| Juiceshop Walkthrough Diploma in CSF  Year 3 Apr 2022 (Semester 5) | Week 2 |
| --- | --- |
| Practical |
| Deluxe Fraud | |

**OBJECTIVES**

* To use BurpSuite and the debugger to manipulate the website
* OWASP vulnerabilities: Insecure Deserialization and Software and Data Integrity (A08:2017, A08:2021)

**Challenge – Deluxe Fraud**

* To obtain a deluxe membership without paying for it
* Deluxe Fraud - Difficulty: 3/6 stars

**Step 1**

In the OWASP Juice Shop homepage, click on the side menu (Hamburger icon). In the side menu, access the deluxe membership page by clicking on the “Deluxe Membership”. On the membership page, click on “Become a member”.

Graphical user interface, application, website, Teams

Description automatically generated

Graphical user interface, website

Description automatically generated

**Step 2**

You should be brought to the payment page for the deluxe membership as shown in the screenshot. Right-click the page and click on “Inspect Element”.

A screenshot of a computer

Description automatically generated

**Step 3**

The HTML code for the payment page will be displayed. Navigate your way through the HTML code to find the <app-payment> tag that is highlighted in the screenshot. Expand the tag once it is found.

Graphical user interface, text, application, website

Description automatically generated

**Step 4**

Expand the code highlighted in the screenshot.

A screenshot of a computer

Description automatically generated

**Step 5**

Expand the code highlighted.

Graphical user interface, text, application, website

Description automatically generated

**Step 6**

Expand the highlighted code.

Graphical user interface, text, application, website

Description automatically generated

**Step 7**

Expand the last <div> tag in the expanded code of Step 6, and you should be able to see a <button> tag.

Graphical user interface, text, application, website

Description automatically generated

**Step 8**

Double click on the <button> tag to edit its parameters. Delete “mat-button disabled” in its parameters.

Graphical user interface, text, website

Description automatically generated

Graphical user interface, application, website

Description automatically generated

**Step 9**

Double click the <button> tag again to edit it. Delete the “ disabled=”true” “ parameter in the tag.

Graphical user interface, text, website

Description automatically generated

Graphical user interface, text, website

Description automatically generated

**Step 10**

Open your BurpSuite. Create a new project with the default settings as shown in the screenshots.

Graphical user interface, text, application

Description automatically generated

Graphical user interface, application, Word

Description automatically generated

**Step 11**

Click on the “Proxy” Tab. Then, click on the “Intercept” tab. Ensure that the intercept is turned on as shown.

Graphical user interface, text, application, Word

Description automatically generated

**Step 12**

Return to your browser (in this case is the Firefox browser). Ensure that the browser network settings is using “Manual Proxy Configuration” with the following parameters shown in the screenshot. Click “Ok” once done.

Graphical user interface

Description automatically generated

**Step 13**

If you have noticed from Step 9, the “Pay” button is clickable even though the account’s balance is insufficient to pay for the deluxe membership. This is because we have deleted the disabled parameters in the <button> tag. Click on the “Pay” button.

Graphical user interface, text, website

Description automatically generated

**Step 14**

Switch back to your BurpSuite again, and you should be able to see that your pay request is intercepted by the BurpSuite.

Graphical user interface, text, application, email

Description automatically generated

**Step 15**

Right-click the page, and click on “Send to Repeater” as shown in the screenshot.

Graphical user interface, text, application, email

Description automatically generated

**Step 16**

Change the value of “paymentMode” from “wallet” to “paid” and click the “Go” button. You should receive a response from the server that has a success status. This indicates that you are able to pay for the membership without having sufficient funds. Challenge solved!

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text

Description automatically generated

**~ End of Challenge 1 ~**