



Burp Suite基本用法

问题：

你把某个网站的密码忘记了，你只记得密码是由6个纯数字组成，该网站没有忘记密码的功能，也没有图形验证码，如何找回密码呢？





学院介绍

学院宗旨：专注网安人才实战技能培养

学院官网：<https://edu.hetianlab.com/>

合天网安实验室：<https://www.hetianlab.com/>

主打课程：

《web安全》：OWASP TOP 10漏洞原理及测试

《渗透测试》：渗透测试流程及工具的使用

《安全开发》：用python写一个综合的扫描器

《CTF-PWN》：CTF中的PWN相关

《CTF-WEB》：CTF中WEB相关



目录

CONTENTS



01

Burp Suite基本介绍



02

浏览器代理及抓包



03

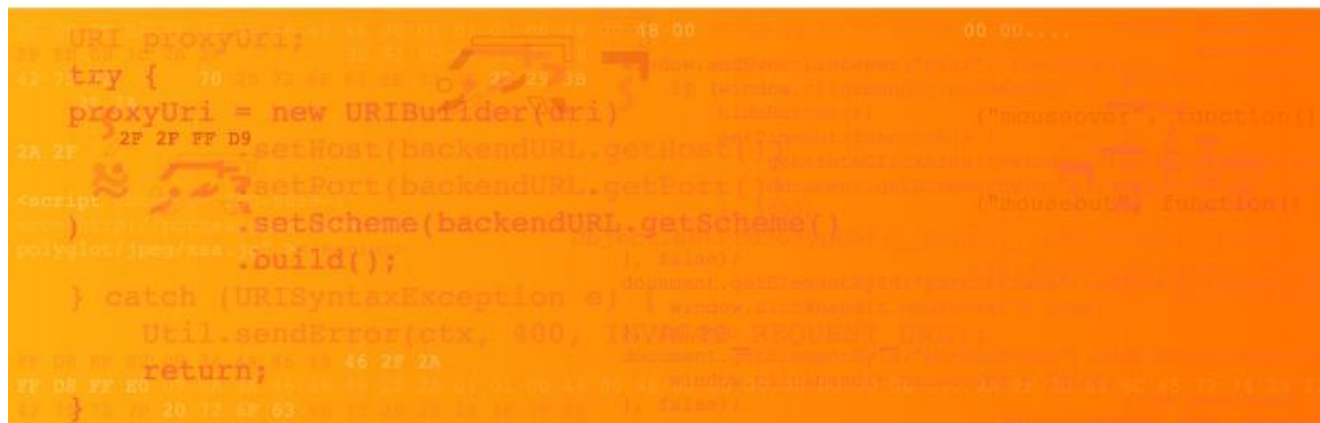
Intruder模块的使用



/01 Burp Suite基本介绍


1.1 Burp Suite简介


Burp Suite是一个集成化的渗透测试工具，它集合了多种渗透测试组件，使我们自动化地或手工地能更好的完成对web应用的渗透测试和攻击。



1.2 Burp Suite代理

Burp Suite是以拦截代理的方式，拦截所有通过代理的网络流量，如客户端的请求数据、服务器端的返回信息等。

 **Proxy Listeners**

 Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server.

Add

Edit

Remove

Running	Interface	Invisible	Redirect	Certificate
<input checked="" type="checkbox"/>	127.0.0.1:8080			Per-host

Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating SSL connections. You can import or export this certificate for use in other tools or another installation of Burp.

Import / export CA certificate

Regenerate CA certificate



/02 浏览器代理及抓包



2.1 代理服务器

提供代理服务的电脑系统或其它类型的网络终端称为代理服务器。代理服务器作为一种既是服务器又是客户机的中间程序，主要用于转发客户系统的网络访问请求。



2.2 浏览器设置代理

网络设置

配置 Firefox 如何连接互联网。 [详细了解](#)

设置...(E)

连接设置

配置访问互联网的代理服务器

☐ 不使用代理服务器(Y)

☐ 自动检测此网络的代理设置(W)

☐ 使用系统代理设置(U)

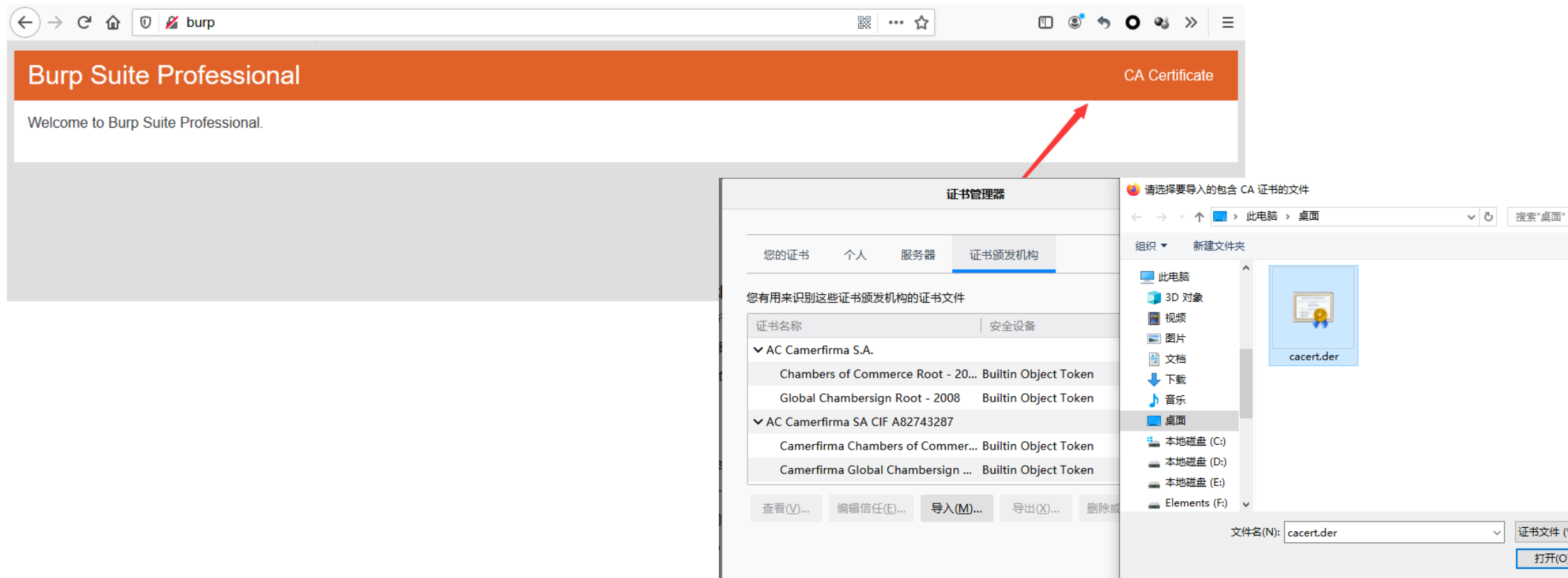
☒ 手动配置代理(M)

HTTP 代理(X)

端口(P)

☒ 也将此代理用于 FTP 和 HTTPS

2.3 证书安装

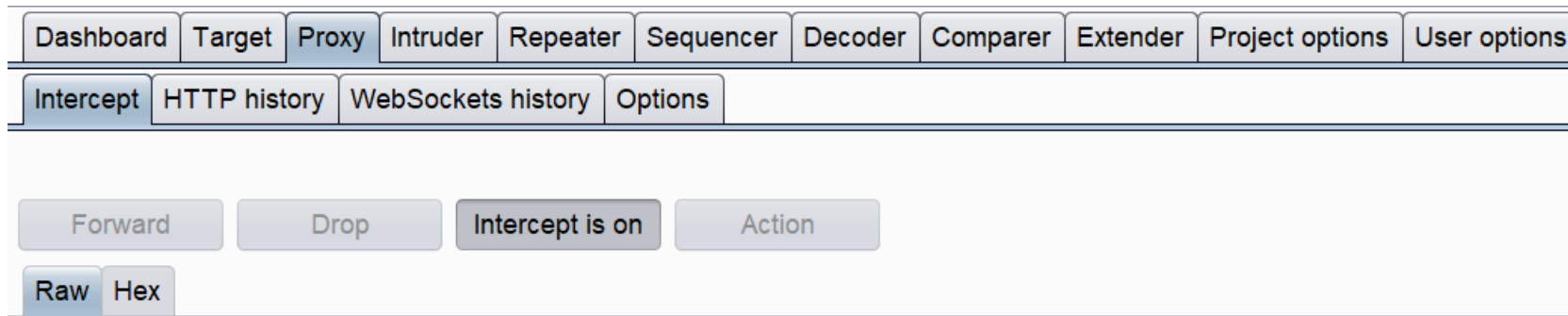




/03 Intruder模块的使用

3.1 Proxy模块

Proxy代理模块作为BurpSuite的核心功能，拦截HTTP/S的代理服务器，作为一个在浏览器和目标应用程序之间的中间人，允许你拦截，查看，修改在两个方向上的原始数据流(请求和响应)。





3.1.1 Intercept

用于显示修改HTTP请求及响应内容，并可将拦截的HTTP请求发送至其他模块处理。

1. Forward：用于发送数据。当把所需要的HTTP请求编辑完成后，手动发送数据。
2. Drop：将该请求包丢弃。
3. Intercept is off/on:拦截开关。当处于off状态下时，会自动转发所拦截的所有请求；当处于on状态下时，会将所有拦截所有符合规则的请求并将它显示出来等待编辑或其他操作。
4. Action：将请求发送到其它模块进行交互

3.2 Intruder模块

用于自动对Web应用程序自定义的攻击。它可以用来自动执行测试过程中可能出现的所有类型的任务。例如目录爆破，注入，密码爆破等。

Dashboard

Target

Proxy

Intruder

Repeater

Sequencer

Decoder

Comparer

Extender

Project options

User options

1 × ...

Target

Positions

Payloads

Options

?

Attack Target

Configure the details of the target for the attack.

Host:

Port:

☐ Use HTTPS



3.2.1 Target

用于配置目标服务器进行攻击的详细信息。

1 × ...

Target

Positions

Payloads

Options

?

Attack Target

Configure the details of the target for the attack.

Host:

Port:

☐ Use HTTPS

3.2.2 Positions

设置Payloads的插入点以及攻击类型（攻击模式）。

Sniper：狙击手模式，对标记变量依次进行爆破。特点：不管添加多少个标记位，只有一个字典。

Battering ram：攻城锤模式，可对多个变量同时破解。特点：一个字典对应多个标记位。

Pitchfork：草叉模式：每一个变量对应一个字典。特点：爆破次数取决于变量少的字典。

Cluster bomb：集束炸弹模式，组合爆破，每个变量对应一个字典，并交集爆破。特点：爆破次数为字典1x字典2。



The screenshot shows the 'Payload Positions' configuration window. At the top, there are tabs for 'Target', 'Positions', 'Payloads', and 'Options'. The 'Positions' tab is active. Below the tabs, there is a title bar with a question mark icon and the text 'Payload Positions'. A 'Start attack' button is located in the top right corner. The main area contains a description: '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.' Below this, there is a dropdown menu for 'Attack type' with the following options: 'Battering ram' (selected), 'Sniper', 'Pitchfork', and 'Cluster bomb'. To the right of the dropdown menu are four buttons: 'Add \$', 'Clear \$', 'Auto \$', and 'Refresh'. Below the dropdown menu, there is a text area containing a sample HTTP request. The request is a POST to '/20210' with various headers and a body. The body contains a payload: 'un= \$ admin \$ &pw= \$ admin \$'.

Target Positions Payloads Options

? Payload Positions

Start attack

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: Battering ram

- Sniper
- Battering ram
- Pitchfork
- Cluster bomb

Add \$

Clear \$

Auto \$

Refresh

```
POST /20210
Host: 192.168.81.222
Content-Length: 300
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.77 Safari/537.36
Origin: http://192.168.81.222
Content-Type: application/x-www-form-urlencoded
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://192.168.81.222/20210607/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,zh-TW;q=0.7,en-US;q=0.6
Connection: close

un= $ admin $ &pw= $ admin $
```




3.2.3 Payloads

配置Positions设置的标记位的字典。

? Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are

Paste

Load ...

Remove

Clear

Add

Enter a new item

Add from list ...

? Payload Encoding

This setting can be used to URL-encode selected characters within the final pay

☒ URL-encode these characters:

Target Positions Payloads Options

? Payload Sets

You can define one or more payload sets. The number of payload se
be customized in different ways.

Payload set: 1 Payload count: 0

Payload type: Simple list Request count: 0

? Payload Processing

You can define rules to perform various processing tasks on each p

Add

Edit

Remove

Up

Down

Enabled Rule



感谢您的聆听

▶ 学习工具、资料及课程回放



扫码免费领取

