Burp Suite

Introdução

Burp Suite - Introdução

O Burp Suite é uma plataforma para testes de segurança em aplicações Web desenvolvida pela empresa PortSwigger Ltd. Esta plataforma engloba um conjunto de ferramentas que permite fazer testes de segurança a praticamente todos os componentes das aplicações web modernas.

Isto inclui testes a:

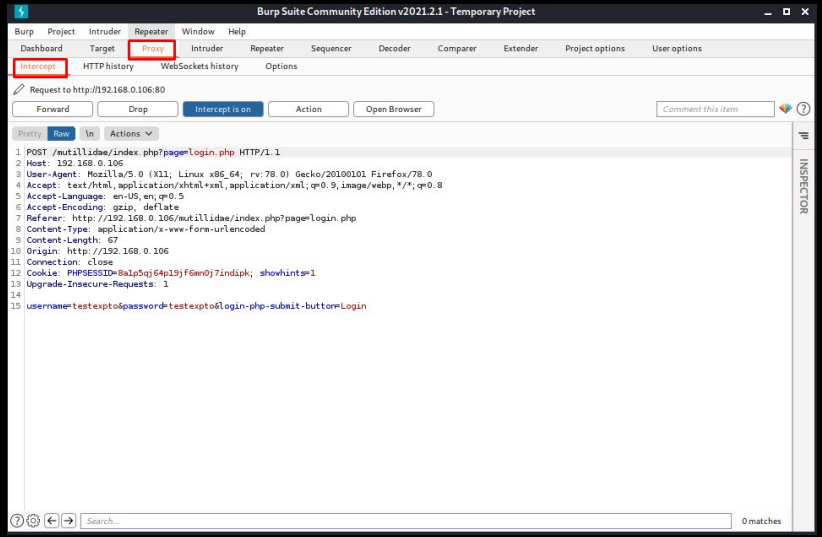
- Mecanismos de autenticação robustos;
- Previsibilidade de tokens de sessão;
- Validação de inputs / entradas presentes na aplicação;

Para além de realização de testes de segurança manuais, a versão Pro (paga) desta plataforma disponibiliza scans automatizados configuráveis para enumeração e análise de tecnologias e vulnerabilidades presentes nas aplicações web.

Burp Suite - Introdução

O Burp é na verdade um proxy web local que permite interceptar, inspecionar e modificar requisições e respostas HTTP trocados entre o browser do usuário e o website a ser testado. Enquanto o usuário navega na aplicação web, esta plataforma recolhe todas as páginas visitadas, scripts, parametros e outros componentes. O tráfego entre o browser do usuário e o website alvo pode eventualmente ser visualizado, analizado, modificado e repetido várias vezes.

Burp Suite - Proxy

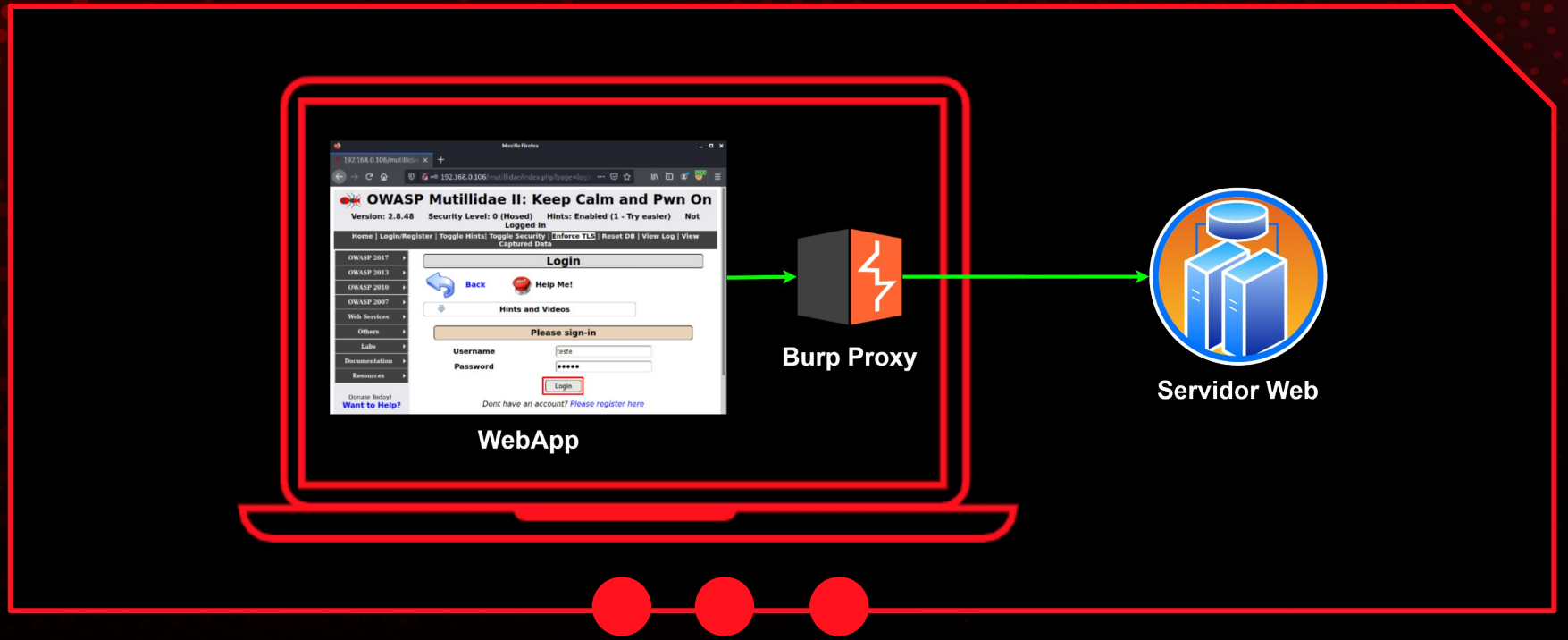


Proxy

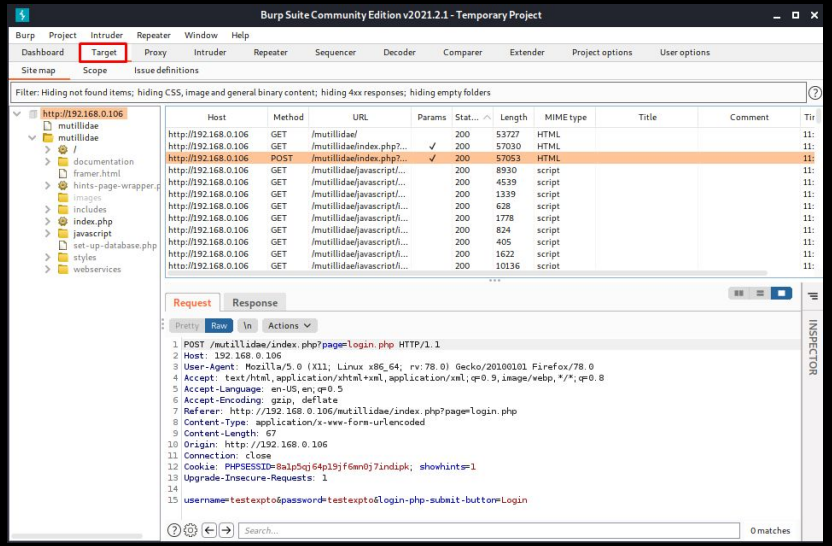
É a ferramenta core do burp suite e, permite interceptar e modificar todo o trafego web.

Na imagem ao lado, interceptamos uma requisição de login, ou seja, o browser enviou a requisição de login para o Burp Suite. Na ferramenta Proxy, podemos visualizar e manipular a requisição consoante os nossos objectivos. Podemos, por exemplo, alterar o "POST" para "GET" e escolher a opção "forward" para encaminhar a requisição para o servidor da aplicação web e analisar a respetiva resposta.

Burp Suite - Proxy



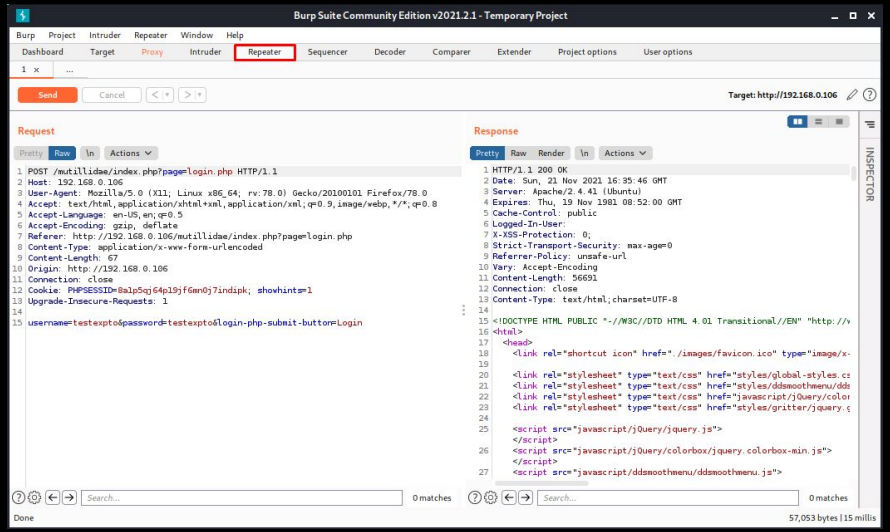
Burp Suite - Target



Target

Quando queremos fazer uma auditoria de segurança a uma ou mais aplicações web específicas, podemos colocar essas aplicações web dentro do "scope" (âmbito). Assim sendo, a ferramenta Target permite agregar todos os recursos das aplicações web que se encontram no âmbito da auditoria. Isto torna o processo dos testes de segurança mais ágil, sendo assim mais fácil situar-nos dentro dos recursos das aplicações web a auditar.

Burp Suite - Repeater

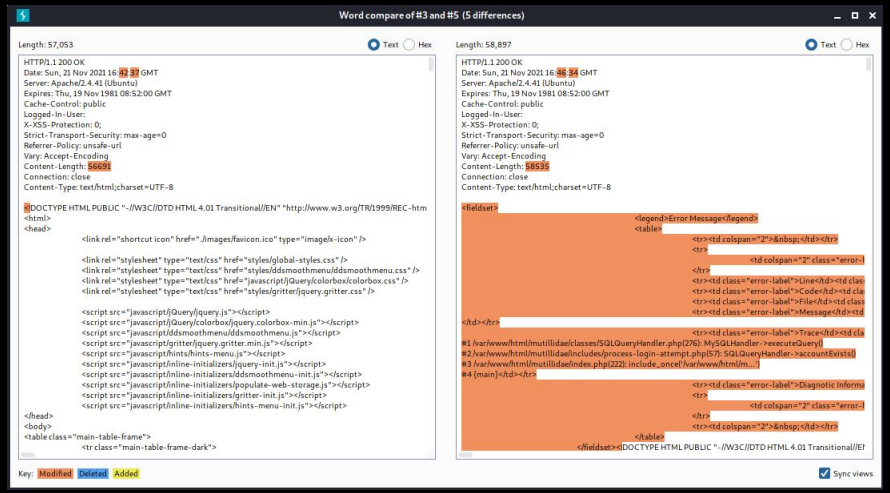


Repeater

Esta ferramenta permite repetir qualquer requisição web interceptada.

Na imagem ao lado, interceptamos uma requisição de login, e enviamos a mesmo para o Repeater. Agora, podemos fazer as modificações que desejarmos, repetir a requisição com essas modificações e analisar a respetiva resposta.

Burp Suite - Comparer



Comparer

Esta ferramenta permite comparar alterações entre páginas web.

Na imagem ao lado, interceptamos uma requisição de login, e enviamos a mesmo para o Repeater. No repeater alteramos a requisição 2 vezes e enviamos as respetivas respostas para a ferramenta Comparer. Esta ferramenta permite-nos analisar as diferenças entre a resposta da primeira requisição submetida no repeater e a resposta da segunda requisição.

Burp Suite - Edições