Artigo
Henrique Dias · Dez. 4, 2021 6min de leitura

Open Exchange

Por que? Como? O que é zap-api-scan-sample?

Opa pessoal, tudo bem?

E se você pudesse verificar se sua aplicação REST está suscetível a algum tipo de vulnerabilidade? E se você pudesse verificar se existe algum ataque conhecido que afete sua aplicação?

São com essas questões em mente, que trouxemos nossa aplicação de exemplo usando a ferramenta de testes ZAP. Uma forma de fornecer de maneira rápida, prática e acessível ferramentas para que os desenvolvedores validem questões de segurança com praticidade e de uma maneira acessível.

Por que é importante validar a segurança da sua aplicação?

Cada vez mais, brechas de segurança tem sido exploradas por mais e mais pessoas mal intencionadas. E como desenvolvedores, oferecer segurança para as pessoas que fazem uso de nossa aplicação, faz parte de nosso trabalho.

Como fazer a validação?

Para realizar a validação é necessário seguir os passos abaixo para que sua aplicação REST, tire proveito das funcionalidades e testes de segurança que oferecemos com ZAP. Veja mais abaixo.

Porque optamos pela OWASP?

Optamos por utilizar, OWASP® Foundation, testes criados por especialistas que mantém um repositório de testes de vulnerabilidade constantemente atualizado.

Mas quem é OWASP® Foundation?

Open Web Application Security Project® (OWASP) é uma fundação sem fins lucrativos que trabalha para melhorar a segurança dos softwares. Por meio de projetos de software de código aberto liderados pela comunidade, centenas de divisões locais em todo o mundo, dezenas de milhares de membros e principais conferências educacionais e de treinamento, a Fundação OWASP é a fonte para desenvolvedores e tecnólogos protegerem a

web.

Para o nosso projeto utilizamos OWASP® Zed Attack Proxy (ZAP),
O scanner de aplicativos da web mais usado do mundo. Gratuito e de código aberto. Mantido ativamente por uma equipe internacional dedicada de voluntários.

Mas convenhamos, perderam a chance de nomear o projeto com o nome de quem entende realmente de ataques e invasões: Zod, General Zod!!!

Como fazer uso do ZAP?

Prerequisites

Tenha certeza de possuir git e Docker desktop instalados.

Installation for development with Docker

Faça o Clone/git pull do repositório em um diretório local:

```
$ git clone https://github.com/jrpereirajr/zap-api-scan-sample.git
$ cd zap-api-scan-sample
```

Abra o terminal neste diretório e execute:

```
$ docker-compose up -d --build
```

Nota: como nesta versão, uma transferência de arquivo é usada para permitir que os contêineres se comuniquem entre si, é necessário conceder alguns privilégios para escrever no volume compartilhado:

```
$ chmod 777 -R zap-pool
```

Verificando suas APIs

Este exemplo permite que você verifique cada API REST ou todos eles de uma vez.

Por exemplo, se você gostaria de verificar a API * / crud *, execute este comando:

```
Do ##class(dc.sample.zap.filepool.ZapOpenApiScanService).%New().Print("/crud")
```

Se você gostaria de verificar todas as APIs REST em um namespace - USER, por exemplo, execute este comando:

```
Do ##class(dc.sample.zap.filepool.ZapOpenApiScanService).%New().PrintAllWebApps("USER
")
```

Se você omitir o namespace, o namespace atual será utilizado.

Resultados do scanneamento

Este projeto usa três recursos do ZAP para fornecer relatórios: texto simples, HTML e Markdown.

O texto simples mostra apenas quais testes foram aprovados e quais falharam, bem como um resumo no final. Um código para detalhes sobre a vulnerabilidade OWASP também é apresentado para cada teste.

```
-----------------------------------------
ZAP API Scan for: /crud
-----------------------------------------
2021-11-29 03:44:16,920 Could not find custom hooks file at /home/zap/.zap_hooks.py
2021-11-29 03:44:32,869 Number of Imported URLs: 8
Total of 19 URLs
PASS: Directory Browsing [0]
PASS: Vulnerable JS Library [10003]
PASS: Cookie No HttpOnly Flag [10010]
...
PASS: Loosely Scoped Cookie [90033]
WARN-NEW: Content Security Policy (CSP) Header Not Set [10038] x 6
       http://host.docker.internal:52773/crud/persons/all (401 Unauthorized)
       http://host.docker.internal:52773/crud/ (401 Unauthorized)
       http://host.docker.internal:52773/crud/_spec (401 Unauthorized)
       http://host.docker.internal:52773/crud/persons/id (401 Unauthorized)
       http://host.docker.internal:52773/crud/persons/id (401 Unauthorized)
...
FAIL-NEW: 0     FAIL-INPROG: 0  WARN-NEW: 3     WARN-
INPROG: 0  INFO: 0 IGNORE: 0       PASS: 74
-----------------------------------------
Markdown: /irisdev/app/zap-pool/report-md/6607713456438727.md
HTML: /irisdev/app/zap-pool/report-html/6607713456438727.html
```

Na parte inferior do relatório de texto, o caminho para os relatórios HTML e Markdown é exibido. Esses relatórios são semelhantes e possuem muito mais detalhes, como descrição da vulnerabilidade e uma ajuda rápida para corrigi-los, por exemplo:

Content Security Policy (CSP) Header Not Set

Medium (High)

Description

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

- URL: http://host.docker.internal:52773/crud/persons/id
  - Method: DELETE
  - Parameter: `
  - Attack: `
  - Evidence: `

...

- URL: http://host.docker.internal:52773/crud/persons/id
  - Method: PUT
  - Parameter: `
  - Attack: `
  - Evidence: `

Instances: 6

Solution

Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header, to achieve optimal browser support: "Content-Security-Policy" for Chrome 25+, Firefox 23+ and Safari 7+, "X-Content-Security-Policy" for Firefox 4.0+ and Internet Explorer 10+, and "X-WebKit-CSP" for Chrome 14+ and Safari 6+.

Como isso funciona?

O ZAP possui várias maneiras de realizar testes de segurança, como scripts ou API. Este projeto usou a execução de scripts executados em uma imagem docker oficial do ZAP.

Portanto, para permitir que o contêiner IRIS execute scripts no contêiner ZAP, um volume compartilhado foi configurado no arquivo docker-compose.yaml. Neste volume, o IRIS grava scripts que são detectados e executados pelo contêiner ZAP. Da mesma forma, o contêiner ZAP grava a saída no mesmo volume compartilhado, para que o contêiner IRIS possa lê-los.

Como uma melhoria neste projeto, estou planejando usar a API ZAP no lugar do compartilhamento de arquivos. Também está prevista uma API para execução de testes e apresentação de relatórios diretamente no navegador.

Ideias para uso do ZAP

Podemos utilizar conforme demonstrado no exemplo acima, no entanto, uma ideia que tivemos foi da possibilidade de ter isso integrado dentro do portal de administração.

Onde você poderia selecionar qual aplicação REST passaria pelo teste de vulnerabilidades e segurança.

Ou simplesmente, criar uma tarefa agenda para ser executada de tempos em tempos.

O relatório gerado é simples, direto, objetivo e bem ilustrativo. Também há versão mais detalhada, contendo além de uma descrição das vulnerabilidades encontradas, dicas de como resolver o problema de segurança.

Encerramento

Mais uma vez, gostaríamos de agradecer todo o apoio da comunidade em cada uma das aplicações que criamos.

Se achou interessante nossa aplicação, se pudemos de alguma forma contribuir com algum insight, considere votar em nossa aplicação.

Se você curtiu o aplicativo, curte o que estamos fazendo na comunidade, por favor vote em **zap-api-scan-sample** e nos ajude nessa jornada!
https://openexchange.intersystems.com/contest/current

#InterSystems IRIS
Confira o aplicativo relacionado no InterSystems Open Exchange

URL de origem:https://pt.community.intersystems.com/post/por-que-como-o-que-%C3%A9-zap-api-scan-sample