-trace-context: bccbdb7c061d2d5009d67b2ae3eb5bac
date: Tue, 19 Nov 2024 06:12:37 GMT
server: Google Frontend
content-length: 1539
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/db/

Identification

OUTPUT

```
The scanner detected the lack of X-XSS-Protection header in the target application response.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/db/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 00:39:25 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=7330f8397d6d6ed7b0975d370f2d06ee
Content-Length=1778
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/apps/

Identification

OUTPUT

```
The scanner detected the lack of X-XSS-Protection header in the target application response.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/apps/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 00:30:17 GMT
```

```
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=b57b66949c25563ad77a69e4a354af47
Content-Length=1782
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/passwords/web.config.bak

Identification

OUTPUT

```
The scanner detected the lack of X-XSS-Protection header in the target application response.
```

HTTP Info

REQUEST MADE

```
GET /passwords/web.config.bak HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 200
last-modified: Wed, 13 Nov 2024 02:15:28 GMT
etag: "1d84-626c1e84a7000"
accept-ranges: bytes
content-type: application/x-trash
x-cloud-trace-context: dd8a0753fe21b8d0d381c2313f0202d5
date: Tue, 19 Nov 2024 06:08:24 GMT
server: Google Frontend
content-length: 7556
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/stylesheets/

Identification

OUTPUT

```
The scanner detected the lack of X-XSS-Protection header in the target application response.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/stylesheets/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
```

```
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 01:34:22 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=91660b485a30bbed64793dbe904193d3
Content-Length=2275
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/db/bwapp.sqlite

Identification

OUTPUT

```
The scanner detected the lack of X-XSS-Protection header in the target application response.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/db/bwapp.sqlite
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Accept-Ranges=bytes
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type=text/html
Date=Tue, 19 Nov 2024 03:57:01 GMT
Etag="3000-626c1e84a7000"
Last-Modified=Wed, 13 Nov 2024 02:15:28 GMT
Server=Google Frontend
X-Cloud-Trace-Context=2a74d2d814c14512fd8fac93e4bfc679
Content-Length=12288
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/training.php

Identification

OUTPUT

```
The scanner detected the lack of X-XSS-Protection header in the target application response.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/training.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 08:36:37 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=beee281846f3b9b9397b531ce1a92fef
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4656
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/soap/

Identification

OUTPUT

```
The scanner detected the lack of X-XSS-Protection header in the target application response.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/soap/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
```

```
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 01:24:49 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=00c8cab83d92eca2ba95785b966a73c5
Content-Length=4201
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/passwords/

Identification

OUTPUT

```
The scanner detected the lack of X-XSS-Protection header in the target application response.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/passwords/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 01:15:47 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=23cbd446a1bfac87a66163e22db42b14
Content-Length=2204
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/js/

Identification

OUTPUT

```
The scanner detected the lack of X-XSS-Protection header in the target application response.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/js/
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html;charset=UTF-8
Date=Tue, 19 Nov 2024 01:06:45 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=92dbc4630193c57aa70de731a23c4521
Content-Length=2393
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/login.php

Identification

OUTPUT

```
The scanner detected the lack of X-XSS-Protection header in the target application response.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/login.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
```

```
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control=no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 01:51:06 GMT
Expires=Thu, 19 Nov 1981 08:52:00 GMT
Pragma=no-cache
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=97249a7d3363c12f26d1d625a5fdf4df
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4826
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/user_new.php

Identification

OUTPUT

```
The scanner detected the lack of X-XSS-Protection header in the target application response.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/user_new.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 07:45:52 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=1de28a3c31c89c397b35ab9cf352eeaf
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4224
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/soap/nusoap.php

Identification

OUTPUT

```
The scanner detected the lack of X-XSS-Protection header in the target application response.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/soap/nusoap.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type=text/html
Date=Tue, 19 Nov 2024 07:07:36 GMT
Server=Google Frontend
X-Cloud-Trace-Context=9b95efa061e2e33130bff09373a821c4
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=811
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/soap/class.nusoap_base.php

Identification

OUTPUT

```
The scanner detected the lack of X-XSS-Protection header in the target application response.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/soap/class.nusoap_base.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
```

```
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type=text/html
Date=Tue, 19 Nov 2024 06:46:36 GMT
Server=Google Frontend
X-Cloud-Trace-Context=c53cd0b0ef8c298766ed3c1bd61168b7
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=811
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/apps/movie_search

Identification

OUTPUT

```
The scanner detected the lack of X-XSS-Protection header in the target application response.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/apps/movie_search
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Arch=""
Sec-Ch-Ua-Bitness=""
Sec-Ch-Ua-Full-Version-List="Chromium", "HeadlessChrome", "Not-A.Brand";v="99.0.0.0"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Model=""
Sec-Ch-Ua-Platform="Linux"
Sec-Ch-Ua-Platform-Version=""
Sec-Ch-Ua-Wow64=?0
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Accept-Ranges=bytes
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type=text/html
Date=Tue, 19 Nov 2024 03:18:44 GMT
Etag="d9a7-626c1e84a7000"
Last-Modified=Wed, 13 Nov 2024 02:15:28 GMT
Server=Google Frontend
X-Cloud-Trace-Context=4a149f49b940643dfb9c9bcafe0604bb
Content-Length=55719
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/training_install.php

Identification

OUTPUT

```
The scanner detected the lack of X-XSS-Protection header in the target application response.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/training_install.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 02:31:16 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=dc248926d66de31d4ae1d4212ab637d0
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4629
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/info_install.php

Identification

OUTPUT

```
The scanner detected the lack of X-XSS-Protection header in the target application response.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/info_install.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
```

```
Sec-Ch-Ua-Arch=""
Sec-Ch-Ua-Bitness=""
Sec-Ch-Ua-Full-Version-List="Chromium", "HeadlessChrome", "Not-A.Brand";v="99.0.0.0"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Model=""
Sec-Ch-Ua-Platform="Linux"
Sec-Ch-Ua-Platform-Version=""
Sec-Ch-Ua-Wow64=?0
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 02:21:07 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=3305fabc85563bee1adce5fca1986cef
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4188
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/info.php

Identification

OUTPUT

```
The scanner detected the lack of X-XSS-Protection header in the target application response.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/info.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 08:28:20 GMT
Server=Google Frontend
Vary=Accept-Encoding
```

```
X-Cloud-Trace-Context=d1dec854dbe62de69a7b5ea639baba79
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4239
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/install.php

Identification

OUTPUT

```
The scanner detected the lack of X-XSS-Protection header in the target application response.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/install.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Arch=""
Sec-Ch-Ua-Bitness=""
Sec-Ch-Ua-Full-Version-List="Chromium", "HeadlessChrome", "Not-A.Brand";v="99.0.0.0"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Model=""
Sec-Ch-Ua-Platform="Linux"
Sec-Ch-Ua-Platform-Version=""
Sec-Ch-Ua-Wow64=?0
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 00:19:04 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=793633ff205741c27021c36f1f4362a8
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=3083
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/passwords/heroes.xml

Identification

OUTPUT

```
The scanner detected the lack of X-XSS-Protection header in the target application response.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/passwords/heroes.xml
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
H3 200
Accept-Ranges=bytes
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=application/xml
Date=Tue, 19 Nov 2024 06:00:20 GMT
Etag="4b8-626c1e84a7000-gzip"
Last-Modified=Wed, 13 Nov 2024 02:15:28 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=d0db3cb698fff35d3398f6d368ed869f
Content-Length=433
```

SSL/TLS Versions Supported

VULNERABILITY INFO PLUGIN ID 112530

Description

This plugin displays information about the SSL/TLS versions supported by remote server for HTTPS connection.

Solution

-

See Also

https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml

Plugin Details

PUBLICATION DATE	2018-10-03T00:00:00+00:00
MODIFICATION DATE	2020-10-02T00:00:00+00:00
FAMILY	SSL/TLS
SEVERITY	Info
PLUGIN ID	112530

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

SSL/TLS Versions Supported Instances (1)

VULNERABILITY INFO PLUGIN ID 112530

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/#/

Identification

OUTPUT

```
Protocol Supported
---------------------
SSL 2.0 No
SSL 3.0 No
TLS 1.0 No
TLS 1.1 No
TLS 1.2 Yes
TLS 1.3 Yes
```

SSL/TLS Server Cipher Suite Preference Not Detected

VULNERABILITY INFO PLUGIN ID 112599

Description

The remote server is not configured with a SSL/TLS cipher suite preference list, making the cipher suite selection during the negotiation use the ordered list from the client.

Solution

-

See Also

http://www.exploresecurity.com/testing-for-cipher-suite-preference/
https://wiki.mozilla.org/Security/Server_Side_TLS

Plugin Details

PUBLICATION DATE	2020-09-24T00:00:00+00:00
MODIFICATION DATE	2021-08-25T00:00:00+00:00
FAMILY	SSL/TLS
SEVERITY	Info
PLUGIN ID	112599

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

SSL/TLS Server Cipher Suite Preference Not Detected Instances (1)

VULNERABILITY INFO PLUGIN ID 112599

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/#/

Identification

OUTPUT

```
The scanner detected that the remote host is not configured with a cipher suite preference for the following protocol
(s) : TLS v1.2, TLS v1.3
```

Allowed HTTP Versions

VULNERABILITY INFO PLUGIN ID 112613

Description

The Hypertext Transfer Protocol (HTTP) is the underlying protocol of the World Wide Web. Since its first release, HTTP has evolved to support modern web usages and currently exists in three versions:
- HTTP/1.0
- HTTP/1.1
- HTTP/2

The scanner identified the supported versions of the HTTP protocol on the target web application.

Solution

-

See Also

https://developer.mozilla.org/en-US/docs/Web/HTTP/Basics_of_HTTP/Evolution_of_HTTP

Plugin Details

PUBLICATION DATE	2020-10-13T00:00:00+00:00
MODIFICATION DATE	2023-01-17T00:00:00+00:00
FAMILY	Web Applications
SEVERITY	Info
PLUGIN ID	112613

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

Allowed HTTP Versions Instances (1)

VULNERABILITY INFO PLUGIN ID 112613

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/#/

Identification

OUTPUT

```
The scanner detected the following HTTP versions on the target application :

- HTTP/1.0
- HTTP/1.1
- HTTP/2

The list of requests and responses observed is provided in attachment.
```

Security.txt File Not Detected

VULNERABILITY INFO PLUGIN ID 112723

Description

A Security.txt file has not been detected on the target.

When security risks in web services are discovered by independent security researchers, this file defines the channels to disclose them properly & enables 3rd party researchers to disclose issues securely in a manner defined by the organization.

Organizations should consider creating a security.txt file containing contact and other information in the defined format and place it under the .well-known directory of the server.

Solution

-

See Also

https://securitytxt.org/
https://tools.ietf.org/html/draft-foudil-securitytxt-11

Plugin Details

PUBLICATION DATE	2021-03-17T00:00:00+00:00
MODIFICATION DATE	2021-03-17T00:00:00+00:00
FAMILY	Web Servers
SEVERITY	Info
PLUGIN ID	112723

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

Security.txt File Not Detected Instances (1)

VULNERABILITY INFO PLUGIN ID 112723

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/.well-known/security.txt

Identification

OUTPUT

```
No or a malformed security.txt was found at 'https://juice-shop-388277804329.us-west1.run.app/.well-known/security.txt'.
```

HTTP Info

REQUEST MADE

```
GET /.well-known/security.txt HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
```

RESPONSE HEADERS

```
HTTP/2 404
content-type: text/html; charset=iso-8859-1
x-cloud-trace-context: 38b4de5541ac2e0d3c96ad261354853f
date: Tue, 19 Nov 2024 00:11:23 GMT
server: Google Frontend
content-length: 327
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

SSL/TLS Certificate Contains Wildcard Entries

VULNERABILITY INFO PLUGIN ID 113045

Description

The remote server presents an SSL/TLS certificate with wildcard entries. The use of a wildcard character in a entry permits a certificate to cover a number of subdomains of a domain.

Solution

-

See Also

Plugin Details

PUBLICATION DATE	2021-11-10T00:00:00+00:00
MODIFICATION DATE	2021-11-10T00:00:00+00:00
FAMILY	SSL/TLS
SEVERITY	Info
PLUGIN ID	113045

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

SSL/TLS Certificate Contains Wildcard Entries Instances (1)

VULNERABILITY INFO PLUGIN ID 113045

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/#/

Identification

OUTPUT

```
A wildcard symbol (*) has been detected in the following certificate entries:
Certificate Common Name: *.a.run.app
Certificate Subject Alternative Names:
- *.a.run.app
- *.africa-south1.run.app
- *.asia-east1.run.app
- *.asia-east2.run.app
- *.asia-northeast1.run.app
- *.asia-northeast2.run.app
- *.asia-northeast3.run.app
- *.asia-south1.run.app
- *.asia-south2.run.app
- *.asia-southeast1.run.app
- *.asia-southeast2.run.app
- *.australia-southeast1.run.app
- *.australia-southeast2.run.app
- *.europe-central2.run.app
- *.europe-north1.run.app
- *.europe-north2.run.app
- *.europe-southwest1.run.app
- *.europe-west1.run.app
- *.europe-west10.run.app
- *.europe-west12.run.app
- *.europe-west2.run.app
- *.europe-west3.run.app
- *.europe-west4.run.app
- *.europe-west5.run.app
- *.europe-west6.run.app
- *.europe-west8.run.app
- *.europe-west9.run.app
- *.me-central1.run.app
- *.me-central2.run.app
- *.me-west1.run.app
- *.northamerica-northeast1.run.app
- *.northamerica-northeast2.run.app
- *.northamerica-south1.run.app
- *.southamerica-east1.run.app
- *.southamerica-west1.run.app
- *.us-central1.run.app
- *.us-central2.run.app
- *.us-east1.run.app
- *.us-east4.run.app
- *.us-east5.run.app
- *.us-east7.run.app
- *.us-south1.run.app
- *.us-west1.run.app
- *.us-west2.run.app
- *.us-west3.run.app
- *.us-west4.run.app
- *.us-west8.run.app
```

Performance Telemetry

VULNERABILITY INFO PLUGIN ID 113393

Description

This finding provides information to assist in scan performance tuning.

Solution

-

See Also

Plugin Details

PUBLICATION DATE	2022-10-17T00:00:00+00:00
MODIFICATION DATE	2024-10-03T00:00:00+00:00
FAMILY	General
SEVERITY	Info
PLUGIN ID	113393

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

Performance Telemetry Instances (1)

VULNERABILITY INFO PLUGIN ID 113393

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/#/

Identification

OUTPUT

```
Three attachments are included in this finding to assist in performance tuning of your scan:
-pages_telemetry.csv: Scan statistics organized by page
-plugins_telemetry.csv: Scan statistics organized by plugin
-time_telemetry.csv: Chronological scan statistics
```

HTML Comments Detected

VULNERABILITY INFO PLUGIN ID 113897

Description

HTML comments are often used by developers to include information related to the application inline, which are ignored by a clients browser during rendering. These comments may include sensitive information such as SQL queries, credentials or internal IP for example.

Solution

Review the HTML comments identified on the page for any information leakage, and remove any sensitive information identified.

See Also

https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/05-Review_Webpage_Content_for_Information_Leakage

Plugin Details

PUBLICATION DATE	2023-06-09T00:00:00+00:00
MODIFICATION DATE	2024-11-08T00:00:00+00:00
FAMILY	Data Exposure
SEVERITY	Info
PLUGIN ID	113897

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

HTML Comments Detected Instances (9)

VULNERABILITY INFO PLUGIN ID 113897

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/install.php?install=yes

Identification

OUTPUT

```
2 HTML comments have been detected in the application HTTP response. Please see the attachment for further details.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/install.php?install=yes
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 02:39:05 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=b8eba21cccffcc35373450a248516ba1
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=3085
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/db/bwapp.sqlite

Identification

OUTPUT

```
2 HTML comments have been detected in the application HTTP response. Please see the attachment for further details.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/db/bwapp.sqlite
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Accept-Ranges=bytes
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type=text/html
Date=Tue, 19 Nov 2024 03:57:01 GMT
Etag="3000-626c1e84a7000"
Last-Modified=Wed, 13 Nov 2024 02:15:28 GMT
Server=Google Frontend
X-Cloud-Trace-Context=2a74d2d814c14512fd8fac93e4bfc679
Content-Length=12288
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/training_install.php

Identification

OUTPUT

```
2 HTML comments have been detected in the application HTTP response. Please see the attachment for further details.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/training_install.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 02:31:16 GMT
Server=Google Frontend
```

```
Vary=Accept-Encoding
X-Cloud-Trace-Context=dc248926d66de31d4ae1d4212ab637d0
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4629
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/info_install.php

Identification

OUTPUT

```
2 HTML comments have been detected in the application HTTP response. Please see the attachment for further details.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/info_install.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Arch=""
Sec-Ch-Ua-Bitness=""
Sec-Ch-Ua-Full-Version-List="Chromium", "HeadlessChrome", "Not-A.Brand";v="99.0.0.0"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Model=""
Sec-Ch-Ua-Platform="Linux"
Sec-Ch-Ua-Platform-Version=""
Sec-Ch-Ua-Wow64=?0
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 02:21:07 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=3305fabc85563bee1adce5fca1986cef
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4188
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/install.php

Identification

OUTPUT

```
2 HTML comments have been detected in the application HTTP response. Please see the attachment for further details.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/install.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Arch=""
Sec-Ch-Ua-Bitness=""
Sec-Ch-Ua-Full-Version-List="Chromium", "HeadlessChrome", "Not-A.Brand";v="99.0.0.0"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Model=""
Sec-Ch-Ua-Platform="Linux"
Sec-Ch-Ua-Platform-Version=""
Sec-Ch-Ua-Wow64=?0
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 00:19:04 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=793633ff205741c27021c36f1f4362a8
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=3083
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/login.php

Identification

OUTPUT

```
2 HTML comments have been detected in the application HTTP response. Please see the attachment for further details.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/login.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
```

```
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control=no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 01:51:06 GMT
Expires=Thu, 19 Nov 1981 08:52:00 GMT
Pragma=no-cache
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=97249a7d3363c12f26d1d625a5fdf4df
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4826
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/info.php

Identification

OUTPUT

```
2 HTML comments have been detected in the application HTTP response. Please see the attachment for further details.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/info.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 08:28:20 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=d1dec854dbe62de69a7b5ea639baba79
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4239
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/training.php

Identification

OUTPUT

```
2 HTML comments have been detected in the application HTTP response. Please see the attachment for further details.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/training.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 08:36:37 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=beee281846f3b9b9397b531ce1a92fef
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4656
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/user_new.php

Identification

OUTPUT

```
2 HTML comments have been detected in the application HTTP response. Please see the attachment for further details.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/user_new.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
```

```
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 07:45:52 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=1de28a3c31c89c397b35ab9cf352eeaf
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4224
```

Input Reflected

VULNERABILITY INFO PLUGIN ID 114135

Description

This is an informational plugin to inform that user data controlled input is reflected in the response.

Solution

-

See Also
https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html

Plugin Details

PUBLICATION DATE	2023-12-18T00:00:00+00:00
MODIFICATION DATE	2023-12-18T00:00:00+00:00
FAMILY	Injection
SEVERITY	Info
PLUGIN ID	114135

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

Input Reflected Instances (19)

VULNERABILITY INFO PLUGIN ID 114135

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/phpinfo.php

INPUT TYPE	cookie
INPUT NAME	PHPSESSID

Identification

PAYLOAD

```
was-tnb-hsv
```

PROOF

```
Input reflected in the response body : 'was-tnb-hsv'.
```

OUTPUT

```
The scanner was able to detect an input reflected in the response body.
```

HTTP Info

REQUEST MADE

```
GET /phpinfo.php HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=was-tnb-hsv
```

RESPONSE HEADERS

```
HTTP/2 200
x-powered-by: PHP/5.5.9-1ubuntu4.14
vary: Accept-Encoding
content-type: text/html
content-encoding: gzip
x-cloud-trace-context: 4b33b4fe743d33dc598474a645a4a9c9
date: Tue, 19 Nov 2024 01:44:48 GMT
server: Google Frontend
content-length: 19009
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/phpinfo.php

INPUT TYPE	header
INPUT NAME	Sec-Fetch-User

Identification

PAYLOAD

```
was-tnb-hsv
```

PROOF

```
Input reflected in the response body : 'was-tnb-hsv'.
```

OUTPUT

```
The scanner was able to detect an input reflected in the response body.
```

HTTP Info

REQUEST MADE

```
GET /phpinfo.php HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Sec-Fetch-User: was-tnb-hsv
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 200
x-powered-by: PHP/5.5.9-1ubuntu4.14
vary: Accept-Encoding
content-type: text/html
content-encoding: gzip
x-cloud-trace-context: 9edc63b81b036d20bcb03073582961e9
date: Tue, 19 Nov 2024 01:44:53 GMT
server: Google Frontend
content-length: 19083
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/phpinfo.php

INPUT TYPE	header
INPUT NAME	Accept-Charset

Identification

PAYLOAD

```
was-tnb-hsv
```

PROOF

```
Input reflected in the response body : 'was-tnb-hsv'.
```

OUTPUT

```
The scanner was able to detect an input reflected in the response body.
```

HTTP Info

REQUEST MADE

```
GET /phpinfo.php HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
```

```
Accept-Charset: was-tnb-hsv
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 200
x-powered-by: PHP/5.5.9-1ubuntu4.14
vary: Accept-Encoding
content-type: text/html
content-encoding: gzip
x-cloud-trace-context: 2d1a41bc8c84029c1e3b1609d8b5dfe7
date: Tue, 19 Nov 2024 01:44:49 GMT
server: Google Frontend
content-length: 19075
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/phpinfo.php

INPUT TYPE	header
INPUT NAME	Sec-Ch-Ua

Identification

PAYLOAD

```
was-tnb-hsv
```

PROOF

```
Input reflected in the response body : 'was-tnb-hsv'.
```

OUTPUT

```
The scanner was able to detect an input reflected in the response body.
```

HTTP Info

REQUEST MADE

```
GET /phpinfo.php HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Sec-Ch-Ua: was-tnb-hsv
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 200
x-powered-by: PHP/5.5.9-1ubuntu4.14
vary: Accept-Encoding
content-type: text/html
content-encoding: gzip
x-cloud-trace-context: 443d1475fc03f23cacb38eff2400ce4d
date: Tue, 19 Nov 2024 01:44:51 GMT
server: Google Frontend
content-length: 19086
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/phpinfo.php

INPUT TYPE	header
INPUT NAME	Sec-Ch-Ua-Platform

Identification

PAYLOAD

```
was-tnb-hsv
```

PROOF

```
Input reflected in the response body : 'was-tnb-hsv'.
```

OUTPUT

```
The scanner was able to detect an input reflected in the response body.
```

HTTP Info

REQUEST MADE

```
GET /phpinfo.php HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Sec-Ch-Ua-Platform: was-tnb-hsv
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 200
x-powered-by: PHP/5.5.9-1ubuntu4.14
vary: Accept-Encoding
content-type: text/html
content-encoding: gzip
x-cloud-trace-context: 45d02a0089b88bf1fda49b86c99bf4ec
date: Tue, 19 Nov 2024 01:44:51 GMT
server: Google Frontend
content-length: 19106
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/phpinfo.php

INPUT TYPE	header
INPUT NAME	Accept-Encoding

Identification

PAYLOAD

```
was-tnb-hsv
```

PROOF

```
Input reflected in the response body : 'was-tnb-hsv'.
```

OUTPUT

```
The scanner was able to detect an input reflected in the response body.
```

HTTP Info

REQUEST MADE

```
GET /phpinfo.php HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: was-tnb-hsv
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 200
x-powered-by: PHP/5.5.9-1ubuntu4.14
vary: Accept-Encoding
content-type: text/html
date: Tue, 19 Nov 2024 01:44:49 GMT
server: Google Frontend
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/phpinfo.php

INPUT TYPE	header
INPUT NAME	Sec-Fetch-Mode

Identification

PAYLOAD

```
was-tnb-hsv
```

PROOF

```
Input reflected in the response body : 'was-tnb-hsv'.
```

OUTPUT

```
The scanner was able to detect an input reflected in the response body.
```

HTTP Info

REQUEST MADE

```
GET /phpinfo.php HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Sec-Fetch-Mode: was-tnb-hsv
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 200
x-powered-by: PHP/5.5.9-1ubuntu4.14
vary: Accept-Encoding
content-type: text/html
content-encoding: gzip
x-cloud-trace-context: 44621a89430473c6f5bb7291f6d24247
date: Tue, 19 Nov 2024 01:44:53 GMT
```

```
server: Google Frontend
content-length: 19093
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/phpinfo.php

INPUT TYPE	cookie
INPUT NAME	was-tnb-hsv

Identification

PAYLOAD

```
was-tnb-hsv
```

PROOF

```
Input reflected in the response body : 'was-tnb-hsv'.
```

OUTPUT

```
The scanner was able to detect an input reflected in the response body.
```

HTTP Info

REQUEST MADE

```
GET /phpinfo.php HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: was-tnb-hsv=711vt1tpgrucudl1kaq9t074f5; PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 200
x-powered-by: PHP/5.5.9-1ubuntu4.14
vary: Accept-Encoding
content-type: text/html
content-encoding: gzip
x-cloud-trace-context: 743ec9a2b4bc81f94bc04c1700706ba5
date: Tue, 19 Nov 2024 01:44:48 GMT
server: Google Frontend
content-length: 19070
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/phpinfo.php

INPUT TYPE	header
INPUT NAME	Priority

Identification

PAYLOAD

```
was-tnb-hsv
```

PROOF
```
Input reflected in the response body : 'was-tnb-hsv'.
```

OUTPUT
```
The scanner was able to detect an input reflected in the response body.
```

HTTP Info

REQUEST MADE
```
GET /phpinfo.php HTTP/2
```

REQUEST HEADERS
```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Priority: was-tnb-hsv
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS
```
HTTP/2 200
x-powered-by: PHP/5.5.9-1ubuntu4.14
vary: Accept-Encoding
content-type: text/html
content-encoding: gzip
x-cloud-trace-context: 29652da3a208b0400f03055f02d5295d
date: Tue, 19 Nov 2024 01:44:51 GMT
server: Google Frontend
content-length: 19079
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/phpinfo.php

INPUT TYPE	header
INPUT NAME	Sec-Fetch-Site

Identification

PAYLOAD
```
was-tnb-hsv
```

PROOF
```
Input reflected in the response body : 'was-tnb-hsv'.
```

OUTPUT
```
The scanner was able to detect an input reflected in the response body.
```

HTTP Info

REQUEST MADE
```
GET /phpinfo.php HTTP/2
```

REQUEST HEADERS
```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
```

```
Sec-Fetch-Site: was-tnb-hsv
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 200
x-powered-by: PHP/5.5.9-1ubuntu4.14
vary: Accept-Encoding
content-type: text/html
content-encoding: gzip
x-cloud-trace-context: c7e28f643e43c0735842589e6b4e0e58
date: Tue, 19 Nov 2024 01:44:53 GMT
server: Google Frontend
content-length: 19097
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/phpinfo.php

INPUT TYPE	header
INPUT NAME	Parameter name fuzzing

Identification

PAYLOAD

```
was-tnb-hsv
```

PROOF

```
Input reflected in the response body : 'was-tnb-hsv'.
```

OUTPUT

```
The scanner was able to detect an input reflected in the response body.
```

HTTP Info

REQUEST MADE

```
GET /phpinfo.php HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Was-Tnb-Hsv: tenable_wasscan_name_fuzz
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 200
x-powered-by: PHP/5.5.9-1ubuntu4.14
vary: Accept-Encoding
content-type: text/html
content-encoding: gzip
x-cloud-trace-context: fd5f349db417baf1c9a7bcd68dbd9a46
date: Tue, 19 Nov 2024 01:44:49 GMT
server: Google Frontend
content-length: 19101
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/phpinfo.php

INPUT TYPE	header
INPUT NAME	Upgrade-Insecure-Requests

Identification

PAYLOAD

```
was-tnb-hsv
```

PROOF

```
Input reflected in the response body : 'was-tnb-hsv'.
```

OUTPUT

```
The scanner was able to detect an input reflected in the response body.
```

HTTP Info

REQUEST MADE

```
GET /phpinfo.php HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Upgrade-Insecure-Requests: was-tnb-hsv
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 200
x-powered-by: PHP/5.5.9-1ubuntu4.14
vary: Accept-Encoding
content-type: text/html
content-encoding: gzip
x-cloud-trace-context: e1563793ed0c3f1d68e6688b09a644a0
date: Tue, 19 Nov 2024 01:44:54 GMT
server: Google Frontend
content-length: 19121
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/phpinfo.php

INPUT TYPE	header
INPUT NAME	Cookie

Identification

PAYLOAD

```
was-tnb-hsv
```

PROOF

```
Input reflected in the response body : 'was-tnb-hsv'.
```

OUTPUT

```
The scanner was able to detect an input reflected in the response body.
```

HTTP Info

REQUEST MADE

```
GET /phpinfo.php HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5; was-tnb-hsv=
```

RESPONSE HEADERS

```
HTTP/2 200
x-powered-by: PHP/5.5.9-1ubuntu4.14
vary: Accept-Encoding
content-type: text/html
content-encoding: gzip
x-cloud-trace-context: bc7097e9b5c6aa0183f7f9f0dadd0d3d
date: Tue, 19 Nov 2024 01:44:51 GMT
server: Google Frontend
content-length: 19065
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/phpinfo.php

INPUT TYPE	header
INPUT NAME	Accept-Language

Identification

PAYLOAD

```
was-tnb-hsv
```

PROOF

```
Input reflected in the response body : 'was-tnb-hsv'.
```

OUTPUT

```
The scanner was able to detect an input reflected in the response body.
```

HTTP Info

REQUEST MADE

```
GET /phpinfo.php HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: was-tnb-hsv
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 200
x-powered-by: PHP/5.5.9-1ubuntu4.14
vary: Accept-Encoding
content-type: text/html
content-encoding: gzip
```

```
x-cloud-trace-context: a4eb9b45cd4aefc9f5787d7d64b05865
date: Tue, 19 Nov 2024 01:44:50 GMT
server: Google Frontend
content-length: 19026
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/phpinfo.php

INPUT TYPE	header
INPUT NAME	Pragma

Identification

PAYLOAD

```
was-tnb-hsv
```

PROOF

```
Input reflected in the response body : 'was-tnb-hsv'.
```

OUTPUT

```
The scanner was able to detect an input reflected in the response body.
```

HTTP Info

REQUEST MADE

```
GET /phpinfo.php HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Pragma: was-tnb-hsv
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 200
x-powered-by: PHP/5.5.9-1ubuntu4.14
vary: Accept-Encoding
content-type: text/html
content-encoding: gzip
x-cloud-trace-context: 6f78588dd18c6a5f5a8c0436fffb6b3e
date: Tue, 19 Nov 2024 01:44:49 GMT
server: Google Frontend
content-length: 19068
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/phpinfo.php

INPUT TYPE	header
INPUT NAME	Sec-Fetch-Dest

Identification

PAYLOAD

```
was-tnb-hsv
```

PROOF

```
Input reflected in the response body : 'was-tnb-hsv'.
```

OUTPUT

```
The scanner was able to detect an input reflected in the response body.
```

HTTP Info

REQUEST MADE

```
GET /phpinfo.php HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Sec-Fetch-Dest: was-tnb-hsv
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 200
x-powered-by: PHP/5.5.9-1ubuntu4.14
vary: Accept-Encoding
content-type: text/html
content-encoding: gzip
x-cloud-trace-context: 85c74afd91cee710e334b28f839f448e
date: Tue, 19 Nov 2024 01:44:53 GMT
server: Google Frontend
content-length: 19088
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/phpinfo.php

INPUT TYPE	header
INPUT NAME	Accept

Identification

PAYLOAD

```
was-tnb-hsv
```

PROOF

```
Input reflected in the response body : 'was-tnb-hsv'.
```

OUTPUT

```
The scanner was able to detect an input reflected in the response body.
```

HTTP Info

REQUEST MADE

```
GET /phpinfo.php HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: was-tnb-hsv
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 200
x-powered-by: PHP/5.5.9-1ubuntu4.14
vary: Accept-Encoding
content-type: text/html
content-encoding: gzip
x-cloud-trace-context: 3b97f070b2df7007dd9ecc4e9d4cc419
date: Tue, 19 Nov 2024 01:44:49 GMT
server: Google Frontend
content-length: 19036
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/phpinfo.php

INPUT TYPE	header
INPUT NAME	User-Agent

Identification

PAYLOAD

```
was-tnb-hsv
```

PROOF

```
Input reflected in the response body : 'was-tnb-hsv'.
```

OUTPUT

```
The scanner was able to detect an input reflected in the response body.
```

HTTP Info

REQUEST MADE

```
GET /phpinfo.php HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: was-tnb-hsv
Accept: */*
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 200
x-powered-by: PHP/5.5.9-1ubuntu4.14
vary: Accept-Encoding
content-type: text/html
content-encoding: gzip
x-cloud-trace-context: 45457e06906344d0e138f9dbea91adf7
date: Tue, 19 Nov 2024 01:44:49 GMT
server: Google Frontend
content-length: 18891
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/phpinfo.php

INPUT TYPE	header
INPUT NAME	Sec-Ch-Ua-Mobile

Identification

PAYLOAD

```
was-tnb-hsv
```

PROOF

```
Input reflected in the response body : 'was-tnb-hsv'.
```

OUTPUT

```
The scanner was able to detect an input reflected in the response body.
```

HTTP Info

REQUEST MADE

```
GET /phpinfo.php HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-388277804329.us-west1.run.app
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Sec-Ch-Ua-Mobile: was-tnb-hsv
Cookie: PHPSESSID=711vt1tpgrucudl1kaq9t074f5
```

RESPONSE HEADERS

```
HTTP/2 200
x-powered-by: PHP/5.5.9-1ubuntu4.14
vary: Accept-Encoding
content-type: text/html
content-encoding: gzip
x-cloud-trace-context: 338f7bbd5530f425075726ff433a619d
date: Tue, 19 Nov 2024 01:44:51 GMT
server: Google Frontend
content-length: 19097
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

Path Relative Stylesheet Import

VULNERABILITY INFO PLUGIN ID 114466

Description

A Path Relative Style Sheet Import occurs when the application imports a style sheet via a relative URL and uses user input in the file name. This vulnerability mainly affects older browsers such as Internet Explorer and allows an attacker to exploit the way the browser handles stylesheet imports in order to perform CSS Injection.

Solution

It is preferable not to use path-related URLs in stylesheet imports, and also to use the 'X-Content-Type-Options: nosnif' and 'X-Frame-Options: deny' headers.

See Also

https://csplite.com/csp290/

Plugin Details

PUBLICATION DATE	2024-10-30T00:00:00+00:00
MODIFICATION DATE	2024-11-08T00:00:00+00:00
FAMILY	Injection
SEVERITY	Info
PLUGIN ID	114466

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

Path Relative Stylesheet Import Instances (8)

VULNERABILITY INFO PLUGIN ID 114466

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/login.php

Identification

PROOF

```
The following value is extracted from a <link> tag that imports a style sheet with a 'href' that does not begin with a
/ :
* stylesheets/stylesheet.css
```

OUTPUT

```
The scanner was able to detect a Path Relative Stylesheet Import.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/login.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control=no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 01:51:06 GMT
Expires=Thu, 19 Nov 1981 08:52:00 GMT
Pragma=no-cache
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=97249a7d3363c12f26d1d625a5fdf4df
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4826
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/install.php?install=yes

Identification

PROOF

```
The following value is extracted from a <link> tag that imports a style sheet with a 'href' that does not begin with a
/ :
* stylesheets/stylesheet.css
```

OUTPUT

```
The scanner was able to detect a Path Relative Stylesheet Import.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/install.php?install=yes
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 02:39:05 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=b8eba21cccffcc35373450a248516ba1
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=3085
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/info_install.php

Identification

PROOF

```
The following value is extracted from a <link> tag that imports a style sheet with a 'href' that does not begin with a
/ :
* stylesheets/stylesheet.css
```

OUTPUT

```
The scanner was able to detect a Path Relative Stylesheet Import.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/info_install.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
```

```
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Arch=""
Sec-Ch-Ua-Bitness=""
Sec-Ch-Ua-Full-Version-List="Chromium", "HeadlessChrome", "Not-A.Brand";v="99.0.0.0"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Model=""
Sec-Ch-Ua-Platform="Linux"
Sec-Ch-Ua-Platform-Version=""
Sec-Ch-Ua-Wow64=?0
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 02:21:07 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=3305fabc85563bee1adce5fca1986cef
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4188
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/training_install.php

Identification

PROOF

```
The following value is extracted from a <link> tag that imports a style sheet with a 'href' that does not begin with a
/ :
* stylesheets/stylesheet.css
```

OUTPUT

```
The scanner was able to detect a Path Relative Stylesheet Import.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/training_install.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 02:31:16 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=dc248926d66de31d4ae1d4212ab637d0
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4629
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/install.php

Identification

PROOF

```
The following value is extracted from a <link> tag that imports a style sheet with a 'href' that does not begin with a
/ :
* stylesheets/stylesheet.css
```

OUTPUT

```
The scanner was able to detect a Path Relative Stylesheet Import.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/install.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Arch=""
Sec-Ch-Ua-Bitness=""
Sec-Ch-Ua-Full-Version-List="Chromium", "HeadlessChrome", "Not-A.Brand";v="99.0.0.0"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Model=""
Sec-Ch-Ua-Platform="Linux"
Sec-Ch-Ua-Platform-Version=""
Sec-Ch-Ua-Wow64=?0
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 00:19:04 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=793633ff205741c27021c36f1f4362a8
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=3083
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/training.php

Identification

PROOF

```
The following value is extracted from a <link> tag that imports a style sheet with a 'href' that does not begin with a
/ :
* stylesheets/stylesheet.css
```

OUTPUT

```
The scanner was able to detect a Path Relative Stylesheet Import.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/training.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 08:36:37 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=beee281846f3b9b9397b531ce1a92fef
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4656
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/info.php

Identification

PROOF

```
The following value is extracted from a <link> tag that imports a style sheet with a 'href' that does not begin with a
/ :
* stylesheets/stylesheet.css
```

OUTPUT

```
The scanner was able to detect a Path Relative Stylesheet Import.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/info.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 08:28:20 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=d1dec854dbe62de69a7b5ea639baba79
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4239
```

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/user_new.php

Identification

PROOF

```
The following value is extracted from a <link> tag that imports a style sheet with a 'href' that does not begin with a
/ :
* stylesheets/stylesheet.css
```

OUTPUT

```
The scanner was able to detect a Path Relative Stylesheet Import.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-388277804329.us-west1.run.app/user_new.php
```

REQUEST HEADERS

```
Accept=*/*
Accept-Encoding=gzip, deflate, br
Accept-Language=en-US,en;q=0.5
Cookie=PHPSESSID=711vt1tpgrucudl1kaq9t074f5
Priority=u=0, i
Sec-Ch-Ua="Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile=?0
Sec-Ch-Ua-Platform="Linux"
Sec-Fetch-Dest=document
Sec-Fetch-Mode=navigate
Sec-Fetch-Site=none
```

```
Sec-Fetch-User=?1
Upgrade-Insecure-Requests=1
User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc=h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding=gzip
Content-Type=text/html
Date=Tue, 19 Nov 2024 07:45:52 GMT
Server=Google Frontend
Vary=Accept-Encoding
X-Cloud-Trace-Context=1de28a3c31c89c397b35ab9cf352eeaf
X-Powered-By=PHP/5.5.9-1ubuntu4.14
Content-Length=4224
```

SSL/TLS Cipher Suites Supported

VULNERABILITY INFO PLUGIN ID 115491

Description

This plugin displays supported SSL/TLS cipher suites.

Solution

-

See Also

https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml

Plugin Details

PUBLICATION DATE	2019-01-09T00:00:00+00:00
MODIFICATION DATE	2022-10-07T00:00:00+00:00
FAMILY	SSL/TLS
SEVERITY	Info
PLUGIN ID	115491

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

SSL/TLS Cipher Suites Supported Instances (1)

VULNERABILITY INFO PLUGIN ID 115491

INSTANCE

https://juice-shop-388277804329.us-west1.run.app/#/

Identification

OUTPUT

```
Protocol Cipher Suite Name (RFC) Key Exchange Strength
----------------------------------------------------------------------------
TLS1.2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 x25519 256
TLS1.2 TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305 x25519 256
TLS1.2 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 x25519 256
TLS1.2 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA x25519 256
TLS1.2 TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA x25519 256
TLS1.2 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 x25519 256
TLS1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 x25519 256
TLS1.2 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA x25519 256
TLS1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA x25519 256
TLS1.2 TLS_RSA_WITH_AES_128_GCM_SHA256 RSA 4096
TLS1.2 TLS_RSA_WITH_AES_256_GCM_SHA384 RSA 4096
TLS1.2 TLS_RSA_WITH_AES_128_CBC_SHA RSA 4096
TLS1.2 TLS_RSA_WITH_AES_256_CBC_SHA RSA 4096
TLS1.3 TLS_AES_128_GCM_SHA256 x25519 256
TLS1.3 TLS_AES_256_GCM_SHA384 x25519 256
TLS1.3 TLS_CHACHA20_POLY1305_SHA256 x25519 256
```