

## Class Activity: Penetration Testing with OWASP ZAP on Juice Shop

### Objective:

Learn how to conduct both automated and manual security tests using OWASP ZAP to identify and exploit vulnerabilities in a web application.

### Tools Needed:

- OWASP ZAP
- OWASP Juice Shop (deployed locally or accessible via a web server)

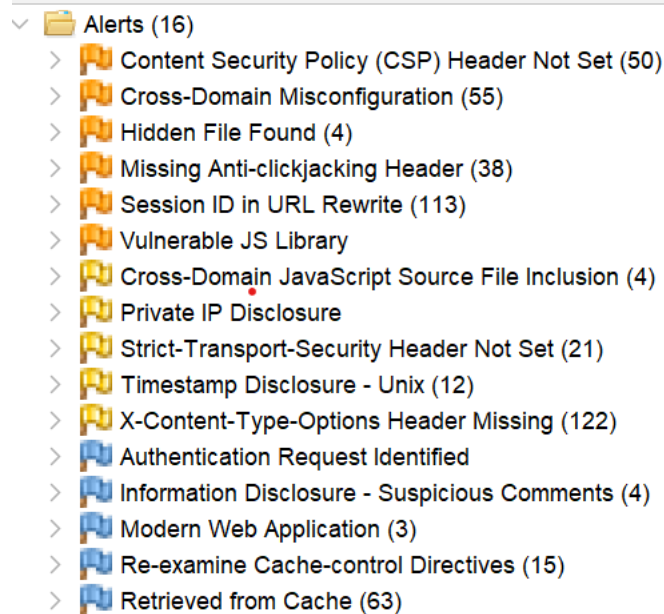
### Instructions:

#### 1. Automated Scan

1. **Goal:** Automatically scan the Juice Shop application to identify potential vulnerabilities.

#### 2. Tasks:

1. Launch OWASP ZAP.
2. Configure ZAP to point to the Juice Shop URL.
3. Initiate an automated scan and allow ZAP to crawl the application.
4. Document all identified vulnerabilities and alerts.



#### 2. Manual Exploration

1.**Goal:** Manually explore the application to find vulnerabilities that might not be detected by automated scans.

**2.Tasks:**

1.Manually navigate through the application using the ZAP proxy.

2.Try to identify any unusual behavior or potential security issues.

3.Use ZAP tools like the spider or active scanner to investigate specific parts of the application further.

**3. Save the Report**

1.**Goal:** Generate and save a report of the findings from the automated and manual testing.

**2.Tasks:**

1.Use ZAP's reporting feature to generate a detailed report of all findings.

2.Save the report in a chosen format (HTML, XML, etc.) for later review and analysis.

Hidden File Found	Medium	4 (25.0%)
-------------------	--------	--------------

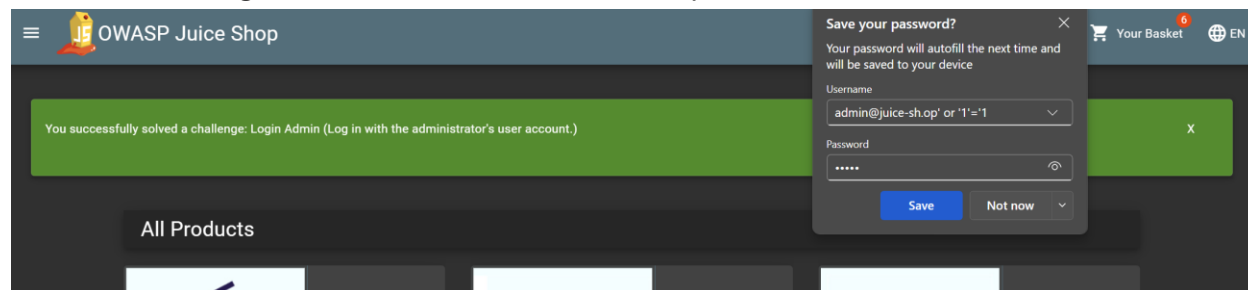
**4. Admin Password Crack**

1.**Goal:** Identify the admin's email address and attempt to crack the admin password.

**2.Tasks:**

1.Explore the application to find hints or functionalities that might reveal the admin's email address (e.g., forgotten password functionality, exposed emails on user profiles).

2.Once the email is found, use ZAP or other tools to attempt brute force or dictionary attacks on the login function to crack the admin's password.



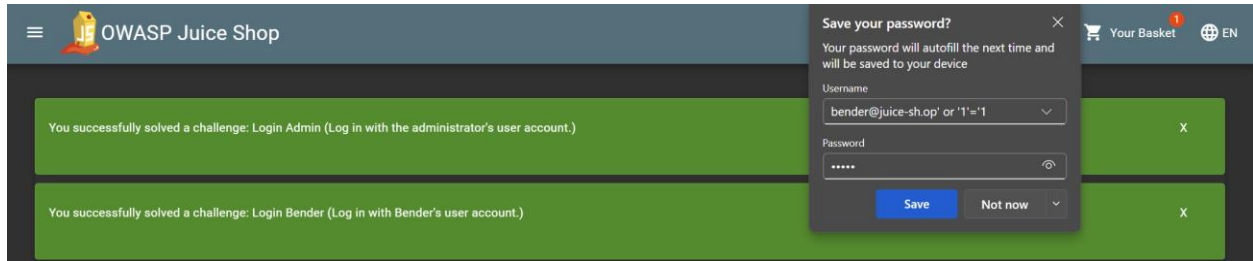
## 5. Log in to Bender's Account

1.**Goal:** Gain unauthorized access to Bender's user account.

### 2.Tasks:

1.Identify possible SQL injection points or insecure direct object references that allow access to Bender's account without authentication.

2.Document the method used and any vulnerabilities exploited.



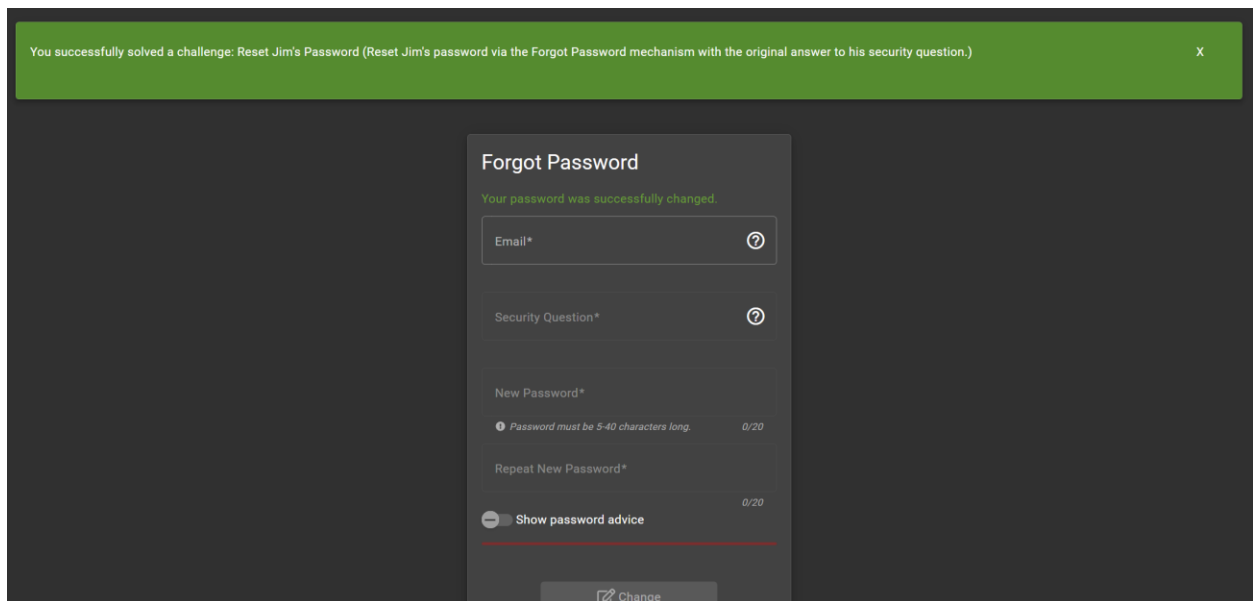
## 6. Reset Jim's Password

1.**Goal:** Demonstrate the ability to reset a user's password without authorization.

### 2.Tasks:

1.Exploit any vulnerabilities such as insecure reset password features or intercepting reset tokens using ZAP.

2.Successfully change Jim's password and document the steps.



Solution for this was too hard had to look it up.

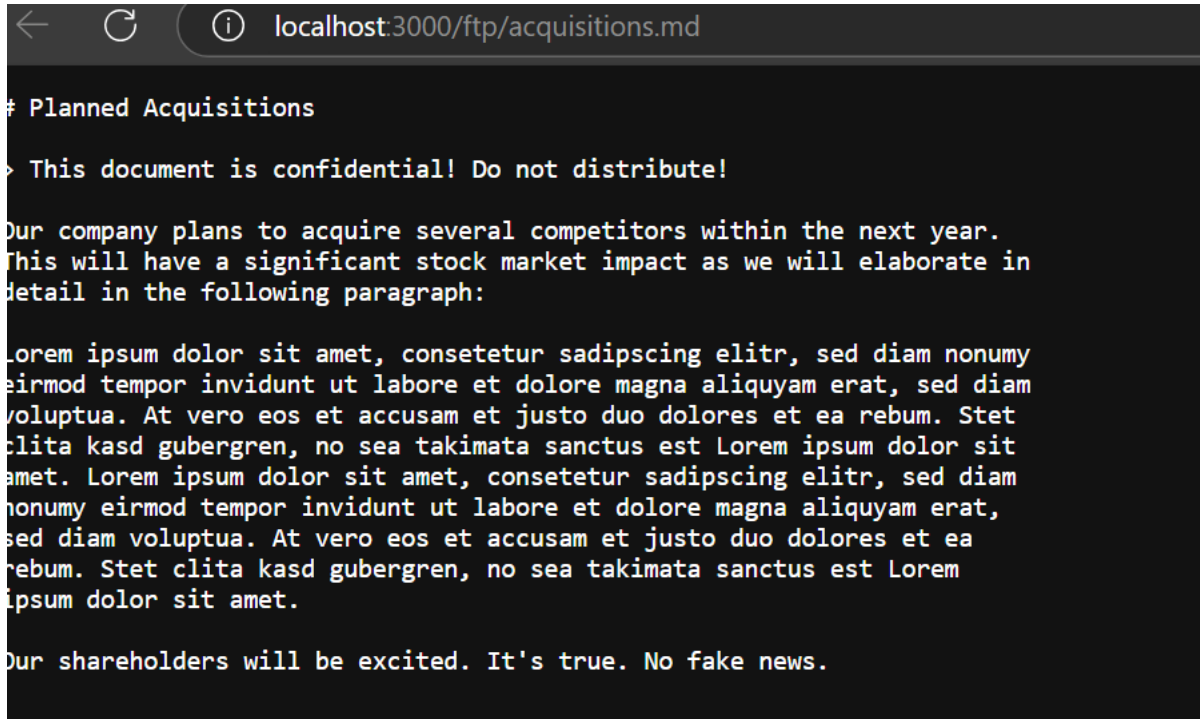
## 7. Access Confidential Document

1.**Goal:** Access a confidential document not intended for general user access.

### 2.Tasks:

1.Identify and exploit vulnerabilities that allow document access, such as path traversal or access control flaws.

2.Access and report on the document.



```
← ↻ ⓘ localhost:3000/ftp/acquisitions.md

# Planned Acquisitions

> This document is confidential! Do not distribute!

Our company plans to acquire several competitors within the next year.
This will have a significant stock market impact as we will elaborate in
detail in the following paragraph:

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy
eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam
voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet
clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit
amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam
nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat,
sed diam voluptua. At vero eos et accusam et justo duo dolores et ea
rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem
ipsum dolor sit amet.

Our shareholders will be excited. It's true. No fake news.
```