Tecnológico de Monterrey

Campus Santa Fe

Pruebas de seguridad

Realizadas por:

Lucía Barrenechea Carrancedo

Andrea Alexandra Barrón Córdova

Pablo Bolio Pradilla

Emilia Salazar Leipen

María Fernanda Osorio Arroyo

Bajo la supervisión de:

Jorge Rodríguez Ruíz

Índice

Análisis de la página web

172.28.69.54

ZAP

En esta sección se muestran diferentes niveles de riesgo y confianza según las vulnerabilidades encontradas. Las medidas para estas son las siguientes:

Niveles de riesgo

Bajo	Moderado	Medio	Elevado	Alto

Niveles de confianza

Baja	Moderada	Media	Elevada	Alta

Una prueba ZAP revela 4 alertas, de las cuales ninguna presenta una amenaza grave para el funcionamiento o seguridad de la aplicación.

1. Cabecera Content Security Policy (CSP) no configurada
   Referencia: CWE-693
   La política de seguridad de contenido es una capa adicional de seguridad que ayuda a mitigar Cross Site Scripting (XSS).

URL	http://172.28.69.54	http://172.28.69.54 /robots.txt	http://172.28.69.54 /sitemap.xml
Riesgo	Medio		
Confianza	Alta		

   Solución: Configure la cabecera para definir orígenes confiables desde los que se pueden cargar recursos.

2. Falta de cabecera Anti-Clickjacking
   Referencia: CWE-1021
   La aplicación web no restringe o restringe incorrectamente objetos de marco o capas de interfaz de usuario que pertenecen a otra aplicación o dominio, lo que puede llevar a confusión al usuario sobre con qué interfaz está interactuando.

URL	http://172.28.69.54
Riesgo	Medio
Confianza	Elevada

   Solución: Agregue la cabecera HTTP X-Frame-Options: DENY en las respuestas.

3. El servidor filtra información de versión a través del campo "Server" del encabezado de respuesta HTTP
   Referencia: CWE-497
   El producto no previene adecuadamente que la información sensible a nivel de sistema sea accedida por actores no autorizados que no tienen el mismo nivel de acceso al sistema subyacente que el producto.

URL	http://172.28.69.54	http://172.28.69.54 /robots.txt	http://172.28.69.54 /sitemap.xml
Riesgo	Bajo		
Confianza	Alta		

   Solución: Configure el servidor para que no incluya el encabezado server o lo reemplace por una cadena genérica.

4. Falta encabezado X-Content-Type-Options
   Referencia: CWE-693
   La política de seguridad de contenido mencionada anteriormente (CSP) también ayuda a que el navegador no interfiera en MIME-sniffing.

URL	http://172.28.69.54
Riesgo	Bajo
Confianza	Media

   Solución:
   Agregando “X-Content-Type-Options: nosniff”. Esto indica al navegador que no debe inferir el tipo MIME del contenido y debe respetar el tipo indicado por el servidor.

Escaneo de la base de datos

172.28.69.82

Vulnerabilidades

```
PORT     STATE  SERVICE     VERSION
22/tcp   open   ssh         OpenSSH 9.2p1 Debian 2+deb12u6 (protocol 2.0)
80/tcp   closed http
443/tcp  closed https
3000/tcp closed ppp
3306/tcp open   mysql       MySQL 8.0.42
8000/tcp closed http-alt
8001/tcp closed vcom-tunnel
Service Info: OS: Linux; CPE: cpe:/o:linux:linux kernel
```

Puerto 22

```
ssh2-enum-algos:
  kex_algorithms: (12)
      sntrup761x25519-sha512
      sntrup761x25519-sha512@openssh.com
      curve25519-sha256
      curve25519-sha256@libssh.org
      ecdh-sha2-nistp256
      ecdh-sha2-nistp384
      ecdh-sha2-nistp521
      diffie-hellman-group-exchange-sha256
      diffie-hellman-group16-sha512
      diffie-hellman-group18-sha512
      diffie-hellman-group14-sha256
      kex-strict-s-v00@openssh.com
  server_host_key_algorithms: (4)
      rsa-sha2-512
      rsa-sha2-256
      ecdsa-sha2-nistp256
      ssh-ed25519
  encryption_algorithms: (6)
      chacha20-poly1305@openssh.com
      aes128-ctr
      aes192-ctr
      aes256-ctr
      aes128-gcm@openssh.com
      aes256-gcm@openssh.com
  mac_algorithms: (10)
      umac-64-etm@openssh.com
      umac-128-etm@openssh.com
      hmac-sha2-256-etm@openssh.com
      hmac-sha2-512-etm@openssh.com
      hmac-sha1-etm@openssh.com
      umac-64@openssh.com
      umac-128@openssh.com
      hmac-sha2-256
      hmac-sha2-512
      hmac-sha1
  compression_algorithms: (2)
      none
      zlib@openssh.com
```

Puerto 3306

```
Scanning 172.28.69.82 [1 port]
Discovered open port 3306/tcp on 172.28.69.82
Completed SYN Stealth Scan at 15:49, 0.01s elapsed (1 total ports)
NSE: Script scanning 172.28.69.82.
Initiating NSE at 15:49
Completed NSE at 15:49, 40.74s elapsed
Nmap scan report for 172.28.69.82
Host is up (0.0056s latency).

PORT     STATE SERVICE
3306/tcp open  mysql
```

Análisis

IP	172.28.69.82
Puertos abiertos	22(SSH), 3306(MySQL)
Puertos cerrados	80(http), 443(https), 3000(ppp), 8000(http-alt), 8001(vcom-tunnel)
Sistema operativo	Linux (Debian-based) según el banner OpenSSH.
Versiones	- OpenSSH 9.2p1 - `MySQL 8.0.42`
Vulnerabilidades	No se encontraron vulnerabilidades específicas.

Conclusión

Los algoritmos manejados en el puerto 22 tienen una encriptación moderna e intercambio de llaves fuerte. Sin embargo, un análisis más profundo revela una superficie de ataque para ataques dirigidos al cliente o a la baja. El endurecimiento de SSH puede limitar aún más la exposición.

El puerto 3306 está abierto y visible, pero no se filtran banners ni información detallada de la versión. El escaneo no mostró vulnerabilidades o credenciales débiles, mientras la versión no esté desactualizada ni accesible externamente no hay riesgos encontrados.

API 1

172.28.69.19

Vulnerabilidades

```
PORT     STATE  SERVICE     VERSION
22/tcp   open   ssh         OpenSSH 9.2p1 Debian 2+deb12u6 (protocol 2.0)
80/tcp   closed http
443/tcp  closed https
3000/tcp closed ppp
3306/tcp open   mysql       MySQL (unauthorized)
8000/tcp open   http        Uvicorn
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
8001/tcp closed vcom-tunnel
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Puerto 22

```
kex_algorithms: (12)
    sntrup761x25519-sha512
    sntrup761x25519-sha512@openssh.com
    curve25519-sha256
    curve25519-sha256@libssh.org
    ecdh-sha2-nistp256
    ecdh-sha2-nistp384
    ecdh-sha2-nistp521
    diffie-hellman-group-exchange-sha256
    diffie-hellman-group16-sha512
    diffie-hellman-group18-sha512
    diffie-hellman-group14-sha256
    kex-strict-s-v00@openssh.com
server_host_key_algorithms: (4)
    rsa-sha2-512
    rsa-sha2-256
    ecdsa-sha2-nistp256
    ssh-ed25519
```

```
encryption_algorithms: (6)
    chacha20-poly1305@openssh.com
    aes128-ctr
    aes192-ctr
    aes256-ctr
    aes128-gcm@openssh.com
    aes256-gcm@openssh.com
mac_algorithms: (10)
    umac-64-etm@openssh.com
    umac-128-etm@openssh.com
    hmac-sha2-256-etm@openssh.com
    hmac-sha2-512-etm@openssh.com
    hmac-sha1-etm@openssh.com
    umac-64@openssh.com
    umac-128@openssh.com
    hmac-sha2-256
    hmac-sha2-512
    hmac-sha1
compression_algorithms: (2)
    none
    zlib@openssh.com
```

Puerto 3306

```
Scanning 172.28.69.19 [1 port]
Discovered open port 3306/tcp on 172.28.69.19
Completed SYN Stealth Scan at 16:22, 0.01s elapsed (1 total ports)
NSE: Script scanning 172.28.69.19.
Initiating NSE at 16:22
Completed NSE at 16:22, 0.07s elapsed
Nmap scan report for 172.28.69.19
Host is up (0.0071s latency).

PORT     STATE SERVICE
3306/tcp open  mysql
```

Análisis

IP	172.28.69.82
Puertos abiertos	22(SSH), 3306(MySQL), 8000(http-alt)
Puertos cerrados	80(http), 443(https), 3000(ppp), 8001(vcom-tunnel)
Sistema operativo	Linux (Debian-based)
Versiones	- OpenSSH 9.2p1 - `MySQL 8.0.42` -Uvicorn
Vulnerabilidades	No se encontraron vulnerabilidades específicas.

Conclusión

Mismo escenario que IP anterior; sin hallazgos críticos. Recomendación general: restringir acceso externo. Siempre y cuando el puerto 8000 se mantenga vigilado y al día no hay vulnerabilidades en los servicios expuestos. En un futuro se recomienda monitoreo del puerto ya mencionado para reforzar sus rutas internas.

API 2

172.28.69.102

Vulnerabilidades

```
PORT     STATE  SERVICE     VERSION
22/tcp   open   ssh         OpenSSH 9.2p1 Debian 2+deb12u6 (protocol 2.0)
80/tcp   closed http
443/tcp  closed https
3000/tcp closed ppp
3306/tcp closed mysql
8000/tcp open   http        Uvicorn
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
8001/tcp closed vcom-tunnel
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Puerto 22

```
kex_algorithms: (12)
    sntrup761x25519-sha512
    sntrup761x25519-sha512@openssh.com
    curve25519-sha256
    curve25519-sha256@libssh.org
    ecdh-sha2-nistp256
    ecdh-sha2-nistp384
    ecdh-sha2-nistp521
    diffie-hellman-group-exchange-sha256
    diffie-hellman-group16-sha512
    diffie-hellman-group18-sha512
    diffie-hellman-group14-sha256
    kex-strict-s-v00@openssh.com
server_host_key_algorithms: (4)
    rsa-sha2-512
    rsa-sha2-256
    ecdsa-sha2-nistp256
    ssh-ed25519
```

```
encryption_algorithms: (6)
    chacha20-poly1305@openssh.com
    aes128-ctr
    aes192-ctr
    aes256-ctr
    aes128-gcm@openssh.com
    aes256-gcm@openssh.com
mac_algorithms: (10)
    umac-64-etm@openssh.com
    umac-128-etm@openssh.com
    hmac-sha2-256-etm@openssh.com
    hmac-sha2-512-etm@openssh.com
    hmac-sha1-etm@openssh.com
    umac-64@openssh.com
    umac-128@openssh.com
    hmac-sha2-256
    hmac-sha2-512
    hmac-sha1
compression_algorithms: (2)
    none
    zlib@openssh.com
```

Análisis

IP	172.28.69.102
Puertos abiertos	22(SSH), 8000(http-alt)
Puertos cerrados	80(http), 443(https), 3000(ppp), 3306(MySQL), 8001(vcom-tunnel)
Sistema operativo	Linux (Debian-based)
Versiones	- OpenSSH 9.2p1 - Uvicorn
Vulnerabilidades	No se encontraron vulnerabilidades específicas.

Conclusión

La configuración básica es segura ya que cuenta con una superficie de ataque reducida, la más limitada de todas las instancias.

Nginx

172.28.69.158

Vulnerabilidades

```
PORT      STATE  SERVICE     VERSION
22/tcp    open   ssh         OpenSSH 9.2p1 Debian 2+deb12u6 (protocol 2.0)
80/tcp    open   http        nginx 1.22.1
| http-enum:
|   /health/: Spring Boot Actuator endpoint
|   /healthcheck/: Spring Boot Actuator endpoint
|_  /healthchecks/: Spring Boot Actuator endpoint
|_http-server-header: nginx/1.22.1
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
443/tcp  closed https
3000/tcp closed ppp
3306/tcp closed mysql
8000/tcp closed http-alt
8001/tcp closed vcom-tunnel
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Puerto 22

```
kex_algorithms: (12)
    sntrup761x25519-sha512
    sntrup761x25519-sha512@openssh.com
    curve25519-sha256
    curve25519-sha256@libssh.org
    ecdh-sha2-nistp256
    ecdh-sha2-nistp384
    ecdh-sha2-nistp521
    diffie-hellman-group-exchange-sha256
    diffie-hellman-group16-sha512
    diffie-hellman-group18-sha512
    diffie-hellman-group14-sha256
    kex-strict-s-v00@openssh.com
server_host_key_algorithms: (4)
    rsa-sha2-512
    rsa-sha2-256
    ecdsa-sha2-nistp256
    ssh-ed25519
encryption_algorithms: (6)
    chacha20-poly1305@openssh.com
    aes128-ctr
    aes192-ctr
    aes256-ctr
    aes128-gcm@openssh.com
    aes256-gcm@openssh.com
mac_algorithms: (10)
    umac-64-etm@openssh.com
    umac-128-etm@openssh.com
    hmac-sha2-256-etm@openssh.com
    hmac-sha2-512-etm@openssh.com
    hmac-sha1-etm@openssh.com
    umac-64@openssh.com
    umac-128@openssh.com
    hmac-sha2-256
    hmac-sha2-512
    hmac-sha1
compression_algorithms: (2)
    none
    zlib@openssh.com
```

Puerto 80

```
PORT   STATE SERVICE
80/tcp open  http
| http-enum:
|   /health/: Spring Boot Actuator endpoint
|   /healthcheck/: Spring Boot Actuator endpoint
|_  /healthchecks/: Spring Boot Actuator endpoint
```

Análisis

IP	172.28.69.158
Puertos abiertos	22(SSH), 80(http)
Puertos cerrados	443(https), 3000(ppp), 3306(MySQL), 8000(http-alt), 8001(vcom-tunnel)
Sistema operativo	Linux (Debian-based)
Versiones	- OpenSSH 9.2p1 -Uvicorn
Vulnerabilidades	Spring Boot Actuator

Conclusión

Aunque la configuración base no muestra vulnerabilidades críticas, se identificó la presencia de Spring Boot Actuator (CVE-2022-22965), lo cual puede implicar riesgos si no se ha configurado adecuadamente dando la posibilidad de exponer información sensible sobre el sistema. Sin embargo, esta vulnerabilidad no afecta la información de los pacientes ni de los usuarios ya que no corren el riesgo de ser accesibles por este medio.

Actualización

Todo lo anteriormente analizado sigue siendo cierto, por lo cual no sería correcto eliminar el reporte ya realizado.
Sin embargo, un análisis el día el cual se planeaba la apertura de puertos reveló vulnerabilidades más severas, las cuales no solo son graves sino que exponen información sensible. Por esto es que sólo se mostrarán los nombres de las vulnerabilidades y el escaneo que inicialmente expuso la posibilidad de una vulnerabilidad en la instancia de Nginx y los puertos relacionados con la misma.

El puerto 80 es el que mantiene la conexión con el balanceador de cargas.

Análisis de la instancia API 1

Un escaneo de nmap revela la vulnerabilidad del puerto al igual que su conexión con las demás instancias. Profundizando más en la investigación es posible encontrar que el puerto 80, el cual se planeaba utilizar para desplegar la instancia, es vulnerable a un ataque de denegación de servicio, el cual es altamente riesgoso para los datos y la sensibilidad que los constituyen, siendo esta información médica.

Análisis de la instancia Frontend

Al igual que el análisis de la instancia API 1 este puerto es vulnerable a ataques de denegación de servicio. Sobre esta vulnerabilidad se revelan detalles sobre el servidor Apache utilizado, dejándolo abierto a una variedad de ataques diferentes, incluyendo la revelación de tecnologías utilizadas y la opción para causar agotamiento de servicios.

Análisis de la instancia de la base de datos

Dentro de este análisis no serán incluidas capturas de pantalla, ni siquiera censuradas como las anteriores, ya que es una instancia con datos sumamente sensibles en la cual se encontró información explícita sobre el sistema la cual da pie a encontrar información personal y médica de los usuarios.

Con base en el escaneo básico se reveló información sobre la encriptación, esta información revela datos que dan pie a la posibilidad de ejecutar ataques de fuerza bruta los cuales revelan información de los pacientes analizados por los usuarios y sobre sus contraseñas. Aunque no es información suficiente como para hacer una suplantación de identidad o alteración de la información en la página es posible llevar a cabo inyecciones sobre los perfiles de usuario y utilizar la información para vulnerarlos con ataques sociales.

Conclusión actualizada

La aplicación es funcional y segura siempre y cuando se mantenga corriendo en *localhost*, exponer la aplicación, incluso a usuarios de la red del Tecnológico de Monterrey implica un alto riesgo de fuga de información biométrica que incluso llega a infringir violaciones al código ético al cual los usuarios de esta herramienta se comprometen.

Por todo lo anterior mencionado la restricción del puerto 80 es esencial y no es éticamente correcto exponer esta aplicación a la red.