

O que acontece depois da entrega do relatório?

cat AGENDA

- ❖ profile
- ❖ objetivo
- ❖ contexto
- ❖ Entrega do relatório
- ❖ Defectdojo
- ❖ Demo
- ❖ Considerações

echo \$PROFILE

❖ Name: Diógenes Ramos

❖ AKA: M@Tr1xPdB

❖ Role: Security Analyst

❖ Skills:

- Graduação: Redes de computadores
- Pós-graduação: Ethical Hacking e Cyber Security
- Mestrado: Gestão e desenvolvimento regional com ênfase em inovação e tecnologia
- OWASP Chapter Leader – Capitulo São José dos Campos



echo \$PROFILE

❖Membro Beco do Exploit

BO *São Paulo*
SIDES



<https://becodoexploit.com/>

more .objetivo

- ❖ Esta apresentação não tem como objetivo ser um guia de melhores práticas para gestão de vulnerabilidades.
- ❖ A intenção é apresentar algumas necessidades e dificuldades que o cliente possui em gerenciar as vulnerabilidades encontradas em seu ambiente.
- ❖ Chamar atenção dos profissionais de segurança para importância da entrega e apresentação do relatório de pentest.
- ❖ Demonstrar possibilidades para gestão de vulnerabilidades oriundas de fontes diversas com o uso do DefectDojo.

echo \$CONTEXT

BO *São Paulo*
SIDES

Por qual razão as empresas fazem pentest?



NÃO DÁ PRA SABER

Motivos das empresas fazerem teste de invasão

Identificação de
ativos críticos

Verificar ROI de
investimento em
segurança

Regulamentações
(LGPD, PCI por
exemplo)

Boas práticas

Compliance com
frameworks
(ISO 27.000)

Identificar
Vulnerabilidades
Residuais

O que é, e não é um Teste de Invasão ?

- Busca por falhas conhecidas em sistemas
- Processo
- Executada Internamente

Análise de Vulnerabilidades



- Conformidade a uma norma ou standard
- Regulamentação
- Processos e controles definidos

Auditoria de Segurança



O que é, e não é um Teste de Invasão ?

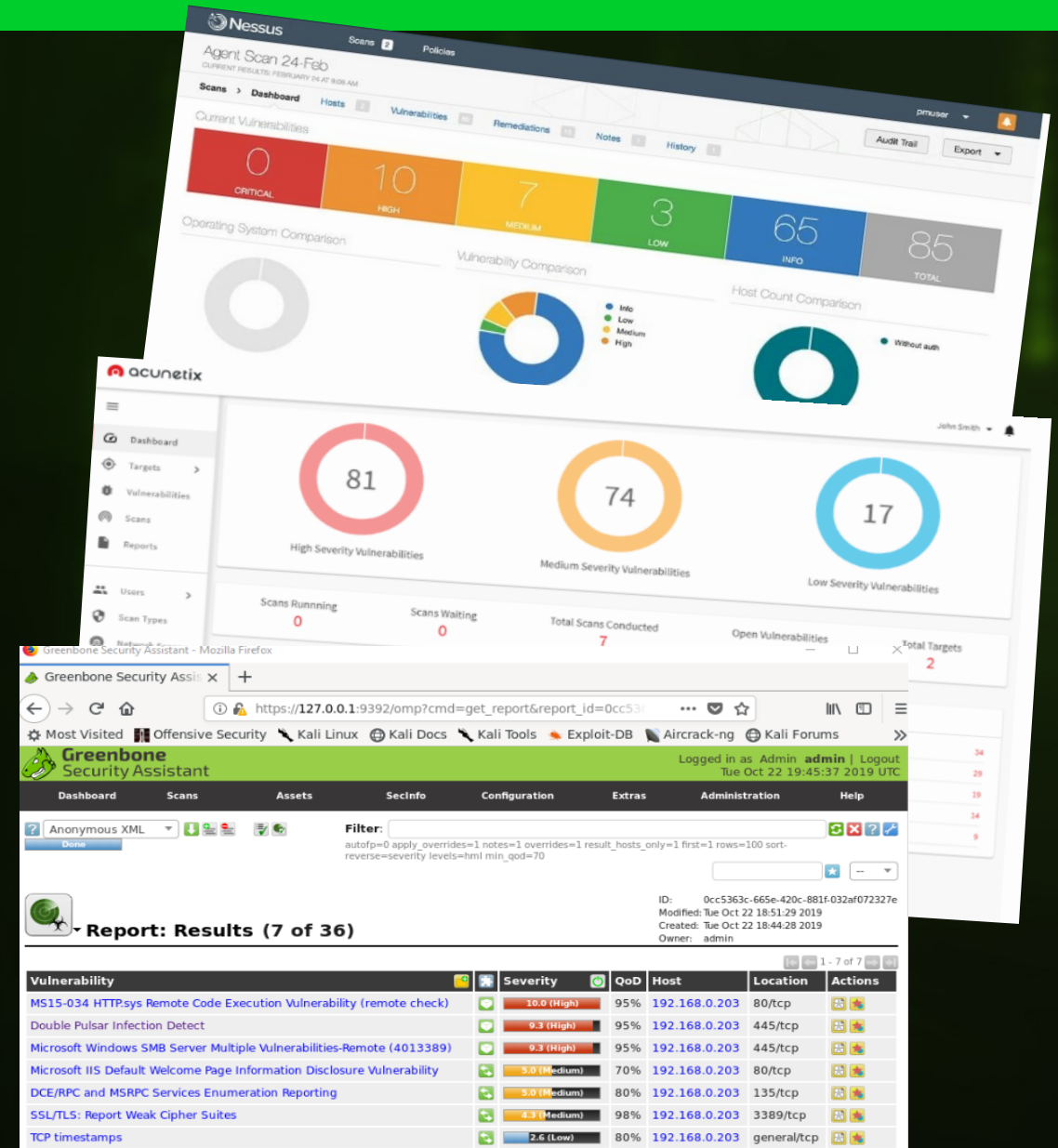
- Busca por falhas conhecidas em sistemas
- Processo
- Executada Internamente

Análise de Vulnerabilidades



- Conformidade a uma norma ou standard
- Regulamentação
- Processos e controles definidos

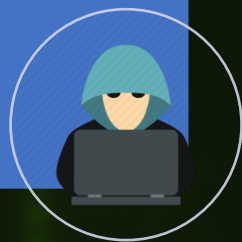
Auditoria de Segurança



Teste de Invasão (Pentest)

- Busca por falhas desconhecidas
- Não limitado a uma tecnologia ou sistema
- Profundidade não Abrangência.

Teste de invasão

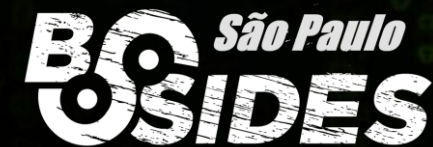


Conforme a ***Publicação 800–53 (Rev. 4) CA-8 1 do **NIST*****, teste de intrusão é definido como:

(...) o teste de intrusão é um ataque simulado **autorizado** contra um sistema, projetado para identificar e medir os riscos associados à exploração da superfície de ataque de um alvo.

Assim, um teste de intrusão, ou pentest é um modo de avaliação de um sistema, ou rede através de um ataque hacker, com o intuito de encontrar vulnerabilidades e determinar o risco delas.

Entrega do Relatório



<http://www.pentest-standard.org/index.php/Reporting>



Entrega do Relatório

Sumário

Sumário	3
1. SUMÁRIO EXECUTIVO	4
2. Escopo dos Ataques Cibernéticos	4
3. Resultado Simplificado	5
4. Recomendações Executivas	6
5. RELATÓRIO TÉCNICO	8
5.1 INTRODUÇÃO	8
5.2 OWASP - SISTEMA DE CLASSIFICAÇÃO DE VULNERABILIDADES.....	8
6 AMBIENTE DE TESTE DE INTRUSÃO	11
6.1 By-pass certificado SSL – Vulnerabilidade ALTA.....	12
6.2 Enumeração de contas válidas – Vulnerabilidade ALTA.....	14
6.3 Vazamento de informações e ou tratamento de erro inapropriado – Vulnerabilidade Baixa.	17
6.4 Configuração incorreta de segurança- chave ssl desatualizada – Vulnerabilidade Baixa.	20
6.5 Configuração incorreta de segurança, Mensagem de erro – Vulnerabilidade Baixa.	23
6.6 Exposição de dados sensíveis – Informativo.	25
7 Ferramentas utilizadas	28
8 Metodologias e padrões Utilizados.....	29



Entreguei o relatório

BO *São Paulo*
SIDES



E AGORA??

Entreguei o relatório, E AGORA??

- O cliente tem dúvidas.
- O cliente pede outra reunião.
- O desenvolvedor ou Sysadmin, diz que o item apontado no relatório não é vulnerável.



echo \$Gestão_de_Vulnerabilidades

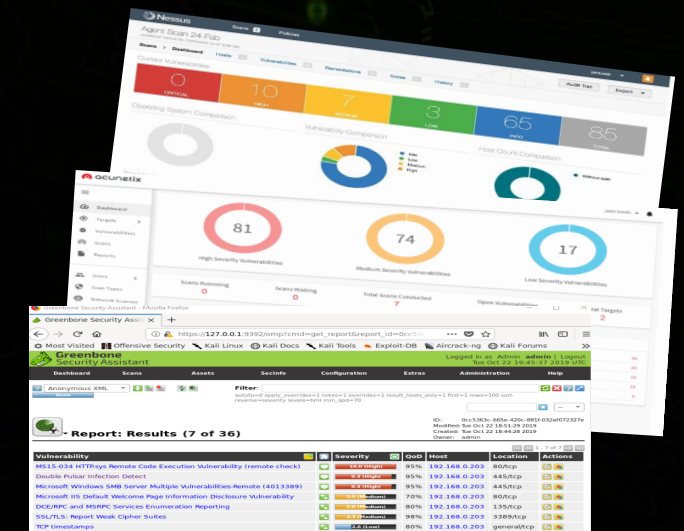
O processo de gestão de vulnerabilidades é uma abordagem estruturada e contínua para identificar, avaliar, priorizar, mitigar e monitorar vulnerabilidades em sistemas, redes, aplicativos e infraestrutura de uma organização.

Esse processo é essencial para garantir a segurança cibernética e proteger os ativos digitais contra ameaças e ataques.



echo \$Gestão_de_Vulnerabilidades

- Descoberta de ativos e inventário
- Verificações de vulnerabilidades
- Gerenciamento de patch
- Gerenciamento de configuração
- SIEM (gerenciamento de eventos e incidentes de segurança)
- Vulnerabilidades de correção



echo \$DefectDojo



O DefectDojo é uma ferramenta de gestão de vulnerabilidades de código aberto projetada para ajudar as equipes de segurança a gerenciar efetivamente as descobertas de vulnerabilidades em seus aplicativos e sistemas. Ele oferece recursos abrangentes para rastrear, priorizar, corrigir e relatar vulnerabilidades, facilitando o processo de segurança cibernética de uma organização.

DefectDojo

The screenshot displays the DefectDojo website and its dashboard. The website header includes the DefectDojo logo, an 'Open Source Security Index' badge, and navigation links for Home, Get Started, Features, Screenshots, and Contact. The main heading is 'Open Source DevSecOps', followed by the tagline 'The leading application vulnerability management tool. Built for both DevSecOps and traditional application security.' and a 'Get Started' button.

The dashboard interface is shown in the foreground, featuring a sidebar with navigation icons and a main content area. The main content area includes a 'Metadata' table, a 'Findings' bar chart, and a 'Metrics' section.

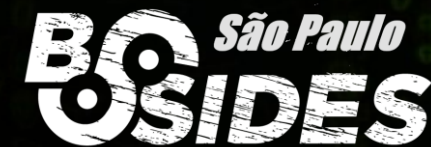
Metadata	
Business Criticality	High
Product Type	Research and Development
Platform	Web
Lifecycle	Construction
Origin	Third Party Library
User Records	1,000
Revenue	50,000.00

The 'Findings' bar chart shows the distribution of findings by severity: Critical (0), High (30), Medium (79), and Low (79). The 'Metrics' section displays a summary of findings by severity: 0 Critical, 30 High, 79 Medium, and 79 Low.

The bottom of the dashboard shows a video player with a progress bar and a 'Got it!' button.

<https://github.com/DefectDojo/django-DefectDojo>

DefectDojo/reposi rio



github.com/DefectDojo/django-DefectDojo

Product Solutions Open Source Pricing Search or jump to... Sign in

DefectDojo / django-DefectDojo Public

Notifications Fork 1.5k Star 3.4k

<> Code Issues 246 Pull requests 89 Discussions Actions Projects Security 8 Insights

master 157 Branches 185 Tags Go to file Code

Maffooch Merge pull request #10194 from DefectDojo/release/2.34.3 2234848 · 2 days ago 10,269 Commits

.github	Update azure/setup-helm action from v4.1.0 to v4.2.0 (.github...	last month
components	Update versions in application files	2 days ago
docker	Gunicorn: Legacy cleanup (#9953)	last month
docs	Fix(api-sq): Doc: typo in multi branch scanning (#10186)	2 days ago
dojo	Update versions in application files	2 days ago
helm/defectdojo	Update versions in application files	2 days ago
nginx	Fix: HTTP->HTTPS redirect path (#8358)	10 months ago
readme-docs	Make the number of request/response pairs returned by the...	3 weeks ago
setup	Fix list indentation in docs (#6419)	2 years ago
tests	Ruff: add isort (#9754)	2 weeks ago
unittests	fix severity in sonarqube scan detailed (#10157)	2 days ago
.dockerignore	test(integration): Install Chromedriver during dockerbuild (#...	3 years ago
.dryrunsecurity.yaml	Updated DryRun Security config (#10037)	3 weeks ago
.flake8	Flake8: Remove useless ignores (#9760)	2 months ago

About

DevSecOps, ASPM, Vulnerability Management. All on one platform.

defectdojo.com

python kubernetes security automation django analytics owasp vulnerability-databases appsec vulnerability-management hactoberfest security-orchestration security-automation devsecops vulnerability-correlation

Readme

BSD-3-Clause license

Security policy

Activity

Custom properties

3.4k stars

208 watching

1.5k forks

Report repository

Releases 176

2.34.3 Latest

https://github.com/DefectDojo/django-DefectDojo

DefectDojo/Documentação

← → ↺ 🏠 🔍 documentation.defectdojo.com

DEFECT DOJO DOCUMENTAÇÃO

🏠 Pagina inicial 📷 Site de demonstração 🌐 GitHub

🔍 Pesquise neste sit

Documentação do DefectDojo

📖 Base de conhecimento

Começando

Arquitetura

Instalação

Configuração

Executando em produção

Atualizando

Demonstração

Uso

Classes de dados principais

Características

Classificação de saúde do produto

Permissões

Documentação do DefectDojo

DEFECT DOJO

Search... 🔍 227 👤

🎯 45 Active Engagements
View Engagement Details

🐛 0 Last Seven Days
View Finding Details

🚫 2 Closed In Last Seven Days
View Finding Details

✅ 4 Accepted In Last Seven Days
View Finding Details

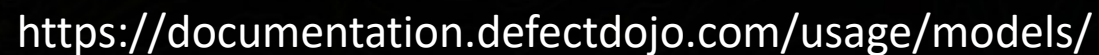
Historical Finding Severity

Reported Finding Severity by Month

O que é DefectDojo?

DefectDojo é uma plataforma DevSecOps. O DefectDojo agiliza o DevSecOps servindo como um agregador e um painel único para suas ferramentas de segurança. O DefectDojo possui recursos inteligentes para aprimorar e ajustar os resultados de suas ferramentas de segurança, incluindo a capacidade de mesclar descobertas, lembrar falsos positivos e destilar duplicatas. O DefectDojo também se integra ao JIRA, fornece métricas/relatórios e também pode ser usado para gerenciamento tradicional de pen test.

<https://documentation.defectdojo.com/>



DefectDojo/Demo

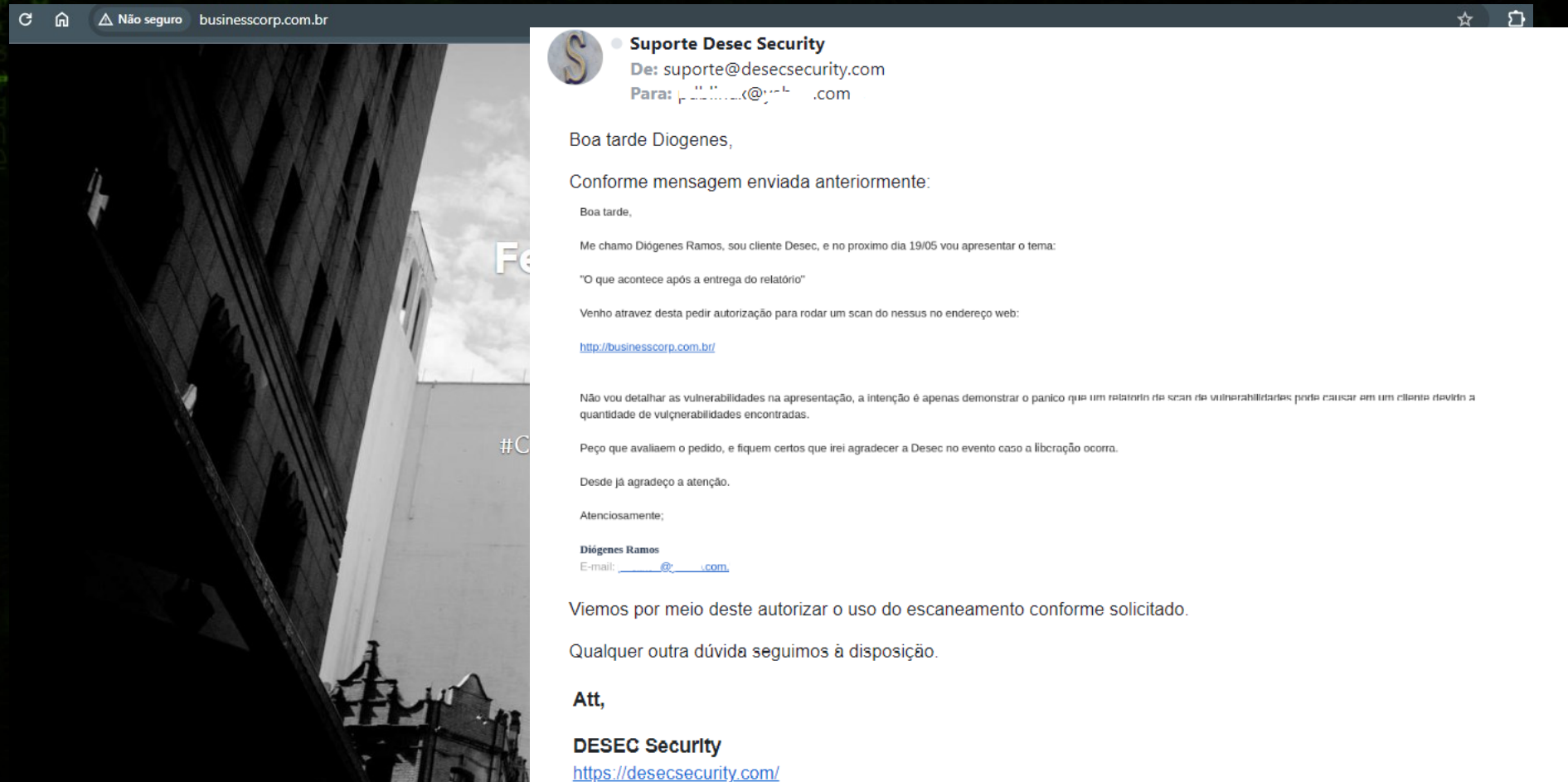
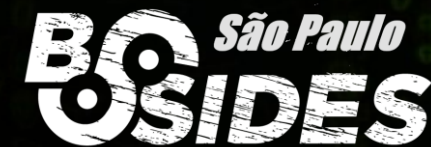


<https://demo.defectdojo.org/login>

User: admin

Pass: 1Defectdojo@demo#appsec

DefectDojo/Demo



Agradecimento ao time Desec Security que autorizou o scan no site Businesscorp

DefectDojo/Demo



teste_DefectDojo

Wed, 15 May 2024 18:29:27 EDT

TABLE OF CONTENTS

Vulnerabilities by Host

- businesscorp.com.br

Vulnerabilities by Host

[Collapse All](#) | [Expand All](#)

businesscorp.com.br



Scan Information

Start time: Wed May 15 16:51:58 2024
End time: Wed May 15 18:29:27 2024

Host Information

DNS Name: businesscorp.com.br
IP: 37.59.174.225
OS: Dell PowerEdge Blade Chassis

```
➦$ nuclei -target businesscorp.com.br -s critical,high,medium,low,info -json-export nuclei_Dojo.json
```



v3.2.4

projectdiscovery.io

```
[INF] Current nuclei version: v3.2.4 (outdated)
[INF] Current nuclei-templates version: v9.8.6 (latest)
[WRN] Scan results upload to cloud is disabled.
[INF] New templates added in latest release: 65
[INF] Templates loaded for current scan: 7923
[INF] Executing 7923 signed templates from projectdiscovery/nuclei-templates
[INF] Targets loaded for current scan: 1
[INF] Running httpx on input host
[INF] Found 1 URL from httpx
[INF] Templates clustered: 1471 (Reduced 1397 Requests)
[nameserver-fingerprint] [dns] [info] businesscorp.com.br ["ns1.businesscorp.com.br.", "ns2.businesscorp.com.br."]
[spf-record-detect] [dns] [info] businesscorp.com.br ["v=spf1 include:key-9283947588214 ?all"]
[txt-fingerprint] [dns] [info] businesscorp.com.br ["v=spf1 include:key-9283947588214 ?all"]
[mx-fingerprint] [dns] [info] businesscorp.com.br ["10 mail.businesscorp.com.br."]
[caa-fingerprint] [dns] [info] businesscorp.com.br
[INF] Using Interactsh Server: oast.online
```

tasks

New scan New live task

3. Crawl and audit of businesscorp.com.br

Summary Audit items Issues Event log Logger Audit log Live crawl view

Filter Search

3. Crawl and audit of businesscorp.com.br

Crawl and Audit - Deep

Finished

Issues: 0 11 1 46

2. Live audit from Proxy (all traffic)

Audit checks - passive

Capturing

Issues: 0 0 11 5

1. Live passive crawl from Proxy (all traffic)

Add links. Add item itself. same domain and URLs in suite scope.

Capturing

Most serious vulnerabilities found (live)

View all

Issue type	Host	Time
HTTP request smuggling	http://businesscorp.com.br	11:01:55 16 May 2024
HTTP request smuggling	http://businesscorp.com.br	11:02:11 16 May 2024
HTTP request smuggling	http://businesscorp.com.br	11:07:51 16 May 2024
HTTP request smuggling	http://businesscorp.com.br	11:07:24 16 May 2024
HTTP request smuggling	http://businesscorp.com.br	11:03:56 16 May 2024
HTTP request smuggling	http://businesscorp.com.br	10:59:54 16 May 2024
HTTP request smuggling	http://businesscorp.com.br	11:08:26 16 May 2024
HTTP request smuggling	http://businesscorp.com.br	11:08:12 16 May 2024
HTTP request smuggling	http://businesscorp.com.br	11:07:56 16 May 2024
HTTP request smuggling	http://businesscorp.com.br	10:59:05 16 May 2024
Vulnerable JavaScript dependency	http://businesscorp.com.br	10:56:20 16 May 2024
Backup file	http://businesscorp.com.br	11:02:10 16 May 2024
Input returned in response (reflected)	http://businesscorp.com.br	11:05:41 16 May 2024
Input returned in response (reflected)	http://businesscorp.com.br	11:05:55 16 May 2024
Input returned in response (reflected)	http://businesscorp.com.br	11:08:13 16 May 2024
Input returned in response (reflected)	http://businesscorp.com.br	11:08:57 16 May 2024
Input returned in response (reflected)	http://businesscorp.com.br	11:11:26 16 May 2024
Input returned in response (reflected)	http://businesscorp.com.br	11:11:33 16 May 2024
Input returned in response (reflected)	http://businesscorp.com.br	11:11:39 16 May 2024
Input returned in response (reflected)	http://businesscorp.com.br	11:11:47 16 May 2024
Input returned in response (reflected)	http://businesscorp.com.br	11:11:49 16 May 2024
Input returned in response (reflected)	http://businesscorp.com.br	11:11:50 16 May 2024
Input returned in response (reflected)	http://businesscorp.com.br	11:11:40 16 May 2024
Input returned in response (reflected)	http://businesscorp.com.br	11:11:40 16 May 2024
Input returned in response (reflected)	http://businesscorp.com.br	11:11:35 16 May 2024
Input returned in response (reflected)	http://businesscorp.com.br	11:11:26 16 May 2024

Task configuration

View configuration

Task type: Crawl & audit

Scope: businesscorp.com.br

Configuration: Crawl and Audit - Deep

Task progress

Total audit items:	58	Unique locations:	54
Audit items pending:	0	Pending actions:	0
Audit items in progress:	0	Current link depth:	0
Audit items completed:	58	Requests:	15090
		Network errors:	5

Task log

Auditing "http://businesscorp.com.br/js/jquery.migrate-1.2.1.min.js" for Backdash Powered Scanning Differences

Auditing "http://businesscorp.com.br/js/jquery.migrate-1.2.1.min.js" for Plain Reflections

Auditing "http://businesscorp.com.br/robots.txt" for Backup Files Replace Extension

Auditing "http://businesscorp.com.br/robots.txt" for Backup Files Prefix Filename

Auditing "http://businesscorp.com.br/robots.txt" for Backup Files Append Extension

Auditing "http://businesscorp.com.br/robots.txt" for Backup Files Append Filename

Auditing "http://businesscorp.com.br/robots.txt" for Broken Access Control

Auditing "http://businesscorp.com.br/robots.txt" for GraphQL Content Type Not validated

Auditing "http://businesscorp.com.br/robots.txt" for GraphQL Suggestions Enabled

Auditing "http://businesscorp.com.br/robots.txt" for GraphQL Introspection Enabled

Auditing "http://businesscorp.com.br/robots.txt" for Web Cache Entanglement

Auditing "http://businesscorp.com.br/robots.txt" for Web Cache Poisoning

Auditing "http://businesscorp.com.br/robots.txt" for ASP.NET Tracing Enabled

Auditing "http://businesscorp.com.br/robots.txt" for Path Traversal StyleSheet Import

Auditing "http://businesscorp.com.br/robots.txt" for Cross Site Request Forgery

echo \$Considerações

BO *São Paulo*
SIDES



echo \$Considerações

- ❖ Tanto o Scan de vulnerabilidades quanto ao pentest fornece ao cliente uma foto momentânea do ambiente.
- ❖ A gestão de vulnerabilidades é o comparativo destas “fotos” ao longo do tempo, permitindo a empresa como está a evolução da maturidade de segurança ao longo do tempo.
- ❖ O Defectdojo permite que a gestão de diferentes “produtos” sejam gerenciados em um mesmo ambiente.
- ❖ Assim como toda solução Open Source é necessário capacitação do time para suportar a aplicação, assim como realizar as customizações necessárias para adequações da empresa.

Referências para estudos posteriores

Site DefectDojo:

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

Repositório:

<https://github.com/DefectDojo/django-DefectDojo>

Ambiente de demonstração :

<https://demo.defectdojo.org/login>

Documentação:

<https://documentation.defectdojo.com/>

echo \$CONTATOS

BOSIDES *São Paulo*



<https://www.linkedin.com/in/diogenes-r-9a0427a/>



<https://becodoexploit.com/>

echo \$OBRIGADO

BO São Paulo
SIDES



<https://www.linkedin.com/in/diogenes-r-9a0427a/>