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

**OBJECTIVES**

* To perform cryptographic identification and analysis on sensitive information
* To use Postman to manipulate the website.
* OWASP vulnerabilities: Sensitive Data Exposure and Cryptographic Failures (A03:2017, A02:2021)

**Challenge – Imaginary Challenge**

* To solve challenge #999 which does not exist
* Imaginary Challenge - Difficulty: 6/6 stars

**Step 1**

Check the cookies stored on the Juiceshop website.

Graphical user interface, text, application, email

Description automatically generated

**Step 2**

Identify continueCode and examine it.

Graphical user interface, text, application

Description automatically generated

**Step 3**

Since z85 encryption was used previously, try looking into hashids.

Graphical user interface, application

Description automatically generated

One important detail here is that hashids generates its IDs from integers. Since we are solving challenge #999, maybe the number 999 can be converted with hashids.

**Step 4**

Go into hashid’s demo code and analyse its contents

A screenshot of a computer

Description automatically generated with medium confidence

It takes an integer, runs it through its functions, and returns a hash of whatever length we choose. The important section of code, is the generator for the encoded output.

Text

Description automatically generated

While most of it does not appear necessary to change, the number ‘6’ appears to match the output’s length. Therefore, this number, when changed, should change the output’s length, and thus change the hash that is generated. As for what length the output should be, it only makes sense if it matches the ‘continueCode’ cookie’s length. Using a character counter, we can see that the cookie is 60 characters long.

Graphical user interface, application

Description automatically generated

**Step 5**

Therefore, change the length to 60, and the input integer to 999.

Text

Description automatically generated

Text

Description automatically generated

The final output is as seen below.

Graphical user interface, text, application

Description automatically generated

**Step 6**

Launch BurpSuite to override the current ‘continueCode’ cookie and scan the website.

Graphical user interface, text, application

Description automatically generated

**Step 7**

Search for ‘continuecode’ and analyse the results.

Graphical user interface, text, application

Description automatically generated

**Step 8**

Find ‘/rest/continue-code/apply’ URL and use ‘Postman’, to send a PUT request.

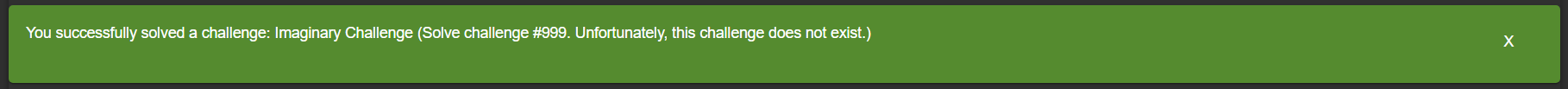
The request looks as follows.

Graphical user interface, text

Description automatically generated

**Step 9**

After doing so, the challenge is solved.



**~ End of Challenge ~**