



UNIVERSIDADE
FEDERAL DO CEARÁ



UNIVERSIDADE
ESTADUAL DO CEARÁ

Ferramentas de Teste de Segurança



Leonardo Oliveira Silva

Ismayle de Sousa Santos

Agenda

- Ferramentas de Segurança da Informação
 - Tipos de Ferramentas
- Exemplos de Ferramentas
 - Nmap
 - Burp Suite
 - OWASP Zap
 - WireShark
- Estudo de Caso de Testes de Segurança



Ferramentas de Segurança da Informação

Ferramentas de Segurança da Informação

- São programas ou conjuntos de software desenvolvidos para auxiliar na avaliação, identificação e mitigação de vulnerabilidades e ameaças em sistemas de TI e aplicações
- Desempenham um papel crucial na proteção contra ataques cibernéticos e na manutenção da integridade, confidencialidade e disponibilidade dos sistemas

Tipos de Ferramentas

- **Scanners de Vulnerabilidade:** Essas ferramentas escaneiam redes, sistemas ou aplicativos em busca de vulnerabilidades conhecidas. Elas identificam pontos fracos que podem ser explorados por atacantes.
- **Ferramentas de Teste de Intrusão (PenTest Tools):** São usadas para simular ataques cibernéticos reais em um ambiente controlado. Testes de invasão são conduzidos para identificar e explorar vulnerabilidades em sistemas

Tipos de Ferramentas

- **Firewall e IDS/IPS (Intrusion Detection/Prevention Systems):** Essas soluções monitoram o tráfego de rede em tempo real para identificar e responder a atividades suspeitas ou maliciosas.
- **Antivírus e Anti-Malware:** Essas ferramentas são projetadas para detectar e remover softwares maliciosos, como vírus, worms, trojans, entre outros

Tipos de Ferramentas

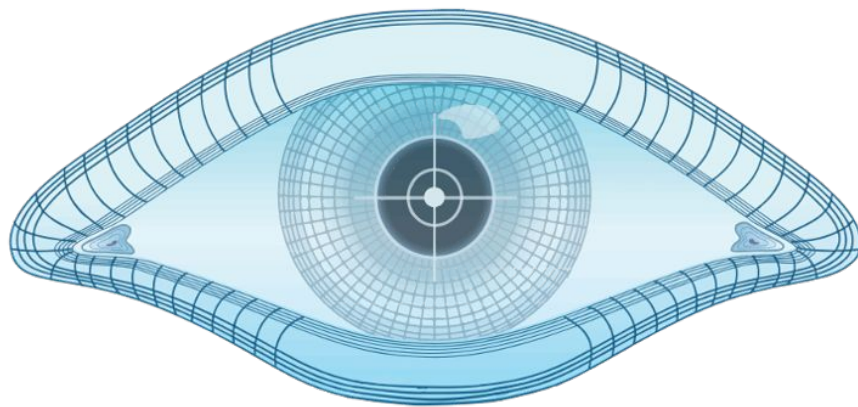
- **Ferramentas de Criptografia:** Oferecem meios para criptografar dados em trânsito e em repouso, garantindo que apenas as partes autorizadas possam acessar as informações.
- **Ferramentas de Análise de Tráfego:** Permitem a inspeção detalhada do tráfego de rede para identificar padrões suspeitos ou anômalos.

Tipos de Ferramentas

- **Gerenciadores de Senhas e Cofres de Credenciais:** São projetados para armazenar senhas e credenciais de forma segura, garantindo a gestão eficaz de autenticação
- **Ferramentas de Monitoramento de Segurança:** Permitem a supervisão constante de eventos de segurança e a geração de alertas em caso de atividades suspeitas

Tipos de Ferramentas

- **Ferramentas de Forense Digital:** Ajudam na coleta, preservação e análise de evidências digitais para investigação de incidentes de segurança.
- **Honeypots e Honeynets:** Simulam sistemas ou redes falsas para atrair e monitorar atividades de atacantes, permitindo a identificação de táticas e técnicas utilizadas



Nmap

O que é Nmap?

- Abreviação de "Network Mapper"
- É uma ferramenta de código aberto para exploração de rede e auditoria de segurança
- É frequentemente utilizado para avaliar a segurança de uma rede, identificar hosts ativos, descobrir quais serviços estão sendo executados e verificar se há vulnerabilidades ou portas abertas que possam ser exploradas por atacantes
 - Pode ser utilizado tanto em sistemas Unix/Linux como em sistemas Windows

O que é Nmap?

- É uma das ferramentas mais importantes no que se refere a fases iniciais do PenTest
- Documentação
 - https://nmap.org/man/pt_BR/index.html
- Instalação
 - <https://nmap.org/download.html>

Funcionalidades do Nmap

- Determina quais hospedeiros estão disponíveis nas redes, quais serviços eles estão oferecendo, quais sistemas operacionais (e suas versões) estão rodando, que tipo de pacotes / firewalls estão em uso, etc.
- Para Windows, sua versão mais utilizada é a com interface gráfica: o Zenmap

Funcionalidades do Nmap

- Scanning de redes e de portas
- Scanning de serviços e de versões
- Descoberta dos sistemas operacionais dos computadores escaneados
- Exploração de vulnerabilidades

Funcionalidades do Nmap

Hosts Services

Saída do Nmap Ports / Hosts Topology Detalhes da Máquina Scans

OS Host

192.168.0.241

```
nmap -T4 -A -v 192.168.0.241

Host is up (0.00075s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE          VERSION
135/tcp    open  msrpc            Microsoft Windows RPC
139/tcp    open  netbios-ssn      Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds?    Microsoft Windows [unidentified]
808/tcp    open  mc-nmf           .NET Message Framing
9001/tcp   open  http             Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

|_ http-title: Not Found
|_ http-server-header: Microsoft-HTTPAPI/2.0
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1809 - 1909
Network Distance: 0 hops
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_ smb2-security-mode:
|   3.1.1:
|     Message signing enabled but not required
|_ smb2-time:
|   date: 2022-04-01T07:23:45
|_ start_date: N/A

NSE: Script Post-scanning.
Initiating NSE at 04:24
Completed NSE at 04:24, 0.00s elapsed
Initiating NSE at 04:24
Completed NSE at 04:24, 0.00s elapsed
Initiating NSE at 04:24
Completed NSE at 04:24, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/
Nmap done: 1 IP address (1 host up) scanned in 46.64 seconds
Raw packets sent: 1019 (46.402KB) | Rcvd: 2044 (86.894KB)
```

Hosts Services

Saída do Nmap Ports / Hosts Topology Detalhes da Máquina Scans

OS Host

192.168.0.241

Port	Protocol	State	Service	Version
135	tcp	open	msrpc	Microsoft Windows RPC
139	tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
445	tcp	open	microsoft-ds	
808	tcp	open	mc-nmf	.NET Message Framing
9001	tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

Zenmap

Scan Tools Perfil Ajuda

Alvo: 192.168.0.241

Comando: nmap -T4 -A -v 192.168.0.241

Hosts Services

Saída do Nmap Ports / Hosts Topology Detalhes da Máquina Scans

OS Host

192.168.0.241

192.168.0.241

- Status da Máquina
 - Estado: up
 - Open ports: 5
 - Portas Filtradas: 0
 - Portas Fechadas: 995
 - Portas analisadas: 1000
 - Tempo ligado: Indisponível
 - Última inicialização: Indisponível
- Endereços
 - IPv4: 192.168.0.241
 - IPv6: Indisponível
 - MAC: Indisponível
- Sistema Operacional
 - Nome: Microsoft Windows 10 1809 - 1909
 - Precisão: 100%
 - Portas usadas
 - OS Classes
- Sequência TCP
- Sequência IP ID
- Sequência TCP TS
- Comentários



Burp Suite

O que é o Burp Suite?

- É uma plataforma integrada para a realização de testes de segurança
- Suas diversas ferramentas funcionam desde o mapeamento e análise de superfície de ataque de uma requisição inicial até o encontro e exploração de vulnerabilidades de segurança

O que é o Burp Suite?

- Documentação
 - <https://portswigger.net/burp/documentation>
- Instalação
 - <https://portswigger.net/burp/releases/professional-community-2022-5-1?requestededition=community&requestedplatform=>

Funcionalidades do Burp Suite

- Intercepção do tráfego HTTP entre cliente e servidor
- Modificação, coleta e análise das requisições e respostas de aplicações
- Detecção de vulnerabilidades de segurança e geração automática de um relatório (Scanner Pro)
- Penetration testing
 - <https://portswigger.net/burp/documentation/desktop/penetration-testing>
 - <https://portswigger.net/burp/pro/features>



OWASP ZAP

O que é OWASP ZAP?

- O Zed Attack Proxy (ZAP) é uma ferramenta gratuita de teste de penetração de código aberto mantida sob a égide do Open Web Application Security Project (OWASP)
- O ZAP foi projetado especificamente para testar aplicativos da Web e é flexível e extensível



O que é OWASP ZAP?

- Em sua essência, o ZAP é o que é conhecido como “proxy man-in-the-middle”
- Ele fica entre o navegador do testador e o aplicativo da Web para que possa interceptar e inspecionar as mensagens enviadas entre o navegador e o aplicativo da Web, modificar o conteúdo, se necessário, e encaminhar esses pacotes para o destino

O que é OWASP ZAP?

- Documentação
 - <https://www.zaproxy.org/docs/>
- Instalação
 - <https://www.zaproxy.org/download/>



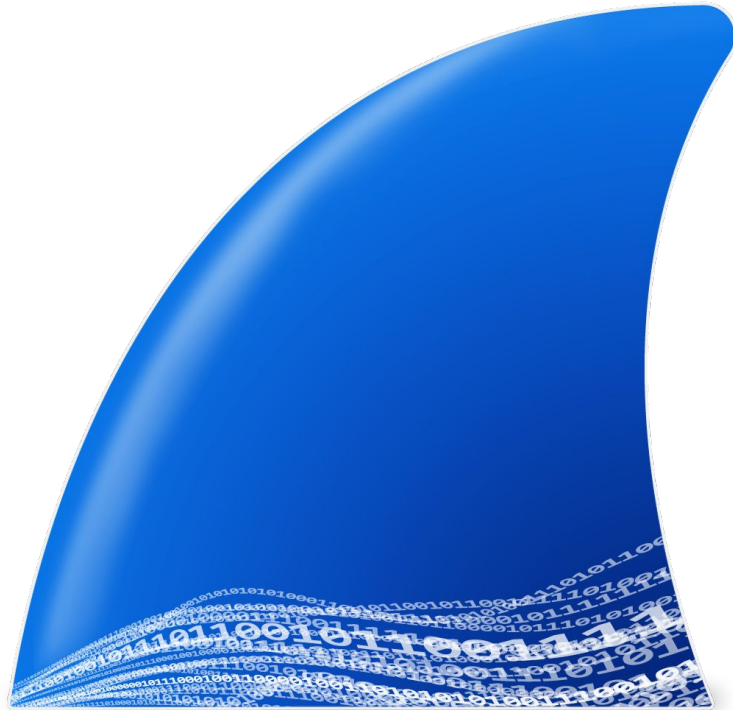
O que é OWASP ZAP?

- Se já houver outro proxy de rede em uso, como em muitos ambientes corporativos, o ZAP pode ser configurado para se conectar a esse proxy



O que é OWASP ZAP?

- Como o ZAP é de código aberto, o código-fonte pode ser examinado para ver exatamente como a funcionalidade é implementada
- Qualquer pessoa pode se voluntariar para trabalhar no ZAP, corrigir bugs, adicionar recursos, criar pull requests para fazer correções no projeto e criar complementos para dar suporte a situações especializadas



WireShark

O que é WireShark?

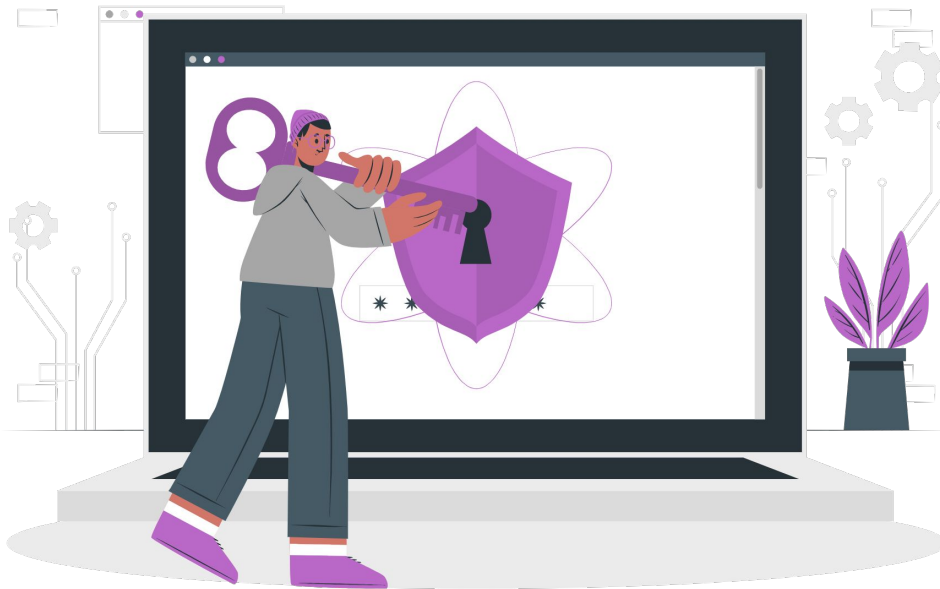
- É uma ferramenta open source de análise de protocolos, que permite capturar o tráfego de rede na rede local e armazenar esses dados para analisar offline
- Tal como no Nmap; órgãos públicos, empresas e instituições de ensino usam o Wireshark para solução de problemas e para fins pedagógicos

O que é WireShark?

- Documentação
 - <https://www.wireshark.org/docs/>
- Instalação
 - <https://www.wireshark.org/#download>

Funcionalidades do Wireshark

- Com essa ferramenta, podemos verificar o funcionamento de uma rede em detalhes e, com isso, entre outras utilidades:
 - Identificar problemas na rede
 - Saber a fonte de ataques de negação de serviço
 - Encontrar programas mal-intencionados
 - Auxiliar desenvolvedores na resolução de problemas encontrados na implementação de protocolos
 - Ensinar sobre o funcionamento de redes



Estudo de Caso de Testes de Segurança Do sistema X

Varreduras de Portas e Serviços Nmap

- Utilizando a ferramenta **Nmap**, foram analisadas as portas ativas do host **177.xx.xxx.128** do domínio **xxxxxxx.xxxxxxxxxx.xx.xxx.br**

```
1 # Nmap 7.94 scan initiated Tue Jul 18 12:53:01 2023 as: nmap -v -sS -Pn -oN portas_detectadas.txt
2 Host is up (0.13s latency).
3 Not shown: 992 filtered tcp ports (no-response)
4 PORT      STATE SERVICE
5 22/tcp    open  ssh
6 80/tcp    closed http
7 5000/tcp  open  upnp
8 5001/tcp  open  complex-link
9 5002/tcp  open  rfe
10 8080/tcp  open  http-proxy
11 8081/tcp  open  blackice-icecap
12 8082/tcp  open  blackice-alerts
13
14 Read data files from: /usr/bin/../../share/nmap
15 # Nmap done at Tue Jul 18 13:26:05 2023 -- 1 IP address (1 host up) scanned in 1983.99 seconds|
```

Varreduras de Portas e Serviços Nmap

- Foi realizada uma segunda varredura para detectar a versão dos serviços em execução nas portas abertas obtidas da primeira leitura, além da porta 5432

```
1 # Nmap 7.94 scan initiated Tue Jul 18 13:35:42 2023 as: nmap -v -sV -  
  p22,5000,5001,5002,5432,8080,8081,8082 -Pn -oN servicos.txt [REDACTED]  
2 Nmap scan report for ec2[REDACTED].sa-east-1.compute.amazonaws.com ([REDACTED])  
3 Host is up (0.11s latency).  
4  
5 PORT      STATE      SERVICE      VERSION  
6 22/tcp    open      ssh          OpenSSH 8.9p1 Ubuntu 3 (Ubuntu Linux; protocol 2.0)  
7 5000/tcp  open      upnp?  
8 5001/tcp  open      complex-link?  
9 5002/tcp  open      rfe?  
10 5432/tcp  filtered  postgresql  
11 8080/tcp  open      http         Apache Tomcat 9.0.68  
12 8081/tcp  open      http         Apache Tomcat 9.0.68  
13 8082/tcp  open      http         Apache Tomcat 9.0.68
```


Serviço SSH

- A versão do serviço, “openssh 8.9p1 ubuntu 3 (ubuntu linux protocol 2.0)”, apresentou uma vulnerabilidade que será editada e atualizada com mais informações na lista **Common Vulnerabilities and Exposures (CVE)**, com o código **CVE-2023-28531**

Vulnerability Details : [CVE-2023-28531](#)

ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.

Published 2023-03-17 04:15:15 Updated 2023-07-21 19:21:51 Source [MITRE](#) View at [NVD](#), [CVE.org](#)

Exploit prediction scoring system (EPSS) score for CVE-2023-28531

Probability of exploitation activity in the next 30 days: **0.06%**

Percentile, the proportion of vulnerabilities that are scored at or less: **~ 26 %** [EPSS Score History](#) [EPSS FAQ](#)

CVSS scores for CVE-2023-28531

Base Score	Base Severity	CVSS Vector	Exploitability Score	Impact Score	Source
9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	3.9	5.9	nvd@nist.gov



Serviço HTTP

- A versão do serviço, “Apache Tomcat 9.0.68”, apresenta uma vulnerabilidade conhecida com código CVE-2022-45143

CVE-2022-45143 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Description

The JsonErrorReportValve in Apache Tomcat 8.5.83, 9.0.40 to 9.0.68 and 10.1.0-M1 to 10.1.1 did not escape the type, message or description values. In some circumstances these are constructed from user provided data and it was therefore possible for users to supply values that invalidated or manipulated the JSON output.

Severity

CVSS Version 3.x

CVSS Version 2.0

CVSS 3.x Severity and Metrics:



NIST: NVD

Base Score: **7.5 HIGH**

Vector:

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS

Serviço PostgreSQL

- A porta 5432 está sendo filtrada pelo firewall
 - Indicação de proteção ao serviço e aos dados contra um invasor externo
- Outros serviços (portas 5000, 5001 e 5002)
 - Essas portas não apresentaram problemas nas varreduras feitas

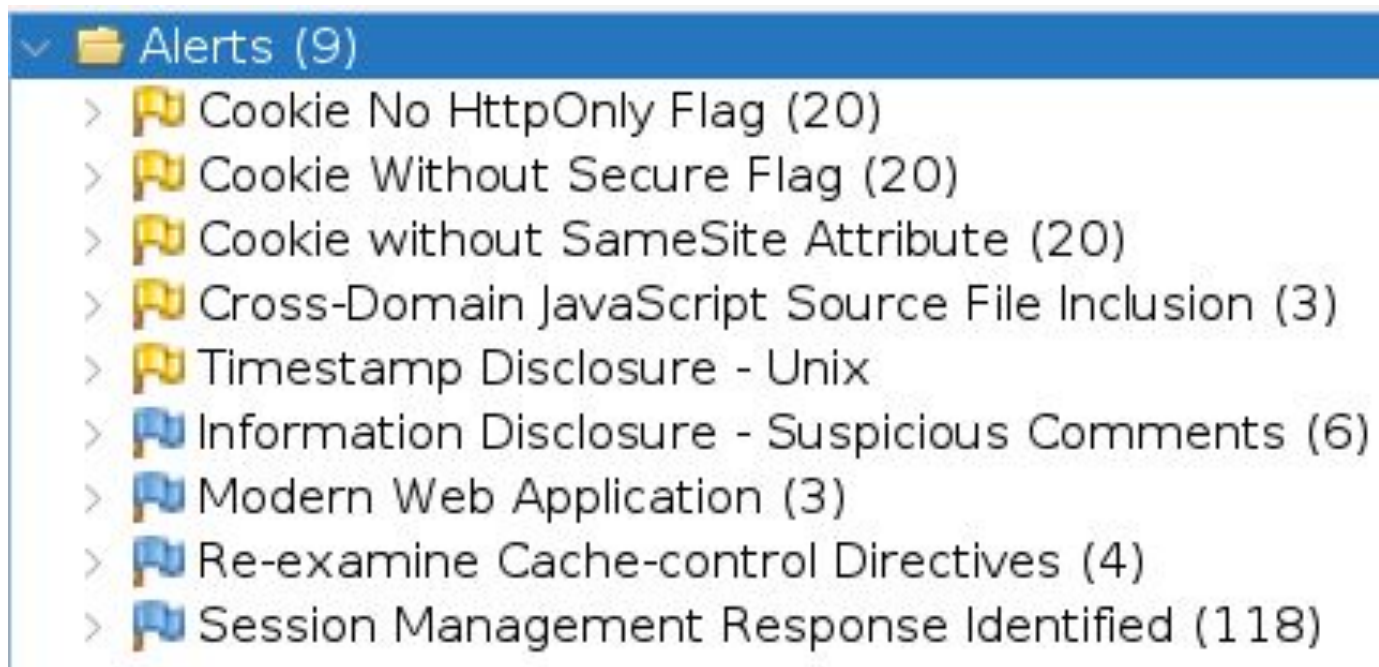
Scanner Web via OWASP ZAP

- Versão utilizada foi a 2.13.0.
- Foram gerados 7 alertas de segurança:
 - 1 de severidade alta: exposição de metadados da instância da nuvem (AWS) ao serem consultados
 - 3 de severidade média: ausência de configuração do cabeçalho da política de segurança de conteúdo (Content Security Policy - CSP)
 - 3 de severidade baixa/informacional

```
Content-Security-Policy: default-src 'self'; font-src 'self' https://fonts.gstatic.com data; img-src 'self' data:
https://d.basemaps.cartocdn.com https://a.basemaps.cartocdn.com
https://b.basemaps.cartocdn.com https://c.basemaps.cartocdn.com; script-src 'self'; style-src 'self'
https://fonts.googleapis.com 'sha256-47DEQpj8HBSa+/TImW+5JCeuQeRkm5NMpJWZG3hSuFU=';
frame-src 'self'; connect-src 'self' https://a[REDACTED]; frame-ancestors 'self';
form-action 'self';
```

Configurado o CSP: Requisições HTTP

- Os alertas em amarelo são de riscos de baixa classificação de vulnerabilidade, enquanto os alertas em azul são só informações sobre a aplicação, sem representar qualquer problema



Scanner Web via Burp Suite

- Versão utilizada foi a Community 2023.6.2.
- Foram verificados dados de entrada nos campos de CPF e senha na página de login
 - A introdução de caracteres especiais e consultas SQL nesses campos **foram testadas a fim de observar** se erros com informações importantes e comprometedoras do código-fonte utilizados eram exibidos

Scanner Web via Burp Suite

- Retornou erros com informações do código-fonte

```
{ "timestamp": 1691156515.189184696, "status": 400, "error":  
"Validation failed for argument [0] in public org.springframework.http.ResponseEntity<com. [REDACTED] responses.auth.LoginResponseDTO> com. [REDACTED].core.controllers.AuthenticationController.authenticateUser(com.bigData [REDACTED] re.dtos.requests.auth.LoginRequestDTO): [Field error in object 'loginRequestDTO' on field 'password': rejected value [ ]; codes [NotBlank.loginRequestDTO.password,NotBlank.password,NotBlank.java.lang.String,NotBlank]; arguments [org.springframework.context.support.DefaultMessageSourceResolvable: codes [loginRequestDTO.password,password]; arguments []; default message [password]]; default message [error.passwordNotBlank.message]] ", "message": "Campos informados estão inválidos", "path":  
"/bigdatafor/api/auth/signin", "type": "WARNING", "messages": [], "errors": [{ "field": "password", "error":  
"A senha não pode estar vazia"}] }
```

- O erro não exibe informações comprometedoras do código-fonte
 - O problema ocorreu com os caracteres problemáticos ('\\': contra-barras, '“': aspas duplas) e para senha vazia e o formato da exibição do erro foi corrigido

Scanner Web via Burp Suite

- Outro problema encontrado foi em relação ao token JWT(JSON Web Token) de sessão do usuário, o qual continuava válido mesmo após o usuário efetuar o

Request

PrettyRawHex

1

GET [REDACTED]th=/painel&resourceModule=Painel%20de%20Monitoramento HTTP/1.1

2

Host: [REDACTED]

3

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0

4

Accept: */*

5

Accept-Language: en-US,en;q=0.5

6

Accept-Encoding: gzip, deflate

7

Referer: [REDACTED]

8

authorization: Bearer eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJyb3NzYW5hQHVmYy5iciIsIm1hdCI6MTY5MDM3NjUyNiwiZXhwIjoxNjkwNDYyOTI2fQ.X_bzXwJRap-4W-6c23uIISjt1JihV7Y1IC4u7QSn1c-7vs1muYQfVDhTtDt5XDNMrcTb91lxflSBmeYkLEf-QQ

9

Origin: http://177.71.240.128:5000

10

Connection: close

11

12

Response

PrettyRawHexRender

1

HTTP/1.1 200

2

Vary: Origin

3

Vary: Access-Control-Request-Method

4

Vary: Access-Control-Request-Headers

5

Access-Control-Allow-Origin: *

6

X-Content-Type-Options: nosniff

7

X-XSS-Protection: 1; mode=block

8

Cache-Control: no-cache, no-store, max-age=0, must-revalidate

9

Pragma: no-cache

10

Expires: 0

11

X-Frame-Options: DENY

12

Content-Type: application/json

13

Date: Wed, 26 Jul 2023 13:03:15 GMT

14

Connection: close

15

Content-Length: 152

16

17

{

"haveAccess":true,

"userPayload":{

"id":"89df711b-527e-4da2-bbbe-9ec99863e516",

"name": [REDACTED]

"email": "[REDACTED]

"roles":[

"ROLE_ADMIN"

]

}

}

}

Scanner Web via Burp Suite

- O time de desenvolvimento corrigiu esse problema com o tratamento correto para os tokens de sessão

Request

Pretty Raw Hex

```
1 GET [REDACTED] HTTP/1.1
2 Host: [REDACTED]
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://177.71.240.128:5001/
8 authorization: Bearer eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiI3aWxzY25jYXN0cm8ucHZA2Z1haWwY29tIiwiaWF0IjoxNjkxMTU3OTM5LCJleHAiOiJlZD3OTM5NDQzMz19.uo01DoZJsOfWYDYr1JRCOBCpranGaEXa9iNb jYTKiL_4xpyJD3RBLKruFp3Ur1MfYFgP_qHNpT3eltHJDeG83A
9 Origin: http://177.71.240.128:5001
10 Connection: close
11
12
```

Response

Pretty Raw Hex Render

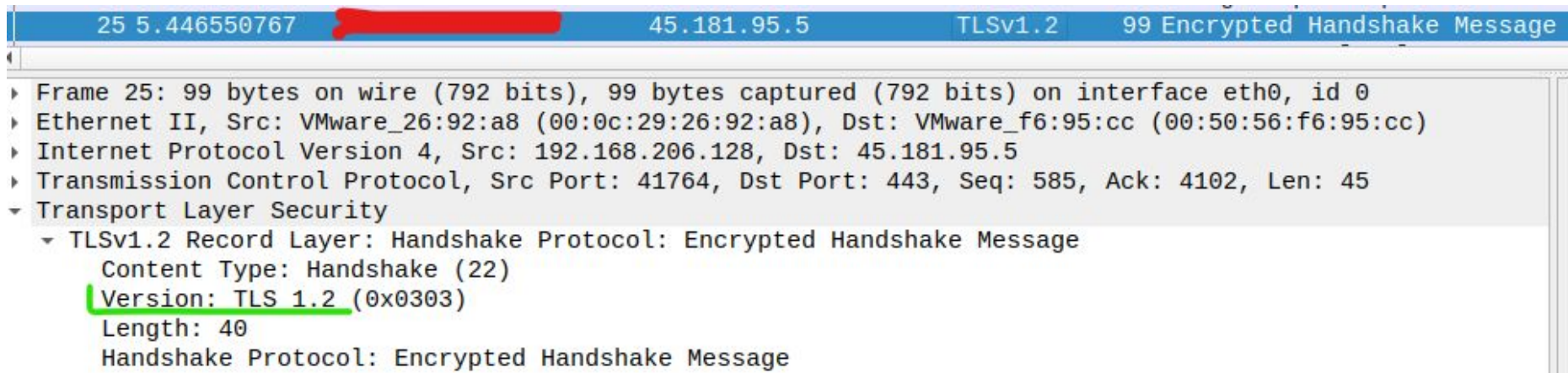
```
1 HTTP/1.1 401
2 Vary: Origin
3 Vary: Access-Control-Request-Method
4 Vary: Access-Control-Request-Headers
5 Access-Control-Allow-Origin: *
6 X-Content-Type-Options: nosniff
7 X-XSS-Protection: 1; mode=block
8 Cache-Control: no-cache, no-store, max-age=0, must-revalidate
9 Pragma: no-cache
10 Expires: 0
11 X-Frame-Options: DENY
12 Content-Type: application/json
13 Content-Length: 127
14 Date: Fri, 04 Aug 2023 14:06:51 GMT
15 Connection: close
16
17 {
  "path": "/api/dashboard",
  "error": "Não autorizado",
  "message": "É necessário estar logado para acessar o recurso",
  "status": 401
}
```

Verificação de Criptografia

- O objetivo era identificar todos os algoritmos criptográficos utilizados e verificar se existem algoritmos criptográficos obsoletos ou más configurações dos mesmos
 - Utilizada a solução **BCrypt**, que contém os padrões criptográficos mais indicados para implementações do Spring

Verificação de Criptografia

- Se tratando do protocolo TLS utilizado nas comunicações HTTP, a versão é a 1.2, que é ainda indicada para o uso em comunicações



The image shows a Wireshark packet capture of a TLS handshake. The top bar indicates the packet is Frame 25, 5.446550767 seconds, from source 45.181.95.5 to destination 45.181.95.5, protocol TLSv1.2, and it's a 99-byte encrypted handshake message. The packet details pane shows the following structure:

- Frame 25: 99 bytes on wire (792 bits), 99 bytes captured (792 bits) on interface eth0, id 0
- Ethernet II, Src: VMware_26:92:a8 (00:0c:29:26:92:a8), Dst: VMware_f6:95:cc (00:50:56:f6:95:cc)
- Internet Protocol Version 4, Src: 192.168.206.128, Dst: 45.181.95.5
- Transmission Control Protocol, Src Port: 41764, Dst Port: 443, Seq: 585, Ack: 4102, Len: 45
- Transport Layer Security
 - TLShv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message
 - Content Type: Handshake (22)
 - Version: TLS 1.2 (0x0303)
 - Length: 40
 - Handshake Protocol: Encrypted Handshake Message

Transport Layer Security = é um protocolo de segurança para fornecer segurança nas comunicações

Obrigado!

Por hoje é só pessoal...

Dúvidas?



IsmayleSantos



leosilva99



ismayle.santos@uece.br



leonardosilva_99@alu.ufc.br