



SEGURIDAD WEB





SEGURIDAD WEB

Es proteger el sitio o la aplicación web detectando, previniendo y respondiendo a los ataques de cualquier mala intención.





CONTRASEÑAS SEGURAS

- Crear contraseñas que tengan al menos 16 caracteres.
- Usar números, caracteres especiales (como \$%&#), letras mayúsculas y letras minúsculas.
- Evitar cualquier palabra relacionada contigo o el servicio que protege la contraseña.





PROVEEDORES HOSTING

Es conveniente para un sitio web un proveedor de hosting que ofrezca respaldos, soporte técnico, tiempo de operatividad superior al 90%.





RESPUESTA DE ANTIVIRUS

Los antivirus tienen la capacidad de identificar cuando un sitio web es de confianza. Si el antivirus de los clientes responden favorablemente al sitio web, ellos lo consideran como confiable.





CERTIFICADO SSL

Los Certificados Secure Sockets Layer (SSL) encriptan la información sensible de los usuarios, como sus datos bancarios y direcciones, haciéndolos que viajen de forma segura en Internet. De esta manera, los datos sensibles no pueden ser vistos o interceptados por los hackers.





PLANES DE SEGURIDAD WEB

Se pueden contratar mediante empresas online y ofrecen:

- Análisis de malware: detectan programas maliciosos que quieren afectar los dispositivos.
- Recuperación del sitio web: lo almacenan en diferentes servidores para fácil recuperación.





PLANES DE SEGURIDAD WEB

Se pueden contratar mediante empresas online y ofrecen:

- Prevención de ataques DDoS: Previenen ataques de denegación de servicio distribuido, en donde envían muchas solicitudes falsas a un sitio web para tumbarlo y hacer que se pierdan clientes y ventas.
- Protección contra piratas informáticos: Evitan que se reciban datos de piratas con el fin de dañar o robar información de la base de datos.





RESPALDO DE LOS SITIOS WEB

Realizar respaldos de tus sitios web manualmente.





ACTUALIZACIONES AUTOMÁTICAS

Configurar que los sitios web, frameworks, plugins, CMS o paneles de gestión web puedan actualizarse automáticamente. Esto ayuda a evitar posibles ataques.





INTEGRIDAD DEL SITIO WEB

Evitar que el sitio web sea modificado por hackers.

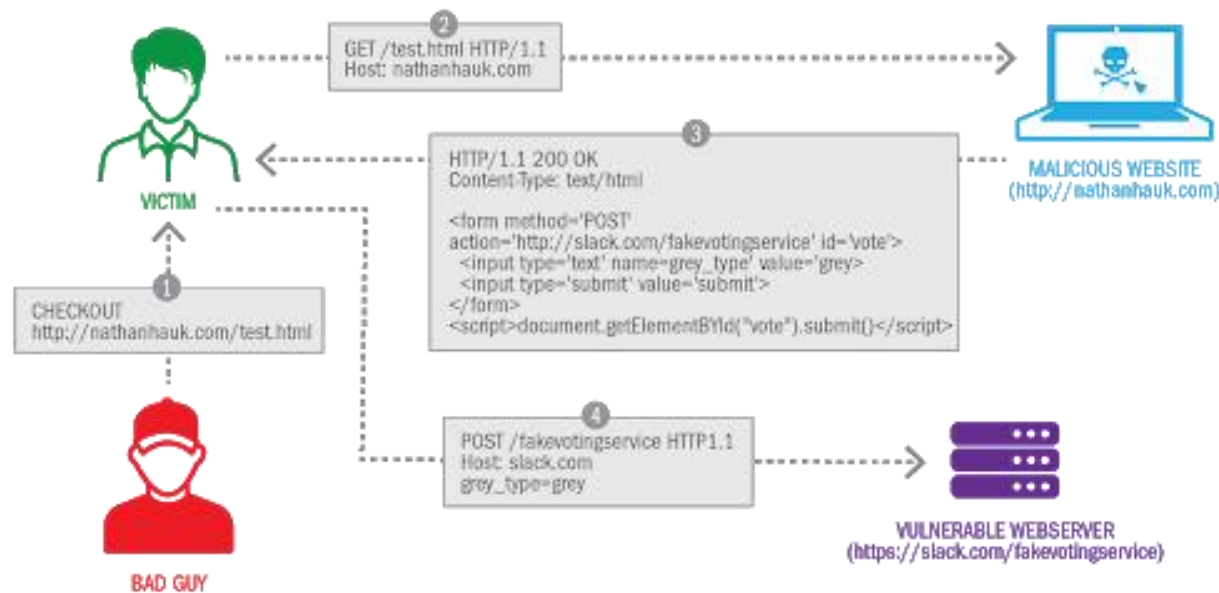
- Inclusión Remota de Archivos (Remote File Inclusion/RFI)
- Secuencia de Comandos en Sitios Cruzados (Cross-site scripting/XSS)
- Falsificación de Petición en Sitios Cruzados





TOKEN DE CSRF

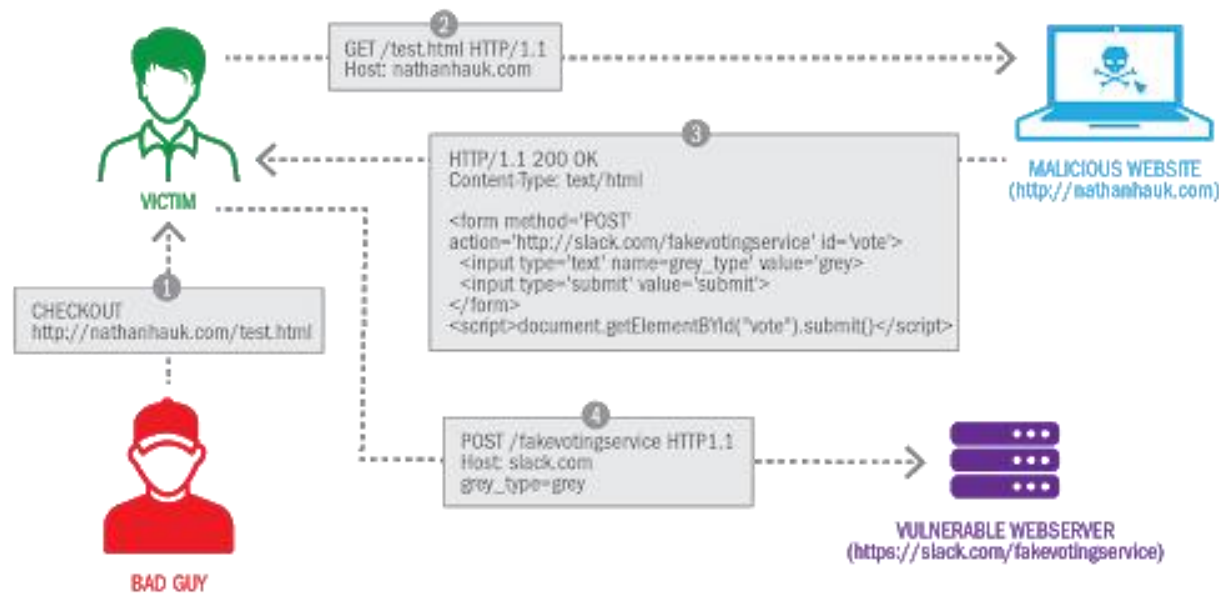
Se debe verificar y comprobar los datos dinámicamente mediante un Token de Seguridad Único cada vez que se inicia una sesión.





TOKEN DE CSRF

Se debe verificar y comprobar los datos dinámicamente mediante un Token de Seguridad Único cada vez que se inicia una sesión.





TECNOLOGÍAS DE SEGURIDAD WEB

- Herramientas de prueba de caja negra
- Herramientas de fuzzing
- Herramientas de prueba de caja blanca
- Cortafuegos de aplicaciones web (WAF)
- Escáneres de seguridad o vulnerabilidad
- Herramientas de craqueo de contraseña
- Probabilidad de amenaza



PROTOCOLOS DE SEGURIDAD WEB

Los protocolos de seguridad web garantizan la seguridad y la integridad de los datos en tránsito a través de una conexión de red como Internet.

HTTPS	TCP/IP	FTP	DNS	SET
IPSec	HTTP	SSH	SSL	