WORKSHOP OWASP

DEBIAN DAY

Palestrante: Marcos Tulio

.DEBIAN DAY JOÃO PESSOA 2025

EXPLORANDO APPSEC COM DEBIAN: UM GUIA PRÁTICO USANDO OS LABORATÓRIOS OPEN SOURCE DA OWASP

.DEBIAN DAY JOÃO PESSOA 2025

AGENDA

01 O Debian

02 AppSec

03 A OWASP e o Capítulo João Pessoa

.DEBIAN DAY JOÃO PESSOA 2025

AGENDA

04 ToolBox AppSec com Debian

05 OWASP Completely Ridiculous API

06 OWASP Juice-Shop

.DEBIAN DAY JOÃO PESSOA 2025

AGENDA

07 OWASP WebGoat

08 Conclusão e agradecimentos

01

O DEBIAN

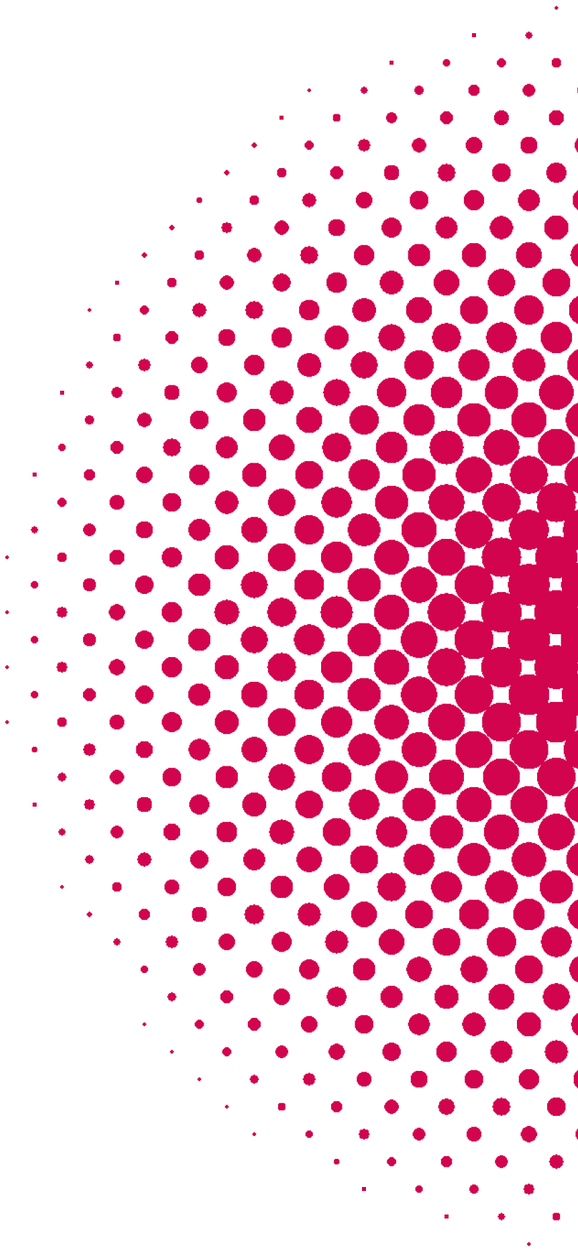
O DEBIAN

Criado em 1993 por **Ian Murdock**, o Debian nasceu como um projeto comunitário comprometido com os princípios do **software livre**, transparência e estabilidade. Sua robustez e confiabilidade fizeram dele **a base de várias distribuições populares**, como o Ubuntu e o Kali Linux. **No Brasil**, o Debian ganhou força por sua estabilidade em **servidores**, facilidade de personalização e compatibilidade com infraestruturas **públicas e educacionais**. Governos, universidades e entusiastas da segurança da informação adotaram o Debian como símbolo de **soberania tecnológica**, impulsionando sua relevância **estratégica nacional**. Hoje, o Debian permanece um dos sistemas mais respeitados globalmente, sustentando a internet e o open source com integridade exemplar.

.DEBIAN DAY JOÃO PESSOA 2025

02

APPSEC

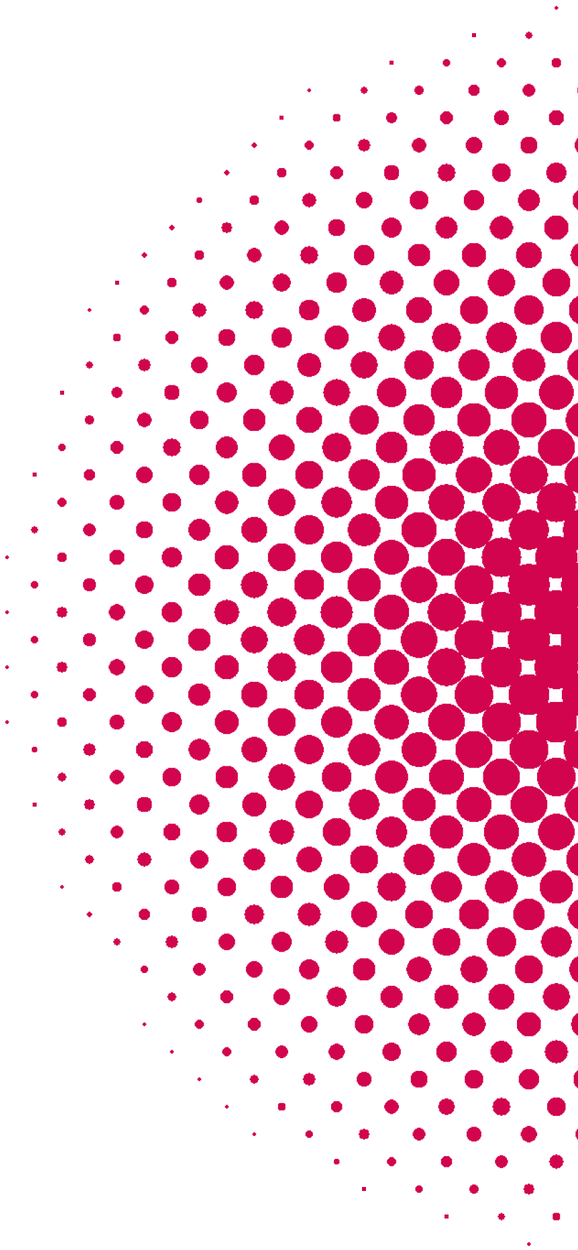


APPSEC

A carreira em Application Security (**AppSec**) exige o domínio de técnicas para **proteger aplicações** desde o desenvolvimento até a produção. Envolve análise de código seguro, testes de segurança, gestão de vulnerabilidades, DevSecOps, threat modeling e atuação direta na cultura de segurança das organizações. O **Debian Linux** se destaca como um sistema operacional confiável e seguro, **amplamente utilizado** por profissionais de AppSec em ambientes de testes, hardening e monitoramento. Seu repositório auditado, políticas de empacotamento rigorosas, resposta rápida a CVEs e compromisso com o software livre, sem esquecer de falar que o Debian é um alicerce **ético e técnico** para profissionais de AppSec.

03

A OWASP E O CAPÍTULO JOÃO PESSOA



A OWASP E O CAPÍTULO JOÃO PESSOA

A OWASP João Pessoa nasceu do desejo de ampliar a cultura de segurança de aplicações (**AppSec**) no estado da Paraíba, conectando profissionais, estudantes, pesquisadores e empresas em torno das boas práticas da segurança do desenvolvimento de software. Desde sua criação, o capítulo tem promovido meetups técnicos, workshops práticos, eventos comunitários e **treinamentos gratuitos**. A presença ativa da OWASP João Pessoa tem impulsionado a **profissionalização do mercado local**, fortalecido comunidades de tecnologia e posicionado a cidade como referência em **AppSec no Nordeste**, liderada pelos **Chapters**: Jessé Neto, Pedro Filho, Anderson Philip, Marcos Tulio e Jansen Holanda.

.DEBIAN DAY JOÃO PESSOA 2025

04

TOOLBOX APPSEC EM DEBIAN

.DEBIAN DAY JOÃO PESSOA 2025

TOOLBOX APPSEC EM DEBIAN

Adicionar o usuário ao grupo dos sudoers:

$su -
#sudo usermod -aG sudo vboxuser
#reboot

Atualizações iniciais

#sudo apt update && sudo apt upgrade -y

TOOLBOX APPSEC EM DEBIAN

Instalação das Ferramentas Essenciais para AppSec

Criando os diretórios da toolbox-appsec

#mkdir -p toolbox-appsec/{recon,fuzzing,scanners,static-analysis,utils,scripts}

Instalando as ferramentas básicas

#sudo apt install -y curl wget git unzip vim jq python3 python3-pip build-essential net-tools iputils-ping nmap tmux zsh docker.io docker-compose golang

TOOLBOX APPSEC EM DEBIAN

Instalação de ferramenta FFUF para fuzzificação **(1/13)**

#go install github.com/ffuf/ffuf/v2@latest

#cp ~/go/bin/ffuf toolbox-appsec/fuzzing/

O ffuf (Fuzz Faster U Fool) é uma ferramenta de fuzzing para descobrir diretórios, arquivos, parâmetros e subdomínios ocultos em aplicações web no Linux.

TOOLBOX APPSEC EM DEBIAN

Instalação de ferramenta de subfinder: **(2/13)**

#git clone https://github.com/projectdiscovery/subfinder.git

#mv subfinder toolbox-appsec/recon/

O Subfinder no Linux serve para encontrar subdomínios de um domínio alvo de forma rápida e automatizada para fins de reconhecimento.

TOOLBOX APPSEC EM DEBIAN

Instalação de ferramenta de reconhecimento de subdomínios: **(3/13)**

#git clone https://github.com/owasp-amass/amass.git

#mv amass toolbox-appsec/recon

O AMaSS no Linux serve para realizar reconhecimento de subdomínios e mapeamento de superfícies de ataque na fase de enumeração de segurança.

TOOLBOX APPSEC EM DEBIAN

Instalação de ferramenta WFUZZ **(4/13)**

#sudo apt install -y wfuzz

#ln -s $(which wfuzz) toolbox-appsec/fuzzing/wfuzz

O Wfuzz é uma ferramenta de fuzzing no Linux usada para descobrir e enumerar recursos ocultos em aplicações web por meio de requisições automatizadas.

TOOLBOX APPSEC EM DEBIAN

Instalação da ferramenta para análise em servidor SQL **(5/13)**

#sudo apt install -y sqlmap

#ln -s $(which sqlmap) toolbox-appsec/scanners/sqlmap

O sqlmap é uma ferramenta no Linux usada para detectar e explorar automaticamente vulnerabilidades de SQL Injection em aplicações web.

TOOLBOX APPSEC EM DEBIAN

Instalação de ferramenta escaneamento web: **(6/13)**

#git clone https://github.com/sullo/nikto.git

#mv nikto toolbox-appsec/scanners

O Nikto é um scanner de vulnerabilidades web no Linux usado para identificar falhas de segurança, configurações inseguras e arquivos expostos em servidores HTTP/HTTPS.

TOOLBOX APPSEC EM DEBIAN

Instalação da ferramenta OWASP ZAP **(7/13)**

#git clone https://github.com/zaproxy/zaproxy.git

#mv zaproxy toolbox-appsec/scanners/zap

O ZAP Proxy (OWASP ZAP) no Linux serve para identificar e explorar vulnerabilidades de segurança em aplicações web por meio de testes de penetração automatizados e manuais.

TOOLBOX APPSEC EM DEBIAN

Instalação da ferramenta para verificação de vulnerabilidade XSS **(8/13)**

#git clone https://github.com/s0md3v/XSStrike toolbox-appsec/scanners/XSStrike

#sudo pip3 install -r toolbox-appsec/scanners/XSStrike/requirements.txt --break-system-packages

O XSStrike é uma ferramenta no Linux usada para detectar e explorar vulnerabilidades de Cross-Site Scripting (XSS) de forma automatizada e avançada.

TOOLBOX APPSEC EM DEBIAN

Instalação da ferramenta DIRSEARCH para verificação fuzzing **(9/13)**

#git clone https://github.com/maurosoria/dirsearch.git

#mv dirsearch toolbox-appsec/fuzzing/

O programa Dirsearch no Linux serve para realizar fuzzing de diretórios e arquivos web, identificando recursos ocultos em servidores web.

TOOLBOX APPSEC EM DEBIAN

Instalação da ferramenta para verificação SAST **(10/13)**

#sudo pip3 install semgrep --break-system-packages

#ln -s $(which semgrep) toolbox-appsec/static-analysis/semgrep

O Semgrep no Linux serve para detectar automaticamente padrões vulneráveis e práticas inseguras em código-fonte, auxiliando na análise estática de segurança.

TOOLBOX APPSEC EM DEBIAN

Instalação da ferramenta para verificação de vazamentos no github **(11/13)**

#sudo pip3 install bandit --break-system-packages

#ln -s $(which bandit) toolbox-appsec/static-analysis/bandit

O programa Bandit no Linux é uma ferramenta automatizada para analisar o código-fonte Python em busca de vulnerabilidades de segurança.

TOOLBOX APPSEC EM DEBIAN

Instalação da ferramenta para verificação de vazamentos no github **(12/13)**

#git clone https://github.com/gitleaks/gitleaks.git

#mv gitleaks toolbox-appsec/utils/

O Gitleaks é uma ferramenta para detectar e prevenir vazamento de segredos e credenciais em repositórios Git no Linux.

TOOLBOX APPSEC EM DEBIAN

Instalação da ferramenta escanear imagens docker **(13/13)**

#git clone https://github.com/aquasecurity/trivy

#mv trivy toolbox-appsec/utils/

O Trivy é uma ferramenta de scanner de vulnerabilidades para containers, imagens e sistemas, usada para identificar falhas de segurança no Linux.

TOOLBOX APPSEC EM DEBIAN

Faça download do meu script aqui em :

#git clone https://github.com/mtgsjr/debiandayjoaopessoa2025.git

Permita a execução com:

#chmod 777 setup.sh

E execute com:

#./setup.sh

.DEBIAN DAY JOÃO PESSOA 2025

TOOLBOX APPSEC EM DEBIAN

Instalação de ferramenta de Pentest Web:

Burp Suite (Community):

- **Baixar de: https://portswigger.net/burp/releases**

Tornar executável:

#chmod +x burpsuite_community_linux_v2025_7_1.sh
#chmod +x burpsuite_community_linux_v*.sh

Executar:

#./burpsuite_community_linux_v*.sh (procure o ícone instalado)

05

OWASP COMPLETELY RIDICULOUS API

OWASP COMPLETELY RIDICULOUS API

Fazer download do projeto crAPI da OWASP:

#wget https://github.com/OWASP/crAPI/archive/refs/heads/main.zip

Descompacte o arquivo e entre na pasta do docker

#unzip main.zip && cd crAPI-main/deploy/docker

Faça o download da imagem

#docker compose pull

Execute o container:

#docker compose -f docker-compose.yml --compatibility up -d

Acesse

http://localhost:8888

06

OWASP JUICE-SHOP

OWASP JUICE-SHOP

OWASP Juice-Shop é provavelmente a mais moderna e sofisticadamente insegura aplicação Web!

Fazer download da imagem

docker pull bkimminich/juice-shop

Executar o container

docker run --rm -p 127.0.0.1:3000:3000 bkimminich/juice-shop

Abrir em

http://localhost:3000

07

OWASP WEBGOAT

OWASP WEBGOAT

Conhecida como o Bode da Web.

O projeto pode ser acessado em

https://github.com/WebGoat/WebGoat

Instale o JDK Java

#apt install -y openjdk-17-jre

Este comando fará o download da imagem se ela não existir no Debian e depois executará o container:

#docker run -it -p 127.0.0.1:8080:8080 -p 127.0.0.1:9090:9090 webgoat/webgoat

Acesse:

http://localhost:8080/WebGoat

08

CONCLUSÃO E AGRADECIMENTOS

.DEBIAN DAY JOÃO PESSOA 2025

CONCLUSÃO E AGRADECIMENTOS

Todos os comandos e scripts foram testados e validados no **debian-12.11.0-amd64-netinst.iso (download aqui)**

O Debian se mostrou um sistema operacional compatível com todas as ferramentas de appsec e com todos os laboratórios da OWASP.

Muito obrigado à todos!

Marcos Tulio Gomes da Silva Junior
https://www.linkedin.com/in/marcos-tulio-gomes-830aa269

.DEBIAN DAY JOÃO PESSOA 2025