



SEGURANÇA DE APLICAÇÕES

VISÃO DE APPSEC

AGENDA

- Papel e Contexto do Appsec
- Ferramentas e exemplos de atuação
- Como se tornar Appsec
- Referências

QUEM SOU EU?

- Especialista de Segurança
- Chapter Leader de Appsec
- Formado em Ciência da Computação com MBA em Cibersegurança
- Certificações:
 - AWS Practitioner
 - Comptia Pentest+
 - DCPT
 - ITIL Foundation
- Contatos: linktr.ee/silva_andre

CONTEXTO DE ATUAÇÃO

O QUE É APPSEC

“Appsec é a abreviação de “Application Security” (Segurança de Aplicativos). Refere-se às práticas e tecnologias utilizadas para proteger aplicativos de software contra ameaças e vulnerabilidades de segurança.”

Fonte: ChatGPT Mar 14 version

AMEAÇA, RISCO E VULNERABILIDADE

- **Ameaça:** é um evento ou ação que pode causar danos aos sistemas de informação ou aos ativos da organização. As ameaças podem vir de várias fontes, como hackers, vírus, desastres naturais, erro humano ou sabotagem.
- **Risco:** é a probabilidade de que uma ameaça se torne realidade e cause danos à organização. Os riscos são avaliados com base na probabilidade de ocorrência e no impacto potencial em caso de ocorrência.
- **Vulnerabilidade:** é uma fraqueza ou falha em um sistema de informação que pode ser explorada por uma ameaça para causar danos. As vulnerabilidades podem existir em software, hardware, processos de negócios ou na equipe de TI.

DEVOPS E DEVSECOPS

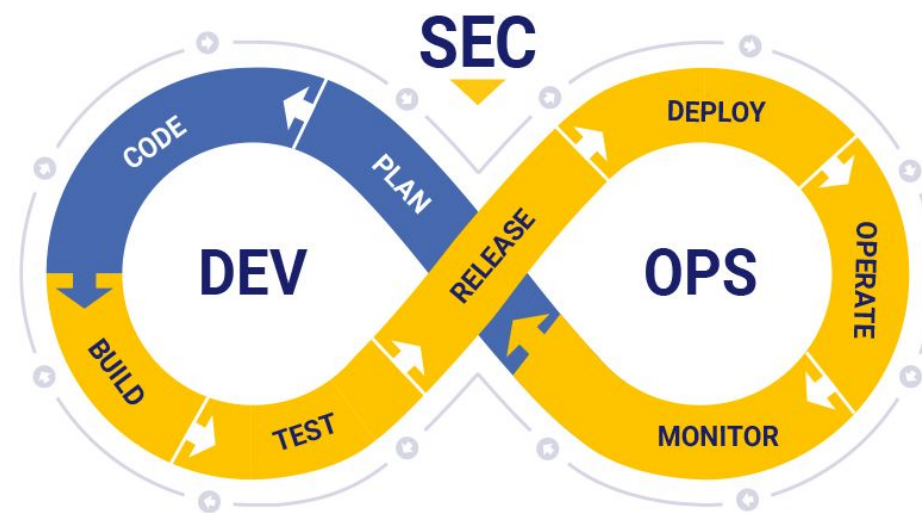
“DevSecOps significa desenvolvimento, segurança e operações. É uma abordagem à cultura, automação e design da plataforma que integra segurança ao DevOps como uma responsabilidade compartilhada em todo o ciclo de vida da TI.”



DevSecOps Maturity Self-Assessment

SECURITY SHIFT LEFT

Implementar medidas de segurança durante o processo completo de Desenvolvimento, melhor que no final, evitando a criação de vulnerabilidades e consequentemente a necessidade de corrigi-las.



PAPEL DO APPSEC

- PPC (Pesquisar, Prevenir e Corrigir) vulnerabilidades de aplicações.
- Atua em níveis diferentes (hardware, software e processos de desenvolvimento)
- É envolvido do início ao fim de um projeto (Modelagem de Ameaças, *AST, etc)
- Ficamos como parte do “Purple Team” dentro do escopo de times de Segurança da Informação

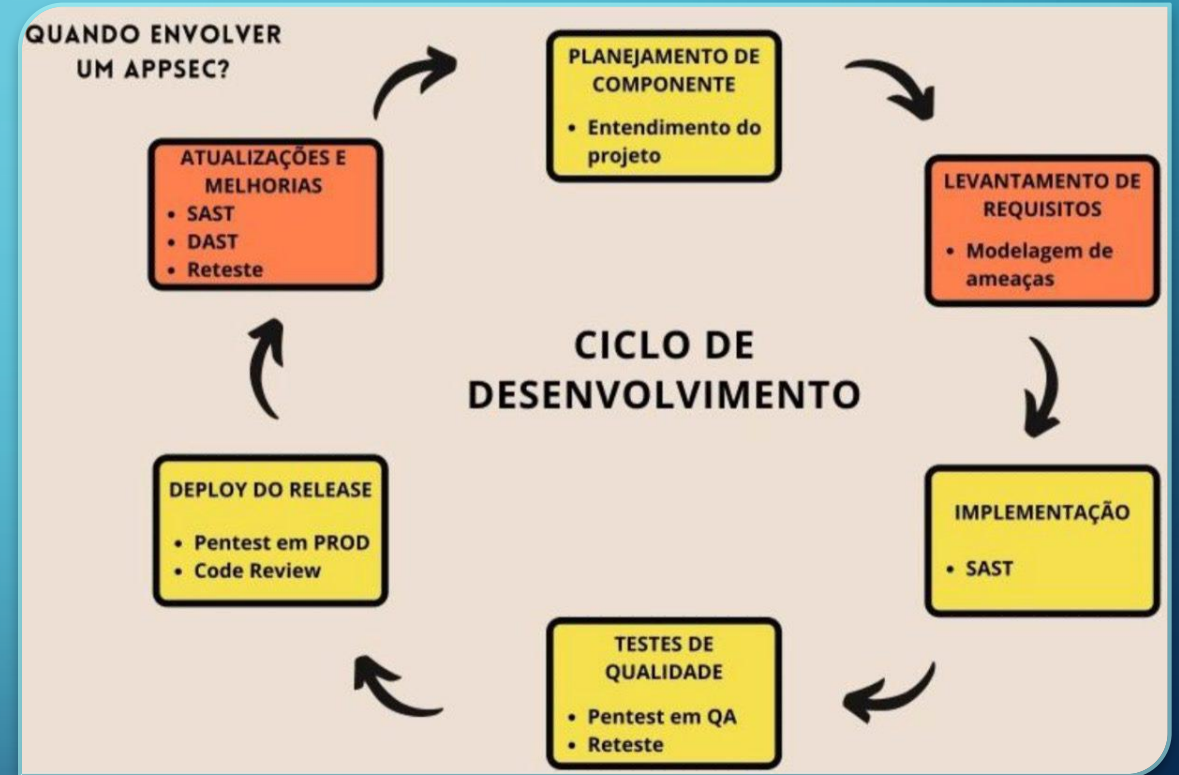


S-SDLC

- A principal atuação de um Appsec é na **Esteira de Desenvolvimento Seguro**, pensando sempre em trazer a **Segurança para o começo do processo**.

- Ciclo de Vida do Desenvolvimento:

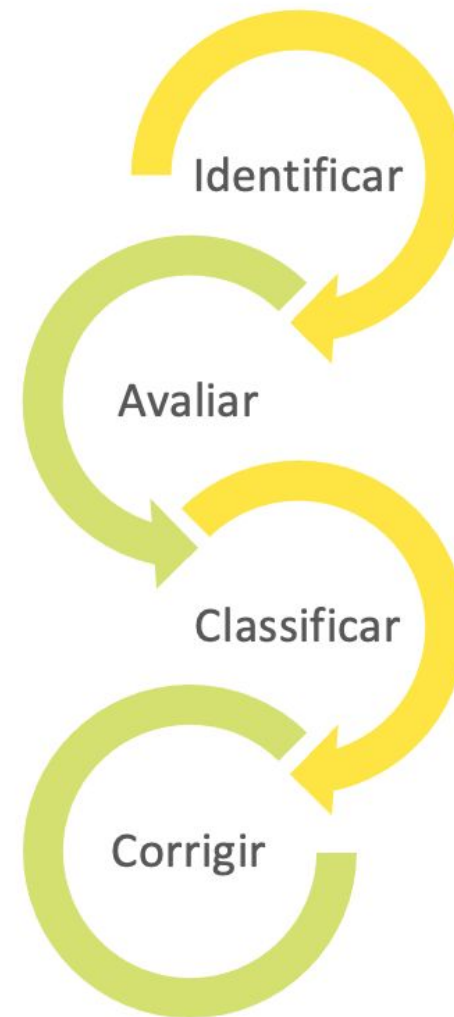
- Modelagem de Ameaças
- SAST
- DAST
- Pentest*



GESTÃO DE VULNERABILIDADES

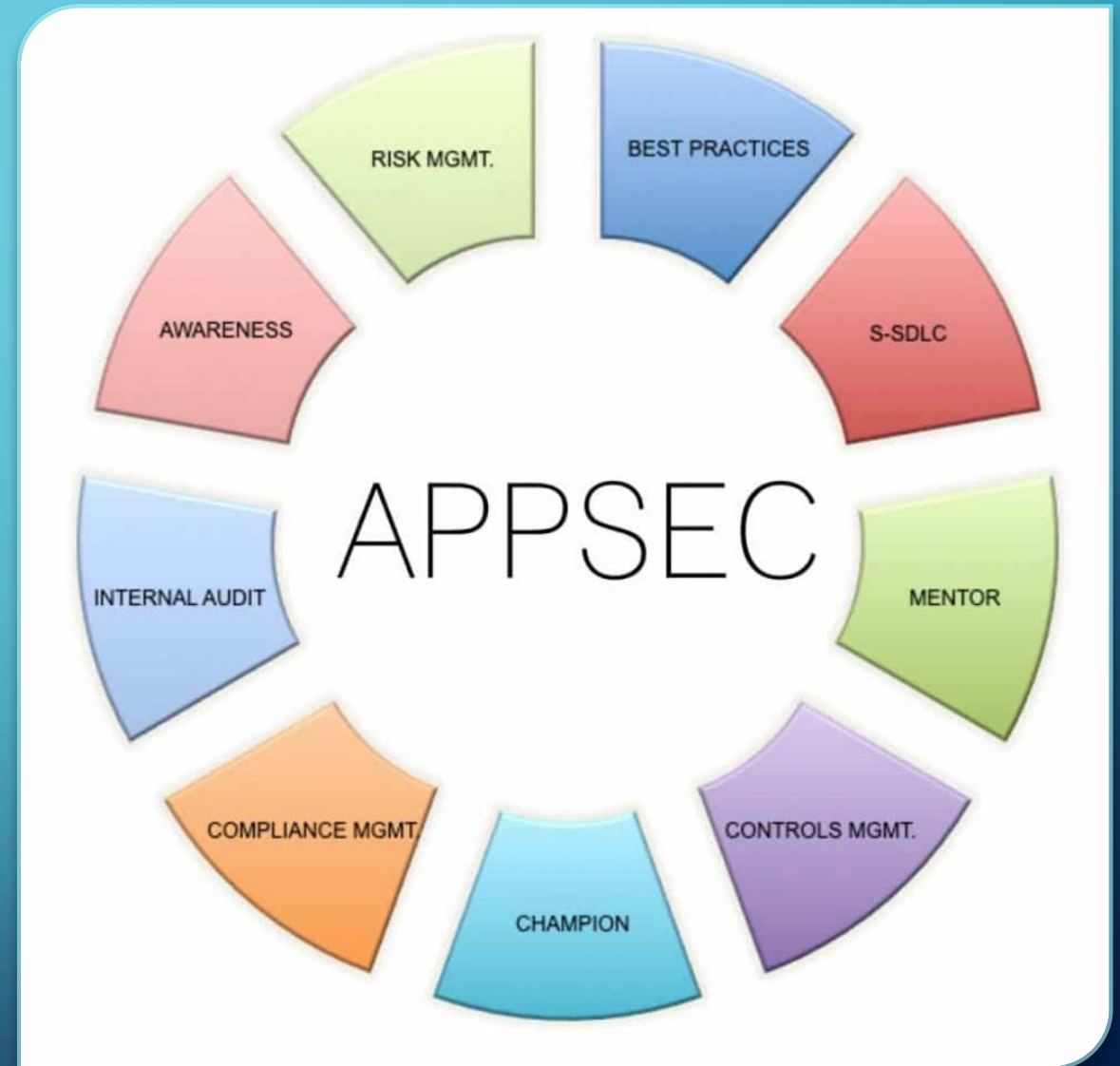
- Idealmente trabalhamos para **evitar que vulnerabilidades seja criadas (modelagem de ameaças)** e quando isso não é possível, como resultado dos testes executados, temos o **registro e gestão das vulnerabilidades**.
- Trabalho conjunto com a Eng. Software:
 - Mitigar
 - Corrigir
 - Aceitar o risco

Gestão de Vulnerabilidades



INTEGRAÇÃO COM AS DEMAIS ÁREAS

- Desafios com times técnicos e negócio:
 - Explicar sobre vulns e correções
 - Agregar e direcionar
 - “Soft skill” de comunicação
- Integração com as demais áreas de Segurança:
 - Blue e Red Teams
 - Governança
 - Riscos
 - Auditoria

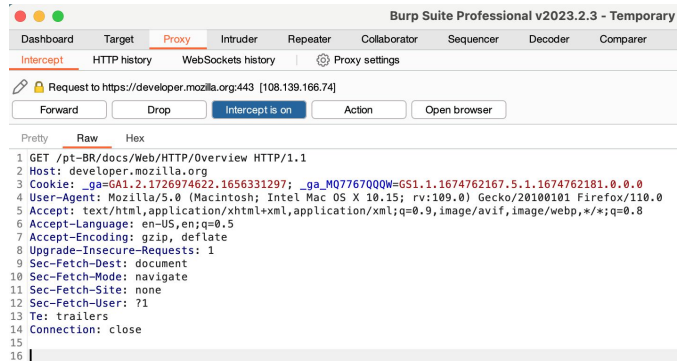


The background is a gradient of blue, darker at the bottom. In the four corners, there are decorative white line-art patterns resembling circuit traces or neural network connections, with small circles at the end of the lines.

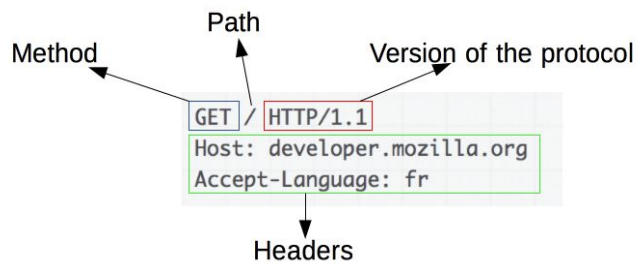
EXEMPLOS E FERRAMENTAS

PROTOCOLO HTTP

“É um protocolo que permite a obtenção de recursos, como documentos HTML. É a base de qualquer troca de dados na Web e um protocolo cliente-servidor, o que significa que as requisições são iniciadas pelo destinatário, geralmente um navegador da Web.”

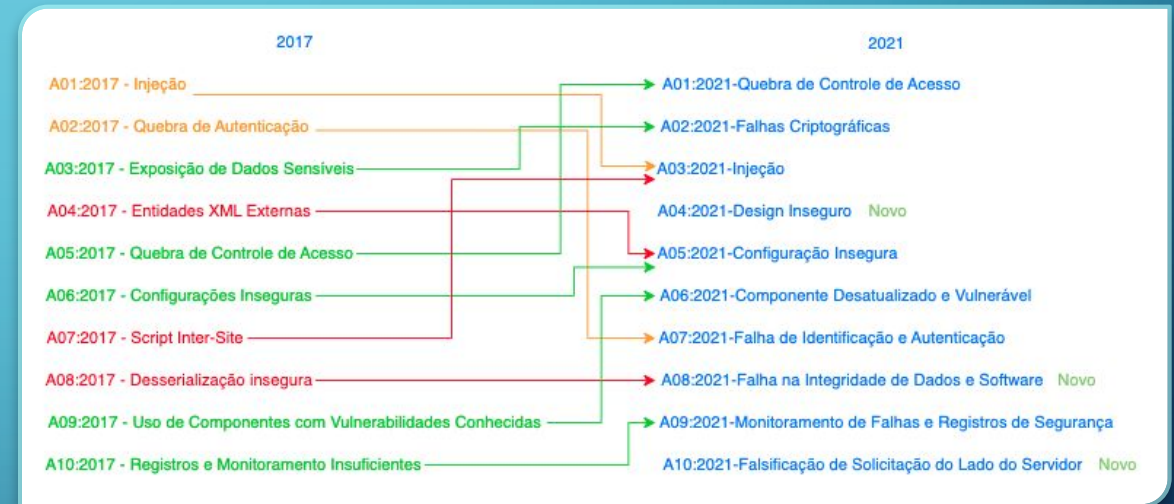


```
1 GET /pt-BR/docs/Web/HTTP/Overview HTTP/1.1
2 Host: developer.mozilla.org
3 Cookie: _ga=GA1.2.1726974622.1656331297; _ga_M0776700QW=GS1.1.1674762167.5.1.1674762181.0.0.0
4 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/110.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Upgrade-Insecure-Requests: 1
9 Sec-Fetch-Dest: document
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-Site: none
12 Sec-Fetch-User: ?1
13 Te: trailers
14 Connection: close
15
16
```



OWASP TOP 10

“The OWASP Top 10 is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications.”



SEGURANÇA E PRIVACIDADE POR DESIGN

- *“A privacidade por design garante que boas práticas de privacidade sejam incorporadas à tomada de decisões de sua organização, bem como ao design e estrutura de seus sistemas de informação, processos de negócios, produtos e serviços.”*
- *“Segurança por design é uma abordagem de garantia de segurança que permite aos clientes, automatizar controles de segurança e simplificar auditoria. É uma abordagem sistemática para garantir a segurança; fornecendo a você a capacidade de criar controle de segurança em todo o processo de desenvolvimento.”*



THREAT MODELING MANIFESTO

What is threat modeling?

Threat modeling is analyzing representations of a system to highlight concerns about security and privacy characteristics.

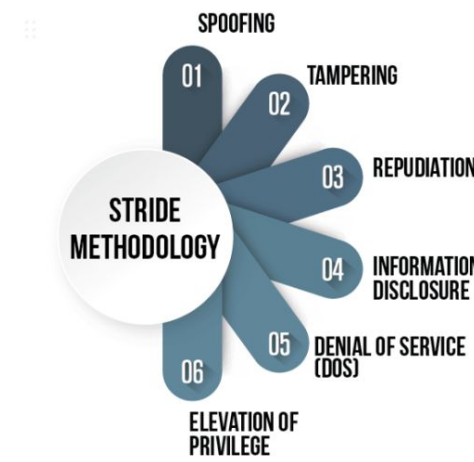
At the highest levels, when we threat model, we ask four key questions:

1. What are we working on?
2. What can go wrong?
3. What are we going to do about it?
4. Did we do a good enough job?

THREAT MODELING MANIFESTO

FRAMEWORKS PARA MODELAGEM

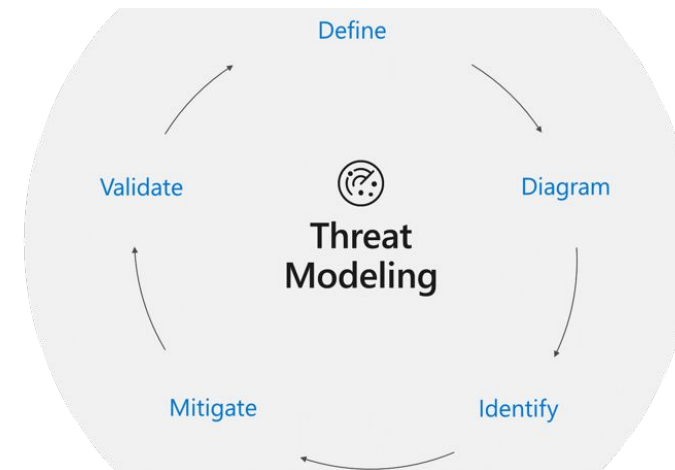
Além desses, temos outros frameworks que Podem nos ajudar na hora de realizar a Modelagem, exemplo: MITRE Att&ck, PASTA, TRIKE, VAST e OCTAVE



DREAD Methodology

D AMAGE	Impact of an Attack
R EPRODUCIBILITY	How Easily the Attack can be Reproduced?
E XPLOITABILITY	How Easy it is to Launch the Attack
A FFECTED USERS	How Many Users will be Impacted
D ISCOVERABILITY	How easily the vulnerability can be found

MICROSOFT THREAT MODELING TOOL

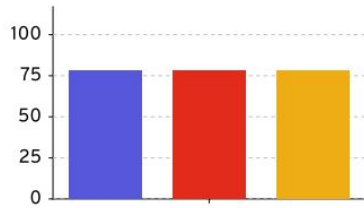


The screenshot shows the Microsoft Threat Modeling Tool interface. At the top, there's a title bar "New Threat Model - Microsoft Threat Modeling Tool (Preview)". Below it is a menu bar with "File", "Edit", "View", "Settings", "Diagram", "Reports", and "Help". The main workspace displays a sequence diagram with nodes: "Human User", "Command", "Web Server", "Configuration", and "Generic Data Store". Below the diagram is a "Threat List" table with columns for ID, Diagram, Changed By, Last Modified, State, Title, Category, Description, Justification, Interaction, and Priority. The table contains 8 rows of threat data. At the bottom, there's a "Threat Properties" section with the text "No threats are selected".

ID	Diagram	Changed By	Last Modified	State	Title	Category	Description	Justification	Interaction	Priority
0	Diagram 1	Generated	Not Started	Specifying Res...	Specifying	Human User...	Command	High	Command	High
1	Diagram 1	Generated	Not Started	Create the Ser...	Interpreting	The web serv...	Command	High	Command	High
2	Diagram 1	Generated	Not Started	Enumerate the...	Enumerate th...	Web Server...	Command	High	Command	High
3	Diagram 1	Generated	Not Started	Specifying of...	Specifying	Generic Data...	Configuration	High	Configuration	High
4	Diagram 1	Generated	Not Started	Potential fac...	Denial Of Ser...	Denial Web Ser...	Configuration	High	Configuration	High
5	Diagram 1	Generated	Not Started	Specifying of...	Specifying	Generic Data...	Results	High	Results	High
6	Diagram 1	Generated	Not Started	Create the Ser...	Interpreting	The web serv...	Results	High	Results	High
7	Diagram 1	Generated	Not Started	Enumerate the...	Enumerate th...	The web serv...	Results	High	Results	High
8	Diagram 1	Generated	Not Started	Weak Access...	Interpreting...	Interpreting de...	Results	High	Results	High

IRIUS RISK

Current Risk Summary



Description	Risk Rating
The Inherent Risk before countermeasures were applied	Critical
The Projected Risk is the level of risk that would be reached should the required countermeasures be implemented	Critical
The Current Risk is based on the current implementation status of the countermeasures and test results	Critical

Component: AWS ECS (Elastic Container Service)

Threat name	Inh. risk	State	Control name	Status	Res. risk	Proj. risk
Use case: Authorization						
Attackers gain unauthorized access to the control of the environment	High	Expose	Control access to Amazon ECS using IAM policies	Recommended	High	High
Use case: General						
Attackers gain unauthorized access to data on EC2 instances	High	Expose	Update the Amazon ECS container agent	Recommended	High	High
Use case: Logging and Monitoring						
Exploitation of insufficient logging and monitoring	Medium	Expose	Enable Amazon ECS CloudWatch Container Insights	Recommended	Medium	Medium
			Create CloudWatch alarms for Amazon ECS metrics	Recommended	Medium	Medium
			Enable the awslogs log driver for containers	Recommended	Medium	Medium
Use case: Networking						
Attackers gain unauthorized network access	Medium	Expose	Connect to ECS using an Interface VPC Endpoint	Recommended	Medium	Medium
			Use VPC security groups	Recommended	Medium	Medium
			Tag all resources	Recommended	Medium	Medium

*AST

Existem diversos tipos de testes automatizados:

- DAST – Dynamic Application Security Testing
- SAST – Static Application Security Testing
- SCA – Software Composition Analysis
- RASP – Runtime Application Self-Protection
- IAST – Interactive Application Security Testing
- MAST – Mobile Application Security Testing

FERRAMENTAS

DAST:

- OWASP ZAP
- Arachni
- W3af
- AppScan
- WebInspect
- BurpSuite Enterprise

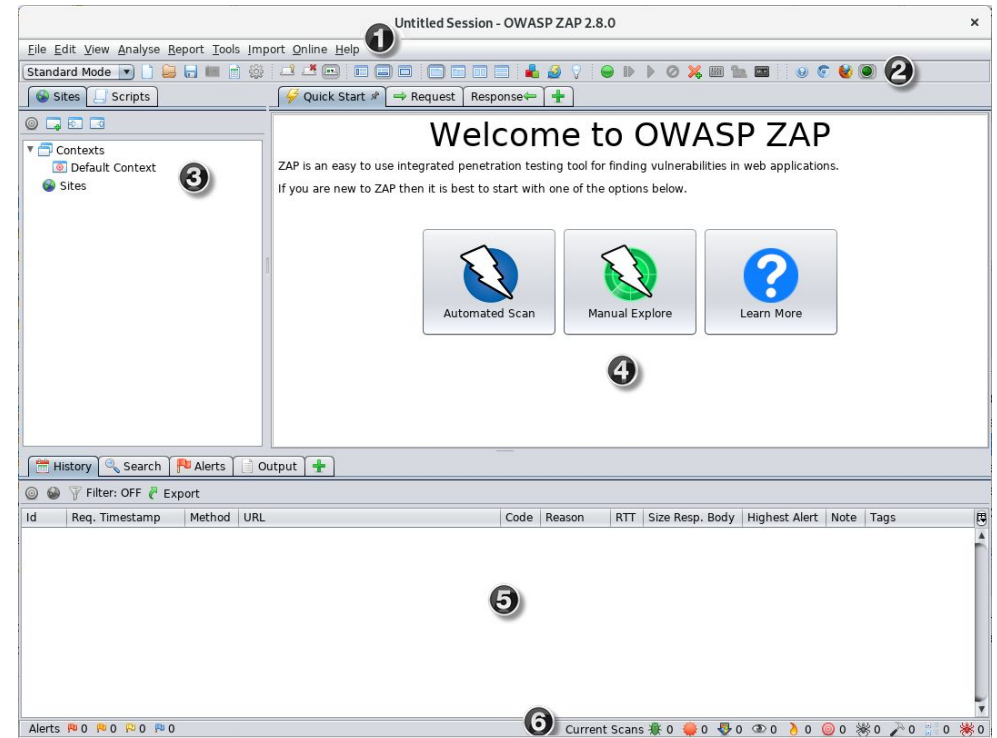
SAST:

- AppScan Source
- Checkmarx
- Fortify
- HuskyCI
- Brakeman
- RIPS
- SonarQube**

Vulnerability Scanning Tools

DAST

OWASP ZAP



SAST

FORTIFY SCANCENTRAL

The screenshot displays the Fortify ScanCentral SAST interface. At the top, there is a navigation bar with 'DASHBOARD', 'APPLICATIONS', 'REPORTS', and 'ADMINISTRATION'. A search bar is located on the right. Below the navigation bar, the project name 'VDH_ADMIN_UI' and version '1.0.0' are shown, along with a warning: 'OFTEN MISUSED: FILE UPLOAD (API ABUSE , CONTENT)'. The main area is divided into three tabs: 'CODE', 'COMMENTS & HISTORY', and 'ATTACHMENTS'. On the right side of this area, there are buttons for 'SUPPRESS' and 'GET TRAINING'. The code editor shows the file 'ui_upload_new_pdf_form.php' with line numbers 52 to 72. Line 61 is highlighted in yellow, containing the code: `<input class="form-control" type="file" name="pdffile" id="pdffile"/>
`. To the right of the code editor, there is an 'AUDIT' section with a dropdown arrow. Below it, the 'USER' is listed as 'Not Assigned', and the 'ANALYSIS' is 'Not Set'. There is also a 'COMMENTS' section with a text input field labeled 'Type Here...'. At the bottom right of the audit section, there are 'SAVE' and 'UNDO' buttons. Below the code editor, an 'Analysis Trace' section shows a single entry: 'ui_upload_new_pdf_form.php:61' with a blue dot next to it.

SCA (SOFTWARE COMPOSITION ANALYSIS)

Podemos definir SCA, como uma prática de desenvolvimento que utiliza de ferramentas de teste de segurança para lidar com o gerenciamento do uso de componentes de software.”

Exemplos de Ferramentas:

- OWASP Dependency Check
- OWASP Dependency Track
- Retire.js
- Snyk
- Veracode SCA
- Synopsys BlackDuck
- Jfrog | X-ray

DEPENDENCY TRACK

SBOM (Software Bill of Materials)

- Lista de componentes de um Software
- Lista de ingredientes para uma receita.



The background is a solid blue gradient. In the four corners, there are decorative white line-art patterns resembling circuit boards or neural networks, with lines and small circles connecting them.

“COMO SE TORNAR APPSEC”

PRECISO CONHECER PENTEST?

- Melhora os resultados entregues mas não deve ser obrigatório, inclusive dependendo da Empresa ou escopo de atuação, o Appsec não realizará nenhum Teste desse tipo.

The screenshot displays the Burp Suite interface with the following sections:

- Tasks:** Shows two tasks. Task 1: 'Live passive crawl from Proxy (all traffic)' with 110 items added to the site map and 6 responses processed. Task 2: 'Live audit from Proxy (all traffic)' with 5 requests and 0 errors.
- Issue activity:** A table listing various issues found during the scan, including 'Lack or Misconfiguration of Security Header(s)', 'Content Sniffing not disabled', and 'Browser cross-site scripting filter misconfiguration'.
- Event log:** A table of system events such as connection failures, task timeouts, and proxy resets.
- Advisory:** A detailed advisory for 'Lack or Misconfiguration of Security Header(s)' with severity 'Low' and confidence 'Certain'. It includes the host and path of the affected resource and a note that the issue was generated by the Headers Analyzer extension.

É PRECISO SABER PROGRAMAR?

Overview Repositories 107 Projects Packages Stars 28

kubernetes-the-hard-way Public
Forked from mmumshad/kubernetes-the-hard-way
Bootstrap Kubernetes the hard way on Vagrant on Local Machine. No scripts.
Shell Apache License 2.0 Updated on Jan 31

certified-kubernetes-administrator-course Public
Forked from kodekloudhub/certified-kubernetes-administrator-course
Certified Kubernetes Administrator - CKA Course
Shell Updated on Jan 30

curso-aws-com-terraform Public
Forked from chgasparoto/curso-aws-com-terraform
BR Arquivos do curso "DevOps: AWS com Terraform. Automatizando sua infraestrutura"
HCL MIT License Updated on Dec 20, 2022

DevSecOps Public
Forked from hahwul/DevSecOps
Collection and Roadmap for everyone who wants DevSecOps. Hope your DevOps are more safe 🤖
Go MIT License Updated on Dec 3, 2022

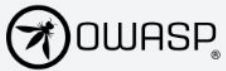
Exemplo de Command Injection

```
<?php
    $host = 'google';

    if (isset( $_GET['host'] ) )
        $host = $_GET['host'];
        system("nslookup " . $host);
?>

<form method="get">
    <select name="host">
        <option value="google.com">google</option>
        <option value="yahoo.com">yahoo</option>
    </select>
    <input type="submit">
</form>
```

Please support the OWASP mission to improve software security through Open Source initiatives and community education. [Donate Now!](#) ✕



PROJECTS CHAPTERS EVENTS ABOUT

Search OWASP.org

Store

Donate

Join

Browse All Projects...

OWASP Top Ten

Dependency Track

Juice Shop

Mobile Application Security

ModSecurity Core Rule Set

Software Assurance Maturity Model (SAMM)

Security Knowledge Framework

Web Security Testing Guide

Zed Attack Proxy

Start a New Project...

Google Summer of Code 2021




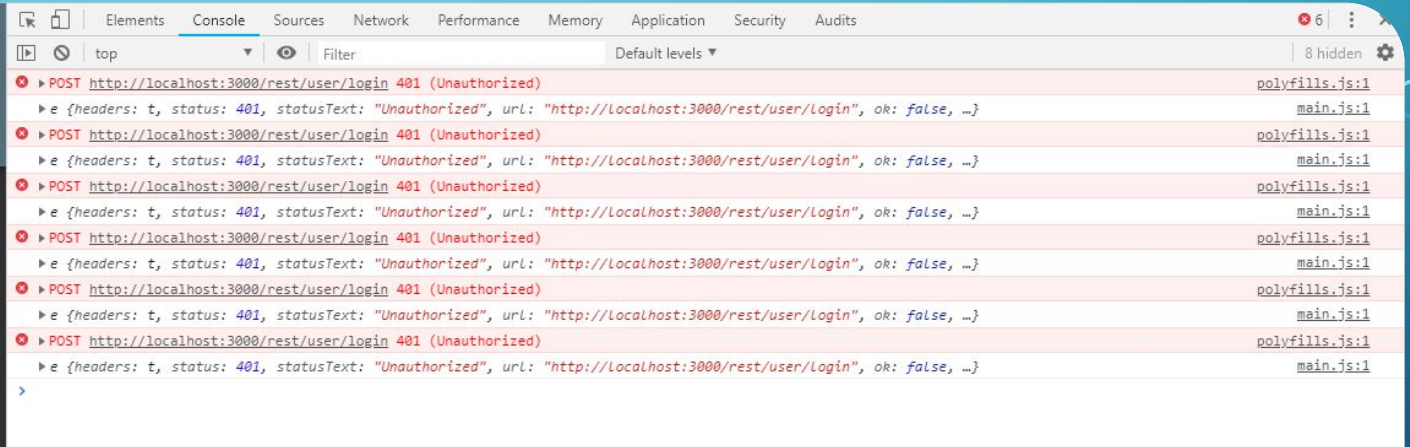
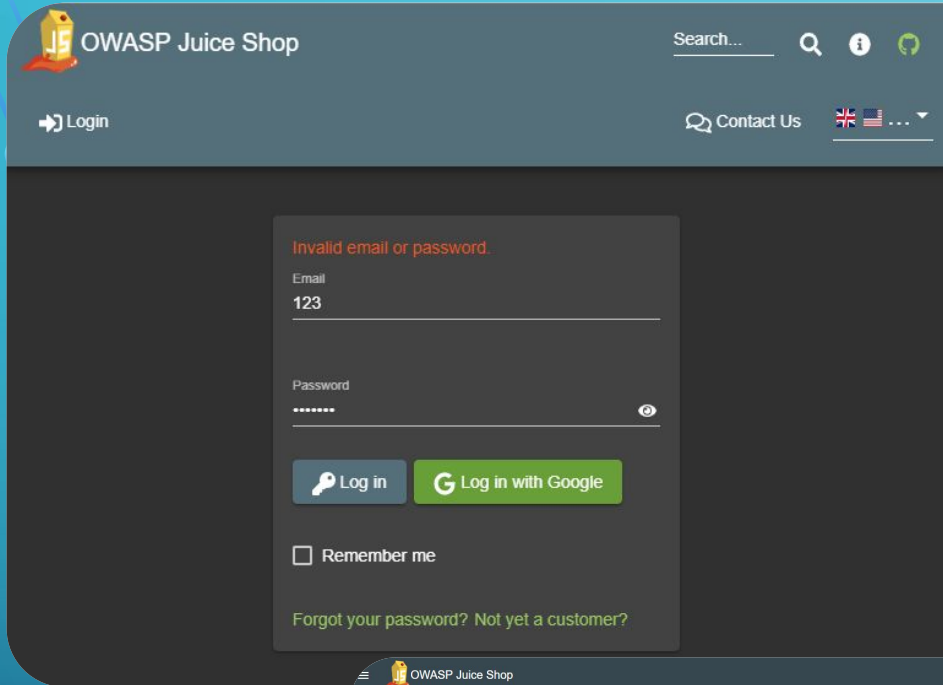
Who is the OWASP® Foundation?

The Open Worldwide Application Security Project® (OWASP) is a nonprofit foundation that works to improve the security of software. Through community-led open-source software projects, hundreds of local chapters worldwide, tens of thousands of members, and leading educational and training conferences, the OWASP Foundation is the source for developers and technologists to secure the web.

- Tools and Resources
- Community and Networking
- Education & Training

For nearly two decades corporations, foundations, developers, and volunteers have supported the OWASP Foundation and its work. [Donate](#), [Join](#), or become a [Corporate Member](#) today.

OWASP JUICE SHOP



OWASP Juice Shop

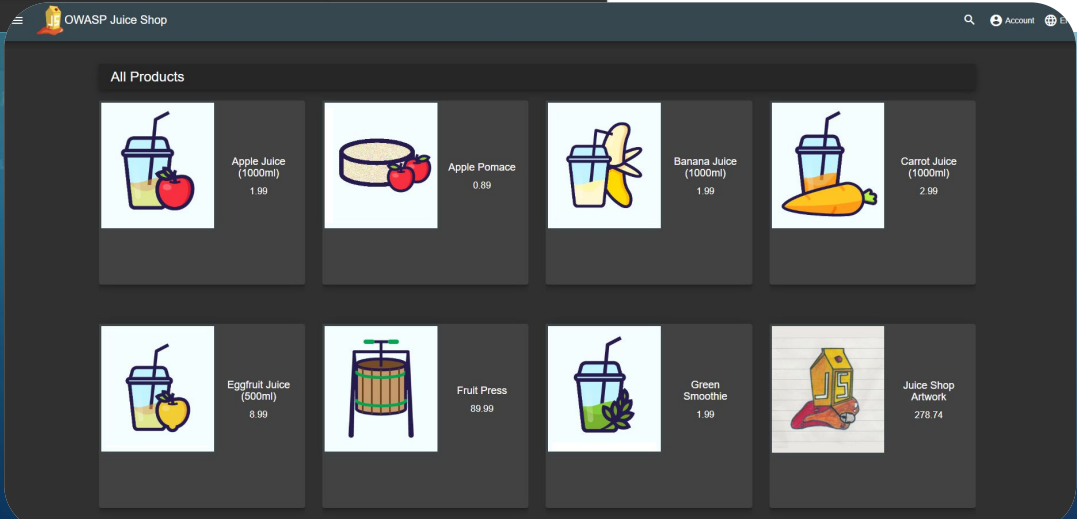
owasp **flagship project** release **v14.5.1** [Follow](#) [Follow /owasp_juiceshop](#) 264

CI/CD Pipeline **passing** test coverage **88%** maintainability **A** technical debt **2%** openssf best practices **gold**

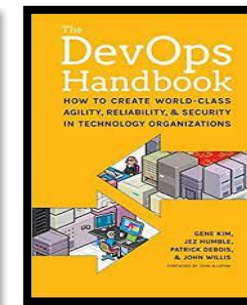
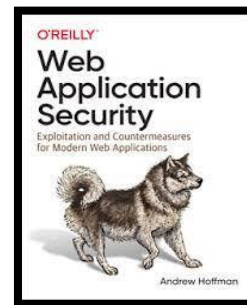
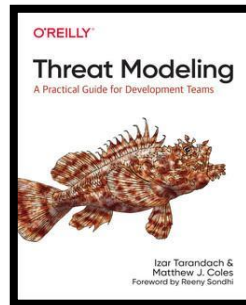
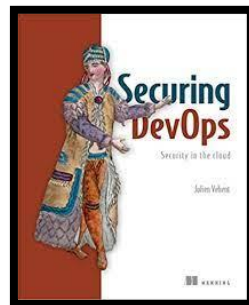
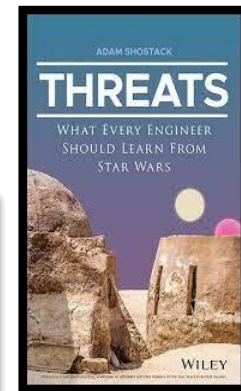
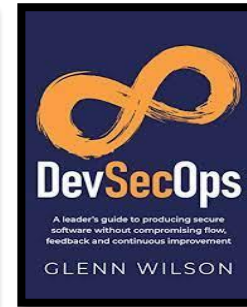
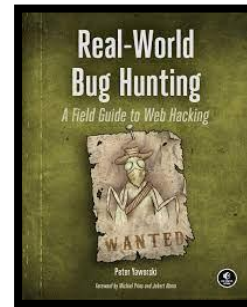
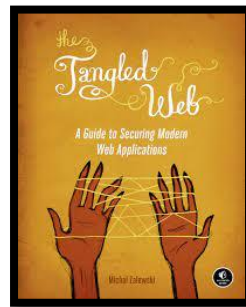
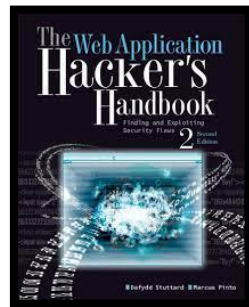
GitHub **7.9k** Contributor Covenant **v2.0 adopted**

The most trustworthy online shop out there. (@dschadow) – The best juice shop on the whole internet! (@shehackspurple) – Actually the most bug-free vulnerable application in existence! (@vanderaj) – First you 🤩🤩 then you 😞😞 (@kramse) – But this doesn't have anything to do with juice. (@coderPatros' wife)

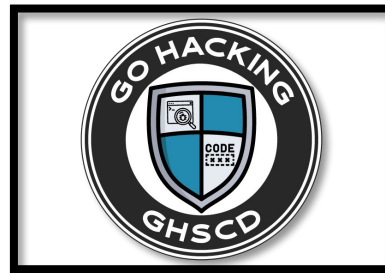
OWASP Juice Shop is probably the most modern and sophisticated insecure web application! It can be used in security trainings, awareness demos, CTFs and as a guinea pig for security tools! Juice Shop encompasses vulnerabilities from the entire OWASP Top Ten along with many other security flaws found in real-world applications!



LIVROS

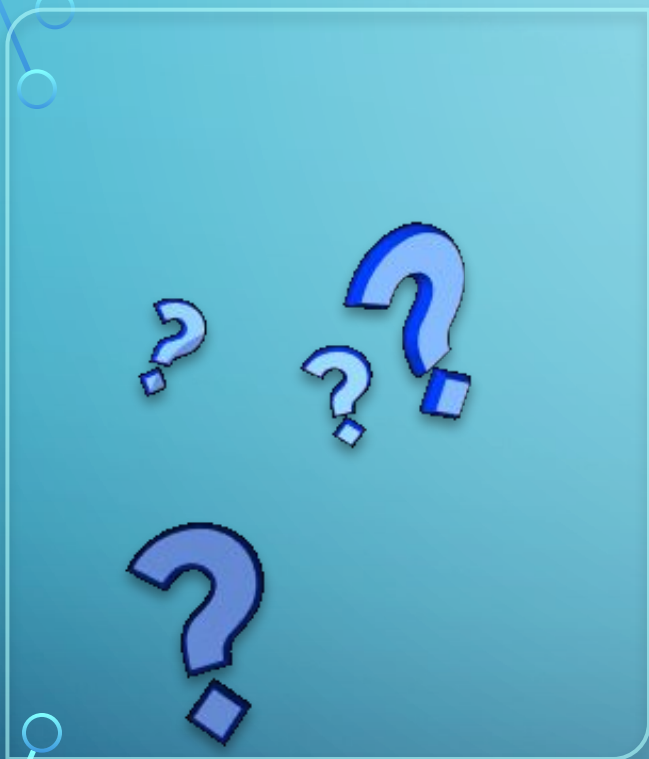


CURSOS



CERTIFICAÇÕES





OBRIGADO!

REFERÊNCIAS

- <https://www.microsoft.com/en-us/securityengineering/sdl/practices>
- <https://developer.mozilla.org/pt-BR/docs/Web/HTTP/Overview>
- <https://blog.convisoappsec.com/devsecops-seguranca-como-cultura/>
- <https://www.redhat.com/pt-br/topics/devops/what-is-devsecops>
- <https://www.datadoqhq.com/resources/devsecops-assessment/>
- https://owasp.org/Top10/pt_BR/A00_2021_Introduction/
- <https://www.ipc.nsw.gov.au/fact-sheet-privacy-design>
- https://d1.awsstatic.com/whitepapers/compliance/Intro_to_Security_by_Design.pdf
- <https://www.threatmodelingmanifesto.org/>
- <https://silva-andre.medium.com/design-b2fd2881e8fd>
- <https://www.securitymadesimple.org/cybersecurity-blog/top-7-popular-cyber-threat-models>
- <https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling>

REFERÊNCIAS

- https://owasp.org/www-community/Vulnerability_Scanning_Tools
- <https://www.interstell.com/wordpress/fortify-static-code-analyzer-and-family-reporting-basic-statistics/>
- <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>
- <https://www.nova8.com.br/2020/12/o-que-e-sca-software-composition-analysis/>
- <https://www.infosec.com.br/command-injection/>
- <https://owasp.org/www-project-juice-shop/>
- <https://pwning.owasp-juice.shop/>

REFERÊNCIAS

- <https://www.amazon.com.br/Web-Application-Hackers-Handbook-Exploiting/dp/1118026470>
- <https://www.amazon.com.br/Tangled-Web-Securing-Modern-Applications/dp/1593273886>
- <https://www.amazon.com.br/Real-World-Bug-Hunting-Field-Hacking/dp/1593278616>
- <https://www.amazon.com.br/DevSecOps-producing-compromising-continuous-improvement-ebook/dp/B08QRRNX6K>
- <https://www.amazon.com.br/Securing-DevOps-Safe-services-Julien-Vehent/dp/1617294136>
- https://www.amazon.com//dp/1492056553?tag=oreilly20-20&language=pt_BR¤cy=BRL
- <https://www.amazon.com.br/Web-Application-Security-Andrew-Hoffman/dp/1492053112>
- <https://a.co/d/gM6GQN7>
- <https://a.co/d/9wyOggN>

REFERÊNCIAS

- <https://gohacking.com.br/curso/GHSCD>
- <https://sec4us.com.br/treinamentos/web-api-exploitation/>
- <https://www.appsecengineer.com/>
- <https://www.sans.org/cyber-security-courses/application-security-securing-web-apps-api-microservices/>
- <https://tryhackme.com/>
- <https://academy.hackthebox.com/>
- <https://secops.group/product/certified-application-security-practitioner/>
- <https://www.eccouncil.org/train-certify/certified-devsecops-engineer-ecde/>
- <https://www.eccouncil.org/train-certify/application-security/>
- <https://www.isc2.org/Certifications/CSSLP#>
- <https://www.comptia.org/pt/certificacoes/pentest>
- <https://www.comptia.org/pt/certificacoes/security>