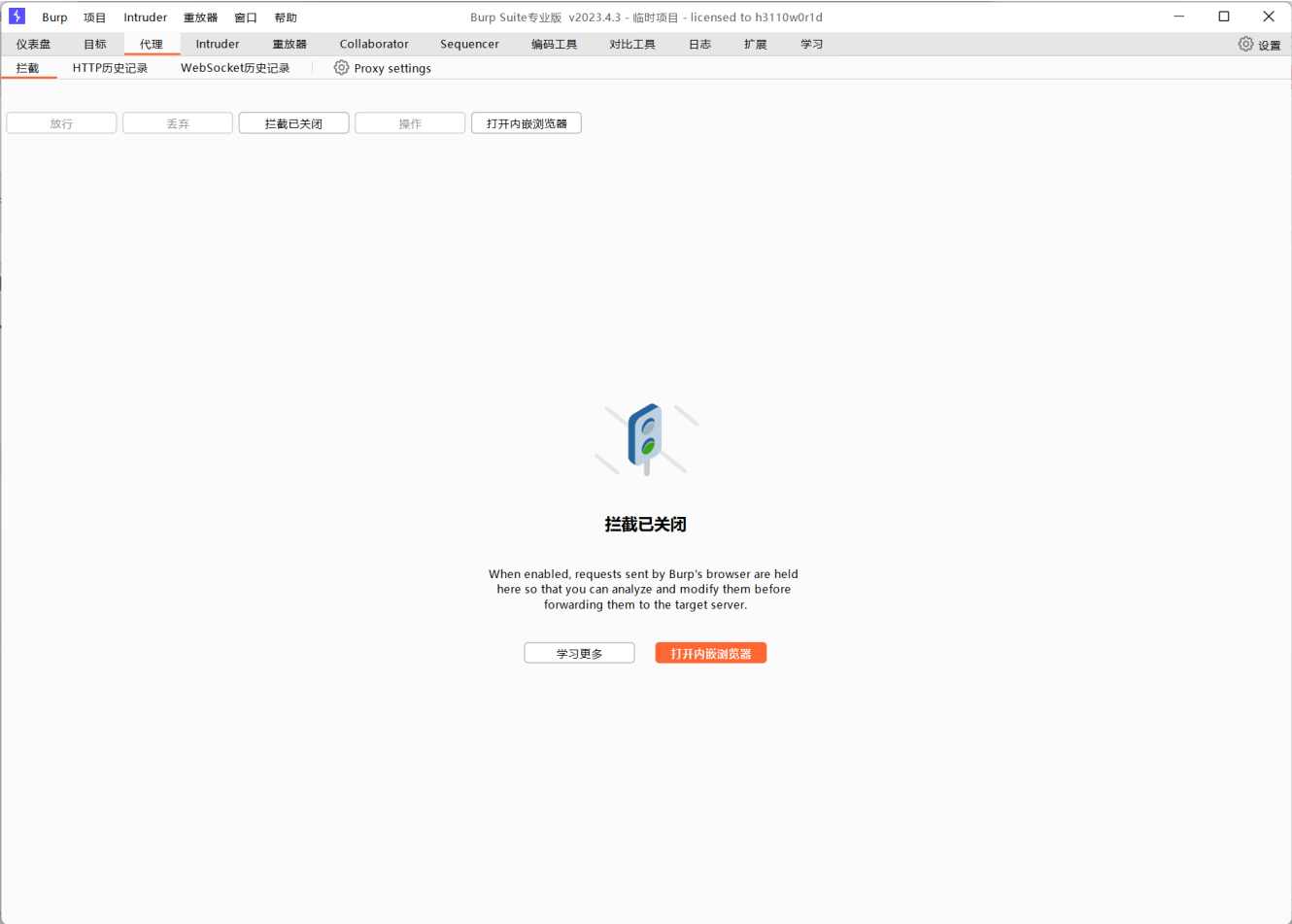


使用Brup Suite的爆破模块破解pikachu靶场登陆密码

1.打开Brup的内嵌浏览器，进入虚拟机配置好的靶场中



Get the pikachu

不安全 | 192.168.137.134/pika/

Pikachu 漏洞练习平台 pika~pika~

欢迎
骚年

系统介绍

Pikachu是一个带有漏洞的Web应用系统，在这里包含了常见的web安全漏洞。如果你是一个Web渗透测试学习人员且正发愁没有合适的靶场进行练习，那么Pikachu可能正合你意。

Pikachu上的漏洞类型列表如下：

- Burt Force(暴力破解漏洞)
- XSS(跨站脚本漏洞)
- CSRF(跨站请求伪造)
- SQL-Inject(SQL注入漏洞)
- RCE(远程命令/代码执行)
- Files Inclusion(文件包含漏洞)
- Unsafe file downloads(不安全的文件下载)
- Unsafe file uploads(不安全的文件上传)
- Over Permission(越权漏洞)
- ../../../../(目录遍历)
- I can see your ABC(敏感信息泄露)
- PHP反序列化漏洞
- XXE(XML External Entity attack)
- 不安全的URL重定向
- SSRF(Server-Side Request Forgery)
- More...(找找看?..有彩蛋!)
- 管理工具里面提供了一个简易的xss管理后台,供你测试钓鱼和捞cookie~
- 后续会持续更新一些新的漏洞进来,也欢迎你提交漏洞案例给我,最新版本请关注[pikachu](#)

每类漏洞根据不同的情况又分别设计了不同的子类

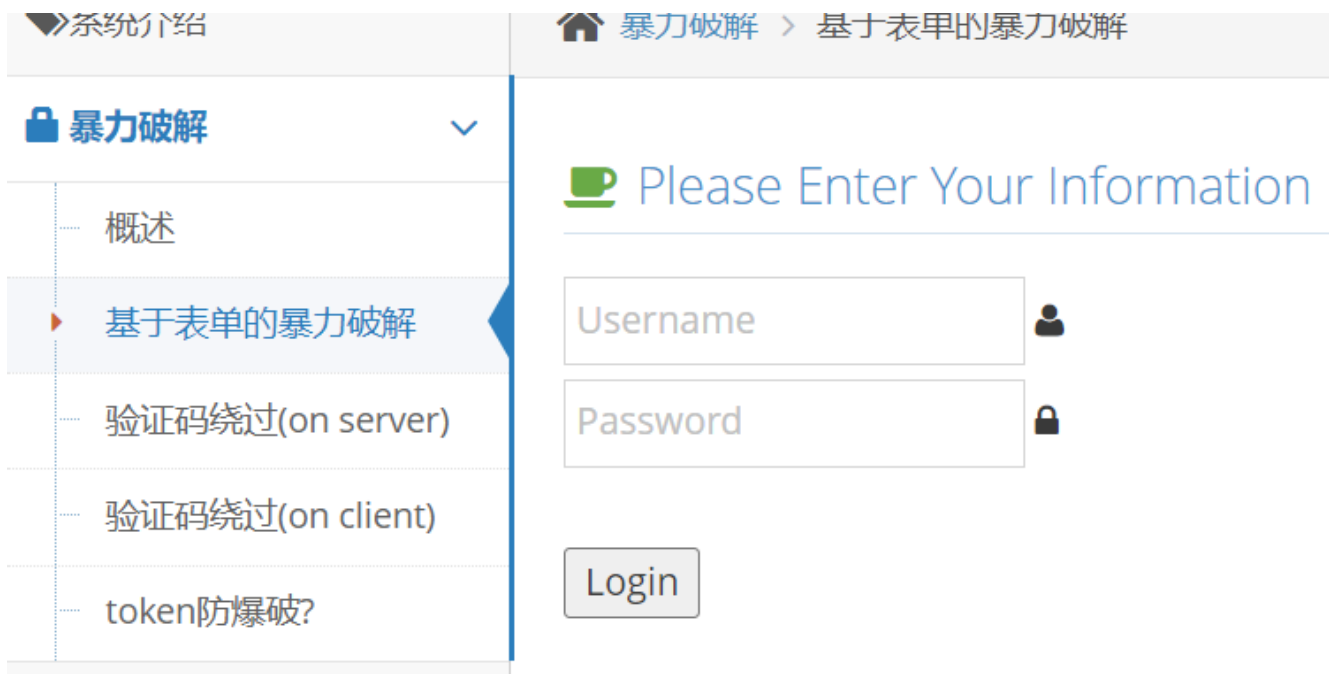
同时,为了让这些漏洞变的有意思一些,在Pikachu平台上为每个漏洞都设计了一些小的场景,点击漏洞页面右上角的"提示"可以查看到帮助信息。

如何安装和使用

Pikachu使用世界上最好的语言PHP进行开发-_-，数据库使用的是mysql，因此运行Pikachu你需要提前安装好"PHP+MYSQL+中间件(如apache,nginx等)"的基础环境，建议在你的测试环境直接使用 一些集成软件来搭建这些基础环境,比如XAMPP,WAMP等,作为一个搞安全的人,这些东西对你来说应该不是什么难事。接下来:

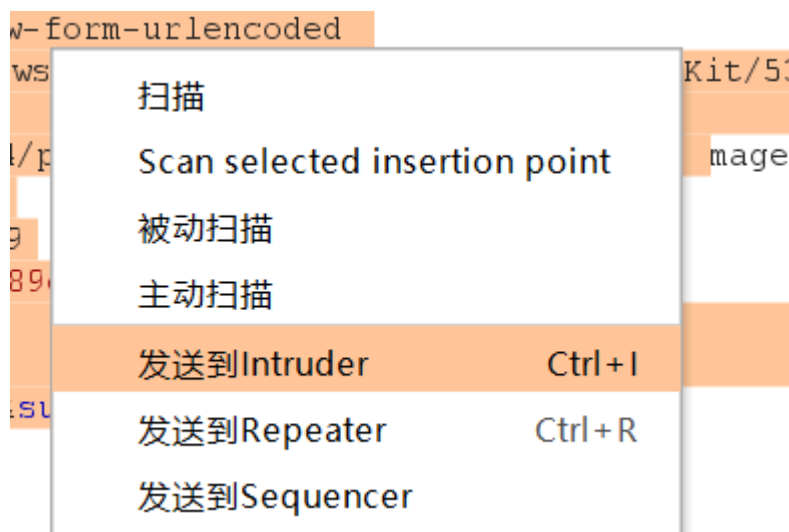
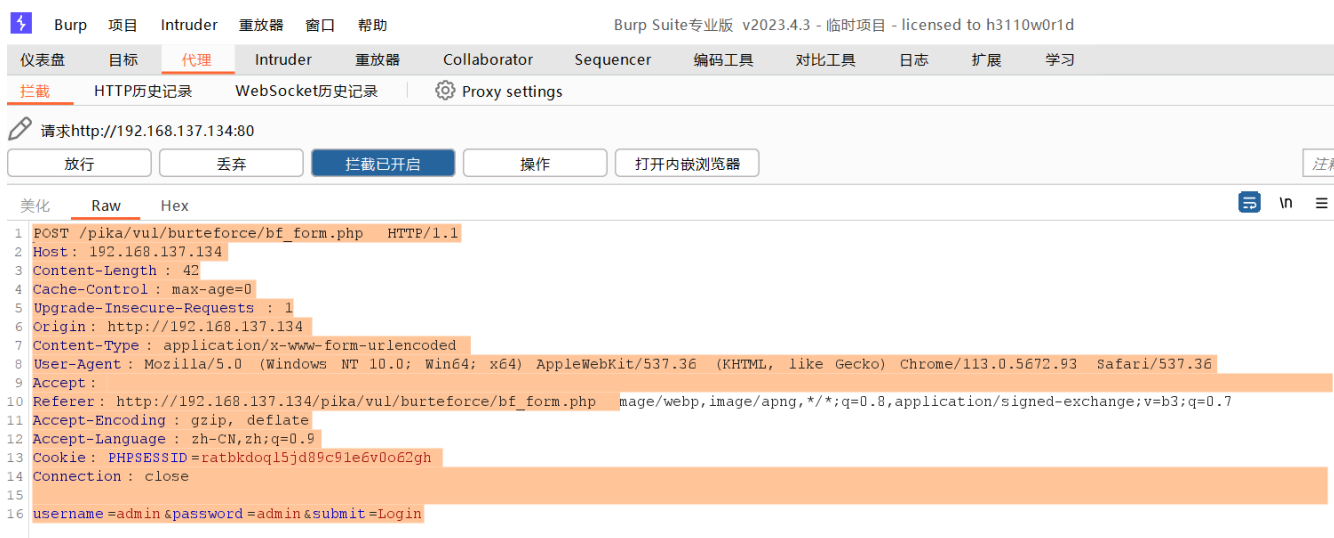
- >把下载下来的pikachu文件夹放到web服务器根目录下;
- >根据实际情况修改inc/config.inc.php里面的数据库连接配置;
- >访问<http://x.x.x.x/pikachu>,会有一个红色的热情提示"欢迎使用,pikachu还没有初始化，点击进行初始化安装!",点击即可完成安装。

2.在靶场中选择基于表单的暴力破解



3.开启拦截

4.在靶场中随便输入一个账号进行登录，将拦截信息发送给intruder



5.在intruder中框选出需要破解的区域，并选择添加payload位置

Burp Suite 专业版 v2023.4.3 - 临时项目 - licensed to h3110w0r1d

仪表盘 目标 代理 Intruder 重放器 窗口 帮助

1 x 2 x +

位置 payload 资源池 设置

选择攻击类型: 开始攻击

攻击类型: 狙击手-单个payload(Sniper)

Payload positions

配置payload插入位置，它们可以添加到目标以及基本请求中。

目标: http://192.168.137.134 ☒ 更新Host报头来匹配目标

添加payload位置 \$

清除payload位置 \$

自动添加payload位置 \$

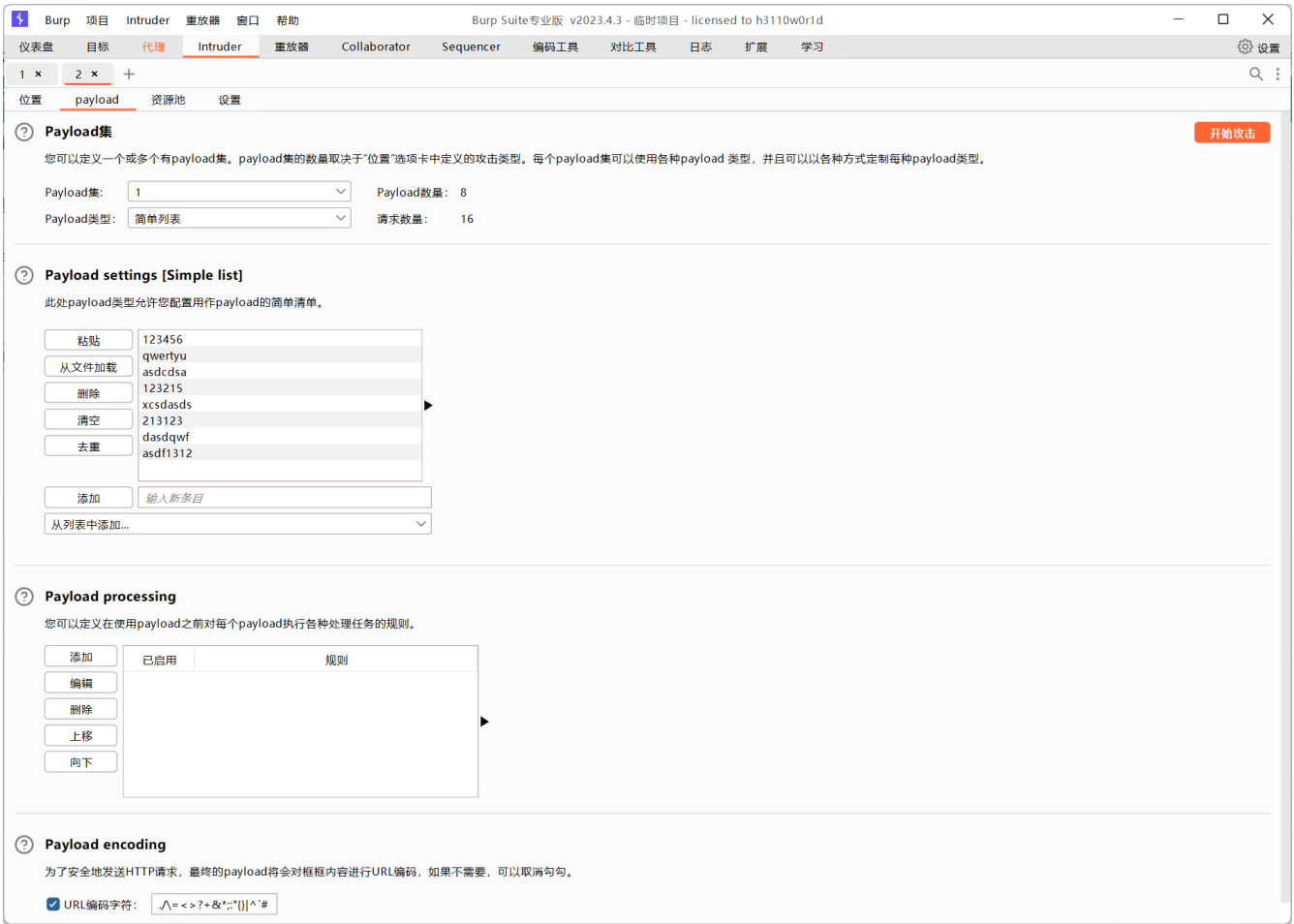
刷新

```
1 $POST /pika/vul/burteforce/bf_form.php HTTP/1.1
2 Host: 192.168.137.134
3 Content-Length: 42
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.137.134
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.5672.93 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Referer: http://192.168.137.134/pika/vul/burteforce/bf_form.php
11 Accept-Encoding: gzip, deflate
12 Accept-Language: zh-CN,zh;q=0.9
13 Cookie: PHPSESSID=ratbkdoql5jd89c91e6v0o62gh
14 Connection: close
15
16 username=admin&password=admin&submit=Login$
```

0匹配 清空

1个payload位置? 长度:743

6.在payload中导入密码本，开始攻击



7.找出与其他长度不同的密码

8	1	asdf1312	400	<input type="checkbox"/>	<input type="checkbox"/>	2529
9	2	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	35074
10	2	qwertyu	200	<input type="checkbox"/>	<input type="checkbox"/>	35074
11	2	asdcdsa	200	<input type="checkbox"/>	<input type="checkbox"/>	35074
12	2	123215	200	<input type="checkbox"/>	<input type="checkbox"/>	35074
13	2	xcsdasds	200	<input type="checkbox"/>	<input type="checkbox"/>	35074
14	2	213123	200	<input type="checkbox"/>	<input type="checkbox"/>	35074
15	2	dasdqwf	200	<input type="checkbox"/>	<input type="checkbox"/>	35074
16	2	asdf1312	200	<input type="checkbox"/>	<input type="checkbox"/>	35074

8.成功登入

暴力破解



概述

基于表单的暴力破解

验证码绕过(on server)

验证码绕过(on client)

token防爆破?



Please Enter Your Information

Username



Password



Login

login success