ZAP Scanning Report

Generated with ZAP on Sat 12 Aug 2023, at 16:33:22

ZAP Version: 2.13.0

Contents

- About this report
  - Report parameters
- Summaries
  - Alert counts by risk and confidence
  - Alert counts by site and risk
  - Alert counts by alert type
- Alerts
  - Risk=Medium, Confidence=High (2)
  - Risk=Medium, Confidence=Medium (2)
  - Risk=Low, Confidence=Medium (3)
  - Risk=Low, Confidence=Low (1)
  - Risk=Informational, Confidence=Medium (1)
  - Risk=Informational, Confidence=Low (1)
- Appendix
  - Alert types

About this report

Report parameters

Contexts

No contexts were selected, so all contexts were included by default.

Sites

The following sites were included:

- `http://juice-shop.herokuapp.com`

(If no sites were selected, all sites were included by default.)

An included site must also be within one of the included contexts for its data to be included in the report.

Risk levels

Included: `High`, `Medium`, `Low`, `Informational`

Excluded: None

Confidence levels

Included: `User Confirmed`, `High`, `Medium`, `Low`

Excluded: `User Confirmed`, `High`, `Medium`, `Low`, `False Positive`

Summaries

Alert counts by risk and confidence

This table shows the number of alerts for each level of risk and confidence included in the report.

(The percentages in brackets represent the count as a percentage of the total number of alerts included in the report, rounded to one decimal place.)

		Confidence				
		User Confirmed	High	Medium	Low	Total
Risk	High	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
	Medium	0 (0.0%)	2 (20.0%)	2 (20.0%)	0 (0.0%)	4 (40.0%)
	Low	0 (0.0%)	0 (0.0%)	3 (30.0%)	1 (10.0%)	4 (40.0%)
	Informational	0 (0.0%)	0 (0.0%)	1 (10.0%)	1 (10.0%)	2 (20.0%)
	Total	0 (0.0%)	2 (20.0%)	6 (60.0%)	2 (20.0%)	10 (100%)

Alert counts by site and risk

This table shows, for each site for which one or more alerts were raised, the number of alerts raised at each risk level.

Alerts with a confidence level of "False Positive" have been excluded from these counts.

(The numbers in brackets are the number of alerts raised for the site at or above that risk level.)

	Risk			
	High (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informational)

		Risk			
		High (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informational)
Site	http://juice-shop.herokuapp.com	0 (0)	4 (4)	4 (8)	2 (10)

Alert counts by alert type

This table shows the number of alerts of each alert type, together with the alert type's risk level.

(The percentages in brackets represent each count as a percentage, rounded to one decimal place, of the total number of alerts included in this report.)

Alert type	Risk	Count
Content Security Policy (CSP) Header Not Set	Medium	4 (40.0%)
Cross-Domain Misconfiguration	Medium	32 (320.0%)
Missing Anti-clickjacking Header	Medium	2 (20.0%)
Session ID in URL Rewrite	Medium	8 (80.0%)
Cross-Domain JavaScript Source File Inclusion	Low	4 (40.0%)
Private IP Disclosure	Low	1 (10.0%)
Timestamp Disclosure - Unix	Low	5
Total		10

Alert type	Risk	Count
		(50.0%)
X-Content-Type-Options Header Missing	Low	8 (80.0%)
Information Disclosure - Suspicious Comments	Informational	3 (30.0%)
Modern Web Application	Informational	2 (20.0%)
Total		10

Alerts

Risk=Medium, Confidence=High (2)

http://juice-shop.herokuapp.com (2)

Content Security Policy (CSP) Header Not Set (1)

▼ GET http://juice-shop.herokuapp.com/

Alert tags

- OWASP_2021_A05
- OWASP_2017_A06

Alert description

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should

	be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

Request	▼ Request line and header section (249 bytes)
	
	`GET http://juice-shop.herokuapp.com/ HTTP/1.1`
	`host: juice-shop.herokuapp.com`
	`user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36`
	`pragma: no-cache`
	`cache-control: no-cache`
	
	▼ Request body (0 bytes)

Response	▼ Status line and header section (475 bytes)
	
	`HTTP/1.1 200 OK`
	`Server: Cowboy`
	`Connection: keep-alive`
	`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: Sat, 12 Aug 2023 01:07:03 GMT`
	`Etag: W/"7c3-189e7484fd7"`
	`Content-Type: text/html; charset=UTF-8`
	`Content-Length: 1987`

```
Vary: Accept-Encoding
Date: Sat, 12 Aug 2023 10:31:55 GMT
Via: 1.1 vegur
```

▼ Response body (1987 bytes)

```
<!--
  ~ Copyright (c) 2014-2023 Bjoern
Kimminich & the OWASP Juice Shop
contributors.
  ~ SPDX-License-Identifier: MIT
  --><!DOCTYPE html><html lang="en">
<head>
  <meta charset="utf-8">
  <title>OWASP Juice Shop</title>
  <meta name="description"
content="Probably the most modern
and sophisticated insecure web
application">
  <meta name="viewport"
content="width=device-width,
initial-scale=1">
  <link id="favicon" rel="icon"
type="image/x-icon"
href="assets/public/favicon_js.ico">
  <link rel="stylesheet"
type="text/css"
href="//cdnjs.cloudflare.com/ajax/li
bs/cookieconsent2/3.1.0/cookieconsen
t.min.css">
  <script
src="//cdnjs.cloudflare.com/ajax/lib
s/cookieconsent2/3.1.0/cookieconsent
.min.js"></script>
  <script
src="//cdnjs.cloudflare.com/ajax/lib
s/jquery/2.2.4/jquery.min.js">
</script>
  <script>
    window.addEventListener("load",
function(){
```

```
window.cookieconsent.initialise({
        "palette": {
          "popup": { "background":
"#546e7a", "text": "#ffffff" },
          "button": { "background":
"#558b2f", "text": "#ffffff" }
        },
        "theme": "classic",
        "position": "bottom-right",
        "content": { "message":
"This website uses fruit cookies to
ensure you get the juiciest
tracking experience.", "dismiss":
"Me want it!", "link": "But me
wait!", "href":
"https://www.youtube.com/watch?
v=9PnbKL3wuH4" }
      })});
  </script>
<style>.bluegrey-lightgreen-
theme.mat-app-background{background-
color:#303030;color:#fff}@charset
"UTF-8";@media screen and (-webkit-
min-device-pixel-ratio:0){}</style>
<link rel="stylesheet"
href="styles.css" media="print"
onload="this.media='all'"><noscript>
<link rel="stylesheet"
href="styles.css"></noscript></head>
<body class="mat-app-background
bluegrey-lightgreen-theme">
  <app-root></app-root>
<script src="runtime.js"
type="module"></script><script
src="polyfills.js" type="module">
</script><script src="vendor.js"
type="module"></script><script
src="main.js" type="module">
</script>

</body></html>
```

Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Session ID in URL Rewrite (1)

▶ POST http://juice-shop.herokuapp.com/socket.io/?EIO=4&transport=polling&t=OdfJXGr&sid=dkmOedJLEAZdiEwGACee

Risk=Medium, Confidence=Medium (2)

http://juice-shop.herokuapp.com (2)

Cross-Domain Misconfiguration (1)

▼ GET http://juice-shop.herokuapp.com/

Alert tags	▪ OWASP_2021_A01 ▪ OWASP_2017_A05
Alert description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server
Other info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.

Request

▼ Request line and header section (249 bytes)

```
GET http://juice-
shop.herokuapp.com/ HTTP/1.1
host: juice-shop.herokuapp.com
user-agent: Mozilla/5.0 (Windows NT
10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/114.0.0.0
Safari/537.36
pragma: no-cache
cache-control: no-cache
```

▼ Request body (0 bytes)

Response

▼ Status line and header section (475 bytes)

```
HTTP/1.1 200 OK
Server: Cowboy
Connection: keep-alive
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: Sat, 12 Aug 2023
01:07:03 GMT
Etag: W/"7c3-189e7484fd7"
Content-Type: text/html;
charset=UTF-8
Content-Length: 1987
Vary: Accept-Encoding
Date: Sat, 12 Aug 2023 10:31:55 GMT
Via: 1.1 vegur
```

▼ Response body (1987 bytes)

```
<!--
  ~ Copyright (c) 2014-2023 Bjoern
Kimminich & the OWASP Juice Shop
contributors.
  ~ SPDX-License-Identifier: MIT
  --><!DOCTYPE html><html lang="en">
<head>
  <meta charset="utf-8">
  <title>OWASP Juice Shop</title>
  <meta name="description"
content="Probably the most modern
and sophisticated insecure web
application">
  <meta name="viewport"
content="width=device-width,
initial-scale=1">
  <link id="favicon" rel="icon"
type="image/x-icon"
href="assets/public/favicon_js.ico">
  <link rel="stylesheet"
type="text/css"
href="//cdnjs.cloudflare.com/ajax/li
bs/cookieconsent2/3.1.0/cookieconsen
t.min.css">
  <script
src="//cdnjs.cloudflare.com/ajax/lib
s/cookieconsent2/3.1.0/cookieconsent
.min.js"></script>
  <script
src="//cdnjs.cloudflare.com/ajax/lib
s/jquery/2.2.4/jquery.min.js">
</script>
  <script>
    window.addEventListener("load",
function(){

window.cookieconsent.initialise({
        "palette": {
          "popup": { "background":
"#546e7a", "text": "#ffffff" },
          "button": { "background":
"#558b2f", "text": "#ffffff" }
        },
```

```
        "theme": "classic",
        "position": "bottom-right",
        "content": { "message":
"This website uses fruit cookies to
ensure you get the juiciest
tracking experience.", "dismiss":
"Me want it!", "link": "But me
wait!", "href":
"https://www.youtube.com/watch?
v=9PnbKL3wuH4" }
      })});
  </script>
<style>.bluegrey-lightgreen-
theme.mat-app-background{background-
color:#303030;color:#fff}@charset
"UTF-8";@media screen and (-webkit-
min-device-pixel-ratio:0){}</style>
<link rel="stylesheet"
href="styles.css" media="print"
onload="this.media='all'"><noscript>
<link rel="stylesheet"
href="styles.css"></noscript></head>
<body class="mat-app-background
bluegrey-lightgreen-theme">
  <app-root></app-root>
<script src="runtime.js"
type="module"></script><script
src="polyfills.js" type="module">
</script><script src="vendor.js"
type="module"></script><script
src="main.js" type="module">
</script>

</body></html>
```


Evidence

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

Solution

Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).

	Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.

Missing Anti-clickjacking Header (1)

▼ POST http://juice-shop.herokuapp.com/socket.io/?EIO=4&transport=polling&t=OdfJXGr&sid=dkmOedJLEAZdiEwGACee

Alert tags	▪ OWASP_2021_A05 ▪ WSTG-v42-CLNT-09 ▪ OWASP_2017_A06
Alert description	The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks.
Request	▼ Request line and header section (448 bytes) POST http://juice-shop.herokuapp.com/socket.io/?EIO=4&transport=polling&t=OdfJXGr&sid=dkmOedJLEAZdiEwGACee HTTP/1.1 host: juice-shop.herokuapp.com User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0 Accept: */* Accept-Language: en-US,en;q=0.5 Referer: http://juice-shop.herokuapp.com/ Content-type: text/plain;charset=UTF-8 Content-Length: 2 Origin: http://juice-

```
shop.herokuapp.com
Connection: keep-alive
```

▼ Request body (2 bytes)

```
40
```

Response

▼ Status line and header section (156 bytes)

```
HTTP/1.1 200 OK
Server: Cowboy
Connection: keep-alive
Content-Type: text/html
Content-Length: 2
Date: Sat, 12 Aug 2023 10:32:34 GMT
Via: 1.1 vegur
```

▼ Response body (2 bytes)

```
ok
```

Parameter

`x-frame-options`

Solution

Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app.

If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.

Risk=Low, Confidence=Medium (3)

http://juice-shop.herokuapp.com (3)

Cross-Domain JavaScript Source File Inclusion (1)

▼ GET http://juice-shop.herokuapp.com/

Alert tags

- OWASP_2021_A08

Alert description

The page includes one or more script files from a third-party domain.

Request

▼ Request line and header section (249 bytes)

```
GET http://juice-
shop.herokuapp.com/ HTTP/1.1
host: juice-shop.herokuapp.com
user-agent: Mozilla/5.0 (Windows NT
10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/114.0.0.0
Safari/537.36
pragma: no-cache
cache-control: no-cache
```

▼ Request body (0 bytes)

Response

▼ Status line and header section (475 bytes)

```
HTTP/1.1 200 OK
Server: Cowboy
Connection: keep-alive
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: Sat, 12 Aug 2023
01:07:03 GMT
Etag: W/"7c3-189e7484fd7"
Content-Type: text/html;
charset=UTF-8
Content-Length: 1987
Vary: Accept-Encoding
Date: Sat, 12 Aug 2023 10:31:55 GMT
Via: 1.1 vegur
```

▼ Response body (1987 bytes)

```
<!--
  ~ Copyright (c) 2014-2023 Bjoern
Kimminich & the OWASP Juice Shop
contributors.
  ~ SPDX-License-Identifier: MIT
  --><!DOCTYPE html><html lang="en">
<head>
  <meta charset="utf-8">
  <title>OWASP Juice Shop</title>
  <meta name="description"
content="Probably the most modern
and sophisticated insecure web
application">
  <meta name="viewport"
content="width=device-width,
initial-scale=1">
  <link id="favicon" rel="icon"
type="image/x-icon"
href="assets/public/favicon_js.ico">
  <link rel="stylesheet"
type="text/css"
href="//cdnjs.cloudflare.com/ajax/li
bs/cookieconsent2/3.1.0/cookieconsen
t.min.css">
  <script
src="//cdnjs.cloudflare.com/ajax/lib
s/cookieconsent2/3.1.0/cookieconsent
.min.js"></script>
```

```
  <script
src="//cdnjs.cloudflare.com/ajax/lib
s/jquery/2.2.4/jquery.min.js">
</script>
  <script>
    window.addEventListener("load",
function(){

window.cookieconsent.initialise({
        "palette": {
          "popup": { "background":
"#546e7a", "text": "#ffffff" },
          "button": { "background":
"#558b2f", "text": "#ffffff" }
        },
        "theme": "classic",
        "position": "bottom-right",
        "content": { "message":
"This website uses fruit cookies to
ensure you get the juiciest
tracking experience.", "dismiss":
"Me want it!", "link": "But me
wait!", "href":
"https://www.youtube.com/watch?
v=9PnbKL3wuH4" }
      })});
  </script>
<style>.bluegrey-lightgreen-
theme.mat-app-background{background-
color:#303030;color:#fff}@charset
"UTF-8";@media screen and (-webkit-
min-device-pixel-ratio:0){}</style>
<link rel="stylesheet"
href="styles.css" media="print"
onload="this.media='all'"><noscript>
<link rel="stylesheet"
href="styles.css"></noscript></head>
<body class="mat-app-background
bluegrey-lightgreen-theme">
  <app-root></app-root>
<script src="runtime.js"
type="module"></script><script
src="polyfills.js" type="module">
```

	`</script><script src="vendor.js" type="module"></script><script src="main.js" type="module"> </script>`
	
	`</body></html>`

Parameter	`//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js`
Evidence	`<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>`
Solution	Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.

Private IP Disclosure (1)

▼ `GET http://juice-shop.herokuapp.com/rest/admin/application-configuration`

Alert tags	▪ OWASP_2021_A01 ▪ OWASP_2017_A03
Alert description	A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.
Other info	192.168.99.100:3000 192.168.99.100:4200

Request

▼ Request line and header section (344 bytes)

```
GET http://juice-
shop.herokuapp.com/rest/admin/applic
ation-configuration HTTP/1.1
host: juice-shop.herokuapp.com
User-Agent: Mozilla/5.0 (X11; Linux
x86_64; rv:102.0) Gecko/20100101
Firefox/102.0
Accept: application/json,
text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: http://juice-
shop.herokuapp.com/
Connection: keep-alive
```

▼ Request body (0 bytes)

Response

▼ Status line and header section (398 bytes)

```
HTTP/1.1 200 OK
Server: Cowboy
Connection: keep-alive
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
Content-Length: 18843
Etag: W/"499b-
ti9KmawfWG7Y+IqBcogANHT4LB4"
Vary: Accept-Encoding
Date: Sat, 12 Aug 2023 10:32:31 GMT
Via: 1.1 vegur
```

▶ Response body (18843 bytes)

Evidence	`192.168.99.100:3000`
Solution	Remove the private IP address from the HTTP response body. For comments, use JSP/ASP/PHP comment instead of HTML/JavaScript comment which can be seen by client browsers.

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

▼ `GET http://juice-shop.herokuapp.com/socket.io/?EIO=4&transport=polling&t=OdfJWTW`

Alert tags	▪ OWASP_2021_A05 ▪ OWASP_2017_A06
Alert description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Other info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

Request

▼ Request line and header section (322 bytes)

```
GET http://juice-
shop.herokuapp.com/socket.io/?
EIO=4&transport=polling&t=OdfJWTW
HTTP/1.1
host: juice-shop.herokuapp.com
User-Agent: Mozilla/5.0 (X11; Linux
x86_64; rv:102.0) Gecko/20100101
Firefox/102.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Referer: http://juice-
shop.herokuapp.com/
Connection: keep-alive
```

▼ Request body (0 bytes)

Response

▼ Status line and header section (173 bytes)

```
HTTP/1.1 200 OK
Server: Cowboy
Connection: keep-alive
Content-Type: text/plain;
charset=UTF-8
Content-Length: 96
Date: Sat, 12 Aug 2023 10:32:31 GMT
Via: 1.1 vegur
```

▼ Response body (96 bytes)

```
0{"sid":"dkmOedJLEAZdiEwGACee","upgr
ades":
["websocket"],"pingInterval":25000,"
pingTimeout":5000}
```

Parameter

x-content-type-options

Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages. If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.

Risk=Low, Confidence=Low (1)

http://juice-shop.herokuapp.com (1)

Timestamp Disclosure - Unix (1)

▼ GET http://juice-shop.herokuapp.com/main.js

Alert tags	▪ OWASP_2021_A01 ▪ OWASP_2017_A03
Alert description	A timestamp was disclosed by the application/web server - Unix
Other info	1734944650, which evaluates to: 2024-12-23 04:04:10
Request	▼ Request line and header section (310 bytes) GET http://juice-shop.herokuapp.com/main.js HTTP/1.1 host: juice-shop.herokuapp.com user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like

Gecko) Chrome/114.0.0.0
Safari/537.36
pragma: no-cache
cache-control: no-cache
referer: http://juice-
shop.herokuapp.com/sitemap.xml

▼ Request body (0 bytes)

Response

▼ Status line and header section (492 bytes)

HTTP/1.1 200 OK
Server: Cowboy
Connection: keep-alive
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, 19 May 2023
22:57:12 GMT
Etag: W/"61983-188363b3d40"
Content-Type:
application/javascript;
charset=UTF-8
Content-Length: 399747
Vary: Accept-Encoding
Date: Sat, 12 Aug 2023 10:31:56 GMT
Via: 1.1 vegur

▶ Response body (399747 bytes)

Evidence

1734944650

Solution

Manually confirm that the timestamp data is not sensitive, and that the data

cannot be aggregated to disclose exploitable patterns.

Risk=Informational, Confidence=Medium (1)

http://juice-shop.herokuapp.com (1)

Modern Web Application (1)

▼ GET http://juice-shop.herokuapp.com/

Alert tags

Alert description	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Other info	No links have been found while there are scripts, which is an indication that this is a modern web application.

Request	▼ Request line and header section (249 bytes)
	
	`GET http://juice-shop.herokuapp.com/ HTTP/1.1`
	`host: juice-shop.herokuapp.com`
	`user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36`
	`pragma: no-cache`
	`cache-control: no-cache`
	
	▼ Request body (0 bytes)

Response

▼ Status line and header section (475 bytes)

```
HTTP/1.1 200 OK
Server: Cowboy
Connection: keep-alive
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: Sat, 12 Aug 2023
01:07:03 GMT
Etag: W/"7c3-189e7484fd7"
Content-Type: text/html;
charset=UTF-8
Content-Length: 1987
Vary: Accept-Encoding
Date: Sat, 12 Aug 2023 10:31:55 GMT
Via: 1.1 vegur
```

▼ Response body (1987 bytes)

```
<!--
  ~ Copyright (c) 2014-2023 Bjoern
Kimminich & the OWASP Juice Shop
contributors.
  ~ SPDX-License-Identifier: MIT
  --><!DOCTYPE html><html lang="en">
<head>
  <meta charset="utf-8">
  <title>OWASP Juice Shop</title>
  <meta name="description"
content="Probably the most modern
and sophisticated insecure web
application">
  <meta name="viewport"
content="width=device-width,
initial-scale=1">
  <link id="favicon" rel="icon"
```

```
type="image/x-icon"
href="assets/public/favicon_js.ico">
  <link rel="stylesheet"
type="text/css"
href="//cdnjs.cloudflare.com/ajax/li
bs/cookieconsent2/3.1.0/cookieconsen
t.min.css">
  <script
src="//cdnjs.cloudflare.com/ajax/lib
s/cookieconsent2/3.1.0/cookieconsent
.min.js"></script>
  <script
src="//cdnjs.cloudflare.com/ajax/lib
s/jquery/2.2.4/jquery.min.js">
</script>
  <script>
    window.addEventListener("load",
function(){

window.cookieconsent.initialise({
        "palette": {
          "popup": { "background":
"#546e7a", "text": "#ffffff" },
          "button": { "background":
"#558b2f", "text": "#ffffff" }
        },
        "theme": "classic",
        "position": "bottom-right",
        "content": { "message":
"This website uses fruit cookies to
ensure you get the juiciest
tracking experience.", "dismiss":
"Me want it!", "link": "But me
wait!", "href":
"https://www.youtube.com/watch?
v=9PnbKL3wuH4" }
      })});
  </script>
<style>.bluegrey-lightgreen-
theme.mat-app-background{background-
color:#303030;color:#fff}@charset
"UTF-8";@media screen and (-webkit-
min-device-pixel-ratio:0){}</style>
```

```
<link rel="stylesheet"
href="styles.css" media="print"
onload="this.media='all'"><noscript>
<link rel="stylesheet"
href="styles.css"></noscript></head>
<body class="mat-app-background
bluegrey-lightgreen-theme">
  <app-root></app-root>
<script src="runtime.js"
type="module"></script><script
src="polyfills.js" type="module">
</script><script src="vendor.js"
type="module"></script><script
src="main.js" type="module">
</script>

</body></html>
```

Evidence

```
<script
src="//cdnjs.cloudflare.com/ajax/lib
s/cookieconsent2/3.1.0/cookieconsent
.min.js"></script>
```

Solution

This is an informational alert and so no changes are required.

Risk=Informational, Confidence=Low (1)

http://juice-shop.herokuapp.com (1)

Information Disclosure - Suspicious Comments (1)

▼ GET http://juice-shop.herokuapp.com/main.js

Alert tags

- OWASP_2021_A01
- WSTG-v42-INFO-05
- OWASP_2017_A03

Alert description

The response appears to contain suspicious comments which may help

an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.

Other info

The following pattern was used: \bQUERY\b and was detected in the element starting with: ""use strict"; (self.webpackChunkfrontend=self.webpackChunkfrontend||[]).push([[179], {902:(at,Bt,d)=>{var J=d(1481),t=d(4650),k=d(", see evidence field for the suspicious comment/snippet.

Request

▼ Request line and header section (310 bytes)

```
GET http://juice-shop.herokuapp.com/main.js HTTP/1.1
host: juice-shop.herokuapp.com
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36
pragma: no-cache
cache-control: no-cache
referer: http://juice-shop.herokuapp.com/sitemap.xml
```

▼ Request body (0 bytes)

Response

▼ Status line and header section (492 bytes)

```
HTTP/1.1 200 OK
Server: Cowboy
Connection: keep-alive
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, 19 May 2023
22:57:12 GMT
Etag: W/"61983-188363b3d40"
Content-Type:
application/javascript; charset=UTF-
8
Content-Length: 399747
Vary: Accept-Encoding
Date: Sat, 12 Aug 2023 10:31:56 GMT
Via: 1.1 vegur
```

▶ Response body (399747 bytes)

Evidence query

Solution Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.

Appendix

Alert types

This section contains additional information on the types of alerts in the report.

Content Security Policy (CSP) Header Not Set

Source raised by a passive scanner (Content Security Policy (CSP) Header Not Set)

CWE ID	693
WASC ID	15
Reference	▪ https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy ▪ https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html ▪ http://www.w3.org/TR/CSP/ ▪ http://w3c.github.io/webappsec/specs/content-security-policy/csp-specification.dev.html ▪ http://www.html5rocks.com/en/tutorials/security/content-security-policy/ ▪ http://caniuse.com/#feat=contentsecuritypolicy ▪ http://content-security-policy.com/

Cross-Domain Misconfiguration

Source	raised by a passive scanner (Cross-Domain Misconfiguration)
CWE ID	264
WASC ID	14
Reference	▪ https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Missing Anti-clickjacking Header

Source	raised by a passive scanner (Anti-clickjacking Header)
CWE ID	1021
WASC ID	15
Reference	▪ https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

Session ID in URL Rewrite

Source	raised by a passive scanner (Session ID in URL Rewrite)
CWE ID	200
WASC ID	13
Reference	▪ http://seclists.org/lists/webappsec/2002/Oct-Dec/0111.html

Cross-Domain JavaScript Source File Inclusion

Source	raised by a passive scanner (Cross-Domain JavaScript Source File Inclusion)
CWE ID	829
WASC ID	15

Private IP Disclosure

Source	raised by a passive scanner (Private IP Disclosure)
CWE ID	200

WASC ID	13
Reference	▪ https://tools.ietf.org/html/rfc1918

Timestamp Disclosure - Unix

Source	raised by a passive scanner (Timestamp Disclosure)
CWE ID	200
WASC ID	13
Reference	▪ http://projects.webappsec.org/w/page/13246936/Information%20Leakage

X-Content-Type-Options Header Missing

Source	raised by a passive scanner (X-Content-Type-Options Header Missing)
CWE ID	693
WASC ID	15
Reference	▪ http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx ▪ https://owasp.org/www-community/Security_Headers

Information Disclosure - Suspicious Comments

Source	raised by a passive scanner (Information Disclosure - Suspicious Comments)
CWE ID	200
WASC ID	13

Modern Web Application

Source	raised by a passive scanner (Modern Web Application)