|  |  |
| --- | --- |
| Juiceshop Walkthrough Diploma in CSF  Year 3 Apr 2022 (Semester 5) | Week 2 |
| Practical |
| Forged Signed JWT | |

**OBJECTIVES**

* To perform cryptographic identification and analysis on sensitive information
* OWASP vulnerabilities: Sensitive Data Exposure and Cryptographic Failures (A03:2017, A02:2021)

**Challenge – Forged Signed JWT**

* To forge an almost properly RSA-signed JWT token that impersonates the (non-existing) under rsa\_lord@juice-sh.op.
* Forged Signed JWT - Difficulty: 6/6 stars

**Step 1**

Launch Burpsuite and turn intercept off and sign into your account on Juiceshop.

Graphical user interface, application

Description automatically generated

**Step 2**

Locate this HTTP request that contains the JWT and send to repeater. Graphical user interface, application

Description automatically generated

**Step 3**

Copy the JWT.

Graphical user interface, text, application

Description automatically generated

**Step 4**

Paste the JWT inside.

Graphical user interface, text

Description automatically generated

**Step 5**

Change the algorithm from ‘RS256’ to ‘HS256’ and the email from your own email to ‘rsa\_lord@juice-sh.op’

Graphical user interface, text

Description automatically generated

**Step 6**

Locate the encryption files from Juiceshop by adding ‘encryptionkeys’ to the back of the home page URL.

Graphical user interface, application, Word

Description automatically generated

**Step 7**

Click on the jwt file and save to your computer.

Text

Description automatically generated

**Step 8**

Locate the file within your computer and open it with the ‘cat’ command to read its contents.

A screenshot of a computer

Description automatically generated with medium confidence

**Step 9**

Load <https://www.devglan.com/online-tools/hmac-sha256-online> and paste the entire content of the file into the secret key box. Copy the front section of the JWT into the plain text box as well.

Graphical user interface, text

Description automatically generated

**Step 10**

Select Base64 and compute the hash.

Graphical user interface, text, application

Description automatically generated

**Step 11**

Load <https://simplycalc.com/base64url-encode.php> and input the computed hash.

Graphical user interface, text, application

Description automatically generated

**Step 12**

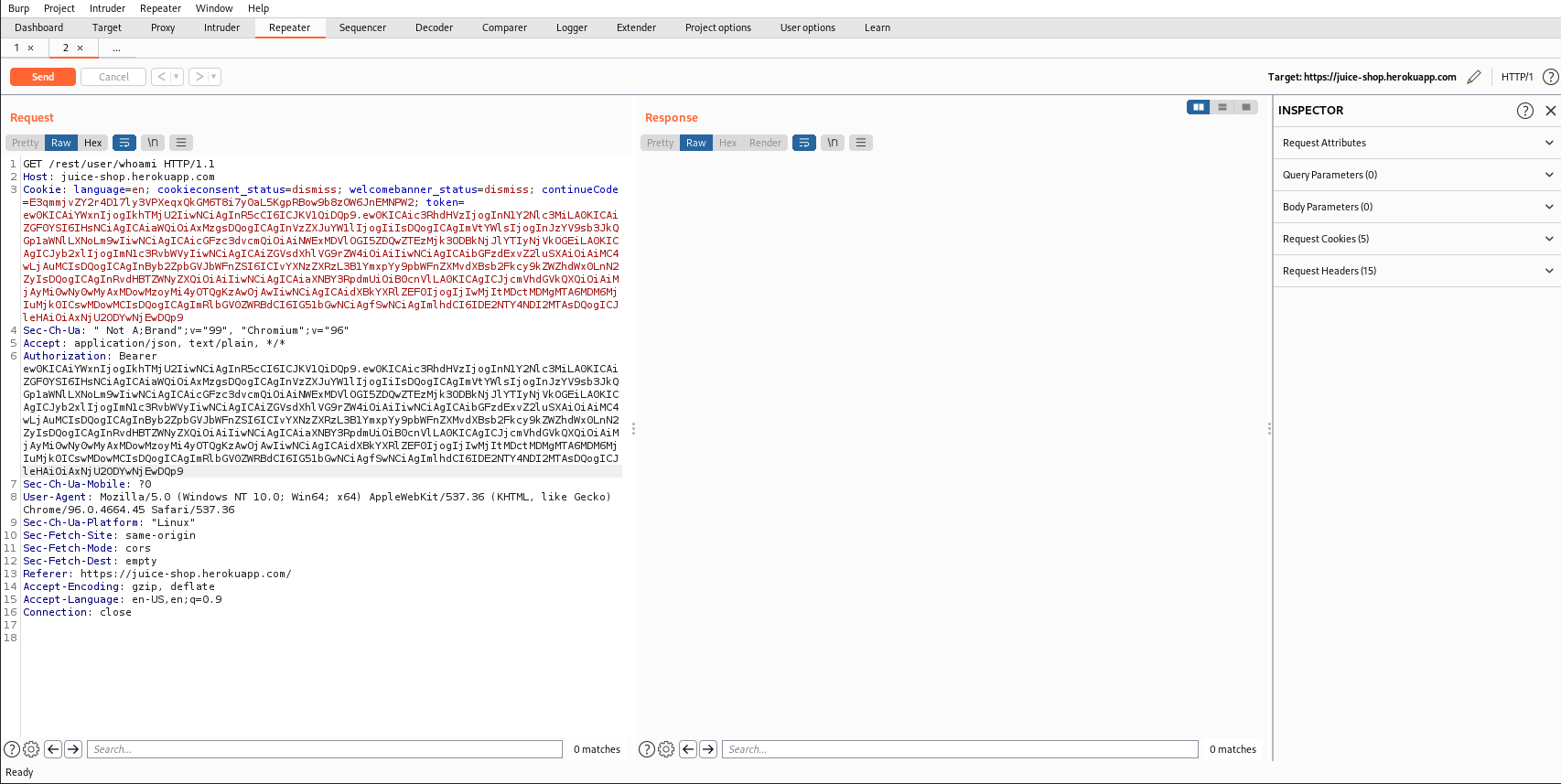
Replace the part after the full stop with the result as seen below.

Graphical user interface, text

Description automatically generated

**Step 13**

Copy the newly formed JWT and paste it into the bearer and token section in burpsuite and click send and the challenge should be completed.



**~ End of Challenge ~**