Burp Suite

O Burp Suite é um framework baseado em Java projetado para servir como uma solução abrangente para a realização de pentests em aplicações web.

O Burp Suite captura e permite a manipulação de todo o tráfego HTTP /HTTPS entre um navegador e um servidor web.

Principais Recursos: proxy, repeater, intruder, decoder, comparer, sequencer

O painel é dividido em 4 quadrantes:

1. Tasks: Onde é pode ser definidas tarefas em segundo plano
2. Event Log: O registro de eventos fornece informações sobre as ações executadas pelo Burp Suite.
3. Issue Activity: exclusivo do professional, usado para ver as vulnerabilidades identificadas.
4. Advisory: É a seção de aviso, fornece informações mais detalhadas sobres as vulnerabilidades encontradas

Atalhos:

`Ctrl + Shift + D`	Dashboard
`Ctrl + Shift + T`	Target tab
`Ctrl + Shift + P`	Proxy tab
`Ctrl + Shift + I`	Intruder tab
`Ctrl + Shift + R`	Repeater tab

Burp Proxy

Essa ferramenta permite a captura de requisições e respostas entre o usuário e o servidor web alvo. Esse tráfego interceptado pode ser manipulado, enviado

para outras ferramentas para processamento posterior ou explicitamente autorizado a continuar até seu destino.

Quando requisições são feitas através do Burp Proxy , elas são interceptadas e retidas, impedindo que cheguem ao servidor de destino. As requisições aparecem na aba Proxy, permitindo ações adicionais como encaminhamento, descarte, edição ou envio para outros módulos do Burp.

A capacidade de interceptar solicitações permite obtenhamos controle total sobre o tráfego da web.

O Burp Suite captura e registra as requisições feitas através do proxy por padrão, mesmo quando a interceptação está desativada. (Isso pode ser desativado nas configurações caso queira). Também captura e registra a comunicação WebSocket, fornecendo assistência adicional na análise de aplicações web.
Por padrão, o proxy não intercepta as respostas do servidor, a menos que isso seja explicitamente solicitado para cada requisição.

Configurando o Burp Suite Proxy Com FoxyProxy (extensão Firefox):

1. **Instalar o FoxyProxy** em https://addons.mozilla.org/en-US/firefox/addon/foxyproxy-basic/
2. **Acesse as opções do FoxyProxy:** Após a instalação, um botão aparecerá no canto superior direito do navegador Firefox. Clique no botão do FoxyProxy para acessar a janela de opções do FoxyProxy
3. **Criar configuração de proxy do Burp :** Na janela de opções do FoxyProxy, clique no botão **Opções** . Isso abrirá uma nova aba do navegador com as configurações do FoxyProxy. Clique no botão **Adicionar** para criar uma nova configuração de proxy .
4. **Adicionar detalhes do proxy** : Na página "Adicionar proxy ", preencha os seguintes valores:
    - Título: `Burp` (ou qualquer nome de sua preferência)

- IP do proxy: `127.0.0.1`

- Porta: `8080`

5. **Salvar configuração:** Clique em **Salvar** para salvar a configuração do Burp Proxy .
6. **Ativar configuração de proxy :** Clique no ícone do FoxyProxy no canto superior direito do navegador Firefox e selecione a `Burp` configuração. Isso redirecionará o tráfego do seu navegador através do FoxyProxy `127.0.0.1:8080`. Observe que o Burp Suite precisa estar em execução para que seu navegador faça requisições quando essa configuração estiver ativada.
7. **Ative a interceptação de proxy no Burp Suite :** Alterne para o Burp Suite e certifique-se de que a interceptação esteja ativada na guia **Proxy** .
8. **Teste o proxy :** Abra o Firefox e tente acessar um site. Seu navegador ficará travado e o proxy exibirá a requisição HTTP.

Aba Target

Essa aba consiste em três sub-abas:

1. **Site Map**: permite mapear os aplicativos web que estamos visando em uma estrutura de árvore. Cada página visitada enquanto o proxy estiver ativo será exibida no mapa do site. Este recurso permite gerar automaticamente um mapa do site simplesmente navegando pelo aplicativo web.
2. **Issue definition:** fornece uma lista extensa de vulnerabilidades web, completa com descrições e referências.
3. **Scope settings**: possibilita incluir ou excluir domínios/ IPs específicos para definir o escopo do teste. Ao gerenciar o escopo, podemos nos concentrar nos aplicativos web que estamos visando especificamente e evitar a captura de tráfego desnecessário.

Escopo

Podemos restringir o Burp Suite para testar apenas os aplicativos web específicos que desejamos. A maneira mais fácil de fazer isso é alternar para a aba `Target`, clicar com o botão direito do mouse no alvo na lista à esquerda e selecionar `Add To Scope`. O Burp então solicitará que escolhamos se queremos interromper o registro de tudo o que não estiver no escopo e, na maioria dos casos, devemos selecionar `yes`.

No entanto, mesmo que desativemos o registro de tráfego fora do escopo, o proxy ainda interceptará tudo. Para evitar isso, precisamos acessar a subguia **Scope settings** e selecionar a opção `And` `URL` `Is in target scope` em "Request Interception Rules" e “Response Interception Rules”.

Proxy HTTPS

Ao interceptar tráfego HTTP , podemos encontrar um problema ao navegar para sites com TLS habilitado. Por exemplo, ao acessar um site como `https://google.com/`, podemos receber um erro indicando que a Autoridade Certificadora (CA) do PortSwigger não está autorizada a proteger a conexão. Isso ocorre porque o navegador não confia no certificado apresentado pelo Burp Suite .

Para contornar esse problema, podemos adicionar manualmente o certificado da Autoridade Certificadora (CA) PortSwigger à lista de autoridades certificadoras confiáveis do nosso navegador. Veja como fazer:

1. **Baixe o certificado da CA :** Com o Burp Proxy ativado, acesse http ://burp/cert. Isso fará o download de um arquivo chamado `cacert.der`. Salve este arquivo em algum lugar do seu computador.
2. **Para acessar as configurações de certificado do Firefox:** Digite o endereço `about:preferences` na barra de endereços do Firefox e pressione **Enter** . Isso o levará à página de configurações do Firefox. Procure por "certificados" na página e clique no botão **"Exibir certificados "**.
3. **Importe o certificado da CA :** Na janela Gerenciador de Certificados, clique no botão **Importar** . Selecione o `cacert.der` arquivo que você baixou na etapa

anterior.

4. **Configurar a confiança no certificado da CA :** Na janela seguinte, marque a caixa que diz "Confiar nesta CA para identificar sites" e clique em OK.