



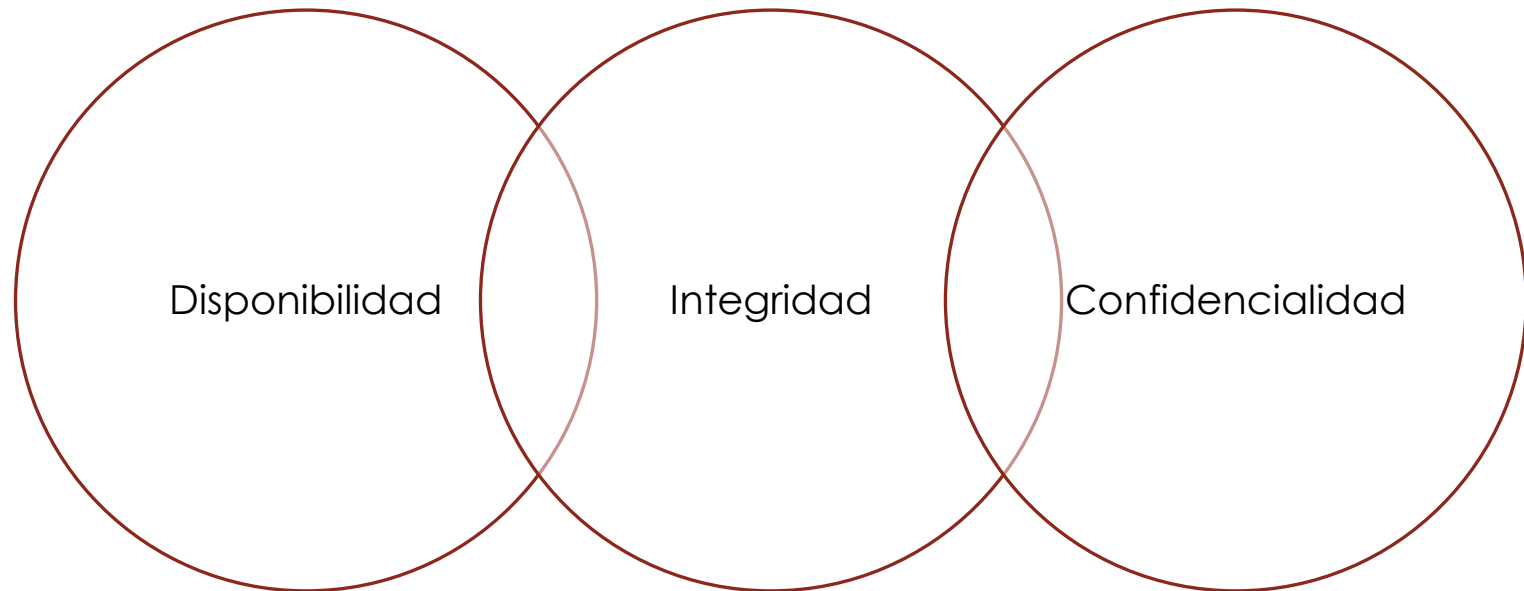
Unidad 3: ¿QUÉ ES LA CIBERSEGURIDAD?

BLOQUE I - Los fundamentos
de la Informática y
de la Seguridad

CONTENIDOS

1. Los pilares de la ciberseguridad.
2. Conceptos de riesgo, amenaza y vulnerabilidad.
3. Incidentes de seguridad.
4. Arquitecturas y principios de ciberseguridad.

1. Los pilares de la ciberseguridad



1. Los pilares de la ciberseguridad

- La disponibilidad: Siempre que un usuario autorizado quiera tener acceso o utilizar un activo, tendrá la posibilidad de hacerlo.
- La integridad: Los activos no pueden ser alterados o modificados por personas no autorizadas.
- La confidencialidad: Este pilar sí que tiene que ver con la información y se refiere a su privacidad, sólo deben tener acceso a ella las personas autorizadas.

1. Los pilares de la ciberseguridad

- En muchos casos se añaden otros dos aspectos básicos:
 - Control de acceso: Se trata de prevenir el uso no autorizado (del tipo que sea) de un activo o recurso.
 - No repudio: Se trata de prevenir que un emisor niegue su participación en una comunicación.

1. Los pilares de la ciberseguridad

- Pregunta: ¿Cuál de ellos es el más importante? Depende del contexto.



2. Conceptos de riesgo, amenaza y vulnerabilidad

- El riesgo suele definirse como la probabilidad de que ocurra un incidente de seguridad.
 - No sólo tiene que ver con la probabilidad.



Asignatura completa: **Análisis y gestión del riesgo**, en cuarto curso del Grado

2. Conceptos de riesgo, amenaza y vulnerabilidad

- La amenaza, por otro lado, no es más que una acción que podría tener un potencial efecto negativo sobre un activo.
 - Las amenazas pueden afectar a la disponibilidad, a la confidencialidad o la integridad.
 - Una amenaza por sí misma no provoca un daño.
 - Es necesario que exista una debilidad o fallo en el sistema que permita que se materialice.

2. Conceptos de riesgo, amenaza y vulnerabilidad

- Estas debilidades, fallos o “agujeros” son las vulnerabilidades, que pueden ser de diferente naturaleza:

Diseño

Fabricante/Comunidad/
Desarrollador

Arquitectura y configuración

Software

Hardware

Comunicaciones

Estándares de uso/Procedimientos

Usuario

Administrador

2. Conceptos de riesgo, amenaza y vulnerabilidad



Asignaturas completas: **Técnicas de Hacking y Malware y amenazas dirigidas** en segundo y tercer curso del Grado



Asignaturas completas: **Auditoría y Pentesting**, en cuarto curso del Grado

2. Conceptos de riesgo, amenaza y vulnerabilidad

- Existen diferentes bases de datos de vulnerabilidades (casi siempre, de diseño y que afectan a software).
 - Cada gobierno, por ejemplo, suele manejar la suya (aunque sólo sea por el idioma y por información específica que pueda interesar en cada contexto dependiendo de legislación nacional, etc.).
 - También los fabricantes de software mantienen las suyas, relativas a sus boletines de seguridad y centrándose en las de sus propios productos.
 - Además suelen existir bases de datos verticales o sectoriales, con las vulnerabilidades que afectan de manera específica a un sector de actividad.
- Pero el hito importante en el ciclo de vida de la vulnerabilidad suele ser la asignación definitiva del CVE-ID y su publicación en la lista CVE.

Common Vulnerabilities and Exposures
The Standard for Information Security Vulnerability Names

New CVE-ID Format as of January 1, 2014 — [learn more](#)

TOTAL CVEs: 61669

About CVE
Terminology
Documents
FAQs

CVE List
CVE-ID Syntax Change
About CVE Identifiers
Search CVE
Search NVD
Updates & RSS Feeds
Request a CVE-ID

CVE In Use
CVE-Compatible Products
NVD for CVE Fix
Information
CVE Numbering
Authorities

News & Events
Calendar
Free Newsletter

Community
CVE Editorial Board
Sponsor
Contact Us

Search the Site
Site Map

CVE® International in scope and free for public use, CVE is a dictionary of publicly known information security vulnerabilities and exposures. CVE's common identifiers enable data exchange between security products and provide a baseline index point for evaluating coverage of tools and services.

Widespread Use of CVE

- ▲ [Vulnerability Management](#)
- ▲ [Patch Management](#)
- ▲ [Vulnerability Alerting](#)
- ▲ [Intrusion Detection](#)
- ▲ [Security Content Automation Protocol \(SCAP\)](#)
- ▲ [NVD \(National Vulnerability Database\)](#)
- ▲ [US-CERT Bulletins](#)
- ▲ [CVE Numbering Authorities \(CNAAs\)](#)
- ▲ [Recommendation ITU-T X.1520 Common Vulnerabilities and Exposures \(CVE\), ITU-T CYBEX Series](#)

Focus On
Technical Guidance and Test Data for the New CVE-ID Syntax
Technical Guidance for Handling the New CVE-ID Syntax is now available on the CVE Web site. As of January 1, 2014, the format for CVE-IDs changed from 4 fixed digits to arbitrary digits in CVE-IDs. This new [resource](#) on the CVE Web site provides technical guidance and test data for developers and consumers for tools, web sites, and other capabilities that use [CVE Identifiers \(CVE-IDs\)](#), including the following: considerations for input and output formats, considerations for extraction or parsing, extraction and conversion methods for CVE-IDs, an example conversion algorithm for incoming IDs, and [CVE-ID Test Data for Implementers](#) available for download in a ZIP file.

Feedback about this guidance, and/or the test data, is welcome at cve-id-change@mitre.org.

Latest News
CVE, CWE, and CAPEC Are Main Topics of Article about the "Heartbleed" Bug on MITRE's Cybersecurity Blog
CVE Identifier "CVE-2014-0160" Cited in Numerous Security Advisories and News
Media References about the Heartbleed Vulnerability
CVE and CWE Cited in White Paper about the Heartbleed Vulnerability
CVE Mentioned in Preface of March/April 2014 Issue of *Crosstalk: The Journal of Defense Software Engineering*
CVE and CWE Mentioned in Article about Mitigating Risks of Counterfeit and Tainted Components in March/April 2014 Issue of *Crosstalk*
1 Product from Altex-Soft Now Registered as Officially "CVE-Compatible"

More News »

Page Last Updated: April 30, 2014

MITRE
Use of the Common Vulnerabilities and Exposures List and the associated references from this Web site are subject to the [Terms of Use](#). For more information, please email cve@mitre.org.
CVE is co-sponsored by the office of [Cybersecurity and Communications](#) at the U.S. Department of Homeland Security. Copyright © 1999-2014, The MITRE Corporation. CVE and the CVE logo are registered trademarks and CVE-Compatible is a trademark of The MITRE Corporation. This Web site is sponsored and managed by The MITRE Corporation to enable stakeholder collaboration.

Site Map
Privacy policy
Terms of use
Contact us

Member of
Making
Security
Measurable™



Otras dos bases de datos muy útiles y que están relacionadas con ésta son el CWE y el CAPEC, ve echando un vistazo... Por cierto ¿cuál es la diferencia entre vulnerabilidad y debilidad?

IC, Beltrán 2022-2023

2. Conceptos de riesgo, amenaza y vulnerabilidad

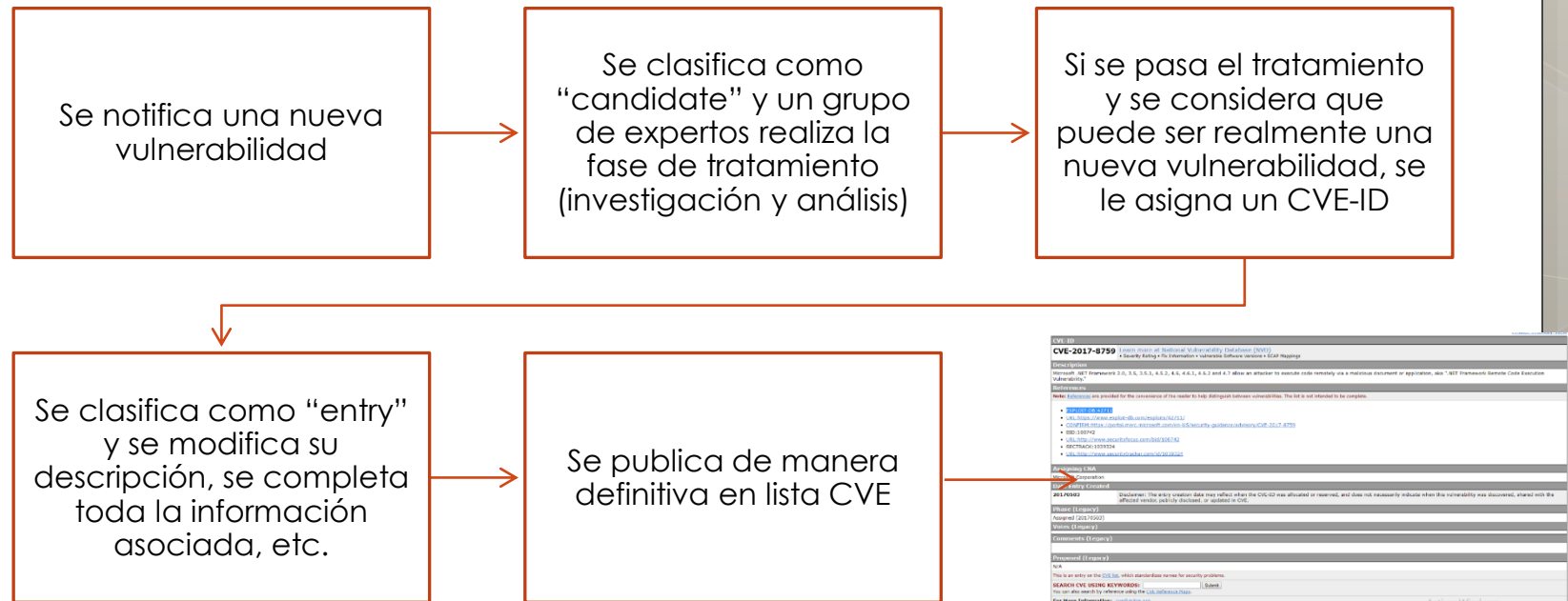
CVE-2013-7518

Siglas de Common Vulnerabilities and Exposures	Año de registro	Numero de cuatro cifras asignado a la vulnerabilidad
---	--------------------	--

- Desde el año 2014 se contempla utilizar más dígitos para el código de la vulnerabilidad (por si se detectaran más de 9999 en un año):

CVE-2014-1234...N

2. Conceptos de riesgo, amenaza y vulnerabilidad



2. Conceptos de riesgo, amenaza y vulnerabilidad

- Para que el CVE publique una nueva vulnerabilidad, debe poderse comprobar que:
 - Permite a un atacante ejecutar comandos como otro usuario.
 - Permite a un atacante acceder a datos violando las restricciones de control de acceso específicas para dichos datos.
 - Permite a un atacante suplantar a otra entidad.
 - Permite a un atacante llevar a cabo una denegación de servicio.

2. Conceptos de riesgo, amenaza y vulnerabilidad

- La organización internacional FIRST ha propuesto y gestiona y mantiene el CVSS (Common Vulnerability Scoring System), un sistema de valoración de vulnerabilidades creado como un método estándar para determinar la criticidad de las vulnerabilidades desde diferentes puntos de vista y poder clasificarlas.
 - Base, Temporal y Environmental metrics.

CVE Details

The ultimate security vulnerability datasource

(e.g.: CVE-2009

Vulnerabilit

[Log In](#) [Register](#) [Reset Password](#) [Activate Account](#)

[Home](#)

Browse :

- [Vendors](#)
- [Products](#)
- [Vulnerabilities By Date](#)
- [Vulnerabilities By Type](#)

Reports :

- [CVSS Score Report](#)
- [CVSS Score Distribution](#)

Search :

- [Vendor Search](#)
- [Product Search](#)
- [Version Search](#)
- [Vulnerability Search](#)
- [By Microsoft References](#)

Top 50 :

- [Vendors](#)
- [Vendor Cvss Scores](#)
- [Products](#)
- [Product Cvss Scores](#)
- [Versions](#)

Other :

- [Microsoft Bulletins](#)
- [Bugtraq Entries](#)
- [CWE Definitions](#)
- [About & Contact](#)
- [Feedback](#)
- [CVE Help](#)
- [FAQ](#)
- [Articles](#)

External Links :

- [NVD Website](#)
- [CWE Web Site](#)

You can generate a custom RSS feed or an embedable vulnerability list widget or a json API call url.

Selected vulnerability types are OR'ed. If you don't select any criteria "all" CVE entries will be returned

- | | | |
|--|--|---|
| <input type="checkbox"/> Vulnerabilities with exploits | <input type="checkbox"/> Code execution | <input type="checkbox"/> Overflows |
| <input type="checkbox"/> Cross Site Request Forgery | <input type="checkbox"/> File inclusion | <input type="checkbox"/> Gain privilege |
| <input type="checkbox"/> Sql injection | <input type="checkbox"/> Cross site scripting | <input type="checkbox"/> Directory trav |
| <input type="checkbox"/> Memory corruption | <input type="checkbox"/> Http response splitting | <input type="checkbox"/> Bypass somet |
| <input type="checkbox"/> Gain information | <input type="checkbox"/> Denial of service | |

Order By:

CVSS score >= :

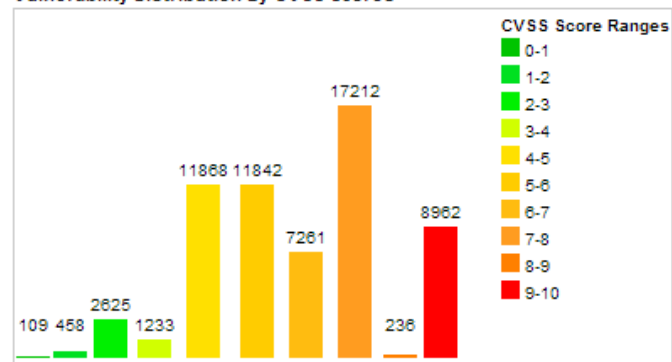
Current CVSS Score Distribution For All Vulnerabilities

Distribution of all vulnerabilities by CVSS Scores

CVSS Score	Number Of Vulnerabilities	Percentage
0-1	109	0.20
1-2	458	0.70
2-3	2625	4.20
3-4	1233	2.00
4-5	11868	19.20
5-6	11842	19.20
6-7	7261	11.70
7-8	17212	27.80
8-9	236	0.40
9-10	8962	14.50
Total	61806	

Weighted Average CVSS Score: 6.9

Vulnerability Distribution By CVSS Scores



2. Conceptos de riesgo, amenaza y vulnerabilidad

- Hace tiempo que no se confía en la seguridad por oscuridad.
 - Es decir, en no difundir información sobre las vulnerabilidades esperando con ello que los agentes de amenaza (los potenciales atacantes) no tengan información para buscarlas y explotarlas.
- Al contrario, se trabaja sobre las bases de la transparencia, la compartición de información, etc.
- Pero existe un debate, todavía sin resolver, acerca de la mejor manera de hacer pública una vulnerabilidad.
 - Ya que además es muy complicado estandarizar, se dan muchas situaciones diferentes: responsible disclosure, full disclosure, coordinated disclosure.

2. Conceptos de riesgo, amenaza y vulnerabilidad

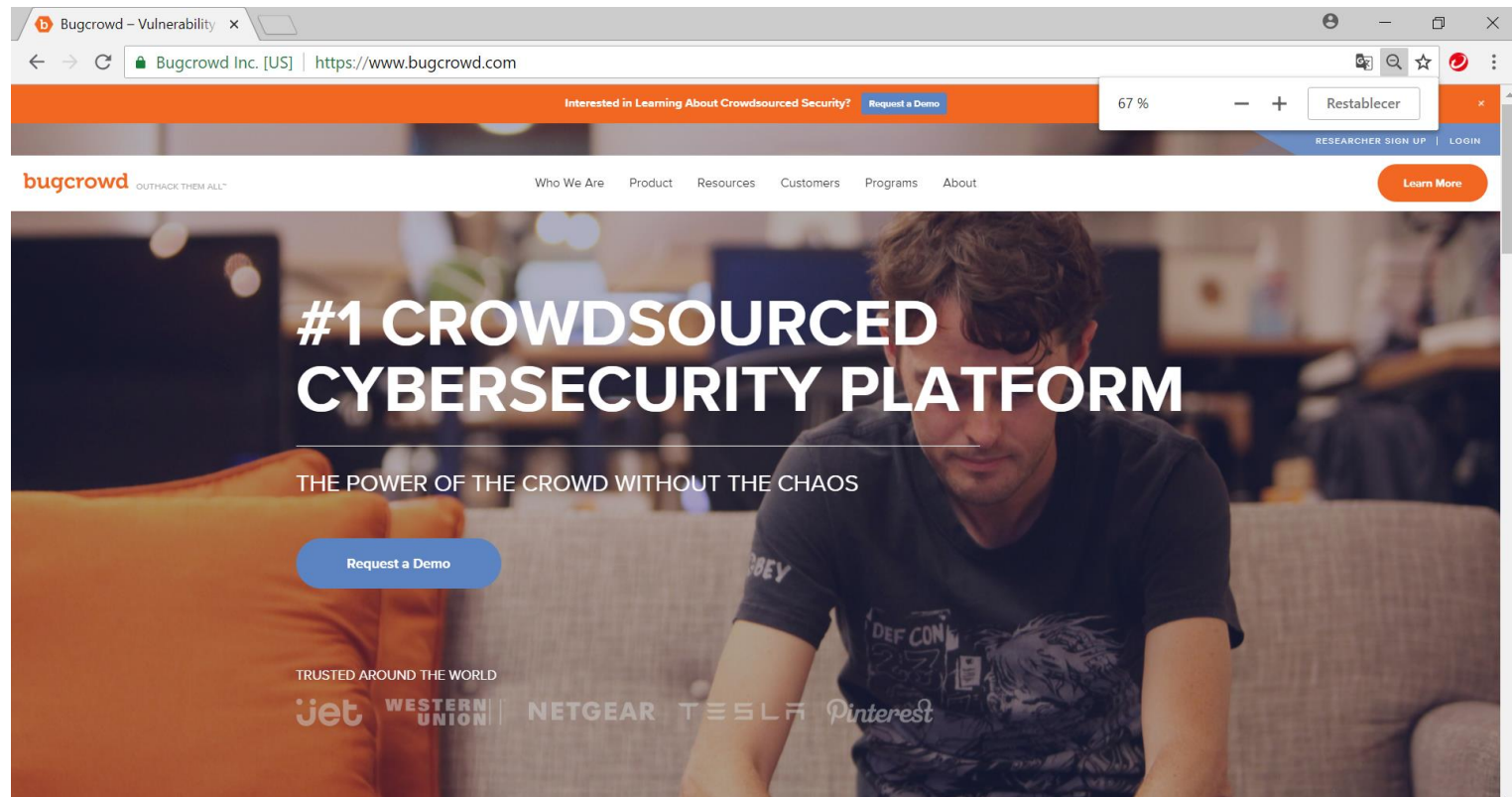
- En relación con esto último, se han hecho muy populares los programas de Bug Bounty.
- En estos programas un fabricante de software o proveedor de servicios lanza una campaña en la que recompensa a los investigadores capaces de encontrar bugs en sus productos y servicios.
- Fechas concretas, productos y servicios específicos, tipo de vulnerabilidad muy acotado.



2. Conceptos de riesgo, amenaza y vulnerabilidad

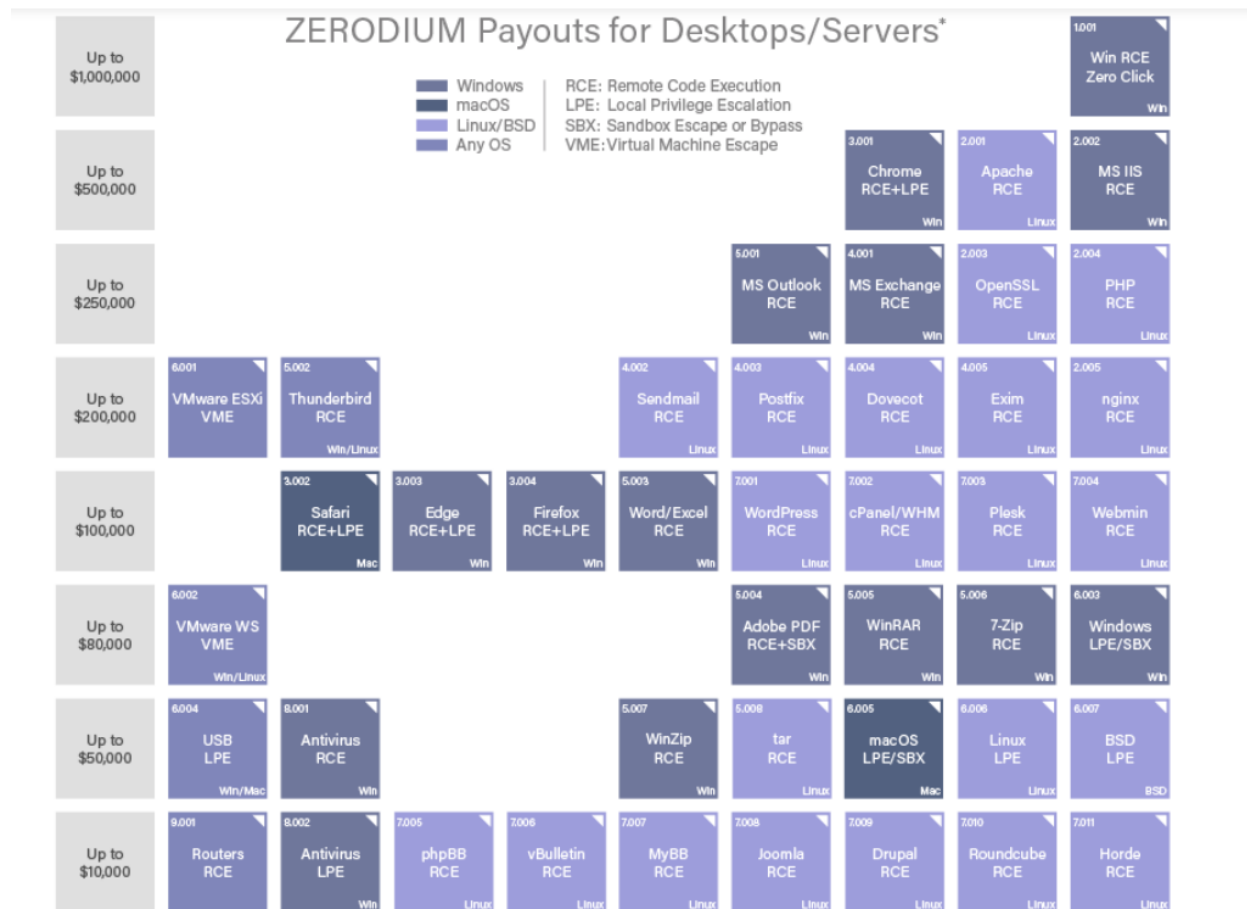


2. Conceptos de riesgo, amenaza y vulnerabilidad



The screenshot shows the Bugcrowd website homepage. The browser address bar displays "Bugcrowd Inc. [US] | https://www.bugcrowd.com". The page features a navigation menu with links for "Who We Are", "Product", "Resources", "Customers", "Programs", and "About", along with a "Learn More" button. The main content area has a large heading: "#1 CROWDSOURCED CYBERSECURITY PLATFORM" and a sub-heading: "THE POWER OF THE CROWD WITHOUT THE CHAOS". A "Request a Demo" button is prominently displayed. Below this, it states "TRUSTED AROUND THE WORLD" and lists logos for Jet, Western Union, Netgear, Tesla, and Pinterest. The background image shows a man sitting on a couch, looking at a laptop.

2. Conceptos de riesgo, amenaza y vulnerabilidad



* All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.

2019/01 © zerodium.com

-2023

2. Conceptos de riesgo, amenaza y vulnerabilidad

- Si echas un vistazo a la página web de Zerodium verás que hablan de “exploits”, es lo que compran.
 - Es un concepto que también ha aparecido en las bases de datos de vulnerabilidades que hemos estudiado, lo habrás visto en algunas de las fichas de vulnerabilidad.
- Un exploit no es más que el código que permite explotar una vulnerabilidad.
- De nuevo existe un debate acerca de su publicación: arma de doble filo.

2. Conceptos de riesgo, amenaza y vulnerabilidad

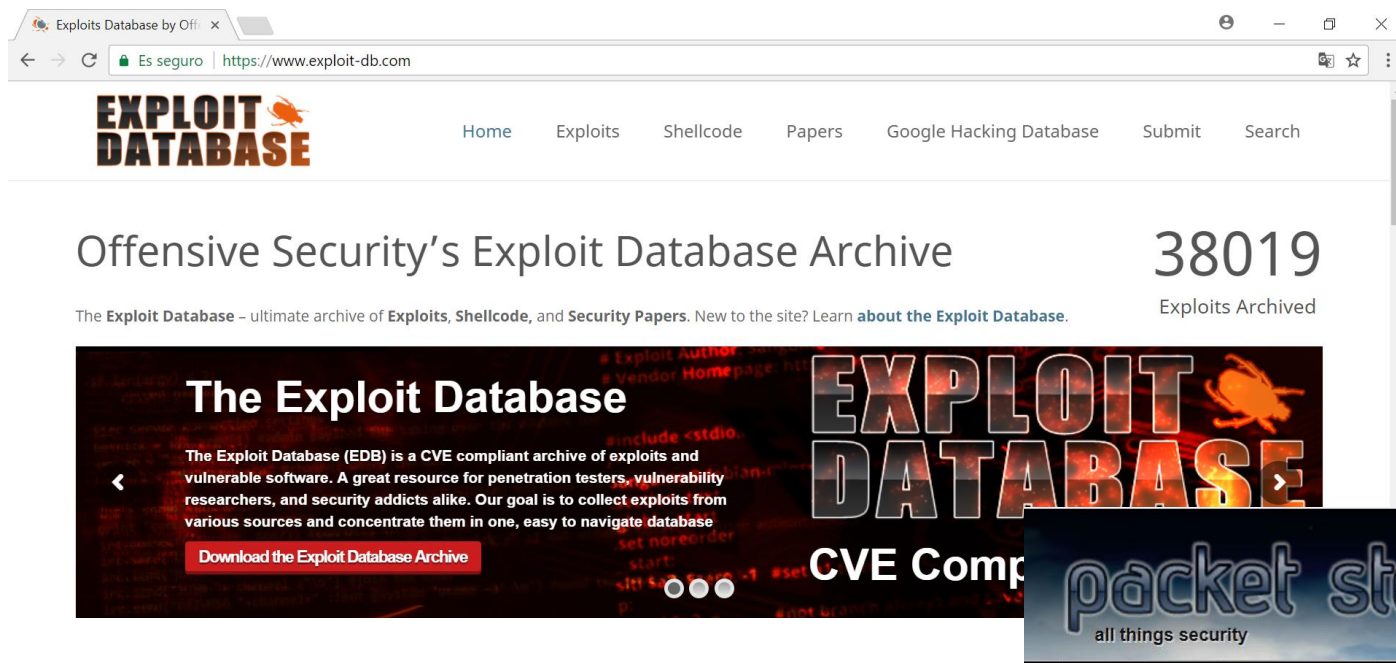
Tiempo de reacción

- Tiempo que transcurre desde que el fabricante de software conoce la vulnerabilidad hasta que genera un parche o actualización que la mitiga.

Día cero

- Día en que una vulnerabilidad se convierte en conocida para el público general.
- El tiempo de reacción se suele medir desde este día.

2. Conceptos de riesgo, amenaza y vulnerabilidad



The screenshot shows the Exploit Database website. The browser address bar displays "Es seguro | https://www.exploit-db.com". The navigation menu includes "Home", "Exploits", "Shellcode", "Papers", "Google Hacking Database", "Submit", and "Search". The main content area features the title "Offensive Security's Exploit Database Archive" with a count of "38019 Exploits Archived". Below this is a banner for "The Exploit Database" with a description: "The Exploit Database (EDB) is a CVE compliant archive of exploits and vulnerable software. A great resource for penetration testers, vulnerability researchers, and security addicts alike. Our goal is to collect exploits from various sources and concentrate them in one, easy to navigate database". A button labeled "Download the Exploit Database Archive" is visible. The banner also includes the text "CVE Comp" and "packet storm all things security".

2. Conceptos de riesgo, amenaza y vulnerabilidad

- Cuidado con distinguir bien el concepto de Exploit del concepto de Payload.
- El exploit explota la vulnerabilidad, aprovechando el error o debilidad de un código.
 - Muchos programados en C o Python.
- El payload no es más que el código que el exploit consigue que se ejecute en el activo víctima del ataque.
 - Muchos directamente programados en ensamblador.
- Por lo tanto, un mismo payload puede ser utilizado por varios exploits y un exploit puede utilizar distintos payloads dependiendo del objetivo del atacante al explotar la vulnerabilidad.

3. Incidentes de seguridad

- Además de los equipos que se encargan de mantener los listados y las bases de datos que acabamos de estudiar, el personal más estrechamente relacionado con los procesos de análisis y gestión de vulnerabilidades es el que forma los CERT (Computer Emergency Response Team) ó CSIRT (Computer Security Incident Response Team).



Asignatura completa: **Inteligencia de la Seguridad**, en cuarto curso del Grado

3. Incidentes de seguridad

- Hoy en día todas las grandes organizaciones cuentan con un equipo de estas características, un CSIRT.
- Y si no pueden crearlo con personal interno, lo externalizan o sub-contratan a otra organización.
- El término CERT suele utilizarse para el centro de referencia, casi siempre externo.



3. Incidentes de seguridad

- CERTs gubernamentales en España, de referencia:



<https://www.ccn-cert.cni.es/>



<https://www.certs.es/>

INCIDENTE

30

ATAQUE

EVENTO

Atacante

Herramienta

Vulnerabilidad

Acción

Target

Resultado

Objetivos

Hacker

Sniffer

Diseño

Espiar

Cuentas de usuario

Brecha de datos

Reto, aprendizaje o renombre

Script kiddie

Scanner

Escanear

Datos

Denegación de servicio

Beneficio político

Hacker

Ataque físico

Arquitectura y configuración

Interrumpir

Procesos

Escalado de privilegios

Beneficio financiero

Terrorista

Kit de exploits

Estándares de uso y procedimientos

Modificar

Sistemas

Destrucción de datos o sistemas

Daño a la reputación

Criminal

Comandos

Inundar

Redes

Espía

Cracker

Suplantar

Servicios

Kit de malware

Secuestrar

Aplicaciones

Injectar

IC, Beltrán 2022-2023

3. Incidentes de seguridad

- ¿De qué se encarga un CSIRT?
 - Estar al día en las nuevas vulnerabilidades y estrategias de ataque empleadas por los atacantes.
 - Realizar/posibilitar auditorías de sistemas y redes.
 - Analizar y desarrollar nuevas tecnologías y soluciones para minimizar las vulnerabilidades.
 - Revisar, perfeccionar y actualizar continuamente los estándares, procedimientos y guías.
 - Ser punto central de comunicación, tanto para recibir los informes de incidentes de seguridad, como para difundir información esencial sobre los incidentes a las entidades correspondientes.
 - Documentar y catalogar los incidentes de seguridad producidos.
 - Obtener lecciones aprendidas.

3. Incidentes de seguridad

Realizar una
evaluación inicial

Contener los
daños con una
respuesta inicial y
minimizar el riesgo

Reunir y proteger
pruebas forenses

Implementar una
solución temporal

Comunicar dentro
y fuera

Consultar/notificar
a las autoridades

Implementar
soluciones
permanentes

Determinar la
repercusión
financiera en el
negocio

4. Arquitecturas y principios de ciberseguridad



4. Arquitecturas y principios de ciberseguridad



4. Arquitecturas y principios de ciberseguridad

- La Seguridad Informática es un campo cada vez más amplio que involucra a diferentes niveles de una estructura TIC:

Servicios y aplicaciones

Bases de datos y repositorios

Comunicaciones

Arquitectura hardware y SO

4. Arquitecturas y principios de ciberseguridad

- Por este motivo suelen proponerse modelos conceptuales que tengan en cuenta diferentes dominios.
 - Cada uno de ellos se estudia por separado para analizar los riesgos, las amenazas, las vulnerabilidades, las contramedidas, etc.
- Existen modelos horizontales y verticales (sectoriales) que abordan el problema de manera más o menos general.
 - A veces se asocian a metodologías y herramientas específicas.



Para practicar un poco

1. Busca el patrón de ataque "Identity Spoofing" en CAPEC y analiza en detalle la información que te proporciona esta base de datos. ¿Con qué debilidad de software se asocia?
2. Busca esta debilidad en la base de datos CWE y analiza la información que se proporciona en detalle. Obtén la lista de vulnerabilidades en productos software concretos que tienen que ver con esta debilidad. ¿Te parece que hay información suficiente en el CWE para que los desarrolladores se conciencien y adquieran buenas prácticas para la producción de software seguro?
3. Busca la vulnerabilidad más reciente provocada por esta debilidad de software (de este mismo año). Analiza la información que te proporciona el CVE, y complétala con la NVD y el CVE details. ¿Se trata de una vulnerabilidad muy crítica? ¿A qué aspecto de la seguridad puede afectar principalmente?

Referencias

- Fotografías
 - <https://unsplash.com>
- Iconos
 - <https://www.flaticon.es/>



**Reconocimiento-CompartirIgual 3.0
España (CC BY-SA 3.0 ES)**

©2019-2022 Marta Beltrán URJC (marta.beltran@urjc.es)
Algunos derechos reservados.

Este documento se distribuye bajo la licencia “Reconocimiento-CompartirIgual 3.0 España” de Creative Commons, disponible en
<https://creativecommons.org/licenses/by-sa/3.0/es/>