11

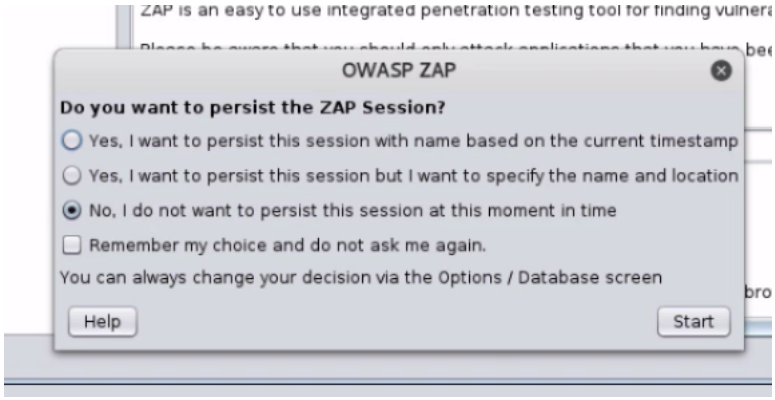
Falhas de segurança - Zap

Transcrição

Já verificamos diversas vulnerabilidades que ocorrem nos sistemas de maneira manual, isto é, por meio de erros e acertos.

Desenvolvedores da **OWASP** criaram a **OWASP ZAP** - uma ferramenta capaz de checar diversas falhas de uma única vez. Na primeira vez que abrirmos a aplicação pode ser que demore um pouco para iniciar, pois além de pesada estamos em um ambiente virtual.

A primeira janela que aparecerá nos questiona sobre manter ou não a sessão, responderemos com "No, I do not want to persist this session at this moment in time":



Lembrando que não podemos utilizar essa ferramenta com sites reais da internet, pois ela é muito intrusiva. A **OWASP ZAP** insere códigos e os testa a fim de verificar a existência de fraquezas nos sites.

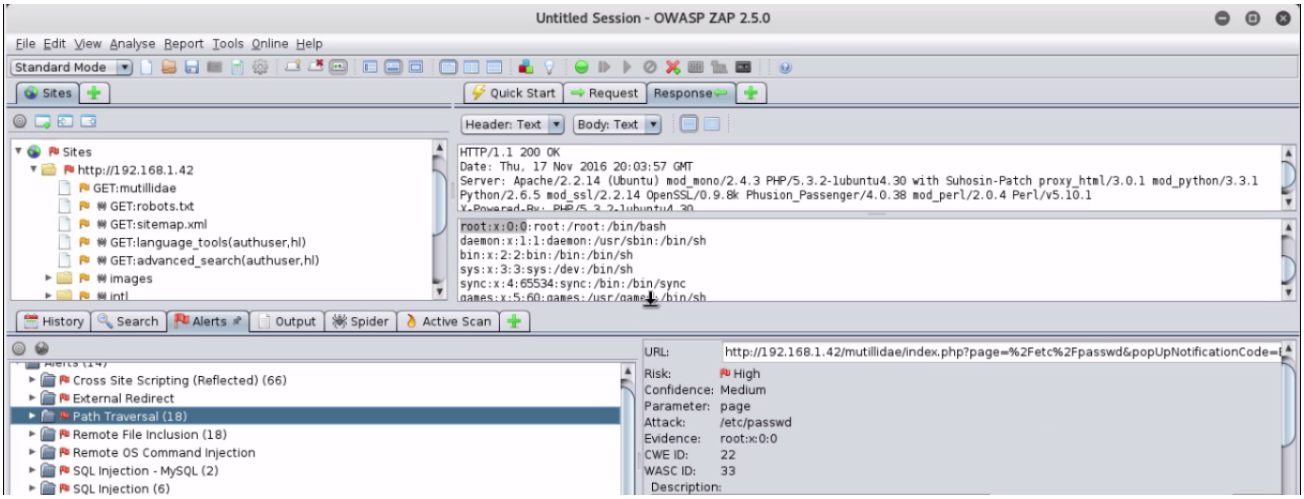
Podemos utilizar, mais uma vez , o site do **Multillidae**. No *OWASP ZAP*, vamos inserir o endereço IP do site que desejamos verificar:

Feito isso basta pressionar o botão *Attack*, o ataque pode demorar um pouco, pois **todas** as vulnerabilidades que vimos neste curso são testadas.

Na aba **Alerts** as fraquezas são definidas conforme os níveis de risco:

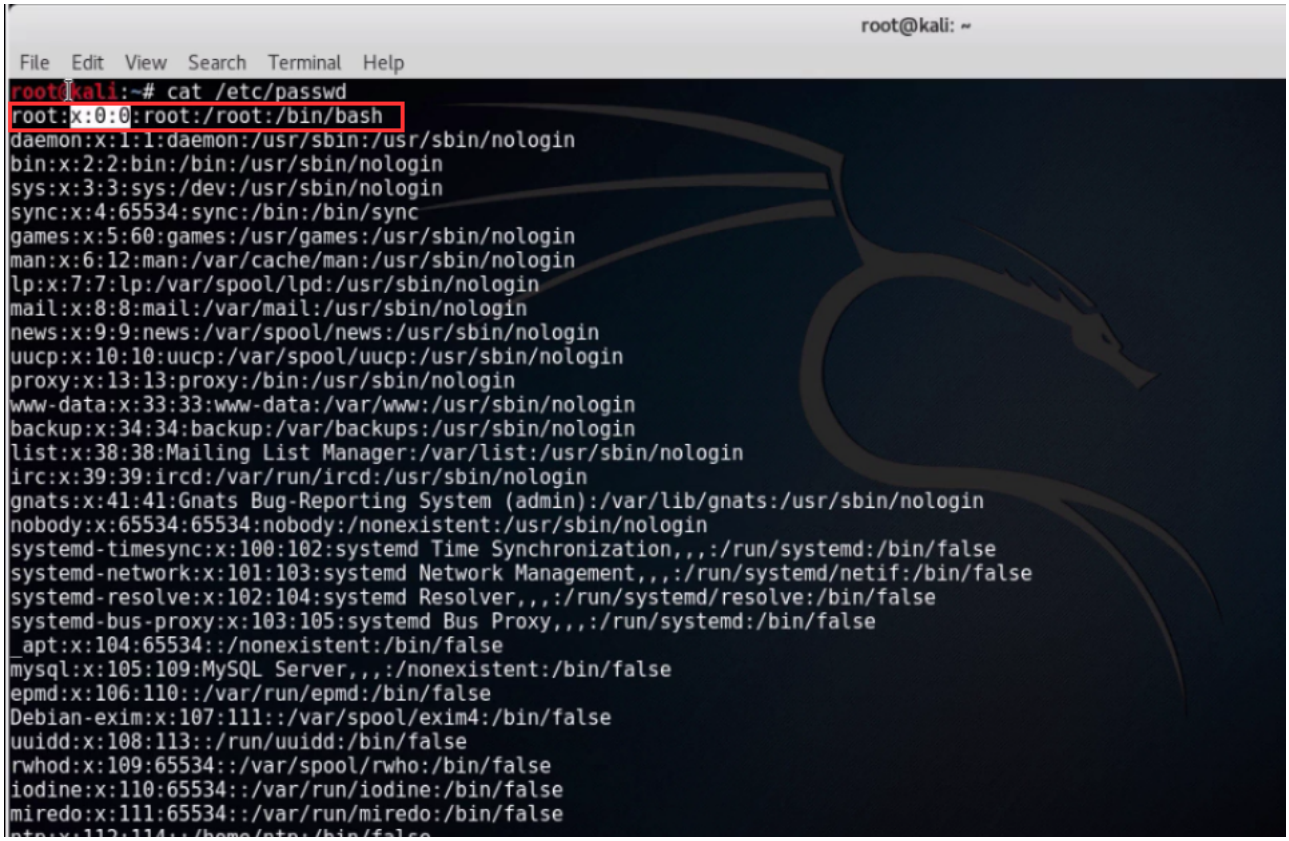
- Bandeira vermelha: Risco alto
- Bandeira azul: não necessariamente um risco, mas sua correção melhora ainda mais o desempenho do site
- Bandeira amarela: Risco mediano

Com o teste finalizado, iremos nos deparar com o seguinte resultado:



Dos resultados obtidos, quase todos nós encontramos quando fizemos verificações manuais. Vamos analisar o **Path Tranversal**, vulnerabilidade que não abordamos até o momento.

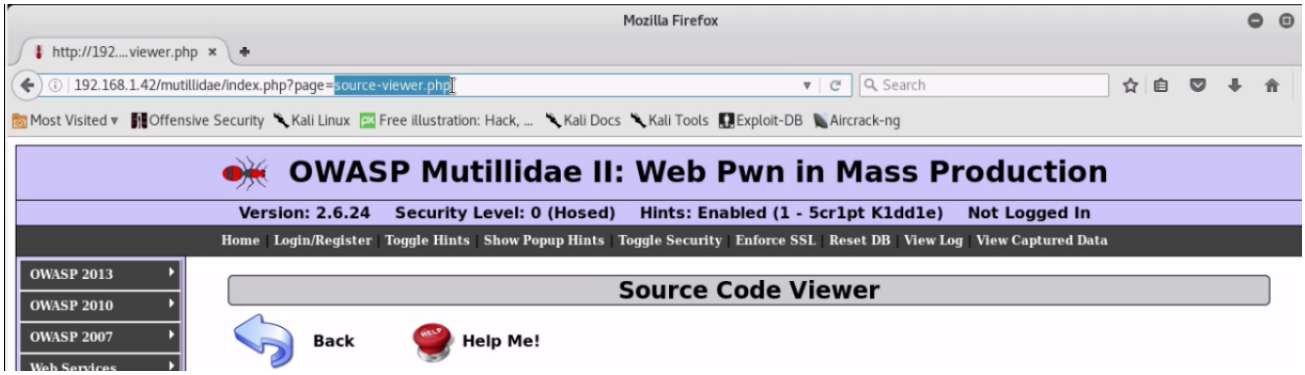
Para verificar o **Path Tranversal**, abriremos o Terminal e usando o Kali Linux digitaremos `cat /etc/password` :



Fazendo isso, temos acesso a diversas informações de diferentes usuários. E isso nas mãos de alguém mal intencionado pode facilitar a realização de um ataque. A primeira informação desta lista é a `-root` e ela está acompanhada de alguns números que são, na verdade, senhas criptografadas.

Assim, com o simples acesso a isso, um *hacker* é capaz de tentar diversos métodos a fim de decifrar a senha escondida.

Vamos retornar à página da **Multillidae** e acessar "OWASP 2013 > A4 - Insecure Direct Object References > Spource Viewer". Repare na URL:

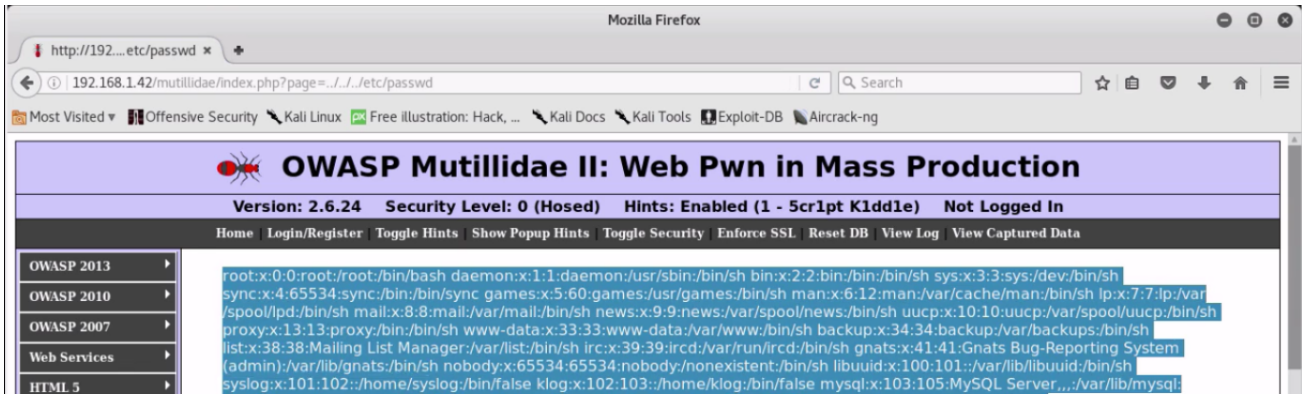


O `index.php` e o `source-viewer` ficam em uma região que é, com certeza, a do diretório `/var/wwww` . Vamos supor que nós estamos no seguinte diretório: `/var/www/html source-viewer.php` . Nós podemos retornar diretórios e acessar o `password` simplesmente escrevendo: `../../../etc/passwd` .

Utilizando isso junto a URL do site teremos no navegador o seguinte :

```
192.168.1.42/multillidae/index.php?page=../../../etc/passwd
```

O que nos mostra a página abaixo:



Ou seja, temos acesso a diversas informações referentes aos usuários. Idealmente um usuário não deveria ser capaz de voltar diretórios até que ele encontre algum arquivo que seja interessante. Mesmo que a senha esteja criptografada, o acesso a esse tipo de dados abre margem para várias ações por parte de hackers.

Retornando a ferramenta do *OWASP*, selecionaremos o item do *Path Traversal*. Ao clicarmos em qualquer requisição vinculada a esse elemento, é possível descobrir em que consiste o ataque em questão. A **OWASP ZAP**, portanto, permite uma grande economia de tempo e esforço, pois, checa diversas vulnerabilidades de maneira automática e todas de uma única vez.