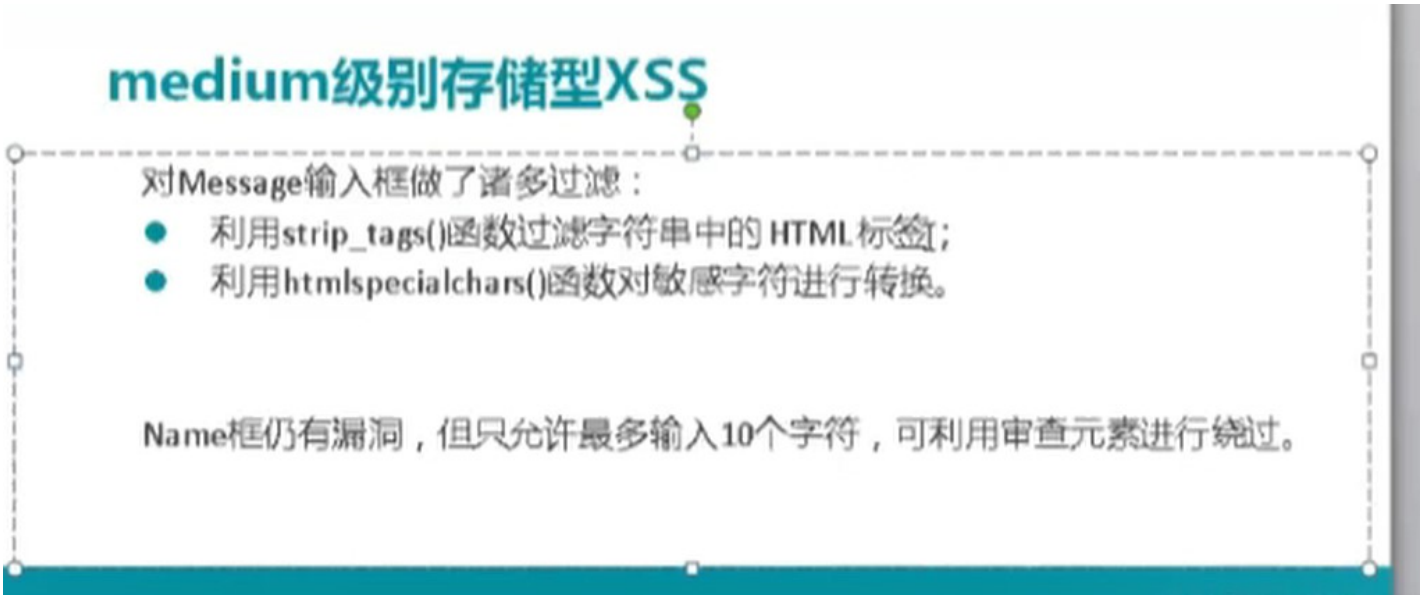
26-27主要讲了windows下面的网站搭建,这里只要讲28

存储型XSS

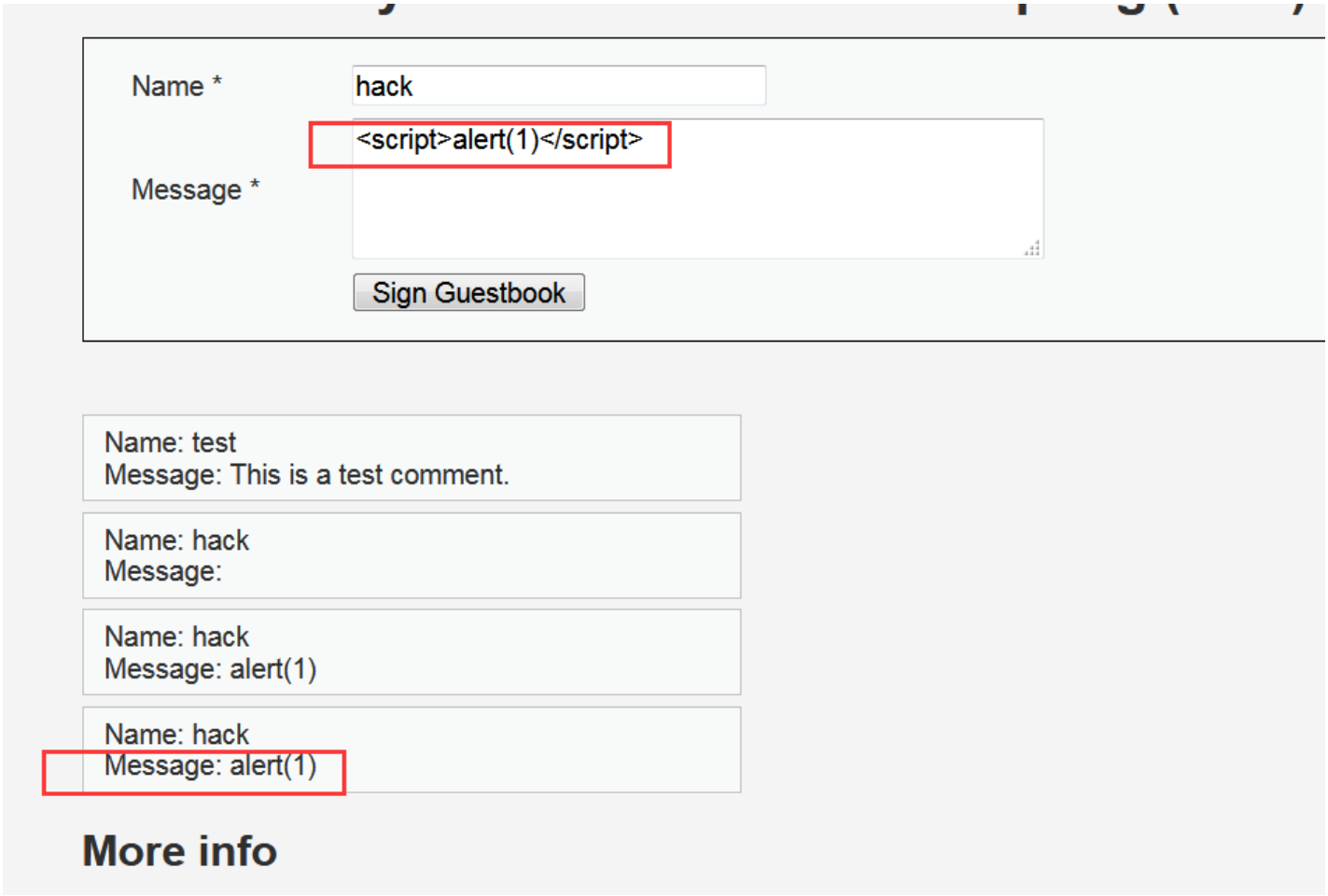
低级别源代码:

```php
 <?php

if(isset($_POST['btnSign']))
{

   $message = trim($_POST['mtxMessage']);
   $name    = trim($_POST['txtName']);    //trim是吧左右两侧的信息里面的空格给去掉!

   // Sanitize message input
   $message = stripslashes($message);
   $message = mysql_real_escape_string($message);//这个函数做转义!可以防止sql注入,对xss无

   // Sanitize name input
   $name = mysql_real_escape_string($name);

   $query = "INSERT INTO guestbook (comment,name) VALUES ('$message','$name');";

   $result = mysql_query($query) or die('<pre>' . mysql_error() . '</pre>' );

}

?>
```

Medium Stored XSS Source




```php
<?php

if(isset($_POST['btnSign']))
{

   $message = trim($_POST['mtxMessage']);
   $name    = trim($_POST['txtName']);

   // Sanitize message input
   $message = trim(strip_tags(addslashes($message)));//strip_tags：过滤字符串里面的标签，
   $message = mysql_real_escape_string($message);
   $message = htmlspecialchars($message);//用于防止跨站

   // Sanitize name input,name这一栏没有用htmlspecialchars这个函数!
   $name = str_replace('<script>', '', $name);//这里用绕过的话很简单,只要用大写即可:<SCRIPT
   $name = mysql_real_escape_string($name);

   $query = "INSERT INTO guestbook (comment,name) VALUES ('$message','$name');";

   $result = mysql_query($query) or die('<pre>' . mysql_error() . '</pre>' );

}

?>
```

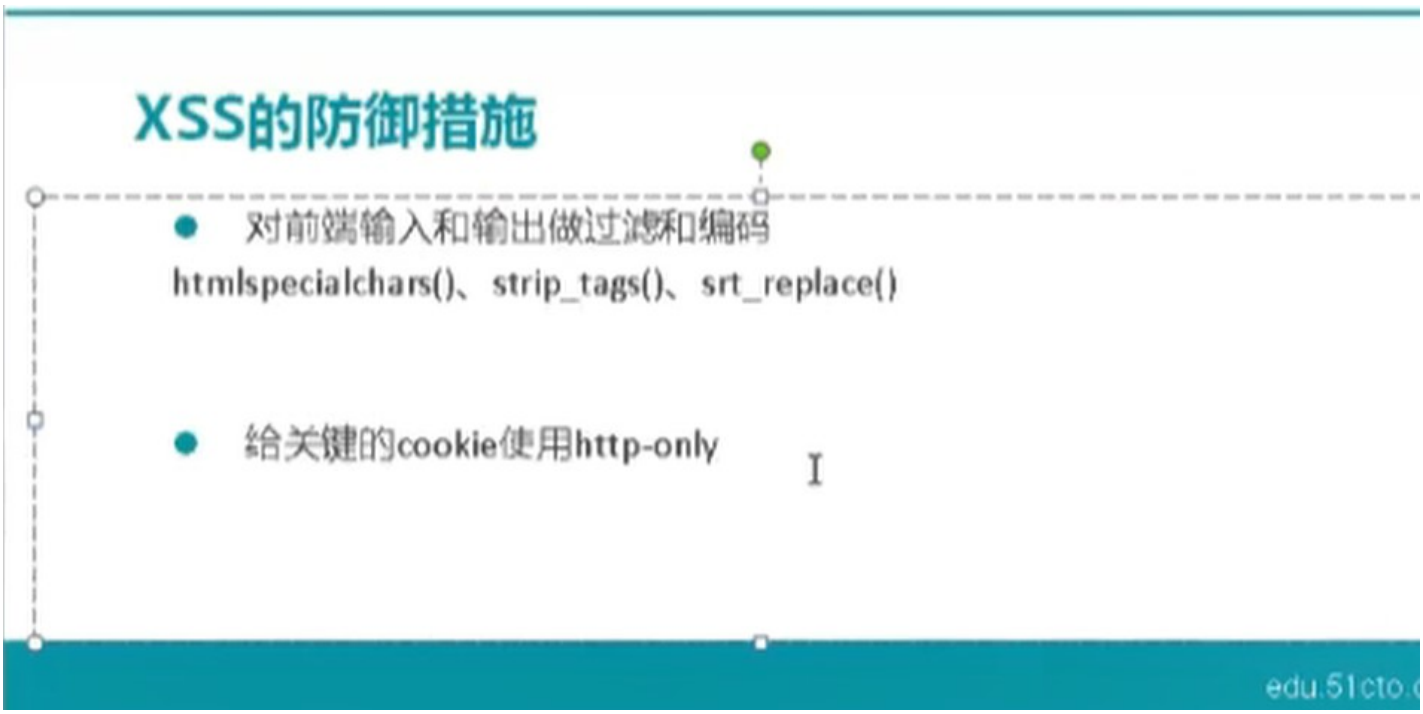


High Stored XSS Source

```php
<?php

if(isset($_POST['btnSign']))
{

   $message = trim($_POST['mtxMessage']);
   $name    = trim($_POST['txtName']);

   // Sanitize message input
   $message = stripslashes($message);
   $message = mysql_real_escape_string($message);
   $message = htmlspecialchars($message);//加了htmlspecialchars这个函数

   // Sanitize name input
   $name = stripslashes($name);
   $name = mysql_real_escape_string($name);
   $name = htmlspecialchars($name);//加了htmlspecialchars这个函数

   $query = "INSERT INTO guestbook (comment,name) VALUES ('$message','$name');";

   $result = mysql_query($query) or die('<pre>' . mysql_error() . '</pre>' );
```

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

防御



扫描工具

漏洞扫描工具

- safe3wvs

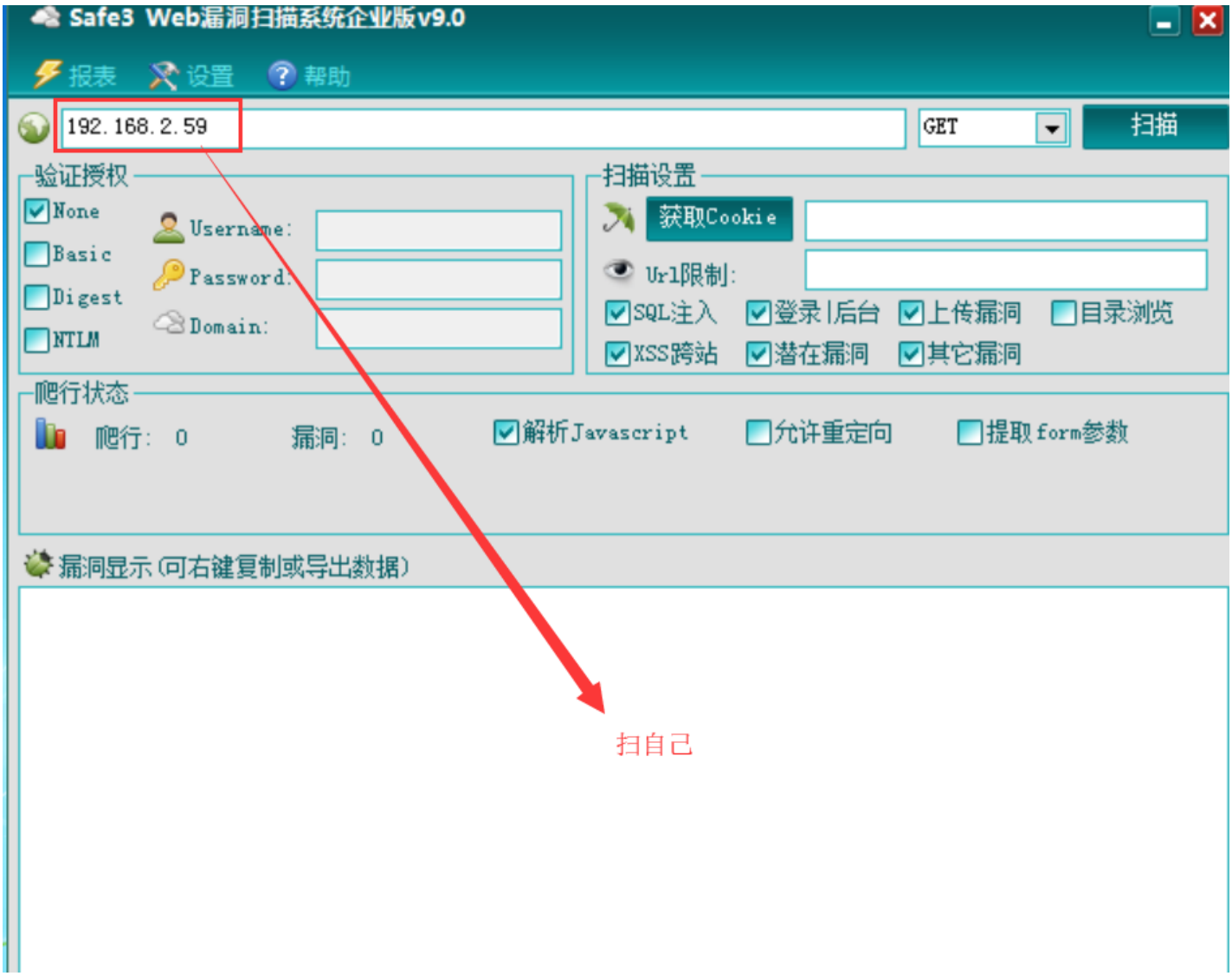
扫描速度比较快，需要安装.net 2.0

- 椰树I

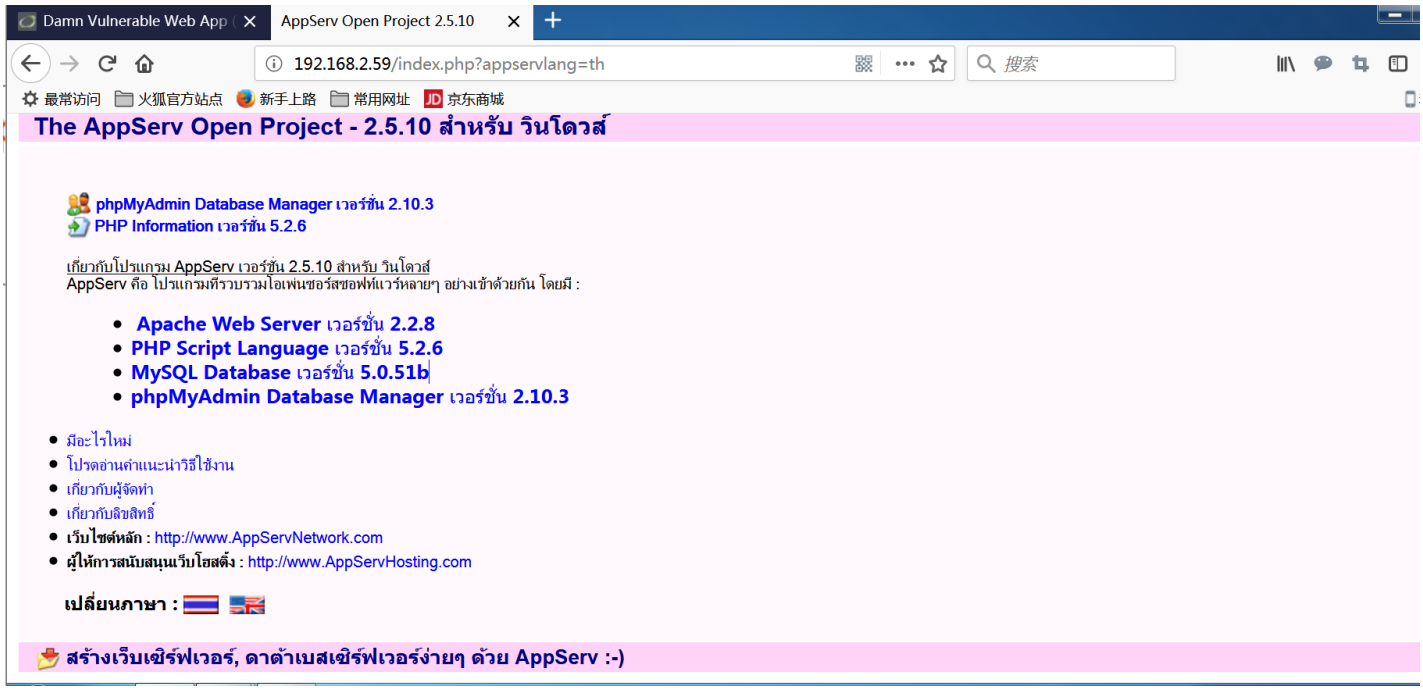
- BruteXSS

通过自带的字典文件对XSS漏洞进行暴力测试

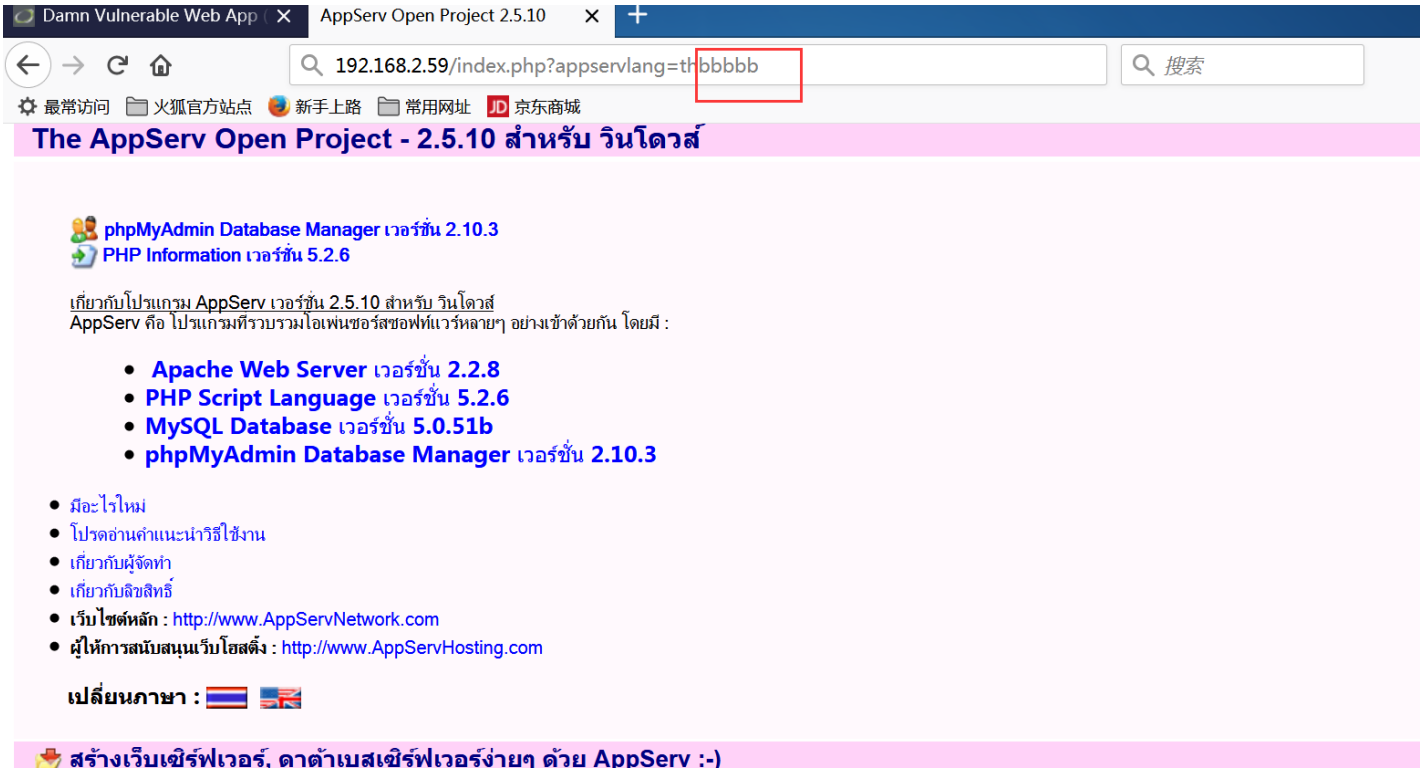
需要安装Python



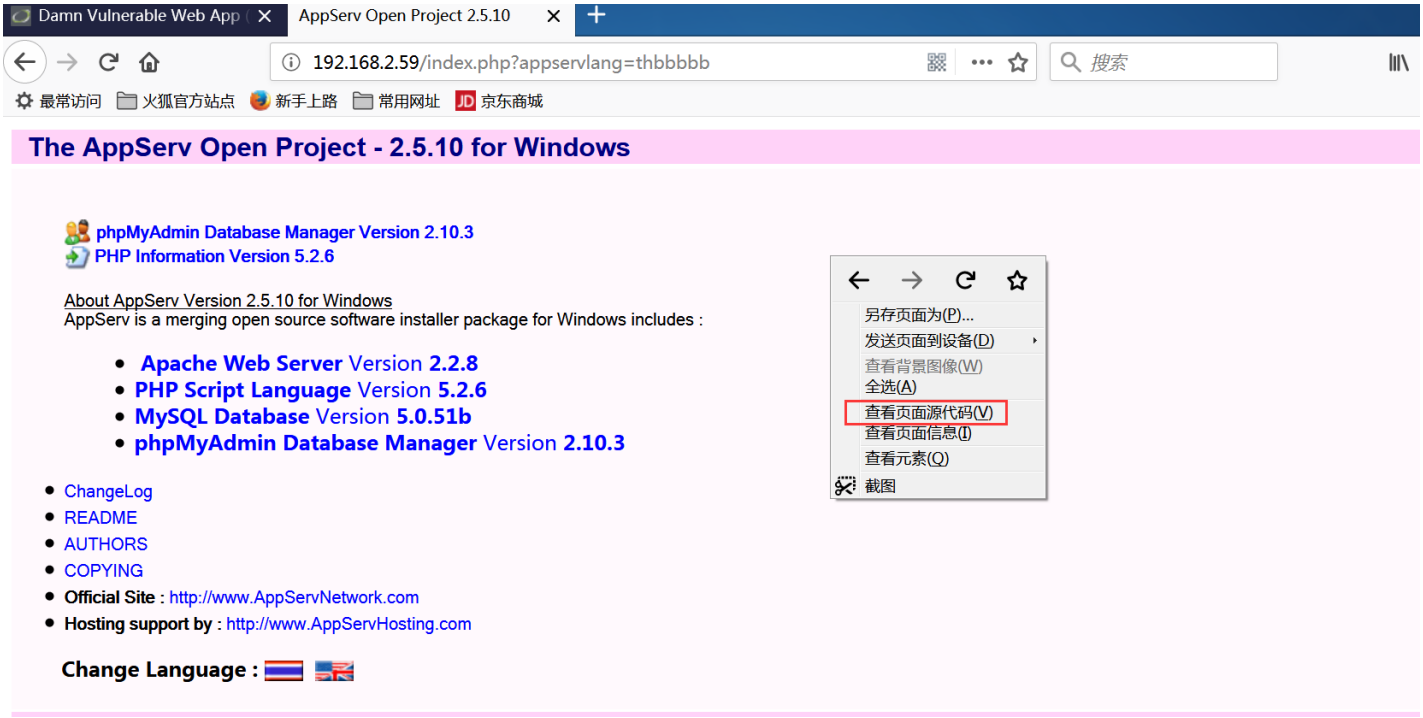
扫出这个页面有问题:



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-thbbbbb.php?appservlang=thbbbbb"><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://
    <li><span class="app"><b>Hosting support by :</b> <a href="http://www.AppServHosting.com/?appserv">htt
   </li> </ul>

p;      <b> Change Language : </b><a href="index.php?appservlang=th"><img src="appserv/flag-t
<br>
  </td>
```

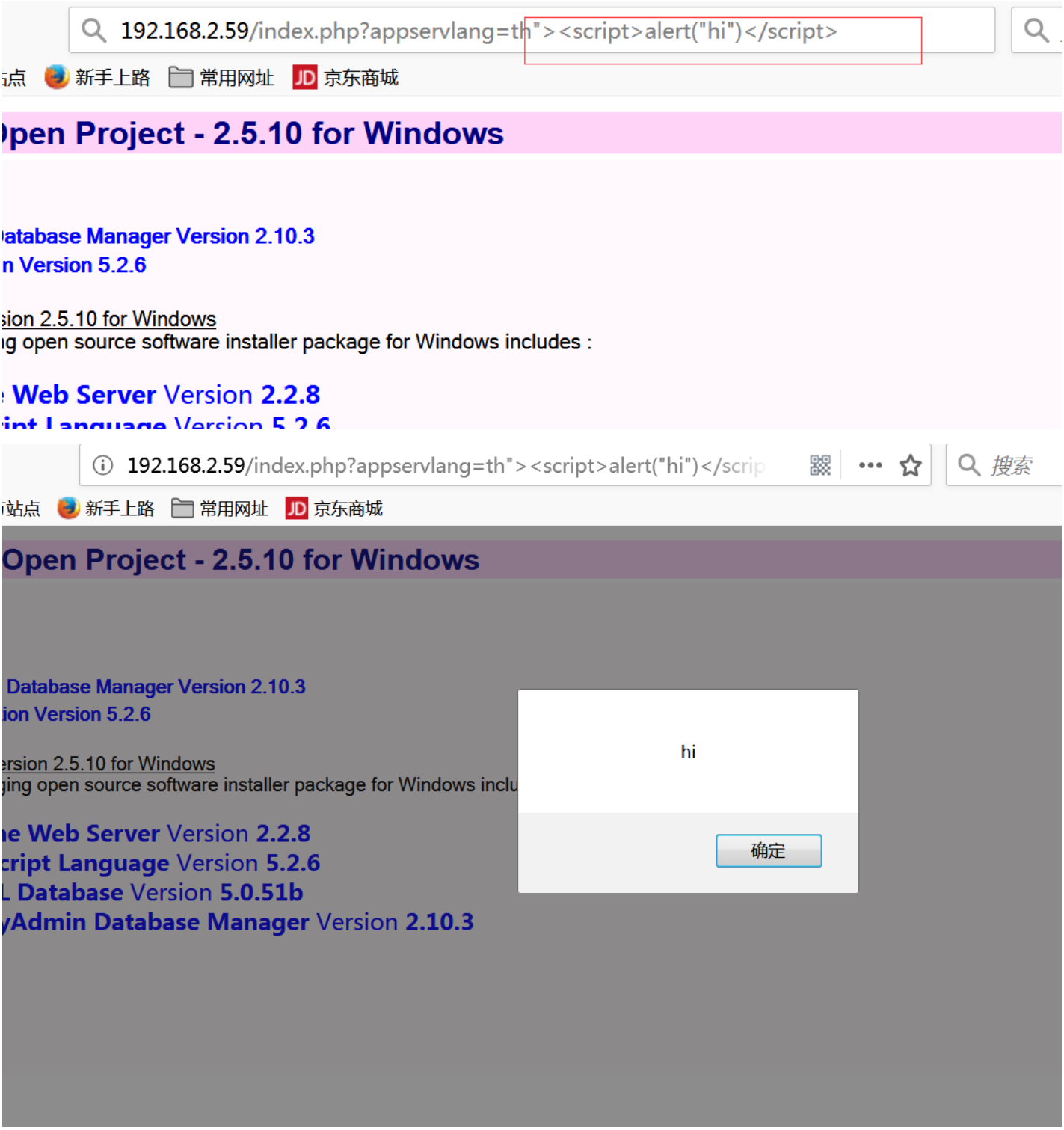
发现其放在一个标签属性里面！

构造跨站语句，首先考虑闭合问题；

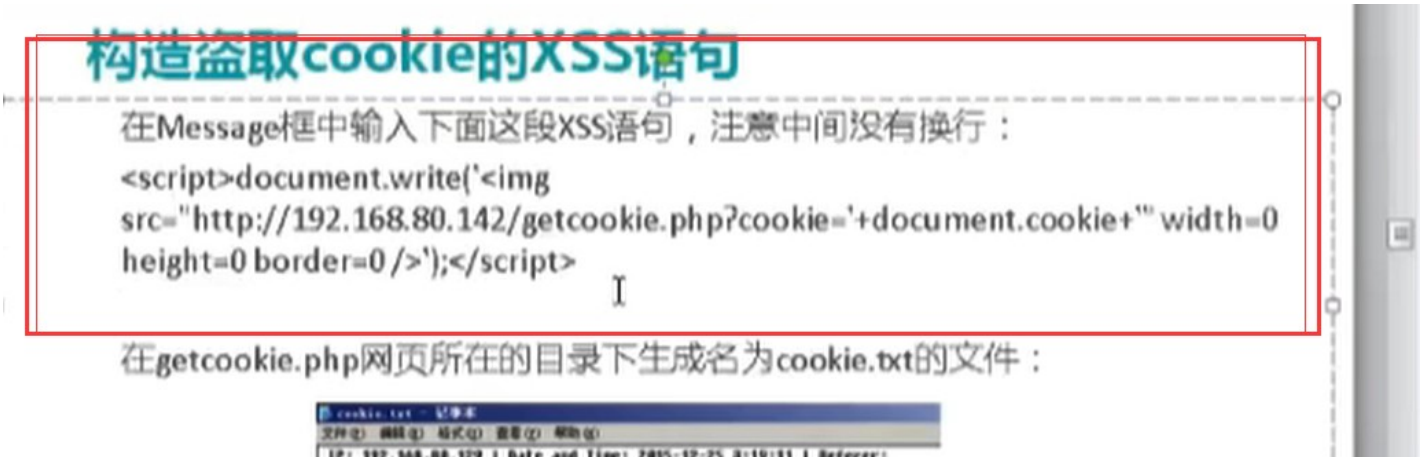
现加个引号,再加一个 > :

```
          </p>
        </blockquote>
        <ul>
          <li><a href="appserv/ChangeLog.txt"><span class="app">ChangeLog</span></a></li>
          <li> <a href="appserv/README-thbbbbb.php?appservlang=thbbbbb"><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>

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

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



这是一个典型的反射性 跨站!



这个语句很重要!

怎么利用盗取的cookie!可以自己研究研究!