



AppSec Tools



WHO AM I?



jPr3sc0t

Padre Six

Analista de Segurança da
Informação (AppSec);

Formado em ADS e
Pós-Graduado em Offensive
Security;

15 anos de xp na area de tech;

fã de Star Wars e
pseudo-padre nas horas vagas.

MISSION STATEMENT

Apresentar de forma breve, algumas tools OWASP para Application Security (AppSec)



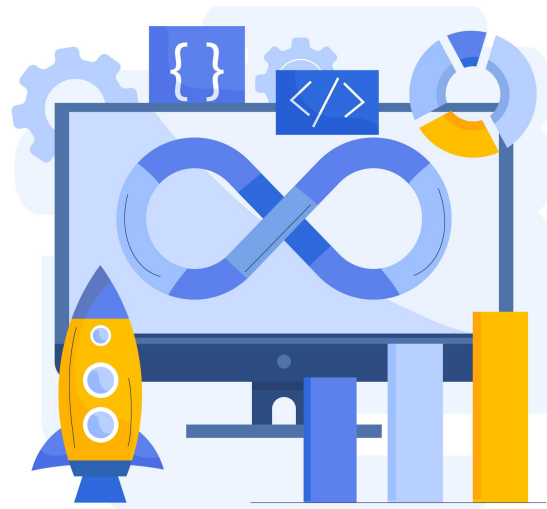
APPSEC CONTEXT



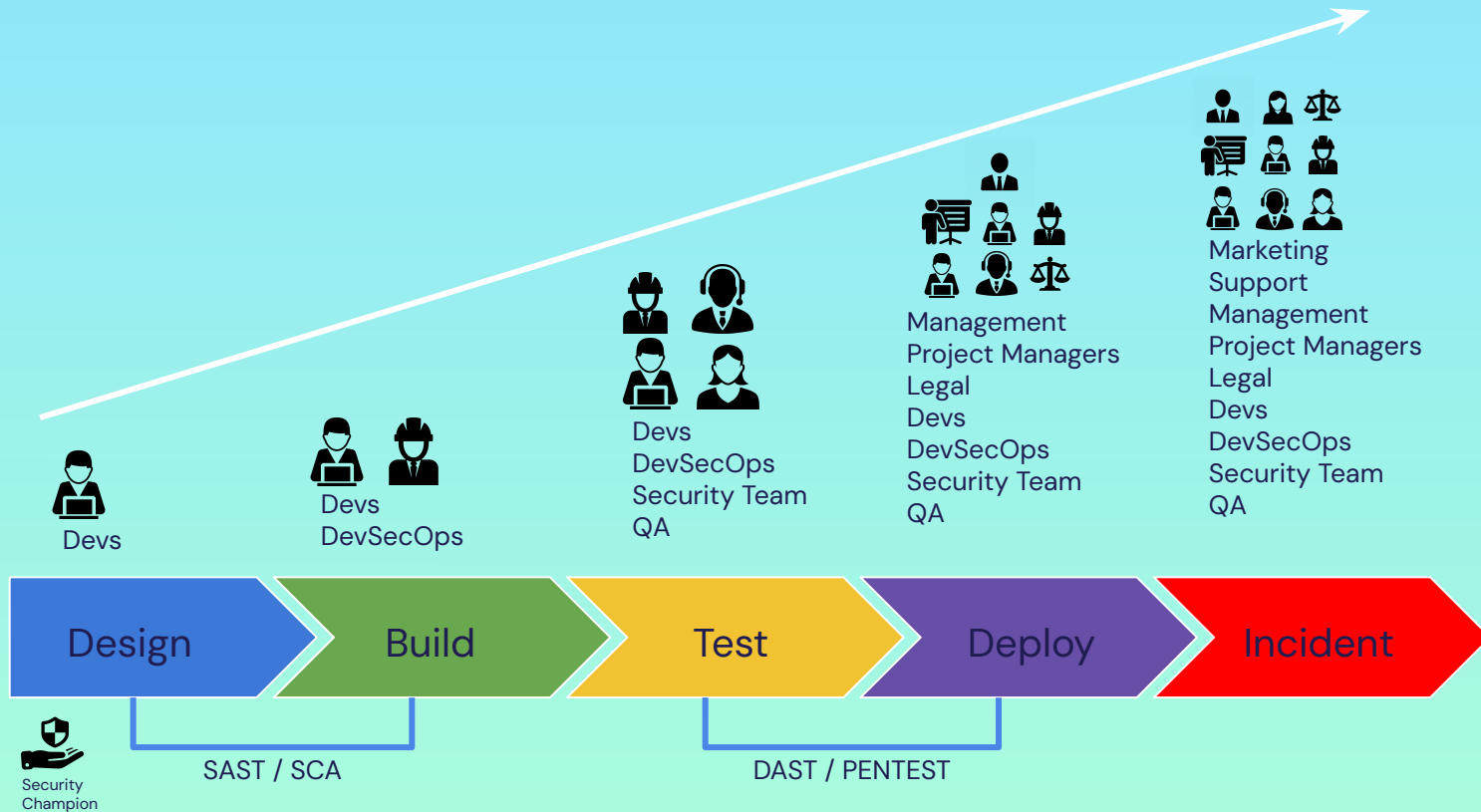
Prática de incorporar segurança no ciclo de vida de desenvolvimento de software (SDLC) para identificar e mitigar possíveis vulnerabilidades de segurança em aplicativos de software.

DEVSECOPS CONTEXT

DevSecOps integra controles e processos de segurança em todo o ciclo de vida de desenvolvimento de software, desde o planejamento até a implantação



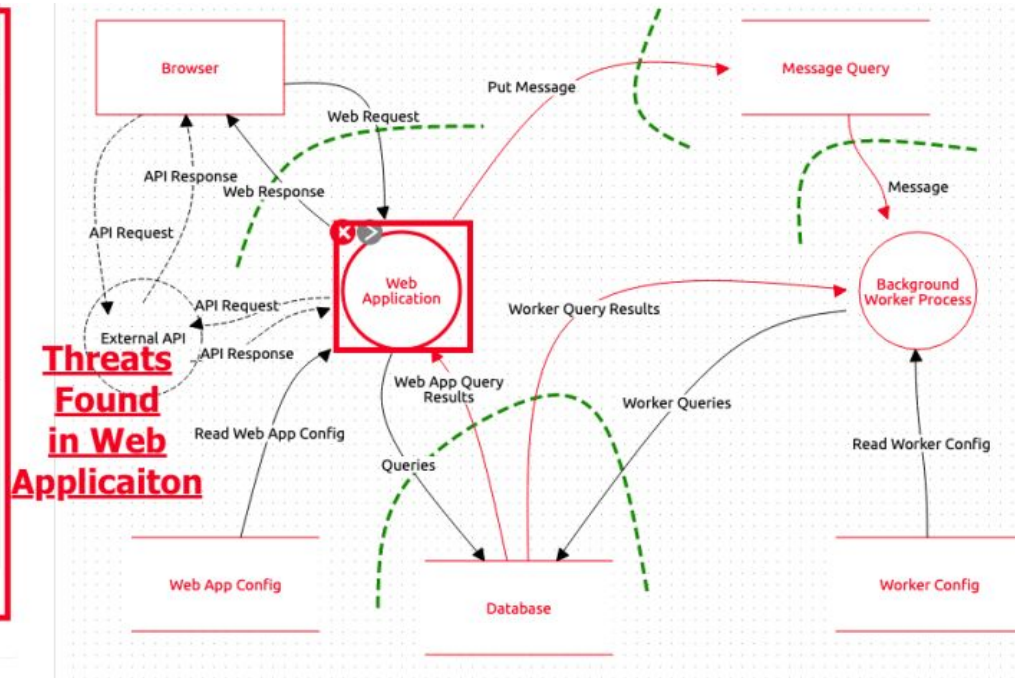
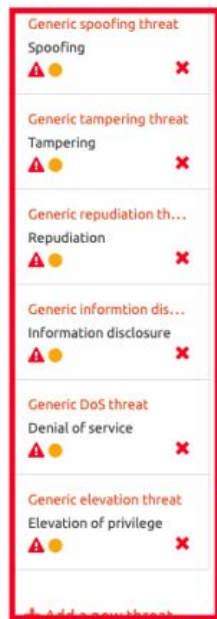
APPSEC ROI



OWASP THREAT DRAGON



Interface gráfica amigável que permite criar e modificar modelos de ameaças usando o amplamente utilizado **STRIDE** (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) e **DREAD** (Damage, Reproducibility, Exploitability, usuários afetados, descoberta)



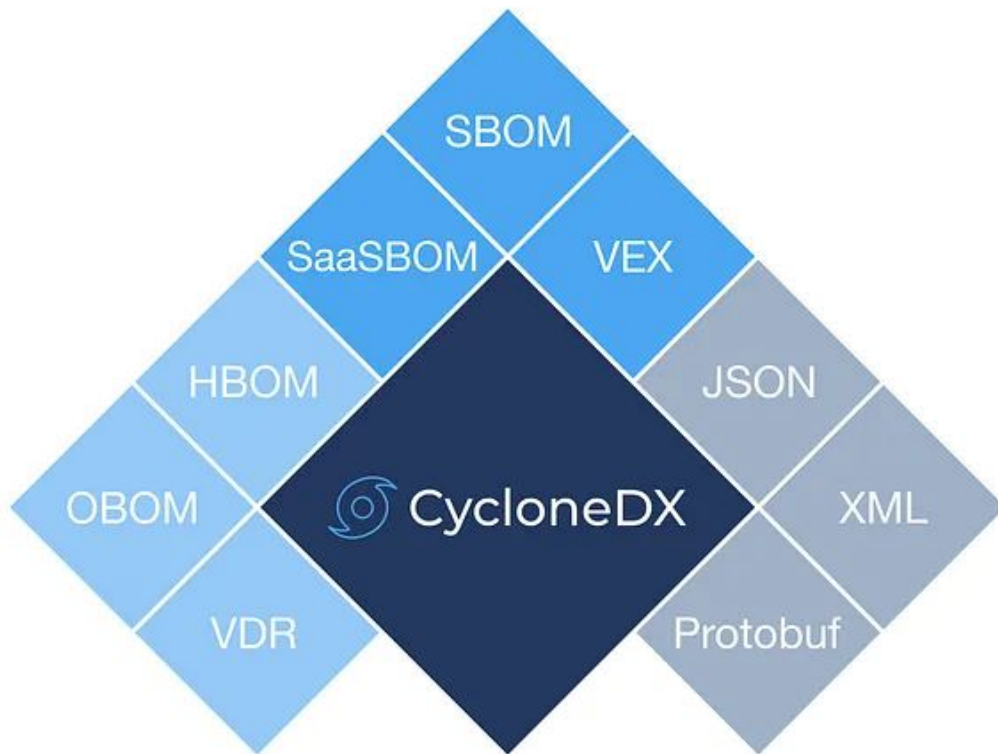
<https://owasp.org/www-project-threat-dragon/>

CYCLONEDX

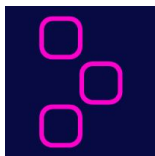


Padrão para codificação de listas de materiais (SBOM – Software Bill of Materials), que descreve detalhadamente os componentes de um software, auxiliando na rastreabilidade de vulnerabilidades.

O Cyclone também facilita a comunicação entre times de desenvolvimento e segurança, automatiza a criação e compartilhamento de SBOMs, garantindo a segurança do ciclo de vida de softwares.



DEPENDENCY CHECK / TRACK



Permite que você examine seus projetos para identificar as bibliotecas, estruturas e outros componentes de terceiros dos quais seu código depende. Em seguida, ele usa várias fontes de informações de vulnerabilidade, incluindo o banco de dados National Vulnerability Database (NVD) e o banco de dados Common Vulnerabilities and Exposures (CVE), para identificar quaisquer vulnerabilidades conhecidas nessas dependências.

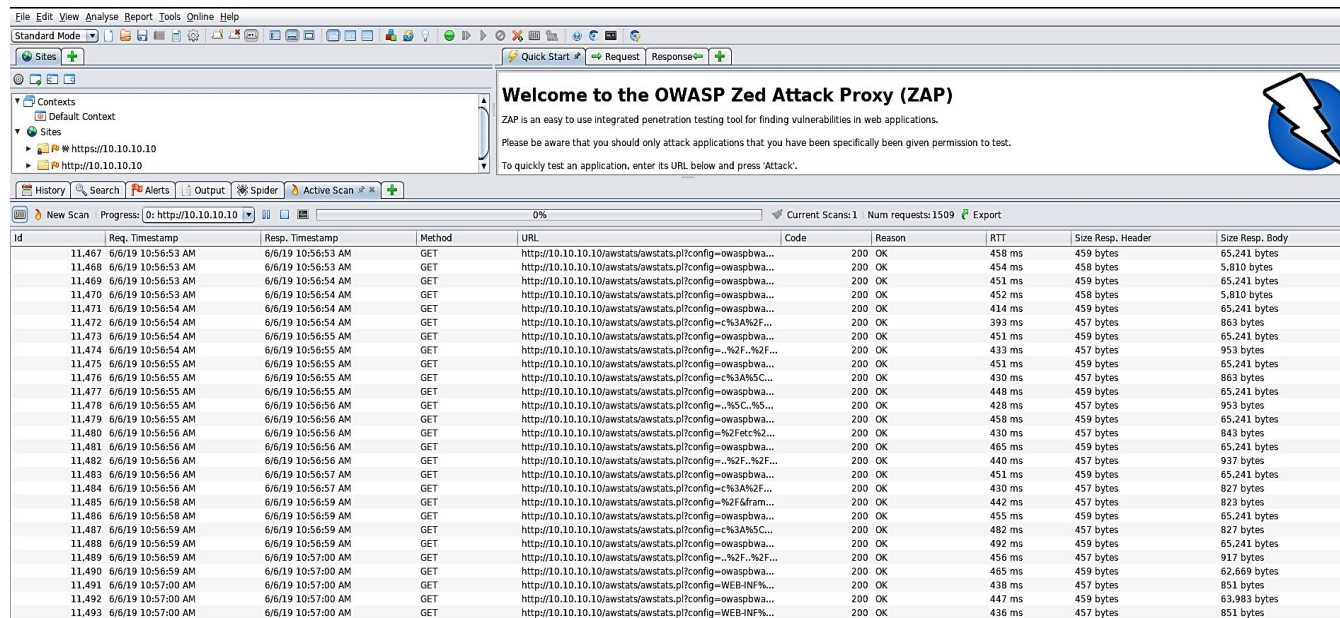
Component	Version	Group	Internal	License	Risk Score	Vulnerabilities
7zip	0.0.6			GNU LGPL	0	0
abbrev	1.1.1			ISC	0	0
accepts	1.3.4			MIT	0	0
acorn	6.0.7			MIT	8	1
acorn-dynamic-import	3.0.0			MIT	0	0
agent-base	4.2.1			MIT	0	0
ajv	6.8.1			MIT	0	0
ajv-keywords	3.2.0			MIT	0	0
alphanum-sort	1.0.2			MIT	0	0
amdefine	1.0.1			BSD-3-Clause OR MIT	0	0

<https://owasp.org/www-project-dependency-check/>
<https://owasp.org/www-project-dependency-track/>

ZAP (ZAPROXY)



Baseada em Java e pode ser usada em qualquer plataforma que suporte Java. Permite aos usuários verificar vulnerabilidades em aplicativos da Web, bem como uma API que pode ser usada para automação e integração com outras ferramentas.



File Edit View Analyse Report Tools Online Help

Standard Mode

Quick Start Request Response

Welcome to the OWASP Zed Attack Proxy (ZAP)

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

Please be aware that you should only attack applications that you have been specifically given permission to test.

To quickly test an application, enter its URL below and press 'Attack'.

History Search Alerts Output Spider Active Scan

New Scan Progress: 0% Current Scans: 1 Num requests: 1509 Export

Id	Req. Timestamp	Resp. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Header	Size Resp. Body
11.467	6/6/19 10:56:53 AM	6/6/19 10:56:53 AM	GET	http://10.10.10.10/awstats/awstats.pl?config=owaspbwa...	200	OK	458 ms	459 bytes	65,241 bytes
11.468	6/6/19 10:56:53 AM	6/6/19 10:56:53 AM	GET	http://10.10.10.10/awstats/awstats.pl?config=owaspbwa...	200	OK	454 ms	458 bytes	5,810 bytes
11.469	6/6/19 10:56:53 AM	6/6/19 10:56:54 AM	GET	http://10.10.10.10/awstats/awstats.pl?config=owaspbwa...	200	OK	451 ms	459 bytes	65,241 bytes
11.470	6/6/19 10:56:53 AM	6/6/19 10:56:54 AM	GET	http://10.10.10.10/awstats/awstats.pl?config=owaspbwa...	200	OK	452 ms	458 bytes	5,810 bytes
11.471	6/6/19 10:56:54 AM	6/6/19 10:56:54 AM	GET	http://10.10.10.10/awstats/awstats.pl?config=owaspbwa...	200	OK	414 ms	459 bytes	65,241 bytes
11.472	6/6/19 10:56:54 AM	6/6/19 10:56:54 AM	GET	http://10.10.10.10/awstats/awstats.pl?config=c%3A%2F...	200	OK	393 ms	457 bytes	863 bytes
11.473	6/6/19 10:56:54 AM	6/6/19 10:56:55 AM	GET	http://10.10.10.10/awstats/awstats.pl?config=owaspbwa...	200	OK	451 ms	459 bytes	65,241 bytes
11.474	6/6/19 10:56:54 AM	6/6/19 10:56:55 AM	GET	http://10.10.10.10/awstats/awstats.pl?config=owaspbwa...	200	OK	433 ms	457 bytes	953 bytes
11.475	6/6/19 10:56:55 AM	6/6/19 10:56:55 AM	GET	http://10.10.10.10/awstats/awstats.pl?config=owaspbwa...	200	OK	451 ms	459 bytes	65,241 bytes
11.476	6/6/19 10:56:55 AM	6/6/19 10:56:55 AM	GET	http://10.10.10.10/awstats/awstats.pl?config=c%3A%5C...	200	OK	430 ms	457 bytes	863 bytes
11.477	6/6/19 10:56:55 AM	6/6/19 10:56:55 AM	GET	http://10.10.10.10/awstats/awstats.pl?config=owaspbwa...	200	OK	448 ms	459 bytes	65,241 bytes
11.478	6/6/19 10:56:55 AM	6/6/19 10:56:56 AM	GET	http://10.10.10.10/awstats/awstats.pl?config=owaspbwa...	200	OK	428 ms	457 bytes	953 bytes
11.479	6/6/19 10:56:55 AM	6/6/19 10:56:56 AM	GET	http://10.10.10.10/awstats/awstats.pl?config=owaspbwa...	200	OK	458 ms	459 bytes	65,241 bytes
11.480	6/6/19 10:56:56 AM	6/6/19 10:56:56 AM	GET	http://10.10.10.10/awstats/awstats.pl?config=%2Fetc%2...	200	OK	430 ms	457 bytes	843 bytes
11.481	6/6/19 10:56:56 AM	6/6/19 10:56:56 AM	GET	http://10.10.10.10/awstats/awstats.pl?config=owaspbwa...	200	OK	465 ms	459 bytes	65,241 bytes
11.482	6/6/19 10:56:56 AM	6/6/19 10:56:56 AM	GET	http://10.10.10.10/awstats/awstats.pl?config=%2F,%2F...	200	OK	440 ms	457 bytes	937 bytes
11.483	6/6/19 10:56:56 AM	6/6/19 10:56:57 AM	GET	http://10.10.10.10/awstats/awstats.pl?config=owaspbwa...	200	OK	451 ms	459 bytes	65,241 bytes
11.484	6/6/19 10:56:56 AM	6/6/19 10:56:57 AM	GET	http://10.10.10.10/awstats/awstats.pl?config=c%3A%2F...	200	OK	430 ms	457 bytes	827 bytes
11.485	6/6/19 10:56:58 AM	6/6/19 10:56:59 AM	GET	http://10.10.10.10/awstats/awstats.pl?config=%2F&fram...	200	OK	442 ms	457 bytes	823 bytes
11.486	6/6/19 10:56:58 AM	6/6/19 10:56:59 AM	GET	http://10.10.10.10/awstats/awstats.pl?config=owaspbwa...	200	OK	455 ms	459 bytes	65,241 bytes
11.487	6/6/19 10:56:59 AM	6/6/19 10:56:59 AM	GET	http://10.10.10.10/awstats/awstats.pl?config=c%3A%5C...	200	OK	482 ms	457 bytes	827 bytes
11.488	6/6/19 10:56:59 AM	6/6/19 10:56:59 AM	GET	http://10.10.10.10/awstats/awstats.pl?config=owaspbwa...	200	OK	492 ms	459 bytes	65,241 bytes
11.489	6/6/19 10:56:59 AM	6/6/19 10:57:00 AM	GET	http://10.10.10.10/awstats/awstats.pl?config=%2F,%2F...	200	OK	456 ms	457 bytes	917 bytes
11.490	6/6/19 10:56:59 AM	6/6/19 10:57:00 AM	GET	http://10.10.10.10/awstats/awstats.pl?config=owaspbwa...	200	OK	465 ms	459 bytes	62,669 bytes
11.491	6/6/19 10:57:00 AM	6/6/19 10:57:00 AM	GET	http://10.10.10.10/awstats/awstats.pl?config=WEB-INF%...	200	OK	438 ms	457 bytes	851 bytes
11.492	6/6/19 10:57:00 AM	6/6/19 10:57:00 AM	GET	http://10.10.10.10/awstats/awstats.pl?config=owaspbwa...	200	OK	447 ms	459 bytes	63,983 bytes
11.493	6/6/19 10:57:00 AM	6/6/19 10:57:00 AM	GET	http://10.10.10.10/awstats/awstats.pl?config=WEB-INF%...	200	OK	436 ms	457 bytes	851 bytes

<https://www.zaproxy.org/>

AMASS



Amass é uma ferramenta de código aberto desenvolvida pela OWASP para mapeamento e enumeração de domínios e subdomínios. Coleta informações através de consultas passivas e ativas, ajudando a identificar a superfície de ataque de uma organização.



<https://owasp.org/www-project-amass/>

OWTF



Offensive Web Testing Framework (OWTF) é uma ferramenta focada em automação de pentest em aplicações web. Desenvolvida para ajudar profissionais de segurança a identificar e relatar vulnerabilidades de maneira eficiente, OWTF integra diversos recursos e ferramentas para fornecer uma análise abrangente



Offensive Web Testing Framework!

OWASP OWTF is a project that aims to make security assessments as efficient as possible. Some of the ways in which this is achieved are:

- Separating the tests that require no permission from the ones that require permission (i.e. active/ bruteforce).
- Launching a number of tools automatically.
- Running tests not found in other tools.
- Providing an interactive interface/report.
- More info: https://www.owasp.org/index.php/OWASP_OWTF

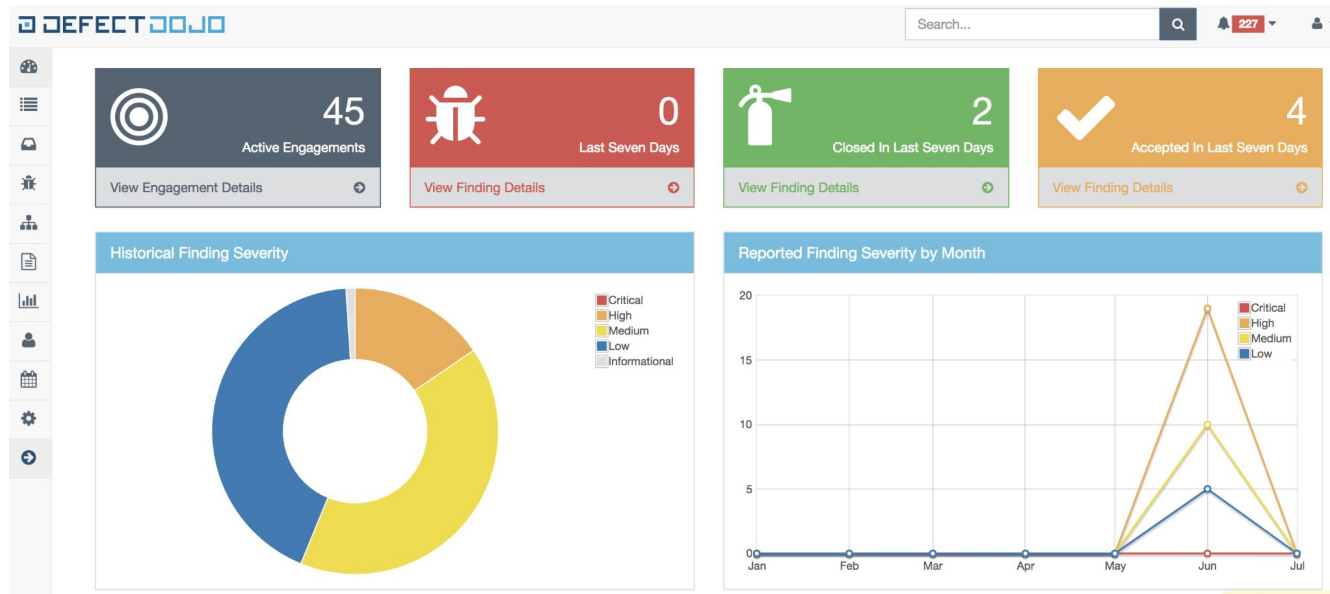
Learn more

<https://owasp.org/www-project-owtf/>

DEFECT DOJO



Ferramenta de gerenciamento de vulnerabilidades que ajuda as equipes de segurança no rastreamento de vulnerabilidades de segurança descobertas durante os vários estágios do ciclo de vida de desenvolvimento de software, incluindo teste, implantação e produção.

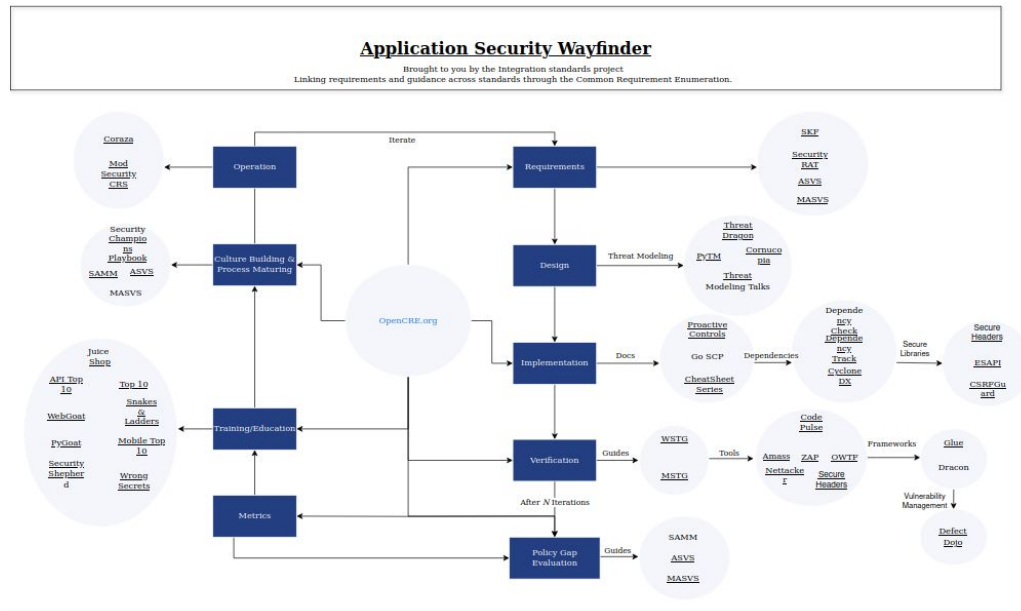


<https://defectdojo.com/>

OWASP FRAMEWORKS



- **OWASP SAMM (Software Assurance Maturity Model):** Estrutura para construir e melhorar práticas de segurança. Fornece um conjunto de diretrizes e práticas recomendadas para cada estágio do SDLC.
- **OWASP ASVS (Application Security Verification Standard):** estrutura para verificar a segurança de aplicativos da web. Fornece um conjunto de requisitos e diretrizes de segurança que podem ser usados para testar a segurança de aplicativos da Web em diferentes níveis de garantia.
- **OWASP Top 10:** Fornece orientação sobre vulnerabilidades comuns e vetores de ataque que devem ser abordados no desenvolvimento e teste de aplicativos da web.
- **OWASP Web Security Testing Guide:** Orientações mais abrangentes para testar a segurança de aplicativos da web. Fornece orientação sobre metodologias, ferramentas e técnicas para identificar e lidar com vulnerabilidades web.
- **OWASP Application Security Architecture Cheat Sheet:** Orientações sobre como projetar e implementar arquiteturas de software seguras. Conjunto de práticas recomendadas e princípios de design para a construção de sistemas seguros.



<https://owasp.org/projects/#flagship-projects>

**MUITO
OBRIGADO!**

May the AppSec be with you!