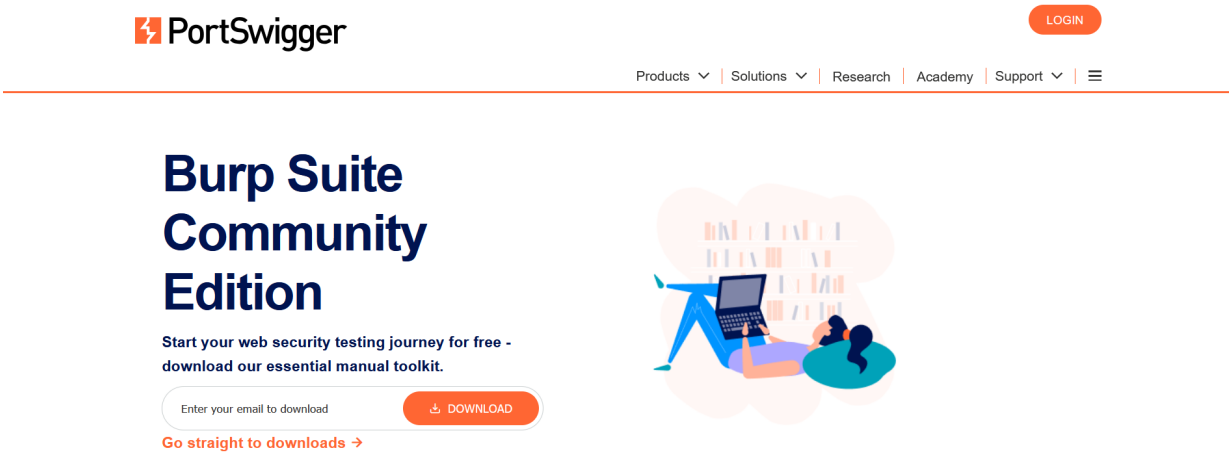
Burp Suite

O **Burp Suite** é uma ferramenta essencial para avaliar a segurança de aplicações web, permitindo identificar e explorar vulnerabilidades. Desenvolvida pela **PortSwigger**, é amplamente utilizada por profissionais de cibersegurança para realizar testes de penetração e auditorias de segurança.

Instalação

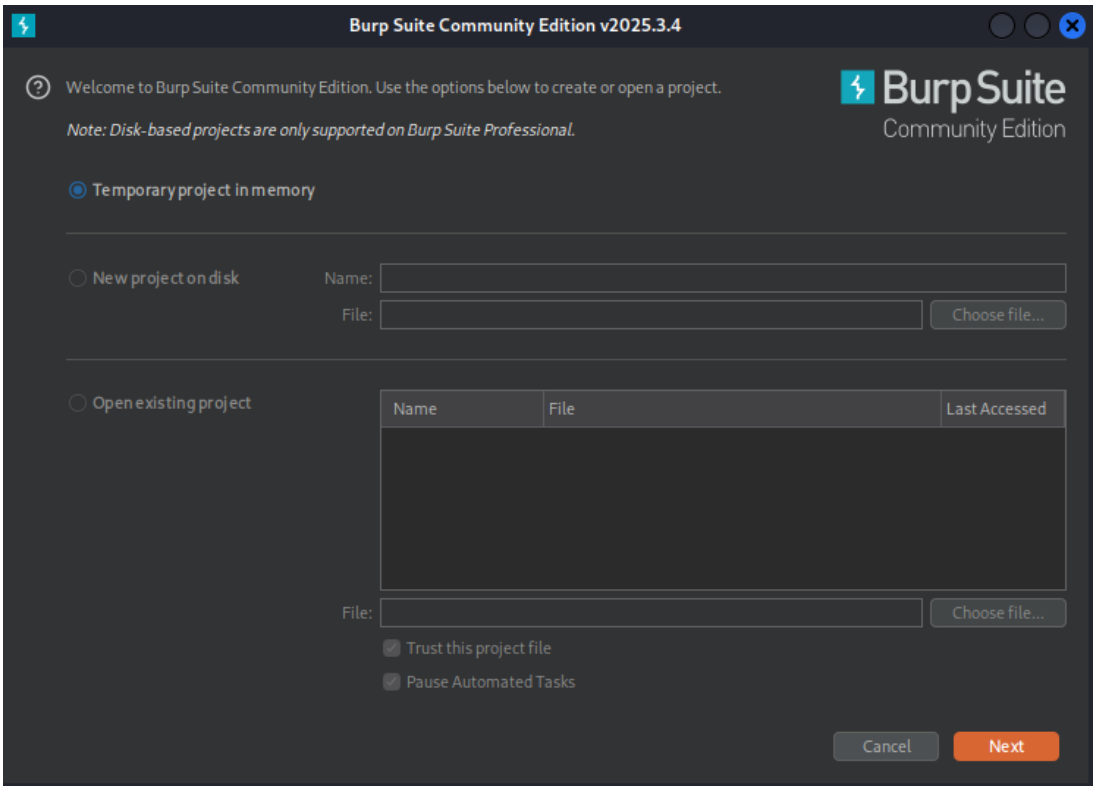
Para instalar o Burp Suite, basta acessar o site oficial da PortSwigger e baixar a versão **Community Edition**, que é gratuita. A instalação é simples e pode ser feita em sistemas operacionais Windows, macOS e Linux.

https://portswigger.net/burp/communitydownload



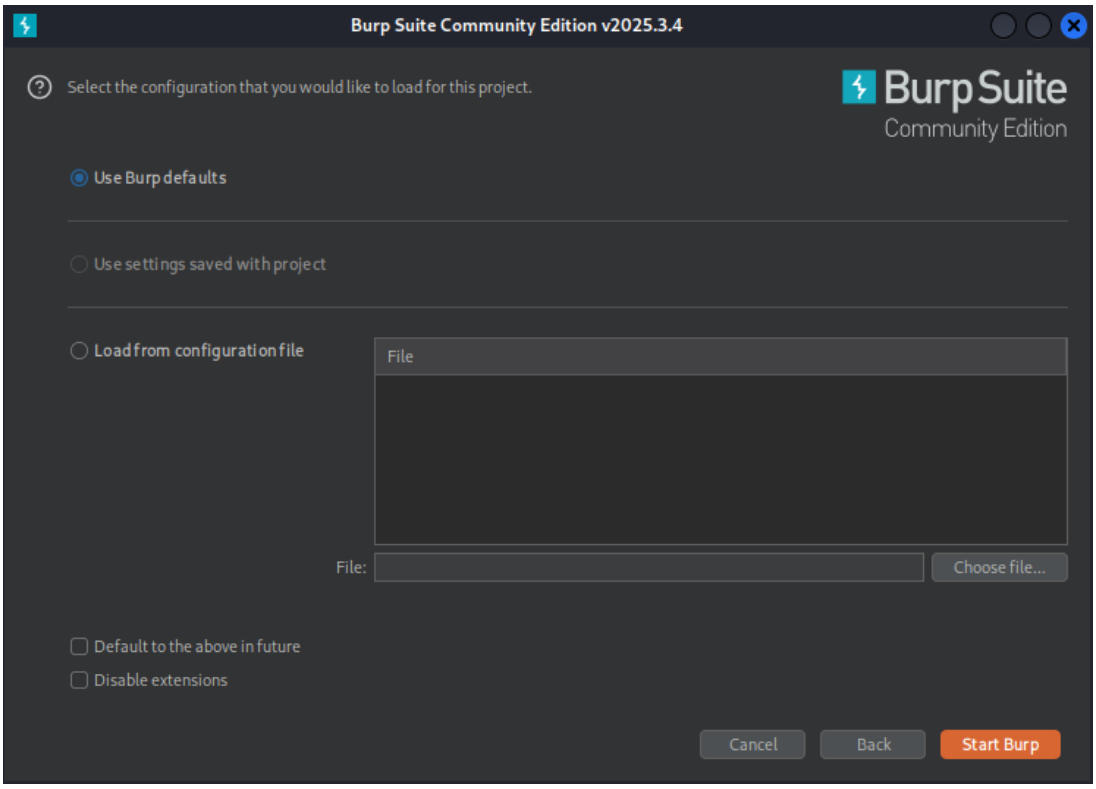
Inicialização

Após a instalação, inicie o Burp Suite. Na primeira execução, você será apresentado a uma tela de configuração. Escolha a opção "*Temporary project*" para iniciar um projeto temporário.

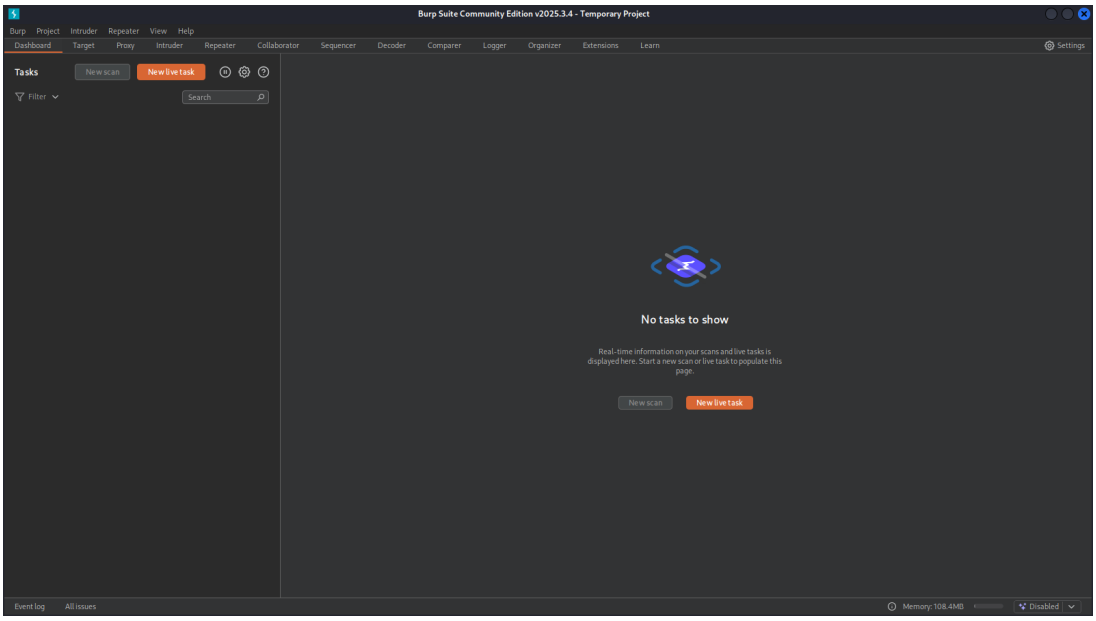


Após isso você pode selecionar uma configuração. A opção padrão é *"Use Burp defaults"*, que é adequada para a maioria. Caso tenha um arquivo de configuração personalizado, você pode escolher *"Load from configuration file"*.

Se caso não quiser que essa mensagem apareça novamente, marque a opção *"Default to the above in future"*.

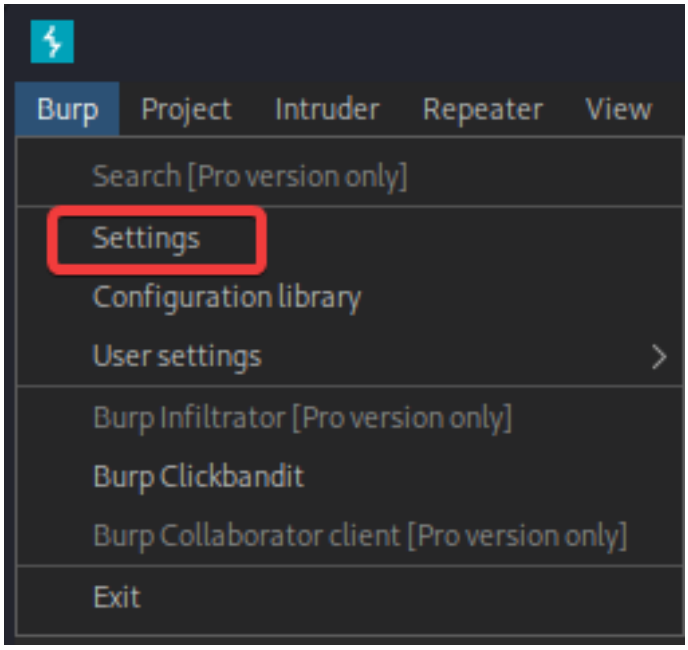


Pronto, você verá a interface principal do Burp Suite, que é dividida em várias abas, cada uma com funcionalidades específicas.



Configurações

Caso queira mudar alguma configuração padrão, vá até a aba "*Burp*" e selecione "*Settings*". Você pode ajustar configurações de proxy, extensões, aparência e muito mais.



Configurando proxy para o Firefox

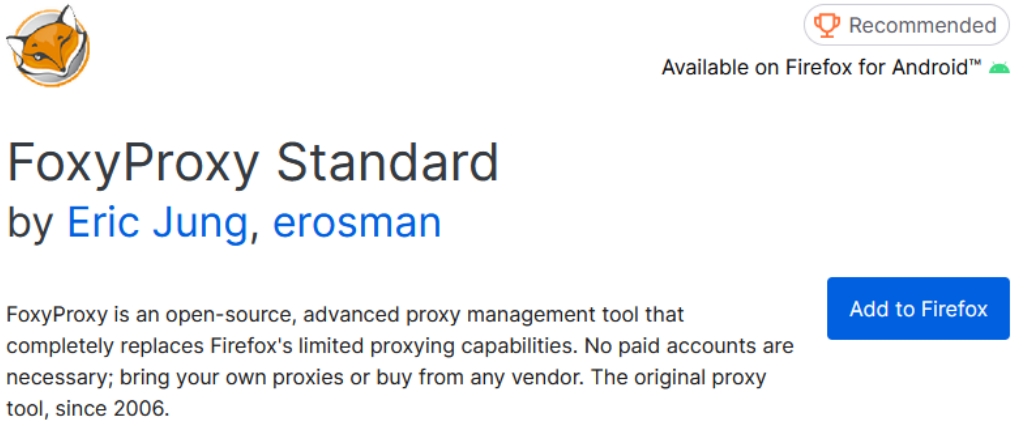
O Burp Suite atua como um proxy entre o navegador e a aplicação web. Ele já vem com um navegador embutido (chromium), mas você pode configurá-lo para trabalhar com outros navegadores, como o Firefox.

> *Esse é um passo opcional, você pode utilizar o navegador embutido do Burp Suite que será mostrado mais adiante.*

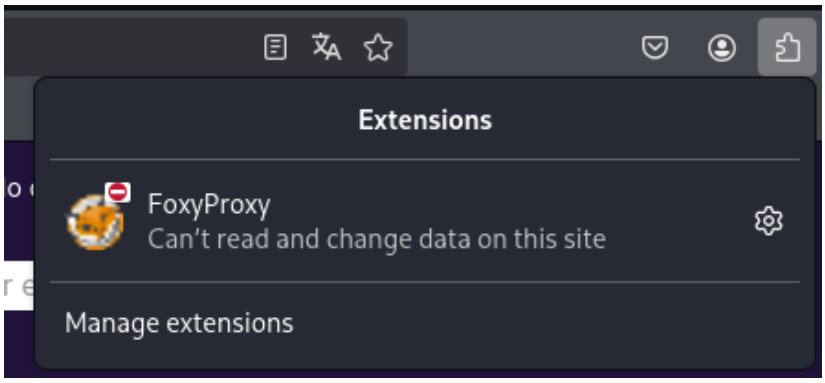
Baixando a extensão FoxyProxy

Vamos utilizar a extensão **FoxyProxy**, que vai nos permitir ligar e desligar o proxy facilmente.

Para instalar, acesse a página da extensão no Firefox https://addons.mozilla.org/en-US/firefox/addon/foxyproxy-standard/ e clique em "*Adicionar ao Firefox/Add to Firefox*".

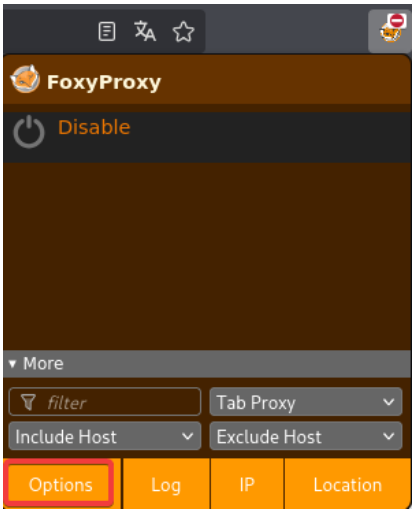


A extensão pedirá confirmação para instalação. Clique em "*Adicionar/Add*". Após isso, ela estará disponível na barra de ferramentas do Firefox.

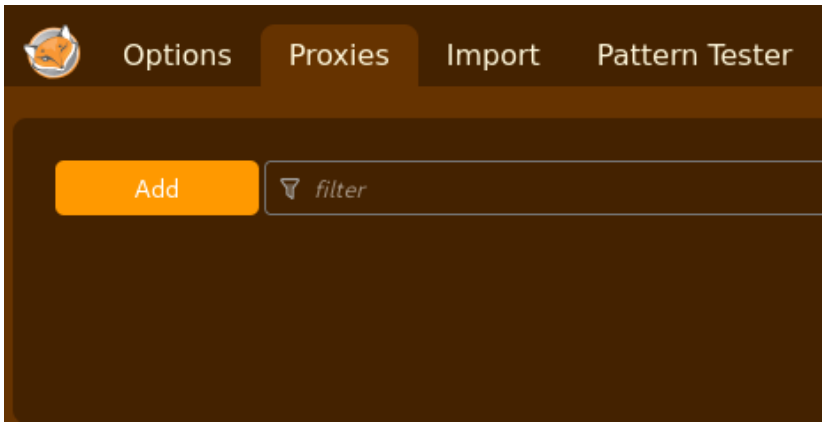


Configurando o FoxyProxy

Abra a extensão clicando no ícone do FoxyProxy na barra de ferramentas e selecione "*Options*".



Na janela aberta, vá para a aba "*Proxies*" e clique em "*Add*".

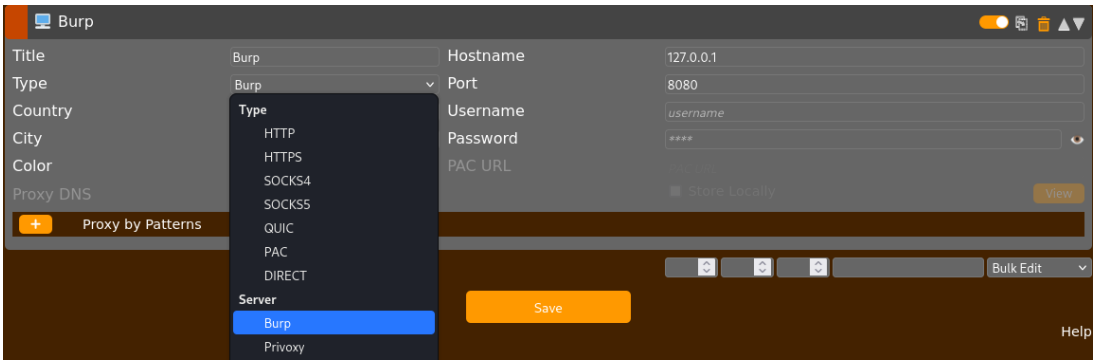


Preencha o campo de nome, você pode colocar como quiser, e depois selecione o *Type* como "*Burp*". Os campos de *Host* e *Port* já vão ser preenchidos automaticamente com os valores do Burp Suite padrão:

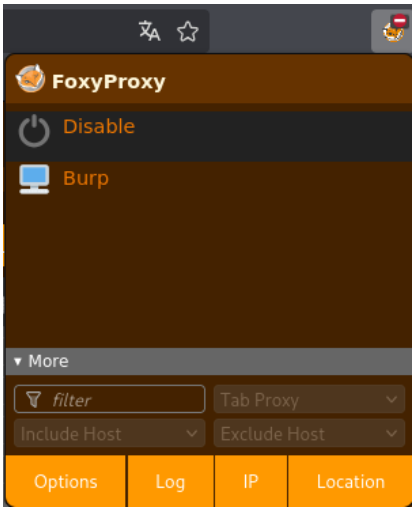
- **Host**: `127.0.0.1`
- **Port**: `8080`

> *Caso tenha alterado esses valores, coloque os que você configurou.*

Após preencher, clique em "*Save*".



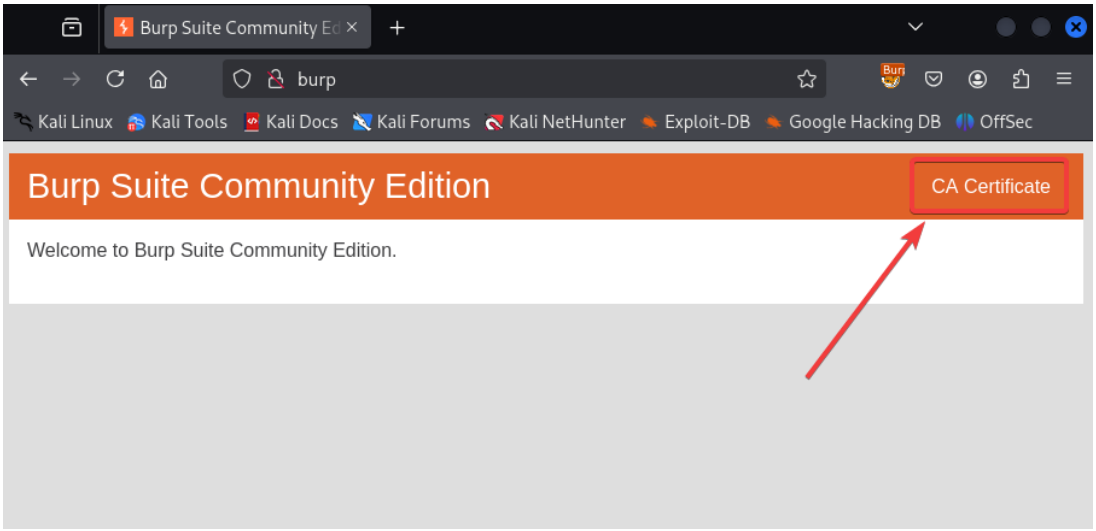
Agora, você verá o proxy adicionado na lista. Para ativá-lo, clique sobre o proxy recém-criado, e para desativá-lo, basta seleciona a opção "*Disable*".



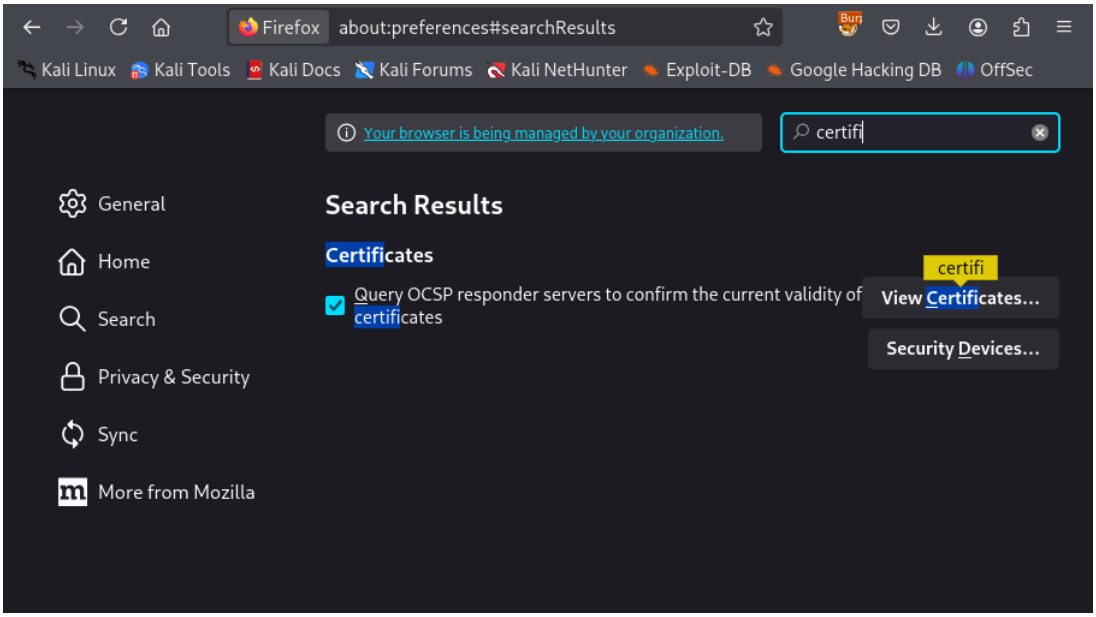
Configurando certificado

Para que o Burp Suite possa interceptar o tráfego HTTPS, é necessário instalar o certificado CA do Burp no Firefox. Se não fizer isso, você verá erros de certificado ao tentar acessar sites HTTPS.

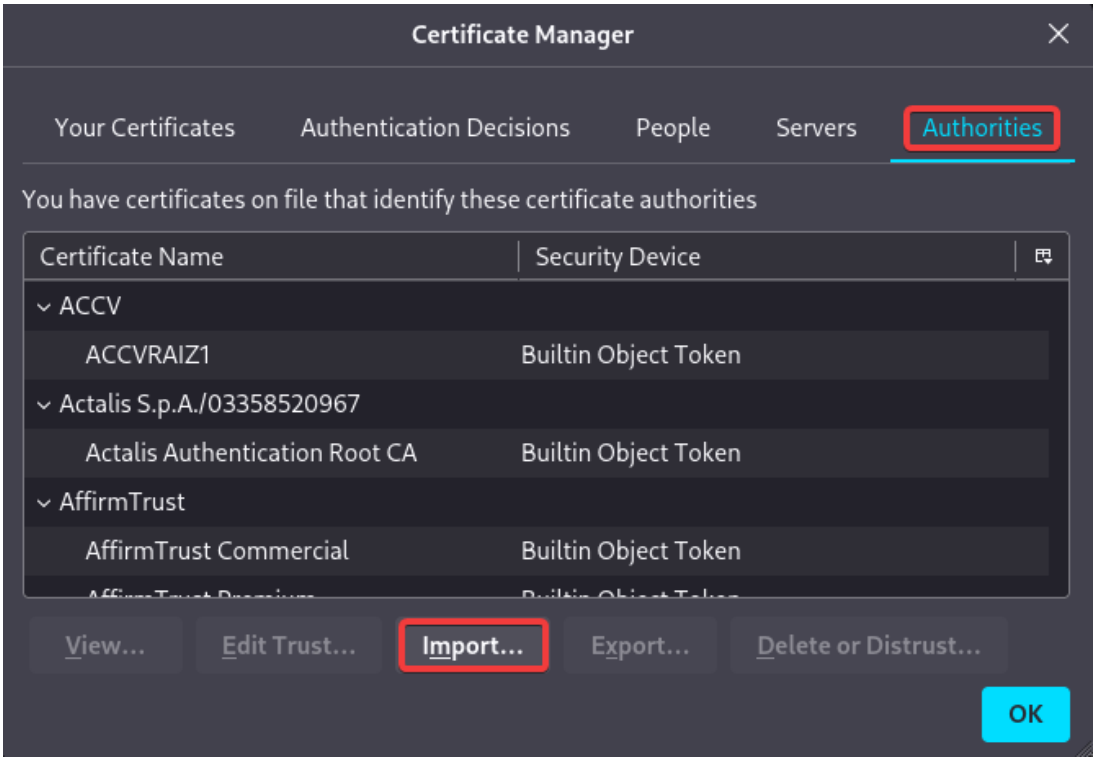
Primeiro, vá para http://burp com o proxy ativado e clique em "*CA Certificate*" no canto superior direto para baixar o certificado.



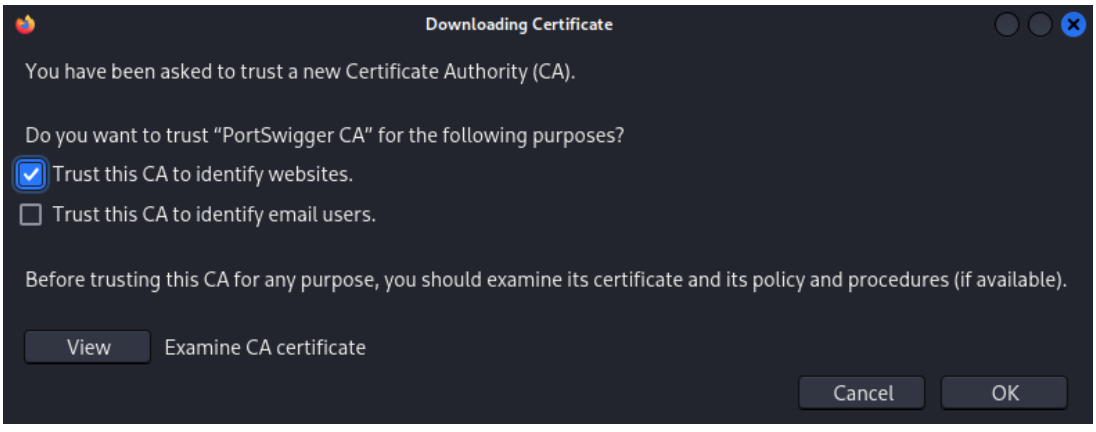
Agora, acesse about:preferences (configurações do Firefox) e pesquise por "*Certificates*" ou "*Certificados*". Você também pode acessar diretamente about:preferences#privacy e rolar até a seção "*Security*" e "*Certificates*".



Clique em "*View Certificates*", selecione a aba "*Authorities*" e clique em "*Import*". Selecione o certificado que você baixou anteriormente (geralmente chamado de `cacert.der`) e clique em "*Open*".



Marque a opção "*Trust this CA to identify websites*" e clique em "*OK*".



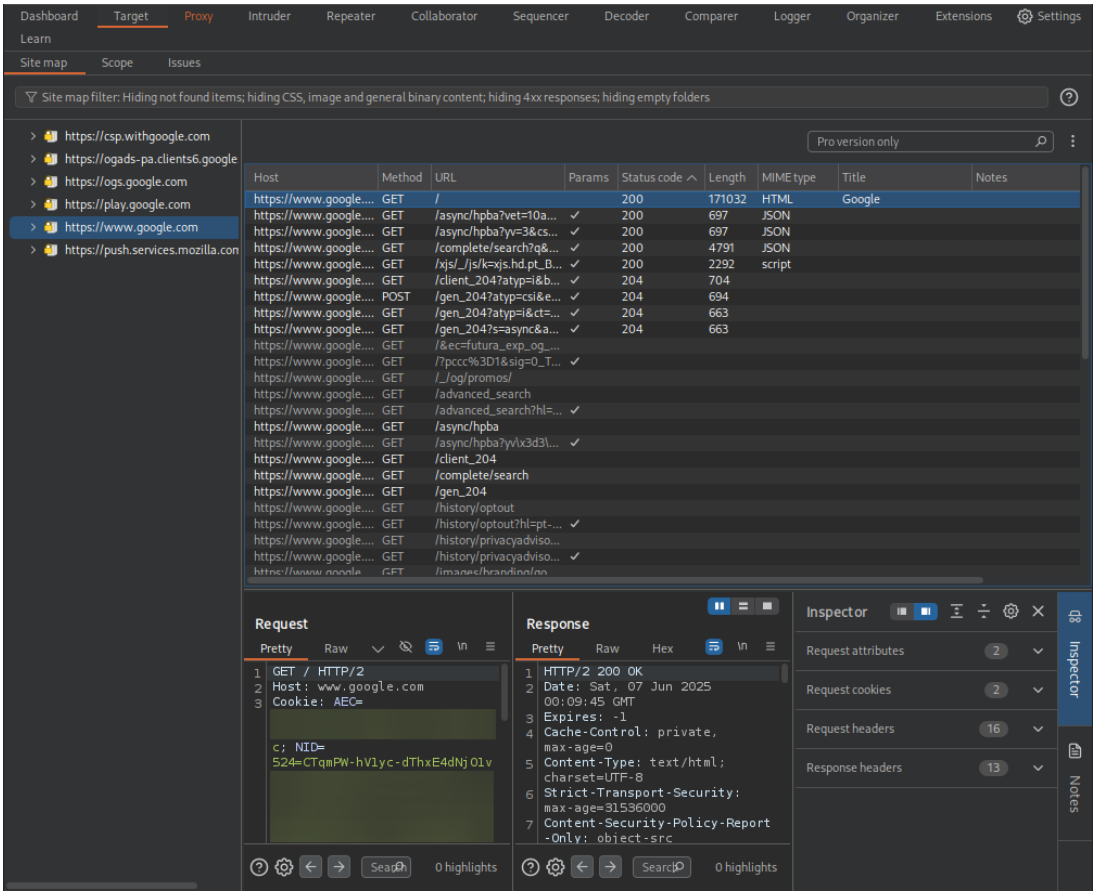
Agora, o Firefox está configurado para usar o Burp Suite como proxy e confiar no certificado CA do Burp. Você pode começar a interceptar o tráfego HTTPS.

Ferramentas

O Burp Suite possui várias ferramentas integradas, cada uma com funcionalidades específicas. Iremos explorar algumas das principais.

Target

O **Target** é onde você define o escopo do seu teste. Aqui, você pode adicionar URLs, definir o escopo de interceptação e visualizar os hosts que estão sendo monitorados. Ele gera um site map, com informações sobre os endpoints da aplicação.

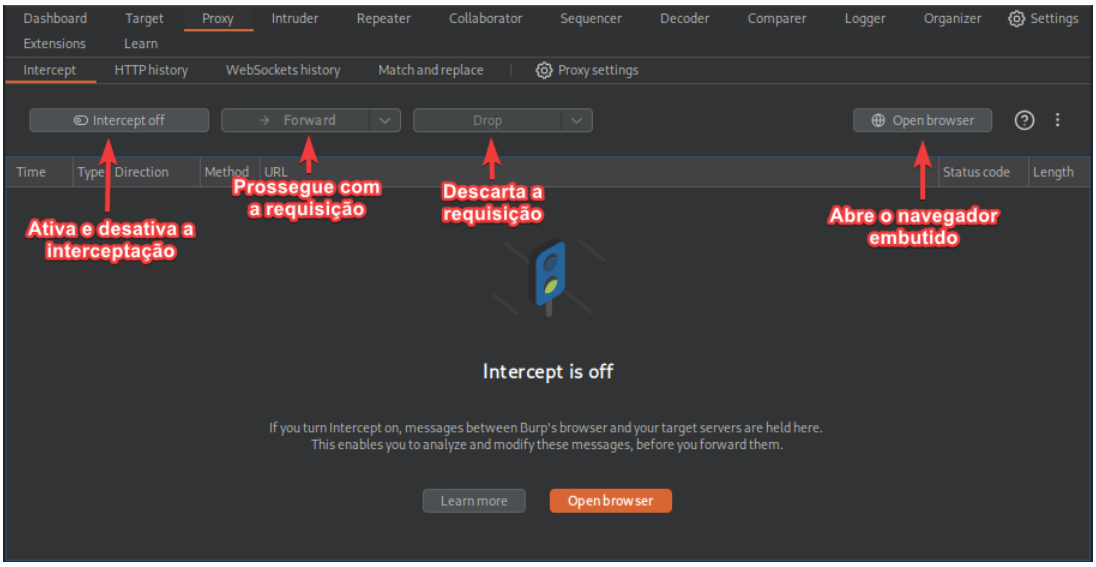


Proxy

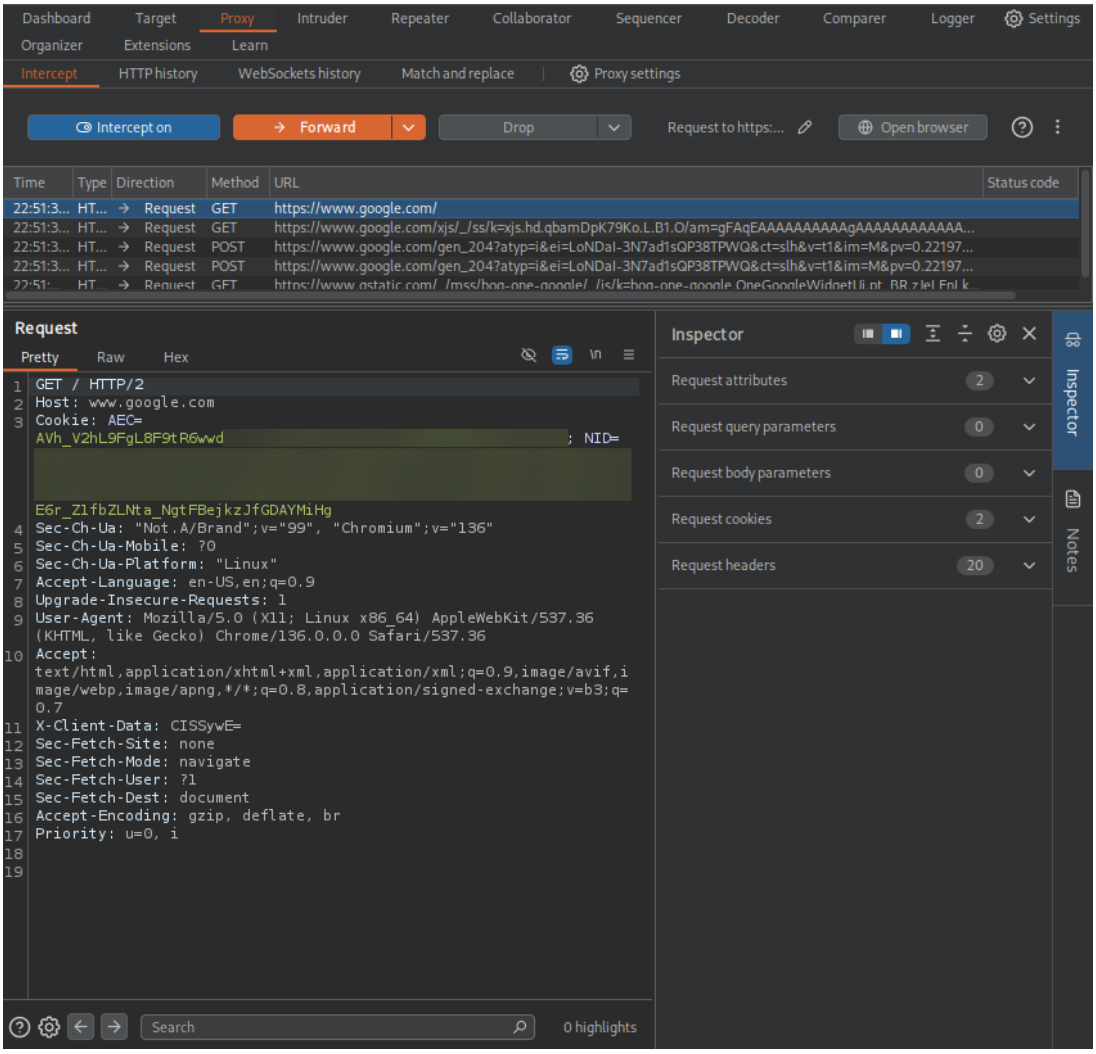
Permite interceptar e modificar requisições HTTP entre o navegador e a aplicação web. Você pode visualizar, editar e reenviar requisições, além de analisar as respostas do servidor. Temos 4 abas: **Intercept**, **HTTP history**, **WebSockets history** e **Match and Replace**.

Intercept

A aba **Intercept** permite que você pause as requisições e respostas HTTP e WebSocket, permitindo que você as modifique antes de serem enviadas ou recebidas. Você pode ativar ou desativar a interceptação clicando no botão "*Intercept is on/off*".



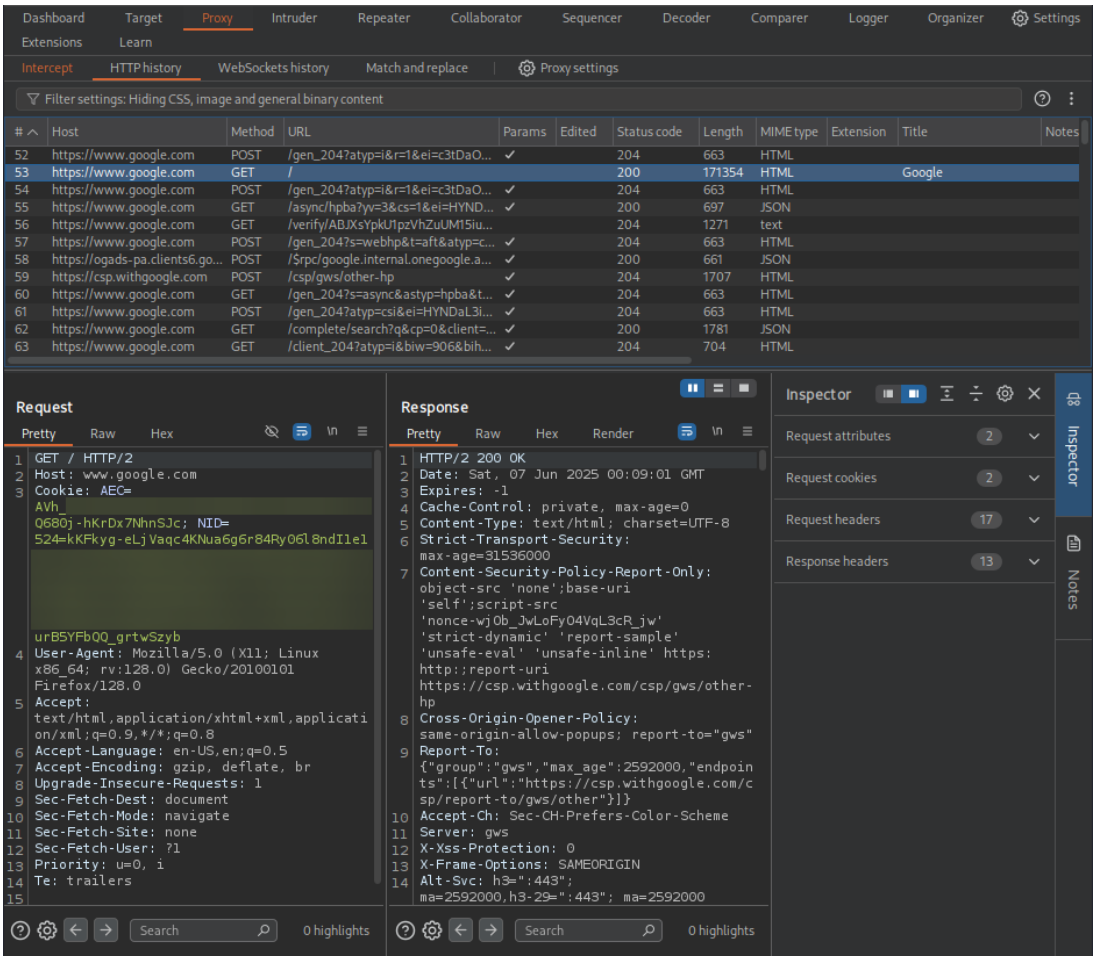
Você também pode modificar os dados da requisição antes de enviá-la ao servidor, o que é útil para testar como a aplicação lida com entradas inesperadas. Para isso, basta editar os campos desejados e clicar em "*Forward*" para enviar a requisição modificada. Também é possível rejeitar a requisição clicando em "*Drop*", o que fará com que ela não seja enviada ao servidor.



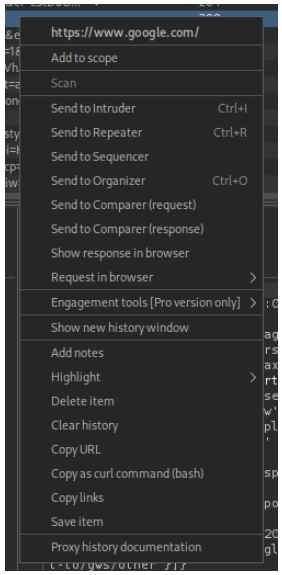
HTTP history

A aba **HTTP history** exibe um histórico de todas as requisições e respostas HTTP interceptadas. Você pode visualizar detalhes de cada requisição, incluindo cabeçalhos, parâmetros e corpo da mensagem. Isso é útil

para analisar o tráfego e identificar vetores de ataque.

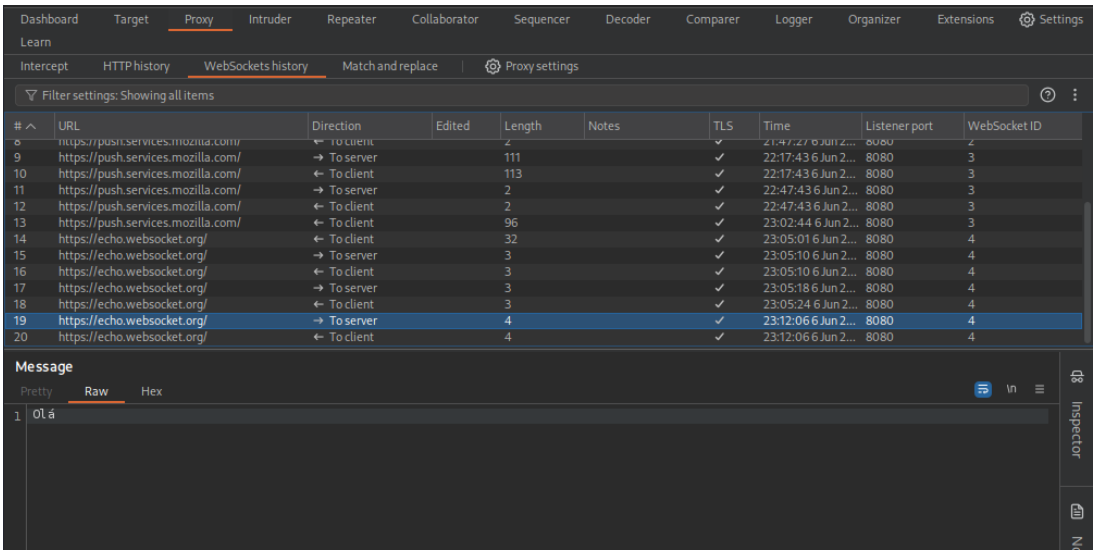


Você pode acessar o menu de contexto clicando com o botão direito em uma requisição específica, permitindo que você a reenvie, edite ou envie para outras ferramentas do Burp Suite, como o **Repeater** ou **Intruder**.



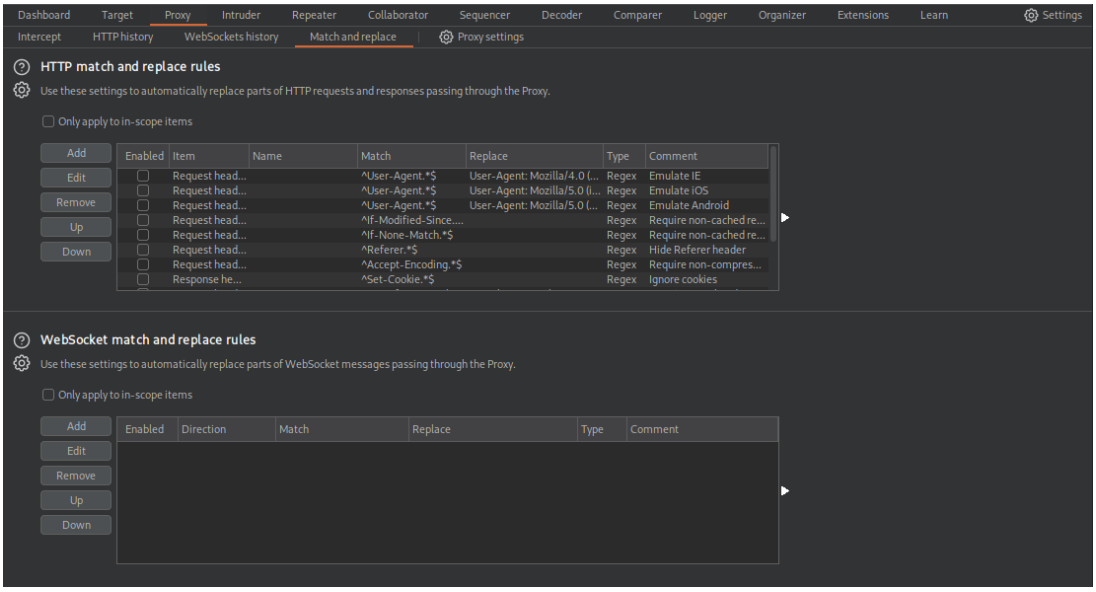
WebSockets history

A aba **WebSockets history** funciona de maneira semelhante ao **HTTP history**, mas é específica para conexões WebSocket. Você pode visualizar as mensagens enviadas e recebidas através de WebSockets. As requisições WebSocket também podem ser interceptadas e modificadas, assim como as requisições HTTP.



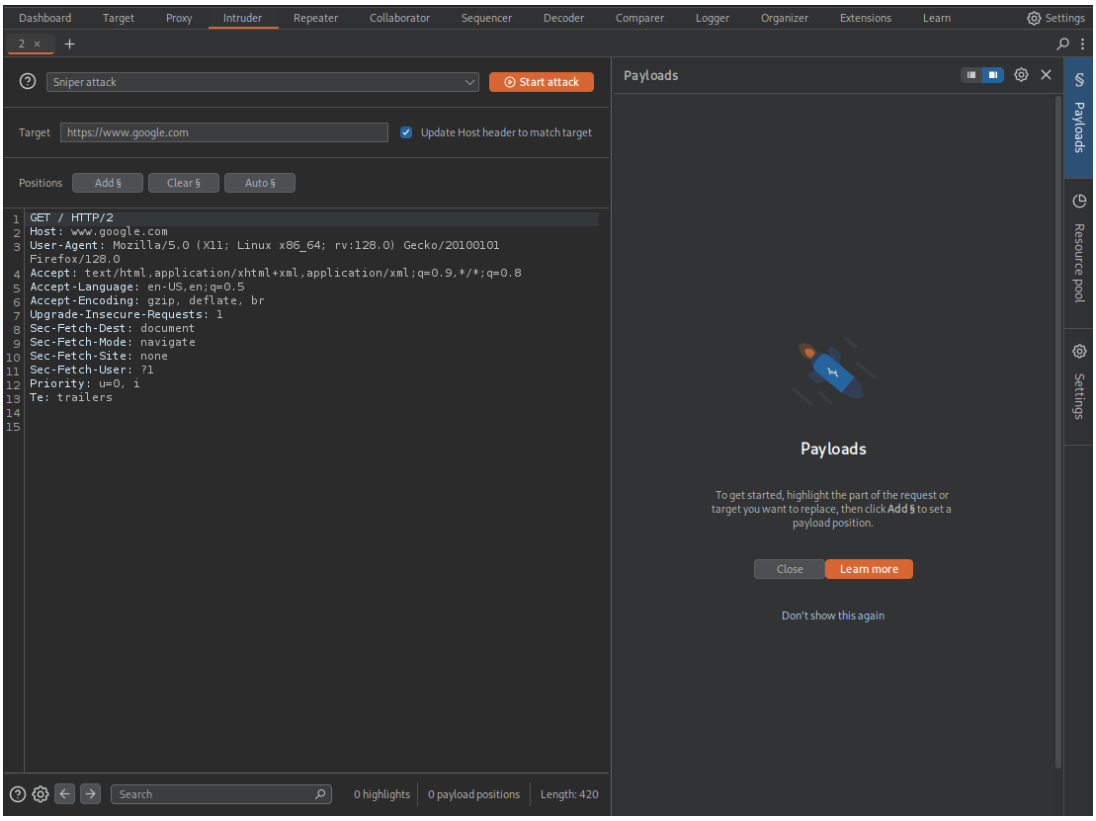
Match and Replace

A aba **Match and Replace** permite que você configure regras para modificar automaticamente requisições e respostas com base em padrões específicos. Isso é útil para automatizar testes e simular diferentes cenários de ataque.

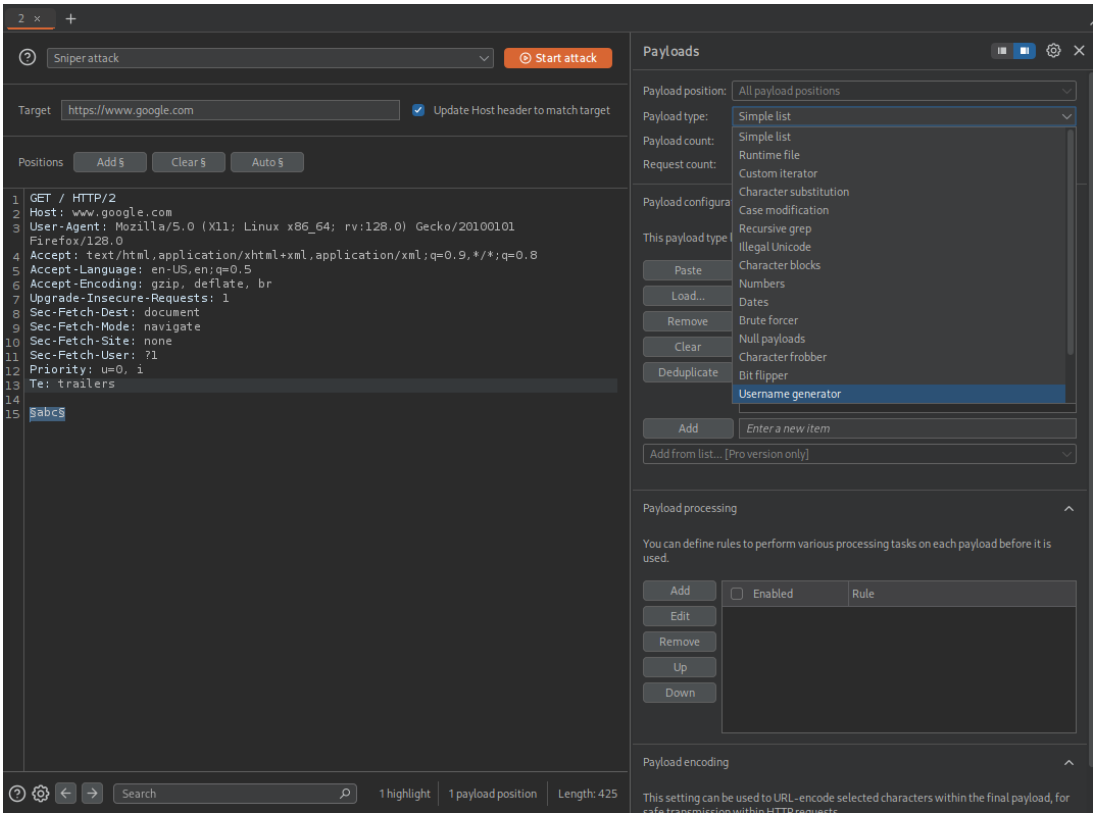


Intruder

O **Intruder** é uma ferramenta poderosa para realizar ataques automatizados, como força bruta e fuzzing. Ele permite que você envie requisições personalizadas com diferentes payloads. Basta selecionar uma requisição no **HTTP history**, clicar com o botão direito e escolher "*Send to Intruder*".



Na aba **Intruder**, você pode definir os pontos de ataque (payload positions) e escolher os payloads que serão usados. Existem várias opções de payloads, como listas de palavras, números sequenciais e mais.



Você tem diferentes modos de ataque:

- **Sniper**: Testa um payload por vez em múltiplas posições.
- **Battering Ram**: Usa o mesmo payload em todas as posições simultaneamente.
- **Pitchfork**: Usa diferentes conjuntos de payloads, iterando simultaneamente.

- **Cluster Bomb**: Testa todas as combinações de múltiplos conjuntos, útil mas pode gerar muitas requisições.

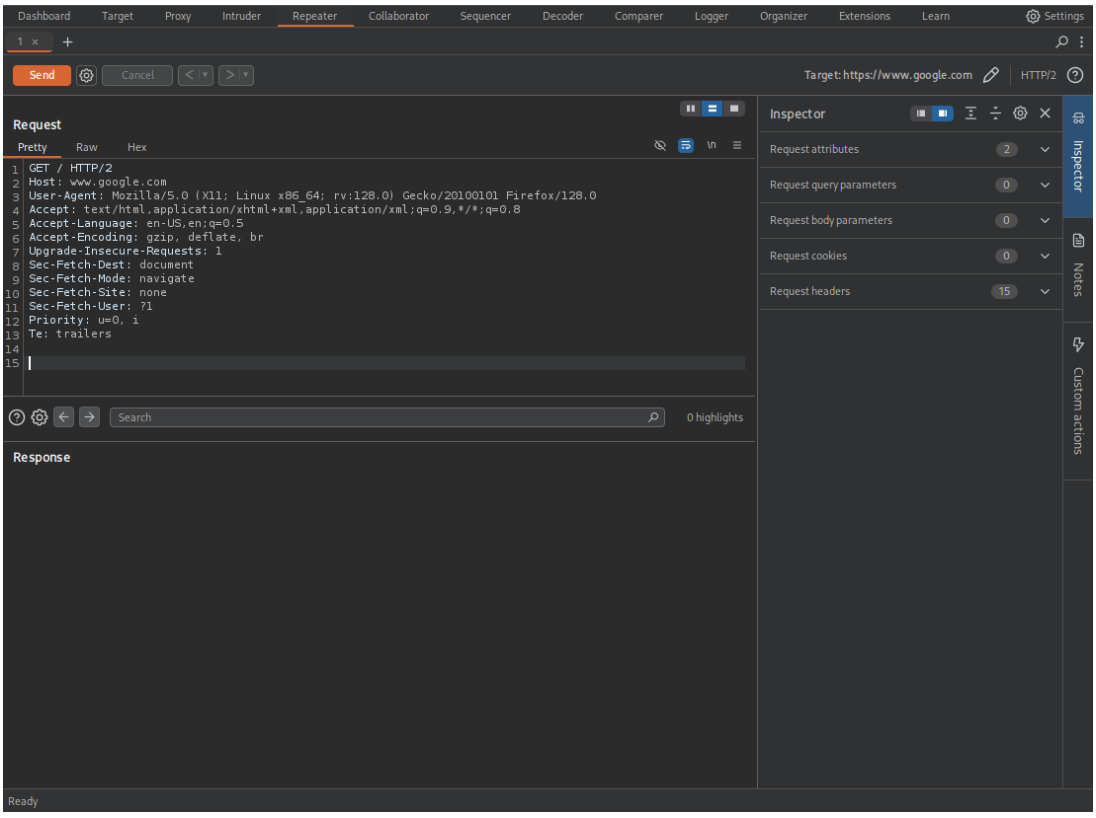
Primeiro, você deve definir as posições dos payloads na requisição. Para isso, selecione a parte da requisição que deseja modificar e clique em "*Add §*" para marcar a posição.

Depois, configure os payloads na aba **Payloads**. Você pode escolher entre diferentes tipos de payloads, como listas de palavras, números sequenciais ou até mesmo criar seus próprios payloads personalizados.

Após configurar os payloads, clique em "*Start attack*" para iniciar o ataque. O Burp Suite irá enviar as requisições e exibir os resultados na aba **Intruder**.

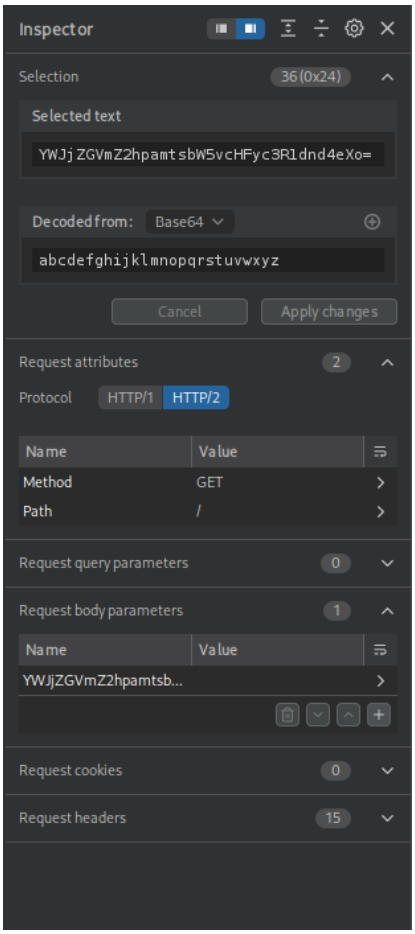
Repeater

O **Repeater** permite que você envie requisições HTTP e WebSocket manualmente, edite e visualize as respostas. Para enviar uma requisição para o Repeater, selecione uma requisição no **HTTP history**, clique com o botão direito e escolha "*Send to Repeater*".



Inspector

Na aba **Inspector**, você pode visualizar e editar os cabeçalhos, parâmetros e corpo da requisição, além de decodificar ou codificar os dados conforme necessário. Isso é útil para testar como a aplicação responde a diferentes entradas.



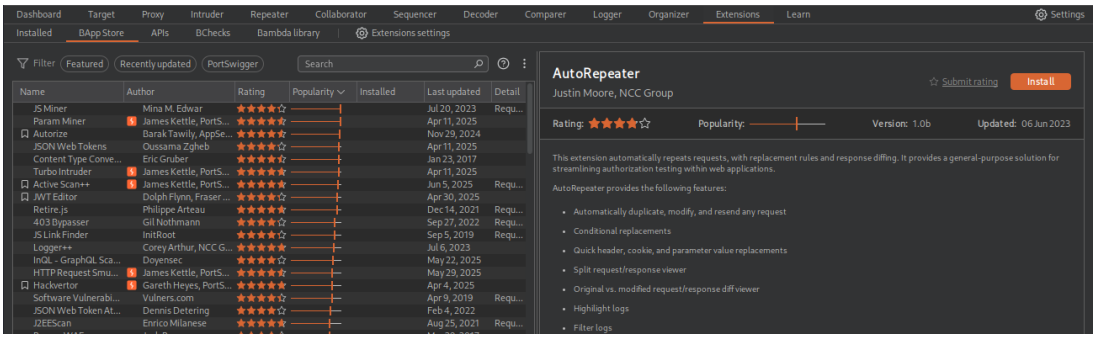
Decoder

O **Decoder** é uma ferramenta para decodificar e codificar dados em diferentes formatos, como Base64, URL encoding, Hexadecimal, entre outros. Você pode colar dados na aba **Decoder** e escolher o formato de decodificação ou codificação desejado.

Extensões

O Burp Suite permite a instalação de extensões para adicionar funcionalidades extras. Você pode acessar o *BApp Store* diretamente na aba **Extensions** e instalar extensões desenvolvidas pela comunidade ou pela PortSwigger.

> *Algumas extensões são somente compatíveis com a versão **Professional** do Burp Suite, mas muitas são disponíveis para a versão **Community**.*



Algumas extensões populares:

- **Autorize**: Ajuda a identificar problemas de autorização em aplicações web.
- **JSON Web Tokens**: Facilita a manipulação e análise de tokens JWT.
- **JS Miner**: Detecta e analisa arquivos JavaScript em aplicações web.

Praticando

https://tryhackme.com/room/burpsuiterepeater
https://tryhackme.com/room/owaspjuiceshop

Links úteis

Download do Burp Suite: https://portswigger.net/burp/communitydownload
Documentação: https://portswigger.net/burp/documentation
Sobre as ferramentas disponíveis: https://portswigger.net/burp/documentation/desktop/tools
Dominando o Burp Suite - Solyd Offensive Security: https://youtu.be/qOJmTB_9-3g
Vídeo resolvendo JuiceShop com Burp Suite: https://youtu.be/QiNLNDSLuJY
Lista de extensões para o Burp Suite: https://github.com/snoopysecurity/awesome-burp-extensions
Caido - Alternativa ao Burp Suite: https://caido.io/
OWASP ZAP - Alternativa Open Source: https://www.zaproxy.org/