

Relatório

Trabalho Individual – OWASP

Aluno(a): Jessica Regina dos Santos

Matrícula: 22100626

Disciplina: Segurança em Computação

Data de Entrega: 22/06/25

Agradeço a aluna Myllena, que sem o auxílio e empréstimo de notebook, não seria possível realizar esse trabalho.

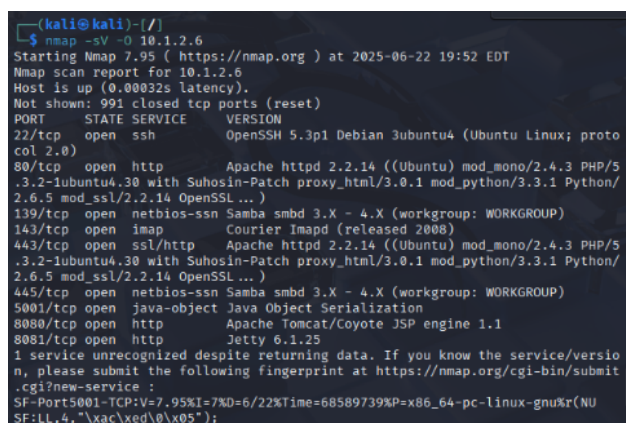
Parte 1 – NMAP

Questão 1. nmap -sV -O 10.1.2.6

A varredura NMAP no endereço IP 10.1.2.6 identificou diversos serviços em execução, muitos com versões desatualizadas que representam potenciais vulnerabilidades.

O sistema opera com Linux kernel 2.6.x e possui serviços críticos como SSH (OpenSSH 5.3p1 na porta 22), HTTP/HTTPS (Apache 2.2.14 nas portas 80 e 443), Samba (portas 139/445), Apache Tomcat 1.1 (porta 8080), Jetty 6.1.25 (porta 8081) e um serviço de serialização Java não identificado na porta 9001.

A presença destas versões antigas sugere riscos significativos, incluindo possíveis explorações conhecidas. Recomenda-se a atualização dos softwares, a revisão das configurações de segurança – especialmente em serviços como SSH e HTTP – e a realização de testes de vulnerabilidade com ferramentas especializadas.



```
(kali@kali)-[~]
$ nmap -sV -O 10.1.2.6
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-22 19:52 EDT
Nmap scan report for 10.1.2.6
Host is up (0.00032s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http         Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL ...)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp   open  imap         Courier Imapd (released 2008)
443/tcp   open  ssl/http     Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL ...)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
5001/tcp  open  java-object  Java Object Serialization
8080/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
8081/tcp  open  http         Jetty 6.1.25
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port5001-TCP:V=7.95%I=7%D=6/22%Time=68589739%P=x86_64-pc-linux-gnu%r(NU
SF:LL,4,`\xac\xed\0\x05*);
```

```

143/tcp open  imap        Courier Imapd (released 2008)
443/tcp open  ssl/http    Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5
.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/
2.6.5 mod_ssl/2.2.14 OpenSSL ...)
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
5001/tcp open  java-object Java Object Serialization
8080/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
8081/tcp open  http        Jetty 6.1.25
1 service unrecognized despite returning data. If you know the service/version
n, please submit the following fingerprint at https://nmap.org/cgi-bin/submit
.cgi?new-service :
SF-Port5001-TCP:V=7.95%I=7%D=6/22%T=68589739P=x86_64-pc-linux-gnu%r(NU
SF:LL,4,"\\xac\\xed\\0\\x05");
MAC Address: 08:00:27:03:DF:55 (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.17 - 2.6.36
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.01 seconds

```

Questão 2. nmap -v -A 10.1.2.6

Resultados: trata-se da máquina virtual OWASP Broken Web Applications (OWASPBWA), um ambiente projetado para testes de segurança.

O sistema opera com uma versão antiga do Linux (kernel 2.6.x), o que já representa um risco devido a vulnerabilidades conhecidas nessa versão desatualizada.

Falhas encontradas: certificado SSL vencido, método TRACE ativado no servidor web e uma configuração insegura do Samba, com a assinatura de mensagens desativada.

Este é um cenário frágil, perfeito para treinamento em segurança ofensiva.

```

(kali@kali)-[/]
$ nmap -v -A 10.1.2.6
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-22 20:03 EDT
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 20:03
Completed NSE at 20:03, 0.00s elapsed
Initiating NSE at 20:03
Completed NSE at 20:03, 0.00s elapsed
Initiating NSE at 20:03
Completed NSE at 20:03, 0.00s elapsed
Initiating ARP Ping Scan at 20:03
Scanning 10.1.2.6 [1 port]
Completed ARP Ping Scan at 20:03, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:03
Completed Parallel DNS resolution of 1 host. at 20:03, 0.09s elapsed
Initiating SYN Stealth Scan at 20:03
Scanning 10.1.2.6 [1000 ports]
Discovered open port 445/tcp on 10.1.2.6
Discovered open port 139/tcp on 10.1.2.6
Discovered open port 80/tcp on 10.1.2.6
Discovered open port 443/tcp on 10.1.2.6
Discovered open port 8080/tcp on 10.1.2.6
Discovered open port 143/tcp on 10.1.2.6
Discovered open port 22/tcp on 10.1.2.6
Discovered open port 5001/tcp on 10.1.2.6
Discovered open port 8081/tcp on 10.1.2.6
Completed SYN Stealth Scan at 20:03, 0.03s elapsed (1000 total ports)
Initiating Service scan at 20:03
Scanning 9 services on 10.1.2.6
Completed Service scan at 20:03, 12.13s elapsed (9 services on 1 host)

```

```

Completed SYN Stealth Scan at 20:03, 0.03s elapsed (1000 total ports)
Initiating Service scan at 20:03
Scanning 9 services on 10.1.2.6
Completed Service scan at 20:03, 12.13s elapsed (9 services on 1 host)
Initiating OS detection (try #1) against 10.1.2.6
NSE: Script scanning 10.1.2.6.
Initiating NSE at 20:03
Completed NSE at 20:03, 5.24s elapsed
Initiating NSE at 20:03
Completed NSE at 20:03, 1.19s elapsed
Initiating NSE at 20:03
Completed NSE at 20:03, 0.00s elapsed
Nmap scan report for 10.1.2.6
Host is up (0.00027s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu Linux; proto
col 2.0)
|_ ssh-hostkey:
|_  1024 ea:83:1e:45:5a:a6:8c:43:1c:3c:a3:18:dd:fc:88:a5 (DSA)
|_  2048 3a:94:d8:3f:e0:a2:7a:b8:c3:94:d7:5e:00:55:0c:a7 (RSA)
80/tcp    open  http         Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5
.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/
2.6.5 mod_ssl/2.2.14 OpenSSL ...)
|_ http-methods:
|_   Supported Methods: GET HEAD POST OPTIONS TRACE
|_   Potentially risky methods: TRACE
|_ http-favicon: Unknown favicon MD5: 1f8c0b08fb6b556a6587517a8d5f290b
|_ http-title: owaspbwa OWASP Broken Web Applications
|_ http-server-header: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu
4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ss

```

```

4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp open  imap Courier Imapd (released 2008)
|_imap-capabilities: CAPABILITY THREAD=REFERENCES ACL completed IMAP4rev1 THRE
EAD=ORDEREDSUBJECT ACL2=UNIONA0001 CHILDREN SORT UIDPLUS IDLE OK QUOTA NAMESP
ACE
443/tcp open  ssl/http Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5
.3.2-lubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/
2.6.5 mod_ssl/2.2.14 OpenSSL ...)
|_http-favicon: Unknown favicon MD5: 1F8C0B08F86B556A6587517A8D5F290B
|_http-methods:
|_Supported Methods: GET HEAD POST OPTIONS TRACE
|_Potentially risky methods: TRACE
|_http-server-header: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-lubuntu
4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/
2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1
|_http-title: owaspbwa OWASP Broken Web Applications
|_ssl-date: 2025-06-22T21:03:23+00:00; -3h00m01s from scanner time.
|_ssl-cert: Subject: commonName=owaspbwa
|_Issuer: commonName=owaspbwa
|_Public Key type: rsa
|_Public Key bits: 1024
|_Signature Algorithm: sha1withRSAEncryption
|_Not valid before: 2013-01-02T21:12:38
|_Not valid after: 2022-12-31T21:12:38
|_MD5: 0fb9:ca0b:e9b7:b26f:de6c:3555:6106:2390
|_SHA-1: e469:e1f2:9877:40c3:3aee:ee7c:f630:ca19:21be:05ae
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
5001/tcp open  java-object Java Object Serialization
8080/tcp open  http Apache Tomcat/Coyote JSP engine 1.1

```

```

8080/tcp open  http Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-title: Site doesn't have a title.
8081/tcp open  http Jetty 6.1.25
|_http-methods:
|_Supported Methods: GET HEAD POST TRACE OPTIONS
|_Potentially risky methods: TRACE
|_http-server-header: Jetty(6.1.25)
|_http-title: Choose Your Path
1 service unrecognized despite returning data. If you know the service/version
n, please submit the following fingerprint at https://nmap.org/cgi-bin/submit
.cgi?new-service :
SF:Port5001-TCP:V=7.95XI=7ND=6/22Time=6050990EIP=x86_64-pc-linux-gnuKr(NU
SF:LL,4,"\\xac\\xed\\x05");
MAC Address: 08:00:27:03:DF:55 (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.17 - 2.6.36
Uptime guess: 0.006 days (since Sun Jun 22 19:55:28 2025)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=202 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: OWASPBWA, NetBIOS user: <unknown>, NetBIOS MAC: <unkn
own> (unknown)
|_Names:

```

```

File Actions Edit View Help
|_Names:
|_OWASPBWA<00> Flags: <unique><active>
|_OWASPBWA<03> Flags: <unique><active>
|_OWASPBWA<20> Flags: <unique><active>
|_\\x01\\x02_MSBROWSE_\\x02<01> Flags: <group><active>
|_WORKGROUP<1d> Flags: <unique><active>
|_WORKGROUP<1e> Flags: <group><active>
|_WORKGROUP<00> Flags: <group><active>
|_smb-security-mode:
|_account_used: guest
|_authentication_level: user
|_challenge_response: supported
|_message_signing: disabled (dangerous, but default)
|_clock-skew: mean: -3h00m01s, deviation: 0s, median: -3h00m01s

TRACEROUTE
HOP RTT ADDRESS
1 0.27 ms 10.1.2.6

NSE: Script Post-scanning.
Initiating NSE at 20:03
Completed NSE at 20:03, 0.00s elapsed
Initiating NSE at 20:03
Completed NSE at 20:03, 0.00s elapsed
Initiating NSE at 20:03
Completed NSE at 20:03, 0.00s elapsed
Read data files from: /usr/share/nmap
OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 20.77 seconds
Raw packets sent: 1020 (45.620KB) | Rcvd: 1016 (41.374KB)

```

Questão 3. `nmap -sS -v --top-ports 10 --reason -oA saidanmap www.ufsc.br`

Realizei uma análise de segurança no domínio `www.ufsc.br` utilizando o Nmap 7.95, com foco nos 10 principais ports TCP. O scan identificou o servidor 150.162.2.10 (TTL 255) como ativo, com um IPv6 (2801:184:1912::110) não escaneado.

A configuração mostrou boas práticas de segurança: apenas as portas 80 (HTTP) e 443 (HTTPS) estão abertas (SYN-ACK, TTL 64), enquanto serviços como FTP (21), SSH (22), Telnet (23), SMTP (25), POP3 (110), SMB (139/445) e RDP (3389) aparecem filtrados.

Essa configuração equilibra acessibilidade e segurança e reduz significativamente a superfície de ataque ao expor apenas serviços web essenciais. A presença de IPv4/IPv6 também demonstra uma infraestrutura atualizada, adequada para um servidor web institucional.

```
(kali@kali)-[~]
$ nmap -sS -v --top-ports 10 --reason -oA saidanmap www.ufsc.br
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-22 20:18 EDT
Initiating Ping Scan at 20:18
Scanning www.ufsc.br (150.162.2.10) [4 ports]
Completed Ping Scan at 20:18, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:18
Completed Parallel DNS resolution of 1 host. at 20:18, 8.00s elapsed
Initiating SYN Stealth Scan at 20:18
Scanning www.ufsc.br (150.162.2.10) [10 ports]
Discovered open port 443/tcp on 150.162.2.10
Discovered open port 80/tcp on 150.162.2.10
Completed SYN Stealth Scan at 20:18, 1.24s elapsed (10 total ports)
Nmap scan report for www.ufsc.br (150.162.2.10)
Host is up, received reset ttl 255 (0.014s latency).
Other addresses for www.ufsc.br (not scanned): 2801:84:0:2::10
rDNS record for 150.162.2.10: paginas.ufsc.br

PORT      STATE SERVICE REASON
21/tcp    filtered ftp      no-response
22/tcp    filtered ssh      no-response
23/tcp    filtered telnet   no-response
25/tcp    filtered smtp     no-response
80/tcp    open  http      syn-ack ttl 64
110/tcp   filtered pop3     no-response
139/tcp   filtered netbios-ssn no-response
443/tcp   open  https     syn-ack ttl 64
445/tcp   filtered microsoft-ds no-response
3389/tcp  filtered ms-wbt-server no-response

445/tcp   filtered microsoft-ds no-response
3389/tcp  filtered ms-wbt-server no-response

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 9.61 seconds
Raw packets sent: 22 (944B) | Rcvd: 3 (128B)
```

Questão 4. Crie um comando nmap com opções diferentes das usadas nas questões anteriores e explique a saída obtida pelo seu comando.

Comando: **nmap -sU -sV -p 53,67,68,123,161 -T4 -v --script=dns-recursion 200.200.200.1**

O comando executado realiza uma varredura de portas UDP específicas (53, 67, 68, 123 e 161) no endereço IP 200.200.200.1, utilizando o Nmap com os parâmetros -sU para escaneamento UDP, -sV para tentar identificar a versão dos serviços, e o script dns-recursion para verificar se o servidor DNS permite consultas recursivas.

O resultado indica que o host está ativo, com baixa latência (0.032 segundos), mas todas as portas testadas retornaram com o estado “open|filtered”.

O script dns-recursion foi executado, mas não apresentou resultados visíveis, o que sugere que o servidor não permite recursão DNS ou que o tráfego está sendo filtrado. Assim, a saída mostra que há possíveis serviços ativos no host, mas o comportamento silencioso do UDP ou a presença de mecanismos de proteção limitaram a coleta de informações detalhadas.

```
l-$ nmap -sU -sV -p 53,67,68,123,161 -T4 -v --script=dns-recursion 200.200.200.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-22 21:00 EDT
NSE: Loaded 48 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 21:00
Completed NSE at 21:00, 0.00s elapsed
Initiating NSE at 21:00
Completed NSE at 21:00, 0.00s elapsed
Initiating Ping Scan at 21:00
Scanning 200.200.200.1 [4 ports]
Completed Ping Scan at 21:00, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:00
Completed Parallel DNS resolution of 1 host. at 21:00, 0.02s elapsed
Initiating UDP Scan at 21:00
Scanning 200.200.200.1 [5 ports]
Completed UDP Scan at 21:00, 1.56s elapsed (5 total ports)
Initiating Service scan at 21:00
Scanning 5 services on 200.200.200.1
Service scan Timing: About 20.00% done; ETC: 21:08 (0:06:32 remaining)
Completed Service scan at 21:02, 103.05s elapsed (5 services on 1 host)
NSE: Script scanning 200.200.200.1.
Initiating NSE at 21:02
Completed NSE at 21:02, 7.12s elapsed
Initiating NSE at 21:02
Completed NSE at 21:02, 1.06s elapsed
Nmap scan report for 200.200.200.1
Host is up (0.032s latency).

PORT      STATE      SERVICE VERSION
53/udp    open|filtered domain
67/udp    open|filtered dhcp
68/udp    open|filtered dhcp
123/udp   open|filtered ntp
161/udp   open|filtered snmp

NSE: Script Post-scanning.
Initiating NSE at 21:02
Completed NSE at 21:02, 0.00s elapsed
Initiating NSE at 21:02
Completed NSE at 21:02, 0.00s elapsed
Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 113.13 seconds
Raw packets sent: 23 (1.774KB) | Rcvd: 2 (80B)
```

Questão 5.

a. Qual a diferença entre um scan de conexão TCP e um SYN scan?

A principal diferença está na forma como cada técnica interage com as portas do host alvo durante uma varredura de rede.

A conexão TCP, também conhecida como full-open scan, realiza uma conexão completa com a porta de destino por meio do *three-way handshake* do protocolo TCP (SYN → SYN-ACK → ACK). Após detectar que a porta está aberta, é finalizada a conexão com um pacote RST ou FIN.

Essa técnica é simples de implementar e pode ser executada sem privilégios elevados. Porém, ela é facilmente detectável por firewalls e sistemas de detecção de intrusão (IDS), já que a conexão completa geralmente é registrada nos logs do sistema alvo (Skoudis & Liston, 2006; Lyon, 2009).

Já o SYN Scan, também chamado de half-open scan, não completa a conexão TCP. Nessa técnica, é enviado apenas um pacote SYN à porta. Se a porta estiver aberta, o alvo responde com um SYN-ACK, e é imediatamente enviado um pacote RST para abortar a conexão, sem completar o handshake. Caso a porta esteja fechada, o alvo responde com um pacote RST. Isso torna o SYN Scan significativamente mais furtivo, pois evita que a conexão seja completamente estabelecida, reduzindo assim a chance de registro em logs e detecção por IDS (Lyon, 2009; Nmap, 2024). Entretanto, como o envio de pacotes brutos é necessário, o SYN Scan exige privilégios de root ou administrador para ser executado (Skoudis & Liston, 2006).

Ou seja, enquanto a conexão TCP é mais acessível e fácil de usar, ela também é mais ruidosa e propensa à detecção. Já o SYN Scan, embora exija permissões elevadas, é mais eficaz quando há a necessidade de realizar varreduras discretas em sistemas de rede (Lyon, 2009).

b. Qual questão anterior usa scan de conexão TCP e qual questão usa SYN scan?

A Questão 2 utiliza scan de conexão TCP porque o comando nmap -A executa uma varredura que, na ausência de privilégios administrativos, usa o método padrão do sistema operacional para completar a conexão TCP (*three-way handshake*). Esse método estabelece a conexão completa com a porta. Já a Questão 3 usa o SYN scan, pois o comando inclui explicitamente a opção -sS, que envia pacotes SYN para iniciar a conexão, mas não a completa. Esse método é conhecido como *half-open scan*. (Lyon, 2009).

- c. Comente pelo menos uma vulnerabilidade da máquina Owasp Broken, listando a identificação CVE (cve.mitre.org) da vulnerabilidade.

Uma das vulnerabilidades encontradas está relacionada ao módulo de segurança ModSecurity em conjunto com o OWASP Core Rule Set (CRS). Este conjunto de regras é utilizado como uma camada de proteção para aplicações web, funcionando como um firewall de aplicação (WAF). No entanto, uma falha foi identificada na forma como essas regras lidam com determinados padrões de entrada, resultando na vulnerabilidade CVE-2018-16384.

Essa falha permite que um atacante burle as regras de detecção do CRS usando uma sintaxe específica que confunde o mecanismo de análise do WAF. Por exemplo, ao utilizar uma estrutura como {ab}`, onde “a” representa uma função lógica e “b” uma expressão SQL, o sistema de proteção falha em interpretar corretamente o conteúdo e deixa passar comandos maliciosos. Como resultado, a vulnerabilidade abre espaço para ataques de SQL Injection, permitindo que o invasor envie comandos diretamente ao banco de dados da aplicação, sem autorização (CVE, 2018; OWASP, 2024).

A vulnerabilidade CVE-2018-16384 está classificada como de alta severidade, segundo o sistema CVSS (Common Vulnerability Scoring System). Isso significa que, se explorada com sucesso, ela pode comprometer dados sensíveis, alterar a lógica da aplicação ou até expor informações confidenciais dos usuários (MITRE, 2024).

Parte 2 – Nikto

Questão 6.

```
nikto -host http://10.1.2.6/WackoPicko/ -o nikto.html -format htm
Nikto v2.5.0

+ Target IP: 10.1.2.6
+ Target Hostname: 10.1.2.6
+ Target Port: 80
+ Start Time: 2025-06-22 21:04:53 (GMT-4)

+ Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.38 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8
+ Phusion Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1
+ /WackoPicko/: Retrieved x-powered-by header: PHP/5.3.2-1ubuntu4.38.
+ /WackoPicko/: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /WackoPicko/: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /WackoPicko/: Cookie PHPSESSID created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /images/: The web server may reveal its internal or real IP in the Location header via a request to with HTTP/1.0. The value is '127.0.1.1'. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0690
+ /WackoPicko/index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ mod_perl/2.0.4 appears to be outdated (current is at least 2.0.11).
+ OpenSSL/0.9.8k appears to be outdated (current is at least 3.0.7). OpenSSL 1.1.1s is current for the 1.x branch and will be supported until Nov 11 2023.
+ Apache/2.2.14 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ mod_python/3.3.1 appears to be outdated (current is at least 3.5.0).
+ PHP/5.3.2-1ubuntu4.38 appears to be outdated (current is at least 8.1.5). PHP 7.4.28 for the 7.4 branch.
+ mod_ssl/2.2.14 appears to be outdated (current is at least 2.9.6) (may depend on server version).
+ Python/2.6.5 appears to be outdated (current is at least 3.9.6).
+ proxy_html/3.0.1 appears to be outdated (current is at least 3.1.2).
+ Perl/v5.10.1 appears to be outdated (current is at least v5.32.1).

+ Perl/v5.10.1 appears to be outdated (current is at least v5.32.1).
+ mod_mono/2.4.3 appears to be outdated (current is at least 3.12).
+ Phusion Passenger/4.0.38 appears to be outdated (current is at least 6.0.7).
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XSS. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1 - mod_ssl 2.8.7 and lower are vulnerable to a remote buffer overflow which may allow a remote shell.
+ PHP/5.3 - PHP 3/4/5 and 7.0 are End of Life products without support.
+ /WackoPicko/guestbook/guestbookdat: PHP-Gastebuch 1.60 Beta reveals sensitive information about its configuration.
+ /WackoPicko/guestbook/pwd: PHP-Gastebuch 1.60 Beta reveals the md5 hash of the admin password.
+ /WackoPicko/guestbook/admin.php: Guestbook admin page available without authentication.
+ /WackoPicko/guestbook/admin/o1guest.mdb: Ocean12 ASP Guestbook Manager allows download of SQL database which contains admin password. See: https://www.exploit-db.com/exploits/22484
+ /WackoPicko/guestbook/?number=55Ing%3Cscript%3Ealert(document.domain);%3C/script%3E: MPW Guestbook 1.2 and previous are vulnerable to XSS attacks. See: OSVDB-2754
+ /WackoPicko/admin/login.php?action=insert&username=test&password=test: phpAuction may allow user admin accounts to be inserted without proper authentication. Attempt to log in with user 'test' password 'test' to verify. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0995
+ /WackoPicko/?PHP9568F3AB-3C92-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /WackoPicko/?PHP9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /WackoPicko/?PHP9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /WackoPicko/?PHP9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /WackoPicko/cart/: Directory indexing found.
+ /WackoPicko/cart/: This might be interesting.
+ /WackoPicko/css/: Directory indexing found.
+ /WackoPicko/css/: This might be interesting.
+ /WackoPicko/guestbook/: This might be interesting.

+ /WackoPicko/users/: This might be interesting.
+ /WackoPicko/images/: Directory indexing found.
+ /WackoPicko/admin/login.php: Admin login page/section found.
+ /WackoPicko/test.php: This might be interesting.
+ /WackoPicko/#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8103 requests: 0 error(s) and 45 item(s) reported on remote host
```

b. Explique o que mais chamou sua atenção na saída obtida. Explique também alguma vulnerabilidade encontrada nessa aplicação (WackoPicko) que consta no relatório do arquivo nikto.html.

A análise do relatório gerado pela ferramenta Nikto revela uma série de vulnerabilidades críticas na aplicação WackoPicko, sendo que o aspecto que mais chama atenção é a grande quantidade de componentes desatualizados e falhas de segurança já documentadas, muitas com exploits públicos disponíveis.

A combinação dessas fragilidades evidencia que a aplicação está exposta a diversos vetores de ataque fáceis de explorar por agentes mal-intencionados. Uma das vulnerabilidades mais preocupantes é a presença do arquivo wp-config.php acessível publicamente (/WackoPicko/wp-config.php), que contém credenciais sensíveis, possibilitando a um invasor o acesso direto ao banco de dados da aplicação, comprometendo a confidencialidade e integridade das informações (NIKTO, 2025). Além disso, o relatório aponta arquivos como admin.php, login.php e guestbook vulneráveis a Cross-Site Scripting (XSS) e à exposição de dados sensíveis por meio de parâmetros em requisições HTTP GET, conforme registrado na base OSVDB sob o código 12184 (OWASP, 2023).

Também é possível observar que o servidor utiliza tecnologias obsoletas e vulneráveis, como Apache 2.2.14, OpenSSL 0.9.8k e PHP 5.3.3, todas com falhas conhecidas e listadas na base do MITRE, como, por exemplo, a falha de exposição de IP interno via cabeçalhos HTTP (CVE-2000-0690) e falha na autenticação de usuários

(CVE-2002-0995), o que amplia significativamente a superfície de ataque (MITRE, 2025).

Esses problemas indicam que o sistema não segue práticas básicas de segurança, como atualizações periódicas e restrição de acesso a arquivos sensíveis, contrariando recomendações estabelecidas por diretrizes de segurança como o OWASP Top 10 (OWASP, 2023).

Parte 3 – OWASP: Vulnerabilidades em Aplicações Web

Questão 7. Explique as vulnerabilidades A1, A2, A3 e A7 do documento TOP TEN 2017.

A01:2017 – Injection

Injection ocorre quando dados não confiáveis são enviados para um interpretador como parte de um comando ou consulta. Os ataques de injeção mais comuns incluem SQL Injection e Command Injection. O atacante explora falhas de validação nos dados de entrada para executar comandos maliciosos no backend da aplicação, podendo, por exemplo, acessar, modificar ou excluir informações no banco de dados. (OWASP, 2017).

A02:2017 – Broken Authentication

Abrange falhas relacionadas a gerenciamento inadequado de sessões e credenciais de usuários, permitindo que invasores comprometam senhas, tokens de sessão ou implementações incorretas de autenticação. Isso pode resultar no “roubo” de identidade de outros usuários, incluindo administradores, e no acesso não autorizado a recursos sensíveis. Problemas comuns incluem a ausência de autenticação multifator, senhas fracas, tokens previsíveis e tempo de expiração de sessão mal configurado (OWASP, 2017).

A03:2017 – Sensitive Data Exposure

Exposição acidental ou inadequada de dados sensíveis, como informações pessoais, senhas, números de cartão de crédito ou registros médicos. A exposição pode ocorrer quando a aplicação não implementa corretamente criptografia forte ou armazena dados de forma insegura. Também envolve práticas fracas, como uso de algoritmos de criptografia obsoletos ou falta de proteção adequada no transporte de dados (por exemplo, não usar HTTPS) (OWASP, 2017).

A07:2017 – Cross-Site Scripting (XSS)

Permite que atacantes injetem scripts maliciosos em páginas web visualizadas por outros usuários. Esses scripts são geralmente executados no navegador da vítima e podem roubar cookies, sessões, redirecionar para sites maliciosos ou modificar dinamicamente o conteúdo da página. (OWASP, 2017).

Questão 8.

OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Not Logged In

Home Login/Register Toggle Hints Show Popup Hints Toggle Security Enforce SSL Reset DB View Log View Captured Data

Register for an Account

[Back](#) [Help Me!](#)

Hints

Account created for or 1=1 --. 1 rows inserted.

[Switch to RESTful Web Service Version of this Page](#)

Please choose your username, password and signature

Username

Password [Password Generator](#)

Confirm Password

Signature

[Create Account](#)

- a.
- b. Explique o resultado obtido e a vulnerabilidade explorada no experimento (pesquise no documento do TOP 10 da OWASP).
- A mensagem “Account created for or 1=1 --. 1 rows inserted” mostra que o sistema aceitou a entrada maliciosa no campo Username, o que confirma a exploração de uma vulnerabilidade do tipo Injeção de SQL (SQL Injection).
- A string ' OR 1=1 -- manipula a lógica da consulta SQL interna, fazendo com que a condição de autenticação sempre seja verdadeira, já que 1=1 é uma expressão booleana que sempre retorna verdadeiro. Os dois hífen (--) servem para comentar o restante da consulta, ignorando quaisquer outras cláusulas como verificação de senha. Segundo o OWASP Top 10 (OWASP, 2023), essa vulnerabilidade está classificada como A03:2021 – Injection, e ocorre quando dados fornecidos pelo usuário são inseridos diretamente em comandos SQL sem qualquer validação, sanitização ou uso de prepared statements. Isso pode permitir que atacantes leiam, modifiquem ou excluam dados não autorizados no banco de dados, além de, executar comandos no sistema operacional.
- c. O que pode ser feito para impedir a exploração dessa vulnerabilidade?
- Validar e sanitizar todas as entradas fornecidas por usuários, assegurando que correspondam ao tipo e formato esperado.
 - Implementar controle de erros que não exponha detalhes técnicos da aplicação ou do banco de dados.
 - Utilizar frameworks e bibliotecas que tratem automaticamente da segurança contra injeções.

Questão 9.

- a. Explique a vulnerabilidade explorada no experimento (pesquise no documento do TOP 10 da OWASP).
- A vulnerabilidade explorada neste experimento é uma Injeção SQL (SQL Injection) A injeção SQL ocorre quando um atacante consegue inserir comandos SQL maliciosos em uma consulta de banco de dados.

b.

The screenshot shows a web application interface. At the top, there is a 'Hints' dropdown menu. Below it, there are two links: 'Switch to SOAP Web Service version' and 'Switch to XPath version'. The main content area has a pink box with the text 'Please enter username and password to view account details'. Below this box are input fields for 'Name' and 'Password', and a 'View Account Details' button. At the bottom, there is a grey box with the text 'Results for "or 1=1 --". 2 records found.' and a list of search results showing 'Username=or 1=1 --', 'Password=', and 'Signature='.

c. O que pode ser feito para impedir a exploração dessa vulnerabilidade?

Resposta semelhante a 8-c.

Questão 10.

- a.
- b.
- c.

Questão 11.

Parte 4 – Vulnerabilidades em IoT

Questão 12.

a. O que é o Shodan e o que é possível fazer com este site?

O Shodan é um buscador especializado em dispositivos conectados à internet. Ele indexa informações de dispositivos e serviços acessíveis diretamente pela internet, como câmeras de segurança, roteadores, servidores web, bancos de dados, sistemas industriais, impressoras, entre outros (Security Newspaper, 2018). Com o Shodan, é possível realizar buscas por tipo de dispositivo, sistema operacional, localidade geográfica, faixas de IP, portas abertas, banners de serviços e vulnerabilidades conhecidas. O site também permite filtrar dispositivos com base em critérios como fabricante, localização e até protocolos específicos.

b. Faça o registro no site, pesquise e liste algum dispositivo IoT que você encontrou.

Identifiquei um dispositivo IoT com IP 104.251.232.144 (104.251.232.144), localizado em Singapura, que executa o servidor embarcado GoAhead-Webs. Ele apresenta três serviços expostos: HTTP (porta 80), HTTPS (porta 443) com certificado autoassinado, e IPMI (porta 623/UDP) com autenticação via senha e MD5, indicando um possível roteador ou servidor com interfaces de gerenciamento remoto ativas, o que representa um risco de segurança se não estiver adequadamente configurado e protegido.

Questão 13. Na reportagem, é indicado um link para acessar uma câmera Mobotix: <http://166.161.197.253:5001/cgi-bin/guestimage.html>. No entanto, a mesma se encontra offline. Acesse o link a seguir, que é para outra câmera Mobotix encontrada no Shodan: <http://201.102.80.190:5001/cgi-bin/guestimage.html>.

- O que é possível visualizar?
- Um atacante poderia fazer o que com este acesso?

Relato que os links no enunciado da questão estavam quebrados.

Parte 5 – Metasploit

Questão 14.

```
File Actions Edit View Help
msf6 auxiliary(scanner/http/tomcat_mgr_login) > exploit
[*] No active DB -- Credential data will not be saved!
[*] 10.1.2.6:8080 - LOGIN FAILED: admin:admin (Incorrect)
[*] 10.1.2.6:8080 - LOGIN FAILED: admin:manager (Incorrect)
[*] 10.1.2.6:8080 - LOGIN FAILED: admin:role1 (Incorrect)
[*] 10.1.2.6:8080 - LOGIN FAILED: admin:root (Incorrect)
[*] 10.1.2.6:8080 - LOGIN FAILED: admin:tomcat (Incorrect)
[*] 10.1.2.6:8080 - LOGIN FAILED: admin:s3cret (Incorrect)
[*] 10.1.2.6:8080 - LOGIN FAILED: admin:vagrant (Incorrect)
[*] 10.1.2.6:8080 - LOGIN FAILED: admin:QLogic66 (Incorrect)
[*] 10.1.2.6:8080 - LOGIN FAILED: admin:password (Incorrect)
[*] 10.1.2.6:8080 - LOGIN FAILED: admin:Password1 (Incorrect)
[*] 10.1.2.6:8080 - LOGIN FAILED: admin:changethis (Incorrect)
[*] 10.1.2.6:8080 - LOGIN FAILED: admin:r00t (Incorrect)
[*] 10.1.2.6:8080 - LOGIN FAILED: admin:toor (Incorrect)
[*] 10.1.2.6:8080 - LOGIN FAILED: admin:password1 (Incorrect)
[*] 10.1.2.6:8080 - LOGIN FAILED: admin:j2deployer (Incorrect)
[*] 10.1.2.6:8080 - LOGIN FAILED: admin:0vW*busr1 (Incorrect)
[*] 10.1.2.6:8080 - LOGIN FAILED: admin:kdsxc (Incorrect)
[*] 10.1.2.6:8080 - LOGIN FAILED: admin:owaspba (Incorrect)
[*] 10.1.2.6:8080 - LOGIN FAILED: admin:ADMIN (Incorrect)
[*] 10.1.2.6:8080 - LOGIN FAILED: admin:xampp (Incorrect)
[*] 10.1.2.6:8080 - LOGIN FAILED: manager:admin (Incorrect)
[*] 10.1.2.6:8080 - LOGIN FAILED: manager:manager (Incorrect)
[*] 10.1.2.6:8080 - LOGIN FAILED: manager:role1 (Incorrect)
[*] 10.1.2.6:8080 - LOGIN FAILED: manager:root (Incorrect)
[*] 10.1.2.6:8080 - LOGIN FAILED: manager:tomcat (Incorrect)
[*] 10.1.2.6:8080 - LOGIN FAILED: manager:s3cret (Incorrect)
[*] 10.1.2.6:8080 - LOGIN FAILED: manager:vagrant (Incorrect)
[*] 10.1.2.6:8080 - LOGIN FAILED: manager:QLogic66 (Incorrect)
[*] 10.1.2.6:8080 - LOGIN FAILED: xampp:ADMIN (Incorrect)
[*] 10.1.2.6:8080 - LOGIN FAILED: xampp:xampp (Incorrect)
[*] 10.1.2.6:8080 - LOGIN FAILED: j2deployer:j2deployer (Incorrect)
[*] 10.1.2.6:8080 - LOGIN FAILED: 0vwebusr:0vW*busr1 (Incorrect)
[*] 10.1.2.6:8080 - LOGIN FAILED: cksdk:kdsxc (Incorrect)
[*] 10.1.2.6:8080 - LOGIN Successful: root:owaspba
[*] 10.1.2.6:8080 - LOGIN FAILED: ADMIN:ADMIN (Incorrect)
[*] 10.1.2.6:8080 - LOGIN FAILED: xampp:xampp (Incorrect)
[*] 10.1.2.6:8080 - LOGIN FAILED: tomcat:s3cret (Incorrect)
[*] 10.1.2.6:8080 - LOGIN FAILED: QCC:QLogic66 (Incorrect)
[*] 10.1.2.6:8080 - LOGIN FAILED: admin:vagrant (Incorrect)
[*] 10.1.2.6:8080 - LOGIN FAILED: admin:password (Incorrect)
[*] 10.1.2.6:8080 - LOGIN FAILED: admin: (Incorrect)
[*] 10.1.2.6:8080 - LOGIN FAILED: admin:Password1 (Incorrect)
[*] 10.1.2.6:8080 - LOGIN FAILED: admin:password1 (Incorrect)
[*] 10.1.2.6:8080 - LOGIN FAILED: admin:admin (Incorrect)
[*] 10.1.2.6:8080 - LOGIN FAILED: admin:tomcat (Incorrect)
[*] 10.1.2.6:8080 - LOGIN FAILED: both:tomcat (Incorrect)
[*] 10.1.2.6:8080 - LOGIN FAILED: manager:manager (Incorrect)
[*] 10.1.2.6:8080 - LOGIN FAILED: role1:role1 (Incorrect)
[*] 10.1.2.6:8080 - LOGIN FAILED: role1:tomcat (Incorrect)
[*] 10.1.2.6:8080 - LOGIN FAILED: role:changethis (Incorrect)
[*] 10.1.2.6:8080 - LOGIN FAILED: tomcat:tomcat (Incorrect)
[*] 10.1.2.6:8080 - LOGIN FAILED: tomcat:password1 (Incorrect)
[*] 10.1.2.6:8080 - LOGIN FAILED: tomcat:password (Incorrect)
[*] 10.1.2.6:8080 - LOGIN FAILED: tomcat: (Incorrect)
[*] 10.1.2.6:8080 - LOGIN FAILED: tomcat:admin (Incorrect)
[*] 10.1.2.6:8080 - LOGIN FAILED: tomcat:changethis (Incorrect)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

- O que é o ataque do dicionário?

O ataque de dicionário é uma técnica utilizada por atacantes para descobrir senhas ou chaves de autenticação por meio da tentativa sistemática de palavras previamente conhecidas. Diferente do ataque de força bruta tradicional, que tenta todas as combinações possíveis de caracteres, o ataque de dicionário utiliza uma lista predefinida de palavras e senhas comuns, chamada de “dicionário”. O objetivo é explorar o fato de que muitos usuários adotam senhas fracas ou previsíveis, facilitando a quebra do sistema de autenticação (Bishop, 2005; OWASP, 2021).

b. O que foi encontrado?

O scanner encontrou credenciais válidas para acesso ao Tomcat Manager:

Login bem-sucedido: root:owaspbwa

Além disso, foram testadas 246 combinações de usuários/senhas comuns (como admin:admin, tomcat:tomcat, manager:manager, etc.), sendo que todas falharam exceto a combinação mencionada acima.

c. Qual foi a vulnerabilidade usada para obter esse resultado?

A vulnerabilidade explorada foi um ataque de força bruta contra a interface de autenticação do Tomcat Manager, utilizando dicionário.

d. Como pode ser explorado esse resultado?

Com as credenciais válidas, um atacante pode:

- Implantar aplicações maliciosas no servidor;
- Obter controle completo do sistema;
- Ler/Modificar arquivos no servidor;
- Elevar privilégios (caso o Tomcat esteja rodando como root);
- Acessar outros sistemas internos da rede.

Questão 15

- a.
- b.
- c.
- d.

Referências

Bishop, M. (2005). *Introduction to Computer Security*. Addison-Wesley.

CVE. (2018). *CVE-2018-16384*. Disponível em: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-16384>

Lyon, G. F. (2009). *Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning*. Insecure.Com LLC.

MITRE. (2024). *Common Vulnerabilities and Exposures*. Disponível em: <https://cve.mitre.org>

NIKTO. *Nikto Web Server Scanner*. cIRT.net, 2025. Disponível em: <https://cirt.net/Nikto2>

Nmap. (2024). *Port Scanning Techniques*. Disponível em: <https://nmap.org/book/man-port-scanning-techniques.html>

OWASP. (2021). *Authentication Cheat Sheet*. Disponível em: https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html

OWASP Foundation. (2017). *OWASP Top 10 - 2017: The Ten Most Critical Web Application Security Risks*. Disponível em: <https://owasp.org/www-project-top-ten/2017/>

OWASP. *OWASP Top Ten Web Application Security Risks – 2021*. Open Web Application Security Project, 2023. Disponível em: <https://owasp.org/www-project-top-ten/>

Security Newspaper. (2018). *Find webcams, databases, boats in the sea using Shodan*. Disponível em: <https://www.securitynewspaper.com/2018/11/27/find-webcams-databases-boats-in-the-sea-using-shodan/>

Skoudis, E., & Liston, T. (2006). *Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses*. Prentice Hall.