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

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 $CONTEXTO

São Paulo BSIDES

Por qual razão as empresas fazem pentest?

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

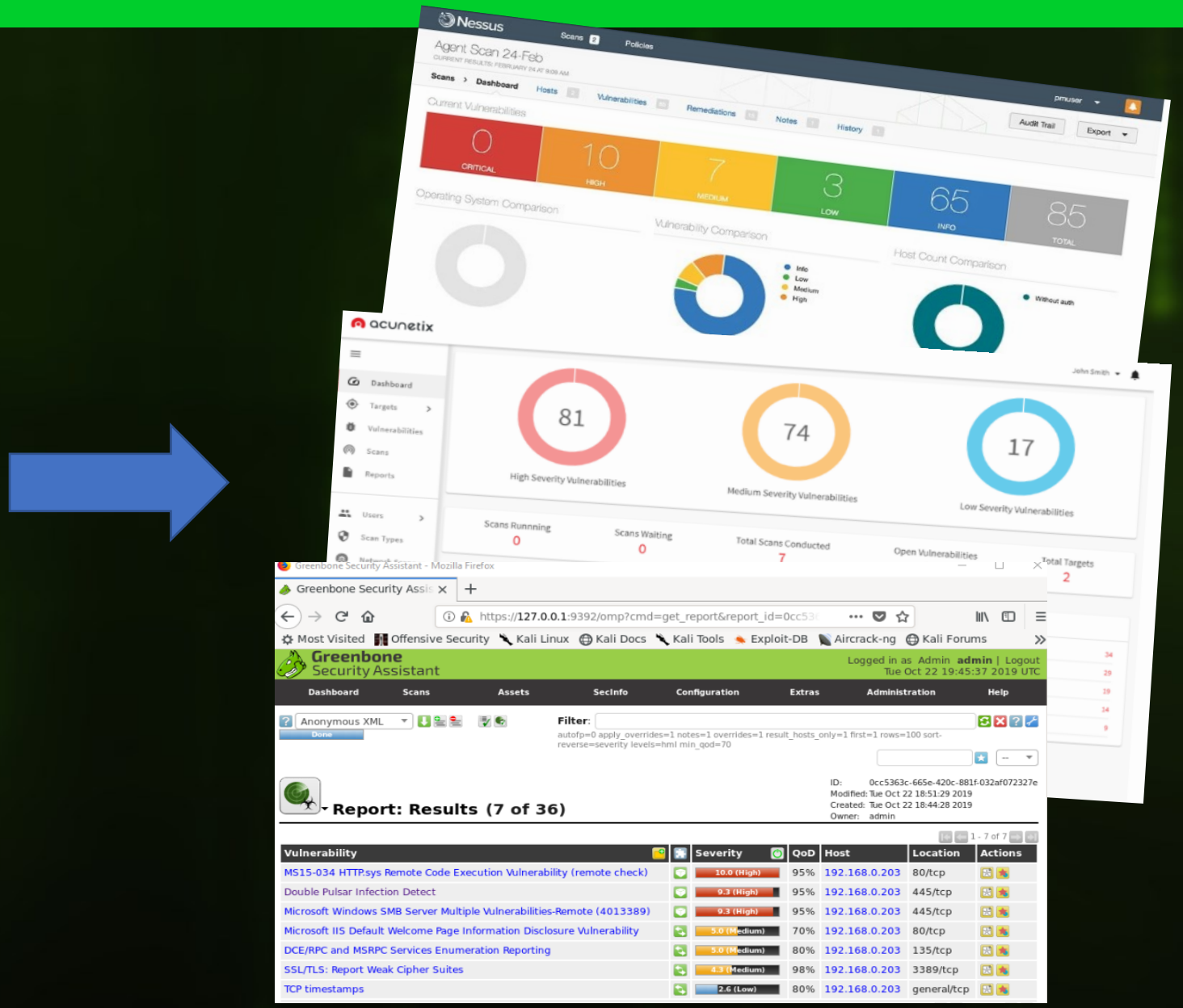
O que é, e não é um Teste de Invasão ?

- 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

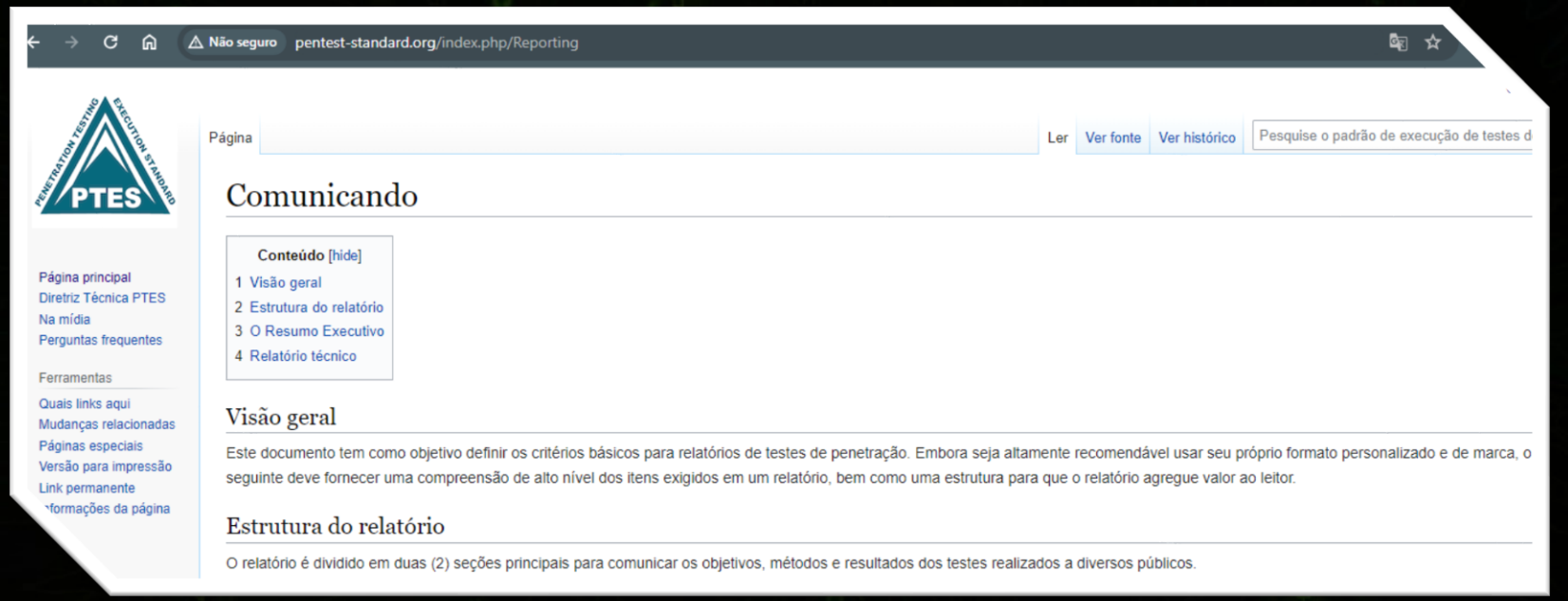
Conforme a ***Publicação 800–53 (Rev. 4) CA-8 1 do **NIST ****, teste de intrusão é definido como:

(...) 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.

https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf

Entrega do Relatório



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

Entrega do Relatório

Sumário

Entreguei o relatório

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

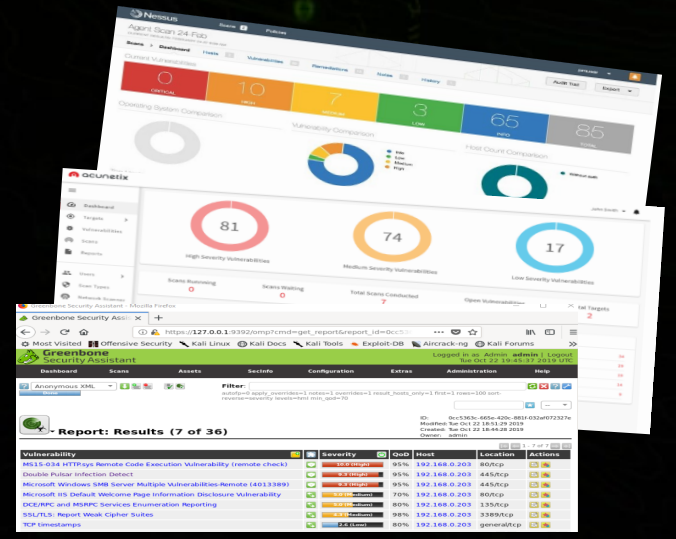
São Paulo BSIDES

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



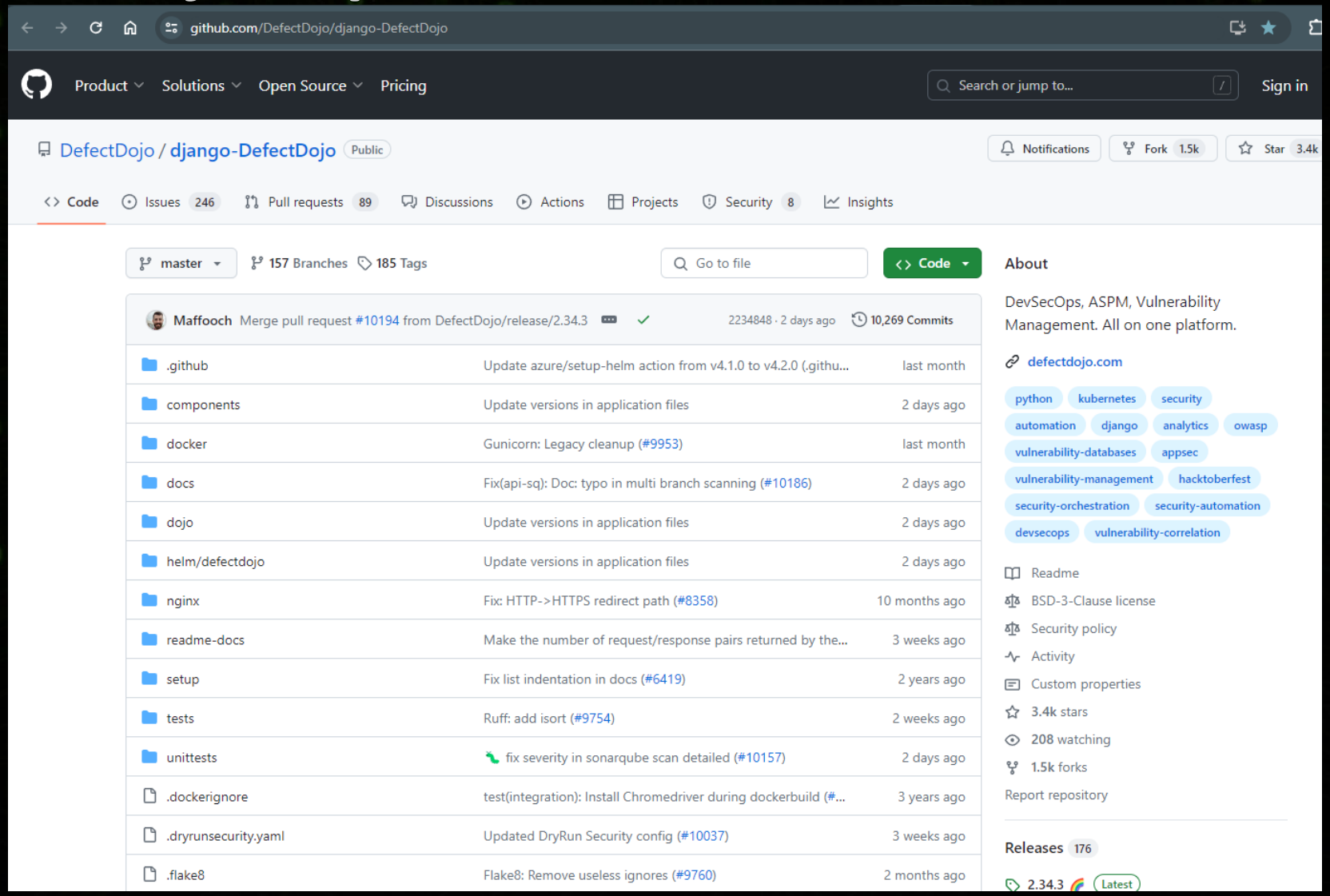
echo $DefectDojo

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

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

DefectDojo/repositório

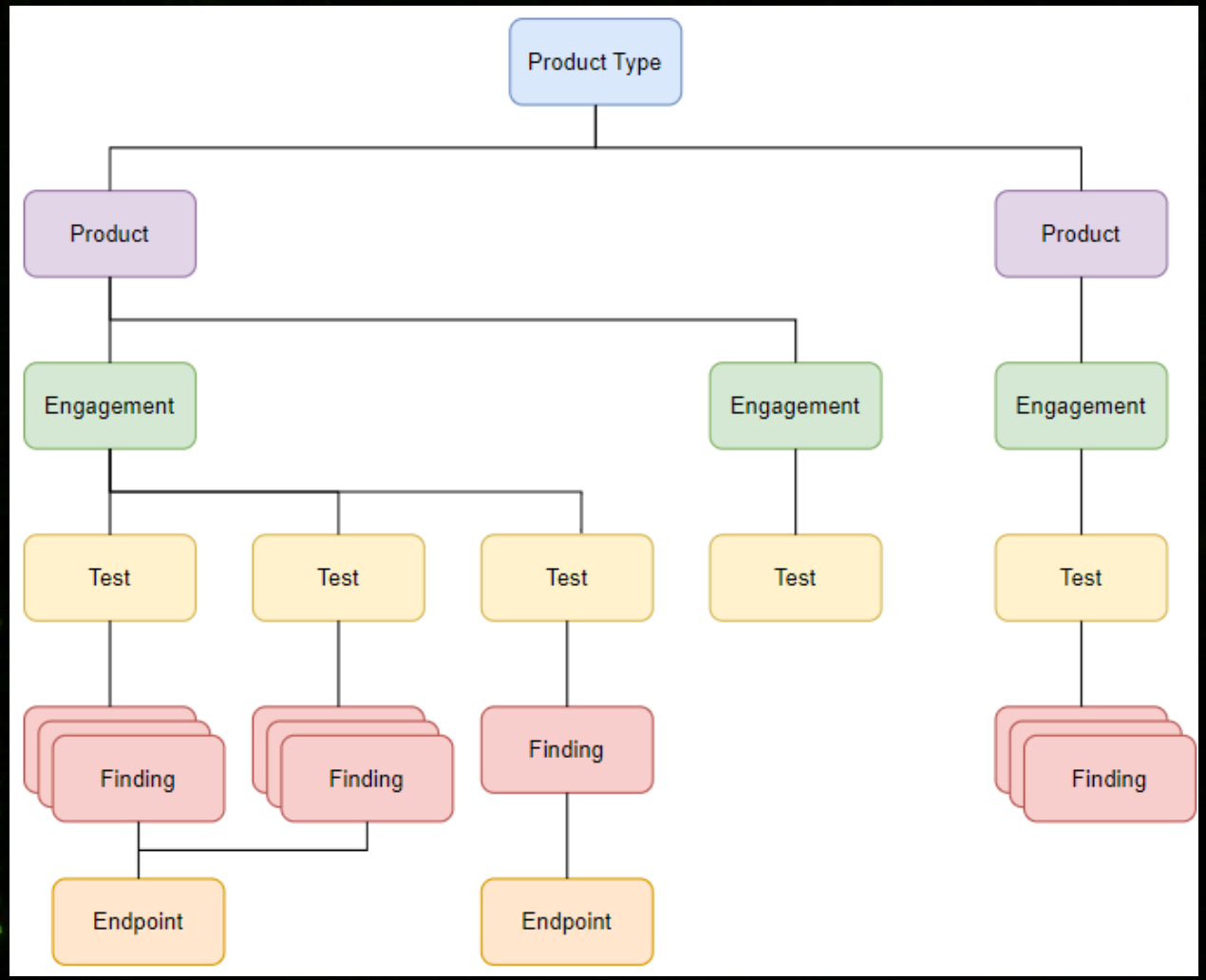


https://github.com/DefectDojo/django-DefectDojo

DefectDojo/Documentação

https://documentation.defectdojo.com/

DefectDojo/Modelo_Uso



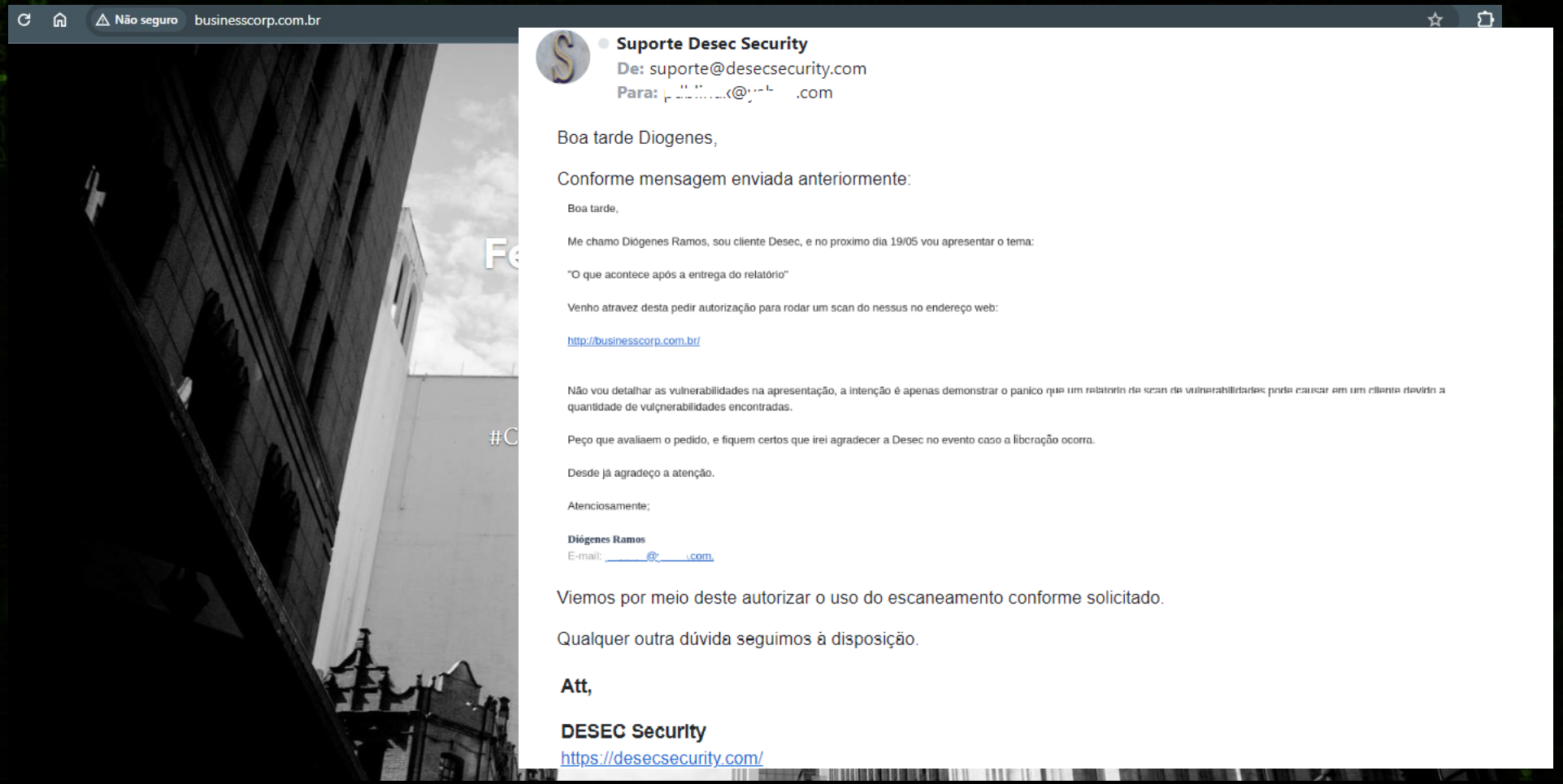
https://documentation.defectdojo.com/usage/models/

DefectDojo/Demo

https://demo.defectdojo.org/login

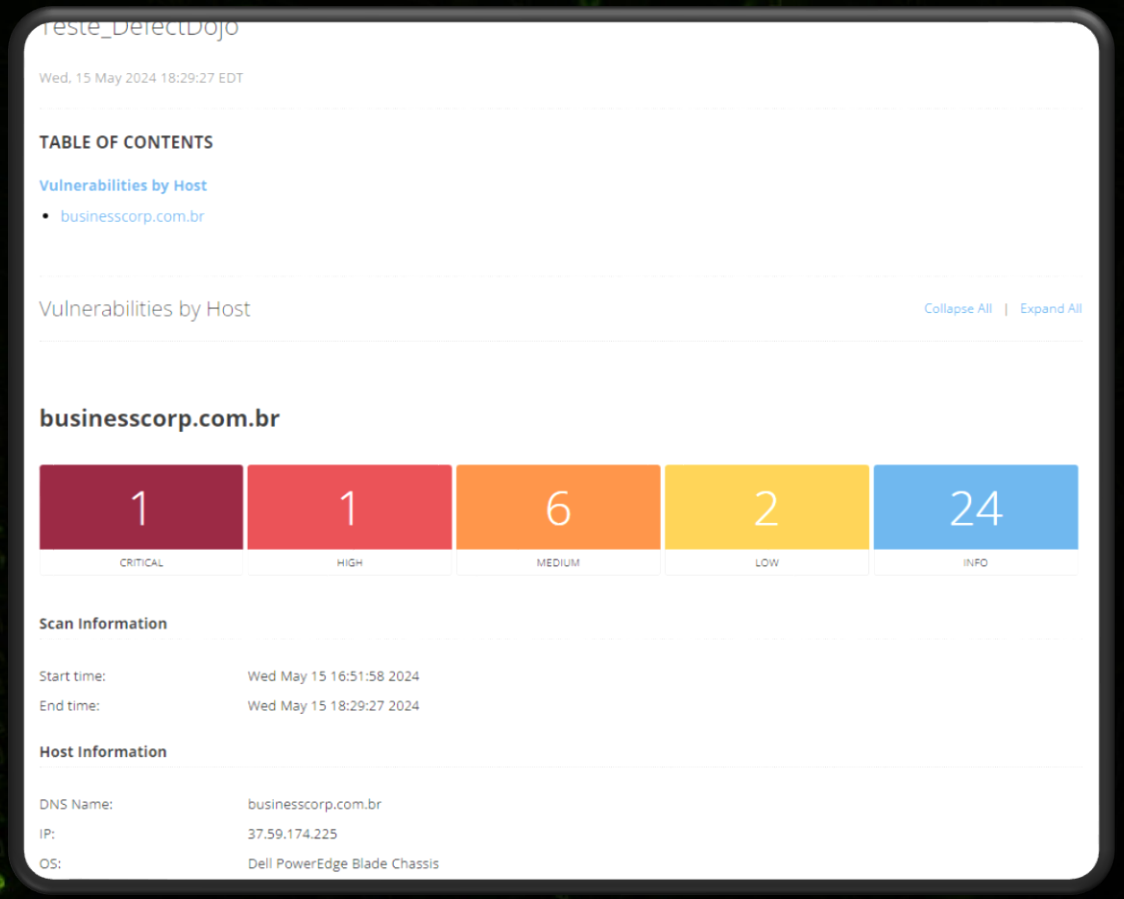
User: admin
Pass: 1Defectdojo@demo#appsec

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

1	1	6	2	24
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Wed May 15 16:51:58 2024

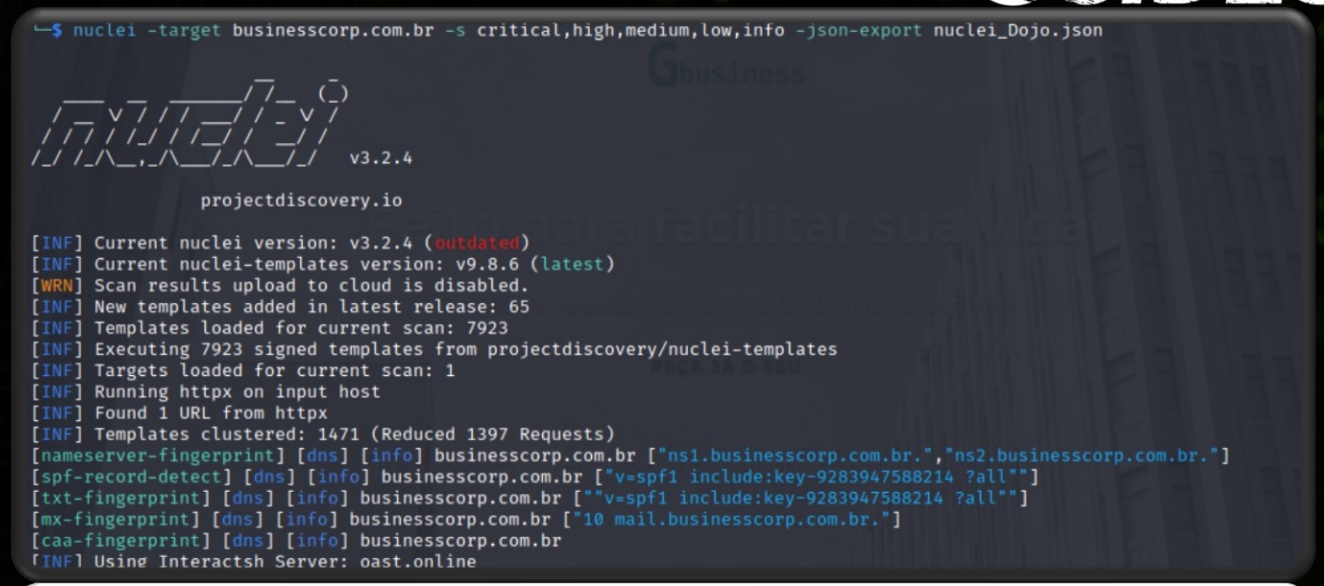
End time: Wed May 15 18:29:27 2024

Host Information

DNS Name: businesscorp.com.br

IP: 37.59.174.225

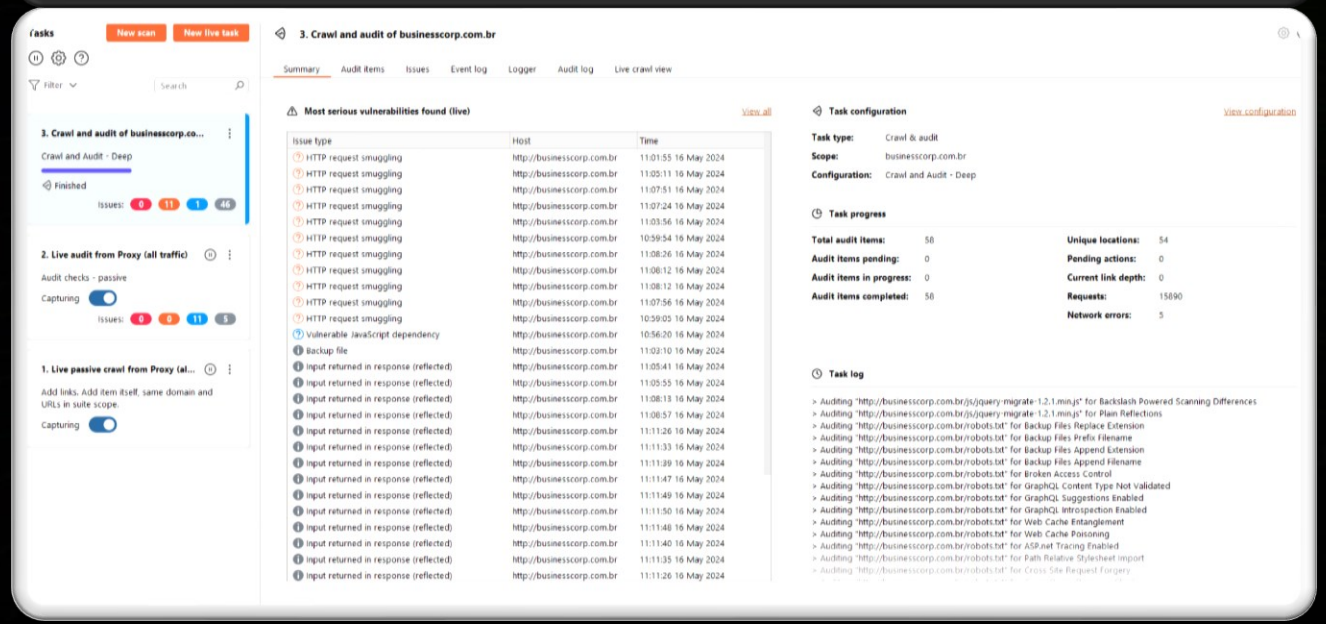
OS: Dell PowerEdge Blade Chassis


```
└─$ 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
```



echo $Considerações

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 logo 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

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

https://becodoexploit.com/

echo $OBRIGADO

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