广西首届网络安全选拔赛 WEB Writeup

原创

zrools 于 2016-02-03 18:15:35 发布 16612 收藏 19

分类专栏： CTF 文章标签： 网络安全 ctf web

本文链接：https://blog.csdn.net/zrools/article/details/50630755

WEB安全(WEB)

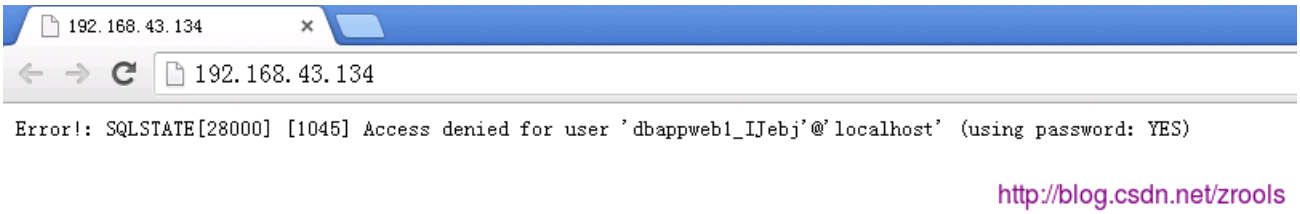
> WEB 题型就是最大众化的WEB漏洞的考察了，他会涉及到注入，代码执行，文件包含等常见的WEB漏洞。

管理员的愤怒

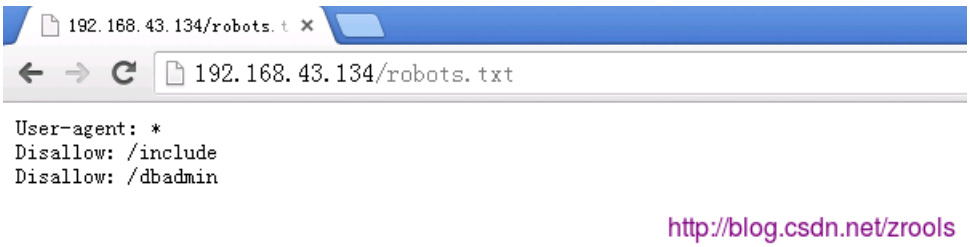
- 分值：100
- 靶机：192.168.43.134

阿水是某部门的网站管理员，一天他发现自己管理的网站被挂上了暗链，链接指向了一个IP。阿水非常愤怒，表示一定要给点对方颜色看看，但是这小子没学过渗透。下面给各位这个IP，看大家如何进入坏蛋的网站获得flag为阿水报仇。

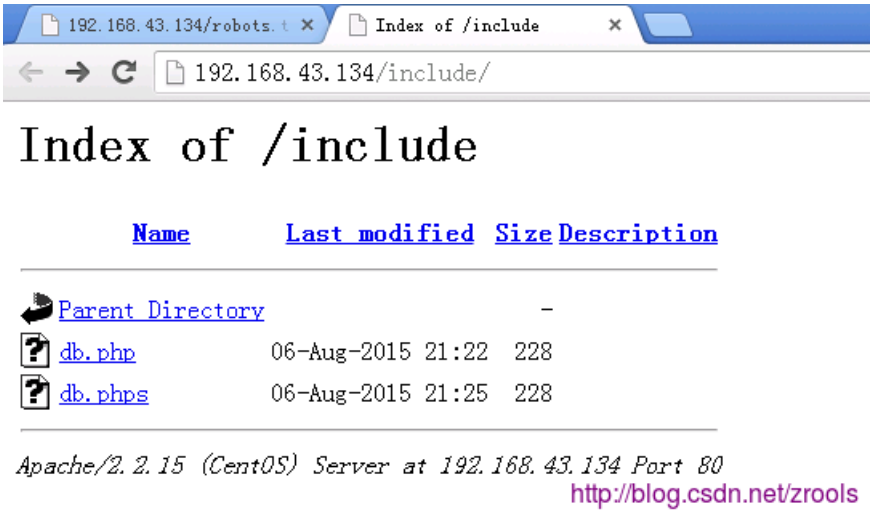
一打开是这样：



丢目录扫描发现`robots.txt`



`/include`下是有一个配置备份`db.phps`



`/dbadmin`下发现phpmyadmin以为是这货是切入点。。。密码错误，加强目录字典继续扫发现`img`有截图

点开最后一个得到答案

http://blog.csdn.net/zrools

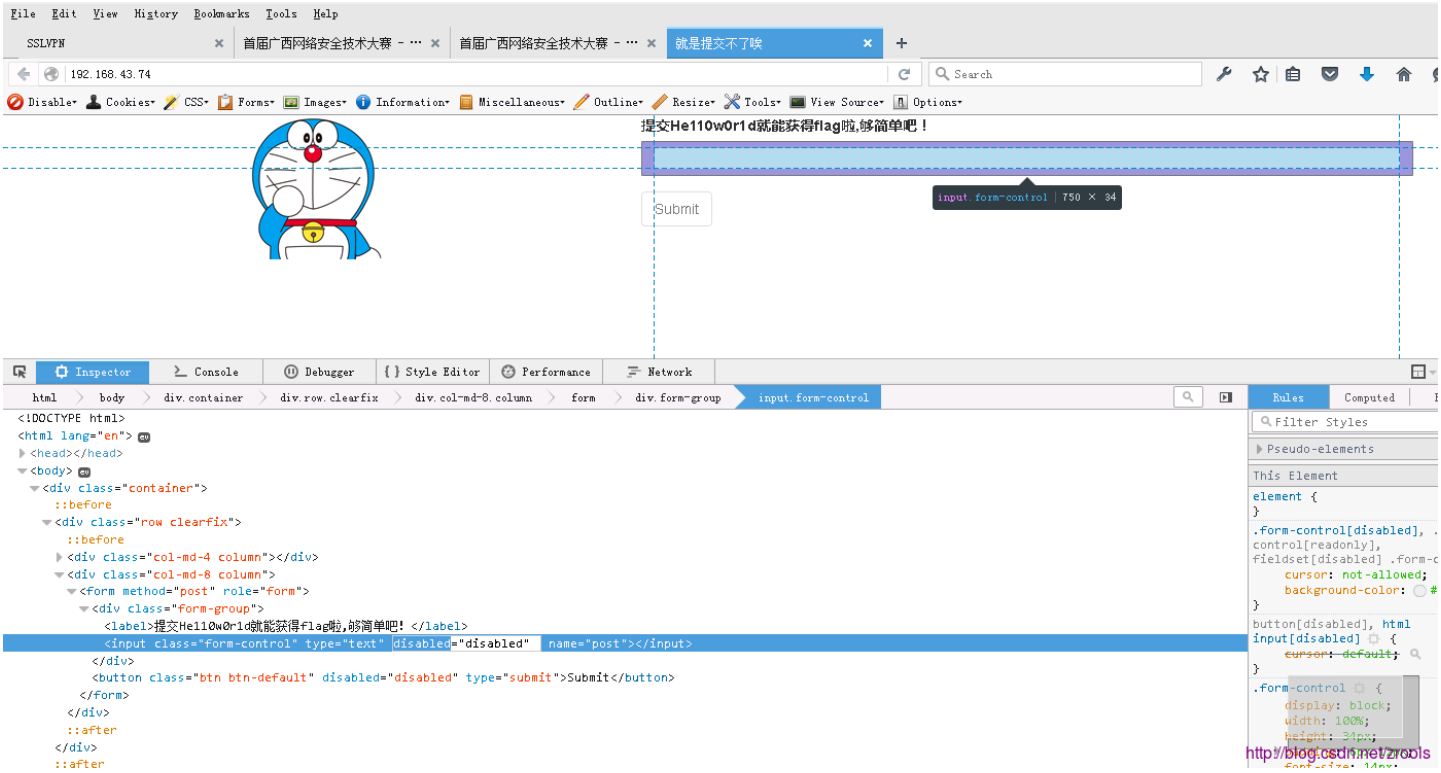
> flag:7e01c19b66330b121c90f6ebcafe8231

你就是提交不了

- 分值：100
- 靶机：192.168.43.74

管理员的技能非常强悍，你如果乱说话，就让你提交不了(答案为flag{}形式，提交{}中内容即可)

直接F12把`disable`属性干掉提交就能得到答案



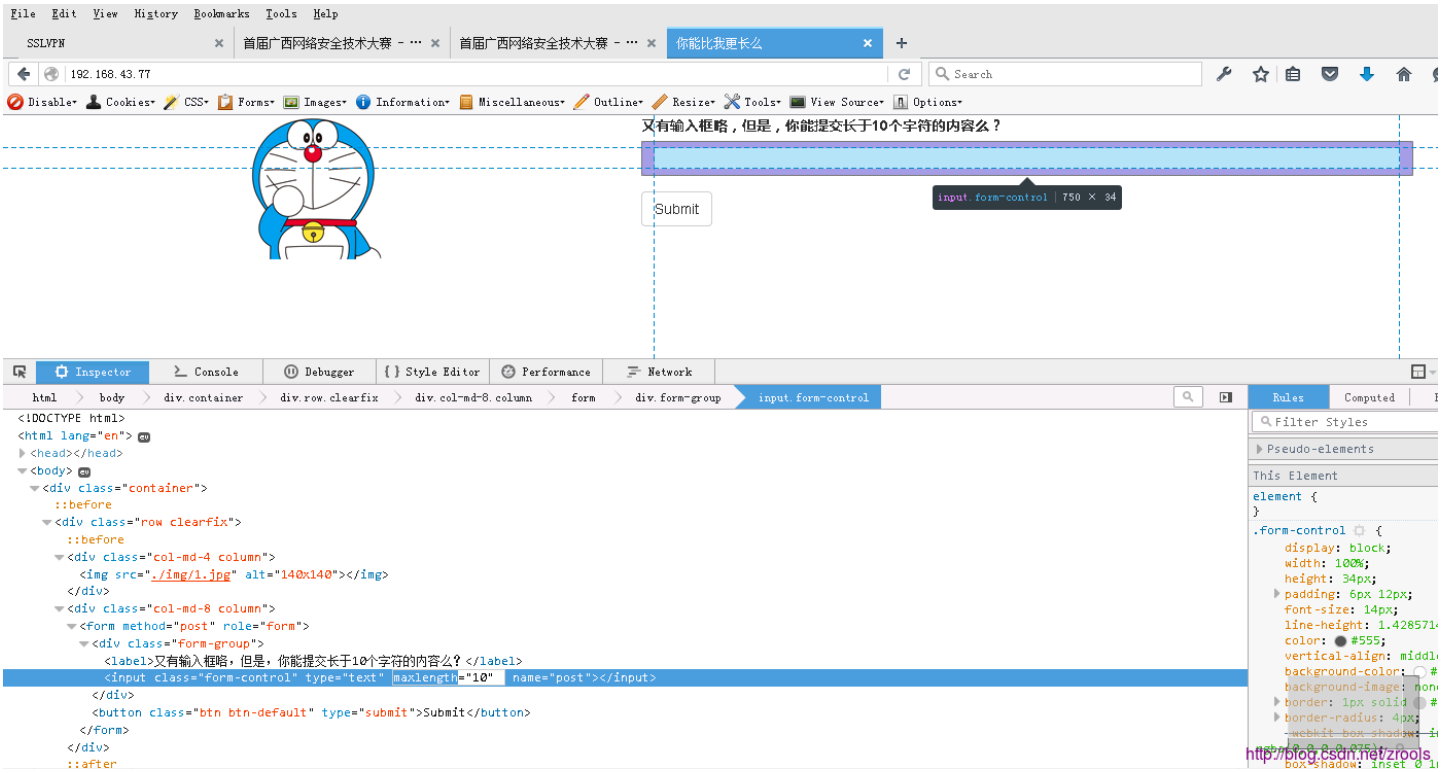
> flag:b0b237b92155c5ba0e0d90b1d01d8798

你就是长不了

- 分值：300
- 靶机：192.168.43.77

其实很多时候，你即使可以输入了，你也输入不长。但是，我们不服！怎么办呢？(答案为flag{}形式，提交{}中内容即可)

直接F12把`maxlength`属性干掉提交就能得到答案



> flag:88c48ff4b554eca6c7f961490aea8373

白云新闻搜索

- 分值：300
- 靶机：192.168.43.72

中国又出现了一个搜索巨头！据报道，中国网络大亨小明近日编写了一个搜索引擎，叫白云新闻搜索，具体链接在下方，该搜索链接功能欠打，界面乏力，小明出一包辣条悬赏漏洞，豪言入侵高手都去试试，你服不服？不服就去试试呗~(答案为flag{}形式，提交{}中内容即可)

扫了下目录没发现可疑点，直接丢sqlmap跑得出答案

```
python sqlmap.py -u "http://192.168.43.72/index.php" --data "word=1&number=5" --current-db

python sqlmap.py -u "http://192.168.43.72/index.php" --data "word=1&number=5" -D news --table

python sqlmap.py -u "http://192.168.43.72/index.php" --data "word=1&number=5" -D news --dump -T admin
```

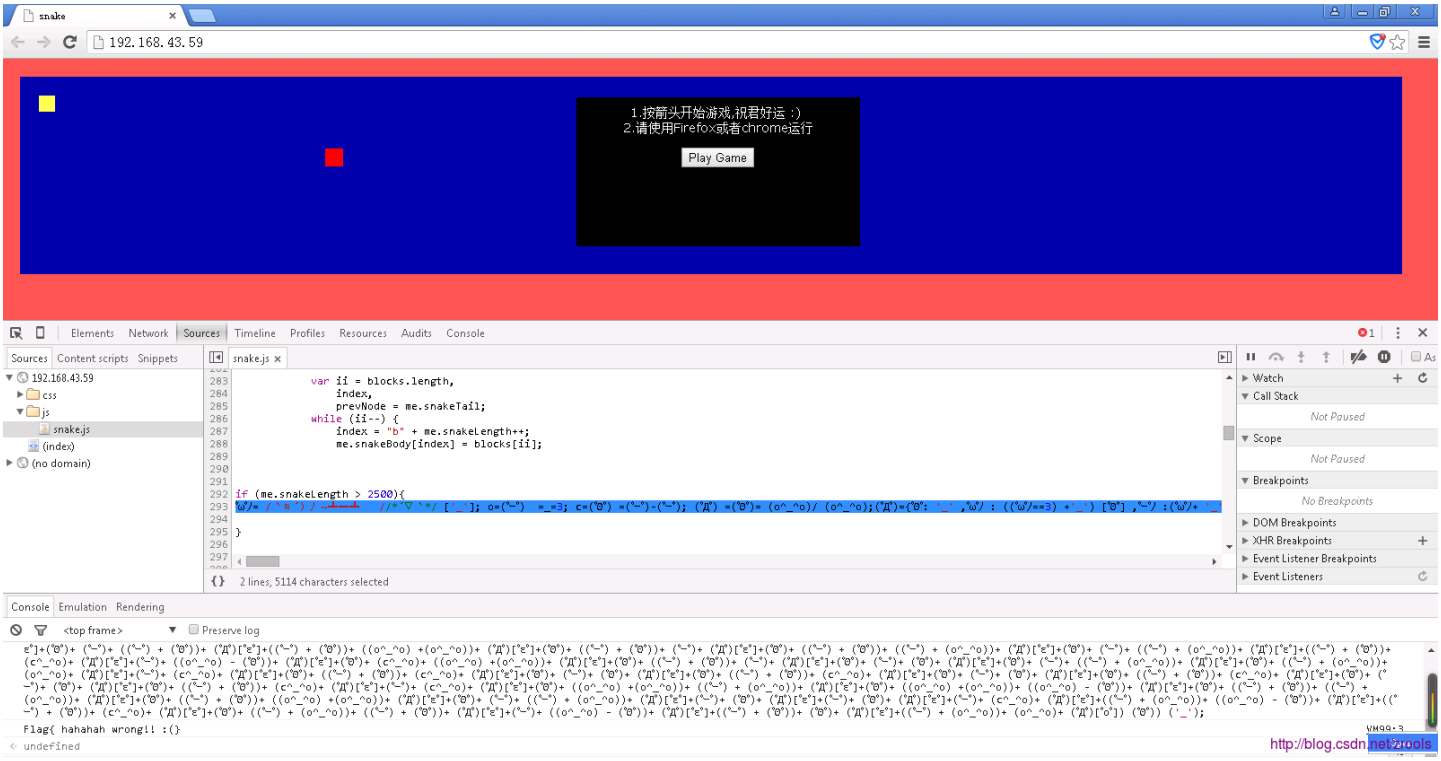
> flag:fabbf4abe040f2fdac8234099facdccb

贪食蛇

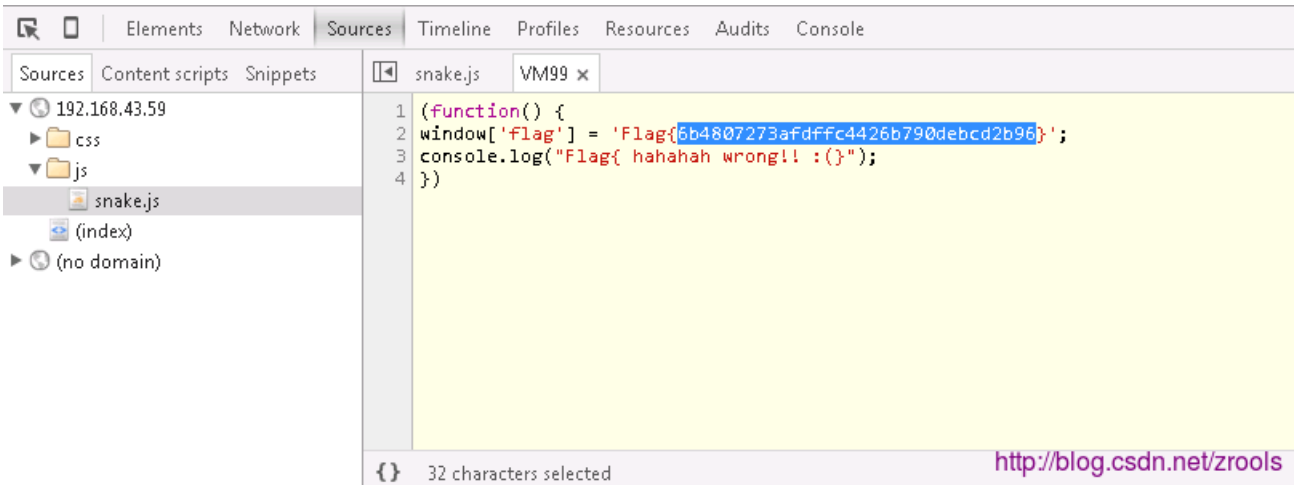
- 分值：210
- 靶机：192.168.43.59

贪吃蛇是经典手机游戏，既简单又耐玩！大家一定可以通关的！

源码有个`snake.js`大于2500是执行一段脚本，直接复制出来扔console执行



发现不对，直接点后面报错`Open`得到答案



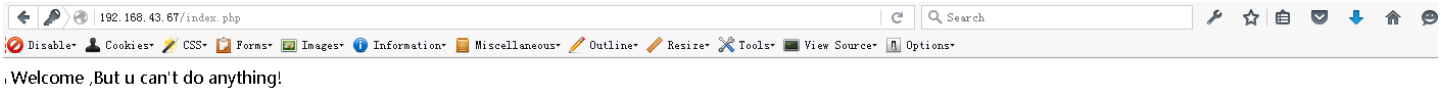
> flag:6b4807273afdffc4426b790debcd2b96

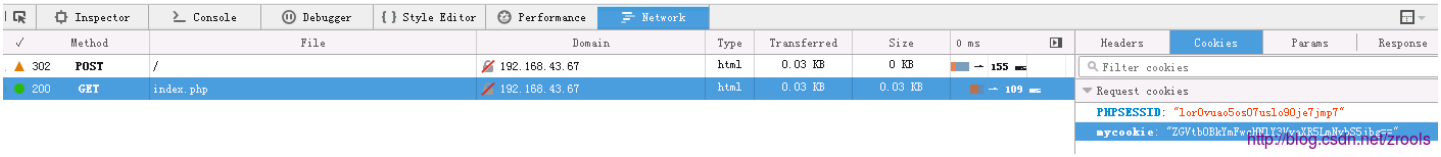
Easy Login

- 分值：200
- 靶机：192.168.43.67

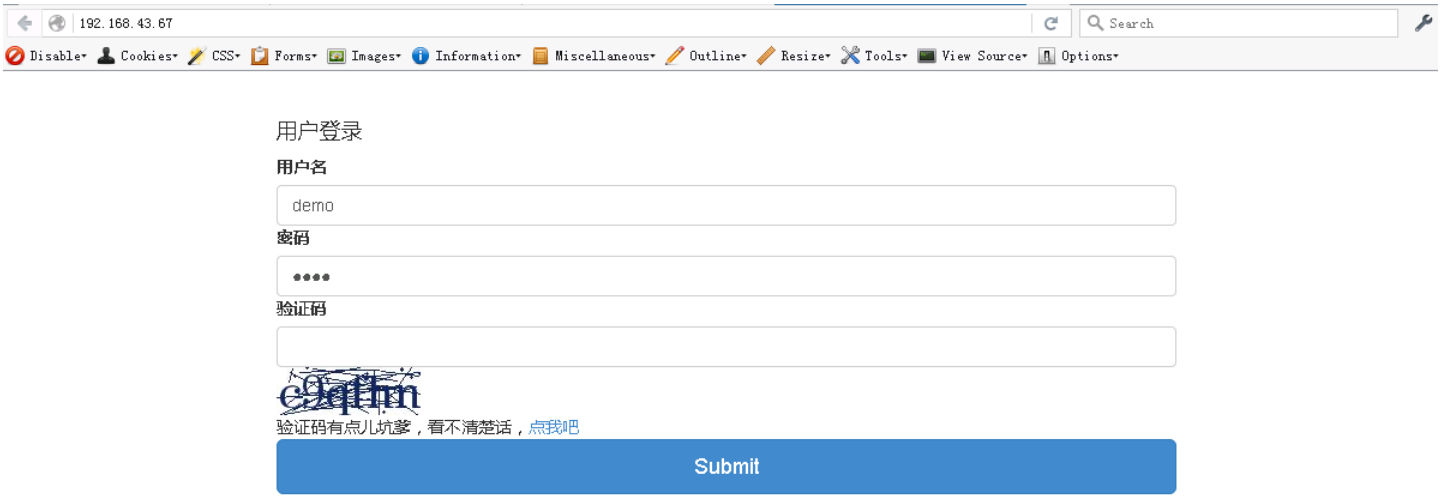
Easy Login…So Easy…

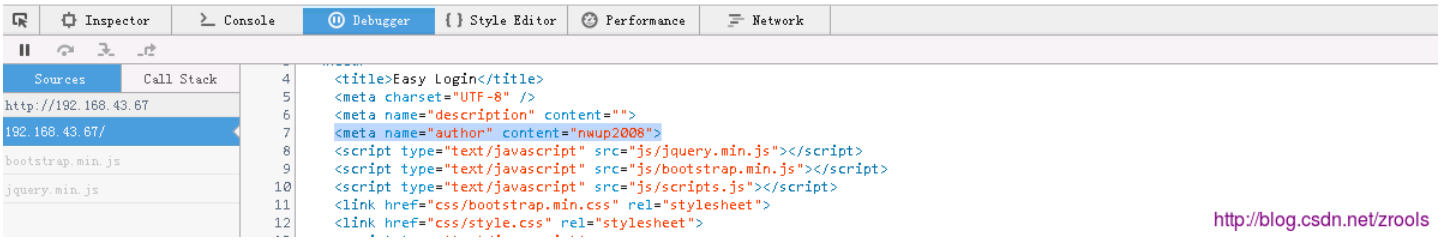
直接登录后什么都干不了



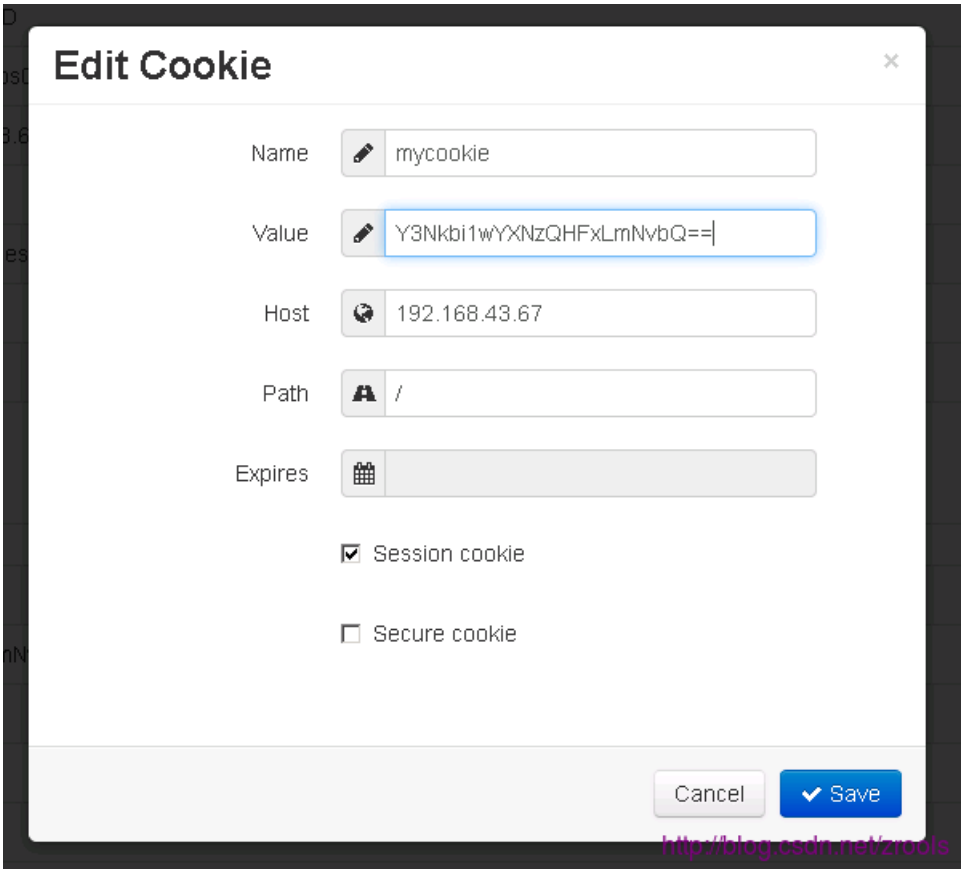


但发现`cookie`有点像base64编码，解密后是一个邮箱，但没什么用，清除`cookie`回到登录界面看源码，发现一个可疑字符串`nwup2008`





扔百度搜索无果，丢社工库查询得到邮箱`csdn-pass@qq.com`，base64加密修改`cookie`刷新得到答案



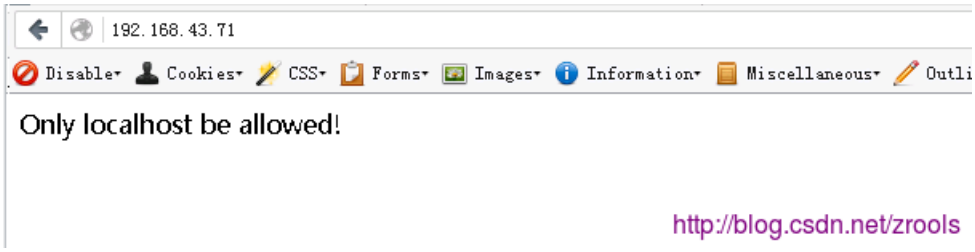
> flag:a327f27394c63ef5d6b1eed9591b90a4

Be Allowed?

- 分值：300
- 靶机：192.168.43.71

小黑终于闯进了内网，找到了目标Web主机，但是却被做了限制！

试过X-Forwarded-For、Referer、X-Real-IP无果，比赛结束无人解出不知考什么鬼。。。



> flag:

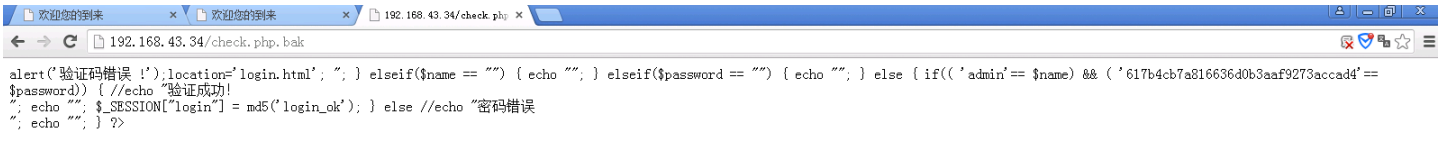
运维失误

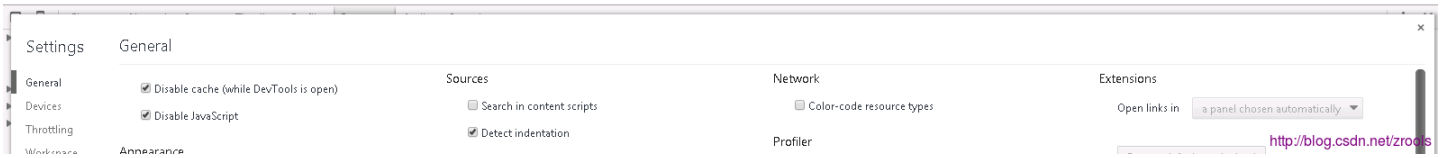
- 分值：250
- 靶机：192.168.43.34

公司的运维人员小王因为运维不当导致资料泄露，但粗心的他不知道问题出在哪里，你能帮小王找到问题的所在吗？

运维失误一般都是备份文件`.bak`什么鬼的，查看源码，

尝试`check.php.bak`有跳转，禁用`javascript`刷新





拿到验证密码，登录可得到答案

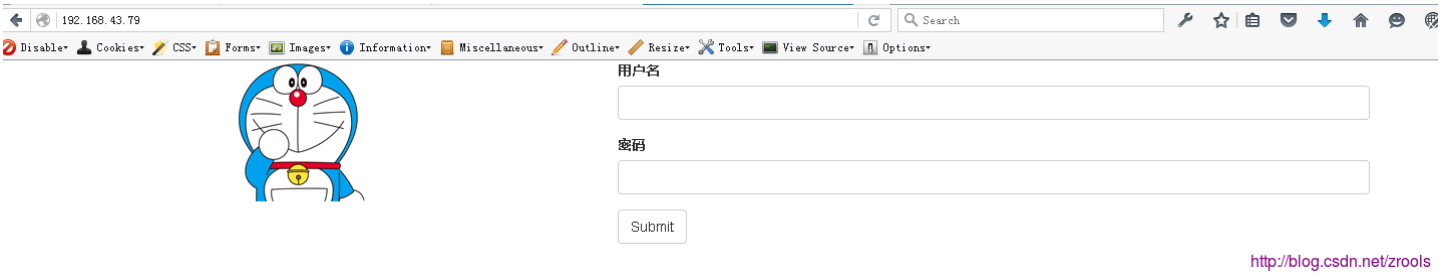
> flag:642fa4d74603f7d5303f7ee085ac2f95

admin123456

- 分值：300
- 靶机：192.168.43.79

入门级入侵，你以为就这样你就能得分了？太小看admin 了。(答案为flag{}形式，提交{}中内容即可)

就一个登录框

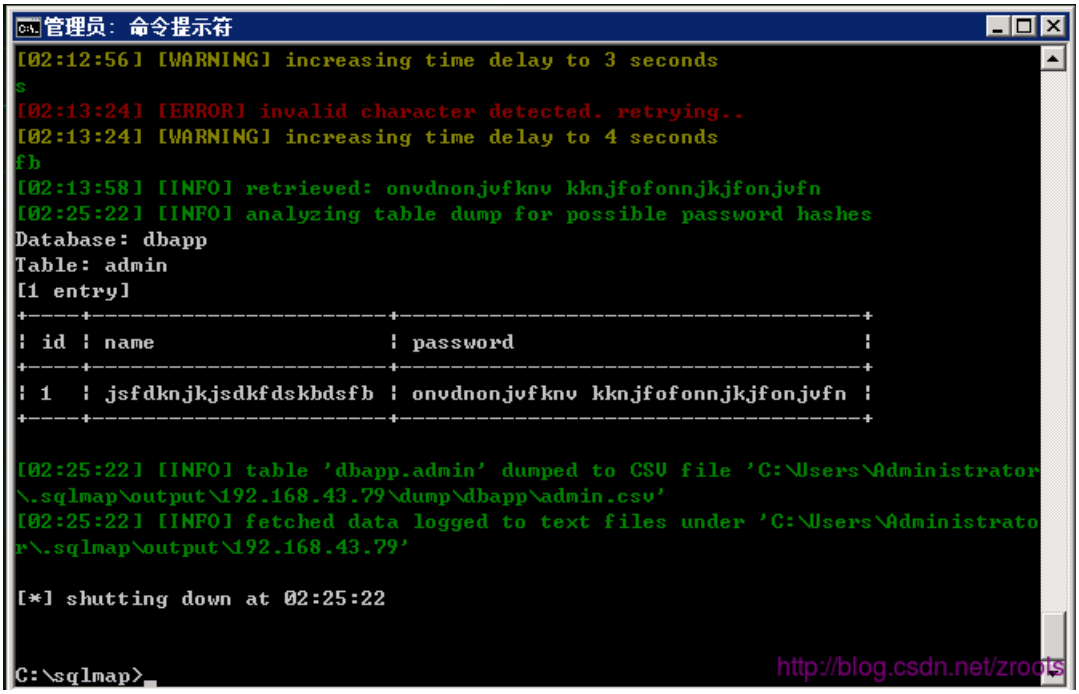


入门级，尝试TOP200用户/密码组合爆破无果，看看没验证码，扔sqlmap跑得到用户密码，登录得到答案

```
python sqlmap.py -u "http://192.168.43.79/index.php" --data "name=1&password=1" --current-db

python sqlmap.py -u "http://192.168.43.79/index.php" --data "name=1&password=1" -D dbapp --table

python sqlmap.py -u "http://192.168.43.79/index.php" --data "name=1&password=1" -D dbapp -T admin --dum
```



另外一种解法是屏蔽验证用万能登录`'or''='`

> flag:c406be9d45e34cdab33ad1e9673bc04c

刀塔

- 分值：300
- 靶机：192.168.43.68

无论你喜欢打Dota还是LOL，都进网站里学习一下吧！

直接目录扫描得到站点备份`www.zip`解压打开`flag.php`可得到答案

另外一种解法是：http://靶机/index.php?action=news&nid=../* 文件读取

> flag:ef167fd977019c10e6aa761a419c5240