

Presentación de Ciberseguridad

PARTICIPANTES:

Mihai Mardale.

Gema Montejano.

Adrián Martínez.

Mariana Gutiérrez.

Jorge Vidales.

Christian Espinosa.

Antonio Fernández.

Ignacio de Pablos.

1. Consejos

- Consejos de buenas prácticas del departamento de ciber:
- Agregar cabeceras HTTP de seguridad a la página web:
- HTTP Strict Transport Security (HSTS)
- X-XSS Protection
- X-Content-Type-Options
- X-Frame-Options
- Content Security Policy
- Referrer Policy
- Expect-CT

2. ¿La aplicación es vulnerable a SQL INJECTION?

Definición: Una vulnerabilidad de inyección SQL es una falla en la seguridad de una aplicación web que permite a un atacante ejecutar comandos SQL no autorizados en la base de datos subyacente. Esto puede llevar a la manipulación de datos, la divulgación de información confidencial o la destrucción del sistema.

Se han llevado a cabo pruebas exhaustivas de inyección SQL en diversos puntos de entrada utilizando herramientas como sqlmap, burp suite e introduciendo parámetros con los que se pueda interactuar con la base de datos.

El análisis reveló que la aplicación web implementa de manera efectiva medidas de protección contra la inyección SQL. Se observó una adecuada validación y sanitización de las entradas del usuario en todos los puntos de entrada identificados. Además, se emplearon consultas parametrizadas o se implementaron controles de entrada estrictos para evitar la ejecución de comandos SQL no autorizados.



















2. No vulnerable a PATH TRAVERSAL.

Definición: Un ataque de Path Traversal, es una técnica utilizada por los atacantes para acceder a archivos o directorios fuera del directorio permitido en una aplicación web. Esto se logra manipulando las rutas de archivo en las solicitudes HTTP para navegar a ubicaciones sensibles del sistema de archivos.

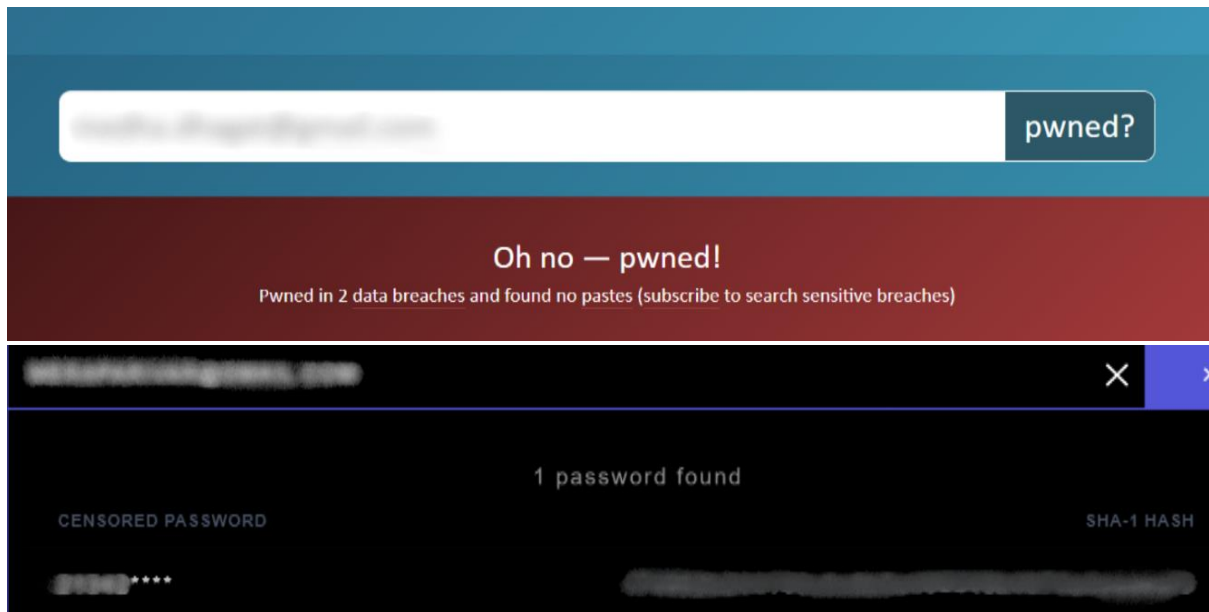
La página web ha sido diseñada con medidas de seguridad sólidas para prevenir este tipo de ataque. Implementamos controles estrictos de acceso y validación de entrada para garantizar que las solicitudes de los usuarios no puedan manipular las rutas de archivo y acceder a ubicaciones no autorizadas.

3. Resultados obtenidos mediante investigación de OSINT

Una verificación adicional reveló que la dirección de correo electrónico personal de "Medha Dhagat" ha sido comprometida en una brecha de seguridad. Esta situación plantea un riesgo potencial para la seguridad de la empresa, ya que los correos electrónicos personales comprometidos pueden exponer información confidencial y ser utilizados para ataques de ingeniería social u otras actividades maliciosas.

<input type="checkbox"/>	 Anil Landge Managing Director 	Mera Parivar Ngo Gurugram, HR, IN	  anil@meraparivar.org  
<input type="checkbox"/>	 Medha Dhagat Consultant for Management and... 	Mera Parivar NGO Gurugram, HR, IN	  medha.dhagat@gmail.com  
<input type="checkbox"/>	 Akshita Dhamija Digital Marketing Intern 	Mera Parivar NGO Haryana, India	  akshita@meraparivar.org  

Es fundamental abordar este riesgo de manera proactiva, implementando medidas de seguridad adicionales y proporcionando capacitación en conciencia de seguridad para proteger tanto los datos corporativos como la privacidad de los empleados.



4. La página integra la utilización de Certificado SSL

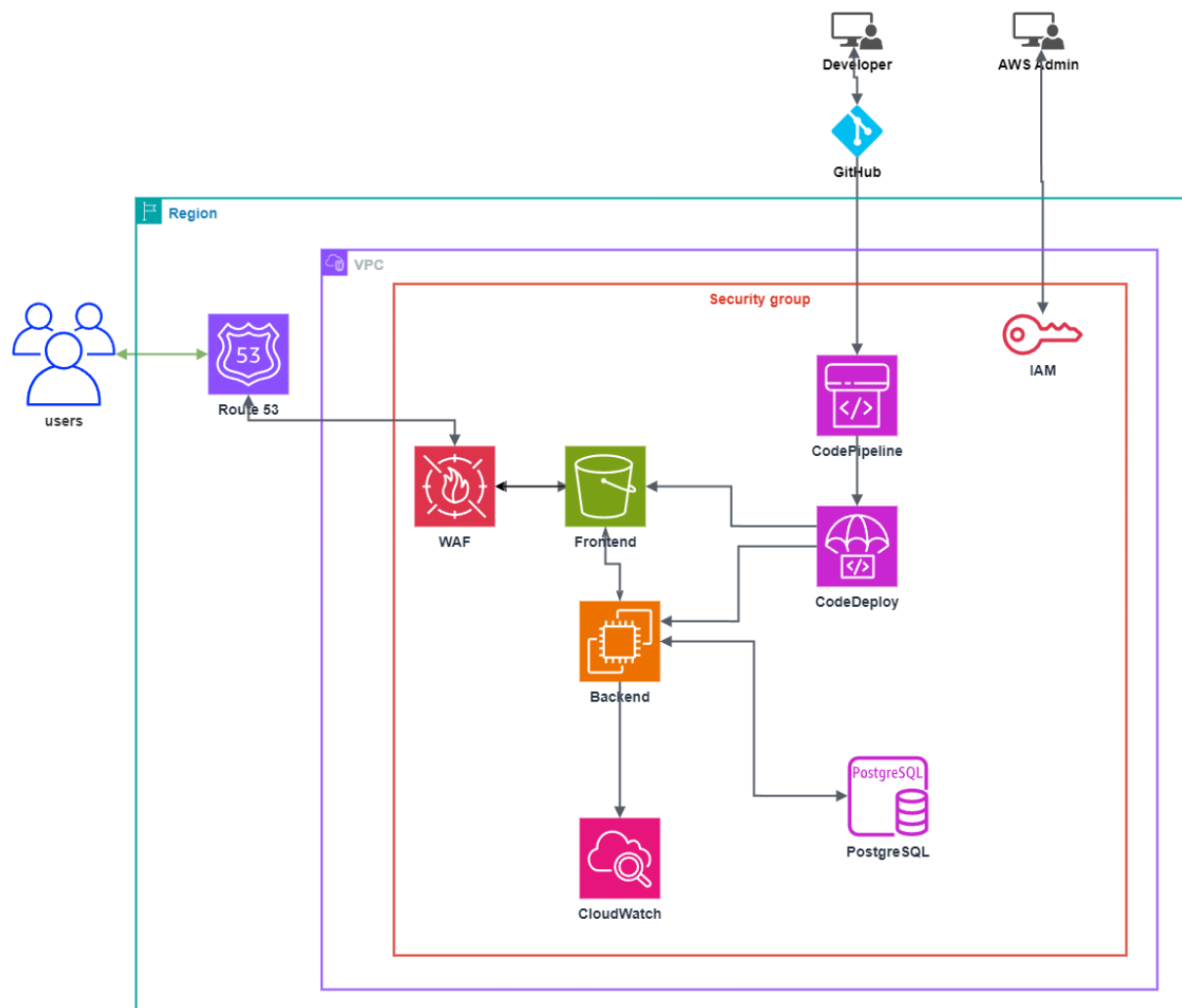
El uso de un certificado SSL es fundamental para garantizar la seguridad y la privacidad de los datos transmitidos entre el navegador del usuario y el servidor web. Este tipo de certificado cifra la información confidencial, como contraseñas, detalles de tarjetas de crédito y otra información personal, evitando que sea interceptada por terceros no autorizados durante la comunicación

5. Informe de Seguridad: Análisis de Puertos Abiertos y Evaluación de Vulnerabilidades en la Máquina

Se han revisado los puertos abiertos en la máquina, y se ha determinado que únicamente están accesibles los puertos HTTP y HTTPS. Sin embargo, tras un análisis detallado de estos puertos, no se ha encontrado ninguna vulnerabilidad que pueda comprometer la seguridad de la máquina. Ambos puertos están configurados de manera segura y no presentan riesgos significativos para la integridad del sistema

6. Futuro despliegue

A continuación se muestra un diagrama de AWS sugerido para tu configuración:



- Para el registro del dominio, se va a utilizar el Route 53.

- Para proteger el entorno frente a ataques maliciosos y vulnerabilidades, vamos a utilizar AWS WAF (Web Application Firewall)
- Utiliza Amazon S3 para alojar tu aplicación frontend de React.
- Despliega de la API de backend Node.js en instancias de Amazon EC2.
- Utilizamos PostgreSQL con Prisma.
- Las instancias EC2, S3 y otros servicios los vamos a colocar dentro de una Virtual Private Cloud (VPC) para aislar la red.
- Se han configurado Grupos de Seguridad para controlar el tráfico de entrada y salida.
- Se va a utilizar Amazon CloudWatch para monitorear las instancias EC2 y otros servicios de AWS.
- Vamos a implementar AWS Identity and Access Management (IAM) para controlar el acceso a los recursos de AWS.
- Para Integración Continua/Despliegue Continuo (CI/CD), se va a utilizar AWS CodePipeline y AWS CodeDeploy para automatizar tu proceso de despliegue.
- También se va a integrar con GitHub para la gestión de código fuente.

7. Conclusiones

Aquí hay algunos consejos que el departamento de ciberseguridad podría ofrecer a la asociación sobre los riesgos de seguir utilizando papel y lápiz para llevar registros de donaciones y cómo podrían mitigar estos riesgos:

Riesgo de pérdida o robo: Los registros en papel son susceptibles de ser extraviados o robados fácilmente, lo que podría comprometer la información sensible de los donantes, como nombres, direcciones y detalles de pago. Una vez que se pierde esta información, puede ser difícil o imposible de recuperar.

Falta de seguridad física: Los documentos en papel no tienen protecciones físicas robustas. Pueden ser accesibles para cualquier persona que tenga acceso al lugar donde se almacenan los archivos. Esto puede aumentar el riesgo de acceso no autorizado o manipulación de la información.

Dificultad para realizar copias de seguridad: Los registros en papel no pueden respaldarse fácilmente como lo harían los datos digitales. En caso de desastre natural, incendio o cualquier otro incidente que cause daño físico a los documentos, la información podría perderse para siempre.

Cumplimiento legal y regulaciones de protección de datos: Dependiendo de la ubicación de la asociación y las leyes locales, podrían existir regulaciones específicas sobre cómo se deben

almacenar y proteger los datos de donantes. El incumplimiento de estas regulaciones podría resultar en sanciones legales y daños a la reputación de la asociación.

Mayor eficiencia y accesibilidad: Al migrar a un sistema digital, la asociación puede mejorar la eficiencia en la gestión de donaciones y hacer que la información sea más accesible para aquellos que la necesitan, ya sea para informes internos, auditorías externas o cualquier otro propósito.

Encriptación y protección de datos: Al utilizar herramientas y plataformas digitales adecuadas, como software de gestión de donaciones, la asociación puede implementar medidas de seguridad, como la encriptación de datos, para proteger la información confidencial de los donantes contra el acceso no autorizado.

Capacitación del personal: Es importante capacitar al personal sobre las mejores prácticas de seguridad cibernética, incluido el manejo seguro de datos digitales, el uso de contraseñas seguras y la identificación de posibles amenazas de seguridad.

Plan de respuesta a incidentes: A pesar de las medidas preventivas, siempre existe la posibilidad de que ocurra un incidente de seguridad. Por lo tanto, la asociación debería tener un plan de respuesta a incidentes en su lugar para abordar rápidamente cualquier brecha de seguridad y minimizar su impacto.

En resumen, migrar de registros en papel a un sistema digital no solo puede mejorar la seguridad de los datos de la asociación, sino también aumentar la eficiencia y la accesibilidad de la información. Es importante que la asociación comprenda los riesgos asociados con el uso de registros en papel y tome medidas proactivas para mitigarlos mediante la adopción de soluciones digitales seguras.”

La modificación regular de las claves privadas es una medida fundamental para fortalecer la seguridad de los sistemas y proteger la información confidencial de los donantes. Al implementar esta recomendación, la Fundación Mera Parivar estará mejor posicionada para mitigar los riesgos asociados con las amenazas cibernéticas y mantener la confianza de sus donantes en la seguridad de sus transacciones

Tras una evaluación de la página web y la investigación en las redes sociales asociadas proporcionadas por la empresa, se identificaron perfiles de empleados en LinkedIn. Durante el proceso de búsqueda de inteligencia en fuentes abiertas (OSINT), se descubrió que tres de los empleados tenían sus correos electrónicos corporativos asociados, a excepción de "Medha Bhagat", cuyo correo personal está vinculado a una cuenta de Gmail.