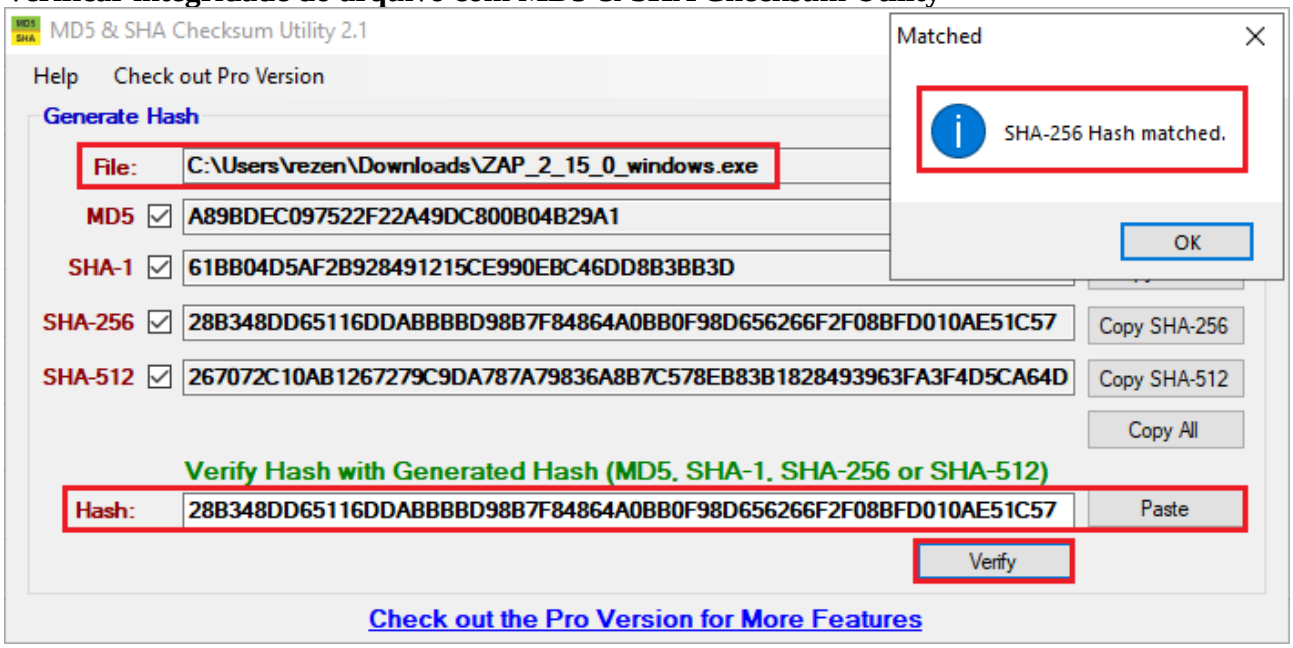
Instalar OWASP-ZAP Zed Attack Proxy no Windows 10/11

1° Acessar o link abaixo e realizar o download da plataforma OpenJDK:
https://adoptium.net/en-GB/temurin/releases/?version=11

2° Acessar o link abaixo e realizar o download da ferramenta ZAP para testes de segurança:
https://www.zaproxy.org/download/

3° Acessar o link abaixo e realizar o download da ferramenta de verificação de integridade de arquivos Checksum (SHA-256):
https://raylin.wordpress.com/downloads/

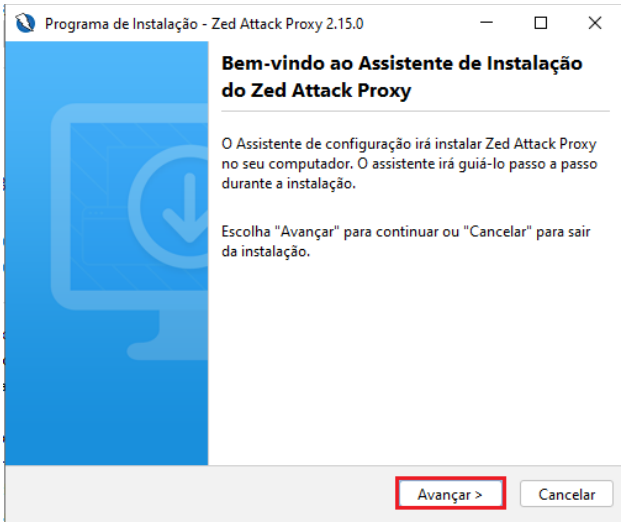
Verificar integridade do arquivo com MD5 & SHA Checksum Utility

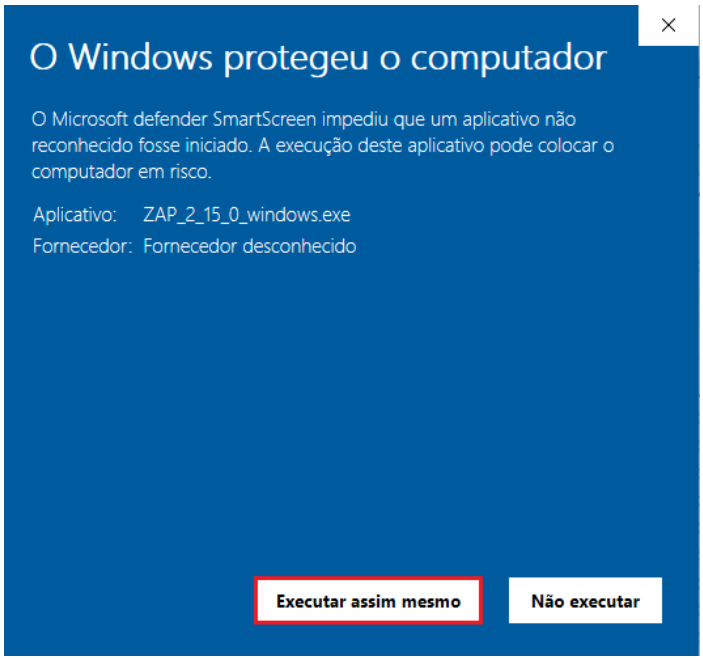


Obs: Verifique hashes com o arquivo correspondente para garantir que a integridade do arquivo esteja correta.

4° Instalar a plataforma OpenJDK e na sequência o ZAP

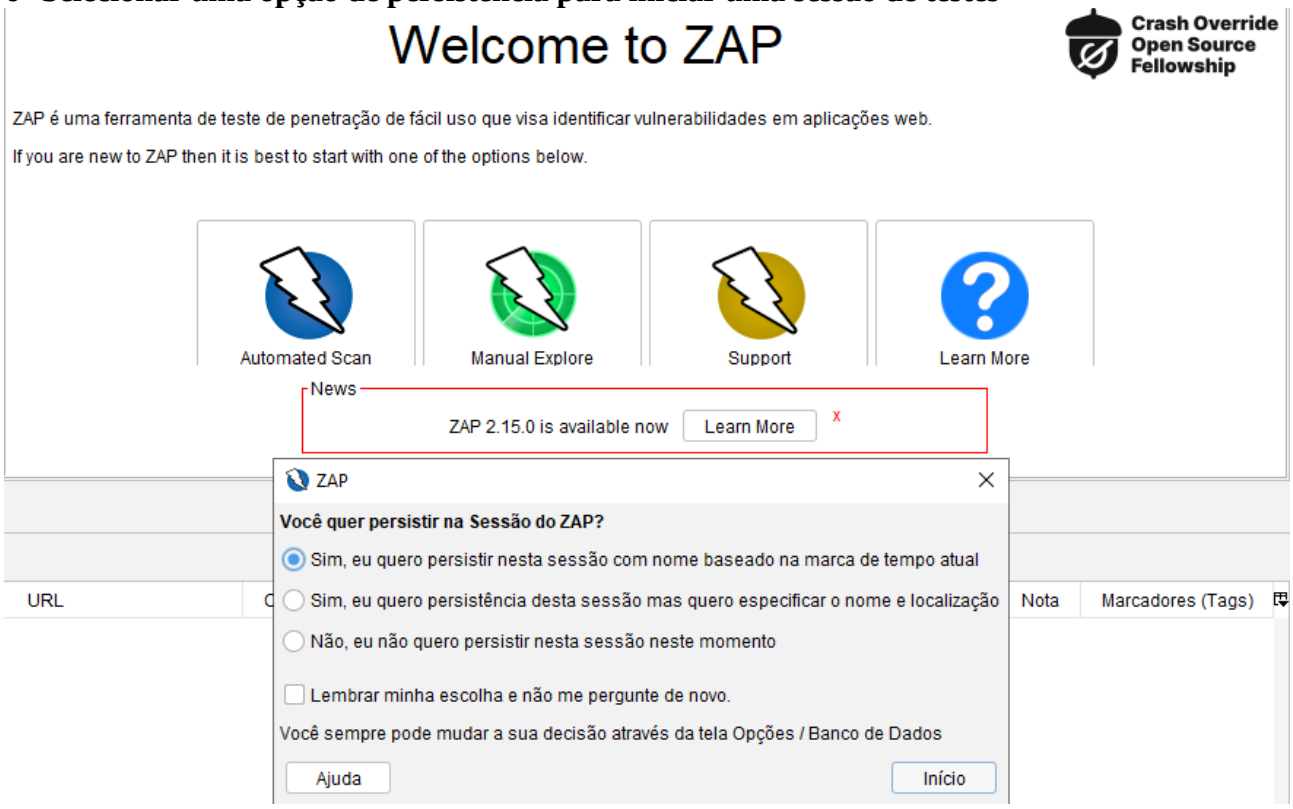
Aceitar a execução no Windows e clicar em avançar:





5° Executar o ZAP clicando no ícone da área de trabalho do Windows

6° Selecionar uma opção de persistência para iniciar uma sessão de testes



Obs: Selecione Não para testes de demonstração e evitar armazenar informações desnecessárias na base de dados do ZAP.

Executar o ZAP nos sites abaixo disponibilizados para testes de ferramentas de segurança:

Para teste automatizado utilize essa URL: http://testphp.vulnweb.com/

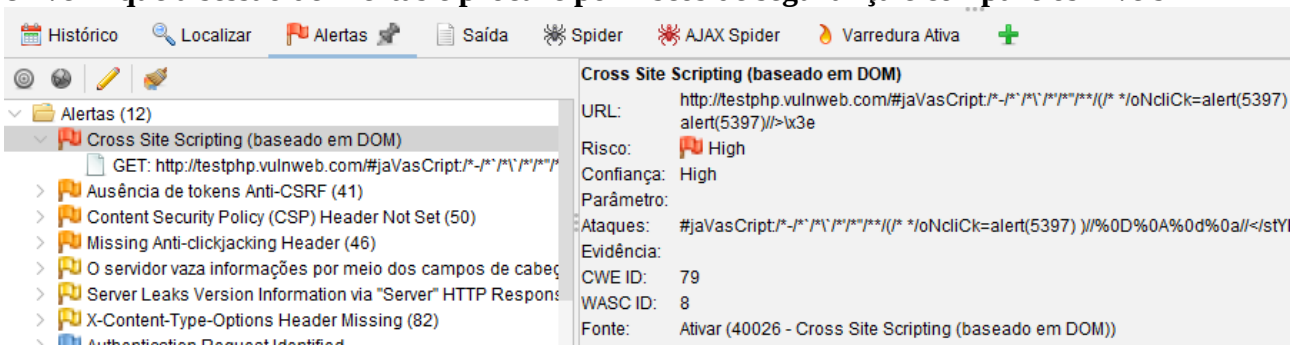
Para exploração manual utilize essa URL: https://pentest-ground.com:81/

Obs: Não utilizar essa ferramente em ambientes, aplicações ou sites sem permissão prévia.

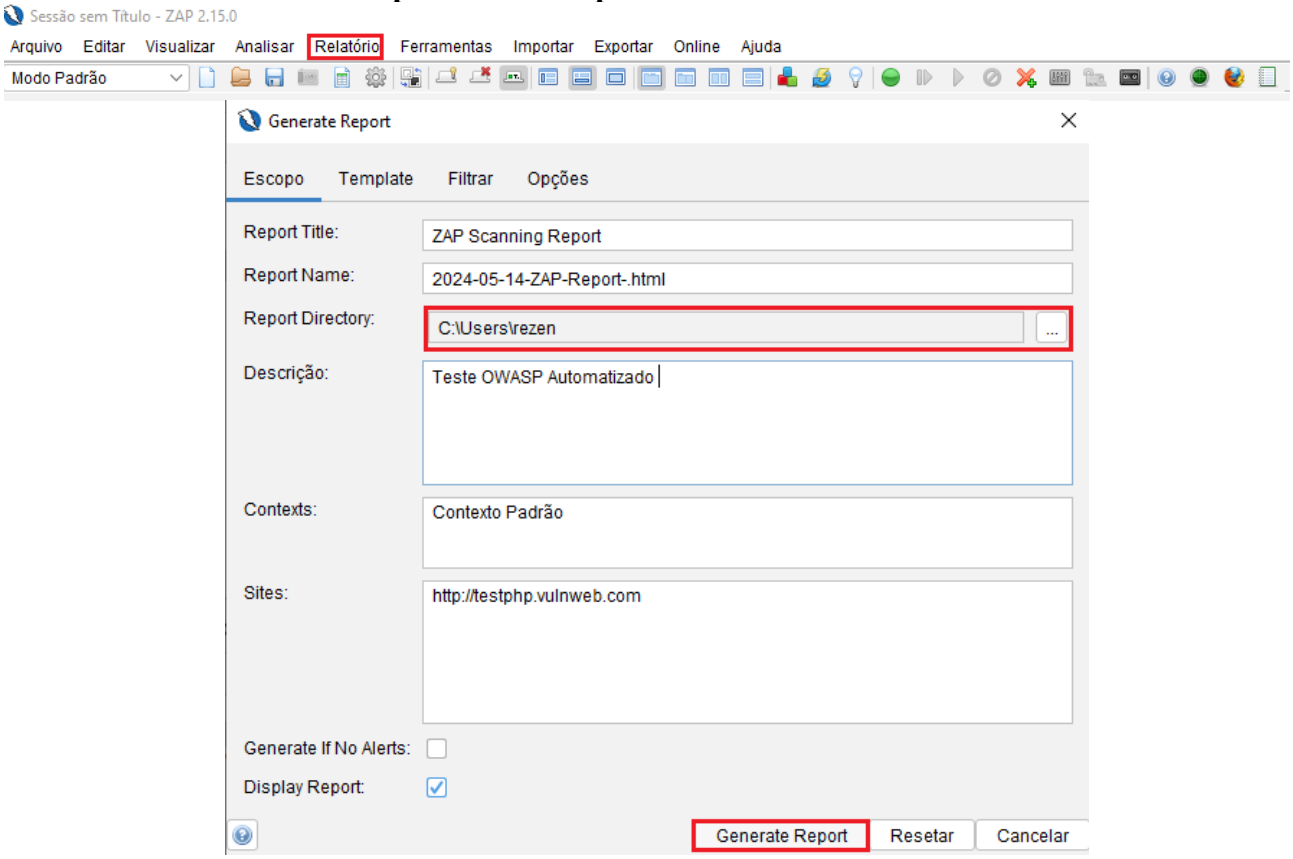
7° Teste automatizado via ZAP

Digite a URL do site que deseja testar, clique no botão Ataque e aguarde até a finalização:

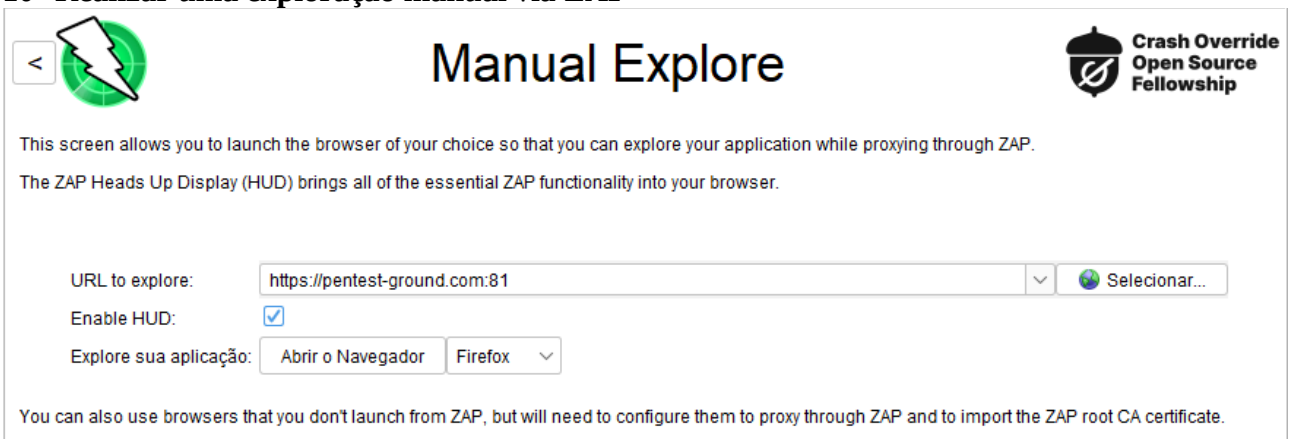
8° Verifique a sessão de Alertas e procure por riscos de segurança e compare os níveis



9° Gere um relatório e salve para consunta posterior

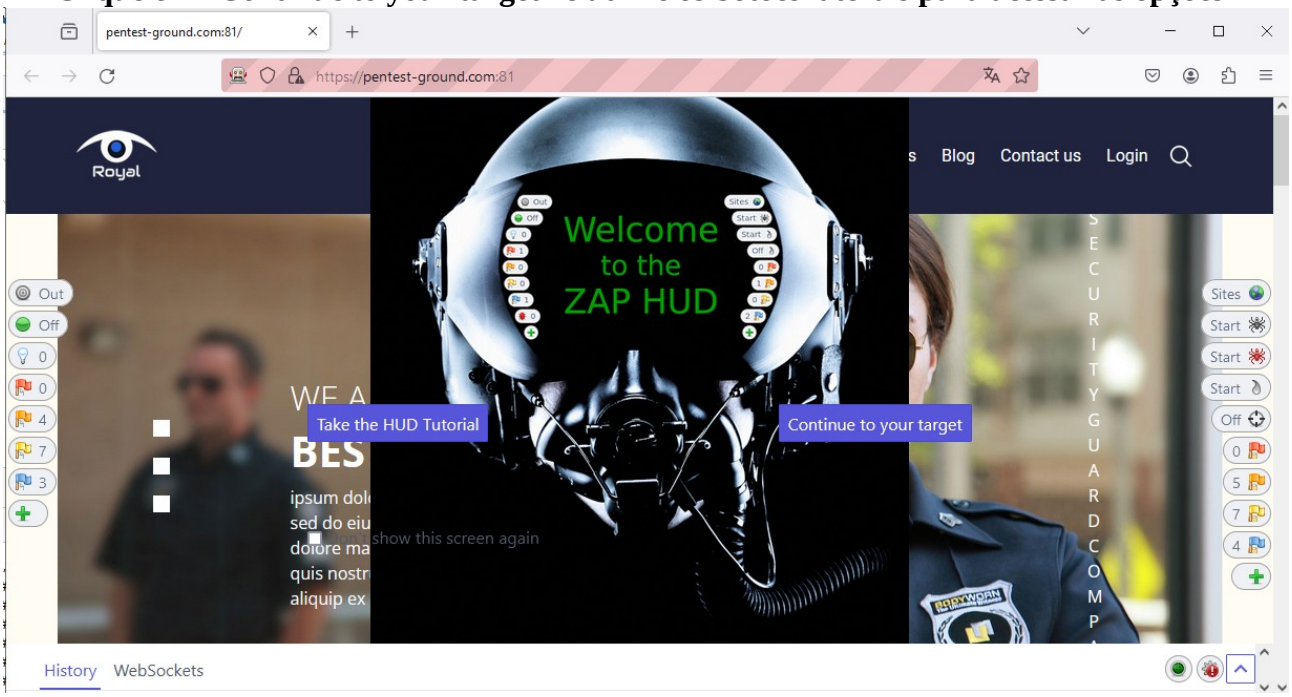


10° Realizar uma exploração manual via ZAP



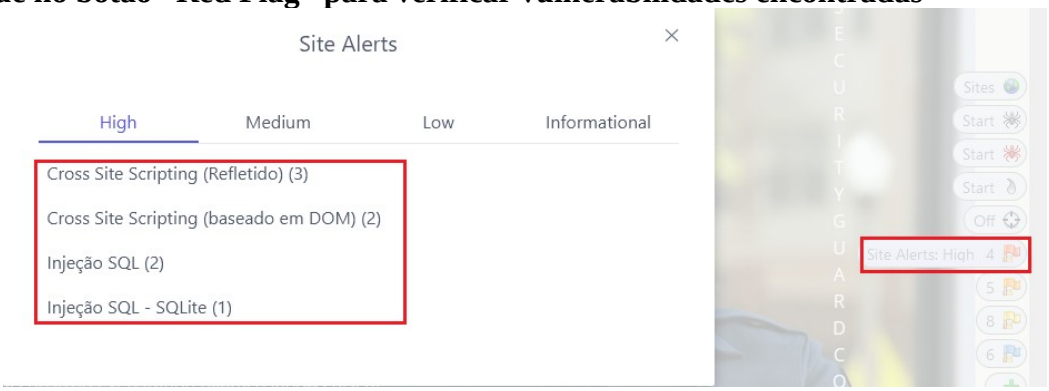
Digite a URL do site/app que deseja testar, marque a opção Enable HUD, clique no botão Abrir o Navegador e aguarde:

11° Clique em "Continue to your target" e utilize os botões laterais para acessar as opções



Clique no botão "**Out**" para adicionar a URL atual no escopo de teste e clique nos botões "**Start**" para executar varreduras de segurança (Spider, Ajax Spider, Active Scan).

12° Clique no botão "Red Flag" para verificar vulnerabilidades encontradas



Obs: Após finalizar os testes é recomendado gerar um relatório para consulta posterior.

Considerações essenciais sobre varreduras com o ZAP

Automated Scan: Primeiro o ZAP realiza uma varredura passiva no aplicativo web ou site com seu módulo Spider, verificando cada página que encontrar na URL do alvo. Assim que finaliza a varredura o ZAP usará o Active Scan para simular um ataque real em todas as páginas, funcionalidades e parâmetros descobertos, não use essa varredura contra alvos que você não tem permissão para testar.

Manual Explore: O ZAP fornece 2 Spiders para rastrear aplicativos web e indexar o conteúdo de sites.

Spider Tradicional: Descobre links examinando linguagem HTML nas respostas da aplicação web. Esse Spider é rápido, mas nem sempre é eficaz ao explorar um aplicativo web interativo que gera links usando JavaScript.

AJAX Spider: Para aplicativos web interativos provavelmente será mais eficaz. Esse spider explora o aplicativo web invocando navegadores que seguem links gerados via JavaScript. O AJAX Spider é mais lento que o tradicional e requer configuração adicional para uso em determinados ambientes.

O ZAP verificará passivamente via Spider todas as solicitações e respostas enviadas por meio dele. A varredura passiva não altera as respostas de forma alguma e é considerada segura. A verificação também é realizada em um “thread” em segundo plano para não retardar a exploração. A varredura passiva é boa para encontrar algumas vulnerabilidades e também como uma forma de ter uma ideia do estado básico de segurança de um aplicativo web ou site.

Active Scan via HUB: A varredura ativa via HUB busca encontrar outras vulnerabilidades usando ataques bem conhecidos contra os alvos selecionados. A varredura ativa é um ataque real a esses alvos e pode colocá-los em risco, portanto, não use a varredura ativa contra alvos que você não tem permissão para testar.

Para informações detalhadas acesse o link: https://www.zaproxy.org/getting-started/

Autor: Sérgio Ricardo de Souza Rezende