IT Security Governance

IT Audit & Security Meetup #2
Traveloka, Maret 2017

Belajar Keamanan Informasi Hal Menyenangkan

Narsis Dikit

Rungga Reksya Sabilillah

Certified Risk Management 1st / BSMR (2010)
Certified Ethical Hacking / CEH (2013)
Lead Auditor ISO 27001 (2013)
Lead Auditor ISO 20000 (2014)
Security Analyst / ECSA (2015)
Security Certified Professional / OSCP (2015)
Certified Network Defender / CND (2016)
Lead Auditor ISO 22301 (2017)

S1 – Teknik Informatika (2005 – 2009)
S2 – Manajemen Sistem Informasi (2011-2013)

Wushu Athletes at The PORDA II Banten (2006)
Leader of Wushu Gunadarma (2007-2008)

Favorite Operating Systems of Hackers

(2017 Lists)

Kali Linux

It was developed by **Mati Aharoni** and Devon Kearns of Offensive Security through the rewrite of BackTrack, their previous forensics Linux distribution based on Ubuntu.

Backbox Linux

BackBox is an Ubuntu-based Linux distribution penetration test and security assessment oriented providing a network and informatic systems analysis toolkit. BackBox desktop environment includes a complete set of tools required for ethical hacking and security testing.

Parrot Security OS

Parrot Security OS (or ParrotSec) is a GNU/LINUX distribution based on Debian. It has been developed by Frozenbox's Team.

https://techlog360.com/top-15-favourite-operating-systems-of-hackers/

Favorite Operating Systems of Hackers

(2017 Lists)

Live Hacking OS

Live Hacking OS is a Linux distribution packed with tools and utilities for ethical hacking, penetration testing and countermeasure verification. It includes the graphical user interface GNOME inbuilt.

Bugtraq

Bugtraq is an electronic mailing list dedicated to issues about computer security. Bugtraq team is experienced freaks and developers, It is available in Debian, Ubuntu and OpenSuSe in 32 and 64 bit architectures.

Dracos Linux

Dracos Linux is an open source operating system provides to penetration testing. Packed with a ton of pentest tools including information gathering, forensics, malware analysis, maintaining access, and reverse engineering.

https://techlog360.com/top-15-favourite-operating-systems-of-hackers/

Incident Classification Patterns

(2015 Data Breach Investigations Report)

40% **Web App Attacks**

23% **POS Intrusions**

Percentage (blue bar), and count of breaches per pattern. The gray line represents the percentage of breaches from the 2015 DBIR. (n=2,260)

831
Hacking - Use of stolen credential

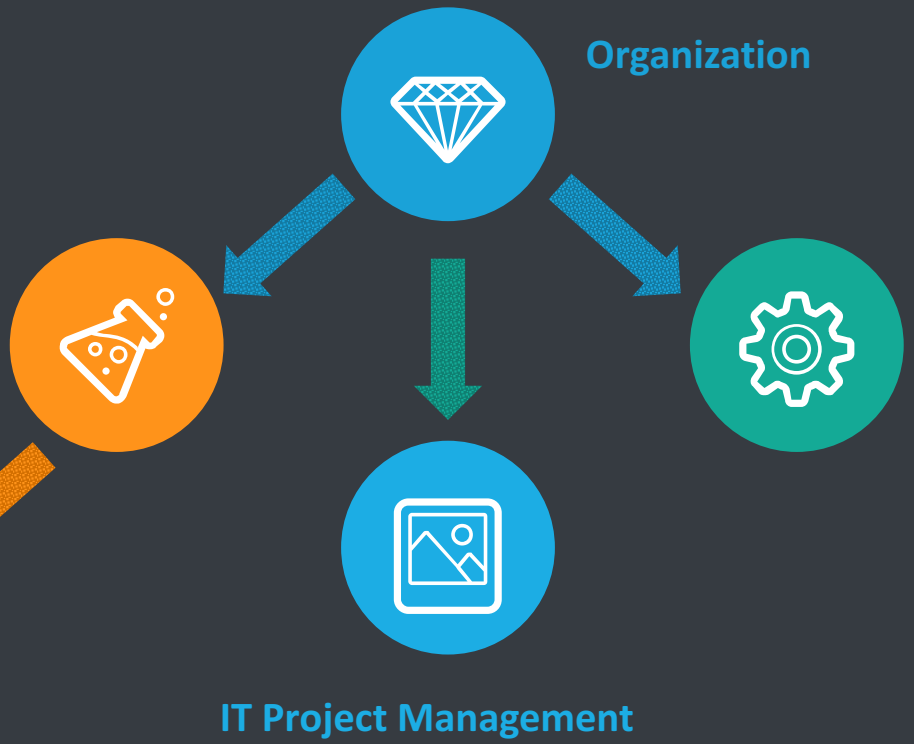
817
Social - Phishing

817
Hacking - Use of backdoor or C2

812
Malware – Spyware / Key logger

Top 10 Threat action varieties within Web App Attack breaches, (n=879)

What is Information Security Governance ?



IT Security Governance

accountability framework and provides **oversight** to ensure that risk are adequately mitigated

IT Security Management

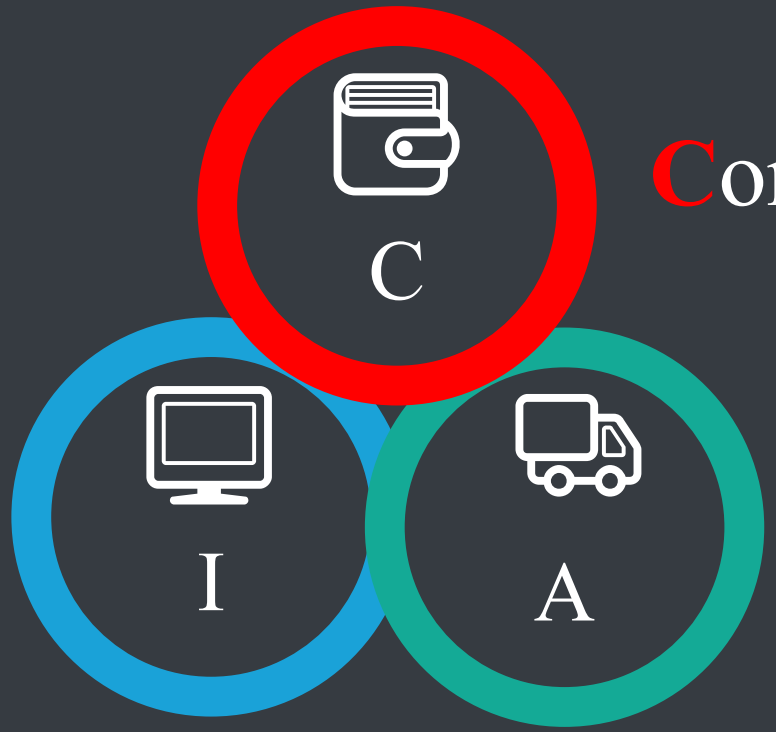
concerned with making decisions and management ensures that control are **implemented** to mitigate risks;

IT Security Governance

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

describes **IT governance** **as the process of establishing and maintaining a framework to provide assurance that information security strategies are aligned with and support business objectives**, are consistent with applicable laws and regulations through adherence to policies and internal controls, and provide assignment of responsibility, all in an effort to manage risk.

Three Critical Components for an Information Security



Confidentiality

Integrity

Availability

Information Security Look Like Football

GK-DEFENDER

Sysadmin, Network, Firewall, SIEM, etc.

MIDFIELDER

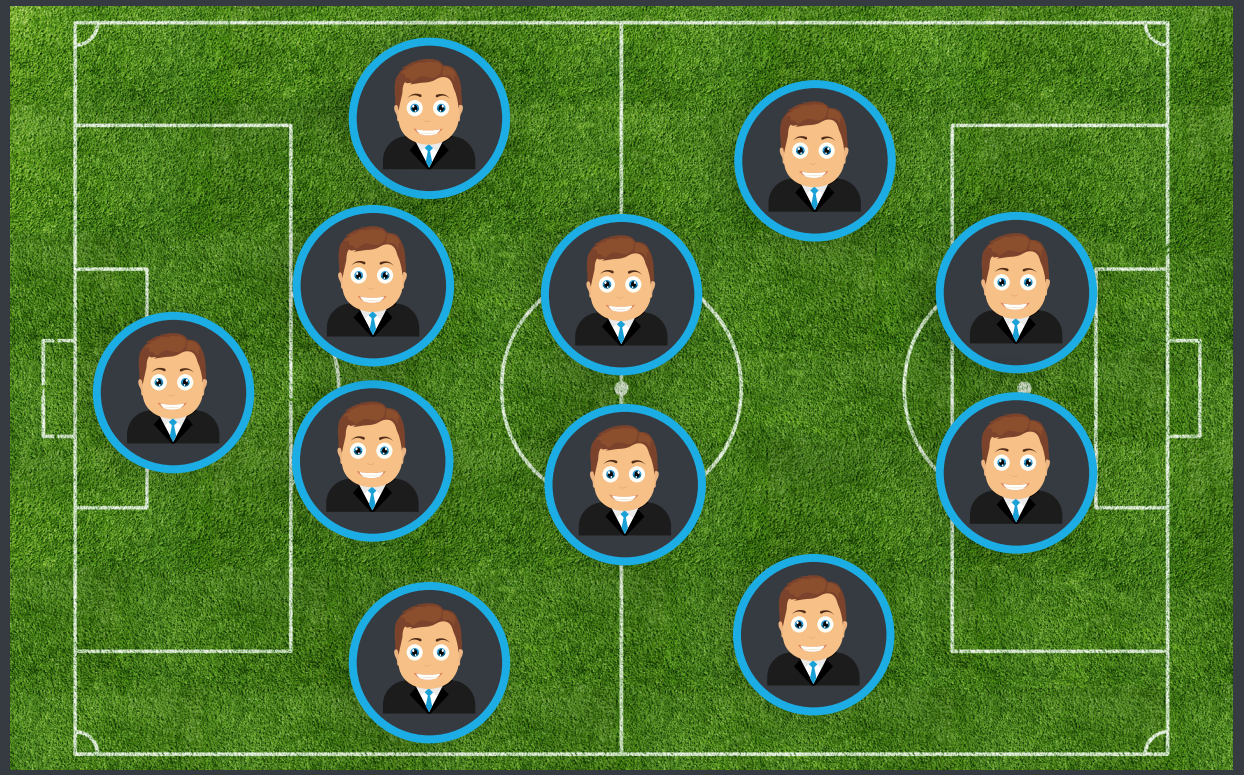
InfoSec Officer, Risk Management Internal, Compliance, etc.

STRIKER

InfoSec Consultant, Pentester, etc.

COACH

Top Management, CISO



Formation = Framework

- ISO/IEC 27001
- NIST SP 800 (Computer Security)
- PCI DSS
- HIPAA
- ISMF

Supporter Soccer

Stakeholder

CRITICAL COMPONENTS of ITSM

Four ITSM Components That Need to be Integrated with ISMS

PEOPLE

Information Security Awareness (Annex 7.2.2), etc.

PRODUCT

Technical Vulnerability Management (Annex 12.6), etc.

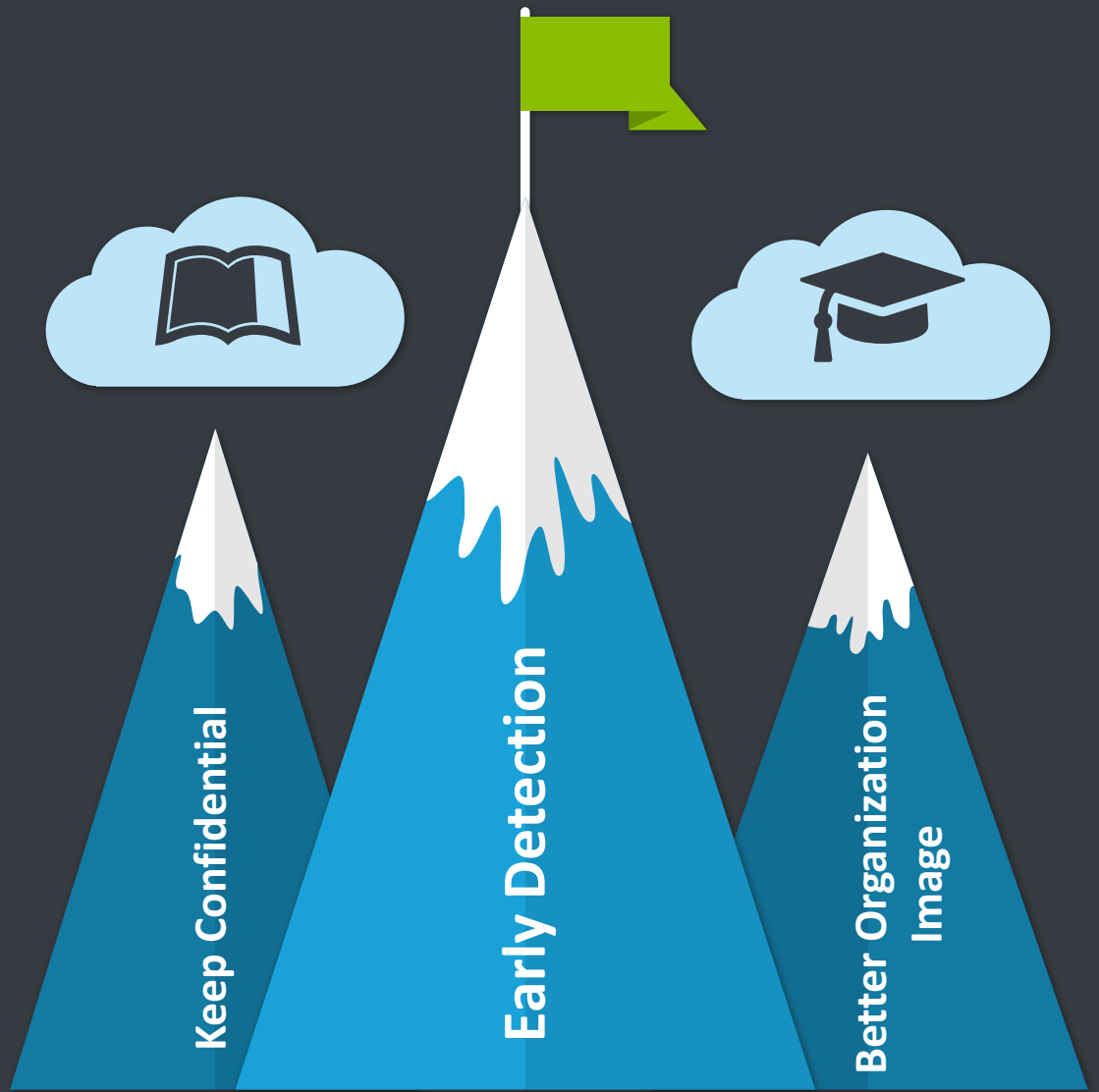
SUPPLIER

Supplier Relationships (Annex 15), etc.

PROCESS

Information Security Policies (Annex 5); Segregation of Duties (Annex 6.1.2), etc.

Effective Governance and Benefits



- Board members understand that **information security is critical** to the organization and demand to be **updated quarterly on security performance and breaches**.
- The organization **reviews** its enterprise **security program**, **security processes**, and **security's role in business processes**.
- **The resulting risk management plan** is **aligned with the entity's strategic goals**, forming the basis for the company's security policies and program.
- The goal of the enterprise security program is **continuous improvement**.

Memenuhi Janji Ke Subes
“K-159”

Common Vulnerabilities and Exposures

The Standard for Information Security Vulnerability Names

Follow CVE

TOTAL CVE IDs: 85937

Request a CVE ID

Click for CNAs, MITRE request form, guidelines, & more

Update info in a CVE ID

Click for MITRE request form, guidelines & more

CVE List downloads

Available in xml, CVRF, txt, & comma-separated

CVE content data feed

Available via CVEnew Twitter Feed

Become a CNA

Click for process, documentation & more

CVE Blog

Why is a CVE entry marked as "RESERVED" when a CVE ID is being publicly used?

A CVE ID is marked as "RESERVED" when it has been reserved for use by a CVE Numbering Authority (CNA) or security researcher but the details of it are not yet included in the CVE entry.

Often, this is because the original requester of the CVE ID assignment has not sent an update to MITRE with the information needed to populate the CVE entry...

More >>

Latest CVE News

- Ambionics Security Makes Declaration of CVE Compatibility
- Bluedon Information Security Technologies Makes Declaration of CVE Compatibility
- New CVE Board Member from Lenovo
- IMPORTANT: CVE Will Reject a Group of Unused CVE IDs on May 11

More >>

Focus On

CVE Now on LinkedIn and Twitter

Please follow us on Twitter for the latest from CVE:

- @CVEnew – feed of the latest CVE IDs
- @CVEannounce – news and announcements about CVE

Please also visit us on LinkedIn to comment on our news articles and CVE Blog posts:

- CVE-CWE-CAPEC on LinkedIn

More >>

Page Last Updated or Reviewed: May 22, 2017

FAQs
Terminology
Documents Archive

ALSO SEE

Privacy Policy
Terms of Use

Introduction

Common Vulnerabilities and Exposures (CVE®) is a dictionary of common names (i.e., CVE Identifiers) for publicly known cybersecurity vulnerabilities. CVE's common identifiers make it easier to share data across separate network security databases and tools, and provide a baseline for evaluating the coverage of an organization's security tools. If a report from one of your security tools incorporates CVE Identifiers, you may then quickly and accurately access fix information in one or more separate CVE-compatible databases to remediate the problem.

Learn about the new format for CVE Identifiers.

CVE is:

- One name for one vulnerability or exposure
- One standardized description for each vulnerability or exposure
- A dictionary rather than a database
- How disparate databases and tools can "speak" the same language
- The way to interoperability and better security coverage
- A basis for evaluation among tools and databases
- Free for public download and use
- Industry-endorsed via the CVE Numbering Authorities, CVE Board, and CVE-Compatible Products

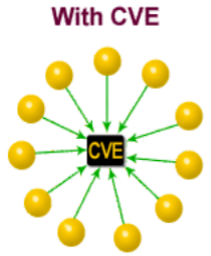
BACK TO TOP

Why CVE

CVE was launched in 1999 when most information security tools used their own databases with their own names for security vulnerabilities. At that time there was no significant variation among products and no easy way to determine when the different databases were referring to the same problem. The consequences were potential gaps in security coverage and no effective interoperability among the disparate databases and tools. In addition, each tool vendor used different metrics to state the number of vulnerabilities or exposures they detected, which meant there was no standardized basis for evaluation among the tools.

CVE's common, standardized identifiers provided the solution to these problems.

CVE is now the industry standard for vulnerability and exposure names. CVE Identifiers — also called "CVE names," "CVE numbers," "CVE IDs," and "CVEs" — provide reference points for data exchange so that information security products and services can speak with each other. CVE Identifiers also provides a baseline for evaluating the coverage of tools and services so that users can determine which tools are most effective and appropriate for their organization's needs. In short, products and services compatible with CVE provide better coverage, easier interoperability, and enhanced security.



CVE-1999-0067: CGI phf program allows remote command execution through shell metacharacters

BACK TO TOP

How CVE Works

Each CVE Identifier includes:

- CVE Identifier number (i.e., "CVE-1999-0067", "CVE-2014-10001", "CVE-2014-100001").
- Brief description of the security vulnerability or exposure.
- Any pertinent references (i.e., vulnerability reports and advisories).

The process of creating a CVE Identifier begins with the discovery of a potential security vulnerability.

The information is then assigned a CVE Identifier by a CVE Numbering Authority (CNA) and posted on the CVE List on the CVE website by the CVE Editor. As part of its management of CVE, The MITRE Corporation functions as Editor and Primary CNA.

Section Menu

CVE IDs
CVEnew Twitter Feed
Other Updates & Feeds

Request a CVE ID
Contact a CVE Numbering Authority (CNA)
Contact Primary CNA (MITRE) – CVE Request web form
Reservation Guidelines

CVE LIST (all existing CVE IDs)
Downloads
Search CVE List
Search Tips
View Entire CVE List (html)
Reference Key/Maps

NVD Advanced CVE Search
CVE ID Scoring Calculator

CVE Numbering Authorities
Participating CNAs
Documentation for CNAs
Requesting CVE IDs from CNAs
Become a CNA

Documentation
About CVE IDs
Terminology
Editorial Policies
Terms of Use

ALSO SEE
Common Vulnerability Scoring System (CVSS)
Common Vulnerability Reporting Framework (CVRF)
U.S. National Vulnerability

Request a CVE ID

CVE prioritizes the assignment of CVE Identifiers (CVE IDs) for the products, vendors, and product categories listed below, but you may request a CVE ID for any vulnerability.

Shortcuts for experienced users:

CNA contact info
MITRE CVE Request web form
Request a block of CVE IDs (CNAs only)

New users, follow these steps to request CVE IDs:

1) Locate the correct CVE Numbering Authority (CNA) for your vulnerability in the CNA coverage or MITRE coverage tables below.

2) Contact the CNA specified below using the contact method provided.

3) If your vulnerability is not listed on this page but you still would like a CVE ID, please contact MITRE (Primary CNA).

BACK TO TOP

CNA Coverage

For open source software products not listed below, request a CVE ID through the Distributed Weakness Filing Project CNA.

Product, Vendor, or Product Category Name	Scope	CNA Contact Email	CNA Website Information (if applicable)
MITRE Corporation	All vulnerabilities listed in the MITRE Coverage table below, plus all vulnerabilities not already listed on this page	MITRE CVE Request web form	https://cveform.mitre.org/
Adobe Systems Incorporated	Adobe issues only	psirt@adobe.com	Adobe security page
Android (associated with Google Inc. or Open Handset Alliance)	Android issues only	security@android.com	Android security page
Apache Software Foundation	Apache Software and Apache HTTP Server issues only	security@apache.org	Apache security page
Apple Inc.	Apple issues only	product-security@apple.com	Apple security page

Section Menu

CVE IDs

CVEnew Twitter Feed

Other Updates & Feeds

Request a CVE ID

Contact a CVE Numbering Authority (CNA)

Contact Primary CNA (MITRE) – CVE Request web form

Reservation Guidelines

CVE LIST (all existing CVE IDs)

Downloads

Search CVE List

Search Tips

View Entire CVE List (html)

Reference Key/Maps

NVD Advanced CVE Search

CVE ID Scoring Calculator

CVE Numbering Authorities

Participating CNAs

Documentation for CNAs

Requesting CVE IDs from CNAs

Become a CNA

Documentation

About CVE IDs

Terminology

Search Results

There are **6772** CVE entries that match your search.

Name	Description
CVE-2017-8917	SQL injection vulnerability in Joomla! 3.7.x before 3.7.1 allows attackers to execute arbitrary SQL commands via unspecified vectors.
CVE-2017-8796	An issue was discovered on Accellion FTA devices before FTA_9_12_180. Because mysql_real_escape_string is misused, seos/courier/communication_p2p.php allows SQL injection with the app_id parameter.
CVE-2017-8789	An issue was discovered on Accellion FTA devices before FTA_9_12_180. A report_error.php?year='payload SQL injection vector exists.
CVE-2017-8377	GeniXCMS 1.0.2 has SQL Injection in inc/lib/Control/Backend/menus.control.php via the menuid parameter.
CVE-2017-7991	Exponent CMS 2.4.1 and earlier has SQL injection via a base64 serialized API key (apikey parameter) in the api function of framework/modules/eaas/controllers/eaasController.php.
CVE-2017-7952	INFOR EAM V11.0 Build 201410 has SQL injection via search fields, related to the filtervalue parameter.
CVE-2017-7886	Dolibarr ERP/CRM 4.0.4 has SQL Injection in doli/theme/eldy/style.css.php via the lang parameter.
CVE-2017-7879	SQL Injection vulnerability in flatCore version 1.4.6 allows an attacker to read the content database.
CVE-2017-7878	SQL Injection vulnerability in flatCore version 1.4.6 allows an attacker to read and write to the users database.
CVE-2017-7719	SQL injection in the Spider Event Calendar (aka spider-event-calendar) plugin before 1.5.52 for WordPress is exploitable with the order_by parameter to calendar_functions.php or widget_Theme_functions.php, related to front_end/frontend_functions.php.
CVE-2017-7717	SQL injection vulnerability in the getUserUddiElements method in the ES UDDI component in SAP NetWeaver AS Java 7.4 allows remote authenticated users to execute arbitrary SQL commands via unspecified vectors, aka SAP Security Note 2356504.
CVE-2017-7628	The "Smart related articles" extension 1.1 for Joomla! has SQL injection in dialog.php (attacker must use search_cats variable in POST method to exploit this vulnerability).
CVE-2017-7581	SQL injection vulnerability in NewsController.php in the News module 5.3.2 and earlier for TYPO3 allows unauthenticated users to execute arbitrary SQL commands via vectors involving overwriteDemand for order and OrderByAllowed.

Trik Riset Agar Dapat CVE

Cari Contoh CVE

- Tentukan CMS atau Aplikasi Apa
- Cek di exploit-db, packetstormsecurity, dll

Unduh Aplikasi

Open Source:
- ampps.com / softaculous
- Github

Tentukan Perimeter Pengujian

Misal:
- XSS, SQL Injection, RFI/LFI, IDOR, CSRF, dll

Tentukan Laporan Mini

- Judul
- Produk, Versinya
- PoC, Saran, dll

Etika Lapor

- Lapor ke pengembang sistem (jika masih hidup) via Github, Email, dll
- Booking nomor CVE
- Kirim ke exploit-db, packetstormsecurity, dkk

Sharing Ke Teman

Semakin sering berbagi maka ilmu akan terus bertambah dan mencerdaskan bangsa. #Eaaaa

Apa Yang Dibutuhkan Menjadi Peneliti CVE Newbie

- Feeling so Good
- Punya Konsep/Apa yg Diteliti
- Ikuti Bisnis Proses/Fungsi Aplikasi dan Out of The Box
- Pengalaman
- Keberuntungan dan Doa

rungga_reksya

Jangan Percaya Sama Saya Gan ^_^