

网站被黑 writeup

原创

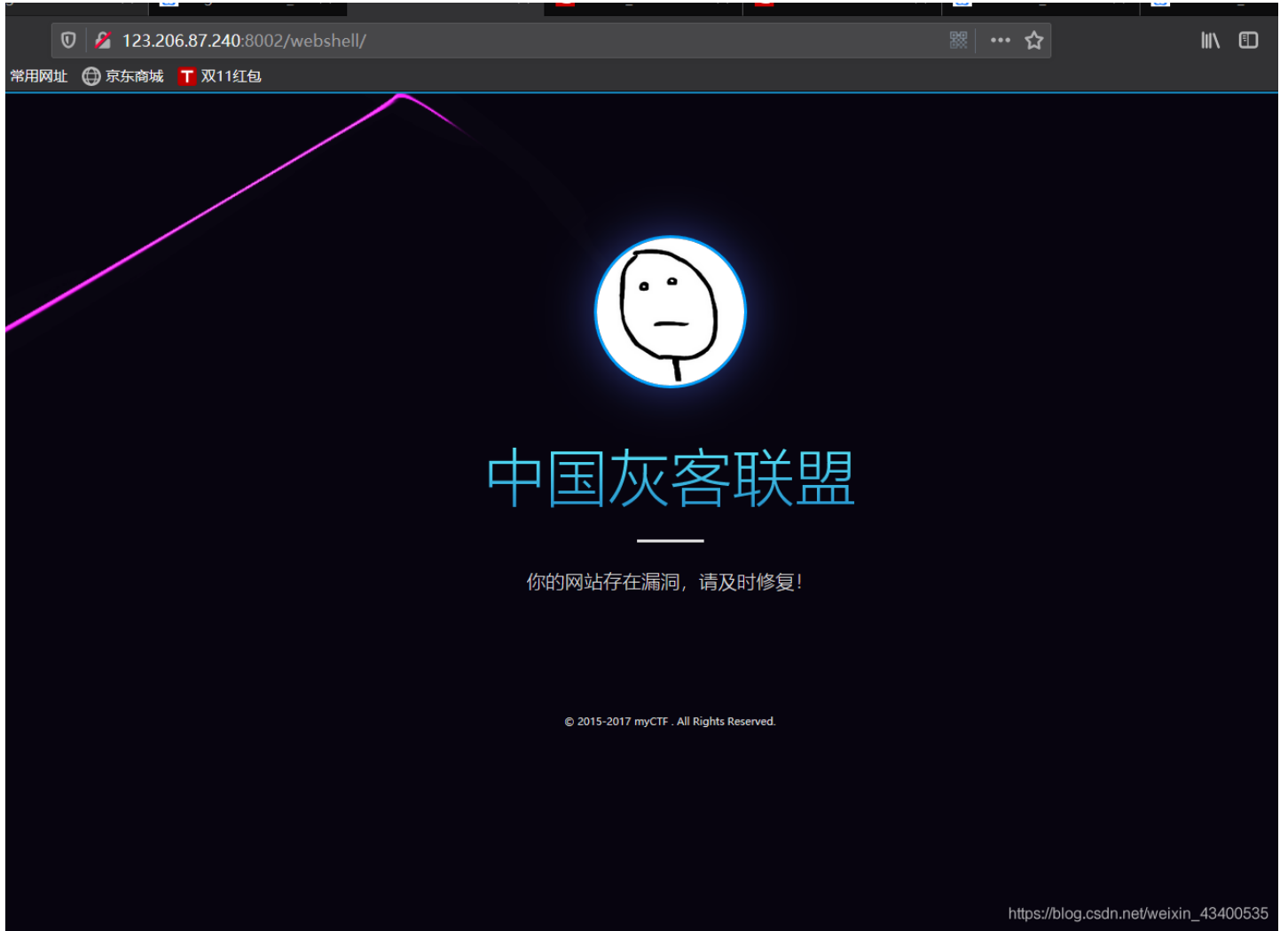
ctf小菜鸡 于 2020-02-12 21:01:03 发布 174 收藏

版权声明：本文为博主原创文章，遵循 [CC 4.0 BY-SA](#) 版权协议，转载请附上原文出处链接和本声明。

本文链接：https://blog.csdn.net/weixin_43400535/article/details/104286266

版权

13.网站被黑 writeup



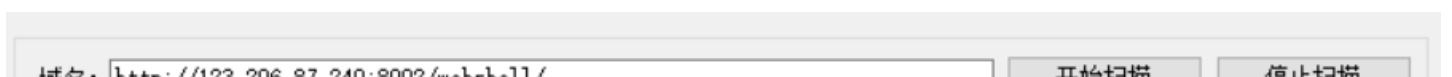
打开网址发现 网址上有个webshell 题目的名字也叫网页被黑。在这里就要提到一个知识，webshell

webshell就是以asp、php、jsp或者cgi等网页文件形式存在的一种命令执行环境，也可以将其称做为一种网页后门。黑客在入侵了一个网站后，通常会将asp或php后门文件与网站服务器WEB目录下正常的网页文件混在一起，然后就可以使用浏览器来访问asp或者php后门，得到一个命令执行环境，以达到控制网站服务器的目的。

顾名思义，“web”的含义是显然需要服务器开放web服务，“shell”的含义是取得对服务器某种程度上操作权限。

webshell常常被称为入侵者通过网站端口对网站服务器的某种程度上操作的权限。由于**webshell**其大多是以动态脚本的形式出现，也有人称之为网站的后门工具。

所以先用御剑扫描一下



域名: http://123.206.87.240:8002/webshell/

线程: 10 (条 CPU核心 * 5最佳) DIR: 1153 ASPX: 822 探测200
 超时: 1 (秒 超时的页面被丢弃) ASP: 1854 PHP: 1066 探测403
 MDB: 419 JSP: 631 探测3XX

扫描信息: 扫描完成... 扫描线程: 0 扫描速度: 0/秒

ID	地址	HTTP响应
1	http://123.206.87.240:8002/webshell/index.php	200
2	http://123.206.87.240:8002/webshell/shell.php	200

https://blog.csdn.net/weixin_43400535

这里扫描到了一个shell.php 我们打开看看

http://123.206.87.240:8002/webshell/shell.php

WebShell

WebShell

PASS:

https://blog.csdn.net/weixin_43400535

貌似是一个登录界面，用burpsuite看看，爆破一下：

Intruder attack 7

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
24	hack	200	<input type="checkbox"/>	<input type="checkbox"/>	1110	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	1125	
1	a1s2d3f4	200	<input type="checkbox"/>	<input type="checkbox"/>	1125	

2	rysj2012	200	<input type="checkbox"/>	<input type="checkbox"/>	1125
3	147.....	200	<input type="checkbox"/>	<input type="checkbox"/>	1125
4	258.....	200	<input type="checkbox"/>	<input type="checkbox"/>	1125
5	NI610B	200	<input type="checkbox"/>	<input type="checkbox"/>	1125
6	yyihacker	200	<input type="checkbox"/>	<input type="checkbox"/>	1125
7	cnsc	200	<input type="checkbox"/>	<input type="checkbox"/>	1125
8	LN 123456	200	<input type="checkbox"/>	<input type="checkbox"/>	1125

Options [Simple]

fhqyvi

lolita
XXM@52013
meizi
pw
woshinibaba
Enter a new item

st ...

https://blog.csdn.net/weixin_43400535

得到了hack 尝试一下

WebShell

PASS:

flag{hack_bug_ku035}

https://blog.csdn.net/weixin_43400535

ok了

flag{hack_bug_ku035}