USM

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

Seguridad de Sistemas

Clase 1: Metodologías de Seguridad en aplicaciones web

Objetivos

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

- Conocer los diferentes modelos de seguridad utilizados en aplicaciones web en la industria

- Conocer la metodología de Pentesting para aplicaciones web

- Conocer la formula de estimación del riesgo monetario para incidentes en aplicaciones web

Modelos de Seguridad

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

- Hoy en día existen varios modelos de Seguridad en Aplicación web, cuyo principal objetivo es poder regular la instalación, configuración y desarrollo de aplicaciones web en forma segura
- Los principales ámbitos que cubren estos modelos son:
  - Desarrollo
  - Arquitectura de red
  - Arquitectura de aplicaciones
  - Metodologías de análisis
  - Pruebas funcionales y de seguridad

OWASP

UNIVERSIDAD TECNICA FEDERICO SANTA MARIA

- OWASP (Open Web Application Security Project):
- Organización sin fines de lucro que existe desde el año 2001, dedicada principalmente a desarrollar, mantener y operar aplicaciones web en forma segura
- OWASP se encarga de la publicación de información que ayuda a mejorar los procesos de desarrollo de aplicaciones web en cada una de sus fases
- Sitio web:
  - https://owasp.org/

OWASP

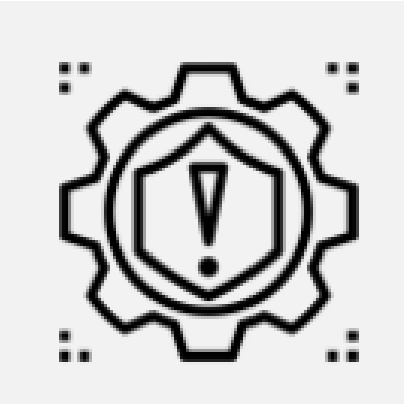
UNIVERSIDAD TECNICA FEDERICO SANTA MARIA

- Guía de revisión de OWASP:
- Una de las publicaciones mas importantes de OWASP es la guía de revisión de aplicaciones:
- https://owasp.org/www-project-web-security-testing-guide/v42/
- Este documento incluye:
  - Aplicaciones para pentesting web
  - Herramientas para desarrollo seguro
  - Métodos de revisión de aplicaciones
  - Métodos de revisión de control de acceso
  - Testing de vulnerabilidades
  - Revisión de criptografía

OWASP

UNIVERSIDAD TECNICA FEDERICO SANTA MARIA

- Guía de mitigación de OWASP:
- En el sitio de OWASP se encuentra la guía de mitigación de las vulnerabilidades en el documento “OWASP Top 10 2017”, el que se puede encontrar en el siguiente link:
- https://owasp.org/www-project-top-ten/
- En este documento se encuentra la información para realizar las mitigaciones de cada una de las vulnerabilidades.



OWASP

- Guía de mitigación OWASP (cont.):

- Ejemplo: Ataques de inyección

Cómo se previene

Para prevenir inyecciones, se requiere separar los datos de los comandos y las consultas.

- La opción preferida es utilizar una API segura, que evite el uso de un intérprete por completo y proporcione una interfaz parametrizada. Se debe migrar y utilizar una herramientas de Mapeo Relacional de Objetos (ORMs).
  Nota: Incluso cuando se parametrizan, los procedimientos almacenados pueden introducir una inyección SQL si el procedimiento PL/SQL o T-SQL concatena consultas y datos, o se ejecutan parámetros utilizando *EXECUTE IMMEDIATE* o *exec()*.
- Realice validaciones de entradas de datos en el servidor, utilizando "listas blancas". De todos modos, esto no es una defensa completa ya que muchas aplicaciones requieren el uso de caracteres especiales, como en campos de texto, APIs o aplicaciones móviles.
- Para cualquier consulta dinámica residual, escape caracteres especiales utilizando la sintaxis de caracteres específica para el intérprete que se trate.
  Nota: La estructura de SQL como nombres de tabla, nombres de columna, etc. no se pueden escapar y, por lo tanto, los nombres de estructura suministrados por el usuario son peligrosos. Este es un problema común en el software de redacción de informes.
- Utilice LIMIT y otros controles SQL dentro de las consultas para evitar la fuga masiva de registros en caso de inyección SQL.

OWASP

UNIVERSIDAD TECNICA FEDERICO SANTA MARIA

OWASP Top 10 2013	±	OWASP Top 10 2017
A1 – Inyección	→	A1:2017 – Inyección
A2 – Pérdida de Autenticación y Gestión de Sesiones	→	A2:2017 – Pérdida de Autenticación y Gestión de Sesiones
A3 – Secuencia de Comandos en Sitios Cruzados (XSS)	↘	A3:2017 – Exposición de Datos Sensibles
A4 – Referencia Directa Insegura a Objetos [Unido+A7]	∪	A4:2017 – Entidad Externa de XML (XXE) [NUEVO]
A5 – Configuración de Seguridad Incorrecta	↘	A5:2017 – Pérdida de Control de Acceso [Unido]
A6 – Exposición de Datos Sensibles	↗	A6:2017 – Configuración de Seguridad Incorrecta
A7 – Ausencia de Control de Acceso a las Funciones [Unido+A4]	∪	A7:2017 – Secuencia de Comandos en Sitios Cruzados (XSS)
A8 – Falsificación de Peticiones en Sitios Cruzados (CSRF)	☒	A8:2017 – Deserialización Insegura [NUEVO, Comunidad]
A9 – Uso de Componentes con Vulnerabilidades Conocidas	→	A9:2017 – Uso de Componentes con Vulnerabilidades Conocidas
A10 – Redirecciones y reenvíos no validados	☒	A10:2017 – Registro y Monitoreo Insuficientes [NUEVO, Comunidad]

OWASP

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

- Application Security Verification Standard (ASVS):
- El proyecto del estándar de verificación de seguridad de aplicaciones (ASVS) de OWASP proporciona una base para probar los controles técnicos de seguridad de las aplicaciones web y también proporciona a los desarrolladores una lista de requisitos para un desarrollo seguro.
- El estándar proporciona una base para probar los controles técnicos de seguridad de las aplicaciones, así como los controles técnicos de seguridad en el entorno, en los que se confía para proteger contra vulnerabilidades como Cross-Site Scripting (XSS) e inyección SQL.

OWASP

UNIVERSIDAD TECNICA FEDERICO SANTA MARIA

- Application Security Verification Standard (ASVS):

- Recursos:
- https://github.com/OWASP/ASVS/tree/v4.0.2#latest-stable-version---402

- https://github.com/shenril/owasp-asvs-checklist

OSSTMM

- Los principales aspectos considerados en la metodología OSSTMM son:
  - Seguridad de la Información
  - Seguridad de Procesos
  - Seguridad de tecnologías de Internet
  - Seguridad en las comunicaciones
  - Seguridad en redes inalámbricas
  - Seguridad Física
  - Cumplimiento normativo
  - Confección de informes

OSSTMM

- Open Source Security Testing Methodology Manual: corresponde a una metodología para realizara análisis y auditorias de seguridad, propuesta por la empresa ISECOM, con bastante aceptación en la industria de la seguridad.
- URL:
  - https://www.isecom.org/research.html#content5-9d
- Incluye un marco de trabajo que describe las fases que se deben realizar en un proceso análisis de seguridad, experiencia recopilada por mas de 150 profesionales que colaboran en modalidad “comunitaria”

NIST

UNIVERSIDAD TECNICA FEDERICO SANTA MARIA

- NIST es el Instituto Nacional de Normas y Tecnologías (ex NBS), dependiente del Departamento de Comercio de EE. UU. y su principal misión es promover la competencia industrial mediante los avances en tecnología de tal forma de mejorar la estabilidad económica y la calidad de vida de las personas
- Ubicada en Maryland y existe desde 1988 y uno de sus principales programa es el de tecnologías de información
- Publica permanentemente documentos respecto a temas de Seguridad de la Información
  - https://www.nist.gov/publications

National Institute of Standards and Technology
U.S. Department of Commerce

NIST

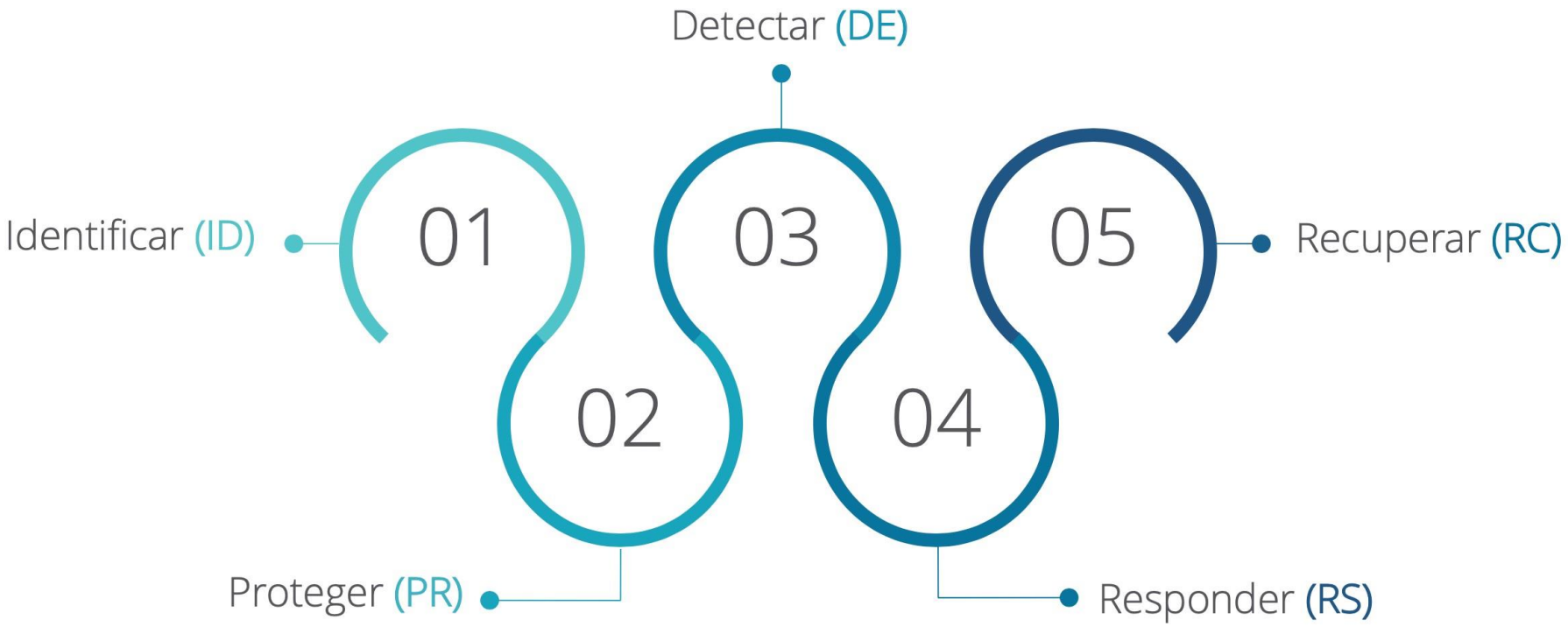
UNIVERSIDAD TECNICA FEDERICO SANTA MARIA

- Una de sus publicaciones, referente a Seguridad en Aplicaciones web es SP 1800-16 que es una guía para mejorar la seguridad de las transacciones en aplicaciones web que utilizan SSL/TLS.
  - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-16.pdf
- En este documento se revisan los principales aspectos de seguridad en aplicaciones web, tales como:
  - Riesgos en el uso de Certificados Digitales
  - Compañías que venden Certificados Digitales
  - Mejores practicas en la implementación de SSL/TLS
  - Implementación de un programa de seguridad para SSL/TLS

NIST

UNIVERSIDAD TECNICA FEDERICO SANTA MARIA

- **Framework NIST de Ciberseguridad**



Framework NIST

UNIVERSIDAD TECNICA FEDERICO SANTA MARIA

- **<u>Identificación:</u>**
- los datos, el personal, los dispositivos, los sistemas y las instalaciones que permiten a la organización alcanzar los objetivos comerciales se identifican y gestionan de acuerdo con su importancia relativa para los objetivos de la organización y la estrategia de riesgo de la organización.
- Ejemplo: Inventario de activos
- Concepto clave: **VISIBILIDAD**

Framework NIST

UNIVERSIDAD TECNICA FEDERICO SANTA MARIA

- **<u>Proteger</u>:**
- El acceso a los activos físicos y lógicos y las instalaciones asociadas está limitado a los usuarios, procesos y dispositivos autorizados, y se gestiona de acuerdo con el riesgo evaluado de acceso no autorizado a las actividades y transacciones autorizadas.
- Ejemplo: Control de acceso a la entrada del edificio
- Concepto clave: **CONTROL**

Framework NIST

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

- **<u>Detectar</u>:**
- El sistema de información y los activos se monitorean para identificar eventos de ciberseguridad y verificar la efectividad de las medidas de protección.
- Ejemplo: Sistema de antimalware
- Concepto clave: **MONITOREO**

Framework NIST

UNIVERSIDAD TECNICA FEDERICO SANTA MARIA

- **<u>Responder</u>:**
- Los procesos y procedimientos de respuesta se ejecutan y mantienen para garantizar la respuesta a los incidentes de ciberseguridad detectados.
- Ejemplo: Sistema de bloqueo
- Concepto clave: **ACTUACION**

Framework NIST

UNIVERSIDAD TECNICA FEDERICO SANTA MARIA

- **<u>Recuperar</u>:**
- Los procesos y procedimientos de recuperación se ejecutan y mantienen para garantizar la restauración de los sistemas o activos afectados por incidentes de ciberseguridad.
- Ejemplo: Sistema de respaldo
- Concepto clave: **RESTAURACION.**

ISSAF

- Marco de evaluación de la seguridad de los sistemas de información.
- Su objetivo es evaluar la política de seguridad de la información y el cumplimiento de una organización con los estándares, leyes y requisitos reglamentarios de la industria de TI.
- Cubre las siguientes etapas:
  - Gestión de proyectos
  - Directrices y mejores prácticas: evaluación previa, evaluación y evaluación posterior
  - Metodología de evaluación
  - Revisión de la política de seguridad de la información y la organización de seguridad.
  - Evaluación de la metodología de evaluación de riesgos
  - Evaluación de control técnico
  - Evaluación de control técnico: metodología
  - Seguridad de la contraseña

Penetration Testing Execution Standard (PTES)

- Este estándar es el estándar más utilizado y cubre casi todo lo relacionado con la prueba de penetración.
- PTES se divide en siete fases:
  - Interacciones previas al compromiso
  - La recogida de información
  - Modelado de amenazas
  - Análisis de vulnerabilidad
  - Explotación
  - Post explotación
  - Reportando
- http://www.pentest-standard.org/index.php/Main_Page

Test de Penetración

USM

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

- Las pruebas de penetración, también conocidas como pruebas de penetración, son un ataque autorizado a un sistema informático que se realiza para evaluar la seguridad del sistema/red.
- La prueba se realiza para identificar vulnerabilidades y los riesgos que representan. Una prueba de penetración típica es un proceso de cinco etapas que identifica los sistemas de destino, sus vulnerabilidades y la capacidad de explotación de cada vulnerabilidad.
- El objetivo es encontrar tantas vulnerabilidades como sea posible e informar en un formato universalmente aceptable para que el cliente las comprenda.

Test de Penetración

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

- Tipos de nivel de acceso:
- Caja blanca (White box): en este escenario el auditor tiene todas las credenciales de acceso para realizar la evaluación, ol objetivo es simular la interacción de un usuario con altos privilegios en la aplicación a evaluar
- Caja gris (Gray box): en este escenario, el auditor tiene permisos básicos de acceso, el objetivo es simular la conexión de un usuario cualquiera, típicamente aplicaciones que operan con clientes
- Caja negra (Black box): en este escenario el auditor solo tiene la dirección de la aplicación y ningún tipo de acceso, el objetivo es simular la conexión de un usuario no autorizado y determinar si es posible violar los controles de acceso.

Test de Penetración

USM
UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

- El test de penetración para aplicaciones web, se compone de las siguientes fases:
  - Etapa 1: Reconocimiento
  - Etapa 2: enumeración
  - Etapa 3: Evaluación y análisis de vulnerabilidad
  - Etapa 4: Explotación (incluye el período posterior a la explotación)
  - Etapa 5: Informes

Reconocimiento

- El reconocimiento es la primera etapa de la realización de una prueba de penetración. En esta etapa, un pentester intentará identificar el sistema o la aplicación en cuestión y encontrar la mayor cantidad de información posible sobre él.
- Esta es la etapa más crucial de las pruebas, ya que este paso define la superficie de ataque.
- En las pruebas de caja blanca, el reconocimiento puede no ser importante porque el cliente ya proporciona toda la información sobre el objetivo dentro del alcance.

Reconocimiento

USM

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

- La siguiente es la lista de herramientas que se pueden utilizar para realizar el reconocimiento en una aplicación web:
  - Identificación de aplicaciones que se ejecutan en un puerto no estándar (puertos personalizados definidos por el usuario): Amap, Nmap, etc.
  - Identificación de DNS y subdominios: dnsenum, dnsmap, dnswalk, dnsrecon, dnstracer, Fierce, dnscan, Sublist3r, etc.
  - Identificación de plataformas tecnológicas: BlindElephant, Wappalyzer, WhatWeb, etc.
  - Identificación de sistemas de gestión de contenido: WPScan, Joomscan, CMScan, Drupscan, etc.

Reconocimiento

UNIVERSIDAD TECNICA FEDERICO SANTA MARIA

- Ejemplo:

```
└─# whatweb 10.0.2.8
http://10.0.2.8 [200 OK] Apache[2.2.8], Country[RESERVED][ZZ], HTTPS
erver[Ubuntu Linux][Apache/2.2.8 (Ubuntu) DAV/2], IP[10.0.2.8], PHP[
5.2.4-2ubuntu5.10], Title[Metasploitable2 - Linux], WebDAV[2], X-Pow
ered-By[PHP/5.2.4-2ubuntu5.10]
```

```
└─# nmap -sV -p 80 10.0.2.8
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-28 15:29 EDT
Nmap scan report for 10.0.2.8
Host is up (0.00039s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
MAC Address: 08:00:27:92:12:09 (Oracle VirtualBox virtual NIC)
```

Análisis de vulnerabilidades

USM

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

- Se realiza una evaluación de vulnerabilidades en la aplicación web para identificar vulnerabilidades en una página web, directorio, método de protocolo HTTP, encabezados HTTP, etc.
- El escaneo se puede realizar utilizando herramientas disponibles públicamente o herramientas con licencia de pago. Todos los tipos de pruebas (caja blanca, caja negra y caja gris) dependen en gran medida de esta etapa.
- Una vez que se ha realizado un escaneo de vulnerabilidades, debemos evaluar y analizar cada vulnerabilidad que se encuentre y luego filtrar los falsos positivos.

Análisis de vulnerabilidades

UNIVERSIDAD TECNICA FEDERICO SANTA MARIA

- Ejemplo:

Cross Site Scripting (Reflected)

URL:	http://10.0.2.8/mutillidae/index.php?page=javascript%3Aalert%281%29%3B
Risk:	High
Confidence:	Medium
Parameter:	page
Attack:	javascript:alert(1);
Evidence:	javascript:alert(1);
CWE ID:	79
WASC ID:	8
Source:	Active (40012 - Cross Site Scripting (Reflected))

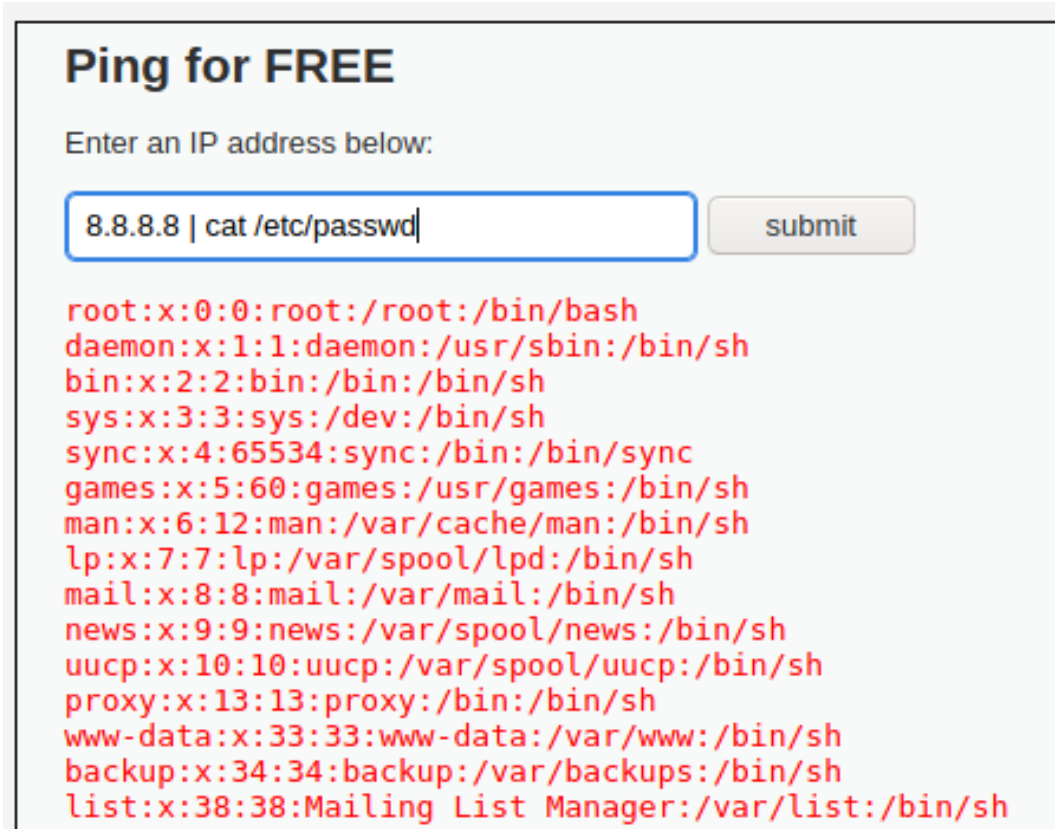
Explotación

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

- La etapa de explotación es la segunda etapa más crucial después de la etapa de reconocimiento. Esta etapa prueba si una determinada vulnerabilidad encontrada en la etapa anterior es explotable.
- Un pentester siempre puede identificar el éxito de los proyectos de pruebas de penetración si puede aprovechar las vulnerabilidades que se encuentran. La explotación se puede realizar automáticamente utilizando ciertas herramientas, como Metasploit Framework y Canvas.
- Esto se debe a que no sabemos cómo se comportará una determinada aplicación web o sistema cuando usamos nuestras cargas útiles.

Explotación

- Ejemplo:



Explotación

USM
UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

- Búsqueda de exploits:
- https://www.exploit-db.com/

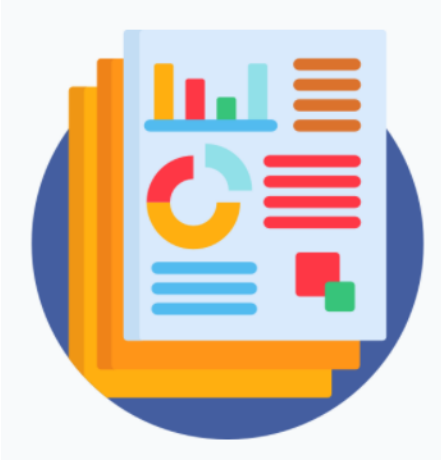
Search: sql injection

V	Title	Type	Platform	Author
✕	Simple Phone book/directory 1.0 - 'Username' SQL Injection (Unauthenticated)	WebApps	PHP	Justin White
✕	Laundry Booking Management System 1.0 - 'Multiple' SQL Injection	WebApps	PHP	Azumah Foresight Xorlali
✕	Online Traffic Offense Management System 1.0 - 'id' SQL Injection (Authenticated)	WebApps	PHP	Justin White

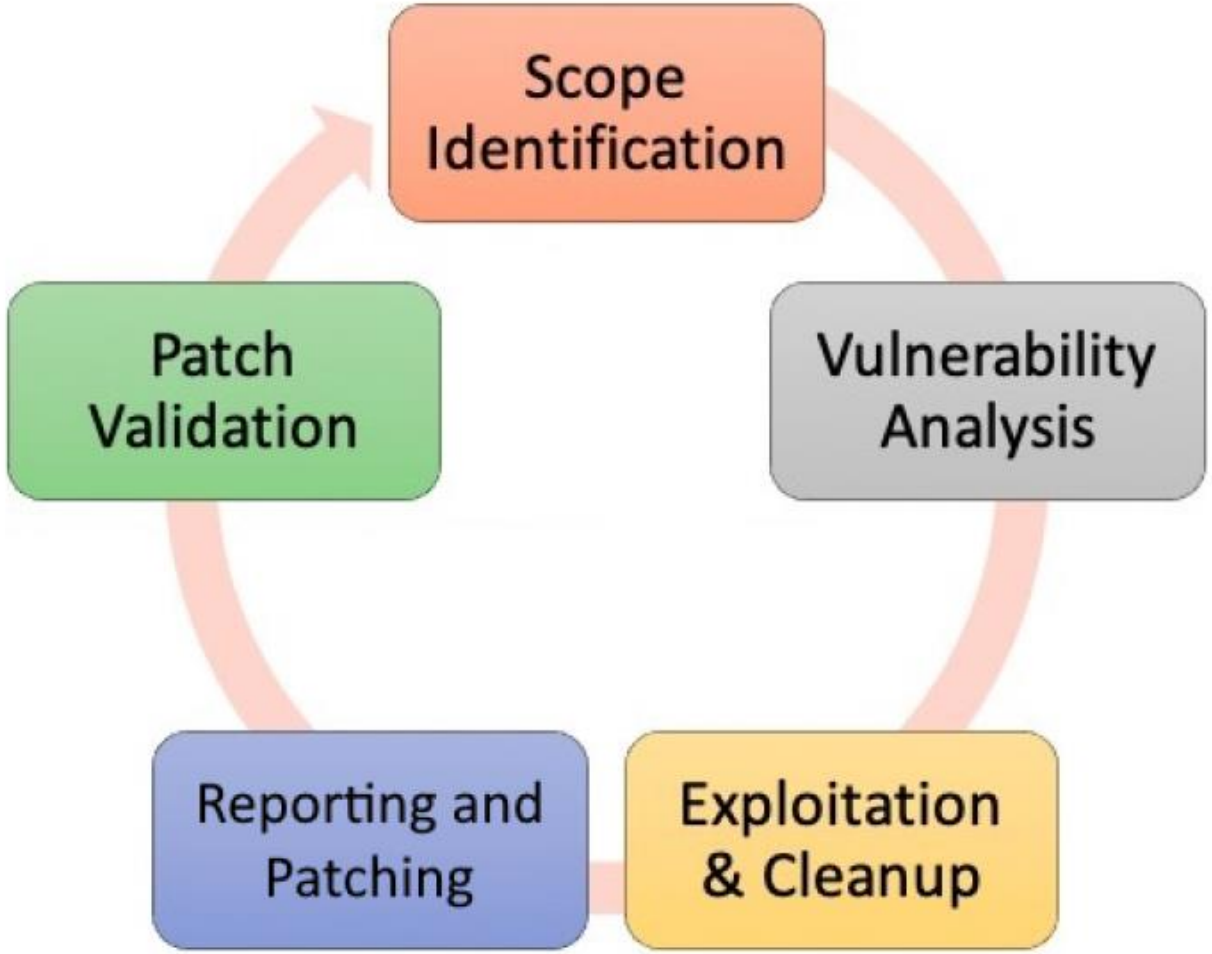
Reporte

UNIVERSIDAD TECNICA FEDERICO SANTA MARIA

- La etapa de informes es la etapa final del proceso de prueba de penetración e implica informar todas y cada una de las vulnerabilidades encontradas en el objetivo (dentro del alcance). Las vulnerabilidades informadas se enumerarán de acuerdo con el nivel de gravedad definido por el Common Vulnerability Scoring System (CVSS), que es un estándar abierto y gratuito que se utiliza para evaluar las vulnerabilidades.



Ciclo de Pentesting



Conclusiones

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

- Dado el alto uso de las aplicaciones web, se hace necesario revisar la seguridad de sus componentes, principalmente por la alta sensibilidad de la información que manejan, datos de usuarios, contraseñas, tarjetas de crédito, catalogo de productos, etc.
- Las diferentes metodologías de Evaluación de Seguridad de aplicaciones web, desarrolladas por las más prestigiosas instituciones, permiten organizar este proceso de manera efectiva.
- Finalmente la explotación de vulnerabilidades es la forma de demostrar, a través de evidencias, que las aplicaciones tienen fallas de seguridad que pueden comprometer su información.

Resumen

- Modelos de Seguridad
- OWASP
  - Guía de revisión
  - Top 10
  - ASVS
- OSSTMM
- NIST
  - Framework de Ciberseguridad
- ISSAF
- PTES
- Test de Penetración