



RNEP-GW

MÓDULO GESTÃO DE VULNERABILIDADES



O QUE É?

Monitorização de vulnerabilidades

Diversos websites

Obter informação para priorizar a mitigação de vulnerabilidades

Destinado a websites de elevada relevância



VULNERABILIDADES



Risco aumenta com a exposição à Internet

As vulnerabilidades exploráveis podem ser um problema sério

Não se pode descurar o aparecimento de novas vulnerabilidades

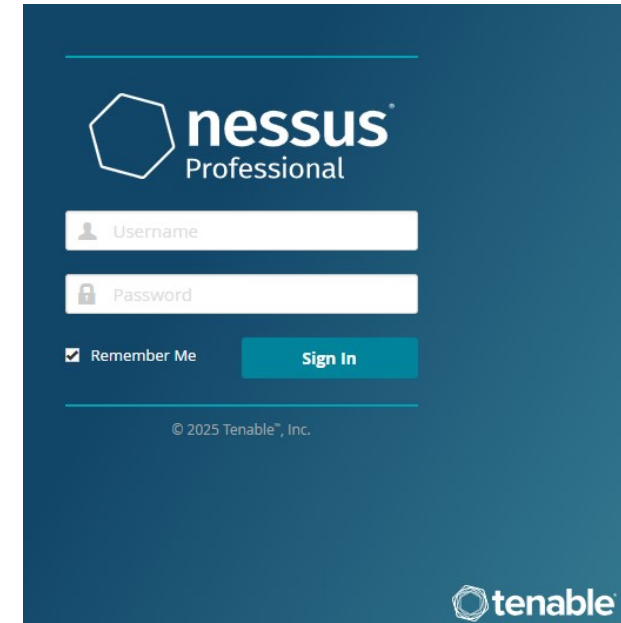
COMO FUNCIONA?

Agendamento periódico de «scans»

Ferramenta comercial (Nessus)

Apenas a pedido das entidades

O objetivo é sempre nunca degradar os serviços analisados



QUE BENEFÍCIOS?



Receber um relatório produzido pela ferramenta

As vulnerabilidades são classificadas

Saber onde são prioritárias intervenções

CONFIGURAÇÃO

Settings | Credentials | Plugins 

BASIC 

- General
- Schedule
- Notifications

DISCOVERY >

ASSESSMENT >

REPORT >

ADVANCED >

General Settings

Name

IPLEIRIA websites

Description

Scans Mensais IPLEIRIA

Folder

RCTS - Membros 

Targets

portaldoestudante.ipleiria.pt, sasocial.ipleiria.pt, intranet.ipleiria.pt, www.ipleiria.pt

Upload Targets

Add File

RESULTADOS

☐ Host	Vulnerabilities ▾	
☐ alc [REDACTED]	22 32 4 69	×
☐ doc [REDACTED]	2 4 29	×
☐ ale [REDACTED]	2 2 22	×
☐ sia [REDACTED]	21	×
☐ sia [REDACTED]	1 14	×
☐ tot [REDACTED]	1 10	×
☐ vir [REDACTED]	2	×

Scan Details

Policy: Web Application Tests
 Status: Completed
 Severity Base: CVSS v2.0 
 Scanner: Local Scanner
 Start: June 24 at 2:00 AM
 End: June 24 at 5:10 AM
 Elapsed: 3 hours

Vulnerabilities



EXEMPLO DE RELATÓRIO



Scan Information

Start time: Sat Nov 19 05:00:34 2022
End time: Sat Nov 19 05:36:04 2022

Host Information

DNS Name: acad[REDACTED]
IP: [REDACTED]
OS: Ubuntu 16.04 Linux Kernel 4.4

Vulnerabilities

142960 - HSTS Missing From HTTPS Server (RFC 6797)

Synopsis

The remote web server is not enforcing HSTS, as defined by RFC 6797.

Description

The remote web server is not enforcing HSTS, as defined by RFC 6797. HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

See Also

<https://tools.ietf.org/html/rfc6797>

Solution

Configure the remote web server to use HSTS.

Risk Factor

Medium

CVSS

Common Vulnerability Scoring System

«Scores» de 0 a 10

Referências:

www.first.org/cvss

nvd.nist.gov/vuln-metrics/cvss

euvd.enisa.europa.eu



IDEIAS CHAVE



É importante mitigar vulnerabilidades



Temos que conseguir estabelecer prioridades



Existem diversas ferramentas que permitem realizar estas análises



Questões?

Obrigado.



csirt.fct.pt/podcast



csirt.fct.pt/mooc



csirt.fct.pt/etc