|  |  |
| --- | --- |
| Juiceshop Walkthrough Diploma in CSF  Year 3 Apr 2022 (Semester 5) | 4 Stars |
| Practical |
| Unsigned JWT | |

**OBJECTIVES**

* Learn and understand how token and unsign JWT works
* OWASP vulnerability: Using Components with Known Vulnerabilities,Vulnerable and Outdated Components (A09:2017) (A06:2021)

**Prerequisite**

* [www.jwt.io](http://www.jwt.io)
* [www.base64.guru](http://www.base64.guru)
* Burp Suite

**Challenge – Unsigned JWT**

* Forge an essentially unsigned JWT token that impersonates the non-existing user jwtn3d@juice-sh.op
* Unsigned JWT - Difficulty: 4/6 stars

JWT stands for JSON Web Token, and it is a proposed Internet standard for creating data with optional signature and/or encryption. That data is read in the form of JSON, hence the name.

**Step 1**

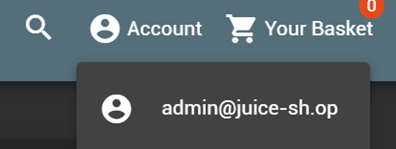
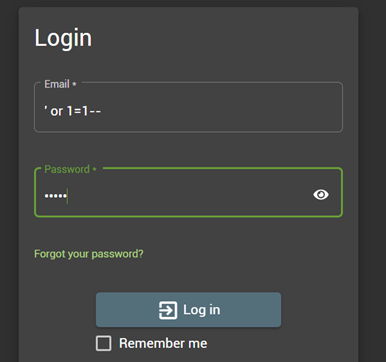
Open Burp Suite and set Intercept to “Off” under the Proxy tab. Click “Open browser” and head to your Juice Shop link

**Step 2**

This challenge involved the exploitation of a vulnerable component that JuiceShop uses for user authentication which are JWT tokens. A JWT token is made up of three components: header, payload and signature. The header consists of the type of the token (which is JWT) and the signing algorithm used (usually either RSA or HMAC SHA256). The payload is where information about the user is stored such as username, email and the token’s issue time and expiry time. The header and payload are then encoded in base64URL to make up two-thirds of the JWT token. The encoded header and payload are then encrypted with the key (public key if RSA, secret key if HMAC) to produce a digital signature. This signature is then base64url encoded and combined with the earlier encoded header and payload to produce a JWT token with a period separating them, hence in format header.payload.signature.

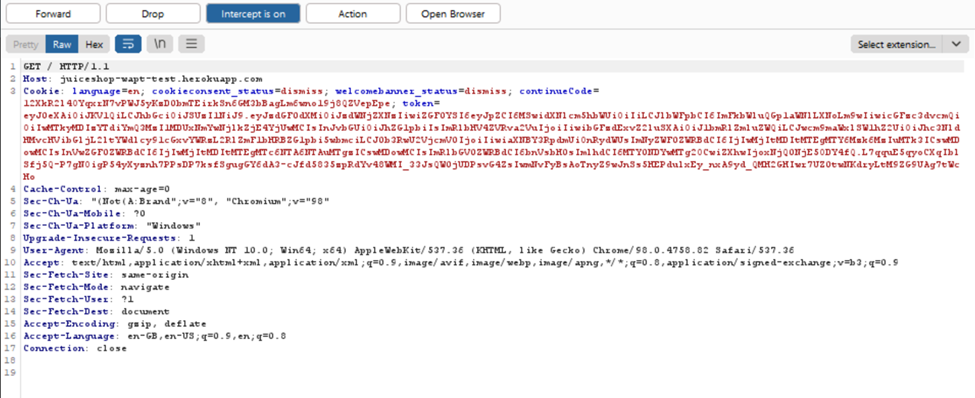
JWT tokens are generally secure, but there is one part about the option of the algorithm used in the header that if configured incorrectly makes it very vulnerable to attacks. JWT allows “none” to be used as a valid value for the algorithm type of the JWT token. Hence, no signing of the token is required. The token could simply be header.payload. and it would be a perfectly valid token to the server, even if the token was forged.

Hence, I carried out an unsigned forged JWT attack to demonstrate how a user that does not exist could be logged into JuiceShop. I first opened up BurpSuite and opened up JuiceShop in BurpSuite’s own proxy browser.



**Step 3**

I logged in as admin into the website using SQL Injection to obtain a valid JWT token.

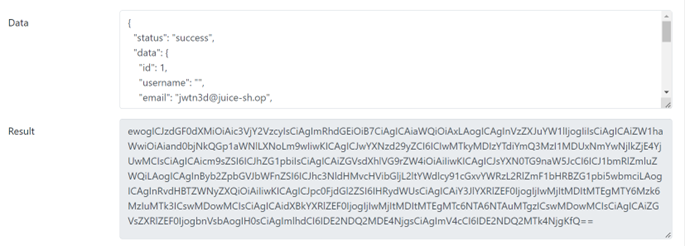
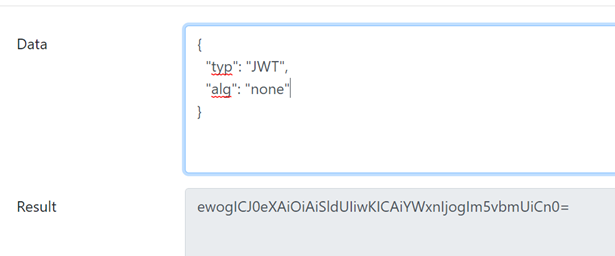
To obtain that JWT token, I went to the Proxy tab and turned on intercept. I then refreshed the JuiceShop page to analyze the requests by the browser in hopes of intercepting the request to retrieve the JWT token.

**Step 4**

The JWT token was stored in the token cookie and hence could easily be retrieved. I then copy pasted the token into a JWT decoder.

**Step 5**

From a glance, it is clear that the signing algorithm used by JuiceShop is RSA256. To forge an unsigned token, the algorithm has to first be changed to “none”. The email also has to be changed to “jwtn3d@juice-sh.op” as specified in the challenge details.



**Step 6**

The header and payload were then encoded in base64URL and combined together with a period at the end of each component, removing the ‘=’ signs as they are simply used for base64 padding.

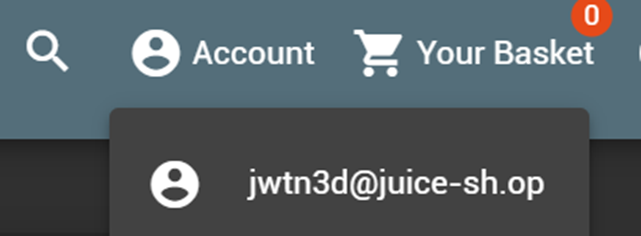
This was the resulting JWT token. The period at the end of the payload is to indicate that the signature field is empty.

**Step 7**

I then returned to BurpSuite to replace the current JWT token with my new forged token. After a few try and errors, I realized that the token had to be replaced for the requests that had the URL GET /rest/user/whoami HTTP/1.1 as that would indicate who the user is.

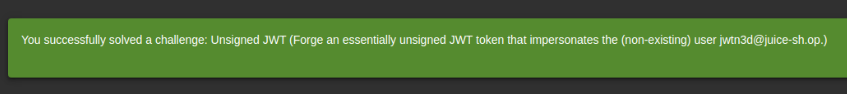
It is also worth mentioning that the token value is the one that affects who the user logged in is, and not the Authorization: Bearer request header.

**Step 8**

From this URL onwards, the new forged token was used instead of the old token. Intercept was then turned off to allow the page to finish loading on its own.

**Step 9**

The website was now using jwtn3d@juice-sh.op as the logged in user instead of the previous admin@juice-sh.op. Even after refreshing the page, the user remains the same, which indicates that the forged unsigned JWT token was a success.



**~ End of Challenge ~**