

# Bugku, Web: 社工-初步收集

原创

Part 02 于 2022-01-14 12:10:10 发布 2179 收藏

文章标签: [安全](#) [Web ctf](#)

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/qq\\_62260856/article/details/121307523](https://blog.csdn.net/qq_62260856/article/details/121307523)

版权

RC Firefox 信息安全维护小组 哔哩哔哩 (°-°)∩口... 在线URL网址16进制... 首页 - Bugku CTF 答

Connect Error (1045) Access denied for user 'admin'@'localhost' (using password: YES)

CSDN @Part 02



《想念初恋》御剑后台扫描工具 珍藏版 By:御剑孤独 QQ:343034656

域名:  正在扫描 停止扫描

线程:  (条 CPU核心 \* 5最佳)  DIR: 446889  ASPX: 42529  探测200

超时:  (秒 超时的页面被丢弃)  ASP: 297812  PHP: 52815  探测403

MDB: 9071  JSP: 19739  探测3XX

扫描信息:  扫描线程: 20 扫描速度: 282/秒

ID	地址	HTTP响应
1	<a href="http://114.67.175.224:18778/includes/">http://114.67.175.224:18778/includes/</a>	200
2	<a href="http://114.67.175.224:18778/admin/">http://114.67.175.224:18778/admin/</a>	200
3	<a href="http://114.67.175.224:18778/static/">http://114.67.175.224:18778/static/</a>	200

GSDN-@Part-02

114.67.175.224:18778/admin/login.php

## 管理登陆

请输入用户名称

请输入用户密码

[立即登录](#)

Copyright © 2020 [一件刷帖](#)

正在传输来自 114.67.175.224 的数据...

CSDN @Part 02

正在捕获 WLAN

文件(F) 编辑(E) 视图(V) 跳转(S) 捕获(C) 分析(A) 统计(S) 电话(V) 无线(W) 工具(T) 帮助(H)

应用显示过滤器: <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
608	53.157566	192.168.43.161	123.126.97.5	SMTP	66	C: AUTH LOGIN
609	53.235214	123.126.97.5	192.168.43.161	SMTP	72	S: 334 dXNlcm5hbWU6
610	53.284367	192.168.43.161	123.126.97.5	TCP	54	12277 → 25 [ACK] Seq=35 Ack=270 Win=66304 Len=0
611	53.411731	192.168.43.161	123.126.97.5	SMTP	76	C: User: YnVna3VrdUAxNjMuY29t
612	53.500175	123.126.97.5	192.168.43.161	SMTP	72	S: 334 UGrZc3dvcnQ6
613	53.553281	192.168.43.161	123.126.97.5	TCP	54	12277 → 25 [ACK] Seq=37 Ack=288 Win=66304 Len=0
614	53.664557	192.168.43.161	123.126.97.5	SMTP	80	C: Pass: WFNmuk9DUe10V1daUURaTA==
615	53.791311	123.126.97.5	192.168.43.161	TCP	54	25 → 12277 [ACK] Seq=288 Ack=83 Win=14720 Len=0
616	53.804383	123.126.97.5	192.168.43.161	SMTP	85	S: 235 Authentication successful
617	53.853381	192.168.43.161	123.126.97.5	TCP	54	12277 → 25 [ACK] Seq=83 Ack=319 Win=66304 Len=0
618	53.917355	192.168.43.161	123.126.97.5	SMTP	83	C: MAIL FROM:<bugkuku@163.com>
619	53.992187	123.126.97.5	192.168.43.161	TCP	54	25 → 12277 [ACK] Seq=319 Ack=112 Win=14720 Len=0
620	53.996063	123.126.97.5	192.168.43.161	SMTP	67	S: 250 Mail OK
621	54.044438	192.168.43.161	123.126.97.5	TCP	54	12277 → 25 [ACK] Seq=112 Ack=332 Win=66304 Len=0

> Frame 611: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface \Device\NPF\_{BE23846F-5180-4A43-B04B-A7347CFD00F0}, id 0  
 > Ethernet II, Src: IntelCor\_f1:a3:c9 (e0:d4:64:f1:a3:c9), Dst: 92:94:67:e5:7a:36 (92:94:67:e5:7a:36)  
 > Internet Protocol Version 4, Src: 192.168.43.161, Dst: 123.126.97.5  
 > Transmission Control Protocol, Src Port: 12277, Dst Port: 25, Seq: 35, Ack: 270, Len: 22  
 > Simple Mail Transfer Protocol

```

0000  92 94 67 e5 7a 36 e0 d4 64 f1 a3 c9 08 00 45 00  ..g-z6...d....E-
0010  00 3e b0 4f 40 00 80 06 00 00 c0 a8 2b a1 7b 7e  ->-0@...+~
0020  61 05 2f f5 00 19 9c 32 19 7a 86 ab d1 45 50 18  a/....2.z...EP
0030  01 03 c8 fd 00 00 59 6e 56 6e 61 33 56 72 64 55  .....Yn Vna3VrdU
0040  41 78 4e 6a 4d 75 59 32 39 74 0d 0a             AxNjMuY2 9t..
  
```

WLAN: <live capture in progress> 分组: 1731 · 已显示: 1731 (100.0%)

bugkuku@163.com

### base编码

base16、base32、base64

YnVna3VrdUAxNjMuY29t

编码

字符集

编码

解码

bugkuku@163.com

## base编码

base16、base32、base64

WFMUK9DUE1OV1daUURaTA==

编码 base64

字符集 utf8(unicode编码)

编码

解码

XSLROCPMNWWZQDZL

CSDN @Part 02

试试登录之前扫描的页面，错误，回头看这个账号是邮箱

[Bugku-社工-初步收集\\_m0\\_46736332的博客-CSDN博客\\_bugku社工初步收集](#)

在邮箱知道信息后，猜账号为 Mara，密码为 20010206

不正确，账号改为 mara，登录成功

The screenshot shows the admin dashboard of the Bugku website. The browser address bar displays the URL `114.67.175.224:15319/admin/`. The dashboard includes a sidebar with navigation options: 首页, 辅助管理, 网站信息, 广告位招租, and 退出登录. The main content area is titled '用户资料' (User Information) and shows the current time as '2022-01-14 12:05:53'. Below this, there are statistics for '辅助总数' (Total Auxiliary) and '已显示总数' (Total Displayed), both showing '1个'. The '服务器信息' (Server Information) section lists the following details:

- PHP 版本: 5.5.9-1ubuntu4.14 非线程安全
- MySQL 版本: 5.5.47-0ubuntu0.14.04.1
- 服务器软件: Apache/2.4.7 (Ubuntu)
- 系统名称: 壮壮后台系统
- 当前程序版本: 1.2
- 高防CDN服务器: kuzhan.la

The footer of the dashboard includes the copyright notice 'Copyright © 2019. 小bug副站 官网' and the text 'CSDN @Part 02'.

找到 flag

114.67.175.224:15319/admin/set.php?mod=site

# Bugku...

后台首页

- 首页
- 辅助管理
- 网站信息
  - 网站设置
  - 设置logo
  - 设置背景图
- 广告位招租
- 退出登录

Copyright © 2019. 小bug网站  
官网

marc

123456

本站URL #

首页背景 系统上传

备案号 京ICP备\*\*\*\*\*

腾讯云智眼

播放器key flag[45814e16d13fe59fbc437f43c22bd53a]

选择模板 default

密码重置 不修改请留空

修改

114.67.175.224:15319/admin/set.php?mod=site

CSDN @Part 02



[创作打卡挑战赛](#) >  
[赢取流量/现金/CSDN周边激励大奖](#)