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

April 26, 2025 at 12:23 (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

0 CRITICAL	3 HIGH	36 MEDIUM	97 LOW

Scan Details

NAME	Web app scan Juice Shop & bWAAP
STATUS	Completed
CREATE TIME	04/25/2025 at 11:08 PM UTC
START TIME	04/25/2025 at 11:10 PM UTC
END TIME	04/26/2025 at 08:12 AM UTC
TEMPLATE	Scan
SCANNER	Cloud
TARGET	https://juice-shop-16-0-1-178712031365.us-west1.run.app/#/
DESCRIPTION	

Scan Notes

Severity	Scan Notes	Description
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 for this plugin ID.
Info	Debug Mode Enabled	This scan has been configured with debug mode enabled. In this mode, the scanner provides extra information in plugin outputs and generate additional logs to facilitate troubleshooting, but this also leads to higher scan duration and is not suited for regular scans. Make sure therefore to use this mode either just before contacting or when advised by Tenable technical support for troubleshooting purposes.

Scan Results

Vulnerabilities

Severity	Plugin Id	Name	Family	Instances
High	98117	Blind SQL Injection (differential analysis)	Injection	1
High	114129	Secret Data Disclosure	Data Exposure	1
High	98115	SQL Injection	Injection	1
Medium	98056	Missing HTTP Strict Transport Security Policy	HTTP Security Header	25
Medium	98084	Directory Listing	Web Servers	2
Medium	98590	jQuery < 3.4.0 Prototype Pollution	Component Vulnerability	1
Medium	98617	SSL/TLS Forward Secrecy Cipher Suites Not Supported	SSL/TLS	1
Medium	98054	Unvalidated Redirection	Web Applications	1
Medium	112383	jQuery 1.2.0 < 3.5.0 Cross-Site Scripting	Component Vulnerability	1
Medium	98779	Source Code Passive Disclosure	Data Exposure	1
Medium	112435	jQuery 1.12.4 < 3.0.0 Cross-Site Scripting	Component Vulnerability	1
Medium	114012	Prometheus Sensitive Endpoint Detected	Data Exposure	1
Medium	113258	OpenAPI Permissive Input Validation	Web Applications	1
Medium	98109	DOM-based Cross-Site Scripting (XSS)	Cross Site Scripting	1
Low	98618	HTTP Header Information Disclosure	HTTP Security Header	25
Low	98057	Insecure 'Access-Control-Allow-Origin' Header	HTTP Security Header	25
Low	112553	Missing 'Cache-Control' Header	HTTP Security Header	21
Low	112551	Missing Content Security Policy	HTTP Security Header	8
Low	115540	Cookie Without SameSite Flag Detected	HTTP Security Header	4
Low	98064	Cookie Without Secure Flag Detected	HTTP Security Header	4
Low	98063	Cookie Without HttpOnly Flag Detected	HTTP Security Header	4
Low	114615	Username Disclosure	Data Exposure	3
Low	112529	Missing 'X-Content-Type-Options' Header	HTTP Security Header	1
Low	98060	Missing 'X-Frame-Options' Header	HTTP Security Header	1
Low	112539	SSL/TLS Weak Cipher Suites Supported	SSL/TLS	1

SQL Injection

VULNERABILITY HIGH PLUGIN ID 98115

Description

Due to the requirement for dynamic content of today's web applications, many rely on a database backend to store data that will be called upon and processed by the web application (or other programs). Web applications retrieve data from the database by using Structured Query Language (SQL) queries.

To meet demands of many developers, database servers (such as MSSQL, MySQL, Oracle etc.) have additional built-in functionality that can allow extensive control of the database and interaction with the host operating system itself.

An SQL injection occurs when a value originating from the client's request is used within a SQL query without prior sanitisation. This could allow cyber-criminals to execute arbitrary SQL code and steal data or use the additional functionality of the database server to take control of more server components.

The successful exploitation of a SQL injection can be devastating to an organisation and is one of the most commonly exploited web application vulnerabilities.

This injection was detected as scanner was able to cause the server to respond to the request with a database related error.

Solution

The only proven method to prevent against SQL injection attacks while still maintaining full application functionality is to use parameterized queries (also known as prepared statements). When utilising this method of querying the database, any value supplied by the client will be handled as a string value rather than part of the SQL query.
Additionally, when utilising parameterized queries, the database engine will automatically check to make sure the string being used matches that of the column. For example, the database engine will check that the user supplied input is an integer if the database column is configured to contain integers.

See Also

http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://en.wikipedia.org/wiki/SQL_injection
http://unixwiz.net/techtips/sql-injection.html
http://projects.webappsec.org/w/page/13246963/SQL%20Injection
http://www.w3schools.com/sql/sql_injection.asp
https://www.owasp.org/index.php/SQL_Injection

Plugin Details

PUBLICATION DATE	2017-03-31T00:00:00+00:00
MODIFICATION DATE	2025-01-07T00:00:00+00:00
FAMILY	Injection
SEVERITY	High
PLUGIN ID	98115

Risk Information

CVSSV4 BASE SCORE	7.2
CVSSV4 VECTOR	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:H/VI:L/VA:L/SC:N/SI:N/SA:N
CVSSV3 BASE SCORE	8.6
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:L
CVSS BASE SCORE	9.0
CVSS VECTOR	CVSS2#AV:N/AC:L/Au:N/C:C/I:P/A:P

Reference Information

CWE	89
WASC	SQL Injection
OWASP	2013-A1, 2021-A3, 2010-A1, 2017-A1, 2019-API8
CVE	-
BID	-

SQL Injection Instances (1)

VULNERABILITY HIGH PLUGIN ID 98115

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/products/search

INPUT TYPE	link
INPUT NAME	q

Identification

PAYLOAD

```
"!`--
```

PROOF

```
SQLITE_ERROR: near &quot;`--%&#39; OR description LIKE &#39;%nessus_was_textjvihbcaq&quot;&#39;`&quot;: syntax error
```

OUTPUT

```
The scanner was able to detect a possible SQL injection. The detected database engine used is 'sqlite'.
```

HTTP Info

REQUEST MADE

```
GET /rest/products/search?q=nessus_was_textjvihbcaq%22%27%60-- HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-16-0-1-178712031365.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: gzip, deflate, br
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Cookie: language=en; continueCode=z67RBJkpxgOw1qjLrbzDM95EnABVfXDUb9A3Y2aePl4VXZvQ8mW7yKo6NXeE;
cookieconsent_status=dismiss; welcomebanner_status=dismiss
```

RESPONSE HEADERS

```
HTTP/2 500
access-control-allow-origin: *
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
feature-policy: payment 'self'
x-recruiting: /#/jobs
content-type: text/html; charset=utf-8
vary: Accept-Encoding
content-encoding: gzip
x-cloud-trace-context: 446103fb28951bd0ab1ca8ad253cae01
date: Sat, 26 Apr 2025 00:50:28 GMT
server: Google Frontend
content-length: 590
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

Blind SQL Injection (differential analysis)

VULNERABILITY HIGH PLUGIN ID 98117

Description

Due to the requirement for dynamic content of today's web applications, many rely on a database backend to store data that will be called upon and processed by the web application (or other programs). Web applications retrieve data from the database by using Structured Query Language (SQL) queries.

To meet demands of many developers, database servers (such as MSSQL, MySQL, Oracle etc.) have additional built-in functionality that can allow extensive control of the database and interaction with the host operating system itself.

An SQL injection occurs when a value originating from the client's request is used within a SQL query without prior sanitisation. This could allow cyber-criminals to execute arbitrary SQL code and steal data or use the additional functionality of the database server to take control of more server components.

The successful exploitation of a SQL injection can be devastating to an organisation and is one of the most commonly exploited web application vulnerabilities.

This injection was detected as scanner was able to inject specific SQL queries, that if vulnerable, result in the responses for each injection being different. This is known as a blind SQL injection vulnerability.

Solution

The only proven method to prevent against SQL injection attacks while still maintaining full application functionality is to use parameterized queries (also known as prepared statements). When utilising this method of querying the database, any value supplied by the client will be handled as a string value rather than part of the SQL query.
Additionally, when utilising parameterized queries, the database engine will automatically check to make sure the string being used matches that of the column. For example, the database engine will check that the user supplied input is an integer if the database column is configured to contain integers.

See Also

http://projects.webappsec.org/w/page/13246963/SQL%20Injection
http://www.w3schools.com/sql/sql_injection.asp
https://www.owasp.org/index.php/Blind_SQL_Injection

Plugin Details

PUBLICATION DATE	2017-03-31T00:00:00+00:00
MODIFICATION DATE	2025-03-18T00:00:00+00:00
FAMILY	Injection
SEVERITY	High
PLUGIN ID	98117

Risk Information

CVSSV4 BASE SCORE	7.2
CVSSV4 VECTOR	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:H/VI:L/VA:L/SC:N/SI:N/SA:N
CVSSV3 BASE SCORE	8.6

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

Reference Information

CWE	89
WASC	SQL Injection
OWASP	2013-A1, 2021-A3, 2010-A1, 2017-A1, 2019-API8
CVE	-
BID	-

Blind SQL Injection (differential analysis) Instances (1)

VULNERABILITY HIGH PLUGIN ID 98117

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/products/search

INPUT TYPE	link
INPUT NAME	q

Identification

PAYLOAD

```
10002'+(select '1')+'1
```

PROOF

```
10002'+(select '1','2')+'1 for TRUE statement and 10002'+(select '1')+'1 for FALSE statement
```

OUTPUT

```
A differential based SQL Injection has been identified by the scanner.
```

HTTP Info

REQUEST MADE

```
GET /rest/products/search?q=10002%27%2B%28select%20%271%27%29%2B%271 HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-16-0-1-178712031365.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: gzip, deflate, br
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
```

RESPONSE HEADERS

```
HTTP/2 200
access-control-allow-origin: *
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
feature-policy: payment 'self'
x-recruiting: /#/jobs
content-type: application/json; charset=utf-8
etag: W/"1e-JkPcI+pGj7BBTxOuZTVVIm91zaY"
vary: Accept-Encoding
x-cloud-trace-context: cbb1f0b0d302c3cc4ed6912733b82958
date: Sat, 26 Apr 2025 00:55:56 GMT
server: Google Frontend
content-length: 30
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

Secret Data Disclosure

VULNERABILITY HIGH PLUGIN ID 114129

Description

Most of the web applications rely on various public services to provide features to their users. In secure designs, consuming these private or cloud services will require authentication like API and private keys, username and password based credentials and similar sensitive data.

Developers sometimes hard code such data in various places of their applications, without realizing that it could become publicly available in client-side JavaScript or, for example, HTML comments. By leveraging these sensitive information, a remote and unauthenticated attacker could gain privileged access to critical services used by the web application and the organization.

Solution

Remove the secret exposure by identifying the root cause of the issue (for example manual data insertion in the code, environment variables being bundled in front-end JavaScript). Rotate the secrets to avoid further reuse in case it has been previously retrieved by a malicious actor.

See Also

https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/01-Information_Gathering/05-Review_Web_Page_Content_for_Information_Leakage

Plugin Details

PUBLICATION DATE	2023-12-11T00:00:00+00:00
MODIFICATION DATE	2025-04-02T00:00:00+00:00
FAMILY	Data Exposure
SEVERITY	High
PLUGIN ID	114129

Risk Information

CVSSV4 BASE SCORE	8.7
CVSSV4 VECTOR	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:L/SI:L/SA:L
CVSSV3 BASE SCORE	8.6
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/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	16, 200
WASC	Application Misconfiguration, Information Leakage
OWASP	2021-A5, 2017-A6, 2021-A1, 2013-A5, 2010-A6, 2023-API8, 2023-API3, 2019-API3, 2019-API7
CVE	-

BID	-

Secret Data Disclosure Instances (1)

VULNERABILITY HIGH PLUGIN ID 114129

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/memories/

Identification

PROOF

```
The following patterns were detected in the HTTP response body :
- "password":"9283f1b2e9669749081963be0462e466"

- "password":"6edd9d726cbdc873c539e41ae8757b8c"

- "password":"2c17c6393771ee3048ae34d6b380c5ec"

- "password":"00479e957b6b42c459ee5746478e4d45"

- "password":"402f1c4a75e316afec5a6ea63147f739"
```

OUTPUT

```
The scanner identified one or more `Generic Password` secret(s) on the target page.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/memories/
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: language=en; cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=z67RBJkpxgOw1qjLrbzDM95EnABVfXDUb9A3Y2aePl4VXZvQ8mW7yKo6NXeE
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding: gzip
Content-Type: application/json; charset=utf-8
Date: Fri, 25 Apr 2025 23:25:12 GMT
Etag: W/"e22-FLHwo+MhT//q5XkiU8jz6hJU1ss"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

Unvalidated Redirection

VULNERABILITY MEDIUM PLUGIN ID 98054

Description

Web applications occasionally use parameter values to store the address of the page to which the client will be redirected -- for example: `yoursite.com/page.asp?redirect=www.yoursite.com/404.asp`

An unvalidated redirect occurs when the client is able to modify the affected parameter value in the request and thus control the location of the redirection. For example, the following URL `yoursite.com/page.asp?redirect=www.anothersite.com` will redirect to `www.anothersite.com`.

There are several ways a redirection can occur:

1) A response with a 3xx status code will tell the browser to redirect to the URL in the "Location" header

2) A response with a "Refresh" header tells the browser to reload the page after a set interval (which can be 0). The header can take an arbitrary URL parameter to load

3) The HTML <meta> tag can take a "http-equiv" attribute which can be used instead of an HTTP response header. Using this, a "Refresh" can be simulated

4) Javascript is used to redirect the browser to an arbitrary URL

Cyber-criminals will abuse these vulnerabilities in social engineering attacks to get users to unknowingly visit malicious web sites.

The scanner has discovered that the server does not validate the parameter value prior to redirecting the client to the injected value.

Solution

The application should ensure that the supplied value for a redirect is permitted. This can be achieved by performing whitelisting on the parameter value.
The whitelist should contain a list of pages or sites that the application is permitted to redirect users to. If the supplied value does not match any value in the whitelist then the server should redirect to a standard error page.

See Also
https://www.owasp.org/index.php/Unvalidated_Redirects_and_Forwards_Cheat_Sheet

Plugin Details

PUBLICATION DATE	2017-03-31T00:00:00+00:00
MODIFICATION DATE	2023-07-13T00:00:00+00:00
FAMILY	Web Applications
SEVERITY	Medium
PLUGIN ID	98054

Risk Information

CVSSV4 BASE SCORE	5.1
CVSSV4 VECTOR	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N
CVSSV3 BASE SCORE	4.7
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N
CVSS BASE SCORE	4.3
CVSS VECTOR	CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N

Reference Information

CWE	601
WASC	URL Redirector Abuse
OWASP	2021-A1, 2013-A10, 2010-A10, 2023-API8, 2019-API7
CVE	-
BID	-

Unvalidated Redirection Instances (1)

VULNERABILITY MEDIUM PLUGIN ID 98054

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/redirect

INPUT TYPE	link
INPUT NAME	to

Identification

PAYLOAD

```
https://98147a45-d7d1-4fb3-a532-d4d4b2db551e.com?x=https://github.com/juice-shop/juice-shop
```

PROOF

```
The issue was raised because the scanner was redirected to https://98147a45-d7d1-4fb3-a532-d4d4b2db551e.com?
x=https://github.com/juice-shop/juice-shop
```

OUTPUT

```
An unvalidated redirect was found on https://juice-shop-16-0-1-178712031365.us-west1.run.app/redirect?to=https%3A%2F%
2F98147a45-d7d1-4fb3-a532-d4d4b2db551e.com%3Fx%3Dhttps%3A%2F%2Fgithub.com%2Fjuice-shop%2Fjuice-shop by injecting
https://98147a45-d7d1-4fb3-a532-d4d4b2db551e.com?x=https://github.com/juice-shop/juice-shop into the query parameter
'to' to create the url 'https://juice-shop-16-0-1-178712031365.us-west1.run.app/redirect?to=https%3A%2F%2F98147a45-d7d1-
4fb3-a532-d4d4b2db551e.com%3Fx%3Dhttps%3A%2F%2Fgithub.com%2Fjuice-shop%2Fjuice-shop'.
```

HTTP Info

REQUEST MADE

```
GET /redirect?to=https%3A%2F%2F98147a45-d7d1-4fb3-a532-d4d4b2db551e.com%3Fx%3Dhttps%3A%2F%2Fgithub.com%2Fjuice-shop%
2Fjuice-shop HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-16-0-1-178712031365.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: language=en; continueCode=5PD2YLPJeo8nyMjZXVOD34wKlWgAOkfJpAra79p51QRExqzYm2bBvN6kklXR;
cookieconsent_status=dismiss; welcomebanner_status=dismiss
```

RESPONSE HEADERS

```
HTTP/2 302
access-control-allow-origin: *
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
feature-policy: payment 'self'
x-recruiting: /#/jobs
location: https://98147a45-d7d1-4fb3-a532-d4d4b2db551e.com?x=https://github.com/juice-shop/juice-shop
vary: Accept, Accept-Encoding
content-type: text/plain; charset=utf-8
x-cloud-trace-context: 7751257c1bff54592351cfa072be4ea1
date: Fri, 25 Apr 2025 23:16:40 GMT
server: Google Frontend
content-length: 113
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

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	6.3
CVSSV4 VECTOR	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N
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-16-0-1-178712031365.us-west1.run.app/assets/i18n/de_DE.json

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-16-0-1-178712031365.us-west1.run.app/assets/i18n/de_DE.json.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/de_DE.json
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=de_DE
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: application/json; charset=UTF-8
Date: Sat, 26 Apr 2025 02:29:48 GMT
Etag: W/"904a-18f05ebb708"
Feature-Policy: payment 'self'
Last-Modified: Mon, 22 Apr 2024 13:08:05 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/Feedbacks/

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-16-0-1-178712031365.us-west1.run.app/api/Feedbacks/.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/Feedbacks/
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: language=en; cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1
If-None-Match: W/"6c6-1n6pt9X8GncrTGxXY8nLWSP9brU"
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding: gzip
Content-Type: application/json; charset=utf-8
Date: Sat, 26 Apr 2025 02:27:40 GMT
Etag: W/"6c6-SIwkJLL3y8euYH1CiBtnE7PUBNY"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/user/whoami

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-16-0-1-178712031365.us-west1.run.app/rest/user/whoami.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/user/whoami
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: language=en; cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=z67RBJkpxgOw1qjLrbzDM95EnABVfXDUb9A3Y2aePl4VXZvQ8mW7yKo6NXeE
If-None-Match: W/"b-/5bSboVjVhGw3qRgvUfZjE1r1Ns"
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Date: Sat, 26 Apr 2025 01:24:03 GMT
Etag: W/"b-/5bSboVjVhGw3qRgvUfZjE1r1Ns"
Feature-Policy: payment 'self'
Server: Google Frontend
X-Cloud-Trace-Context: 6d1efb72a363df96575e77ebdd395b80
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Vary: Accept-Encoding
Content-Length: 11
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/Quantitys/

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-16-0-1-178712031365.us-west1.run.app/api/Quantitys/.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/Quantitys/
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding: gzip
Content-Type: application/json; charset=utf-8
Date: Fri, 25 Apr 2025 23:10:12 GMT
Etag: W/"1767-etMBFb05GTNXcAa1INjMInHcId4"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/memories/

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-16-0-1-178712031365.us-west1.run.app/rest/memories/.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/memories/
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: language=en; continueCode=z67RBJkpxgOw1qjLrbzDM95EnABVfXDUb9A3Y2aePl4VXZvQ8mW7yKo6NXeE;
cookieconsent_status=dismiss; welcomebanner_status=dismiss
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding: gzip
Content-Type: application/json; charset=utf-8
Date: Sat, 26 Apr 2025 02:27:38 GMT
Etag: W/"e22-k4t/skONyGpeL9C7mhMGOYDLOnc"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/languages

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-16-0-1-178712031365.us-west1.run.app/rest/languages.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/languages
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding: gzip
Content-Type: application/json; charset=utf-8
Date: Fri, 25 Apr 2025 23:10:11 GMT
Etag: W/"1308-8EV95V7lUMShnloiieqORKNai/g"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/cs_CZ.json

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-16-0-1-178712031365.us-west1.run.app/assets/i18n/cs_CZ.json.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/cs_CZ.json
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=cs_CZ
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
```

```
Content-Encoding: gzip
Content-Type: application/json; charset=UTF-8
Date: Sat, 26 Apr 2025 02:29:27 GMT
Etag: W/"8814-18f05ebb708"
Feature-Policy: payment 'self'
Last-Modified: Mon, 22 Apr 2024 13:08:05 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/products/1/reviews

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-16-0-1-178712031365.us-west1.run.app/rest/products/1/reviews.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/products/1/reviews
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: language=en; cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=z67RBJkpxgOw1qjLrbzDM95EnABVfXDUb9A3Y2aePl4VXZvQ8mW7yKo6NXeE
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type: application/json; charset=utf-8
Date: Sat, 26 Apr 2025 01:24:03 GMT
Etag: W/"ac-+6TYO+tKceLLbG2Ky9HQ7ZcLMWM"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Cloud-Trace-Context: 7eb022bfa1d0336a575e77ebdd395585
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Length: 172
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/captcha/

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-16-0-1-178712031365.us-west1.run.app/rest/captcha/.

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/captcha/
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: language=en; cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1
If-None-Match: W/"31-6VzwP+6Js6+f/7oOKHud+d4LoO4"
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type: application/json; charset=utf-8
Date: Sat, 26 Apr 2025 02:27:39 GMT
Etag: W/"2f-MIu6CT8WR4M+Wp7TeexBr5Mm7M4"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Cloud-Trace-Context: cd7928d46a143d9e492e25266f1940ed
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Length: 47
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/socket.io/?EIO=4&transport=polling&t=PPlDpDO

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-16-0-1-178712031365.us-west1.run.app/socket.io/?EIO=4&transport=polling&t=PPlDpDO.

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/socket.io/?EIO=4&transport=polling&t=PPlDpDO
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
```

```
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: http://localhost:4200
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type: text/plain; charset=UTF-8
Date: Fri, 25 Apr 2025 23:10:10 GMT
Server: Google Frontend
Vary: Origin
X-Cloud-Trace-Context: 3beb321db23497f8a714d4467a7ab714
Content-Length: 96
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/id_ID.json

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-16-0-1-178712031365.us-west1.run.app/assets/i18n/id_ID.json.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/id_ID.json
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=id_ID
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: application/json; charset=UTF-8
Date: Sat, 26 Apr 2025 02:28:52 GMT
Etag: W/"8269-18f05ebb708"
Feature-Policy: payment 'self'
Last-Modified: Mon, 22 Apr 2024 13:08:05 GMT
Server: Google Frontend
```

```
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/da_DK.json

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-16-0-1-178712031365.us-west1.run.app/assets/i18n/da_DK.json.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/da_DK.json
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=da_DK
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: application/json; charset=UTF-8
Date: Sat, 26 Apr 2025 02:29:39 GMT
Etag: W/"85dd-18f05ebb708"
Feature-Policy: payment 'self'
Last-Modified: Mon, 22 Apr 2024 13:08:05 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/admin/application-configuration

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-16-0-1-178712031365.us-west1.run.app/rest/admin/application-configuration.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/admin/application-configuration
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding: gzip
Content-Type: application/json; charset=utf-8
Date: Fri, 25 Apr 2025 23:10:10 GMT
Etag: W/"4993-Oz9kS67Z/2Q7h9VfrxO8V9OVt0M"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.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-16-0-1-178712031365.us-west1.run.app/.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8
Date: Fri, 25 Apr 2025 23:10:08 GMT
Etag: W/"ea4-1966f2bc520"
Feature-Policy: payment 'self'
Last-Modified: Fri, 25 Apr 2025 22:57:41 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Length: 4619
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/products/search?q=

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-16-0-1-178712031365.us-west1.run.app/rest/products/search?q=.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/products/search?q=
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding: gzip
Content-Type: application/json; charset=utf-8
Date: Fri, 25 Apr 2025 23:10:11 GMT
Etag: W/"325f-8he+HyT41TF0TRRd87FqKb7A8Mg"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
```

```
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/en.json

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-16-0-1-178712031365.us-west1.run.app/assets/i18n/en.json.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/en.json
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: application/json; charset=UTF-8
Date: Fri, 25 Apr 2025 23:10:10 GMT
Etag: W/"8175-18f05ebb708"
Feature-Policy: payment 'self'
Last-Modified: Mon, 22 Apr 2024 13:08:05 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/az_AZ.json

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-16-0-1-178712031365.us-west1.run.app/assets/i18n/az_AZ.json.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/az_AZ.json
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=az_AZ
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: application/json; charset=UTF-8
Date: Sat, 26 Apr 2025 02:28:35 GMT
Etag: W/"8cc1-18f05ebb708"
Feature-Policy: payment 'self'
Last-Modified: Mon, 22 Apr 2024 13:08:05 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/fr_FR.json

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-16-0-1-178712031365.us-west1.run.app/assets/i18n/fr_FR.json.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/fr_FR.json
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=fr_FR
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: application/json; charset=UTF-8
Date: Sat, 26 Apr 2025 02:30:23 GMT
Etag: W/"9137-18f05ebb708"
Feature-Policy: payment 'self'
Last-Modified: Mon, 22 Apr 2024 13:08:05 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/Challenges/?name=Score%20Board

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-16-0-1-178712031365.us-west1.run.app/api/Challenges/?name=Score%20Board.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/Challenges/?name=Score%20Board
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type: application/json; charset=utf-8
Date: Fri, 25 Apr 2025 23:10:12 GMT
Etag: W/"288-+JKo65JYfG3LT9Er5ELTcivVYcQ"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Cloud-Trace-Context: 955c7b2840303fd8a714d4467a7ab0e0
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
```

```
X-Recruiting: /#/jobs
Content-Length: 648
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/et_EE.json

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-16-0-1-178712031365.us-west1.run.app/assets/i18n/et_EE.json.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/et_EE.json
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=et_EE
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: application/json; charset=UTF-8
Date: Sat, 26 Apr 2025 02:29:56 GMT
Etag: W/"8319-18f05ebb708"
Feature-Policy: payment 'self'
Last-Modified: Mon, 22 Apr 2024 13:08:05 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/ca_ES.json

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-16-0-1-178712031365.us-west1.run.app/assets/i18n/ca_ES.json.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/ca_ES.json
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=ca_ES
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: application/json; charset=UTF-8
Date: Sat, 26 Apr 2025 02:29:02 GMT
Etag: W/"826e-18f05ebb708"
Feature-Policy: payment 'self'
Last-Modified: Mon, 22 Apr 2024 13:08:05 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/es_ES.json

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-16-0-1-178712031365.us-west1.run.app/assets/i18n/es_ES.json.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/es_ES.json
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=es_ES
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: application/json; charset=UTF-8
Date: Sat, 26 Apr 2025 02:30:16 GMT
Etag: W/"8d7b-18f05ebb708"
Feature-Policy: payment 'self'
Last-Modified: Mon, 22 Apr 2024 13:08:05 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/ftp/legal.md

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-16-0-1-178712031365.us-west1.run.app/ftp/legal.md.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/ftp/legal.md
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=da_DK
Priority: u=0, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: same-origin
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
```

```
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: text/markdown; charset=UTF-8
Date: Sat, 26 Apr 2025 03:18:01 GMT
Etag: W/"be7-1966fb18775"
Feature-Policy: payment 'self'
Last-Modified: Sat, 26 Apr 2025 01:23:47 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/admin/application-version

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-16-0-1-178712031365.us-west1.run.app/rest/admin/application-version.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/admin/application-version
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type: application/json; charset=utf-8
Date: Fri, 25 Apr 2025 23:10:10 GMT
Etag: W/"14-mWpI2PhnItYY44Y5gln+68A5CNc"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Cloud-Trace-Context: bb00cff05c5f3c45a714d4467a7abcb2
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Length: 20
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/continue-code

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-16-0-1-178712031365.us-west1.run.app/rest/continue-code.

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/continue-code
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: language=en; continueCode=aj4QDO4KyOqPJ7j2novp9EQ38gYVAJlGM1wWxalND5reZRLzmXk6BbmzZRb3;
cookieconsent_status=dismiss
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type: application/json; charset=utf-8
Date: Fri, 25 Apr 2025 23:11:40 GMT
Etag: W/"4f-BtWsDO+6UbKwXn+zhLoc64lHywc"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Cloud-Trace-Context: d28bc164452bf02b9b983bf0f2052948
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Length: 79
```

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 (2)

VULNERABILITY MEDIUM PLUGIN ID 98084

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/ftp/legal.md

Identification

OUTPUT

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

- https://juice-shop-16-0-1-178712031365.us-west1.run.app/ftp/
```

HTTP Info

REQUEST MADE

```
GET /ftp/ HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-16-0-1-178712031365.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: language=en; continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1;
cookieconsent_status=dismiss; welcomebanner_status=dismiss
```

RESPONSE HEADERS

```
HTTP/2 200
access-control-allow-origin: *
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
feature-policy: payment 'self'
x-recruiting: /#/jobs
content-type: text/html; charset=utf-8
vary: Accept-Encoding
content-encoding: gzip
date: Sat, 26 Apr 2025 05:12:55 GMT
server: Google Frontend
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/ftp/quarantine/juicy_malware_linux_amd_64.url

Identification

OUTPUT

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

- https://juice-shop-16-0-1-178712031365.us-west1.run.app/ftp/quarantine/
```

HTTP Info

REQUEST MADE

```
GET /ftp/quarantine/ HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-16-0-1-178712031365.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: language=az_AZ; continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1;
cookieconsent_status=dismiss; welcomebanner_status=dismiss
```

RESPONSE HEADERS

```
HTTP/2 200
access-control-allow-origin: *
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
feature-policy: payment 'self'
x-recruiting: /#/jobs
content-type: text/html; charset=utf-8
vary: Accept-Encoding
content-encoding: gzip
date: Sat, 26 Apr 2025 07:49:02 GMT
server: Google Frontend
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

DOM-based Cross-Site Scripting (XSS)

VULNERABILITY MEDIUM PLUGIN ID 98109

Description

Client-side scripts are used extensively by modern web applications. They perform from simple functions (such as the formatting of text) up to full manipulation of client-side data and Operating System interaction.

Unlike traditional Cross-Site Scripting (XSS), where the client is able to inject scripts into a request and have the server return the script to the client, DOM XSS does not require that a request be sent to the server and may be abused entirely within the loaded page.

This occurs when elements of the DOM (known as the sources) are able to be manipulated to contain untrusted data, which the client-side scripts (known as the sinks) use or execute an unsafe way.

Scanner has discovered that by inserting an HTML element into the page's DOM inputs (sources), it was possible to then have the HTML element rendered as part of the page by the sink.

Solution

Client-side document rewriting, redirection, or other sensitive action, using untrusted data, should be avoided wherever possible, as these may not be inspected by server side filtering.
To remedy DOM XSS vulnerabilities where these sensitive document actions must be used, it is essential to:
1. Ensure any untrusted data is treated as text, as opposed to being interpreted as code or mark-up within the page. 2. Escape untrusted data prior to being used within the page. Escaping methods will vary depending on where the untrusted data is being used. (See references for details.) 3. Use `document.createElement`, `element.setAttribute`, `element.appendChild`, etc. to build dynamic interfaces as opposed to HTML rendering methods such as `document.write`, `document.writeln`, `element.innerHTML`, or `element.outerHTML `etc.

See Also

http://projects.webappsec.org/w/page/13246920/Cross%20Site%20Scripting
https://www.owasp.org/index.php/DOM_Based_XSS
https://www.owasp.org/index.php/DOM_based_XSS_Prevention_Cheat_Sheet

Plugin Details

PUBLICATION DATE	2017-03-31T00:00:00+00:00
MODIFICATION DATE	2025-01-17T00:00:00+00:00
FAMILY	Cross Site Scripting
SEVERITY	Medium
PLUGIN ID	98109

Risk Information

CVSSV4 BASE SCORE	5.1
CVSSV4 VECTOR	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N
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	79
WASC	Cross-Site Scripting
OWASP	2021-A3, 2010-A2, 2013-A3, 2017-A7, 2023-API8, 2019-API7
CVE	-
BID	-

DOM-based Cross-Site Scripting (XSS) Instances (1)

VULNERABILITY MEDIUM PLUGIN ID 98109

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/

INPUT TYPE	ui_input_dom
INPUT NAME	mat-input-0

Identification

PAYLOAD

```
javascript:window.top._tenable_wasscan_js_namespace_taint_tracer.log_execution_flow_sink()//"//`//'//"//--></style><
/select></noscript></noembed></template></title></textarea></script><iframe/srcdoc="<svg/onload=window.top.
_tenable_wasscan_js_namespace_taint_tracer.log_execution_flow_sink()>"><frame/onload=window.top.
_tenable_wasscan_js_namespace_taint_tracer.log_execution_flow_sink()>*/ window.top.
_tenable_wasscan_js_namespace_taint_tracer.log_execution_flow_sink()//
```

OUTPUT

```
Vulnerability has been detected on URL 'https://juice-shop-16-0-1-178712031365.us-west1.run.app/' by exploiting
'ui_input_dom' element named 'mat-input-0' and injecting following payload:

| javascript:window.top._tenable_wasscan_js_namespace_taint_tracer.log_execution_flow_sink()//"//`//'//"//--></style><
/select></noscript></noembed></template></title></textarea></script><iframe/srcdoc="<svg/onload=window.top.
_tenable_wasscan_js_namespace_taint_tracer.log_execution_flow_sink()>"><frame/onload=window.top.
_tenable_wasscan_js_namespace_taint_tracer.log_execution_flow_sink()>*/ window.top.
_tenable_wasscan_js_namespace_taint_tracer.log_execution_flow_sink()//
```

jQuery < 3.4.0 Prototype Pollution

VULNERABILITY MEDIUM PLUGIN ID 98590

Description

According to its self-reported version number, jQuery is prior to 3.4.0. Therefore, it may be affected by a prototype pollution vulnerability due to 'extend' function that can be tricked into modifying the prototype of 'Object'.

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 jQuery version 3.4.0 or later.

See Also
https://github.com/jquery/jquery/pull/4333
https://snyk.io/blog/after-three-years-of-silence-a-new-jquery-prototype-pollution-vulnerability-emerges-once-again/
https://snyk.io/vuln/SNYK-JS-JQUERY-174006

Plugin Details

PUBLICATION DATE	2019-04-25T00:00:00+00:00
MODIFICATION DATE	2023-03-14T00:00:00+00:00
FAMILY	Component Vulnerability
SEVERITY	Medium
PLUGIN ID	98590

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	4.3
CVSS VECTOR	CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N

Reference Information

CWE	1321, 20, 400, 79
WASC	Cross-Site Scripting, Denial of Service, Improper Input Handling
OWASP	2010-A4, 2021-A3, 2021-A6, 2010-A2, 2013-A3, 2013-A9, 2017-A9, 2017-A5, 2013-A4, 2017-A7, 2019-API7, 2023-API8
CVE	CVE-2019-11358
BID	108023

jQuery < 3.4.0 Prototype Pollution Instances (1)

VULNERABILITY MEDIUM PLUGIN ID 98590

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/

Identification

OUTPUT

```
Current Version: 2.2.4
Fixed Version: 3.4.0
Detected technology URL: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
```

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	6.0
CVSSV4 VECTOR	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:P/VC:H/VI:L/VA:N/SC:L/SI:L/SA:L
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-16-0-1-178712031365.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 (1)

VULNERABILITY MEDIUM PLUGIN ID 98779

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/api-docs/swagger-ui-bundle.js

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 https://juice-shop-16-0-1-178712031365.us-west1.run.app/api-docs/swagger-ui-bundle.js
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=az_AZ
If-Modified-Since: Mon, 22 Apr 2024 13:05:27 GMT
If-None-Match: W/"15c6ef-18f05e94dd8"
Priority: u=1
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/api-docs/
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: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

jQuery 1.2.0 < 3.5.0 Cross-Site Scripting

VULNERABILITY MEDIUM PLUGIN ID 112383

Description

According to its self-reported version number, jQuery is at least 1.2.0 and prior to 3.5.0. Therefore, it may be affected by a cross-site scripting vulnerability via the regex operation in jQuery.htmlPrefilter.

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 jQuery version 3.5.0 or later.

See Also

https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/
https://github.com/jquery/jquery/commit/1d61fd9407e6fbe82fe55cb0b938307aa0791f77

Plugin Details

PUBLICATION DATE	2020-05-14T00:00:00+00:00
MODIFICATION DATE	2023-03-14T00:00:00+00:00
FAMILY	Component Vulnerability
SEVERITY	Medium
PLUGIN ID	112383

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	4.3
CVSS VECTOR	CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N

Reference Information

CWE	79
WASC	Cross-Site Scripting
OWASP	2021-A3, 2021-A6, 2010-A2, 2013-A3, 2013-A9, 2017-A7, 2017-A9, 2019-API7, 2023-API8
CVE	CVE-2020-11022, CVE-2020-11023
BID	-

jQuery 1.2.0 < 3.5.0 Cross-Site Scripting Instances (1)

VULNERABILITY MEDIUM PLUGIN ID 112383

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/

Identification

OUTPUT

```
Current Version: 2.2.4
Fixed Version: 3.5.0
Detected technology URL: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
```

jQuery 1.12.4 < 3.0.0 Cross-Site Scripting

VULNERABILITY MEDIUM PLUGIN ID 112435

Description

According to its self-reported version number, jQuery is at least 1.4.0 and prior to 1.12.0 or at least 1.12.4 and prior to 3.0.0-beta1. Therefore, it may be affected by a cross-site scripting vulnerability due to cross-domain ajax request performed without the dataType.

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 jQuery version 3.0.0 or later.

See Also

https://github.com/jquery/jquery/issues/2432
https://github.com/jquery/jquery/pull/2588/commits/c254d308a7d3f1eac4d0b42837804cfffcba4bb2

Plugin Details

PUBLICATION DATE	2018-11-05T00:00:00+00:00
MODIFICATION DATE	2023-03-14T00:00:00+00:00
FAMILY	Component Vulnerability
SEVERITY	Medium
PLUGIN ID	112435

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	4.3
CVSS VECTOR	CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N

Reference Information

CWE	79
WASC	Cross-Site Scripting
OWASP	2021-A3, 2021-A6, 2010-A2, 2013-A3, 2013-A9, 2017-A7, 2017-A9, 2019-API7, 2023-API8
CVE	CVE-2015-9251
BID	105658

jQuery 1.12.4 < 3.0.0 Cross-Site Scripting Instances (1)

VULNERABILITY MEDIUM PLUGIN ID 112435

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/

Identification

OUTPUT

```
Current Version: 2.2.4
Fixed Version: 3.0.0
Detected technology URL: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
```

OpenAPI Permissive Input Validation

VULNERABILITY MEDIUM PLUGIN ID 113258

Description

OpenAPI specification is an API description format for REST APIs. An OpenAPI file is written in YAML or JSON and describes all the API properties like the available endpoints with the related operations or the authentication methods.

The `Schema` object allows the definition of input and output data types which can be objects or primitives and arrays. When some data types properties are missing on objects specified in the definition file, the API implementation could potentially allow malicious input formats, leaving it open to multiple vulnerabilities like Denial of Service (DoS) or Remote Code Execution (RCE).

The scanner analyzed an OpenAPI definition file and detected the lack of properties on some data types.

Solution

Ensure that the missing properties are declared in the OpenAPI definition file according to the file specification and that the API backend enforces the validation of these properties on the inputs.

See Also

https://github.com/OAI/OpenAPI-Specification/blob/main/versions/3.0.2.md#schemaObject

Plugin Details

PUBLICATION DATE	2022-06-28T00:00:00+00:00
MODIFICATION DATE	2023-10-05T00:00:00+00:00
FAMILY	Web Applications
SEVERITY	Medium
PLUGIN ID	113258

Risk Information

CVSSV4 BASE SCORE	6.3
CVSSV4 VECTOR	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N
CVSSV3 BASE SCORE	5.6
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L
CVSS BASE SCORE	6.8
CVSS VECTOR	CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P

Reference Information

CWE	20
WASC	Improper Input Handling
OWASP	2010-A4, 2021-A3, 2013-A4, 2017-A5, 2019-API7, 2023-API8
CVE	-
BID	-

OpenAPI Permissive Input Validation Instances (1)

VULNERABILITY MEDIUM PLUGIN ID 113258

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/api-docs/

Identification

OUTPUT

```
The scanner detected the presence of permissive input(s) in the API host(s) used in the detected OpenAPI file on the
following URL https://juice-shop-16-0-1-178712031365.us-west1.run.app/api-docs/.

The following components have parameter with permissive inputs :

- Component 'Order' has parameter 'cid' (String) without the 'format' property declared

- Component 'Order' has parameter 'cid' (String) without the 'maxLength' property declared

- Component 'Order' has parameter 'cid' (String) without the 'pattern' property declared

- Component 'OrderConfirmation' has parameter 'cid' (String) without the 'format' property declared

- Component 'OrderConfirmation' has parameter 'cid' (String) without the 'maxLength' property declared

- Component 'OrderConfirmation' has parameter 'cid' (String) without the 'pattern' property declared

- Component 'OrderConfirmation' has parameter 'orderNo' (String) without the 'format' property declared

- Component 'OrderConfirmation' has parameter 'orderNo' (String) without the 'maxLength' property declared

- Component 'OrderConfirmation' has parameter 'orderNo' (String) without the 'pattern' property declared

- Component 'OrderConfirmation' has parameter 'paymentDue' (String) without the 'maxLength' property declared

- Component 'OrderConfirmation' has parameter 'paymentDue' (String) without the 'pattern' property declared

- Component 'OrderLine' has parameter 'productId' (Integer) without the 'format' property declared

- Component 'OrderLine' has parameter 'productId' (Integer) without the 'maximum' property declared

- Component 'OrderLine' has parameter 'productId' (Integer) without the 'minimum' property declared

- Component 'OrderLine' has parameter 'quantity' (Integer) without the 'format' property declared

- Component 'OrderLine' has parameter 'quantity' (Integer) without the 'maximum' property declared

- Component 'OrderLine' has parameter 'customerReference' (String) without the 'format' property declared

- Component 'OrderLine' has parameter 'customerReference' (String) without the 'maxLength' property declared

- Component 'OrderLine' has parameter 'customerReference' (String) without the 'pattern' property declared
```

Prometheus Sensitive Endpoint Detected

VULNERABILITY MEDIUM PLUGIN ID 114012

Description

Prometheus is an open-source monitoring solution which is designed to record metrics in a dimensional data model to make it available through its own PromQL query language or built-in visualization capabilities. Prometheus offer multiple libraries (named 'Exporters') to help exporting these endpoints and make it available to third-party tools. When publicly exposed, a remote and unauthenticated attacker could leverage the data to understand the target application environment and try conducting further attack.

Solution

Ensure that the detected sensitive endpoint is not publicly available by requiring authentication or applying IP source filtering.

See Also

https://prometheus.io/
https://prometheus.io/docs/instrumenting/exporters/

Plugin Details

PUBLICATION DATE	2023-09-11T00:00:00+00:00
MODIFICATION DATE	2023-10-30T00:00:00+00:00
FAMILY	Data Exposure
SEVERITY	Medium
PLUGIN ID	114012

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	16, 538
WASC	Application Misconfiguration, Predictable Resource Location
OWASP	2021-A5, 2017-A6, 2021-A1, 2013-A5, 2010-A6, 2023-API8, 2023-API3, 2019-API3, 2019-API7
CVE	-
BID	-

Prometheus Sensitive Endpoint Detected Instances (1)

VULNERABILITY MEDIUM PLUGIN ID 114012

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/metrics

Identification

PROOF

```
# HELP file_uploads_count Total number of successful file uploads grouped by file type.
# TYPE file_uploads_count counter

# HELP file_upload_errors Total number of failed file uploads grouped by file type.
```

OUTPUT

```
The scanner was able to detect the exposure of a sensitive Prometheus endpoint at the following URL : https://juice-shop-16-0-1-178712031365.us-west1.run.app/metrics
```

HTTP Info

REQUEST MADE

```
GET /metrics HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-16-0-1-178712031365.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: language=en; continueCode=z67RBJkpxgOw1qjLrbzDM95EnABVfXDUb9A3Y2aePl4VXZvQ8mW7yKo6NXeE;
cookieconsent_status=dismiss; welcomebanner_status=dismiss
```

RESPONSE HEADERS

```
HTTP/2 200
content-type: text/plain; version=0.0.4; charset=utf-8
x-cloud-trace-context: 611c8cf58acc541f4556546f3e9a0930
date: Fri, 25 Apr 2025 23:22:29 GMT
server: Google Frontend
content-length: 23809
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

Insecure 'Access-Control-Allow-Origin' Header

VULNERABILITY LOW PLUGIN ID 98057

Description

Cross Origin Resource Sharing (CORS) is an HTML5 technology which gives modern web browsers the ability to bypass restrictions implemented by the Same Origin Policy.

The Same Origin Policy requires that both the JavaScript and the page are loaded from the same domain in order to allow JavaScript to interact with the page. This in turn prevents malicious JavaScript being executed when loaded from external domains.

The CORS policy allows the application to specify exceptions to the protections implemented by the browser, and enables the developer to specify allowlisted domains for which external JavaScript is permitted to execute and interact with the page.

The 'Access-Control-Allow-Origin' header is insecure when set to '*' or null, as it allows any domain to perform cross-domain requests and read responses. An attacker could abuse this configuration to retrieve private content from an application which does not use standard authentication mechanisms (for example, an Intranet allowing access from the internal network only).

Solution

Unless the target application is specifically designed to serve public content to any domain, the 'Access-Control-Allow-Origin' should be configured with an allowlist including only known and trusted domains to perform cross-domain requests if needed, or should be disabled.

See Also

https://developer.mozilla.org/en-US/docs/Web/HTTP/Access_control_CORS
https://www.owasp.org/index.php/CORS_OriginHeaderScrutiny

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	98057

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

Insecure 'Access-Control-Allow-Origin' Header Instances (25)

VULNERABILITY LOW PLUGIN ID 98057

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/es_ES.json

Identification

PROOF

```
Access-Control-Allow-Origin: *
```

OUTPUT

```
Vulnerability has been detected on URL 'https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/es_ES.json'

To confirm the presence of the vulnerability, this proof has been identified in the target response:

| Access-Control-Allow-Origin: *

The information used to check the vulnerability have been provided in attachment.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/es_ES.json
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=es_ES
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: application/json; charset=UTF-8
Date: Sat, 26 Apr 2025 02:30:16 GMT
Etag: W/"8d7b-18f05ebb708"
Feature-Policy: payment 'self'
Last-Modified: Mon, 22 Apr 2024 13:08:05 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/continue-code

Identification

PROOF

```
Access-Control-Allow-Origin: *
```

OUTPUT

```
Vulnerability has been detected on URL 'https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/continue-code'

To confirm the presence of the vulnerability, this proof has been identified in the target response:

| Access-Control-Allow-Origin: *

The information used to check the vulnerability have been provided in attachment.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/continue-code
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: language=en; continueCode=aj4QDO4KyOqPJ7j2novp9EQ38gYVAJlGM1wWxalND5reZRLzmXk6BbmzZRb3;
cookieconsent_status=dismiss
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type: application/json; charset=utf-8
Date: Fri, 25 Apr 2025 23:11:40 GMT
Etag: W/"4f-BtWsDO+6UbKwXn+zhLoc64lHywc"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Cloud-Trace-Context: d28bc164452bf02b9b983bf0f2052948
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Length: 79
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/products/search?q=

Identification

PROOF

```
Access-Control-Allow-Origin: *
```

OUTPUT

Vulnerability has been detected on URL 'https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/products/search?q='

To confirm the presence of the vulnerability, this proof has been identified in the target response:

| Access-Control-Allow-Origin: *

The information used to check the vulnerability have been provided in attachment.

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/products/search?q=
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding: gzip
Content-Type: application/json; charset=utf-8
Date: Fri, 25 Apr 2025 23:10:11 GMT
Etag: W/"325f-8he+HyT41TF0TRRd87FqKb7A8Mg"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/

Identification

PROOF

```
Access-Control-Allow-Origin: *
```

OUTPUT

Vulnerability has been detected on URL 'https://juice-shop-16-0-1-178712031365.us-west1.run.app/'

To confirm the presence of the vulnerability, this proof has been identified in the target response:

| Access-Control-Allow-Origin: *

The information used to check the vulnerability have been provided in attachment.

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8
Date: Fri, 25 Apr 2025 23:10:08 GMT
Etag: W/"ea4-1966f2bc520"
Feature-Policy: payment 'self'
Last-Modified: Fri, 25 Apr 2025 22:57:41 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Length: 4619
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/admin/application-version

Identification

PROOF

```
Access-Control-Allow-Origin: *
```

OUTPUT

```
Vulnerability has been detected on URL 'https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/admin/application-version'

To confirm the presence of the vulnerability, this proof has been identified in the target response:

| Access-Control-Allow-Origin: *

The information used to check the vulnerability have been provided in attachment.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/admin/application-version
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type: application/json; charset=utf-8
Date: Fri, 25 Apr 2025 23:10:10 GMT
Etag: W/"14-mWpI2PhnItYY44Y5gln+68A5CNc"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Cloud-Trace-Context: bb00cff05c5f3c45a714d4467a7abcb2
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Length: 20
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/cs_CZ.json

Identification

PROOF

```
Access-Control-Allow-Origin: *
```

OUTPUT

```
Vulnerability has been detected on URL 'https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/cs_CZ.json'

To confirm the presence of the vulnerability, this proof has been identified in the target response:

| Access-Control-Allow-Origin: *

The information used to check the vulnerability have been provided in attachment.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/cs_CZ.json
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=cs_CZ
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
```

```
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: application/json; charset=UTF-8
Date: Sat, 26 Apr 2025 02:29:27 GMT
Etag: W/"8814-18f05ebb708"
Feature-Policy: payment 'self'
Last-Modified: Mon, 22 Apr 2024 13:08:05 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/en.json

Identification

PROOF

```
Access-Control-Allow-Origin: *
```

OUTPUT

```
Vulnerability has been detected on URL 'https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/en.json'

To confirm the presence of the vulnerability, this proof has been identified in the target response:

| Access-Control-Allow-Origin: *

The information used to check the vulnerability have been provided in attachment.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/en.json
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
```

```
Content-Encoding: gzip
Content-Type: application/json; charset=UTF-8
Date: Fri, 25 Apr 2025 23:10:10 GMT
Etag: W/"8175-18f05ebb708"
Feature-Policy: payment 'self'
Last-Modified: Mon, 22 Apr 2024 13:08:05 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/captcha/

Identification

PROOF

```
Access-Control-Allow-Origin: *
```

OUTPUT

```
Vulnerability has been detected on URL 'https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/captcha/'

To confirm the presence of the vulnerability, this proof has been identified in the target response:

| Access-Control-Allow-Origin: *

The information used to check the vulnerability have been provided in attachment.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/captcha/
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: language=en; cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1
If-None-Match: W/"31-6VzwP+6Js6+f/7oOKHud+d4LoO4"
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type: application/json; charset=utf-8
Date: Sat, 26 Apr 2025 02:27:39 GMT
Etag: W/"2f-MIu6CT8WR4M+Wp7TeexBr5Mm7M4"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Cloud-Trace-Context: cd7928d46a143d9e492e25266f1940ed
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
```

```
X-Recruiting: /#/jobs
Content-Length: 47
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/user/whoami

Identification

PROOF

```
Access-Control-Allow-Origin: *
```

OUTPUT

```
Vulnerability has been detected on URL 'https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/user/whoami'

To confirm the presence of the vulnerability, this proof has been identified in the target response:

| Access-Control-Allow-Origin: *

The information used to check the vulnerability have been provided in attachment.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/user/whoami
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: language=en; cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=z67RBJkpxgOw1qjLrbzDM95EnABVfXDUb9A3Y2aePl4VXZvQ8mW7yKo6NXeE
If-None-Match: W/"b-/5bSboVjVhGw3qRgvUfZjE1r1Ns"
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Date: Sat, 26 Apr 2025 01:24:03 GMT
Etag: W/"b-/5bSboVjVhGw3qRgvUfZjE1r1Ns"
Feature-Policy: payment 'self'
Server: Google Frontend
X-Cloud-Trace-Context: 6d1efb72a363df96575e77ebdd395b80
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Vary: Accept-Encoding
Content-Length: 11
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/Quantitys/

Identification

PROOF

```
Access-Control-Allow-Origin: *
```

OUTPUT

```
Vulnerability has been detected on URL 'https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/Quantitys/'

To confirm the presence of the vulnerability, this proof has been identified in the target response:

| Access-Control-Allow-Origin: *

The information used to check the vulnerability have been provided in attachment.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/Quantitys/
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding: gzip
Content-Type: application/json; charset=utf-8
Date: Fri, 25 Apr 2025 23:10:12 GMT
Etag: W/"1767-etMBFb05GTNXcAa1INjMInHcId4"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/et_EE.json

---

Identification

PROOF

```
Access-Control-Allow-Origin: *
```

OUTPUT

```
Vulnerability has been detected on URL 'https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/et_EE.json'

To confirm the presence of the vulnerability, this proof has been identified in the target response:

| Access-Control-Allow-Origin: *
```

The information used to check the vulnerability have been provided in attachment.

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/et_EE.json
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=et_EE
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: application/json; charset=UTF-8
Date: Sat, 26 Apr 2025 02:29:56 GMT
Etag: W/"8319-18f05ebb708"
Feature-Policy: payment 'self'
Last-Modified: Mon, 22 Apr 2024 13:08:05 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/Challenges/?name=Score%20Board

Identification

PROOF

```
Access-Control-Allow-Origin: *
```

OUTPUT

```
Vulnerability has been detected on URL 'https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/Challenges/?
name=Score%20Board'

To confirm the presence of the vulnerability, this proof has been identified in the target response:

| Access-Control-Allow-Origin: *

The information used to check the vulnerability have been provided in attachment.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/Challenges/?name=Score%20Board
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type: application/json; charset=utf-8
Date: Fri, 25 Apr 2025 23:10:12 GMT
Etag: W/"288-+JKo65JYfG3LT9Er5ELTcivVYcQ"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Cloud-Trace-Context: 955c7b2840303fd8a714d4467a7ab0e0
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Length: 648
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/de_DE.json

Identification

PROOF

```
Access-Control-Allow-Origin: *
```

OUTPUT

```
Vulnerability has been detected on URL 'https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/de_DE.json'

To confirm the presence of the vulnerability, this proof has been identified in the target response:

| Access-Control-Allow-Origin: *

The information used to check the vulnerability have been provided in attachment.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/de_DE.json
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=de_DE
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: application/json; charset=UTF-8
Date: Sat, 26 Apr 2025 02:29:48 GMT
Etag: W/"904a-18f05ebb708"
Feature-Policy: payment 'self'
Last-Modified: Mon, 22 Apr 2024 13:08:05 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/admin/application-configuration

Identification

PROOF

```
Access-Control-Allow-Origin: *
```

OUTPUT

```
Vulnerability has been detected on URL 'https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/admin/application-configuration'

To confirm the presence of the vulnerability, this proof has been identified in the target response:

| Access-Control-Allow-Origin: *

The information used to check the vulnerability have been provided in attachment.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/admin/application-configuration
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
```

```
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding: gzip
Content-Type: application/json; charset=utf-8
Date: Fri, 25 Apr 2025 23:10:10 GMT
Etag: W/"4993-Oz9kS67Z/2Q7h9VfrxO8V9OVt0M"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/ftp/legal.md

Identification

PROOF

```
Access-Control-Allow-Origin: *
```

OUTPUT

```
Vulnerability has been detected on URL 'https://juice-shop-16-0-1-178712031365.us-west1.run.app/ftp/legal.md'

To confirm the presence of the vulnerability, this proof has been identified in the target response:

| Access-Control-Allow-Origin: *

The information used to check the vulnerability have been provided in attachment.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/ftp/legal.md
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=da_DK
Priority: u=0, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
```

```
Content-Encoding: gzip
Content-Type: text/markdown; charset=UTF-8
Date: Sat, 26 Apr 2025 03:18:01 GMT
Etag: W/"be7-1966fb18775"
Feature-Policy: payment 'self'
Last-Modified: Sat, 26 Apr 2025 01:23:47 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/Feedbacks/

Identification

PROOF

```
Access-Control-Allow-Origin: *
```

OUTPUT

```
Vulnerability has been detected on URL 'https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/Feedbacks/'

To confirm the presence of the vulnerability, this proof has been identified in the target response:

| Access-Control-Allow-Origin: *

The information used to check the vulnerability have been provided in attachment.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/Feedbacks/
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: language=en; cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1
If-None-Match: W/"6c6-1n6pt9X8GncrTGxXY8nLWSP9brU"
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding: gzip
Content-Type: application/json; charset=utf-8
Date: Sat, 26 Apr 2025 02:27:40 GMT
Etag: W/"6c6-SIwkJLL3y8euYH1CiBtnE7PUBNY"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
```

```
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/languages

Identification

PROOF

```
Access-Control-Allow-Origin: *
```

OUTPUT

```
Vulnerability has been detected on URL 'https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/languages'

To confirm the presence of the vulnerability, this proof has been identified in the target response:

| Access-Control-Allow-Origin: *

The information used to check the vulnerability have been provided in attachment.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/languages
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding: gzip
Content-Type: application/json; charset=utf-8
Date: Fri, 25 Apr 2025 23:10:11 GMT
Etag: W/"1308-8EV95V7lUMShnloiieqORKNai/g"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/products/1/reviews

Identification

PROOF

```
Access-Control-Allow-Origin: *
```

OUTPUT

```
Vulnerability has been detected on URL 'https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/products/1/reviews'

To confirm the presence of the vulnerability, this proof has been identified in the target response:

| Access-Control-Allow-Origin: *

The information used to check the vulnerability have been provided in attachment.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/products/1/reviews
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: language=en; cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=z67RBJkpxgOw1qjLrbzDM95EnABVfXDUb9A3Y2aePl4VXZvQ8mW7yKo6NXeE
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type: application/json; charset=utf-8
Date: Sat, 26 Apr 2025 01:24:03 GMT
Etag: W/"ac-+6TYO+tKceLLbG2Ky9HQ7ZcLMWM"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Cloud-Trace-Context: 7eb022bfa1d0336a575e77ebdd395585
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Length: 172
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/fr_FR.json

Identification

PROOF

```
Access-Control-Allow-Origin: *
```

OUTPUT

```
Vulnerability has been detected on URL 'https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/fr_FR.json'

To confirm the presence of the vulnerability, this proof has been identified in the target response:

| Access-Control-Allow-Origin: *

The information used to check the vulnerability have been provided in attachment.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/fr_FR.json
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=fr_FR
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: application/json; charset=UTF-8
Date: Sat, 26 Apr 2025 02:30:23 GMT
Etag: W/"9137-18f05ebb708"
Feature-Policy: payment 'self'
Last-Modified: Mon, 22 Apr 2024 13:08:05 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/az_AZ.json

Identification

PROOF

```
Access-Control-Allow-Origin: *
```

OUTPUT

```
Vulnerability has been detected on URL 'https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/az_AZ.json'

To confirm the presence of the vulnerability, this proof has been identified in the target response:

| Access-Control-Allow-Origin: *

The information used to check the vulnerability have been provided in attachment.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/az_AZ.json
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=az_AZ
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: application/json; charset=UTF-8
Date: Sat, 26 Apr 2025 02:28:35 GMT
Etag: W/"8cc1-18f05ebb708"
Feature-Policy: payment 'self'
Last-Modified: Mon, 22 Apr 2024 13:08:05 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/id_ID.json

Identification

PROOF

```
Access-Control-Allow-Origin: *
```

OUTPUT

```
Vulnerability has been detected on URL 'https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/id_ID.json'

To confirm the presence of the vulnerability, this proof has been identified in the target response:

| Access-Control-Allow-Origin: *

The information used to check the vulnerability have been provided in attachment.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/id_ID.json
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=id_ID
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: application/json; charset=UTF-8
Date: Sat, 26 Apr 2025 02:28:52 GMT
Etag: W/"8269-18f05ebb708"
Feature-Policy: payment 'self'
Last-Modified: Mon, 22 Apr 2024 13:08:05 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/memories/

Identification

PROOF

```
Access-Control-Allow-Origin: *
```

OUTPUT

```
Vulnerability has been detected on URL 'https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/memories/'

To confirm the presence of the vulnerability, this proof has been identified in the target response:

| Access-Control-Allow-Origin: *

The information used to check the vulnerability have been provided in attachment.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/memories/
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: language=en; continueCode=z67RBJkpxgOw1qjLrbzDM95EnABVfXDUb9A3Y2aePl4VXZvQ8mW7yKo6NXeE;
cookieconsent_status=dismiss; welcomebanner_status=dismiss
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding: gzip
Content-Type: application/json; charset=utf-8
Date: Sat, 26 Apr 2025 02:27:38 GMT
Etag: W/"e22-k4t/skONyGpeL9C7mhMGOYDLOnc"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/ca_ES.json

Identification

PROOF

```
Access-Control-Allow-Origin: *
```

OUTPUT

```
Vulnerability has been detected on URL 'https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/ca_ES.json'

To confirm the presence of the vulnerability, this proof has been identified in the target response:

| Access-Control-Allow-Origin: *

The information used to check the vulnerability have been provided in attachment.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/ca_ES.json
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=ca_ES
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: application/json; charset=UTF-8
Date: Sat, 26 Apr 2025 02:29:02 GMT
Etag: W/"826e-18f05ebb708"
Feature-Policy: payment 'self'
Last-Modified: Mon, 22 Apr 2024 13:08:05 GMT
```

```
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/redirect?to=https://github.com/juice-shop/juice-shop

Identification

PROOF

```
Access-Control-Allow-Origin: *
```

OUTPUT

```
Vulnerability has been detected on URL 'https://juice-shop-16-0-1-178712031365.us-west1.run.app/redirect?
to=https://github.com/juice-shop/juice-shop'

To confirm the presence of the vulnerability, this proof has been identified in the target response:

| Access-Control-Allow-Origin: *

The information used to check the vulnerability have been provided in attachment.
```

HTTP Info

REQUEST MADE

```
GET /redirect?to=https://github.com/juice-shop/juice-shop HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-16-0-1-178712031365.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: language=az_AZ; continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1;
cookieconsent_status=dismiss; welcomebanner_status=dismiss
```

RESPONSE HEADERS

```
HTTP/2 302
access-control-allow-origin: *
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
feature-policy: payment 'self'
x-recruiting: /#/jobs
location: https://github.com/juice-shop/juice-shop
vary: Accept, Accept-Encoding
content-type: text/plain; charset=utf-8
x-cloud-trace-context: 1eafad5317ef340d6ae0ff32a268b67f
date: Sat, 26 Apr 2025 05:21:56 GMT
server: Google Frontend
content-length: 62
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/da_DK.json

Identification

PROOF

```
Access-Control-Allow-Origin: *
```

OUTPUT

```
Vulnerability has been detected on URL 'https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/da_DK.json'

To confirm the presence of the vulnerability, this proof has been identified in the target response:

| Access-Control-Allow-Origin: *

The information used to check the vulnerability have been provided in attachment.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/da_DK.json
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=da_DK
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: application/json; charset=UTF-8
Date: Sat, 26 Apr 2025 02:29:39 GMT
Etag: W/"85dd-18f05ebb708"
Feature-Policy: payment 'self'
Last-Modified: Mon, 22 Apr 2024 13:08:05 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

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	2.1
CVSSV4 VECTOR	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:A/VC:N/VI:L/VA:N/SC:L/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: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 (1)

VULNERABILITY LOW PLUGIN ID 98060

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/socket.io/?EIO=4&transport=polling&t=PPlDpDO

Identification

OUTPUT

```
Page https://juice-shop-16-0-1-178712031365.us-west1.run.app/socket.io/?EIO=4&transport=polling&t=PPlDpDO has no X-Frame-Options header defined
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/socket.io/?EIO=4&transport=polling&t=PPlDpDO
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: http://localhost:4200
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type: text/plain; charset=UTF-8
Date: Fri, 25 Apr 2025 23:10:10 GMT
Server: Google Frontend
Vary: Origin
X-Cloud-Trace-Context: 3beb321db23497f8a714d4467a7ab714
Content-Length: 96
```

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 (4)

VULNERABILITY LOW PLUGIN ID 98063

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/

INPUT TYPE	cookie
INPUT NAME	cookieconsent_status

Identification

PROOF

```
cookieconsent_status=dismiss; Path=/; Expires=2026-04-25 23:10:31 +0000
```

OUTPUT

```
The scanner detected a cookie named 'cookieconsent_status' 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 https://juice-shop-16-0-1-178712031365.us-west1.run.app/
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8
Date: Fri, 25 Apr 2025 23:10:10 GMT
Etag: W/"ea4-1966f2bc520"
Feature-Policy: payment 'self'
Last-Modified: Fri, 25 Apr 2025 22:57:41 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
```

```
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Length: 5055
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/

INPUT TYPE	cookie
INPUT NAME	language

Identification

PROOF

```
language=en; Path=/; Expires=2026-04-25 23:10:11 +0000
```

OUTPUT

```
The scanner detected a cookie named 'language' 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 https://juice-shop-16-0-1-178712031365.us-west1.run.app/
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8
Date: Fri, 25 Apr 2025 23:10:10 GMT
Etag: W/"ea4-1966f2bc520"
Feature-Policy: payment 'self'
Last-Modified: Fri, 25 Apr 2025 22:57:41 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
```

```
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Length: 5055
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/

INPUT TYPE	cookie
INPUT NAME	continueCode

Identification

PROOF

```
continueCode=z67RBJkpxgOw1qjLrbzDM95EnABVfXDUb9A3Y2aePl4VXZvQ8mW7yKo6NXeE; Path=/; Expires=2026-04-25 23:16:47 +0000
```

OUTPUT

```
The scanner detected a cookie named 'continueCode' 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 https://juice-shop-16-0-1-178712031365.us-west1.run.app/
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8
Date: Fri, 25 Apr 2025 23:10:10 GMT
Etag: W/"ea4-1966f2bc520"
Feature-Policy: payment 'self'
Last-Modified: Fri, 25 Apr 2025 22:57:41 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
```

```
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Length: 5055
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/

INPUT TYPE	cookie
INPUT NAME	welcomebanner_status

Identification

PROOF

```
welcomebanner_status=dismiss; Path=/; Expires=2026-04-25 23:13:45 +0000
```

OUTPUT

```
The scanner detected a cookie named 'welcomebanner_status' 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 https://juice-shop-16-0-1-178712031365.us-west1.run.app/
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8
Date: Fri, 25 Apr 2025 23:10:10 GMT
Etag: W/"ea4-1966f2bc520"
Feature-Policy: payment 'self'
Last-Modified: Fri, 25 Apr 2025 22:57:41 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
```

```
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Length: 5055
```

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 (4)

VULNERABILITY LOW PLUGIN ID 98064

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/

INPUT TYPE	cookie
INPUT NAME	continueCode

Identification

PROOF

```
continueCode=z67RBJkpxgOw1qjLrbzDM95EnABVfXDUb9A3Y2aePl4VXZvQ8mW7yKo6NXeE; Path=/; Expires=2026-04-25 23:16:47 +0000
```

OUTPUT

```
The scanner detected a cookie named 'continueCode' set with JavaScript without the Secure flag set.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8
Date: Fri, 25 Apr 2025 23:10:10 GMT
Etag: W/"ea4-1966f2bc520"
Feature-Policy: payment 'self'
Last-Modified: Fri, 25 Apr 2025 22:57:41 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Length: 5055
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/

INPUT TYPE	cookie
INPUT NAME	cookieconsent_status

Identification

PROOF

```
cookieconsent_status=dismiss; Path=/; Expires=2026-04-25 23:10:31 +0000
```

OUTPUT

```
The scanner detected a cookie named 'cookieconsent_status' set with JavaScript without the Secure flag set.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8
Date: Fri, 25 Apr 2025 23:10:10 GMT
Etag: W/"ea4-1966f2bc520"
Feature-Policy: payment 'self'
Last-Modified: Fri, 25 Apr 2025 22:57:41 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Length: 5055
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/

INPUT TYPE	cookie
INPUT NAME	welcomebanner_status

Identification

PROOF

```
welcomebanner_status=dismiss; Path=/; Expires=2026-04-25 23:13:45 +0000
```

OUTPUT

```
The scanner detected a cookie named 'welcomebanner_status' set with JavaScript without the Secure flag set.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8
Date: Fri, 25 Apr 2025 23:10:10 GMT
Etag: W/"ea4-1966f2bc520"
Feature-Policy: payment 'self'
Last-Modified: Fri, 25 Apr 2025 22:57:41 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Length: 5055
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/

INPUT TYPE	cookie
INPUT NAME	language

Identification

PROOF

```
language=en; Path=/; Expires=2026-04-25 23:10:11 +0000
```

OUTPUT

```
The scanner detected a cookie named 'language' set with JavaScript without the Secure flag set.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8
Date: Fri, 25 Apr 2025 23:10:10 GMT
Etag: W/"ea4-1966f2bc520"
Feature-Policy: payment 'self'
Last-Modified: Fri, 25 Apr 2025 22:57:41 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Length: 5055
```

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-16-0-1-178712031365.us-west1.run.app/assets/i18n/fr_FR.json

Identification

OUTPUT

```
The following header information disclosures have been detected on https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/fr_FR.json:

- Server: Google Frontend
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/fr_FR.json
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=fr_FR
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: application/json; charset=UTF-8
Date: Sat, 26 Apr 2025 02:30:23 GMT
Etag: W/"9137-18f05ebb708"
Feature-Policy: payment 'self'
Last-Modified: Mon, 22 Apr 2024 13:08:05 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/Feedbacks/

Identification

OUTPUT

The following header information disclosures have been detected on https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/Feedbacks/:

- Server: Google Frontend

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/Feedbacks/
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: language=en; cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1
If-None-Match: W/"6c6-1n6pt9X8GncrTGxXY8nLWSP9brU"
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding: gzip
Content-Type: application/json; charset=utf-8
Date: Sat, 26 Apr 2025 02:27:40 GMT
Etag: W/"6c6-SIwkJLL3y8euYH1CiBtnE7PUBNY"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/de_DE.json

Identification

OUTPUT

The following header information disclosures have been detected on https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/de_DE.json:

- Server: Google Frontend

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/de_DE.json
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
```

```
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=de_DE
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: application/json; charset=UTF-8
Date: Sat, 26 Apr 2025 02:29:48 GMT
Etag: W/"904a-18f05ebb708"
Feature-Policy: payment 'self'
Last-Modified: Mon, 22 Apr 2024 13:08:05 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/az_AZ.json

Identification

OUTPUT

```
The following header information disclosures have been detected on https://juice-shop-16-0-1-178712031365.us-west1.run.
app/assets/i18n/az_AZ.json:

- Server: Google Frontend
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/az_AZ.json
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=az_AZ
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
```

```
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: application/json; charset=UTF-8
Date: Sat, 26 Apr 2025 02:28:35 GMT
Etag: W/"8cc1-18f05ebb708"
Feature-Policy: payment 'self'
Last-Modified: Mon, 22 Apr 2024 13:08:05 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/admin/application-configuration

Identification

OUTPUT

```
The following header information disclosures have been detected on https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/admin/application-configuration:

- Server: Google Frontend
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/admin/application-configuration
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding: gzip
Content-Type: application/json; charset=utf-8
Date: Fri, 25 Apr 2025 23:10:10 GMT
Etag: W/"4993-Oz9kS67Z/2Q7h9VfrxO8V9OVt0M"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/en.json

Identification

OUTPUT

```
The following header information disclosures have been detected on https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/en.json:

- Server: Google Frontend
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/en.json
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: application/json; charset=UTF-8
Date: Fri, 25 Apr 2025 23:10:10 GMT
Etag: W/"8175-18f05ebb708"
Feature-Policy: payment 'self'
Last-Modified: Mon, 22 Apr 2024 13:08:05 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/products/search?q=

Identification

OUTPUT

```
The following header information disclosures have been detected on https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/products/search?q=:

- Server: Google Frontend
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/products/search?q=
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding: gzip
Content-Type: application/json; charset=utf-8
Date: Fri, 25 Apr 2025 23:10:11 GMT
Etag: W/"325f-8he+HyT41TF0TRRd87FqKb7A8Mg"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/et_EE.json

Identification

OUTPUT

```
The following header information disclosures have been detected on https://juice-shop-16-0-1-178712031365.us-west1.run.
app/assets/i18n/et_EE.json:

- Server: Google Frontend
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/et_EE.json
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=et_EE
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
```

```
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: application/json; charset=UTF-8
Date: Sat, 26 Apr 2025 02:29:56 GMT
Etag: W/"8319-18f05ebb708"
Feature-Policy: payment 'self'
Last-Modified: Mon, 22 Apr 2024 13:08:05 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/continue-code

Identification

OUTPUT

```
The following header information disclosures have been detected on https://juice-shop-16-0-1-178712031365.us-west1.run.
app/rest/continue-code:

- Server: Google Frontend
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/continue-code
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: language=en; continueCode=aj4QDO4KyOqPJ7j2novp9EQ38gYVAJlGM1wWxalND5reZRLzmXk6BbmzZRb3;
cookieconsent_status=dismiss
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type: application/json; charset=utf-8
Date: Fri, 25 Apr 2025 23:11:40 GMT
Etag: W/"4f-BtWsDO+6UbKwXn+zhLoc64lHywc"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Cloud-Trace-Context: d28bc164452bf02b9b983bf0f2052948
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Length: 79
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/cs_CZ.json

Identification

OUTPUT

```
The following header information disclosures have been detected on https://juice-shop-16-0-1-178712031365.us-west1.run.
app/assets/i18n/cs_CZ.json:

- Server: Google Frontend
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/cs_CZ.json
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=cs_CZ
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: application/json; charset=UTF-8
Date: Sat, 26 Apr 2025 02:29:27 GMT
Etag: W/"8814-18f05ebb708"
Feature-Policy: payment 'self'
Last-Modified: Mon, 22 Apr 2024 13:08:05 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/admin/application-version

Identification

OUTPUT

```
The following header information disclosures have been detected on https://juice-shop-16-0-1-178712031365.us-west1.run.
app/rest/admin/application-version:

- Server: Google Frontend
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/admin/application-version
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type: application/json; charset=utf-8
Date: Fri, 25 Apr 2025 23:10:10 GMT
Etag: W/"14-mWpI2PhnItYY44Y5gln+68A5CNc"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Cloud-Trace-Context: bb00cff05c5f3c45a714d4467a7abcb2
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Length: 20
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/products/1/reviews

Identification

OUTPUT

```
The following header information disclosures have been detected on https://juice-shop-16-0-1-178712031365.us-west1.run.
app/rest/products/1/reviews:

- Server: Google Frontend
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/products/1/reviews
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: language=en; cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=z67RBJkpxgOw1qjLrbzDM95EnABVfXDUb9A3Y2aePl4VXZvQ8mW7yKo6NXeE
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
```

```
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type: application/json; charset=utf-8
Date: Sat, 26 Apr 2025 01:24:03 GMT
Etag: W/"ac-+6TYO+tKceLLbG2Ky9HQ7ZcLMWM"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Cloud-Trace-Context: 7eb022bfa1d0336a575e77ebdd395585
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Length: 172
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/id_ID.json

Identification

OUTPUT

```
The following header information disclosures have been detected on https://juice-shop-16-0-1-178712031365.us-west1.run.
app/assets/i18n/id_ID.json:

- Server: Google Frontend
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/id_ID.json
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=id_ID
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: application/json; charset=UTF-8
Date: Sat, 26 Apr 2025 02:28:52 GMT
Etag: W/"8269-18f05ebb708"
Feature-Policy: payment 'self'
Last-Modified: Mon, 22 Apr 2024 13:08:05 GMT
Server: Google Frontend
```

```
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/Challenges/?name=Score%20Board

Identification

OUTPUT

```
The following header information disclosures have been detected on https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/Challenges/?name=Score%20Board:

- Server: Google Frontend
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/Challenges/?name=Score%20Board
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type: application/json; charset=utf-8
Date: Fri, 25 Apr 2025 23:10:12 GMT
Etag: W/"288-+JKo65JYfG3LT9Er5ELTcivVYcQ"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Cloud-Trace-Context: 955c7b2840303fd8a714d4467a7ab0e0
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Length: 648
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/socket.io/?EIO=4&transport=polling&t=PPIDpDO

Identification

OUTPUT

```
The following header information disclosures have been detected on https://juice-shop-16-0-1-178712031365.us-west1.run.app/socket.io/?EIO=4&transport=polling&t=PPlDpDO:

- Server: Google Frontend
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/socket.io/?EIO=4&transport=polling&t=PPlDpDO
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: http://localhost:4200
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type: text/plain; charset=UTF-8
Date: Fri, 25 Apr 2025 23:10:10 GMT
Server: Google Frontend
Vary: Origin
X-Cloud-Trace-Context: 3beb321db23497f8a714d4467a7ab714
Content-Length: 96
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/da_DK.json

Identification

OUTPUT

```
The following header information disclosures have been detected on https://juice-shop-16-0-1-178712031365.us-west1.run.
app/assets/i18n/da_DK.json:

- Server: Google Frontend
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/da_DK.json
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=da_DK
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: application/json; charset=UTF-8
Date: Sat, 26 Apr 2025 02:29:39 GMT
Etag: W/"85dd-18f05ebb708"
Feature-Policy: payment 'self'
Last-Modified: Mon, 22 Apr 2024 13:08:05 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/languages

Identification

OUTPUT

```
The following header information disclosures have been detected on https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/languages:

- Server: Google Frontend
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/languages
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding: gzip
Content-Type: application/json; charset=utf-8
Date: Fri, 25 Apr 2025 23:10:11 GMT
Etag: W/"1308-8EV95V7lUMShnloiieqORKNai/g"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/es_ES.json

Identification

OUTPUT

```
The following header information disclosures have been detected on https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/es_ES.json:

- Server: Google Frontend
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/es_ES.json
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=es_ES
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: application/json; charset=UTF-8
Date: Sat, 26 Apr 2025 02:30:16 GMT
Etag: W/"8d7b-18f05ebb708"
Feature-Policy: payment 'self'
Last-Modified: Mon, 22 Apr 2024 13:08:05 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/user/whoami

Identification

OUTPUT

```
The following header information disclosures have been detected on https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/user/whoami:

- Server: Google Frontend
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/user/whoami
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: language=en; cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=z67RBJkpxgOw1qjLrbzDM95EnABVfXDUb9A3Y2aePl4VXZvQ8mW7yKo6NXeE
If-None-Match: W/"b-/5bSboVjVhGw3qRgvUfZjE1r1Ns"
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Date: Sat, 26 Apr 2025 01:24:03 GMT
Etag: W/"b-/5bSboVjVhGw3qRgvUfZjE1r1Ns"
Feature-Policy: payment 'self'
Server: Google Frontend
X-Cloud-Trace-Context: 6d1efb72a363df96575e77ebdd395b80
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Vary: Accept-Encoding
Content-Length: 11
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/captcha/

Identification

OUTPUT

```
The following header information disclosures have been detected on https://juice-shop-16-0-1-178712031365.us-west1.run.
app/rest/captcha/:

- Server: Google Frontend
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/captcha/
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: language=en; cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1
If-None-Match: W/"31-6VzwP+6Js6+f/7oOKHud+d4LoO4"
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type: application/json; charset=utf-8
Date: Sat, 26 Apr 2025 02:27:39 GMT
Etag: W/"2f-MIu6CT8WR4M+Wp7TeexBr5Mm7M4"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Cloud-Trace-Context: cd7928d46a143d9e492e25266f1940ed
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Length: 47
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/Quantitys/

Identification

OUTPUT

```
The following header information disclosures have been detected on https://juice-shop-16-0-1-178712031365.us-west1.run.
app/api/Quantitys/:

- Server: Google Frontend
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/Quantitys/
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding: gzip
Content-Type: application/json; charset=utf-8
Date: Fri, 25 Apr 2025 23:10:12 GMT
Etag: W/"1767-etMBFb05GTNXcAa1INjMInHcId4"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
```

```
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/ftp/legal.md

Identification

OUTPUT

```
The following header information disclosures have been detected on https://juice-shop-16-0-1-178712031365.us-west1.run.
app/ftp/legal.md:

- Server: Google Frontend
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/ftp/legal.md
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=da_DK
Priority: u=0, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: text/markdown; charset=UTF-8
Date: Sat, 26 Apr 2025 03:18:01 GMT
Etag: W/"be7-1966fb18775"
Feature-Policy: payment 'self'
Last-Modified: Sat, 26 Apr 2025 01:23:47 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/ca_ES.json

Identification

OUTPUT

```
The following header information disclosures have been detected on https://juice-shop-16-0-1-178712031365.us-west1.run.
app/assets/i18n/ca_ES.json:

- Server: Google Frontend
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/ca_ES.json
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=ca_ES
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: application/json; charset=UTF-8
Date: Sat, 26 Apr 2025 02:29:02 GMT
Etag: W/"826e-18f05ebb708"
Feature-Policy: payment 'self'
Last-Modified: Mon, 22 Apr 2024 13:08:05 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/

Identification

OUTPUT

```
The following header information disclosures have been detected on https://juice-shop-16-0-1-178712031365.us-west1.run.
app/:

- Server: Google Frontend
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8
Date: Fri, 25 Apr 2025 23:10:08 GMT
Etag: W/"ea4-1966f2bc520"
Feature-Policy: payment 'self'
Last-Modified: Fri, 25 Apr 2025 22:57:41 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Length: 4619
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/memories/

Identification

OUTPUT

```
The following header information disclosures have been detected on https://juice-shop-16-0-1-178712031365.us-west1.run.
app/rest/memories/:

- Server: Google Frontend
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/memories/
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
```

```
Accept-Language: en-US,en;q=0.5
Cookie: language=en; continueCode=z67RBJkpxgOw1qjLrbzDM95EnABVfXDUb9A3Y2aePl4VXZvQ8mW7yKo6NXeE;
cookieconsent_status=dismiss; welcomebanner_status=dismiss
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding: gzip
Content-Type: application/json; charset=utf-8
Date: Sat, 26 Apr 2025 02:27:38 GMT
Etag: W/"e22-k4t/skONyGpeL9C7mhMGOYDLOnc"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

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	2.1
CVSSV4 VECTOR	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:A/VC:L/VI:N/VA:N/SC:L/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	693
WASC	Application Misconfiguration
OWASP	2017-A6, 2013-A5, 2010-A6, 2023-API8, 2019-API7
CVE	-
BID	-

Missing 'X-Content-Type-Options' Header Instances (1)

VULNERABILITY LOW PLUGIN ID 112529

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/socket.io/?EIO=4&transport=polling&t=PPlDpDO

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-16-0-1-178712031365.us-west1.run.app/socket.io/?EIO=4&transport=polling&t=PPlDpDO
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: http://localhost:4200
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type: text/plain; charset=UTF-8
Date: Fri, 25 Apr 2025 23:10:10 GMT
Server: Google Frontend
Vary: Origin
X-Cloud-Trace-Context: 3beb321db23497f8a714d4467a7ab714
Content-Length: 96
```

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-16-0-1-178712031365.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	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	1021
WASC	Application Misconfiguration
OWASP	2017-A6, 2021-A4, 2013-A5, 2010-A6, 2023-API8, 2019-API7
CVE	-

BID	-

Missing Content Security Policy Instances (8)

VULNERABILITY LOW PLUGIN ID 112551

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/ftp/

Identification

OUTPUT

```
https://juice-shop-16-0-1-178712031365.us-west1.run.app/ftp/ has no Content Security Policy defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/ftp/
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=az_AZ
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding: gzip
Content-Type: text/html; charset=utf-8
Date: Sat, 26 Apr 2025 06:13:25 GMT
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Length: 11894
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/ftp/quarantine

Identification

OUTPUT
https://juice-shop-16-0-1-178712031365.us-west1.run.app/ftp/quarantine has no Content Security Policy defined.

HTTP Info

REQUEST MADE
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/ftp/quarantine

REQUEST HEADERS
```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=az_AZ
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding: gzip
Content-Type: text/html; charset=utf-8
Date: Sat, 26 Apr 2025 07:00:31 GMT
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Length: 10459
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/b2b/v2/orders

Identification

OUTPUT
https://juice-shop-16-0-1-178712031365.us-west1.run.app/b2b/v2/orders has no Content Security Policy defined.

HTTP Info

REQUEST MADE
POST https://juice-shop-16-0-1-178712031365.us-west1.run.app/b2b/v2/orders

REQUEST HEADERS
```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Content-Length: 23
Content-Type: application/json
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=az_AZ
Origin: https://juice-shop-16-0-1-178712031365.us-west1.run.app
```

```
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/api-docs/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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 500
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding: gzip
Content-Type: text/html; charset=utf-8
Date: Sat, 26 Apr 2025 05:53:59 GMT
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Cloud-Trace-Context: 5d8dbc8b0e4649841f389aba1b27aeb2
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Length: 958
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/

Identification

OUTPUT

```
https://juice-shop-16-0-1-178712031365.us-west1.run.app/ has no Content Security Policy defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
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
Access-Control-Allow-Origin: *
```

```
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8
Date: Fri, 25 Apr 2025 23:10:08 GMT
Etag: W/"ea4-1966f2bc520"
Feature-Policy: payment 'self'
Last-Modified: Fri, 25 Apr 2025 22:57:41 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Length: 4619
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/api-docs/

Identification

OUTPUT

```
https://juice-shop-16-0-1-178712031365.us-west1.run.app/api-docs/ has no Content Security Policy defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/api-docs/
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=az_AZ
If-None-Match: W/"c22-H8FH9nKD8DeX/nvIRrte6ZjP2a4"
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Date: Sat, 26 Apr 2025 05:33:11 GMT
Etag: W/"c22-H8FH9nKD8DeX/nvIRrte6ZjP2a4"
Feature-Policy: payment 'self'
Server: Google Frontend
X-Cloud-Trace-Context: b20775ae703a7d2cc1e2eac79d916b92
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Encoding: gzip
Content-Length: 3977
Content-Type: text/html; charset=utf-8
Vary: Accept-Encoding
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/ftp/quarantine/

Identification

OUTPUT

```
https://juice-shop-16-0-1-178712031365.us-west1.run.app/ftp/quarantine/ has no Content Security Policy defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/ftp/quarantine/
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss; language=az_AZ;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding: gzip
Content-Type: text/html; charset=utf-8
Date: Sat, 26 Apr 2025 08:11:45 GMT
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Length: 10409
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/ftp/coupons_2013.md.bak

Identification

OUTPUT

```
https://juice-shop-16-0-1-178712031365.us-west1.run.app/ftp/coupons_2013.md.bak has no Content Security Policy defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/ftp/coupons_2013.md.bak
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
```

```
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=az_AZ
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 403
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding: gzip
Content-Type: text/html; charset=utf-8
Date: Sat, 26 Apr 2025 07:24:52 GMT
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Cloud-Trace-Context: 38f6b36e31409bc448fc2d8078310ed0
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Length: 781
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/public/images/uploads/%F0%9F%98%BC-

Identification

OUTPUT

```
https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/public/images/uploads/%F0%9F%98%BC- has no Content
Security Policy defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/public/images/uploads/%F0%9F%98%BC-
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=az_AZ
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
```

```
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8
Date: Sat, 26 Apr 2025 06:45:12 GMT
Etag: W/"ea4-19670be8e8c"
Feature-Policy: payment 'self'
Last-Modified: Sat, 26 Apr 2025 06:17:38 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Length: 4619
```

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 (21)

VULNERABILITY LOW PLUGIN ID 112553

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/api-docs/

Identification

OUTPUT

```
https://juice-shop-16-0-1-178712031365.us-west1.run.app/api-docs/ has no Cache Control header defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/api-docs/
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=az_AZ
If-None-Match: W/"c22-H8FH9nKD8DeX/nvIRrte6ZjP2a4"
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Date: Sat, 26 Apr 2025 05:33:11 GMT
Etag: W/"c22-H8FH9nKD8DeX/nvIRrte6ZjP2a4"
Feature-Policy: payment 'self'
Server: Google Frontend
X-Cloud-Trace-Context: b20775ae703a7d2cc1e2eac79d916b92
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Encoding: gzip
Content-Length: 3977
Content-Type: text/html; charset=utf-8
Vary: Accept-Encoding
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/captcha/

Identification

OUTPUT

```
https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/captcha/ has no Cache Control header defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/captcha/
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: language=en; cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1
If-None-Match: W/"31-6VzwP+6Js6+f/7oOKHud+d4LoO4"
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type: application/json; charset=utf-8
Date: Sat, 26 Apr 2025 02:27:39 GMT
Etag: W/"2f-MIu6CT8WR4M+Wp7TeexBr5Mm7M4"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Cloud-Trace-Context: cd7928d46a143d9e492e25266f1940ed
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Length: 47
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/products/1/reviews

Identification

OUTPUT

```
https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/products/1/reviews has no Cache Control header defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/products/1/reviews
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: language=en; cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=z67RBJkpxgOw1qjLrbzDM95EnABVfXDUb9A3Y2aePl4VXZvQ8mW7yKo6NXeE
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
```

```
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type: application/json; charset=utf-8
Date: Sat, 26 Apr 2025 01:24:03 GMT
Etag: W/"ac-+6TYO+tKceLLbG2Ky9HQ7ZcLMWM"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Cloud-Trace-Context: 7eb022bfa1d0336a575e77ebdd395585
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Length: 172
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/socket.io/?EIO=4&transport=polling&t=PPlDpDO

Identification

OUTPUT

```
https://juice-shop-16-0-1-178712031365.us-west1.run.app/socket.io/?EIO=4&transport=polling&t=PPlDpDO has no Cache Control header defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/socket.io/?EIO=4&transport=polling&t=PPlDpDO
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: http://localhost:4200
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type: text/plain; charset=UTF-8
Date: Fri, 25 Apr 2025 23:10:10 GMT
Server: Google Frontend
Vary: Origin
X-Cloud-Trace-Context: 3beb321db23497f8a714d4467a7ab714
Content-Length: 96
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/Quantitys/

Identification

OUTPUT

```
https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/Quantitys/ has no Cache Control header defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/Quantitys/
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding: gzip
Content-Type: application/json; charset=utf-8
Date: Fri, 25 Apr 2025 23:10:12 GMT
Etag: W/"1767-etMBFb05GTNXcAa1INjMInHcId4"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/Feedbacks/

Identification

OUTPUT

```
https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/Feedbacks/ has no Cache Control header defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/Feedbacks/
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: language=en; cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1
If-None-Match: W/"6c6-1n6pt9X8GncrTGxXY8nLWSP9brU"
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding: gzip
Content-Type: application/json; charset=utf-8
Date: Sat, 26 Apr 2025 02:27:40 GMT
Etag: W/"6c6-SIwkJLL3y8euYH1CiBtnE7PUBNY"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/ftp/quarantine

Identification

OUTPUT

```
https://juice-shop-16-0-1-178712031365.us-west1.run.app/ftp/quarantine has no Cache Control header defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/ftp/quarantine
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=az_AZ
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding: gzip
Content-Type: text/html; charset=utf-8
Date: Sat, 26 Apr 2025 07:00:31 GMT
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
```

```
X-Recruiting: /#/jobs
Content-Length: 10459
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/user/whoami

Identification

OUTPUT

```
https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/user/whoami has no Cache Control header defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/user/whoami
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: language=en; cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=z67RBJkpxgOw1qjLrbzDM95EnABVfXDUb9A3Y2aePl4VXZvQ8mW7yKo6NXeE
If-None-Match: W/"b-/5bSboVjVhGw3qRgvUfZjE1r1Ns"
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Date: Sat, 26 Apr 2025 01:24:03 GMT
Etag: W/"b-/5bSboVjVhGw3qRgvUfZjE1r1Ns"
Feature-Policy: payment 'self'
Server: Google Frontend
X-Cloud-Trace-Context: 6d1efb72a363df96575e77ebdd395b80
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Vary: Accept-Encoding
Content-Length: 11
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/products/search?q=

Identification

OUTPUT

```
https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/products/search?q= has no Cache Control header defined.
```

HTTP Info

REQUEST MADE
```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/products/search?q=
```

REQUEST HEADERS
```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding: gzip
Content-Type: application/json; charset=utf-8
Date: Fri, 25 Apr 2025 23:10:11 GMT
Etag: W/"325f-8he+HyT41TF0TRRd87FqKb7A8Mg"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/memories/

Identification

OUTPUT
```
https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/memories/ has no Cache Control header defined.
```

HTTP Info

REQUEST MADE
```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/memories/
```

REQUEST HEADERS
```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: language=en; continueCode=z67RBJkpxgOw1qjLrbzDM95EnABVfXDUb9A3Y2aePl4VXZvQ8mW7yKo6NXeE;
cookieconsent_status=dismiss; welcomebanner_status=dismiss
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
```

```
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding: gzip
Content-Type: application/json; charset=utf-8
Date: Sat, 26 Apr 2025 02:27:38 GMT
Etag: W/"e22-k4t/skONyGpeL9C7mhMGOYDLOnc"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/admin/application-version

Identification

OUTPUT

```
https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/admin/application-version has no Cache Control header defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/admin/application-version
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type: application/json; charset=utf-8
Date: Fri, 25 Apr 2025 23:10:10 GMT
Etag: W/"14-mWpI2PhnItYY44Y5gln+68A5CNc"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Cloud-Trace-Context: bb00cff05c5f3c45a714d4467a7abcb2
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Length: 20
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/continue-code

Identification

OUTPUT
https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/continue-code has no Cache Control header defined.

HTTP Info

REQUEST MADE
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/continue-code

REQUEST HEADERS
```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: language=en; continueCode=aj4QDO4KyOqPJ7j2novp9EQ38gYVAJlGM1wWxalND5reZRLzmXk6BbmzZRb3;
cookieconsent_status=dismiss
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type: application/json; charset=utf-8
Date: Fri, 25 Apr 2025 23:11:40 GMT
Etag: W/"4f-BtWsDO+6UbKwXn+zhLoc64lHywc"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Cloud-Trace-Context: d28bc164452bf02b9b983bf0f2052948
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Length: 79
```

INSTANCE
https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/Challenges/?name=Score%20Board

Identification

OUTPUT
https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/Challenges/?name=Score%20Board has no Cache Control header defined.

HTTP Info

REQUEST MADE
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/Challenges/?name=Score%20Board

REQUEST HEADERS
```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type: application/json; charset=utf-8
Date: Fri, 25 Apr 2025 23:10:12 GMT
Etag: W/"288-+JKo65JYfG3LT9Er5ELTcivVYcQ"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Cloud-Trace-Context: 955c7b2840303fd8a714d4467a7ab0e0
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Length: 648
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/products/1/reviews/

Identification

OUTPUT

```
https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/products/1/reviews/ has no Cache Control header defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/products/1/reviews/
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=az_AZ
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type: application/json; charset=utf-8
Date: Sat, 26 Apr 2025 06:30:52 GMT
Etag: W/"ac-7FsXWosAZjri4hTxbusL6AUkxzo"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Cloud-Trace-Context: 8e6939989caf03e82009381e989092e4
X-Content-Type-Options: nosniff
```

```
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Length: 172
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/ftp/quarantine/

Identification

OUTPUT

```
https://juice-shop-16-0-1-178712031365.us-west1.run.app/ftp/quarantine/ has no Cache Control header defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/ftp/quarantine/
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss; language=az_AZ;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding: gzip
Content-Type: text/html; charset=utf-8
Date: Sat, 26 Apr 2025 08:11:45 GMT
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Length: 10409
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/ftp/

Identification

OUTPUT

```
https://juice-shop-16-0-1-178712031365.us-west1.run.app/ftp/ has no Cache Control header defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/ftp/
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=az_AZ
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding: gzip
Content-Type: text/html; charset=utf-8
Date: Sat, 26 Apr 2025 06:13:25 GMT
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Length: 11894
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/admin/application-configuration

Identification

OUTPUT

```
https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/admin/application-configuration has no Cache Control
header defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/admin/application-configuration
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding: gzip
Content-Type: application/json; charset=utf-8
Date: Fri, 25 Apr 2025 23:10:10 GMT
Etag: W/"4993-Oz9kS67Z/2Q7h9VfrxO8V9OVt0M"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/products/search/

Identification

OUTPUT

```
https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/products/search/ has no Cache Control header defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/products/search/
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=az_AZ
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

```
H3 200
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding: gzip
Content-Type: application/json; charset=utf-8
Date: Sat, 26 Apr 2025 06:14:03 GMT
Etag: W/"325f-UjwuZzt119LmgzDMfSC13X+cYs4"
```

```
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/ftp/coupons_2013.md.bak

Identification

OUTPUT

```
https://juice-shop-16-0-1-178712031365.us-west1.run.app/ftp/coupons_2013.md.bak has no Cache Control header defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/ftp/coupons_2013.md.bak
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=az_AZ
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 403
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding: gzip
Content-Type: text/html; charset=utf-8
Date: Sat, 26 Apr 2025 07:24:52 GMT
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Cloud-Trace-Context: 38f6b36e31409bc448fc2d8078310ed0
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Length: 781
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/languages

Identification

OUTPUT

```
https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/languages has no Cache Control header defined.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/languages
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding: gzip
Content-Type: application/json; charset=utf-8
Date: Fri, 25 Apr 2025 23:10:11 GMT
Etag: W/"1308-8EV95V7lUMShnloiieqORKNai/g"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/b2b/v2/orders

Identification

OUTPUT

```
https://juice-shop-16-0-1-178712031365.us-west1.run.app/b2b/v2/orders has no Cache Control header defined.
```

HTTP Info

REQUEST MADE

```
POST https://juice-shop-16-0-1-178712031365.us-west1.run.app/b2b/v2/orders
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Content-Length: 23
Content-Type: application/json
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=az_AZ
Origin: https://juice-shop-16-0-1-178712031365.us-west1.run.app
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/api-docs/
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: empty
Sec-Fetch-Mode: cors
```

```
Sec-Fetch-Site: same-origin
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 500
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding: gzip
Content-Type: text/html; charset=utf-8
Date: Sat, 26 Apr 2025 05:53:59 GMT
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Cloud-Trace-Context: 5d8dbc8b0e4649841f389aba1b27aeb2
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Length: 958
```

Username Disclosure

VULNERABILITY LOW PLUGIN ID 114615

Description

Web Applications can sometimes expose web applications users in various places such as HTML comments, JavaScript code or API requests. By leveraging this information, an attacker can gather information and build further attacks against the target application.

Solution

Avoid disclosing usernames in your application content.

See Also

https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/01-Information_Gathering/05-Review_Web_Page_Content_for_Information_Leakage

Plugin Details

PUBLICATION DATE	2025-03-11T00:00:00+00:00
MODIFICATION DATE	2025-03-11T00:00:00+00:00
FAMILY	Data Exposure
SEVERITY	Low
PLUGIN ID	114615

Risk Information

CVSSV4 BASE SCORE	2.3
CVSSV4 VECTOR	CVSS:4.0/AV:N/AC:H/AT:P/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	16, 200
WASC	Application Misconfiguration, Information Leakage
OWASP	2021-A5, 2017-A6, 2021-A1, 2013-A5, 2010-A6, 2023-API8, 2023-API3, 2019-API3, 2019-API7
CVE	-
BID	-

Username Disclosure Instances (3)

VULNERABILITY LOW PLUGIN ID 114615

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/admin/application-configuration/

Identification

PROOF

```
The following patterns were detected in the HTTP response body :
- "user":"bjoernGoogle"
```

OUTPUT

```
The scanner identified one or more `Generic` username(s) on the target page.
```

HTTP Info

REQUEST MADE

```
GET /rest/admin/application-configuration/?
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=&x=&x=&x=&x=&x=&x=&x=&x=
HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-16-0-1-178712031365.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: language=en; continueCode=z67RBJkpxgOw1qjLrbzDM95EnABVfXDUb9A3Y2aePl4VXZvQ8mW7yKo6NXeE;
cookieconsent_status=dismiss; welcomebanner_status=dismiss
```

RESPONSE HEADERS

```
HTTP/2 200
access-control-allow-origin: *
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
feature-policy: payment 'self'
x-recruiting: /#/jobs
content-type: application/json; charset=utf-8
etag: W/"4993-Oz9kS67Z/2Q7h9VfrxO8V9OVt0M"
vary: Accept-Encoding
content-encoding: gzip
date: Fri, 25 Apr 2025 23:32:15 GMT
server: Google Frontend
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/memories/

Identification

PROOF

```
The following patterns were detected in the HTTP response body :
- "username":"bkimminich"

- "username":"evmrox"
```

OUTPUT

The scanner identified one or more `Generic` username(s) on the target page.

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/memories/
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: language=en; cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=z67RBJkpxgOw1qjLrbzDM95EnABVfXDUb9A3Y2aePl4VXZvQ8mW7yKo6NXeE
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding: gzip
Content-Type: application/json; charset=utf-8
Date: Fri, 25 Apr 2025 23:25:12 GMT
Etag: W/"e22-FLHwo+MhT//q5XkiU8jz6hJU1ss"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/admin/application-configuration

Identification

PROOF

```
The following patterns were detected in the HTTP response body :
- "user":"bjoernGoogle"
```

OUTPUT

```
The scanner identified one or more `Generic` username(s) on the target page.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/admin/application-configuration
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: language=en; cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=q6BKoaN93W5z7k6Z4rn1JVQOAo8f2xF5yIoLdgewPDmvxMyLpqEXbj28lRYD
If-None-Match: W/"4993-Oz9kS67Z/2Q7h9VfrxO8V9OVt0M"
```

```
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Date: Fri, 25 Apr 2025 23:23:20 GMT
Etag: W/"4993-Oz9kS67Z/2Q7h9VfrxO8V9OVt0M"
Feature-Policy: payment 'self'
Server: Google Frontend
X-Cloud-Trace-Context: a4f7e269845884aebaceb4dfd6f35be8
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Encoding: gzip
Content-Type: application/json; charset=utf-8
Vary: Accept-Encoding
```

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 (4)

VULNERABILITY LOW PLUGIN ID 115540

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/

INPUT TYPE	cookie
INPUT NAME	cookieconsent_status

Identification

PROOF

```
cookieconsent_status=dismiss; Path=/; Expires=2026-04-25 23:10:31 +0000
```

OUTPUT

```
The scanner detected a cookie named 'cookieconsent_status' set with JavaScript which does not have the 'SameSite'
attribute set.
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/

INPUT TYPE	cookie
INPUT NAME	continueCode

Identification

PROOF

```
continueCode=z67RBJkpxgOw1qjLrbzDM95EnABVfXDUb9A3Y2aePl4VXZvQ8mW7yKo6NXeE; Path=/; Expires=2026-04-25 23:16:47 +0000
```

OUTPUT

```
The scanner detected a cookie named 'continueCode' set with JavaScript which does not have the 'SameSite' attribute set.
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/

INPUT TYPE	cookie
INPUT NAME	welcomebanner_status

Identification

PROOF

```
welcomebanner_status=dismiss; Path=/; Expires=2026-04-25 23:13:45 +0000
```

OUTPUT

```
The scanner detected a cookie named 'welcomebanner_status' set with JavaScript which does not have the 'SameSite'
attribute set.
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/

INPUT TYPE	cookie

INPUT NAME	language

Identification

PROOF

```
language=en; Path=/; Expires=2026-04-25 23:10:11 +0000
```

OUTPUT

```
The scanner detected a cookie named 'language' 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-16-0-1-178712031365.us-west1.run.app/#/

Identification

OUTPUT

```
Engine Version 2.32.4-1790
Plugins Version 202504170639
Scan ID 98147a45-d7d1-4fb3-a532-d4d4b2db551e

Start Time 2025-04-25 23:10:05 +0000
Duration 09:02:14

Requests 541973
Crawler Requests 98
Requests/s 20.8353
Mean Response Time 0.1956s

Bandwidth Usage
- Data to Target 356 MB
- Data from Target 6.4 GB

Timeouts Encountered
Network Timeouts 3
Browser Timeouts 0

Browser Respawns 0

HTTP Protocols Detected
- HTTPs


Authentication Identified
- None


Plugins
- 811 have been included per scan policy
- 612 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-16-0-1-178712031365.us-west1.run.app/#/

Identification

OUTPUT

```
The scan has discovered 5122 distinct URLs.

The following is a breakdown of which URLs were audited:

- 43 effectively audited
- 5 not audited due to the page was too similar to another page already audited
- 1 not audited due to not being within the bounds of the user defined scan scope
- 4973 not queued due to the URL being considered redundant with other processed URLs
- 49 not queued due to file extension exclusions
- 31 not queued due to the URL not being in the target domain
- 17 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:

- 126 application/json
- 24 application/json; charset=utf-8
- 5 application/octet-stream
- 36 image/jpeg
- 6 image/png
- 2 text/css; charset=utf-8
- 1454 text/html
- 24 text/html; charset=utf-8
- 3 text/markdown; charset=utf-8
- 3400 text/plain; charset=utf-8

Response times ranged between 0.061378s and 0.281365s.

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-16-0-1-178712031365.us-west1.run.app/#/

Identification

OUTPUT

```
The scanner encountered 3 network timeouts during the scan. See the attachment for more details
```

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-16-0-1-178712031365.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-16-0-1-178712031365.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-16-0-1-178712031365.us-
west1.run.app/'.
```

HTTP Info

REQUEST MADE

```
TRACE / HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-16-0-1-178712031365.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: language=en; continueCode=z67RBJkpxgOw1qjLrbzDM95EnABVfXDUb9A3Y2aePl4VXZvQ8mW7yKo6NXeE;
cookieconsent_status=dismiss; welcomebanner_status=dismiss
```

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-16-0-1-178712031365.us-west1.run.app/api/content/

Identification

PROOF

```
HTTP/2 500
```

OUTPUT

```
A response has been received with a response code '500' 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 POST request made on the URL 'https://juice-shop-16-0-1-178712031365.us-
west1.run.app/api/content/'.
```

HTTP Info

REQUEST MADE

```
POST /api/content/ HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-16-0-1-178712031365.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
Content-Type: multipart/form-data; boundary=------------------------aadc326f7ae3eac3
Cookie: language=en; continueCode=z67RBJkpxgOw1qjLrbzDM95EnABVfXDUb9A3Y2aePl4VXZvQ8mW7yKo6NXeE;
cookieconsent_status=dismiss; welcomebanner_status=dismiss
Content-Length: 229
```

RESPONSE HEADERS

```
HTTP/2 500
access-control-allow-origin: *
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
feature-policy: payment 'self'
x-recruiting: /#/jobs
content-type: text/html; charset=utf-8
vary: Accept-Encoding
content-encoding: gzip
x-cloud-trace-context: 442638d240ba4ae7c1d84690c40eb44c
date: Fri, 25 Apr 2025 23:23:27 GMT
server: Google Frontend
content-length: 757
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/?wsdl

Identification

PROOF

```
HTTP/2 500
```

OUTPUT

```
A response has been received with a response code '500' 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-16-0-1-178712031365.us-west1.
run.app/api/?wsdl'.
```

HTTP Info

REQUEST MADE

```
GET /api/?wsdl HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-16-0-1-178712031365.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: language=en; continueCode=z67RBJkpxgOw1qjLrbzDM95EnABVfXDUb9A3Y2aePl4VXZvQ8mW7yKo6NXeE;
cookieconsent_status=dismiss; welcomebanner_status=dismiss
```

RESPONSE HEADERS

```
HTTP/2 500
access-control-allow-origin: *
x-content-type-options: nosniff
```

```
x-frame-options: SAMEORIGIN
feature-policy: payment 'self'
x-recruiting: /#/jobs
content-type: text/html; charset=utf-8
vary: Accept-Encoding
content-encoding: gzip
x-cloud-trace-context: 9b1da326330fe798bbc55044f1e30832
date: Fri, 25 Apr 2025 23:23:41 GMT
server: Google Frontend
content-length: 756
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/v1/swagger.yaml

Identification

PROOF

```
HTTP/2 500
```

OUTPUT

```
A response has been received with a response code '500' 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-16-0-1-178712031365.us-west1.
run.app/api/v1/swagger.yaml'.
```

HTTP Info

REQUEST MADE

```
GET /api/v1/swagger.yaml HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-16-0-1-178712031365.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: language=en; continueCode=z67RBJkpxgOw1qjLrbzDM95EnABVfXDUb9A3Y2aePl4VXZvQ8mW7yKo6NXeE;
cookieconsent_status=dismiss; welcomebanner_status=dismiss
```

RESPONSE HEADERS

```
HTTP/2 500
access-control-allow-origin: *
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
feature-policy: payment 'self'
x-recruiting: /#/jobs
content-type: text/html; charset=utf-8
vary: Accept-Encoding
content-encoding: gzip
x-cloud-trace-context: a7fafe945964854a7329af46f64ec829
date: Fri, 25 Apr 2025 23:24:14 GMT
server: Google Frontend
content-length: 763
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/docs/v2/swagger.yaml

Identification

PROOF

```
HTTP/2 500
```

OUTPUT

```
A response has been received with a response code '500' 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-16-0-1-178712031365.us-west1.
run.app/api/docs/v2/swagger.yaml'.
```

HTTP Info

REQUEST MADE

```
GET /api/docs/v2/swagger.yaml HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-16-0-1-178712031365.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: language=en; continueCode=z67RBJkpxgOw1qjLrbzDM95EnABVfXDUb9A3Y2aePl4VXZvQ8mW7yKo6NXeE;
cookieconsent_status=dismiss; welcomebanner_status=dismiss
```

RESPONSE HEADERS

```
HTTP/2 500
access-control-allow-origin: *
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
feature-policy: payment 'self'
x-recruiting: /#/jobs
content-type: text/html; charset=utf-8
vary: Accept-Encoding
content-encoding: gzip
x-cloud-trace-context: 1adc14169436b2b47329af46f64ecd39
date: Fri, 25 Apr 2025 23:24:14 GMT
server: Google Frontend
content-length: 767
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/swagger.json

---

Identification

PROOF

```
HTTP/2 500
```

OUTPUT

```
A response has been received with a response code '500' 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-16-0-1-178712031365.us-west1.
run.app/api/swagger.json'.
```

HTTP Info

REQUEST MADE

```
GET /api/swagger.json HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-16-0-1-178712031365.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: language=en; continueCode=z67RBJkpxgOw1qjLrbzDM95EnABVfXDUb9A3Y2aePl4VXZvQ8mW7yKo6NXeE;
cookieconsent_status=dismiss; welcomebanner_status=dismiss
```

RESPONSE HEADERS

```
HTTP/2 500
access-control-allow-origin: *
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
feature-policy: payment 'self'
x-recruiting: /#/jobs
content-type: text/html; charset=utf-8
vary: Accept-Encoding
content-encoding: gzip
x-cloud-trace-context: de7ab7769517366d7329af46f64ec9cb
date: Fri, 25 Apr 2025 23:24:13 GMT
server: Google Frontend
content-length: 759
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/swagger.yaml

Identification

PROOF

```
HTTP/2 500
```

OUTPUT

```
A response has been received with a response code '500' 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-16-0-1-178712031365.us-west1.
run.app/api/swagger.yaml'.
```

HTTP Info

REQUEST MADE

```
GET /api/swagger.yaml HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-16-0-1-178712031365.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: language=en; continueCode=z67RBJkpxgOw1qjLrbzDM95EnABVfXDUb9A3Y2aePl4VXZvQ8mW7yKo6NXeE;
cookieconsent_status=dismiss; welcomebanner_status=dismiss
```

RESPONSE HEADERS

```
HTTP/2 500
access-control-allow-origin: *
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
feature-policy: payment 'self'
x-recruiting: /#/jobs
content-type: text/html; charset=utf-8
vary: Accept-Encoding
content-encoding: gzip
```

```
x-cloud-trace-context: 7599e169dd1593c47329af46f64ece3e
date: Fri, 25 Apr 2025 23:24:14 GMT
server: Google Frontend
content-length: 760
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/login

Identification

PROOF

```
HTTP/2 500
```

OUTPUT

```
A response has been received with a response code '500' 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 POST request made on the URL 'https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/login'.
```

HTTP Info

REQUEST MADE

```
POST /api/login HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-16-0-1-178712031365.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
Content-Type: application/json
Cookie: language=en; continueCode=z67RBJkpxgOw1qjLrbzDM95EnABVfXDUb9A3Y2aePl4VXZvQ8mW7yKo6NXeE;
cookieconsent_status=dismiss; welcomebanner_status=dismiss
Content-Length: 337
```

RESPONSE HEADERS

```
HTTP/2 500
access-control-allow-origin: *
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
feature-policy: payment 'self'
x-recruiting: /#/jobs
content-type: text/html; charset=utf-8
vary: Accept-Encoding
content-encoding: gzip
x-cloud-trace-context: 2ab257d47ca412062c28f532bb1e7e5b
date: Fri, 25 Apr 2025 23:22:20 GMT
server: Google Frontend
content-length: 754
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/v2/swagger.json

Identification

PROOF

```
HTTP/2 500
```

OUTPUT

A response has been received with a response code '500' 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-16-0-1-178712031365.us-west1.run.app/api/v2/swagger.json'.

HTTP Info

REQUEST MADE

```
GET /api/v2/swagger.json HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-16-0-1-178712031365.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: language=en; continueCode=z67RBJkpxgOw1qjLrbzDM95EnABVfXDUb9A3Y2aePl4VXZvQ8mW7yKo6NXeE;
cookieconsent_status=dismiss; welcomebanner_status=dismiss
```

RESPONSE HEADERS

```
HTTP/2 500
access-control-allow-origin: *
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
feature-policy: payment 'self'
x-recruiting: /#/jobs
content-type: text/html; charset=utf-8
vary: Accept-Encoding
content-encoding: gzip
x-cloud-trace-context: 4aee3cb67c4510b87329af46f64ecc96
date: Fri, 25 Apr 2025 23:24:14 GMT
server: Google Frontend
content-length: 762
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https%3A%2F%2Fjuice-shop-16-0-1-178712031365.us-west1.run.app%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-16-0-1-178712031365.us-west1.run.app/setup/setup-s/%u002e%u002e/%u002e%u002e/log.jsp'.

HTTP Info

REQUEST MADE

```
GET /setup/setup-s/%u002e%u002e/%u002e%u002e/log.jsp HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-16-0-1-178712031365.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: language=en; continueCode=z67RBJkpxgOw1qjLrbzDM95EnABVfXDUb9A3Y2aePl4VXZvQ8mW7yKo6NXeE;
cookieconsent_status=dismiss; welcomebanner_status=dismiss
```

RESPONSE HEADERS

```
HTTP/2 400
x-content-type-options: nosniff
content-type: text/html; charset=utf-8
vary: Accept-Encoding
content-encoding: gzip
x-cloud-trace-context: 9b45b4648424cfb14556546f3e9a02d9
date: Fri, 25 Apr 2025 23:22:28 GMT
server: Google Frontend
content-length: 842
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/v1/swagger.json

Identification

PROOF

```
HTTP/2 500
```

OUTPUT

```
A response has been received with a response code '500' 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-16-0-1-178712031365.us-west1.
run.app/api/v1/swagger.json'.
```

HTTP Info

REQUEST MADE

```
GET /api/v1/swagger.json HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-16-0-1-178712031365.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: language=en; continueCode=z67RBJkpxgOw1qjLrbzDM95EnABVfXDUb9A3Y2aePl4VXZvQ8mW7yKo6NXeE;
cookieconsent_status=dismiss; welcomebanner_status=dismiss
```

RESPONSE HEADERS

```
HTTP/2 500
access-control-allow-origin: *
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
feature-policy: payment 'self'
x-recruiting: /#/jobs
content-type: text/html; charset=utf-8
vary: Accept-Encoding
content-encoding: gzip
x-cloud-trace-context: 446152e32de0c31b7329af46f64ecf4f
date: Fri, 25 Apr 2025 23:24:14 GMT
server: Google Frontend
content-length: 762
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/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-16-0-1-178712031365.us-
west1.run.app/was-tnb.aspx'.
```

HTTP Info

REQUEST MADE

```
DEBUG /was-tnb.aspx HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-16-0-1-178712031365.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: language=en; continueCode=z67RBJkpxgOw1qjLrbzDM95EnABVfXDUb9A3Y2aePl4VXZvQ8mW7yKo6NXeE;
cookieconsent_status=dismiss; welcomebanner_status=dismiss
```

RESPONSE HEADERS

```
HTTP/2 502
content-length: 87
content-type: text/plain
date: Fri, 25 Apr 2025 23:23:27 GMT
server: Google Frontend
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/docs/v2/swagger.json

Identification

PROOF

```
HTTP/2 500
```

OUTPUT

```
A response has been received with a response code '500' 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-16-0-1-178712031365.us-west1.
run.app/api/docs/v2/swagger.json'.
```

HTTP Info

REQUEST MADE

```
GET /api/docs/v2/swagger.json HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-16-0-1-178712031365.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: language=en; continueCode=z67RBJkpxgOw1qjLrbzDM95EnABVfXDUb9A3Y2aePl4VXZvQ8mW7yKo6NXeE;
cookieconsent_status=dismiss; welcomebanner_status=dismiss
```

RESPONSE HEADERS

```
HTTP/2 500
access-control-allow-origin: *
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
feature-policy: payment 'self'
x-recruiting: /#/jobs
content-type: text/html; charset=utf-8
vary: Accept-Encoding
content-encoding: gzip
x-cloud-trace-context: 35a3c414fcff6bb37329af46f64ec8cc
date: Fri, 25 Apr 2025 23:24:14 GMT
server: Google Frontend
content-length: 765
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/api-docs/

Identification

PROOF

```
HTTP/2 500
```

OUTPUT

```
A response has been received with a response code '500' 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-16-0-1-178712031365.us-west1.
run.app/api/api-docs/'.
```

HTTP Info

REQUEST MADE

```
GET /api/api-docs/ HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-16-0-1-178712031365.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: language=en; continueCode=z67RBJkpxgOw1qjLrbzDM95EnABVfXDUb9A3Y2aePl4VXZvQ8mW7yKo6NXeE;
cookieconsent_status=dismiss; welcomebanner_status=dismiss
```

RESPONSE HEADERS

```
HTTP/2 500
access-control-allow-origin: *
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
feature-policy: payment 'self'
x-recruiting: /#/jobs
content-type: text/html; charset=utf-8
vary: Accept-Encoding
content-encoding: gzip
x-cloud-trace-context: 1ff6b424738ebe8025d94f18362323b7
```

```
date: Fri, 25 Apr 2025 23:23:22 GMT
server: Google Frontend
content-length: 757
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/profile/

Identification

PROOF

```
HTTP/2 500
```

OUTPUT

```
A response has been received with a response code '500' 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-16-0-1-178712031365.us-west1.
run.app/profile/'.
```

HTTP Info

REQUEST MADE

```
GET /profile/ HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-16-0-1-178712031365.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: language=en; continueCode=z67RBJkpxgOw1qjLrbzDM95EnABVfXDUb9A3Y2aePl4VXZvQ8mW7yKo6NXeE;
cookieconsent_status=dismiss; welcomebanner_status=dismiss
```

RESPONSE HEADERS

```
HTTP/2 500
access-control-allow-origin: *
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
feature-policy: payment 'self'
x-recruiting: /#/jobs
content-type: text/html; charset=utf-8
vary: Accept-Encoding
content-encoding: gzip
x-cloud-trace-context: 0f88f2bceee4b4b07494a6c39609858c
date: Fri, 25 Apr 2025 23:19:20 GMT
server: Google Frontend
content-length: 654
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/cors/https/rfi.nessus.org/rfi.txt

Identification

PROOF

```
HTTP/2 500
```

OUTPUT

A response has been received with a response code '500' 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-16-0-1-178712031365.us-west1.run.app/api/cors/https/rfi.nessus.org/rfi.txt'.

HTTP Info

REQUEST MADE

```
GET /api/cors/https/rfi.nessus.org/rfi.txt HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-16-0-1-178712031365.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: language=en; continueCode=z67RBJkpxgOw1qjLrbzDM95EnABVfXDUb9A3Y2aePl4VXZvQ8mW7yKo6NXeE;
cookieconsent_status=dismiss; welcomebanner_status=dismiss
```

RESPONSE HEADERS

```
HTTP/2 500
access-control-allow-origin: *
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
feature-policy: payment 'self'
x-recruiting: /#/jobs
content-type: text/html; charset=utf-8
vary: Accept-Encoding
content-encoding: gzip
x-cloud-trace-context: 0e1323ced890ec3bc5bcc113ea527829
date: Fri, 25 Apr 2025 23:19:02 GMT
server: Google Frontend
content-length: 774
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/docs/

Identification

PROOF

```
HTTP/2 500
```

OUTPUT

A response has been received with a response code '500' 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-16-0-1-178712031365.us-west1.run.app/api/docs/'.

HTTP Info

REQUEST MADE

```
GET /api/docs/ HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-16-0-1-178712031365.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: language=en; continueCode=z67RBJkpxgOw1qjLrbzDM95EnABVfXDUb9A3Y2aePl4VXZvQ8mW7yKo6NXeE;
cookieconsent_status=dismiss; welcomebanner_status=dismiss
```

RESPONSE HEADERS

```
HTTP/2 500
access-control-allow-origin: *
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
feature-policy: payment 'self'
x-recruiting: /#/jobs
content-type: text/html; charset=utf-8
vary: Accept-Encoding
content-encoding: gzip
x-cloud-trace-context: e2c9e6bc4945078c25d94f1836232705
date: Fri, 25 Apr 2025 23:23:22 GMT
server: Google Frontend
content-length: 754
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/redirect?to=1%29%7Bwindow.top._tenable_wasscan_js_namespace_taint_tracer.log_execution_flow_sink%28%29%2F%2F

Identification

PROOF

```
HTTP/1.1 406 Not Acceptable
```

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-16-0-1-178712031365.us-west1.
run.app/redirect?to=1%29%7Bwindow.top._tenable_wasscan_js_namespace_taint_tracer.log_execution_flow_sink%28%29%2F%2F'.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/redirect?to=1%29%7Bwindow.top.
_tenable_wasscan_js_namespace_taint_tracer.log_execution_flow_sink%28%29%2F%2F
```

REQUEST HEADERS

```
Accept: */*
Accept-Language: en-US,en;q=0.5
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
Sec-Ch-Ua: "Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
```

RESPONSE HEADERS

```
HTTP/1.1 406 Not Acceptable
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding: gzip
Content-Length: 859
Content-Type: text/html; charset=utf-8
Date: Fri, 25 Apr 2025 23:17:25 GMT
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Cloud-Trace-Context: 26d72b7a6319eb9024aff2dea2bf999e
X-Content-Type-Options: nosniff
```

```
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/v1/status/config

Identification

PROOF

```
HTTP/2 500
```

OUTPUT

```
A response has been received with a response code '500' 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-16-0-1-178712031365.us-west1.
run.app/api/v1/status/config'.
```

HTTP Info

REQUEST MADE

```
GET /api/v1/status/config HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-16-0-1-178712031365.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: language=en; continueCode=z67RBJkpxgOw1qjLrbzDM95EnABVfXDUb9A3Y2aePl4VXZvQ8mW7yKo6NXeE;
cookieconsent_status=dismiss; welcomebanner_status=dismiss
```

RESPONSE HEADERS

```
HTTP/2 500
access-control-allow-origin: *
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
feature-policy: payment 'self'
x-recruiting: /#/jobs
content-type: text/html; charset=utf-8
vary: Accept-Encoding
content-encoding: gzip
x-cloud-trace-context: 192412a73c1117824556546f3e9a077b
date: Fri, 25 Apr 2025 23:22:29 GMT
server: Google Frontend
content-length: 763
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/restricted/

Identification

PROOF

```
HTTP/2 500
```

OUTPUT

```
A response has been received with a response code '500' 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-16-0-1-178712031365.us-west1.run.app/restricted/'.

HTTP Info

REQUEST MADE

```
GET /restricted/ HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-16-0-1-178712031365.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: language=en; continueCode=z67RBJkpxgOw1qjLrbzDM95EnABVfXDUb9A3Y2aePl4VXZvQ8mW7yKo6NXeE;
cookieconsent_status=dismiss; welcomebanner_status=dismiss
```

RESPONSE HEADERS

```
HTTP/2 500
access-control-allow-origin: *
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
feature-policy: payment 'self'
x-recruiting: /#/jobs
content-type: text/html; charset=utf-8
vary: Accept-Encoding
content-encoding: gzip
x-cloud-trace-context: 4cacbeb0f99fdbd9fb9f2c7b0d1d88ae
date: Fri, 25 Apr 2025 23:21:41 GMT
server: Google Frontend
content-length: 756
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/components/suggestions?recentlyBrowsed=

Identification

PROOF

```
HTTP/2 500
```

OUTPUT

A response has been received with a response code '500' 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-16-0-1-178712031365.us-west1.run.app/api/components/suggestions?recentlyBrowsed='.

HTTP Info

REQUEST MADE

```
GET /api/components/suggestions?recentlyBrowsed= HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-16-0-1-178712031365.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: language=en; continueCode=z67RBJkpxgOw1qjLrbzDM95EnABVfXDUb9A3Y2aePl4VXZvQ8mW7yKo6NXeE;
cookieconsent_status=dismiss; welcomebanner_status=dismiss
```

RESPONSE HEADERS

```
HTTP/2 500
access-control-allow-origin: *
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
feature-policy: payment 'self'
x-recruiting: /#/jobs
content-type: text/html; charset=utf-8
vary: Accept-Encoding
content-encoding: gzip
x-cloud-trace-context: 2f22528a23c418814556546f3e9a03db
date: Fri, 25 Apr 2025 23:22:24 GMT
server: Google Frontend
content-length: 781
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/wls-wsat/CoordinatorPortType

Identification

PROOF

```
HTTP/2 413
```

OUTPUT

```
A response has been received with a response code '413' 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 POST request made on the URL 'https://juice-shop-16-0-1-178712031365.us-
west1.run.app/wls-wsat/CoordinatorPortType'.
```

HTTP Info

REQUEST MADE

```
POST /wls-wsat/CoordinatorPortType HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-16-0-1-178712031365.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
Cmd: echo was_tnb_bsfXqizfMN
Content-Type: text/xml
Cookie: language=en; continueCode=z67RBJkpxgOw1qjLrbzDM95EnABVfXDUb9A3Y2aePl4VXZvQ8mW7yKo6NXeE;
cookieconsent_status=dismiss; welcomebanner_status=dismiss
Content-Length: 206137
```

RESPONSE HEADERS

```
HTTP/2 413
access-control-allow-origin: *
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
feature-policy: payment 'self'
x-recruiting: /#/jobs
content-type: text/html; charset=utf-8
vary: Accept-Encoding
content-encoding: gzip
x-cloud-trace-context: 39faa760efb63ab5c1d84690c40eb346
date: Fri, 25 Apr 2025 23:23:26 GMT
server: Google Frontend
content-length: 831
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/docs/v1/swagger.json

Identification

PROOF

```
HTTP/2 500
```

OUTPUT

```
A response has been received with a response code '500' 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-16-0-1-178712031365.us-west1.
run.app/api/docs/v1/swagger.json'.
```

HTTP Info

REQUEST MADE

```
GET /api/docs/v1/swagger.json HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-16-0-1-178712031365.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: language=en; continueCode=z67RBJkpxgOw1qjLrbzDM95EnABVfXDUb9A3Y2aePl4VXZvQ8mW7yKo6NXeE;
cookieconsent_status=dismiss; welcomebanner_status=dismiss
```

RESPONSE HEADERS

```
HTTP/2 500
access-control-allow-origin: *
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
feature-policy: payment 'self'
x-recruiting: /#/jobs
content-type: text/html; charset=utf-8
vary: Accept-Encoding
content-encoding: gzip
x-cloud-trace-context: a166ece2c5694e837329af46f64ec2ab
date: Fri, 25 Apr 2025 23:24:14 GMT
server: Google Frontend
content-length: 765
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/v1/targets

Identification

PROOF

```
HTTP/2 500
```

OUTPUT

```
A response has been received with a response code '500' 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-16-0-1-178712031365.us-west1.
run.app/api/v1/targets'.
```

HTTP Info

REQUEST MADE

```
GET /api/v1/targets HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-16-0-1-178712031365.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: language=en; continueCode=z67RBJkpxgOw1qjLrbzDM95EnABVfXDUb9A3Y2aePl4VXZvQ8mW7yKo6NXeE;
cookieconsent_status=dismiss; welcomebanner_status=dismiss
```

RESPONSE HEADERS

```
HTTP/2 500
access-control-allow-origin: *
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
feature-policy: payment 'self'
x-recruiting: /#/jobs
content-type: text/html; charset=utf-8
vary: Accept-Encoding
content-encoding: gzip
x-cloud-trace-context: b2362e7ae33639634556546f3e9a05c6
date: Fri, 25 Apr 2025 23:22:29 GMT
server: Google Frontend
content-length: 759
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/docs/v1/swagger.yaml

Identification

PROOF

```
HTTP/2 500
```

OUTPUT

```
A response has been received with a response code '500' 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-16-0-1-178712031365.us-west1.
run.app/api/docs/v1/swagger.yaml'.
```

HTTP Info

REQUEST MADE

```
GET /api/docs/v1/swagger.yaml HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-16-0-1-178712031365.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: language=en; continueCode=z67RBJkpxgOw1qjLrbzDM95EnABVfXDUb9A3Y2aePl4VXZvQ8mW7yKo6NXeE;
cookieconsent_status=dismiss; welcomebanner_status=dismiss
```

RESPONSE HEADERS

```
HTTP/2 500
access-control-allow-origin: *
x-content-type-options: nosniff
```

```
x-frame-options: SAMEORIGIN
feature-policy: payment 'self'
x-recruiting: /#/jobs
content-type: text/html; charset=utf-8
vary: Accept-Encoding
content-encoding: gzip
x-cloud-trace-context: 169c5b1ce525532f7329af46f64ec45f
date: Fri, 25 Apr 2025 23:24:14 GMT
server: Google Frontend
content-length: 767
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-16-0-1-178712031365.us-west1.run.app/#/

Identification

OUTPUT

```
The framework has detected the following technologies in the target application:

- jQuery (v2.2.4)
- Swagger UI (version unknown)
```

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-16-0-1-178712031365.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
- 10 cookie(s) set via JavaScript code
The complete list of the cookies is available in attachment.
```

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 (4)

VULNERABILITY INFO PLUGIN ID 98072

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/products/search/

Identification

OUTPUT

```
The common directory 'search' was identified by the scanner.
```

HTTP Info

REQUEST MADE

```
GET /rest/products/search/ HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-16-0-1-178712031365.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: language=en; continueCode=z67RBJkpxgOw1qjLrbzDM95EnABVfXDUb9A3Y2aePl4VXZvQ8mW7yKo6NXeE;
cookieconsent_status=dismiss; welcomebanner_status=dismiss
```

RESPONSE HEADERS

```
HTTP/2 200
access-control-allow-origin: *
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
feature-policy: payment 'self'
x-recruiting: /#/jobs
content-type: application/json; charset=utf-8
etag: W/"325f-Hp9QBHq/s6OgXcyAXGURrOpZ7T4"
vary: Accept-Encoding
content-encoding: gzip
date: Sat, 26 Apr 2025 00:54:18 GMT
server: Google Frontend
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/api-docs/

Identification

OUTPUT

```
The common directory 'api-docs' was identified by the scanner.
```

HTTP Info

REQUEST MADE

```
GET /api-docs/ HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-16-0-1-178712031365.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: language=en; continueCode=z67RBJkpxgOw1qjLrbzDM95EnABVfXDUb9A3Y2aePl4VXZvQ8mW7yKo6NXeE;
cookieconsent_status=dismiss; welcomebanner_status=dismiss
```

RESPONSE HEADERS

```
HTTP/2 200
access-control-allow-origin: *
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
feature-policy: payment 'self'
x-recruiting: /#/jobs
content-type: text/html; charset=utf-8
etag: W/"c22-H8FH9nKD8DeX/nvIRrte6ZjP2a4"
vary: Accept-Encoding
content-encoding: gzip
date: Fri, 25 Apr 2025 23:20:15 GMT
server: Google Frontend
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/ftp/

Identification

OUTPUT

```
The common directory 'ftp' was identified by the scanner.
```

HTTP Info

REQUEST MADE

```
GET /ftp/ HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-16-0-1-178712031365.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: language=en; continueCode=z67RBJkpxgOw1qjLrbzDM95EnABVfXDUb9A3Y2aePl4VXZvQ8mW7yKo6NXeE;
cookieconsent_status=dismiss; welcomebanner_status=dismiss
```

RESPONSE HEADERS

```
HTTP/2 200
access-control-allow-origin: *
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
feature-policy: payment 'self'
x-recruiting: /#/jobs
content-type: text/html; charset=utf-8
vary: Accept-Encoding
content-encoding: gzip
date: Fri, 25 Apr 2025 23:20:52 GMT
server: Google Frontend
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/products/1/reviews/

Identification

OUTPUT

```
The common directory 'reviews' was identified by the scanner.
```

HTTP Info

REQUEST MADE

```
GET /rest/products/1/reviews/ HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-16-0-1-178712031365.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: language=en; continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1;
cookieconsent_status=dismiss; welcomebanner_status=dismiss
```

RESPONSE HEADERS

```
HTTP/2 200
access-control-allow-origin: *
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
feature-policy: payment 'self'
x-recruiting: /#/jobs
content-type: application/json; charset=utf-8
etag: W/"ac-+6TYO+tKceLLbG2Ky9HQ7ZcLMWM"
vary: Accept-Encoding
x-cloud-trace-context: 12b987cc98b3dbf327a096f2bd7ca2ab
date: Sat, 26 Apr 2025 02:23:01 GMT
server: Google Frontend
content-length: 172
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	2024-12-03T00:00:00+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-16-0-1-178712031365.us-west1.run.app/#/

Identification

OUTPUT

```
Number of Private IP Addresses Collected: 4

Listed below are each private ip address:
127.0.0.1 found on 1 URL
192.168.99.100 found on 1 URL
169.254.169.254 found on 1 URL
169.254.169.126 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-16-0-1-178712031365.us-west1.run.app/#/

Identification

OUTPUT

```
Number of Email Addresses Collected: 10
Listed below are each email address and the number of URLs where the email address has been found:
donotreply@owasp-juice.shop found on 1 URL
admin@juice-sh.op found on 3 URLs
ethereum@juice-sh.op found on 1 URL
john@juice-sh.op found on 1 URL
emma@juice-sh.op found on 1 URL
in@juice-sh.op found on 2 URLs
der@juice-sh.op found on 2 URLs
ereum@juice-sh.op found on 2 URLs
bjoern@owasp.org found on 1 URL
bjoern.kimminich@gmail.com 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-16-0-1-178712031365.us-west1.run.app/#/

Identification

OUTPUT

```
Access to URL 'https://juice-shop-16-0-1-178712031365.us-west1.run.app/#/' has been confirmed.


Target Information
------------------------

Domain Name : juice-shop-16-0-1-178712031365.us-west1.run.app
IP Address : 216.239.32.53


Response Information
---------------------------

Status Code : 200
Return Code : ok
Return Message: No error
Response Time : 0.137635s
Response Size : 4247 bytes
Content-Type : text/html; charset=UTF-8


DEBUG INFORMATION
-----------------------

HTTP Network Timeout : 30s
```

HTTP Info

REQUEST MADE

```
GET / HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-16-0-1-178712031365.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
access-control-allow-origin: *
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
feature-policy: payment 'self'
x-recruiting: /#/jobs
accept-ranges: bytes
cache-control: public, max-age=0
last-modified: Fri, 25 Apr 2025 22:57:41 GMT
etag: W/"ea4-1966f2bc520"
content-type: text/html; charset=UTF-8
vary: Accept-Encoding
content-encoding: gzip
date: Fri, 25 Apr 2025 23:10:07 GMT
server: Google Frontend
```

```
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-16-0-1-178712031365.us-west1.run.app/#/

Identification

OUTPUT

```
WAS Scanner has taken a screenshot of the page at url 'https://juice-shop-16-0-1-178712031365.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 (4)

VULNERABILITY INFO PLUGIN ID 98148

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/b2b/v2/orders

INPUT TYPE	form
INPUT NAME	combined:post::https://juice-shop-16-0-1-178712031365.us-west1.run.app/b2b/v2/orders

Identification

OUTPUT

```
A form with no identifier has been detected on the following URL https://juice-shop-16-0-1-178712031365.us-west1.run.app
/b2b/v2/orders with no input fields

This form is submitted by using the following action : https://juice-shop-16-0-1-178712031365.us-west1.run.app/b2b/v2
/orders
```

HTTP Info

REQUEST MADE

```
POST https://juice-shop-16-0-1-178712031365.us-west1.run.app/b2b/v2/orders
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Content-Length: 23
Content-Type: application/json
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=az_AZ
Origin: https://juice-shop-16-0-1-178712031365.us-west1.run.app
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/api-docs/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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 500
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding: gzip
Content-Type: text/html; charset=utf-8
Date: Sat, 26 Apr 2025 05:53:59 GMT
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Cloud-Trace-Context: 5d8dbc8b0e4649841f389aba1b27aeb2
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Length: 958
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/api-docs/

INPUT TYPE	form
INPUT NAME	combined:get::https://juice-shop-16-0-1-178712031365.us-west1.run.app/api-docs/

Identification

OUTPUT

```
A form with no identifier has been detected on the following URL https://juice-shop-16-0-1-178712031365.us-west1.run.app
/api-docs/ with input fields :
- download-url-input (text)

This form is submitted by using the following action : https://juice-shop-16-0-1-178712031365.us-west1.run.app/api-docs/
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/api-docs/
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=az_AZ
If-None-Match: W/"c22-H8FH9nKD8DeX/nvIRrte6ZjP2a4"
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Date: Sat, 26 Apr 2025 05:33:11 GMT
Etag: W/"c22-H8FH9nKD8DeX/nvIRrte6ZjP2a4"
Feature-Policy: payment 'self'
Server: Google Frontend
X-Cloud-Trace-Context: b20775ae703a7d2cc1e2eac79d916b92
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Encoding: gzip
Content-Length: 3977
Content-Type: text/html; charset=utf-8
Vary: Accept-Encoding
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/socket.io/?EIO=4&transport=polling&t=PPlDpGv&sid=0N98D_jaorFN-7ioAAAK

INPUT TYPE	form
INPUT NAME	combined:post::https://juice-shop-16-0-1-178712031365.us-west1.run.app/socket.io/?EIO=4&transport=polling&t=PPlDpGv&sid=0N98D_jaorFN-7ioAAAK

Identification

OUTPUT

A form with no identifier has been detected on the following URL https://juice-shop-16-0-1-178712031365.us-west1.run.app/socket.io/?EIO=4&transport=polling&t=PPlDpGv&sid=0N98D_jaorFN-7ioAAAK with no input fields

This form is submitted by using the following action : https://juice-shop-16-0-1-178712031365.us-west1.run.app/socket.io/?EIO=4&transport=polling&t=PPlDpGv&sid=0N98D_jaorFN-7ioAAAK

HTTP Info

REQUEST MADE

POST https://juice-shop-16-0-1-178712031365.us-west1.run.app/socket.io/?EIO=4&transport=polling&t=PPlDpGv&sid=0N98D_jaorFN-7ioAAAK

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Content-Length: 2
Content-Type: text/plain;charset=UTF-8
Origin: https://juice-shop-16-0-1-178712031365.us-west1.run.app
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: http://localhost:4200
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type: text/html
Date: Fri, 25 Apr 2025 23:10:11 GMT
Server: Google Frontend
Vary: Origin
X-Cloud-Trace-Context: ce9bf97f35b3827da714d4467a7abb01
Content-Length: 2
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/socket.io/?EIO=4&transport=polling&t=PPlDpGv&sid=0N98D_jaorFN-7ioAAAK

INPUT TYPE	form
INPUT NAME	combined:get::https://juice-shop-16-0-1-178712031365.us-west1.run.app/socket.io/

Identification

OUTPUT

A form with no identifier has been detected on the following URL https://juice-shop-16-0-1-178712031365.us-west1.run.app/socket.io/?EIO=4&transport=polling&t=PPlDpGv&sid=0N98D_jaorFN-7ioAAAK with no input fields

This form is submitted by using the following action : https://juice-shop-16-0-1-178712031365.us-west1.run.app/socket.io/

HTTP Info

REQUEST MADE

```
POST https://juice-shop-16-0-1-178712031365.us-west1.run.app/socket.io/?
EIO=4&transport=polling&t=PPlDpGv&sid=0N98D_jaorFN-7ioAAAK
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Content-Length: 2
Content-Type: text/plain;charset=UTF-8
Origin: https://juice-shop-16-0-1-178712031365.us-west1.run.app
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: http://localhost:4200
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type: text/html
Date: Fri, 25 Apr 2025 23:10:11 GMT
Server: Google Frontend
Vary: Origin
X-Cloud-Trace-Context: ce9bf97f35b3827da714d4467a7abb01
Content-Length: 2
```

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-16-0-1-178712031365.us-west1.run.app/#/

Identification

OUTPUT

```
The scanner detected the presence of 30 URLs on the target application:

- 0 URLs which use a hostname related to the target hostname
- 30 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-16-0-1-178712031365.us-west1.run.app/api/Feedbacks/

Identification

OUTPUT

```
A Feature-Policy header was found on https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/Feedbacks/ but this
header must be renamed to Permissions-Policy.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/Feedbacks/
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: language=en; cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1
If-None-Match: W/"6c6-1n6pt9X8GncrTGxXY8nLWSP9brU"
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding: gzip
Content-Type: application/json; charset=utf-8
Date: Sat, 26 Apr 2025 02:27:40 GMT
Etag: W/"6c6-SIwkJLL3y8euYH1CiBtnE7PUBNY"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/en.json

Identification

OUTPUT

```
A Feature-Policy header was found on https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/en.json but
this header must be renamed to Permissions-Policy.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/en.json
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: application/json; charset=UTF-8
Date: Fri, 25 Apr 2025 23:10:10 GMT
Etag: W/"8175-18f05ebb708"
Feature-Policy: payment 'self'
Last-Modified: Mon, 22 Apr 2024 13:08:05 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/products/1/reviews

Identification

OUTPUT

```
A Feature-Policy header was found on https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/products/1/reviews
but this header must be renamed to Permissions-Policy.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/products/1/reviews
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: language=en; cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=z67RBJkpxgOw1qjLrbzDM95EnABVfXDUb9A3Y2aePl4VXZvQ8mW7yKo6NXeE
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
```

```
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type: application/json; charset=utf-8
Date: Sat, 26 Apr 2025 01:24:03 GMT
Etag: W/"ac-+6TYO+tKceLLbG2Ky9HQ7ZcLMWM"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Cloud-Trace-Context: 7eb022bfa1d0336a575e77ebdd395585
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Length: 172
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/continue-code

Identification

OUTPUT

```
A Feature-Policy header was found on https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/continue-code but
this header must be renamed to Permissions-Policy.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/continue-code
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: language=en; continueCode=aj4QDO4KyOqPJ7j2novp9EQ38gYVAJlGM1wWxalND5reZRLzmXk6BbmzZRb3;
cookieconsent_status=dismiss
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type: application/json; charset=utf-8
Date: Fri, 25 Apr 2025 23:11:40 GMT
Etag: W/"4f-BtWsDO+6UbKwXn+zhLoc64lHywc"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Cloud-Trace-Context: d28bc164452bf02b9b983bf0f2052948
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

```
Content-Length: 79
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/ftp/legal.md

Identification

OUTPUT

```
A Feature-Policy header was found on https://juice-shop-16-0-1-178712031365.us-west1.run.app/ftp/legal.md but this
header must be renamed to Permissions-Policy.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/ftp/legal.md
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=da_DK
Priority: u=0, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: text/markdown; charset=UTF-8
Date: Sat, 26 Apr 2025 03:18:01 GMT
Etag: W/"be7-1966fb18775"
Feature-Policy: payment 'self'
Last-Modified: Sat, 26 Apr 2025 01:23:47 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/

Identification

OUTPUT

A Feature-Policy header was found on https://juice-shop-16-0-1-178712031365.us-west1.run.app/ but this header must be renamed to Permissions-Policy.

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8
Date: Fri, 25 Apr 2025 23:10:08 GMT
Etag: W/"ea4-1966f2bc520"
Feature-Policy: payment 'self'
Last-Modified: Fri, 25 Apr 2025 22:57:41 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Length: 4619
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/Challenges/?name=Score%20Board

Identification

OUTPUT

A Feature-Policy header was found on https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/Challenges/?name=Score%20Board but this header must be renamed to Permissions-Policy.

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/Challenges/?name=Score%20Board
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type: application/json; charset=utf-8
Date: Fri, 25 Apr 2025 23:10:12 GMT
Etag: W/"288-+JKo65JYfG3LT9Er5ELTcivVYcQ"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Cloud-Trace-Context: 955c7b2840303fd8a714d4467a7ab0e0
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Length: 648
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/et_EE.json

Identification

OUTPUT

```
A Feature-Policy header was found on https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/et_EE.json but
this header must be renamed to Permissions-Policy.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/et_EE.json
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=et_EE
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: application/json; charset=UTF-8
Date: Sat, 26 Apr 2025 02:29:56 GMT
Etag: W/"8319-18f05ebb708"
Feature-Policy: payment 'self'
Last-Modified: Mon, 22 Apr 2024 13:08:05 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/socket.io/?EIO=4&transport=polling&t=PPIDpDO

Identification

OUTPUT

```
No Permissions-Policy headers were found on https://juice-shop-16-0-1-178712031365.us-west1.run.app/socket.io/?EIO=4&transport=polling&t=PPlDpDO
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/socket.io/?EIO=4&transport=polling&t=PPlDpDO
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: http://localhost:4200
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type: text/plain; charset=UTF-8
Date: Fri, 25 Apr 2025 23:10:10 GMT
Server: Google Frontend
Vary: Origin
X-Cloud-Trace-Context: 3beb321db23497f8a714d4467a7ab714
Content-Length: 96
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/Quantitys/

Identification

OUTPUT

```
A Feature-Policy header was found on https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/Quantitys/ but this header must be renamed to Permissions-Policy.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/Quantitys/
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding: gzip
Content-Type: application/json; charset=utf-8
Date: Fri, 25 Apr 2025 23:10:12 GMT
Etag: W/"1767-etMBFb05GTNXcAa1INjMInHcId4"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/languages

Identification

OUTPUT

```
A Feature-Policy header was found on https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/languages but this header must be renamed to Permissions-Policy.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/languages
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
```

```
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding: gzip
Content-Type: application/json; charset=utf-8
Date: Fri, 25 Apr 2025 23:10:11 GMT
Etag: W/"1308-8EV95V7lUMShnloiieqORKNai/g"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/de_DE.json

Identification

OUTPUT

```
A Feature-Policy header was found on https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/de_DE.json but
this header must be renamed to Permissions-Policy.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/de_DE.json
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=de_DE
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: application/json; charset=UTF-8
Date: Sat, 26 Apr 2025 02:29:48 GMT
Etag: W/"904a-18f05ebb708"
Feature-Policy: payment 'self'
Last-Modified: Mon, 22 Apr 2024 13:08:05 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
```

```
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/es_ES.json

Identification

OUTPUT

```
A Feature-Policy header was found on https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/es_ES.json but this header must be renamed to Permissions-Policy.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/es_ES.json
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=es_ES
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: application/json; charset=UTF-8
Date: Sat, 26 Apr 2025 02:30:16 GMT
Etag: W/"8d7b-18f05ebb708"
Feature-Policy: payment 'self'
Last-Modified: Mon, 22 Apr 2024 13:08:05 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/cs_CZ.json

Identification

OUTPUT

```
A Feature-Policy header was found on https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/cs_CZ.json but this header must be renamed to Permissions-Policy.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/cs_CZ.json
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=cs_CZ
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: application/json; charset=UTF-8
Date: Sat, 26 Apr 2025 02:29:27 GMT
Etag: W/"8814-18f05ebb708"
Feature-Policy: payment 'self'
Last-Modified: Mon, 22 Apr 2024 13:08:05 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/az_AZ.json

Identification

OUTPUT

```
A Feature-Policy header was found on https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/az_AZ.json but
this header must be renamed to Permissions-Policy.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/az_AZ.json
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=az_AZ
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: application/json; charset=UTF-8
Date: Sat, 26 Apr 2025 02:28:35 GMT
Etag: W/"8cc1-18f05ebb708"
Feature-Policy: payment 'self'
Last-Modified: Mon, 22 Apr 2024 13:08:05 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/fr_FR.json

Identification

OUTPUT

```
A Feature-Policy header was found on https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/fr_FR.json but this header must be renamed to Permissions-Policy.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/fr_FR.json
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=fr_FR
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: application/json; charset=UTF-8
Date: Sat, 26 Apr 2025 02:30:23 GMT
Etag: W/"9137-18f05ebb708"
Feature-Policy: payment 'self'
```

```
Last-Modified: Mon, 22 Apr 2024 13:08:05 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/admin/application-configuration

Identification

OUTPUT

```
A Feature-Policy header was found on https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/admin/application-configuration but this header must be renamed to Permissions-Policy.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/admin/application-configuration
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding: gzip
Content-Type: application/json; charset=utf-8
Date: Fri, 25 Apr 2025 23:10:10 GMT
Etag: W/"4993-Oz9kS67Z/2Q7h9VfrxO8V9OVt0M"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/admin/application-version

Identification

OUTPUT

```
A Feature-Policy header was found on https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/admin/application-version but this header must be renamed to Permissions-Policy.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/admin/application-version
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type: application/json; charset=utf-8
Date: Fri, 25 Apr 2025 23:10:10 GMT
Etag: W/"14-mWpI2PhnItYY44Y5gln+68A5CNc"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Cloud-Trace-Context: bb00cff05c5f3c45a714d4467a7abcb2
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Length: 20
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/captcha/

Identification

OUTPUT

```
A Feature-Policy header was found on https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/captcha/ but this
header must be renamed to Permissions-Policy.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/captcha/
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: language=en; cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1
If-None-Match: W/"31-6VzwP+6Js6+f/7oOKHud+d4LoO4"
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
```

```
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type: application/json; charset=utf-8
Date: Sat, 26 Apr 2025 02:27:39 GMT
Etag: W/"2f-MIu6CT8WR4M+Wp7TeexBr5Mm7M4"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Cloud-Trace-Context: cd7928d46a143d9e492e25266f1940ed
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Length: 47
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/ca_ES.json

Identification

OUTPUT

```
A Feature-Policy header was found on https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/ca_ES.json but
this header must be renamed to Permissions-Policy.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/ca_ES.json
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=ca_ES
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: application/json; charset=UTF-8
Date: Sat, 26 Apr 2025 02:29:02 GMT
Etag: W/"826e-18f05ebb708"
Feature-Policy: payment 'self'
Last-Modified: Mon, 22 Apr 2024 13:08:05 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
```

```
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/id_ID.json

Identification

OUTPUT

```
A Feature-Policy header was found on https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/id_ID.json but this header must be renamed to Permissions-Policy.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/id_ID.json
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=id_ID
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: application/json; charset=UTF-8
Date: Sat, 26 Apr 2025 02:28:52 GMT
Etag: W/"8269-18f05ebb708"
Feature-Policy: payment 'self'
Last-Modified: Mon, 22 Apr 2024 13:08:05 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/da_DK.json

Identification

OUTPUT

```
A Feature-Policy header was found on https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/da_DK.json but this header must be renamed to Permissions-Policy.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/da_DK.json
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=da_DK
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: application/json; charset=UTF-8
Date: Sat, 26 Apr 2025 02:29:39 GMT
Etag: W/"85dd-18f05ebb708"
Feature-Policy: payment 'self'
Last-Modified: Mon, 22 Apr 2024 13:08:05 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/products/search?q=

Identification

OUTPUT

```
A Feature-Policy header was found on https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/products/search?q=
but this header must be renamed to Permissions-Policy.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/products/search?q=
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
```

```
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding: gzip
Content-Type: application/json; charset=utf-8
Date: Fri, 25 Apr 2025 23:10:11 GMT
Etag: W/"325f-8he+HyT41TF0TRRd87FqKb7A8Mg"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/user/whoami

Identification

OUTPUT

```
A Feature-Policy header was found on https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/user/whoami but this header must be renamed to Permissions-Policy.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/user/whoami
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: language=en; cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=z67RBJkpxgOw1qjLrbzDM95EnABVfXDUb9A3Y2aePl4VXZvQ8mW7yKo6NXeE
If-None-Match: W/"b-/5bSboVjVhGw3qRgvUfZjE1r1Ns"
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Date: Sat, 26 Apr 2025 01:24:03 GMT
Etag: W/"b-/5bSboVjVhGw3qRgvUfZjE1r1Ns"
Feature-Policy: payment 'self'
Server: Google Frontend
X-Cloud-Trace-Context: 6d1efb72a363df96575e77ebdd395b80
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Vary: Accept-Encoding
```

```
Content-Length: 11
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/memories/

Identification

OUTPUT

```
A Feature-Policy header was found on https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/memories/ but this header must be renamed to Permissions-Policy.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/memories/
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: language=en; continueCode=z67RBJkpxgOw1qjLrbzDM95EnABVfXDUb9A3Y2aePl4VXZvQ8mW7yKo6NXeE;
cookieconsent_status=dismiss; welcomebanner_status=dismiss
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding: gzip
Content-Type: application/json; charset=utf-8
Date: Sat, 26 Apr 2025 02:27:38 GMT
Etag: W/"e22-k4t/skONyGpeL9C7mhMGOYDLOnc"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

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-16-0-1-178712031365.us-west1.run.app/

Identification

OUTPUT

```
No Referrer-Policy headers or body meta tags were found on https://juice-shop-16-0-1-178712031365.us-west1.run.app/
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8
Date: Fri, 25 Apr 2025 23:10:08 GMT
Etag: W/"ea4-1966f2bc520"
Feature-Policy: payment 'self'
Last-Modified: Fri, 25 Apr 2025 22:57:41 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Length: 4619
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/admin/application-configuration

Identification

OUTPUT

```
No Referrer-Policy headers or body meta tags were found on https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest
/admin/application-configuration
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/admin/application-configuration
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding: gzip
Content-Type: application/json; charset=utf-8
Date: Fri, 25 Apr 2025 23:10:10 GMT
Etag: W/"4993-Oz9kS67Z/2Q7h9VfrxO8V9OVt0M"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/de_DE.json

Identification

OUTPUT

```
No Referrer-Policy headers or body meta tags were found on https://juice-shop-16-0-1-178712031365.us-west1.run.app
/assets/i18n/de_DE.json
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/de_DE.json
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=de_DE
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
```

```
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: application/json; charset=UTF-8
Date: Sat, 26 Apr 2025 02:29:48 GMT
Etag: W/"904a-18f05ebb708"
Feature-Policy: payment 'self'
Last-Modified: Mon, 22 Apr 2024 13:08:05 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/ftp/legal.md

Identification

OUTPUT

```
No Referrer-Policy headers or body meta tags were found on https://juice-shop-16-0-1-178712031365.us-west1.run.app/ftp
/legal.md
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/ftp/legal.md
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=da_DK
Priority: u=0, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: text/markdown; charset=UTF-8
Date: Sat, 26 Apr 2025 03:18:01 GMT
Etag: W/"be7-1966fb18775"
Feature-Policy: payment 'self'
Last-Modified: Sat, 26 Apr 2025 01:23:47 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/products/1/reviews

Identification

OUTPUT

```
No Referrer-Policy headers or body meta tags were found on https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest
/products/1/reviews
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/products/1/reviews
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: language=en; cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=z67RBJkpxgOw1qjLrbzDM95EnABVfXDUb9A3Y2aePl4VXZvQ8mW7yKo6NXeE
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type: application/json; charset=utf-8
Date: Sat, 26 Apr 2025 01:24:03 GMT
Etag: W/"ac-+6TYO+tKceLLbG2Ky9HQ7ZcLMWM"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Cloud-Trace-Context: 7eb022bfa1d0336a575e77ebdd395585
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Length: 172
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/continue-code

Identification

OUTPUT

```
No Referrer-Policy headers or body meta tags were found on https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest
/continue-code
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/continue-code
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: language=en; continueCode=aj4QDO4KyOqPJ7j2novp9EQ38gYVAJlGM1wWxalND5reZRLzmXk6BbmzZRb3;
cookieconsent_status=dismiss
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type: application/json; charset=utf-8
Date: Fri, 25 Apr 2025 23:11:40 GMT
Etag: W/"4f-BtWsDO+6UbKwXn+zhLoc64lHywc"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Cloud-Trace-Context: d28bc164452bf02b9b983bf0f2052948
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Length: 79
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/user/whoami

Identification

OUTPUT

```
No Referrer-Policy headers or body meta tags were found on https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest
/user/whoami
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/user/whoami
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: language=en; cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=z67RBJkpxgOw1qjLrbzDM95EnABVfXDUb9A3Y2aePl4VXZvQ8mW7yKo6NXeE
If-None-Match: W/"b-/5bSboVjVhGw3qRgvUfZjE1r1Ns"
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Date: Sat, 26 Apr 2025 01:24:03 GMT
Etag: W/"b-/5bSboVjVhGw3qRgvUfZjE1r1Ns"
Feature-Policy: payment 'self'
Server: Google Frontend
X-Cloud-Trace-Context: 6d1efb72a363df96575e77ebdd395b80
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Vary: Accept-Encoding
Content-Length: 11
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/products/search?q=

Identification

OUTPUT

```
No Referrer-Policy headers or body meta tags were found on https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest
/products/search?q=
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/products/search?q=
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

```
Content-Encoding: gzip
Content-Type: application/json; charset=utf-8
Date: Fri, 25 Apr 2025 23:10:11 GMT
Etag: W/"325f-8he+HyT41TF0TRRd87FqKb7A8Mg"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/ca_ES.json

Identification

OUTPUT

```
No Referrer-Policy headers or body meta tags were found on https://juice-shop-16-0-1-178712031365.us-west1.run.app
/assets/i18n/ca_ES.json
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/ca_ES.json
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=ca_ES
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: application/json; charset=UTF-8
Date: Sat, 26 Apr 2025 02:29:02 GMT
Etag: W/"826e-18f05ebb708"
Feature-Policy: payment 'self'
Last-Modified: Mon, 22 Apr 2024 13:08:05 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/es_ES.json

Identification

OUTPUT

```
No Referrer-Policy headers or body meta tags were found on https://juice-shop-16-0-1-178712031365.us-west1.run.app
/assets/i18n/es_ES.json
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/es_ES.json
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=es_ES
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: application/json; charset=UTF-8
Date: Sat, 26 Apr 2025 02:30:16 GMT
Etag: W/"8d7b-18f05ebb708"
Feature-Policy: payment 'self'
Last-Modified: Mon, 22 Apr 2024 13:08:05 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/captcha/

Identification

OUTPUT

```
No Referrer-Policy headers or body meta tags were found on https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest
/captcha/
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/captcha/
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
```

```
Accept-Language: en-US,en;q=0.5
Cookie: language=en; cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1
If-None-Match: W/"31-6VzwP+6Js6+f/7oOKHud+d4LoO4"
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type: application/json; charset=utf-8
Date: Sat, 26 Apr 2025 02:27:39 GMT
Etag: W/"2f-MIu6CT8WR4M+Wp7TeexBr5Mm7M4"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Cloud-Trace-Context: cd7928d46a143d9e492e25266f1940ed
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Length: 47
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/cs_CZ.json

Identification

OUTPUT

```
No Referrer-Policy headers or body meta tags were found on https://juice-shop-16-0-1-178712031365.us-west1.run.app
/assets/i18n/cs_CZ.json
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/cs_CZ.json
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=cs_CZ
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
```

```
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: application/json; charset=UTF-8
Date: Sat, 26 Apr 2025 02:29:27 GMT
Etag: W/"8814-18f05ebb708"
Feature-Policy: payment 'self'
Last-Modified: Mon, 22 Apr 2024 13:08:05 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/Feedbacks/

Identification

OUTPUT

```
No Referrer-Policy headers or body meta tags were found on https://juice-shop-16-0-1-178712031365.us-west1.run.app/api
/Feedbacks/
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/Feedbacks/
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: language=en; cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1
If-None-Match: W/"6c6-1n6pt9X8GncrTGxXY8nLWSP9brU"
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding: gzip
Content-Type: application/json; charset=utf-8
Date: Sat, 26 Apr 2025 02:27:40 GMT
Etag: W/"6c6-SIwkJLL3y8euYH1CiBtnE7PUBNY"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/en.json

Identification

OUTPUT

```
No Referrer-Policy headers or body meta tags were found on https://juice-shop-16-0-1-178712031365.us-west1.run.app
/assets/i18n/en.json
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/en.json
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: application/json; charset=UTF-8
Date: Fri, 25 Apr 2025 23:10:10 GMT
Etag: W/"8175-18f05ebb708"
Feature-Policy: payment 'self'
Last-Modified: Mon, 22 Apr 2024 13:08:05 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/da_DK.json

Identification

OUTPUT

```
No Referrer-Policy headers or body meta tags were found on https://juice-shop-16-0-1-178712031365.us-west1.run.app
/assets/i18n/da_DK.json
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/da_DK.json
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=da_DK
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: application/json; charset=UTF-8
Date: Sat, 26 Apr 2025 02:29:39 GMT
Etag: W/"85dd-18f05ebb708"
Feature-Policy: payment 'self'
Last-Modified: Mon, 22 Apr 2024 13:08:05 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/languages

Identification

OUTPUT

```
No Referrer-Policy headers or body meta tags were found on https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest
/languages
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/languages
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
```

```
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding: gzip
Content-Type: application/json; charset=utf-8
Date: Fri, 25 Apr 2025 23:10:11 GMT
Etag: W/"1308-8EV95V7lUMShnloiieqORKNai/g"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/socket.io/?EIO=4&transport=polling&t=PPlDpDO

Identification

OUTPUT

```
No Referrer-Policy headers or body meta tags were found on https://juice-shop-16-0-1-178712031365.us-west1.run.app
/socket.io/?EIO=4&transport=polling&t=PPlDpDO
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/socket.io/?EIO=4&transport=polling&t=PPlDpDO
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: http://localhost:4200
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type: text/plain; charset=UTF-8
Date: Fri, 25 Apr 2025 23:10:10 GMT
Server: Google Frontend
Vary: Origin
X-Cloud-Trace-Context: 3beb321db23497f8a714d4467a7ab714
Content-Length: 96
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/et_EE.json

Identification

OUTPUT

```
No Referrer-Policy headers or body meta tags were found on https://juice-shop-16-0-1-178712031365.us-west1.run.app
/assets/i18n/et_EE.json
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/et_EE.json
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=et_EE
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: application/json; charset=UTF-8
Date: Sat, 26 Apr 2025 02:29:56 GMT
Etag: W/"8319-18f05ebb708"
Feature-Policy: payment 'self'
Last-Modified: Mon, 22 Apr 2024 13:08:05 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/az_AZ.json

Identification

OUTPUT

```
No Referrer-Policy headers or body meta tags were found on https://juice-shop-16-0-1-178712031365.us-west1.run.app
/assets/i18n/az_AZ.json
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/az_AZ.json
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=az_AZ
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: application/json; charset=UTF-8
Date: Sat, 26 Apr 2025 02:28:35 GMT
Etag: W/"8cc1-18f05ebb708"
Feature-Policy: payment 'self'
Last-Modified: Mon, 22 Apr 2024 13:08:05 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/Quantitys/

Identification

OUTPUT

```
No Referrer-Policy headers or body meta tags were found on https://juice-shop-16-0-1-178712031365.us-west1.run.app/api
/Quantitys/
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/Quantitys/
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding: gzip
Content-Type: application/json; charset=utf-8
Date: Fri, 25 Apr 2025 23:10:12 GMT
Etag: W/"1767-etMBFb05GTNXcAa1INjMInHcId4"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
```

```
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/Challenges/?name=Score%20Board

Identification

OUTPUT

```
No Referrer-Policy headers or body meta tags were found on https://juice-shop-16-0-1-178712031365.us-west1.run.app/api
/Challenges/?name=Score%20Board
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/Challenges/?name=Score%20Board
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type: application/json; charset=utf-8
Date: Fri, 25 Apr 2025 23:10:12 GMT
Etag: W/"288-+JKo65JYfG3LT9Er5ELTcivVYcQ"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Cloud-Trace-Context: 955c7b2840303fd8a714d4467a7ab0e0
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Length: 648
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/memories/

Identification

OUTPUT

```
No Referrer-Policy headers or body meta tags were found on https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest
/memories/
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/memories/
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: language=en; continueCode=z67RBJkpxgOw1qjLrbzDM95EnABVfXDUb9A3Y2aePl4VXZvQ8mW7yKo6NXeE;
cookieconsent_status=dismiss; welcomebanner_status=dismiss
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Encoding: gzip
Content-Type: application/json; charset=utf-8
Date: Sat, 26 Apr 2025 02:27:38 GMT
Etag: W/"e22-k4t/skONyGpeL9C7mhMGOYDLOnc"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/id_ID.json

Identification

OUTPUT

```
No Referrer-Policy headers or body meta tags were found on https://juice-shop-16-0-1-178712031365.us-west1.run.app
/assets/i18n/id_ID.json
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/id_ID.json
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=id_ID
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
```

```
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: application/json; charset=UTF-8
Date: Sat, 26 Apr 2025 02:28:52 GMT
Etag: W/"8269-18f05ebb708"
Feature-Policy: payment 'self'
Last-Modified: Mon, 22 Apr 2024 13:08:05 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/fr_FR.json

Identification

OUTPUT

```
No Referrer-Policy headers or body meta tags were found on https://juice-shop-16-0-1-178712031365.us-west1.run.app
/assets/i18n/fr_FR.json
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/i18n/fr_FR.json
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=fr_FR
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: application/json; charset=UTF-8
Date: Sat, 26 Apr 2025 02:30:23 GMT
Etag: W/"9137-18f05ebb708"
Feature-Policy: payment 'self'
Last-Modified: Mon, 22 Apr 2024 13:08:05 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/admin/application-version

Identification

OUTPUT

```
No Referrer-Policy headers or body meta tags were found on https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest
/admin/application-version
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/rest/admin/application-version
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type: application/json; charset=utf-8
Date: Fri, 25 Apr 2025 23:10:10 GMT
Etag: W/"14-mWpI2PhnItYY44Y5gln+68A5CNc"
Feature-Policy: payment 'self'
Server: Google Frontend
Vary: Accept-Encoding
X-Cloud-Trace-Context: bb00cff05c5f3c45a714d4467a7abcb2
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Length: 20
```

Missing Subresource Integrity

VULNERABILITY INFO PLUGIN ID 98647

Description

Subresource Integrity (SRI) is a web security standard that enables browsers to verify that resources hosted by third parties (CDN for example) are delivered without unexpected manipulation.

SRI works by comparing a cryptographic hash declared in the integrity attribute of the resource tag (like script or link) used to fetch the resource and the calculated hash value of this resource.

No SRI have been detected for one or more resources.

Solution

Add a integrity attribute to the resource tag with prefixed and base64 encoded hash of the resource.

See Also

https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity
https://www.owasp.org/index.php/3rd_Party_Javascript_Management_Cheat_Sheet#Subresource_Integrity

Plugin Details

PUBLICATION DATE	2019-08-01T00:00:00+00:00
MODIFICATION DATE	2023-01-17T00:00:00+00:00
FAMILY	Web Applications
SEVERITY	Info
PLUGIN ID	98647

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 Subresource Integrity Instances (1)

VULNERABILITY INFO PLUGIN ID 98647

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/#/

Identification

OUTPUT

```
The scanner detected 4 resources without subresource integrity defined :
- 2 URLs related to 'script' resources
- 2 URLs related to 'link' resources

The list of all the detected resources is provided in attachment.
```

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-16-0-1-178712031365.us-west1.run.app/robots.txt

Identification

OUTPUT

```
A robots.txt file was detected at 'https://juice-shop-16-0-1-178712031365.us-west1.run.app/robots.txt'.
```

HTTP Info

REQUEST MADE

```
GET /robots.txt HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-16-0-1-178712031365.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: language=en; continueCode=z67RBJkpxgOw1qjLrbzDM95EnABVfXDUb9A3Y2aePl4VXZvQ8mW7yKo6NXeE;
cookieconsent_status=dismiss; welcomebanner_status=dismiss
```

RESPONSE HEADERS

```
HTTP/2 200
access-control-allow-origin: *
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
feature-policy: payment 'self'
x-recruiting: /#/jobs
content-type: text/plain; charset=utf-8
etag: W/"1c-8HgF6mNyhsSFK0pascC9uB0wjX0"
vary: Accept-Encoding
x-cloud-trace-context: f44a3e1bfdabb9ee4556546f3e9a0b91
date: Fri, 25 Apr 2025 23:22:23 GMT
server: Google Frontend
content-length: 28
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

Fetch/XHR Detected

VULNERABILITY INFO PLUGIN ID 98772

Description

The scan detected that the web application makes requests that appear to be using Fetch or XMLHTTPRequests (XHRs) to communicate with a backend API server. Fetchs/XHRs allow retrieval of data from an API without triggering a page reload, making them especially useful for Single Page Applications.

Solution

-

See Also

https://developer.mozilla.org/en-US/docs/Web/API/XMLHttpRequest

Plugin Details

PUBLICATION DATE	2019-11-14T00:00:00+00:00
MODIFICATION DATE	2023-11-17T00:00:00+00:00
FAMILY	General
SEVERITY	Info
PLUGIN ID	98772

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

Fetch/XHR Detected Instances (1)

VULNERABILITY INFO PLUGIN ID 98772

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/#/

Identification

OUTPUT

```
The scan detected 7631 unique XMLHttpRequests. Here is the distribution of MIME types used by the detected requests:

- 174 as "application/json"
- 5045 as "text/plain"
- 2284 as "text/html"
- 5 as "application/octet-stream"


- 123 with no specified or detected MIME type

The scan detected 15 unique Fetch Requests. Here is the distribution of MIME types used by the detected requests:

- 5 as "application/json"
- 7 as "text/html"
- 1 as "text/fragment+html"
- 1 as "text/plain"
- 1 with no specified or detected MIME type
```

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-16-0-1-178712031365.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 *.asia-southeast3.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-west15.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: 2025-03-31 08:54:20 UTC
Valid until: 2025-06-23 08:54:19 UTC (expires in 1 month, 3 weeks, 6 days)
Validity Period: 83 days
Key: 256-bit
Signature: ecdsa-with-SHA256

Certificate 2
--------------
Common Name: we2
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 3 years, 9 months, 3 weeks, 5 days)
Validity Period: 1896 days
Key: 256-bit
Signature: ecdsa-with-SHA384

Certificate 3
--------------
Common Name: gts root r4
Issuer: GlobalSign nv
Valid from: 2023-11-15 03:43:21 UTC
Valid until: 2028-01-28 00:00:42 UTC (expires in 2 years, 9 months, 2 days)
Validity Period: 1534 days
Key: RSA 384-bit
Signature: sha256WithRSAEncryption
```

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-16-0-1-178712031365.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
```

Full Path Disclosure

VULNERABILITY INFO PLUGIN ID 112550

Description

The remote web server contains an application which is affected by a path disclosure issue. It may be possible for an attacker to view full path names and conduct further attacks.

Solution

Disable all notice, warning and error displaying.

See Also

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

Plugin Details

PUBLICATION DATE	2018-12-13T00:00:00+00:00
MODIFICATION DATE	2024-10-03T00:00:00+00:00
FAMILY	Data Exposure
SEVERITY	Info
PLUGIN ID	112550

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

Full Path Disclosure Instances (1)

VULNERABILITY INFO PLUGIN ID 112550

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/Challenges/

Identification

PROOF

```
The following patterns were detected in the HTTP response body :
- C:\\Windows\\system
```

OUTPUT

```
The scanner detected the disclosure of full paths in the web application response.
```

HTTP Info

REQUEST MADE

```
GET /api/Challenges/?%22WAS%22%20%2B%20str%2898482%2A19693%29= HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-16-0-1-178712031365.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: gzip, deflate, br
Priority: u=1, i
Referer: https://juice-shop-16-0-1-178712031365.us-west1.run.app/
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: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Cookie: language=en; continueCode=z67RBJkpxgOw1qjLrbzDM95EnABVfXDUb9A3Y2aePl4VXZvQ8mW7yKo6NXeE;
cookieconsent_status=dismiss; welcomebanner_status=dismiss
```

RESPONSE HEADERS

```
HTTP/2 200
access-control-allow-origin: *
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
feature-policy: payment 'self'
x-recruiting: /#/jobs
content-type: application/json; charset=utf-8
etag: W/"134a8-vDiaaIyLCNx+PABW56r1kURLBBA"
vary: Accept-Encoding
content-encoding: gzip
date: Sat, 26 Apr 2025 00:58:25 GMT
server: Google Frontend
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

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-16-0-1-178712031365.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-16-0-1-178712031365.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.
```

OpenAPI File Detected

VULNERABILITY INFO PLUGIN ID 112615

Description

A OpenAPI configuration file has been detected and is available as an attachment below. OpenAPI is a specification that helps with documentation and consumption of REST APIs and may also be used to configure API scanning.

Solution

-

See Also

https://github.com/OAI/OpenAPI-Specification
https://oai.github.io/Documentation/
https://swagger.io/docs/specification/

Plugin Details

PUBLICATION DATE	2020-10-20T00:00:00+00:00
MODIFICATION DATE	2024-01-08T00:00:00+00:00
FAMILY	Web Applications
SEVERITY	Info
PLUGIN ID	112615

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

OpenAPI File Detected Instances (1)

VULNERABILITY INFO PLUGIN ID 112615

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/api-docs/

Identification

OUTPUT

```
The scanner was able to detect a Swagger or OpenAPI definition file on https://juice-shop-16-0-1-178712031365.us-west1.
run.app/api-docs/. The file is available in attachments.
```

API Detected

VULNERABILITY INFO PLUGIN ID 112616

Description

The scan detected that some XHR requests seem to call an API. The scanner generated an OpenAPI file based on the observed requests and attached it to the plugin output. This OpenAPI file can then be used to run a scan against the API with WAS API Scanning.

Solution

-

See Also

Plugin Details

PUBLICATION DATE	2020-10-21T00:00:00+00:00
MODIFICATION DATE	2020-10-21T00:00:00+00:00
FAMILY	General
SEVERITY	Info
PLUGIN ID	112616

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

API Detected Instances (1)

VULNERABILITY INFO PLUGIN ID 112616

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/#/

Identification

OUTPUT

```
API endpoints have been detected for the following host(s):
- https://juice-shop-16-0-1-178712031365.us-west1.run.app
- https://github.com
```

Security.txt File Detected

VULNERABILITY INFO PLUGIN ID 112722

Description

A Security.txt file has 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.

As a result, security issues may be disclosed by 3rd party researchers securely in a manner defined by the organization.

Solution

-

See Also

https://datatracker.ietf.org/doc/html/rfc9116
https://securitytxt.org/

Plugin Details

PUBLICATION DATE	2021-03-17T00:00:00+00:00
MODIFICATION DATE	2022-04-29T00:00:00+00:00
FAMILY	Web Servers
SEVERITY	Info
PLUGIN ID	112722

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 Detected Instances (1)

VULNERABILITY INFO PLUGIN ID 112722

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/.well-known/security.txt

Identification

OUTPUT

```
A security.txt file was detected at 'https://juice-shop-16-0-1-178712031365.us-west1.run.app/.well-known/security.txt'.
```

HTTP Info

REQUEST MADE

```
GET /.well-known/security.txt HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-16-0-1-178712031365.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: language=en; continueCode=z67RBJkpxgOw1qjLrbzDM95EnABVfXDUb9A3Y2aePl4VXZvQ8mW7yKo6NXeE;
cookieconsent_status=dismiss; welcomebanner_status=dismiss
```

RESPONSE HEADERS

```
HTTP/2 200
access-control-allow-origin: *
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
feature-policy: payment 'self'
x-recruiting: /#/jobs
content-type: text/plain; charset=utf-8
etag: W/"197-LVX38tvYUCLARlo2BeGpGE4zLfk"
vary: Accept-Encoding
x-cloud-trace-context: 6128667f553b39844556546f3e9a09dc
date: Fri, 25 Apr 2025 23:22:23 GMT
server: Google Frontend
content-length: 407
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

Out-of-Date JQuery Detected

VULNERABILITY INFO PLUGIN ID 113027

Description

An out-of-date version of JQuery has been detected. An outdated version could have vulnerabilities or missing security features.

Solution

Upgrade to the latest version of JQuery.

See Also
https://blog.jquery.com/
https://github.com/jquery/jquery/tags
https://jquery.com/

Plugin Details

PUBLICATION DATE	2021-10-25T00:00:00+00:00
MODIFICATION DATE	2024-01-11T00:00:00+00:00
FAMILY	Component Vulnerability
SEVERITY	Info
PLUGIN ID	113027

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

Out-of-Date JQuery Detected Instances (1)

VULNERABILITY INFO PLUGIN ID 113027

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/

Identification

OUTPUT

```
Technology jQuery has been detected with version 2.2.4. Latest version available is : 3.7.1
```

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-16-0-1-178712031365.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
- *.asia-southeast3.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-west15.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-16-0-1-178712031365.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
```

PostMessage Wildcard Event Listener Detected

VULNERABILITY INFO PLUGIN ID 113851

Description

Web applications relying on JavaScript often need to perform cross-origin communication between `Window` objects such as a page and an embedded iframe or a popup window. The postMessage API allows developers to circumvent the same-origin policy restrictions in order to exchange data between scripts located on different origins.
Depending on the application needs, messages event listeners could be added to use received messages in part of its logic. However, if the data received in these messages are used, for example, to build the page DOM, an attacker could leverage this issue to inject malicious data and conduct client-side attacks like Cross-Site Scripting (XSS) or Prototype Pollution.

Solution

Remove the message event listener if this is not needed in the application logic or verify that the message sender origin is matching with a trusted allowlist.

See Also
https://blog.yeswehack.com/yeswerhackers/introduction-postmessage-vulnerabilities/
https://developer.mozilla.org/en-US/docs/Web/API/Window/postMessage

Plugin Details

PUBLICATION DATE	2023-05-05T00:00:00+00:00
MODIFICATION DATE	2023-05-05T00:00:00+00:00
FAMILY	Web Applications
SEVERITY	Info
PLUGIN ID	113851

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

PostMessage Wildcard Event Listener Detected Instances (1)

VULNERABILITY INFO PLUGIN ID 113851

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/

Identification

OUTPUT

The scanner detected the presence of listeners which does not check for the message origin. The code of the JavaScript function used by the listener is available in attachment.

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8
Date: Fri, 25 Apr 2025 23:10:08 GMT
Etag: W/"ea4-1966f2bc520"
Feature-Policy: payment 'self'
Last-Modified: Fri, 25 Apr 2025 22:57:41 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Length: 4619
```

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 (2)

VULNERABILITY INFO PLUGIN ID 113897

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/

Identification

OUTPUT

```
3 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-16-0-1-178712031365.us-west1.run.app/
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8
Date: Fri, 25 Apr 2025 23:10:08 GMT
Etag: W/"ea4-1966f2bc520"
Feature-Policy: payment 'self'
Last-Modified: Fri, 25 Apr 2025 22:57:41 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Length: 4619
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/public/images/uploads/%F0%9F%98%BC-

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-16-0-1-178712031365.us-west1.run.app/assets/public/images/uploads/%F0%9F%98%BC-

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=az_AZ
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8
Date: Sat, 26 Apr 2025 06:45:12 GMT
Etag: W/"ea4-19670be8e8c"
Feature-Policy: payment 'self'
Last-Modified: Sat, 26 Apr 2025 06:17:38 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Length: 4619
```

JavaScript Source Map Detected

VULNERABILITY INFO PLUGIN ID 114132

Description

Developers often combine and minify their application JavaScript sources to help the server delivering it more efficiently to the client browsers. Sometimes, web applications JavaScript code may also be transpiled from another language like CoffeeScript of TypeScript.

A source map is a file that maps from the transformed source code to the original source, allowing the browser to reconstruct the original source code and present it to the debugger.

Solution

-

See Also

Plugin Details

PUBLICATION DATE	2023-12-18T00:00:00+00:00
MODIFICATION DATE	2023-12-18T00:00:00+00:00
FAMILY	Web Applications
SEVERITY	Info
PLUGIN ID	114132

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

JavaScript Source Map Detected Instances (1)

VULNERABILITY INFO PLUGIN ID 114132

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/api-docs/swagger-ui-bundle.js

Identification

OUTPUT

```
The scanner was able to detect the presence of JavaScript source maps in the response body.The following source map
files were detected :
- https://juice-shop-16-0-1-178712031365.us-west1.run.app/api-docs/swagger-ui-bundle.js.map
```

HTTP Info

REQUEST MADE

```
GET /api-docs/swagger-ui-bundle.js.map HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-16-0-1-178712031365.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: language=en; continueCode=q6BKoaN93W5z7k6Z4rn1JVQOAo8f2xF5yIoLdgewPDmvxMyLpqEXbj28lRYD;
cookieconsent_status=dismiss; welcomebanner_status=dismiss
```

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 (1)

VULNERABILITY INFO PLUGIN ID 114135

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/redirect

INPUT TYPE	link
INPUT NAME	to

Identification

PAYLOAD

```
was-tnb-jmx
```

PROOF

```
Input reflected in the response body : 'was-tnb-jmx'.
```

OUTPUT

```
The scanner was able to detect an input reflected in the response body.
```

HTTP Info

REQUEST MADE

```
GET /redirect?to=was-tnb-jmx HTTP/2
```

REQUEST HEADERS

```
Host: juice-shop-16-0-1-178712031365.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: language=en; continueCode=5PD2YLPJeo8nyMjZXVOD34wKlWgAOkfJpAra79p51QRExqzYm2bBvN6kklXR;
cookieconsent_status=dismiss
```

RESPONSE HEADERS

```
HTTP/2 406
access-control-allow-origin: *
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
feature-policy: payment 'self'
x-recruiting: /#/jobs
content-type: text/html; charset=utf-8
vary: Accept-Encoding
content-encoding: gzip
x-cloud-trace-context: 66e8f82b9e132da3ccbd2ec16100d20b
date: Fri, 25 Apr 2025 23:11:44 GMT
server: Google Frontend
content-length: 808
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

WebSocket Detected

VULNERABILITY INFO PLUGIN ID 114395

Description

This is an informational plugin to inform the user that the scanner has detected the usage of WebSockets on the target web application.

Solution

-

See Also

https://developer.mozilla.org/en-US/docs/Web/API/WebSockets_API

Plugin Details

PUBLICATION DATE	2024-08-12T00:00:00+00:00
MODIFICATION DATE	2024-08-12T00:00:00+00:00
FAMILY	Web Applications
SEVERITY	Info
PLUGIN ID	114395

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

WebSocket Detected Instances (1)

VULNERABILITY INFO PLUGIN ID 114395

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/

Identification

PROOF

```
The scanner detected a WebSocket creation to the following endpoint: wss://juice-shop-16-0-1-178712031365.us-west1.run.app/socket.io/?EIO=4&transport=websocket&sid=q57_qHGEncDGUU1JAABc.The WebSocket creation has been initialized by the following resource : https://juice-shop-16-0-1-178712031365.us-west1.run.app/vendor.js (script)
```

OUTPUT

```
The scanner was able to identify the usage of WebSockets on the target application.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8
Date: Fri, 25 Apr 2025 23:10:08 GMT
Etag: W/"ea4-1966f2bc520"
Feature-Policy: payment 'self'
Last-Modified: Fri, 25 Apr 2025 22:57:41 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Length: 4619
```

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 (3)

VULNERABILITY INFO PLUGIN ID 114466

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/

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
/ :
* styles.css
```

OUTPUT

```
The scanner was able to detect a Path Relative Stylesheet Import.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8
Date: Fri, 25 Apr 2025 23:10:08 GMT
Etag: W/"ea4-1966f2bc520"
Feature-Policy: payment 'self'
Last-Modified: Fri, 25 Apr 2025 22:57:41 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Length: 4619
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/public/images/uploads/%F0%9F%98%BC-

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
/ :
* styles.css
```

OUTPUT

```
The scanner was able to detect a Path Relative Stylesheet Import.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/assets/public/images/uploads/%F0%9F%98%BC-
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=az_AZ
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8
Date: Sat, 26 Apr 2025 06:45:12 GMT
Etag: W/"ea4-19670be8e8c"
Feature-Policy: payment 'self'
Last-Modified: Sat, 26 Apr 2025 06:17:38 GMT
Server: Google Frontend
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Length: 4619
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/api-docs/

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
/ :
* ./swagger-ui.css
```

OUTPUT

```
The scanner was able to detect a Path Relative Stylesheet Import.
```

HTTP Info

REQUEST MADE

```
GET https://juice-shop-16-0-1-178712031365.us-west1.run.app/api-docs/
```

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Cookie: cookieconsent_status=dismiss; welcomebanner_status=dismiss;
continueCode=VKOkVQ2LxPebaoXnwqZNWjBrdxxsjfj7c7LdEgRDY6M9pK8y7z3J54mvl1O1; language=az_AZ
If-None-Match: W/"c22-H8FH9nKD8DeX/nvIRrte6ZjP2a4"
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
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Date: Sat, 26 Apr 2025 05:33:11 GMT
Etag: W/"c22-H8FH9nKD8DeX/nvIRrte6ZjP2a4"
Feature-Policy: payment 'self'
Server: Google Frontend
X-Cloud-Trace-Context: b20775ae703a7d2cc1e2eac79d916b92
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs
Content-Encoding: gzip
Content-Length: 3977
Content-Type: text/html; charset=utf-8
Vary: Accept-Encoding
```

Virtual Hosts Detected

VULNERABILITY INFO PLUGIN ID 114503

Description

This is an informational plugin to inform the user that the scanner detected the presence of one or multiple virtual hosts on the target server.

Solution

Review all the detected virtual hosts to ensure they are expected to be externally reachable.

See Also

https://httpd.apache.org/docs/2.4/vhosts/examples.html
https://www.thehacker.recipes/web/recon/virtual-host-fuzzing

Plugin Details

PUBLICATION DATE	2024-11-20T00:00:00+00:00
MODIFICATION DATE	2024-11-26T00:00:00+00:00
FAMILY	Web Applications
SEVERITY	Info
PLUGIN ID	114503

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

Virtual Hosts Detected Instances (1)

VULNERABILITY INFO PLUGIN ID 114503

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/#/

Identification

PROOF

```
By crafting a request with a specific 'Host' header the scanner obtained a different response
```

OUTPUT

```
The scanner was able to detect the present of another virtual host on the target ip 216.239.32.53: 'admin.us-west1.run.
app:443'
```

HTTP Info

REQUEST MADE

```
GET / HTTP/2
```

REQUEST HEADERS

```
Host: admin.us-west1.run.app:443
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-length: 272
content-type: text/html; charset=UTF-8
date: Fri, 25 Apr 2025 23:22:33 GMT
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

REST API Detected

VULNERABILITY INFO PLUGIN ID 114608

Description

This is an informational notice that the scanner was able to detect a REST API.

Solution

-

See Also

https://blog.postman.com/rest-api-examples/
https://cheatsheetseries.owasp.org/cheatsheets/Web_Service_Security_Cheat_Sheet.html

Plugin Details

PUBLICATION DATE	2025-03-03T00:00:00+00:00
MODIFICATION DATE	2025-03-03T00:00:00+00:00
FAMILY	Web Applications
SEVERITY	Info
PLUGIN ID	114608

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

REST API Detected Instances (5)

VULNERABILITY INFO PLUGIN ID 114608

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/SecurityQuestions/

Identification

OUTPUT

```
The scanner was able to identify a REST API.
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/Quantitys/

Identification

OUTPUT

```
The scanner was able to identify a REST API.
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/Challenges/

Identification

OUTPUT

```
The scanner was able to identify a REST API.
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/api/Feedbacks/

Identification

OUTPUT

```
The scanner was able to identify a REST API.
```

INSTANCE

https://juice-shop-16-0-1-178712031365.us-west1.run.app/api-docs/

Identification

OUTPUT

```
The scanner was able to identify a REST API.
```

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-16-0-1-178712031365.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
```