



UNIVERSIDADE DA CORUÑA

UD03

Amenazas y vulnerabilidades





Índice de contenidos

Dedicación estimada

Fase a distancia

- | | |
|-------------------------------------|-------|
| 1. Introducción y conceptos previos | 15min |
| 2. Vulnerabilidades | 60min |
| 3. Amenazas | 45min |

Fase presencial

- | | |
|------------------|-------|
| 1. Ataques | 60min |
| 2. OWASP | 50min |
| 3. Contramedidas | 10min |

Al finalizar cada bloque se plantea al alumno la realización de un cuestionario con el que evaluar su asimilación de los conceptos planteados

En cada bloque se añade una serie de material complementario con el que el alumno puede ampliar o profundizar en los conceptos explicados previamente



UNIVERSIDADE DA CORUÑA

UD03

Amenazas y vulnerabilidades

Fase No Presencial





1. Introducción y conceptos previos

Sistema de Gestión de la Seguridad de la Información

- Herramienta que permite conocer y gestionar los riesgos a los que se enfrenta la información de una empresa.
- Puede realizar tareas del estilo de:
 - Definición de políticas y procedimientos que automaticen tareas de seguridad
 - Catalogación de los activos de información
 - Automatización de parches de seguridad
 - Análisis automáticos en busca de virus
 - Etc.

1. Introducción y conceptos previos

Sistema de Gestión de la Seguridad de la Información

- Más formalmente un SGSI es un es un sistema gerencial general basado en un enfoque de riesgos para establecer, implementar, operar, monitorizar, revisar, mantener y mejorar la seguridad de la información
- Establece un **modelo preventivo** para la seguridad de la información
 - 1) Planificar
 - Identificación, análisis y evaluación de riesgos.
 - 2) Hacer
 - Implementación plan tratamiento de los riesgos
 - Procedimientos de detección y respuesta a incidentes de seguridad
 - 3) Revisar
 - Monitorización y revisión del sistema de información
 - Auditorías
 - 4) Actuar
 - Mejora continua del SGSI



1. Introducción y conceptos previos

Sistema de Gestión de la Seguridad de la Información

- Su definición y puesta en marcha es el núcleo principal de la norma ISO 27001
 - www.iso27000.es



1. Introducción y conceptos previos

Consideraremos que un sistema de información es seguro cuando existe garantía de que se comportará de manera correcta en aquello para lo que ha sido diseñado...

... sin embargo, existen multitud de factores que pueden afectar a este correcto funcionamiento (iso27000:2009).

- Vulnerabilidades
- Amenazas
- Ataques



1. Introducción y conceptos previos

Información complementaria

- Sistemas de Gestión de Seguridad de la Información
 - http://www.iso27000.es/download/doc_sgsi_all.pdf



Cuestionario 1



2. Vulnerabilidades

- Debilidad de un activo o control que puede ser explotada por una **amenaza** (ISO 27000:2009).
- Posibilidad de que una amenaza se materialice sobre un activo.
- Es una vía de ataque potencial.
- Una analogía podría ser considerar una vulnerabilidad como el eslabón más débil de la cadena que protege nuestro sistema



2. Vulnerabilidades

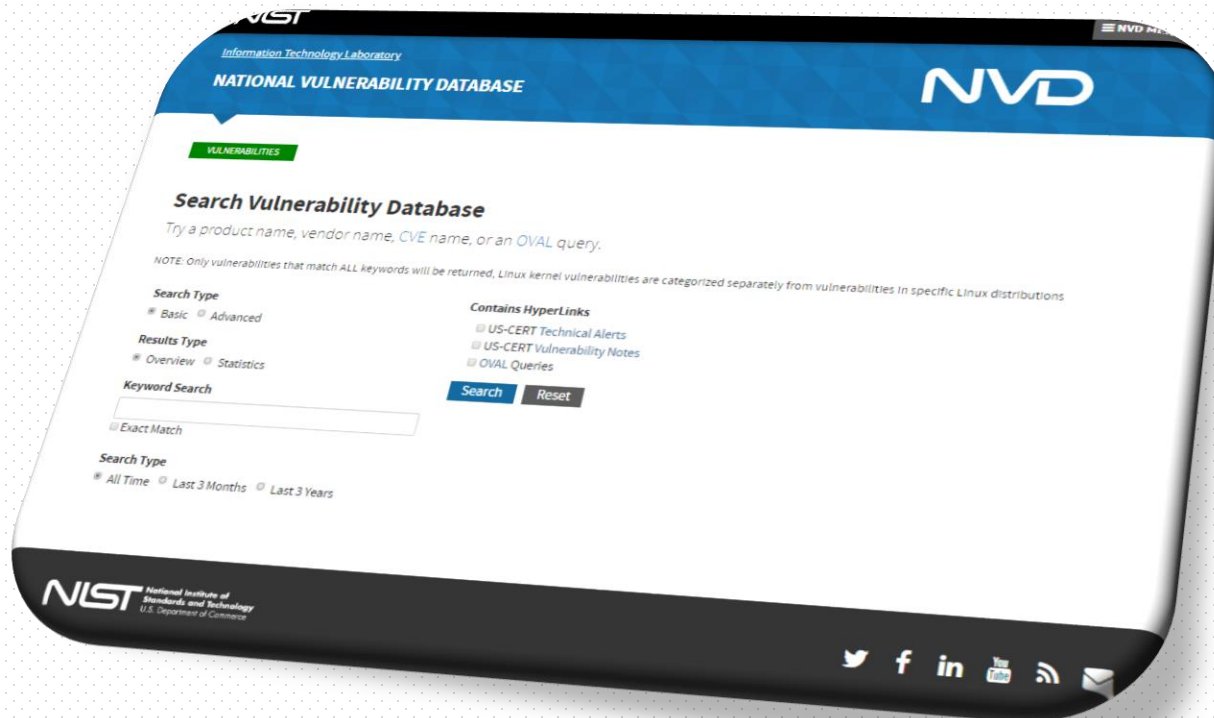
- Ejemplos:
 - Defectos en HW o SW
 - Buffer overflow, consultas no parametrizadas (sql-injection), ...
 - Carencia de políticas y procedimiento
 - Falta de formación en seguridad por parte de los usuarios, controles de acceso no definidos, ...
 - Políticas de backup incorrectas o inexistentes
 - ...

2. Vulnerabilidades

- Terminología
 - **CVE: Common Vulnerabilities and Exposures** (Vulnerabilidades y amenazas comunes). Es un código asignado a una vulnerabilidad que le permite ser identificada de forma unívoca.
 - **Category (CWE):** Tipo de ataque: Authentication Issues, Buffer Errors, Code Injection, Configuration, Credentials Management, Cross-Site Request Forgery (CSRF), Cross-Site Scripting (XSS), SQL Injection, ...
 - **Vector de Acceso (Access Vector):** La métrica que refleja cómo la vulnerabilidad es explotada. Es decir, desde dónde se realiza el ataque. Los valores son: red (network), red local (local network) y sólo acceso local (local access only)
 - **Complejidad de Acceso (Access Complexity):** Low, Medium, High, Insufficient Information
 - **Gravedad (Severity (Base Score Range)):** rango entre 0 (baja) y 10 (alta)

2. Vulnerabilidades

U.S. National Vulnerability Database (NVD):



<https://nvd.nist.gov/vuln/search>

2. Vulnerabilidades

U.S. National Vulnerability Database (NVD):

- Ofrece una métrica para describir las características e impacto de cada vulnerabilidad
 - Common Vulnerability Scoring System (CVSS)
 - Las vulnerabilidades se puntúan de 0 a 10 según su gravedad
 - CVSS versión 2.0 divide las vulnerabilidades en 4 subcategorías (bajo ($\text{score} < 4$), medio ($4 < \text{score} < 7$) y alto impacto ($\text{score} > 7$))
 - CVSS versión 3.0 divide las vulnerabilidades en 5 categorías (None, Bajo, Medio, Alto, Crítico)



2. Vulnerabilidades

U.S. National Vulnerability Database (NVD):

- Para cada vulnerabilidad ofrece:
 - Descripción
 - Enlace a la Base de datos CVE (Common Vulnerabilities and Exposures)
 - Identificador único de la vulnerabilidad
 - Impacto (según CVSS v2.0 y/o CVSS v3.0)
 - Consejos, soluciones, herramientas
 - Detalles técnicos
 - Listado de software vulnerable y versiones
 - Histórico
 - Fecha de registro
 - Modificación

CVE-2018-19723 Detail

Current Description

Adobe Acrobat and Reader versions 2018.011.20050 and earlier, 2017.011.20050 and earlier, and 2015.006.20440 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. Note: A different vulnerability than CVE-2018-19721.

Source: MITRE

Description Last Modified: 01/26/2019

[View this CVE on NVD website](#)

Impact

CVSS v2.0 Severity and Metrics:

Base Score: 7.5 (HIGH)
 Vector: AV:N/AC:L/PR:N/UI:N/S:C/CV:N/IA:N (V2 legend)
 Impact Score: 7.0
 Exploitability Score: 3.0

Attack Vector (AV): Network
 Attack Complexity (AC): Low
 Privileges Required (PR): None
 User Interaction (UI): None
 Scope (S): Unchanged
 Confidentiality (C): High
 Integrity (I): None
 Availability (A): None

CVSS v2.0 Severity and Metrics:

Base Score: 5.0 (MEDIUM)
 Vector: (AV:N/AC:L/PR:N/C:PS:N/IA:N) (V2 legend)
 Impact Subscore: 2.0
 Exploitability Subscore: 10.0

Access Vector (AV): Network
 Access Complexity (AC): Low
 Authentication (AU): None
 Confidentiality (C): Partial
 Integrity (I): None
 Availability (A): None
 Additional Information:
 Allows unauthorized disclosure of information

References to Advisories, Solutions, and Tools

By following these links, you will be leaving NIST webpages. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
https://www.securityfocus.com/bid/132753	Third Party Advisory
https://helpx.adobe.com/security/products/acrobat/aps18-34.html	Patch Vendor Advisory

Technical Details

Vulnerability Type (View All)

- Out-of-bounds Read (CWE-120)

Vulnerable software and versions [Switch to CVE 2.2](#)

Configuration 1

AND

OR

- [cpe:2.3:adobe:acrobat:***classical***](#) + [versions from \[Included: 17.011.20050\] up to \[Included: 17.011.20050\]](#)
- [cpe:2.3:adobe:acrobat_reader:***classical***](#) + [versions from \[Included: 15.006.20440\] up to \[Included: 15.006.20440\]](#)
- [cpe:2.3:adobe:acrobat_reader:***continuous***](#) + [versions from \[Included: 15.006.20440\] up to \[Included: 15.006.20440\]](#)
- [cpe:2.3:adobe:acrobat_reader:***classical***](#) + [versions from \[Included: 17.011.20050\] up to \[Included: 17.011.20050\]](#)
- [cpe:2.3:adobe:acrobat_reader:***classical***](#) + [versions from \[Included: 15.006.20440\] up to \[Included: 15.006.20440\]](#)
- [cpe:2.3:adobe:acrobat_reader:***continuous***](#) + [versions from \[Included: 15.006.20440\] up to \[Included: 15.006.20440\]](#)

OR

- [cpe:2.3:adobe:acrobat_reader:***classical***](#)
- [cpe:2.3:adobe:acrobat_reader:***continuous***](#)

• [Derivative Vulnerable Software](#)

Are we missing a CVE here? Please let us know.

Change History

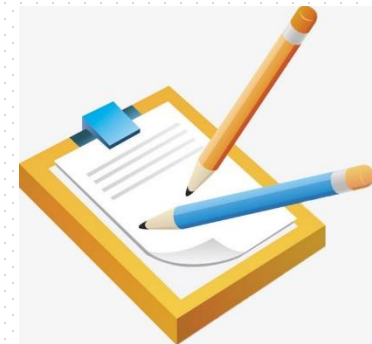
3 change records found [Show changes](#)

<https://nvd.nist.gov/vuln/search>

2. Vulnerabilidades

U.S. National Vulnerability Database (NVD):

- Ejercicio
 - Seleccionar las 2 o 3 aplicaciones de ordenador de uso personal más frecuente
 - E.g. Google Chrome, Adobe Reader, Microsoft Word, etc.
 - Buscar las vulnerabilidades asociadas, prestando especial atención a cuantas están categorizadas como de impacto alto

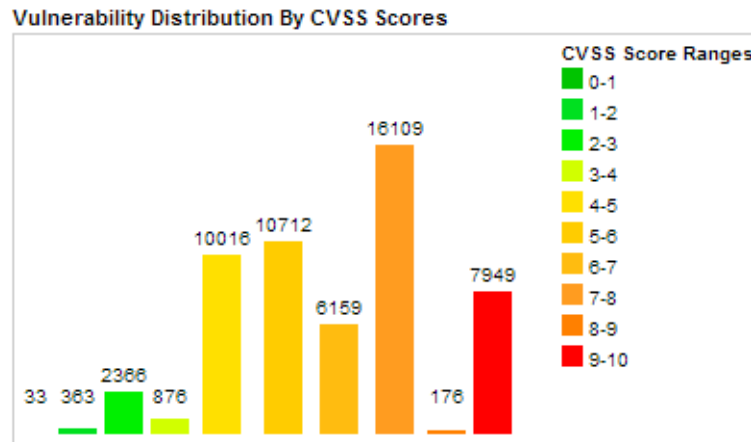


<https://nvd.nist.gov/vuln/search>

2. Vulnerabilidades

CVE Details

- Base de datos similar a NVD o CVE-mitre
- Facilita las búsquedas y genera informes de vulnerabilidades por vendedor, producto, versión o fecha





2. Vulnerabilidades

INCIBE-CERT

- Castellano
- Basado en la base de datos de NVD y CVE
- Incluye un boletín diario con las últimas vulnerabilidades detectadas

The screenshot displays the INCIBE-CERT website interface. At the top, there is a navigation bar with the INCIBE-CERT logo and a menu with items: Alerta, Incidentes, Servicios, Publicaciones, and Sobre INCIBE-CERT. A search icon is also present. Below the navigation bar, the breadcrumb trail reads: Inicio / Alerta Temprana / Vulnerabilidades / CVE-2019-0585. The main heading is "Vulnerabilidad en Microsoft Word (CVE-2019-0585)". The details section includes: Tipo: Validación incorrecta de entrada; Gravedad: Crítica (indicated by four red bars); Fecha publicación: 08/01/2019; Última modificación: 15/01/2019. The Descripción states: "Existe una vulnerabilidad de ejecución remota de código en el software de Microsoft Word cuando no gestiona correctamente objetos en la memoria. Esto también se conoce como 'Microsoft Word Remote Code Execution Vulnerability'. Esto afecta a Word, Microsoft Office, Microsoft Office Word Viewer, Office 365 ProPlus, Microsoft SharePoint, Microsoft Office Online Server, Microsoft Word y Microsoft SharePoint Server." The Impacto section is followed by the Vector de acceso: A través de red; Complejidad de Acceso: Media; Autenticación: No requerida para explotarla; and Tipo de impacto: Compromiso total de la integridad del sistema + Compromiso total de la confidencialidad del sistema + Compromiso total de la disponibilidad del sistema. The Productos y versiones vulnerables section lists: Microsoft Word Automation Services, Microsoft Word 2016, Microsoft Word 2013 Sp1, Microsoft Word 2013 Sp1, and Microsoft Word 2010 Sp2, with a link to "Show more versions". The Referencias a soluciones, herramientas e información section lists: 106392 (Origen: BID) and a link to the Microsoft security advisory (Origen: CONFIRM). At the bottom right, there is a red button labeled "Ir atrás".



2. Vulnerabilidades

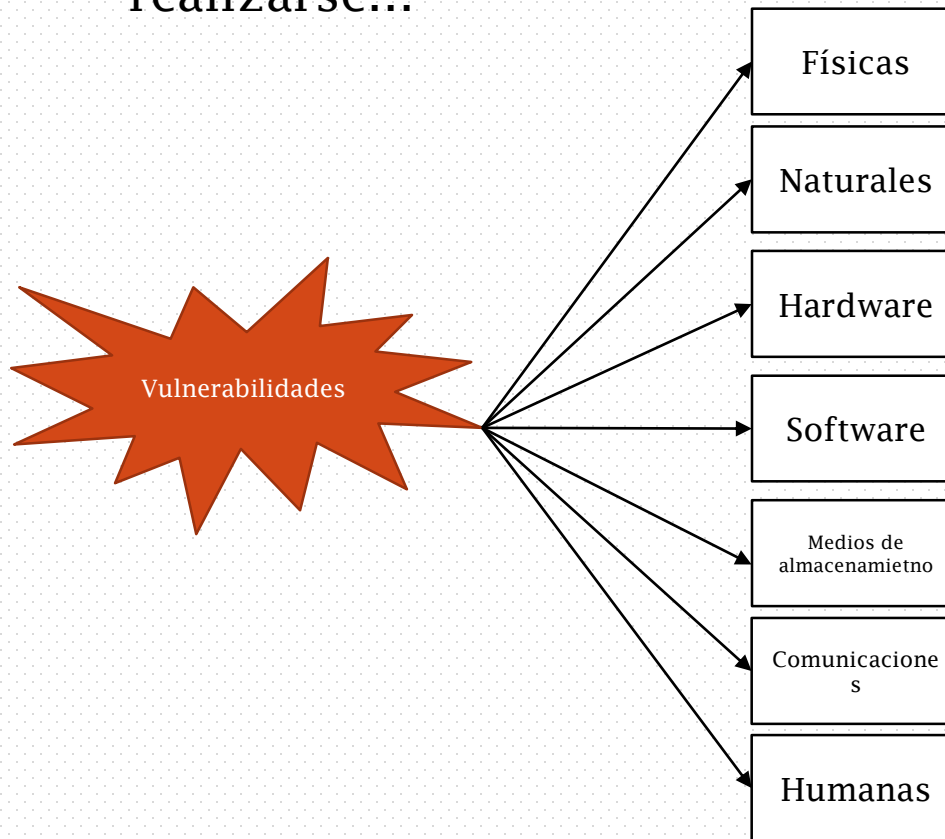
Escaneo de vulnerabilidades

- OpenVAS
 - OpenSource
 - Escaneo y gestión de vulnerabilidades
- Comodo HackerProof
- Nikto
 - Escaneo de aplicaciones web
- Nessus
- Microsoft Baseline Security Analyzer
 - Centrado en estado actualizaciones y configuraciones de seguridad del SO
 - Mantenido hasta versiones Windows 2012 server, aunque aun puede ser empleado
 - <https://www.microsoft.com/en-us/download/details.aspx?id=19892>
- Flexera - Producto Software Vulnerabilty Manager
- ...



2. Vulnerabilidades

Una posible clasificación, de las muchas que pueden realizarse...



2. Vulnerabilidades

- **Vulnerabilidades físicas**

- Relativas al lugar dónde se almacena físicamente la información (CPD, oficinas...)
- Robo de material, sabotaje eléctrico...
- Medidas a adoptar: personal de seguridad, cerraduras biométricas, registros de acceso, etc.

- **Vulnerabilidades naturales**

- Relativas a todas aquellas cuestiones naturales que pueden poner en riesgo los activos de una organización
 - Incendios, inundaciones, terremotos...
- Medidas a adoptar: sistemas de respaldo, políticas de copias de seguridad, sistemas de ventilación, fuentes de alimentación redundantes, etc.



2. Vulnerabilidades

- **Vulnerabilidades hardware**

- Hacen referencia a posibles defectos de fabricación, configuración o instalación del equipamiento informático (ordenadores, routers, ...)
- Medidas a adoptar: equipamiento redundante (sistemas RAID, fuentes de alimentación duplicadas...),

- **Vulnerabilidades software**

- Relativas a todos aquellos errores de configuración o instalación de programas en una organización que posibilitarían el acceso a usuarios, recursos o a información no autorizada.
- Medidas a adoptar: plantillas de configuración de equipos, actualización sistemas operativos, análisis periódico con antivirus, etc.



2. Vulnerabilidades

- **Vulnerabilidades de medios de almacenamiento**

- Podrían considerarse un subtipo de las vulnerabilidades hardware
- Hacen referencia a posibles defectos en los medios que se empleen para almacenar la información: discos duros, cd-roms, dvd, etc.
- Medidas a adoptar: políticas de backup, sistemas RAID, catalogación unidades extraíbles (pendrives, discos externos...), etc.

- **Vulnerabilidades de comunicación**

- Podrían considerarse un subtipo de las vulnerabilidades hardware
- Relativas a todos los incidentes que se puedan originar en el trayecto que recorra la información en una comunicación origen-destino: corte de conexiones, sniffing de datos...
- Medidas a adoptar: cifrado de información, uso de protocolos de transmisión seguros, etc.

2. Vulnerabilidades

- **Vulnerabilidades humanas**

- Desgraciadamente suelen ser las más habituales
- Hacen referencia a los daños que las personas puedan causar a la información o a los activos que la gestionen.
- Pueden ser de origen intencionado (vandalismo, estafas, fraude, robo, etc.) o de origen accidental (falta de formación, negligencia, descuido, olvido, etc.)
- Medidas a adoptar: planes de formación, concienciación del personal, etc.



2. Vulnerabilidades

Información complementaria

- Conceptos básicos sobre la seguridad de la información: SGSI
 - <https://www.youtube.com/watch?v=zV2sfyvfqik>
- ¿Qué son las amenazas, las vulnerabilidades y las contramedidas en Informática?
 - <https://www.youtube.com/watch?v=3zIDicLyfY0>



Cuestionario 2



3. Amenazas

- Posibilidad de violación de la seguridad, que existe cuando se da una circunstancia, capacidad, acción o evento que pudiera romper la seguridad y causar perjuicio (RFC 2828)
- Posible causa de un incidente no deseado, que puede resultar en daños a un sistema u organización (ISO 27000:2009)
- Es decir, una amenaza es un **peligro posible que podría hacer uso de una vulnerabilidad**
- Una amenaza representa la acción que tiende a causar un daño a los dispositivos o sistemas en donde se encuentra almacenada la información, atentando contra su confidencialidad, integridad y disponibilidad.
- Una analogía podría ser considerar una amenaza como la posesión por parte de un atacante de unas tenazas con las que podría cortar nuestra cadena de seguridad

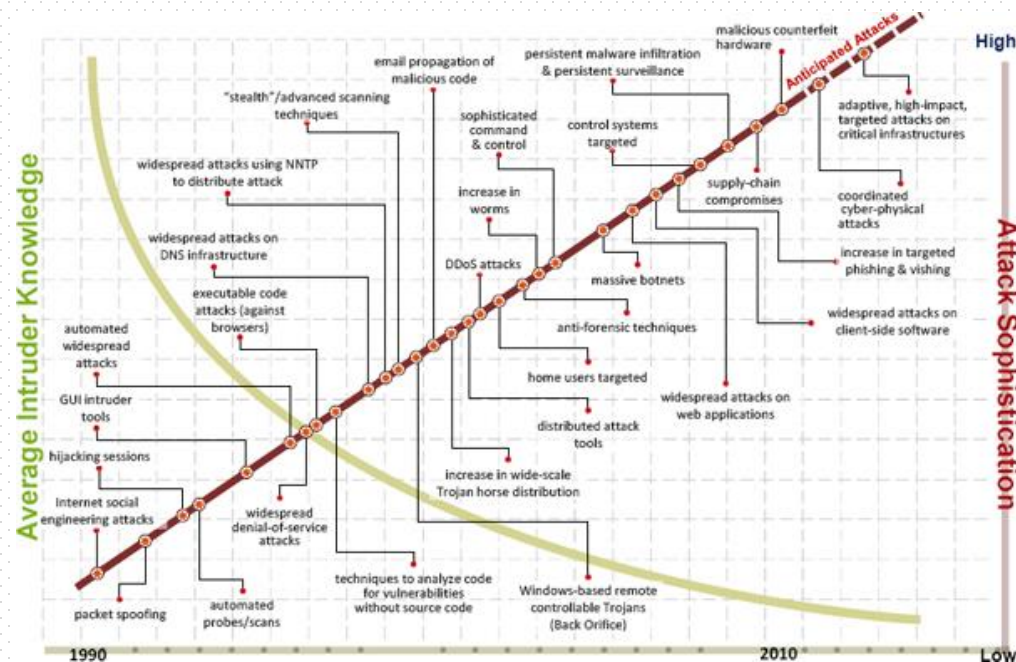


3. Amenazas

- Amenazas más habituales
 - Personal externo
 - Ataques que provienen de individuos que de manera intencionada o no, causan enormes pérdidas aprovechando alguna de las vulnerabilidades que los sistemas puedan presentar.
 - Aunque genéricamente se suele referir a ellos como hackers, existen diversos perfiles, en función del tipo de amenaza que representan:
 - Hacker: persona que vive para aprender y todo para él es un reto, es curioso y paciente, no se mete en el sistema para borrarlo o para vender lo que consiga, quiere aprender y satisfacer su curiosidad. Crea más no destruye.
 - Cracker: personas que rompen o vulneran algún sistema de seguridad. Los crackers pueden estar motivados por una multitud de razones, incluyendo fines de lucro, protesta, o por simple desafío personal
 - Phreaker: Phreaking es un término de argot acuñado para describir la actividad de una cultura de personas que estudian, experimentan o exploran sistemas de telecomunicaciones, tales como equipos y sistemas conectados a redes telefónicas públicas.
 - Lamer: individuos con ganas de hacer Hacking, pero que carecen de cualquier conocimiento. Generalmente reutiliza código o scripts de internet.

3. Amenazas

- Amenazas más habituales: lamer



- La gráfica no es nueva, pero sigue reflejando la situación a día de hoy: cada vez se requieren menos conocimientos por parte de los atacantes... pero cada vez se producen ataques más sofisticados y que producen un mayor daño. ¿Por qué? Pues porque “todo está en internet”



3. Amenazas

- Amenazas más habituales
 - **Ingeniería social:** Un atacante utiliza la interacción humana o habilidad social para obtener información comprometedoras acerca de una organización, de una persona o de un sistema de cómputo. El atacante hace todo lo posible para hacerse pasar por una persona modesta y respetable, por ejemplo, pretende ser un nuevo empleado, un técnico de reparación, un investigador, etc.
 - **Ingeniería social inversa:** El atacante demuestra de alguna manera que es capaz de brindar ayuda a los usuarios y estos lo llaman ante algún imprevisto, aprovechando la oportunidad para pedir la información necesaria y así solucionar el problema tanto del usuario como el propio.
 - **Trashing:** Generalmente, un usuario anota su login y password en un papelito y luego, cuando lo recuerda, lo arroja a la basura. El trashing puede ser físico (como el que se describió) o lógico, como analizar buffers de impresora y memoria bloques de discos, entre otros.
 - **Intrusos remunerados:** Es el grupo de atacantes de un sistema más peligroso aunque es el menos habitual en las redes normales ya que suele afectar más a las grandes empresas u organismos de defensa. Se trata de personas con gran experiencia en problemas de seguridad y con un amplio conocimiento del sistema, que son pagados por una tercera parte generalmente para robar secretos o simplemente dañar la imagen de la entidad afectada.
 - **Personal interno:** Son las amenazas al sistema, provenientes del personal del propio sistema informático, rara vez es tomado en cuenta porque se supone un ámbito de confianza muchas veces inexistente. Estos ataques son accidentes por desconocimiento o inexistencia de las normas básicas de seguridad; pero también pueden ser de tipo intencional
 - **Ex-Empleados:** Se trata de personas descontentas con la organización que aprovechan las debilidades de un sistema que conocen perfectamente.
 - Etc, etc, etc.



3. Amenazas

- **A priori, una vulnerabilidad y una amenaza están directamente relacionadas...**
- ... porque a fin de cuentas ambas son debilidades o peligros potenciales que tiene un sistema de información y ante las que se deberán tomar las medidas necesarias
- Existe un aspecto fundamental que diferencia a ambas...
 - **El conocimiento**
 - Una vulnerabilidad puede ser desconocida (aunque esté presente en el sistema), pero desde el mismo momento en el que se tiene constancia de sus existencia se convierte en una amenaza de la que deberíamos preocuparnos

3. Amenazas

- A priori, una vulnerabilidad y una amenaza están directamente relacionadas...





Cuestionario 3



UNIVERSIDADE DA CORUÑA

UD03

Amenazas y vulnerabilidades

Fase Presencial





4. Ataques

- Cualquier **acción** que comprometa la seguridad de la información de una organización (Stallings).
- Un asalto a la seguridad del sistema, derivado de una **amenaza** inteligente; es decir, un acto inteligente y deliberado (especialmente en el sentido de método o técnica) para eludir los servicios de seguridad y violar la política de seguridad de un sistema (RFC 2828).
- Siguiendo con la analogía, se trataría de una persona que posee unas tenazas con las que vemos que corta nuestra cadena de seguridad





4. Ataques

- Fuerza Bruta
- Cache Poisoning (Envenenamiento de Caché)
- DNS Poisoning (Envenenamiento de DNS)
- Cross-Site Scripting (XSS)
- Denial of Service (DoS)
- LDAP injection
- Man-in-the-middle
- Session hijacking attack
- SQL Injection
- ...

Más en: **<https://www.owasp.org/index.php/Category:Attack>**



4. Ataques

- Zero-day attack: explota una vulnerabilidad no conocida hasta el momento
 - Vulnerabilidad no conocida hasta el momento
 - El ataque ocurre en el "día cero" del aviso/conocimiento de la vulnerabilidad
 - Los desarrolladores han tenido cero días para parchear la vulnerabilidad

4. Ataques

Generalmente se diferencian entre dos tipos de ataques

- Ataques pasivos

Un **ataque pasivo** intenta conocer o hacer uso de información del sistema, pero no afecta a los recursos del mismo

- Ataques activos

Un **ataque activo** intenta alterar los recursos del sistema o afectar a su funcionamiento



4. Ataques

Ataques pasivos

- Un **ataque pasivo** intenta conocer o hacer uso de información del sistema, pero no afecta a los recursos del mismo
- Se dan en forma de escucha o de observación no autorizada de las transmisiones. El objetivo del oponente es obtener información que se esté transmitiendo
- ¿Qué implica esta manera de ataque?
 - Muy difíciles de detectar, ya que no implican alteraciones en los datos
 - Se debe poner más énfasis en la **prevención** que en la detección
 - Solución más ampliamente usada: **cifrado**

4. Ataques

Ataques activos

- Intentan alterar los recursos del sistema o afectar a su funcionamiento
 - Implican modificación del flujo de datos o la creación de un flujo falso
- Presentan características opuestas a los pasivos:
 - Son difíciles de prevenir por completo
 - El objetivo es **detectarlos** y recuperarse de ellos
 - La detección tiene efecto disuasivo -> contribuye a la prevención
- Se pueden dividir en cuatro categorías
 - Interrupción del servicio
 - Impiden el acceso a los usuarios legítimos a un servicio
 - Modificación mensajes
 - Altera cierta información del mensaje original (e.g. modificación del número de cuenta bancaria en una transferencia)
 - Repetición
 - Repiten un mensaje (eg. Envío de contraseñas, realización transferencias...)
 - Suplantación de identidad
 - Hacerse pasar por un origen/destino diferente al que se es en realidad

4. Ataques

- Zone-H (www.zone-h.org)
 - Página en la que se registran los ataques realizados con éxito a una página web (se incluye captura de pantalla a modo de “prueba de verdad”)
 - Generalmente se trata de ataques que cambian la *página de entrada legal* de una web.





Cuestionario 4

5. OWASP

- Open Web Application Application Security Project
 - Organización sin ánimo de lucro
 - Todos los miembros son voluntarios
 - Todo el trabajo es donado por los patrocinadores
 - Ojetivo: proporcionar recursos gratuitos para la comunidad
 - Publicaciones, artículos, normas
 - Software de Testeo y Capacitación
 - Capítulos locales & Listas de correo
 - Su aporte más conocido es el OWASP Top Ten Report
 - Informe que detalla los 10 riesgos más comunes en aplicaciones web (las más habituales hoy en día)
 - Incluye aspectos como probabilidad de aparición (vulnerabilidades), probabilidad de ser aprovechado (amenaza) o daño causado (tras un ataque)

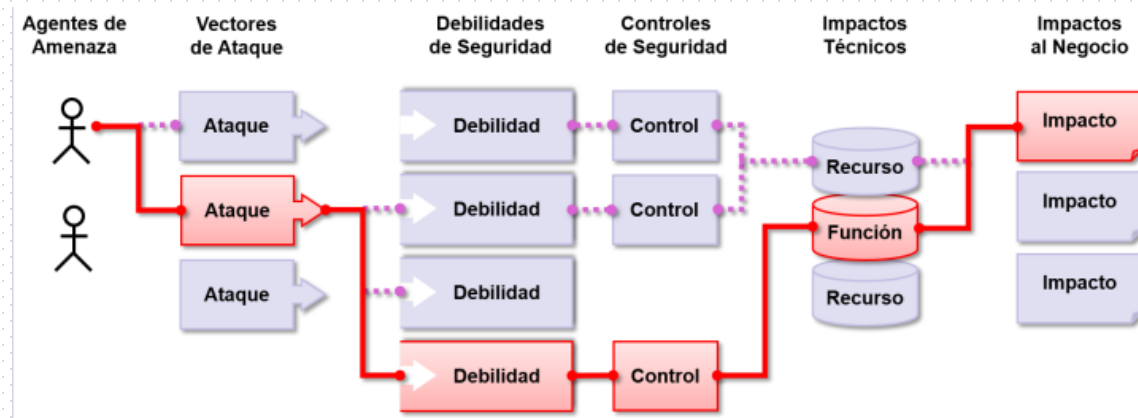


5. OWASP

- OWASP Top 10 Report
- Informe con los **10 riesgos** de seguridad más críticos (y comunes) en aplicaciones web
 - Objetivo: Análisis a Nivel Ejecutivo
- Para cada riesgo proporciona:
 - Descripción
 - Ejemplo de vulnerabilidad
 - Ejemplo de Ataque
 - Guía de cómo evitarlo
 - Referencias
- Versiones
 - 2003, 2004, 2007, 2010
 - 2017 (última versión disponible. Accesible también en castellano)
 - <https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf>

5. OWASP

- Determinación del riesgo
 - Existen múltiples vías de entrada al sistema que pueden ocasionar daños al negocio/organización
 - Cada una de ellas representa un riesgo al que debe prestarse atención



- En resumen:
 $\text{riesgo} = \text{probabilidad de ocurrencia} \times \text{impacto causado}$



5. OWASP

- Ejemplo informe detallado acerca de un riesgo (Injection)

T10 OWASP Top 10 2017
Riesgos en Seguridad de Aplicaciones

A1:2017
Inyección

Las fallas de inyección, como SQL, NoSQL, OS o LDAP ocurren cuando se envían datos no confiables a un intérprete, como parte de un comando o consulta. Los datos dañinos del atacante pueden engañar al intérprete para que ejecute comandos involuntarios o acceda a los datos sin la debida autorización.


5. OWASP

- Ejemplo informe detallado acerca de un riesgo (Injection)

A1
:2017

Inyección

7



App. Específica	Explotabilidad: 3	Prevalencia: 2	Detectabilidad: 3	Técnico: 3	¿Negocio?
<p>Casi cualquier fuente de datos puede ser un vector de inyección: variables de entorno, parámetros, servicios web externos e internos, y todo tipo de usuarios. Los defectos de inyección ocurren cuando un atacante puede enviar información dañina a un intérprete.</p>	<p>Estos defectos son muy comunes, particularmente en código heredado. Las vulnerabilidades de inyección se encuentran a menudo en consultas SQL, NoSQL, LDAP, XPath, comandos del SO, analizadores XML, encabezados SMTP, lenguajes de expresión, parámetros y consultas ORM.</p> <p>Los errores de inyección son fáciles de descubrir al examinar el código y los escáneres y fuzzers ayudan a encontrarlos.</p>			<p>Una inyección puede causar divulgación, pérdida o corrupción de información, pérdida de auditabilidad, o denegación de acceso.</p> <p>El impacto al negocio depende de las necesidades de la aplicación y de los datos.</p>	

¿La aplicación es vulnerable?

Una aplicación es vulnerable a ataques de este tipo cuando:

- Los datos suministrados por el usuario no son validados, filtrados o sanitizados por la aplicación.
- Se invocan consultas dinámicas o no parametrizadas, sin codificar los parámetros de forma acorde al contexto.
- Se utilizan datos dañinos dentro de los parámetros de búsqueda en consultas *Object-Relational Mapping (ORM)*, para extraer registros adicionales sensibles.
- Los datos dañinos se usan directamente o se concatenan, de modo que el SQL o comando resultante contiene datos y estructuras con consultas dinámicas, comandos o procedimientos almacenados.

Algunas de las inyecciones más comunes son SQL, NoSQL, comandos de SO, *Object-Relational Mapping (ORM)*, LDAP, expresiones de lenguaje u *Object Graph Navigation Library (OGNL)*. El concepto es idéntico entre todos los intérpretes. La revisión del código fuente es el mejor método para detectar si las aplicaciones son vulnerables a inyecciones, seguido de cerca por pruebas automatizadas de todos los parámetros, encabezados, URL, cookies, JSON, SOAP y entradas de datos XML.

Las organizaciones pueden incluir herramientas de análisis estático ([SAST](#)) y pruebas dinámicas ([DAST](#)) para identificar errores de inyecciones recientemente introducidas y antes del despliegue de la aplicación en producción.

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 herramienta 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.



5. OWASP

- Ejemplo informe detallado acerca de un riesgo (Injection)

Ejemplos de escenarios de ataque

Escenario #1: la aplicación utiliza datos no confiables en la construcción del siguiente comando SQL vulnerable:

```
String query = "SELECT * FROM accounts WHERE custID=" +  
request.getParameter("id") + "";
```

Escenario #2: la confianza total de una aplicación en su *framework* puede resultar en consultas que aún son vulnerables a inyección, por ejemplo, *Hibernate Query Language (HQL)*:

```
Query HQLQuery = session.createQuery("FROM accounts WHERE  
custID=" + request.getParameter("id") + "");
```

En ambos casos, al atacante puede modificar el parámetro "id" en su navegador para enviar: ' or '1'=1. Por ejemplo:

```
http://example.com/app/accountView?id=' or '1'=1
```

Esto cambia el significado de ambas consultas, devolviendo todos los registros de la tabla "accounts". Ataques más peligrosos podrían modificar los datos o incluso invocar procedimientos almacenados.

Referencias

OWASP

- [OWASP Proactive Controls: Parameterize Queries](#)
- [OWASP ASVS: V5 Input Validation and Encoding](#)
- [OWASP Testing Guide: SQL Injection, Command Injection, ORM Injection](#)
- [OWASP Cheat Sheet: Injection Prevention](#)
- [OWASP Cheat Sheet: SQL Injection Prevention](#)
- [OWASP Cheat Sheet: Injection Prevention in Java](#)
- [OWASP Cheat Sheet: Query Parameterization](#)
- [OWASP Automated Threats to Web Applications – OAT-014](#)

Externos

- [CWE-77: Command Injection](#)
- [CWE-89: SQL Injection](#)
- [CWE-564: Hibernate Injection](#)
- [CWE-917: Expression Language Injection](#)
- [PortSwigger: Server-side template injection](#)



5. OWASP

- OWASP ofrece también aplicaciones web de ejemplo en las que poder explotar los diferentes riesgos documentados
 - E.G. Bricks
 - Permite explotar riesgos típicos en páginas de login, de subida de archivos o de visualización de contenidos
 - Puede descargarse para su ejecución o modificación
 - https://www.owasp.org/index.php/OWASP_Bricks
 - Documentación y ejemplos disponibles en:
 - <https://sechow.com/bricks/docs/index.html>



5. OWASP

- Ejercicio: SQL-Injection
 - Simulación de ataques de SQL-Injection
 - Ejecución aplicación web Bricks
 - Requisitos: Apache + MySQL + PHP
 - Estas aplicaciones pueden instalarse de forma conjunta y portable, por ejemplo, con uWAMP
- Inyección Manual
 - Páginas de login:
 - <https://sechow.com/bricks/docs/login-1.html>
 - Páginas de contenido:
 - <https://sechow.com/bricks/docs/content-page-1.html>
- Inyección automatizada:
 - Havij



5. OWASP

- Información complementaria
 - Resumen: Amenaza, riesgo y vulnerabilidad
 - <https://www.youtube.com/watch?v=9hJ4fgfePfg>
 - Instalación de owasp bricks
 - <https://www.youtube.com/watch?v=Uy1wpjT-uaM>

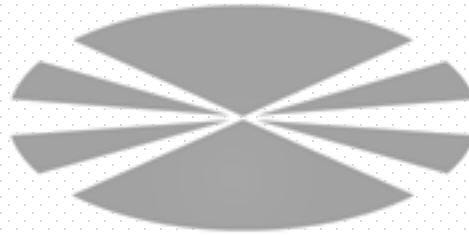
6. Contramedidas

- Acciones que se toman para reducir las amenazas y mitigar los efectos de los ataques
 - Deberán aplicarse contramedidas genéricas y específicas
 - Deberán protegerse todos los niveles del sistema, siendo múltiples las alternativas en cada uno de los niveles.





Cuestionario 5



UNIVERSIDADE DA CORUÑA

Profesor

Marcos Gestal Pose

mgestal@udc.es

<http://sabia.tic.udc.es/mgestal>