

HTTP e Burp Suite

E por Eduardo Panizzon



O Protocolo HTTP

HyperText Transfer Protocol



Cliente-Servidor

Comunicação baseada em requisição/resposta.



Sem Estado

Cada requisição é independente.

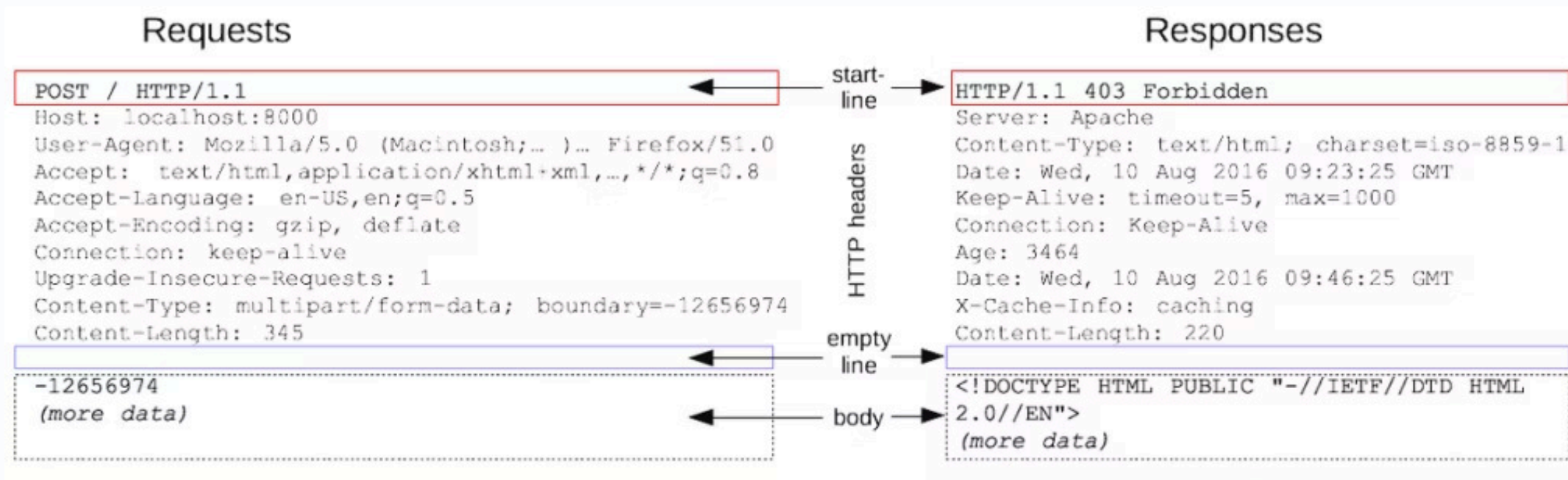


Porta Padrão (80)

O HTTP utiliza a porta 80

O HTTP é a espinha dorsal da web. Ele permite a troca de dados entre navegadores e servidores. Sua natureza sem estado garante que cada interação seja única.

Cabeçalhos HTTP



Métodos de Requisição HTTP

GET

Solicita dados de um recurso. Usado para buscar informações.

POST

Envia dados para processamento. Usado para criar ou enviar formulários.

PUT

Atualiza um recurso existente. Substitui todo o conteúdo.

DELETE

Remove um recurso específico. Usado para exclusão de dados.

Códigos de Resposta HTTP

2xx Sucesso

Indica que a requisição foi recebida e processada com êxito pelo servidor. A ação foi concluída.

200 OK

201 Created

3xx Redirecionamento

Informa que são necessárias ações adicionais. O recurso solicitado pode ser encontrado em outro URL.

301 Moved Permanently

304 Not Modified

4xx Erro do Cliente

Sinaliza um problema na requisição. O cliente cometeu um erro, como uma URL inválida ou acesso negado.

401 Unauthorized

404 Not Found

5xx Erro do Servidor

Indica que o servidor falhou ao processar a requisição. Um erro interno impede a conclusão da operação.

501 Not Implemented

Introdução ao Burp Suite

Ferramenta Completa

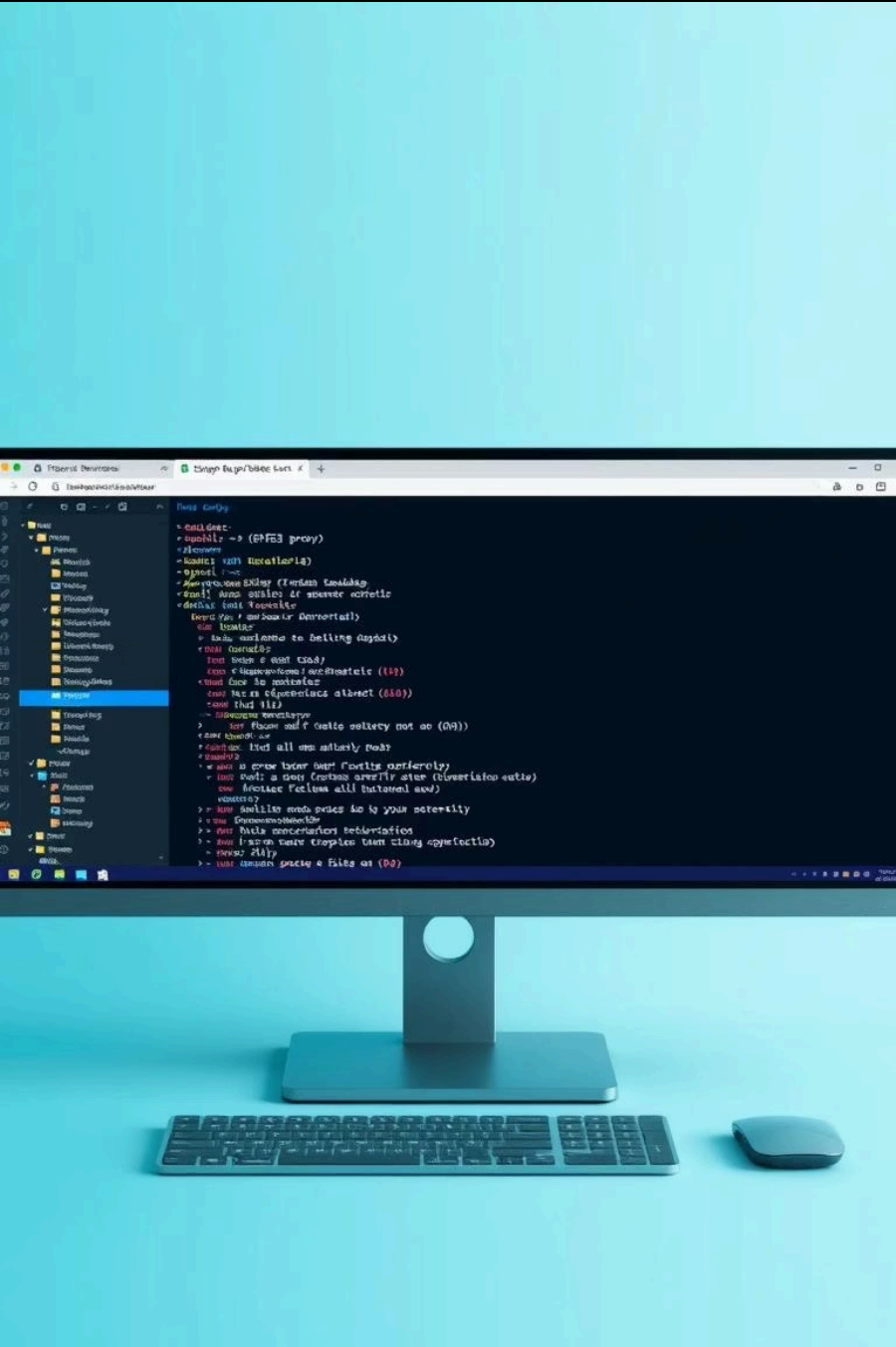
Burp Suite é uma plataforma integrada para testes de segurança de aplicações web. Ele oferece diversas funcionalidades.

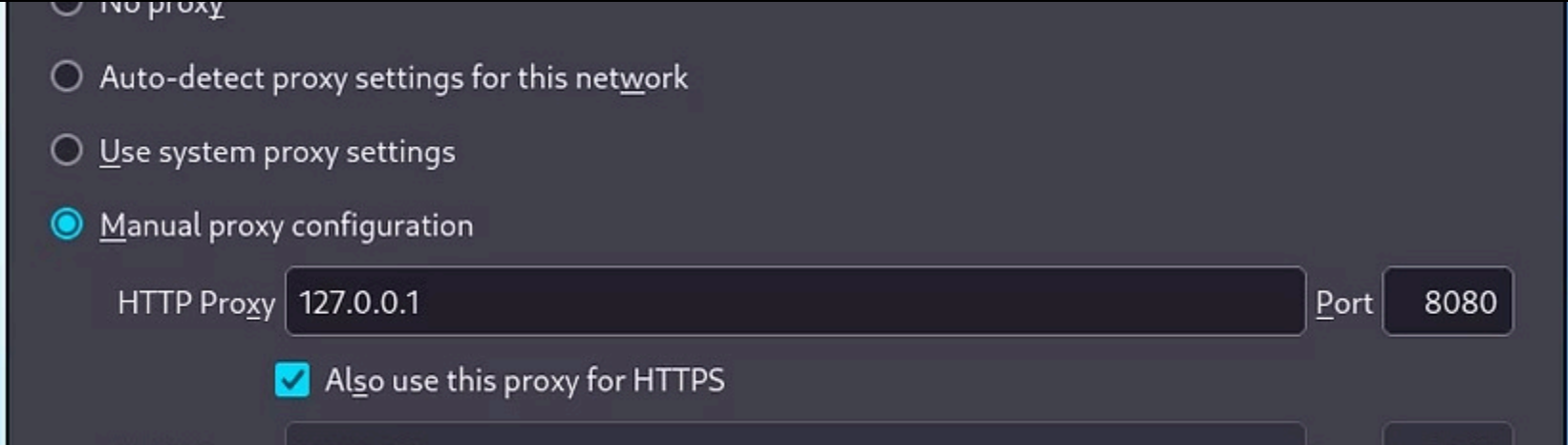
Proxy de Intercepção

Seu recurso principal é o proxy. Ele permite ver e modificar requisições e respostas HTTP/S.

Edições Essenciais

Disponível em versões Community (gratuita) e Professional (paga). A versão Pro oferece mais recursos e automação.





Configurando o Proxy

Iniciar Burp Suite

Abra a aplicação e vá para a aba "Proxy".

Porta Padrão

Verifique a porta padrão, geralmente 8080.

Configurar Navegador

Ajuste as configurações de proxy do seu navegador para 127.0.0.1:8080.

Instalando o Certificado SSL

Para interceptar tráfego HTTPS, o certificado do Burp Suite deve ser instalado.



1

Navegar no Burp

Acesse **http://burp** no navegador. Baixe o certificado CA.

2

Importar Certificado

Importe-o para o armazenamento de certificados confiáveis do sistema.

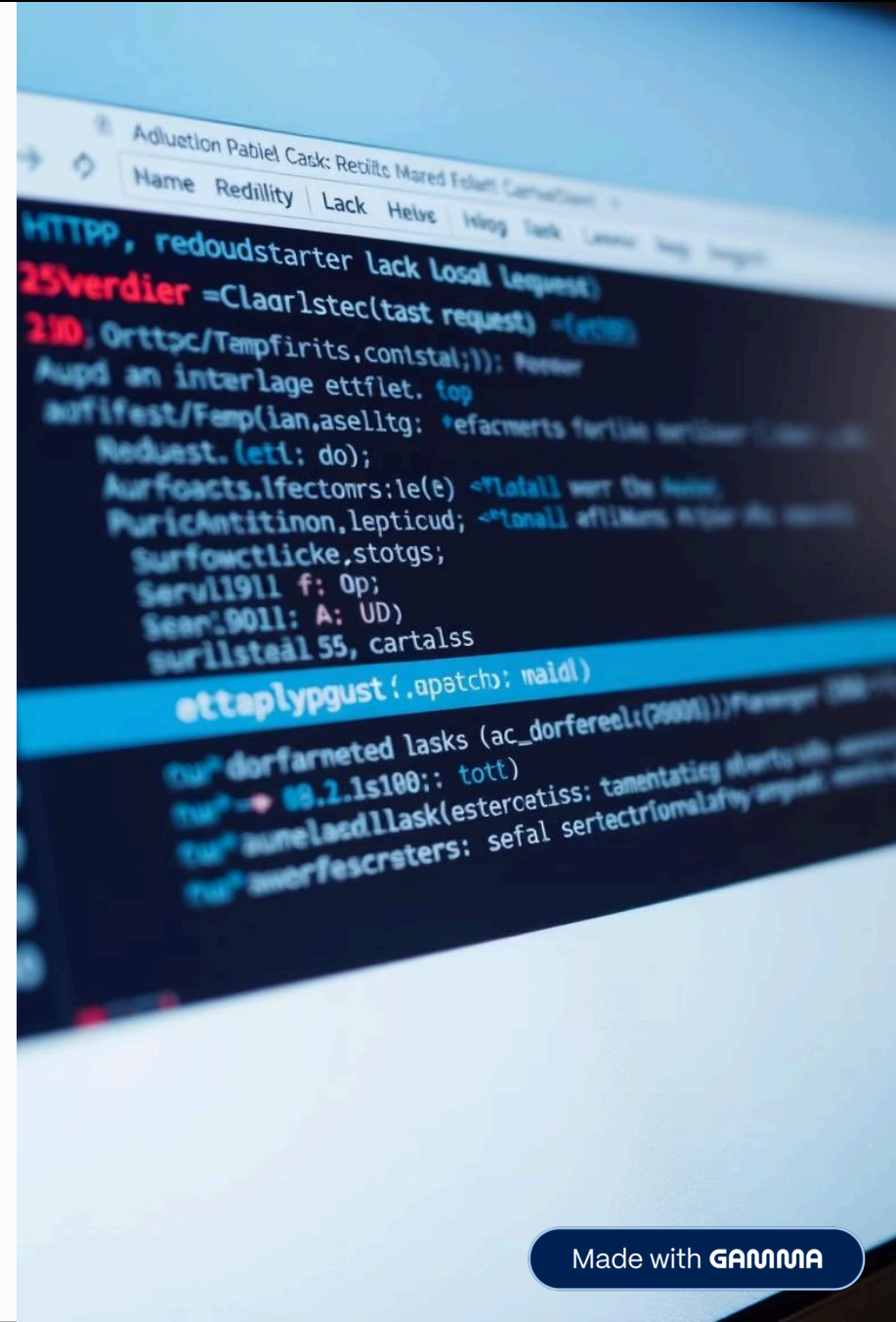
3

Reiniciar Navegador

Reinicie o navegador para que as mudanças façam efeito.

Interceptando Requisições

- 1** — Proxy "Intercept"
Certifique-se que o "Intercept is on" na aba Proxy.
- 2** — Navegar no Alvo
Faça uma requisição no navegador. Ela será interceptada no Burp.
- 3** — Analisar e Modificar
Examine a requisição e modifique parâmetros, se necessário.
- 4** — Forward ou Drop
Encaminhe (forward) ou descarte (drop) a requisição ou a resposta do servidor.



Modificando Requisições

A modificação de requisições é crucial para testes de segurança. Permite manipular inputs.



Alterar Parâmetros

Modifique valores de campos ou cabeçalhos.



Testar Vulnerabilidades

Insira payloads para SQL Injection.



Explorar Autenticação

Tente bypassar mecanismos de login.

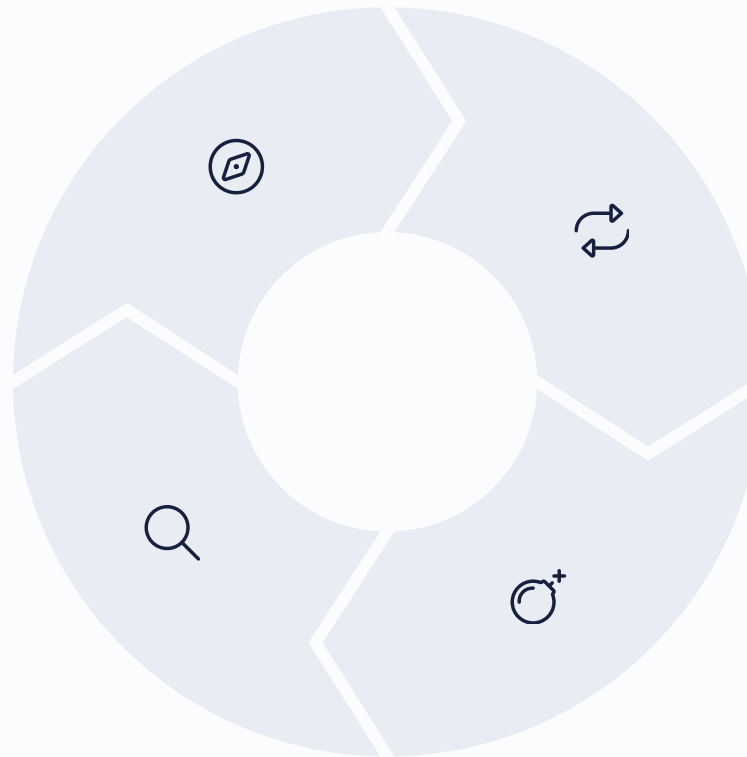


Outras Ferramentas do Burp

Além do proxy, Burp Suite oferece outras ferramentas poderosas para análise.

Target
Mapeia a superfície de ataque da aplicação.

Scanner
Identifica vulnerabilidades automaticamente.



Repeater

Envia requisições manualmente com modificações.

Intruder

Automatiza ataques de força bruta e fuzzing.

Demonstração

