Task 1: Web Application Security Testing

The goal is to identify security flaws using ethical hacking tools and OWASP standards.

What I will do:

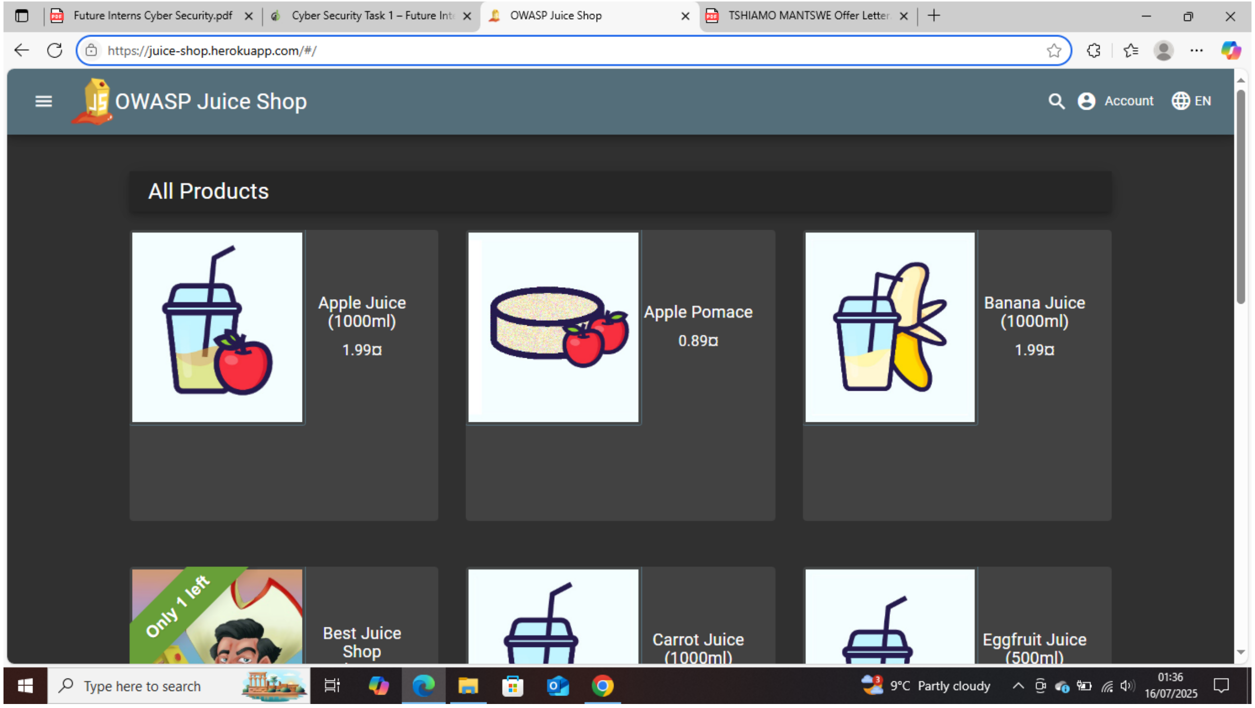
- Set up and explore a test web app (like DVWA or OWASP Juice Shop)
- Use scanning tools like OWASP ZAP, Burp Suite, or Nikto
- Test for common vulnerabilities like SQL injection, XSS, and CSRF
- Map the vulnerabilities to OWASP Top 10 threats
- Document findings with screenshots, impact level, and remediation steps
- Compile a Security Assessment Report (PDF format)

Web Application Security Assessment Report – OWASP Juice Shop

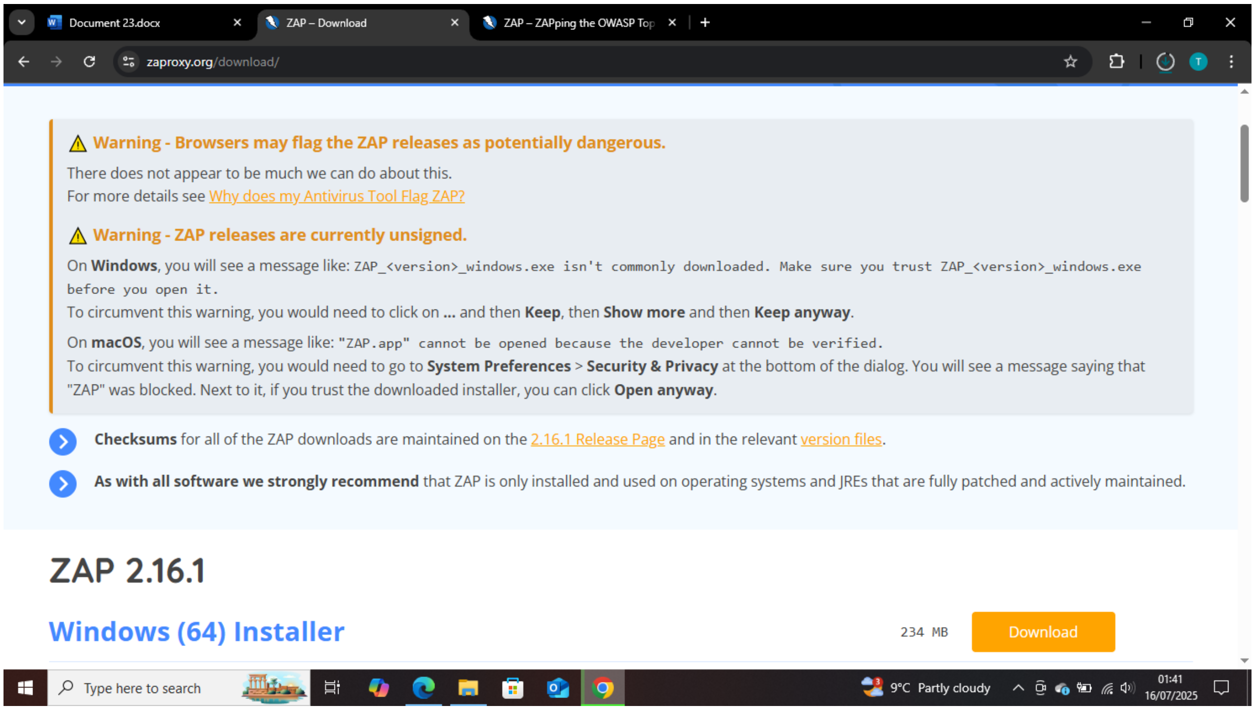
Tools Used:

- Test Web App: OWASP Juice Shop.
- Scanning tool: OWASP ZAP

To open OWASP Juice Shop, open the web browser and insert this link in your web browser; https://juice-shop.herokuapp.com/ which is online demo like below.



Then download OWASP ZAP using this link, https://www.zaproxy.org/download/. Scroll down and choose operating system and OWASP version, preferably latest version.



⚠ **Warning - Browsers may flag the ZAP releases as potentially dangerous.**

There does not appear to be much we can do about this.
For more details see Why does my Antivirus Tool Flag ZAP?

⚠ **Warning - ZAP releases are currently unsigned.**

On **Windows**, you will see a message like: `ZAP_<version>_windows.exe isn't commonly downloaded. Make sure you trust ZAP_<version>_windows.exe before you open it.`
To circumvent this warning, you would need to click on **...** and then **Keep**, then **Show more** and then **Keep anyway**.

On **macOS**, you will see a message like: `"ZAP.app" cannot be opened because the developer cannot be verified.`
To circumvent this warning, you would need to go to **System Preferences** > **Security & Privacy** at the bottom of the dialog. You will see a message saying that "ZAP" was blocked. Next to it, if you trust the downloaded installer, you can click **Open anyway**.

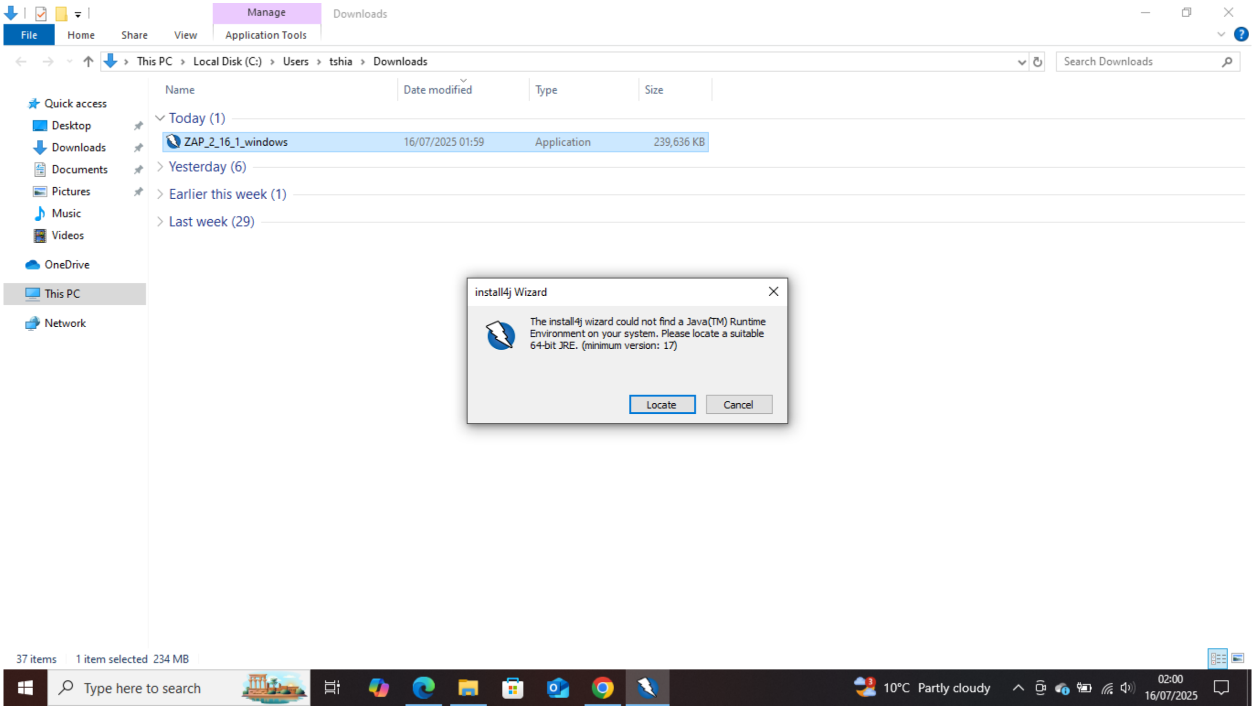
Checksums for all of the ZAP downloads are maintained on the 2.16.1 Release Page and in the relevant version files.

As with all software we strongly recommend that ZAP is only installed and used on operating systems and JREs that are fully patched and actively maintained.

ZAP 2.16.1

Windows (64) Installer 234 MB Download

Wait for the download to finish and launch it. So, I as I try to launch ZAP, I encountered the below problem.



Name	Date modified	Type	Size
ZAP_2_16_1_windows	16/07/2025 01:59	Application	239,636 KB

install4j Wizard

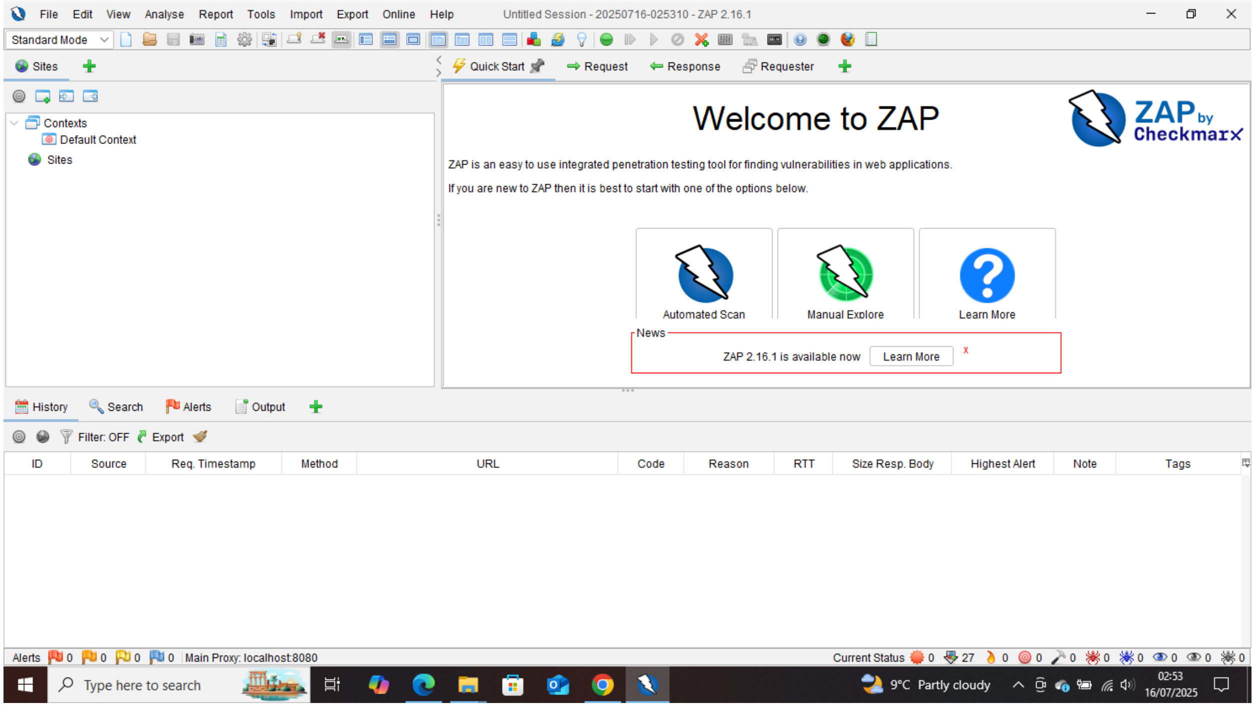
The install4j wizard could not find a Java(TM) Runtime Environment on your system. Please locate a suitable 64-bit JRE. (minimum version: 17)

Locate Cancel

So, it means that OWASP ZAP requires Java, but it's not installed (or not properly detected) on your system. So, I had to install java and try again.

To install java, go to official website of java which is, https://www.oracle.com/java/technologies/downloads/?er=221886 . Choose operating system that you are using and version. As for me, windows and JDK 24 (x64 Installer) and download.

After the download is complete, launch and install it. After installing java, try launching and installing ZAP. It should then open and install since java is installed. Now should display something like below.



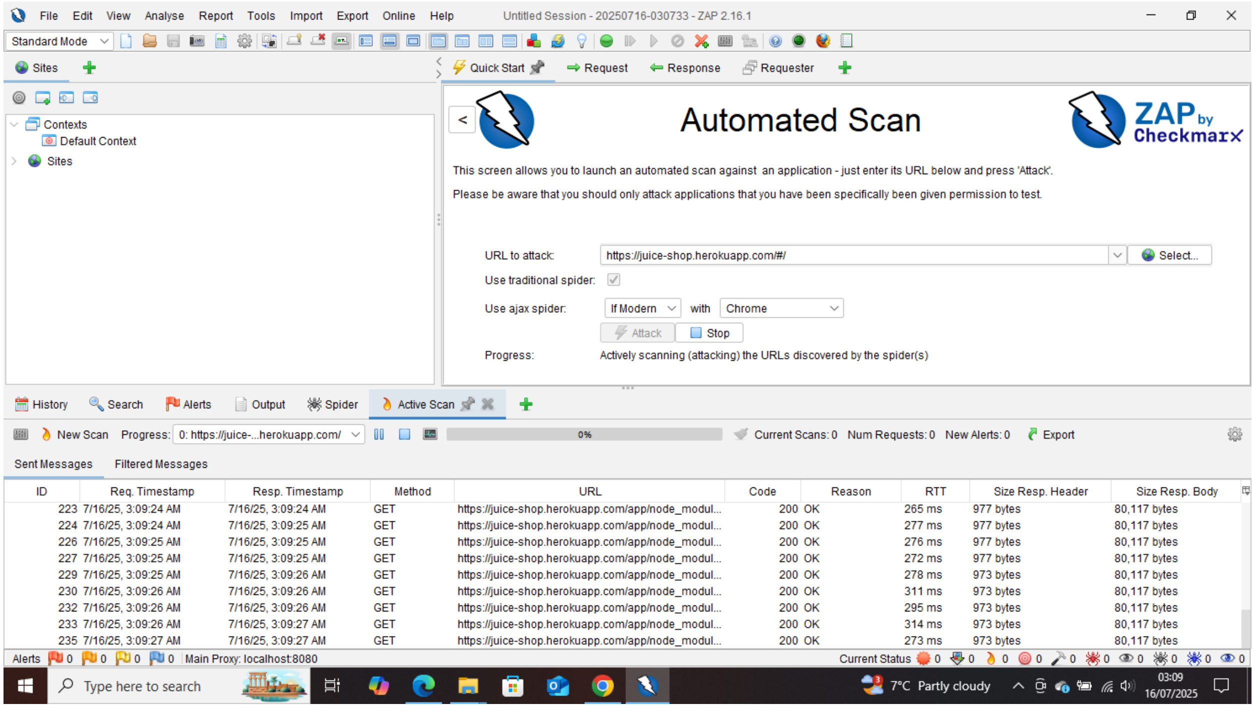
Welcome to ZAP

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

If you are new to ZAP then it is best to start with one of the options below.

ZAP 2.16.1 is available now

Click Automated Scan and paste the link in “URL to attack” or targeted URL and click attack like below.



This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.

Please be aware that you should only attack applications that you have been specifically been given permission to test.

URL to attack: https://juice-shop.herokuapp.com/#/

Use traditional spider: ☑

Use ajax spider: If Modern with Chrome

Attack Stop

Progress: Actively scanning (attacking) the URLs discovered by the spider(s)

Progress: 0: https://juice-...herokuapp.com/ 0% Current Scans: 0 Num Requests: 0 New Alerts: 0

ID	Req. Timestamp	Resp. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Header	Size Resp. Body
223	7/16/25, 3:09:24 AM	7/16/25, 3:09:24 AM	GET	https://juice-shop.herokuapp.com/app/node_modul...	200	OK	265 ms	977 bytes	80,117 bytes
224	7/16/25, 3:09:24 AM	7/16/25, 3:09:25 AM	GET	https://juice-shop.herokuapp.com/app/node_modul...	200	OK	277 ms	977 bytes	80,117 bytes
226	7/16/25, 3:09:25 AM	7/16/25, 3:09:25 AM	GET	https://juice-shop.herokuapp.com/app/node_modul...	200	OK	276 ms	977 bytes	80,117 bytes
227	7/16/25, 3:09:25 AM	7/16/25, 3:09:25 AM	GET	https://juice-shop.herokuapp.com/app/node_modul...	200	OK	272 ms	977 bytes	80,117 bytes
229	7/16/25, 3:09:25 AM	7/16/25, 3:09:26 AM	GET	https://juice-shop.herokuapp.com/app/node_modul...	200	OK	278 ms	973 bytes	80,117 bytes
230	7/16/25, 3:09:26 AM	7/16/25, 3:09:26 AM	GET	https://juice-shop.herokuapp.com/app/node_modul...	200	OK	311 ms	973 bytes	80,117 bytes
232	7/16/25, 3:09:26 AM	7/16/25, 3:09:26 AM	GET	https://juice-shop.herokuapp.com/app/node_modul...	200	OK	295 ms	973 bytes	80,117 bytes
233	7/16/25, 3:09:26 AM	7/16/25, 3:09:27 AM	GET	https://juice-shop.herokuapp.com/app/node_modul...	200	OK	314 ms	973 bytes	80,117 bytes
235	7/16/25, 3:09:27 AM	7/16/25, 3:09:27 AM	GET	https://juice-shop.herokuapp.com/app/node_modul...	200	OK	273 ms	973 bytes	80,117 bytes

Alerts 0 0 0 0 Main Proxy: localhost:8080 Current Status 0 0 0 0 0 0 0 0 0 0

It should start to show files like in the above screenshot.

Vulnerabilities

Vulnerability 1:

Sensitive File Disclosure – .darcs file

Description: A sensitive file was discovered as publicly accessible on the web server.

URL: https://juice-shop.herokuapp.com/._darcs

Impact level: Medium

Tool Used: OWASP ZAP

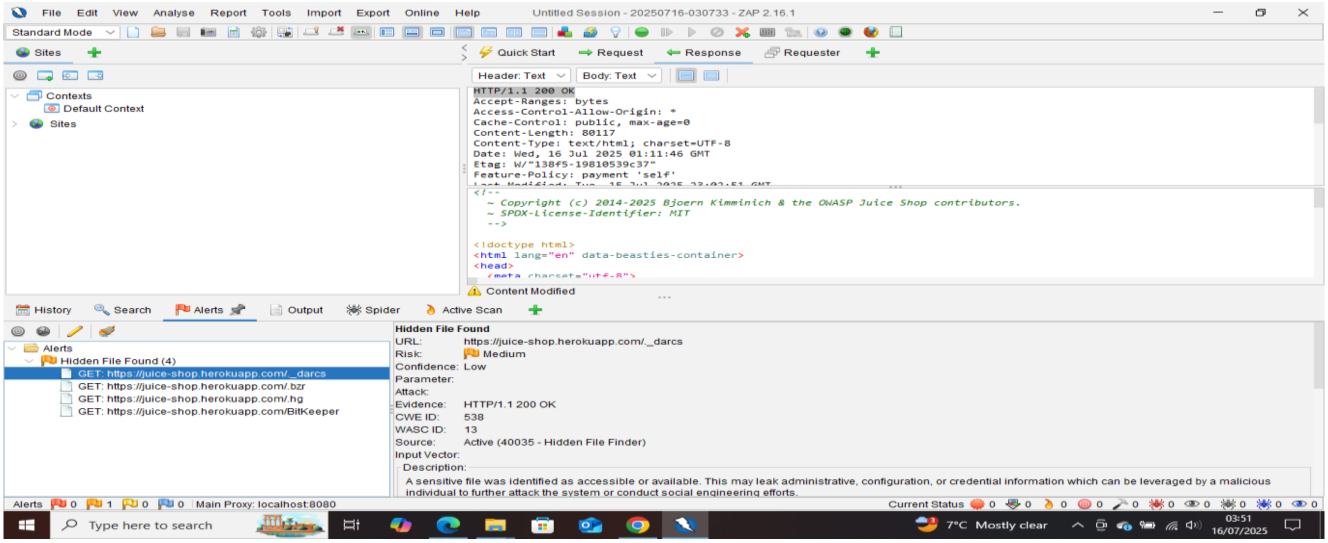
Potential Impact: This may leak administrative, configuration, or credential information which can be leveraged by a malicious individual to further attack the system or conduct social engineering efforts.

OWASP Mapping:

- **OWASP 2021 – A05: Security Misconfiguration**
- **OWASP 2017 – A06: Security Misconfiguration**

Remediation: Consider whether the component is required in production or not, if it isn't then disable it. If it is then ensure that access to it requires appropriate authentication and authorization, or limit exposure to internal systems or specific source IPs, etc.

Screenshot:



```
HTTP/1.1 200 OK
Accept-Ranges: bytes
Access-Control-Allow-Origin: *
Cache-Control: public, max-age=0
Content-Length: 80117
Content-Type: text/html; charset=UTF-8
Date: Wed, 16 Jul 2025 01:11:46 GMT
Etag: W/"138f5-19810539c37"
Feature-Policy: payment 'self'
```

```
<!--
  ~ Copyright (c) 2014-2025 Bjoern Kimminich & the OWASP Juice Shop contributors.
  ~ SPDX-License-Identifier: MIT
  -->

<!doctype html>
<html lang="en" data-beasties-container>
<head>
```

Alerts
Hidden File Found (4)
GET: https://juice-shop.herokuapp.com/._darcs
GET: https://juice-shop.herokuapp.com/.bzr
GET: https://juice-shop.herokuapp.com/.hg
GET: https://juice-shop.herokuapp.com/BitKeeper

Hidden File Found

URL:	https://juice-shop.herokuapp.com/._darcs
Risk:	Medium
Confidence:	Low
Parameter:	
Attack:	
Evidence:	HTTP/1.1 200 OK
CWE ID:	538
WASC ID:	13
Source:	Active (40035 - Hidden File Finder)
Input Vector:	

Description:

A sensitive file was identified as accessible or available. This may leak administrative, configuration, or credential information which can be leveraged by a malicious individual to further attack the system or conduct social engineering efforts.

Alerts 0 1 0 0 Main Proxy: localhost:8080

Current Status 0 0 0 0 0 0 0 0 0 0

Vulnerability 2

Sensitive File Disclosure - .bzr file

Description:

A sensitive file was identified as accessible or available at:

URL: https://juice-shop.herokuapp.com/.bzr

Impact level: Medium

Tool Used: OWASP ZAP

Potential Impact:

This may leak administrative, configuration, or credential information which can be leveraged by a malicious individual to further attack the system or conduct social engineering efforts.

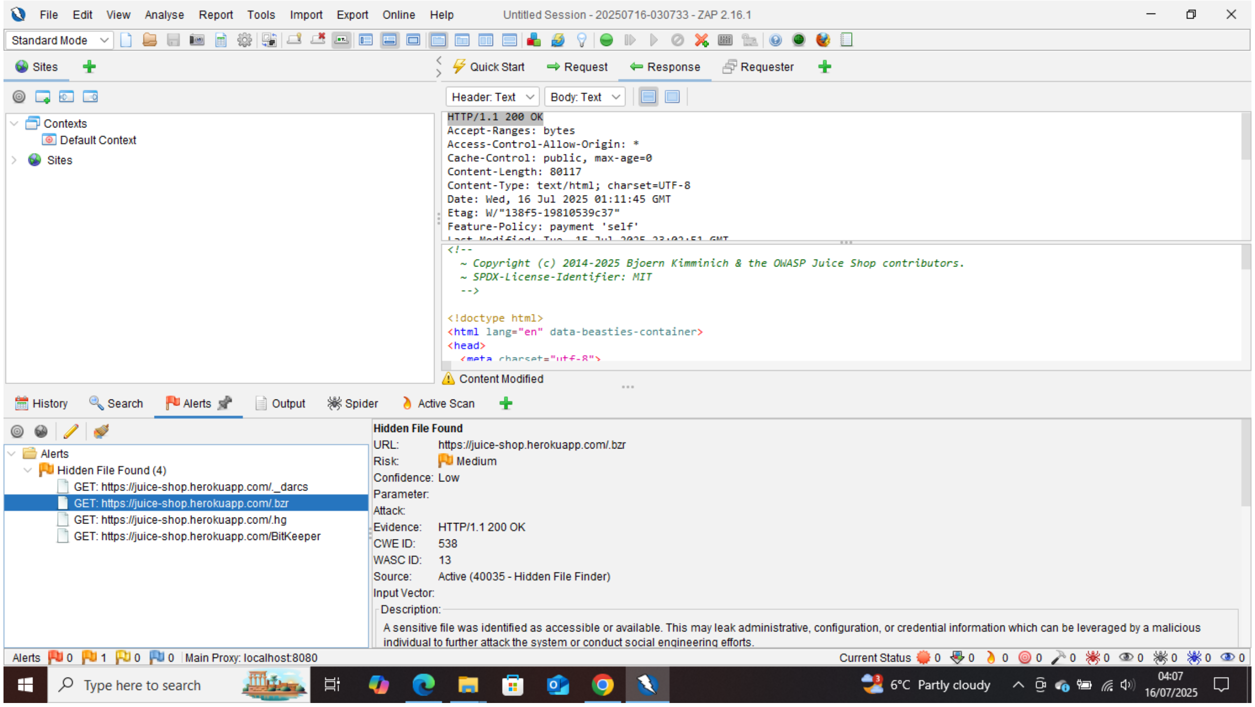
OWASP Mapping:

- OWASP_2021_A05 (Security Misconfiguration)
- OWASP_2017_A06 (Security Misconfiguration)

Remediation:

Consider whether the component is required in production or not, if it isn't then disable it. If it is then ensure access to it requires appropriate authentication and authorization, or limit exposure to internal systems or specific source IPs, etc.

Screenshot:



```
HTTP/1.1 200 OK
Accept-Ranges: bytes
Access-Control-Allow-Origin: *
Cache-Control: public, max-age=0
Content-Length: 80117
Content-Type: text/html; charset=UTF-8
Date: Wed, 16 Jul 2025 01:11:45 GMT
Etag: W/"138f5-19810539c37"
Feature-Policy: payment 'self'
```

```
<!--
  ~ Copyright (c) 2014-2025 Bjoern Kimminich & the OWASP Juice Shop contributors.
  ~ SPDX-License-Identifier: MIT
  -->

<!doctype html>
<html lang="en" data-beasties-container>
<head>
```

GET: https://juice-shop.herokuapp.com/._darcs
GET: https://juice-shop.herokuapp.com/.bzr
GET: https://juice-shop.herokuapp.com/.hg
GET: https://juice-shop.herokuapp.com/BitKeeper

Hidden File Found
URL: https://juice-shop.herokuapp.com/.bzr
Risk: Medium
Confidence: Low
Parameter:
Attack:
Evidence: HTTP/1.1 200 OK
CWE ID: 538
WASC ID: 13
Source: Active (40035 - Hidden File Finder)
Input Vector:
Description:
A sensitive file was identified as accessible or available. This may leak administrative, configuration, or credential information which can be leveraged by a malicious individual to further attack the system or conduct social engineering efforts.

Vulnerability 3

Sensitive File Disclosure - .hg file

Description:

A sensitive file was identified as accessible or available at:

URL: https://juice-shop.herokuapp.com/.hg

Impact level: Medium

Tool Used: OWASP ZAP

Potential Impact:

This may leak administrative, configuration, or credential information which can be leveraged by a malicious individual to further attack the system or conduct social engineering efforts.

OWASP Mapping:

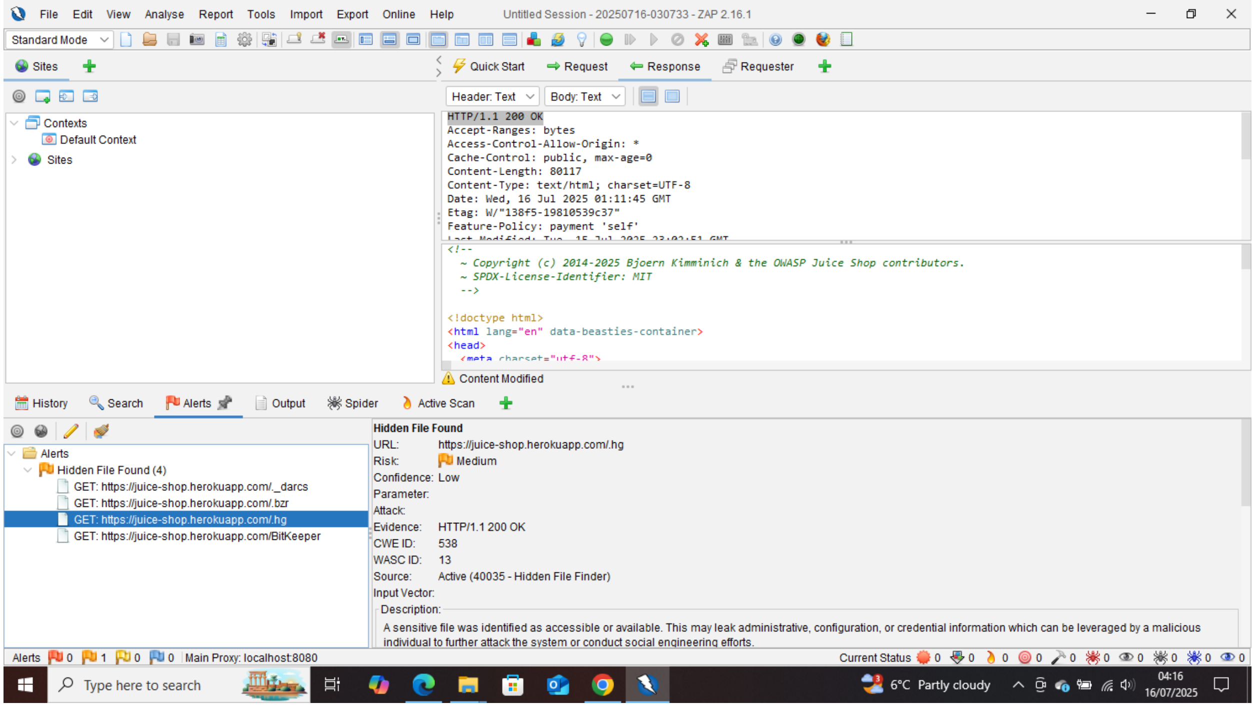
- OWASP_2021_A05

- OWASP_2017_A06

Remediation:

Consider whether the component is required in production or not, if it isn't then disable it. If it is then ensure access to it requires appropriate authentication and authorization, or limit exposure to internal systems or specific source IPs, etc.

Screenshot:



```
HTTP/1.1 200 OK
Accept-Ranges: bytes
Access-Control-Allow-Origin: *
Cache-Control: public, max-age=0
Content-Length: 80117
Content-Type: text/html; charset=UTF-8
Date: Wed, 16 Jul 2025 01:11:45 GMT
Etag: W/"138f5-19810539c37"
Feature-Policy: payment 'self'
Last-Modified: Tue, 15 Jul 2025 23:02:51 GMT
```

```
<!--
  ~ Copyright (c) 2014-2025 Bjoern Kimminich & the OWASP Juice Shop contributors.
  ~ SPDX-License-Identifier: MIT
  -->

<!doctype html>
<html lang="en" data-beasties-container>
<head>
  <meta charset="utf-8">
```

Alerts
- Hidden File Found (4)
  - GET: https://juice-shop.herokuapp.com/._darcs
  - GET: https://juice-shop.herokuapp.com/.bzr
  - GET: https://juice-shop.herokuapp.com/.hg
  - GET: https://juice-shop.herokuapp.com/BitKeeper

Hidden File Found

URL: https://juice-shop.herokuapp.com/.hg
Risk: Medium
Confidence: Low
Parameter:
Attack:
Evidence: HTTP/1.1 200 OK
CWE ID: 538
WASC ID: 13
Source: Active (40035 - Hidden File Finder)
Input Vector:

Description:

A sensitive file was identified as accessible or available. This may leak administrative, configuration, or credential information which can be leveraged by a malicious individual to further attack the system or conduct social engineering efforts.

Vulnerability 4

Sensitive File Disclosure – BitKeeper file

Description:

A sensitive file was identified as accessible or available at:

URL: https://juice-shop.herokuapp.com/BitKeeper

Impact Level: Medium

Tool Used: OWASP ZAP

Potential Impact:

This may leak administrative, configuration, or credential information which can be leveraged by a malicious individual to further attack the system or conduct social engineering efforts.

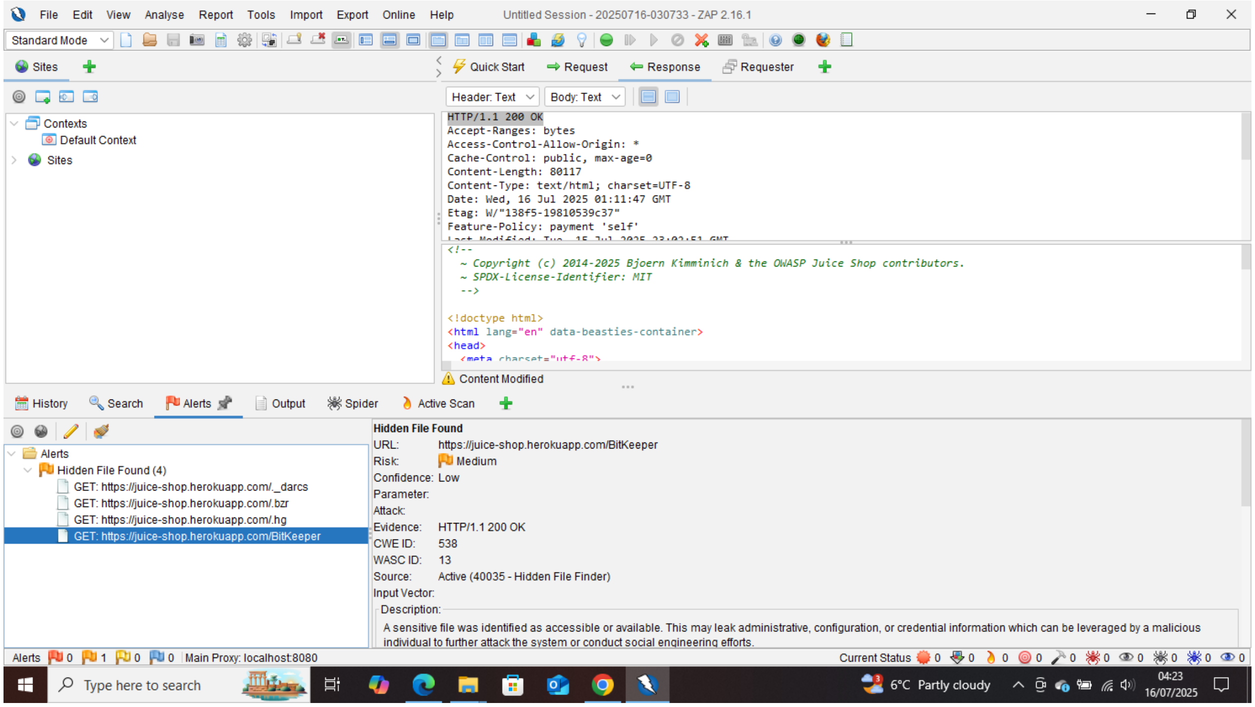
OWASP Mapping:

- OWASP_2021_A05
- OWASP_2017_A06

Remediation:

Consider whether the component is required in production or not, if it isn't then disable it. If it is then ensure access to it requires appropriate authentication and authorization, or limit exposure to internal systems or specific source IPs, etc.

Screenshot:



```
HTTP/1.1 200 OK
Accept-Ranges: bytes
Access-Control-Allow-Origin: *
Cache-Control: public, max-age=0
Content-Length: 80117
Content-Type: text/html; charset=UTF-8
Date: Wed, 16 Jul 2025 01:11:47 GMT
Etag: W/"138f5-19810539c37"
Feature-Policy: payment 'self'
```

```
<!--
  ~ Copyright (c) 2014-2025 Bjoern Kimminich & the OWASP Juice Shop contributors.
  ~ SPDX-License-Identifier: MIT
  -->

<!doctype html>
<html lang="en" data-beasties-container>
<head>
```

- Alerts
  - Hidden File Found (4)
    - GET: https://juice-shop.herokuapp.com/._darcs
    - GET: https://juice-shop.herokuapp.com/.bzr
    - GET: https://juice-shop.herokuapp.com/.hg
    - GET: https://juice-shop.herokuapp.com/BitKeeper

Hidden File Found

URL: https://juice-shop.herokuapp.com/BitKeeper
Risk: Medium
Confidence: Low
Parameter:
Attack:
Evidence: HTTP/1.1 200 OK
CWE ID: 538
WASC ID: 13
Source: Active (40035 - Hidden File Finder)
Input Vector:
Description:
A sensitive file was identified as accessible or available. This may leak administrative, configuration, or credential information which can be leveraged by a malicious individual to further attack the system or conduct social engineering efforts.

Conclusion:

This security assessment of OWASP Juice Shop identified multiple sensitive file disclosure vulnerabilities, highlighting common misconfigurations that can expose critical internal components to unauthorized users. Using OWASP ZAP, the vulnerabilities were detected, analyzed, and mapped to the OWASP Top 10 standards, with recommended remediation steps provided for each issue. This hands-on exercise enhanced practical skills in ethical hacking, vulnerability scanning, and secure coding awareness. Addressing these flaws is essential for maintaining a secure web application environment and preventing potential exploitation in real-world scenarios.