Nomor : 06/UDN.FST-STI/J/II/2026
Perihal : Permohonan Sebagai Narasumber
Lampiran : -

Yth.
Rektor Universitas IPWIJA
Jl. Letda Nasir No.7, Nagrak, Kec. Gn. Putri
Bogor

Assalamualaikum Warahmatullahi Wabarakatuh

Puji syukur kehadirat Allah SWT yang telah melimpahkan rahmat dan karuniaNya kepada kita semua.

Dalam rangka peningkatan kompetensi bidang Sistem dan Teknologi Informasi Universitas Darunnajah Jakarta, dengan ini kami mohon perkenan Saudara menugaskan Sdri. Siti Sarah, M.Kom, Sdr. Yodi Susanto, M.Kom. dan Sdr. Amin Muzaeni, M.Kom. untuk menjadi narasumber kegiatan dimaksud yang dilaksanakan pada:

Hari : Sabtu
Tanggal : 21 Februari 2026
Waktu : 10:00 S.D. Selesai
Agenda : Webinar "Introduction Vulnerability Assessment"
Tempat : Link Meeting Online

Demikian surat permohonan ini dibuat, atas perhatian dan kerjasamanya kami ucapkan terima kasih.

Wassalamualaikum, Wr. Wb.

Jakarta, 13 Februari 2026
Kaprodi Sistem dan Teknologi Informasi

Supriadi Panggabean, S.Kom M.Pd., M.Kom.

UNIVERSITAS IPWIJA
LEMBAGA PENELITIAN DAN PENGABDIAN KEPADA MASYARAKAT
Jl. Letda Natsir No.7 Cikeas Ds. Nagrak, Kec. Gunung Putri
Kab. Bogor. 16967 Telp. +62-21-8233737
lp2m@ipwija.ac.id https://lp2m.ipwija.ac.id
UNIVERSITAS IPWIJA

SURAT TUGAS PENGABDIAN KEPADA MASYARAKAT

No:015 /IPWIJA.LP2M/PkM-00/2026

Berdasarkan Surat Edaran Pengabdian Kepada Masyarakat (PKM) Semester Ganjil 2025/2026 No.148/IPWIJA.LP2M/PkM-00/2025 tanggal 1 September 2025 dan surat permohonan dari Universitas Darunnajah No. 06/UDN.FST-STI/J/II/2026 tanggal 13 Februari 2026 perihal permohonan Narasumber, Pendamping dan Pemberi Materi, dengan ini Kepala LP2M Universitas IPWIJA menugaskan::

1. Siti Sarah, S.Kom., M.Kom. (NIDN: 0302129401)
2. Yodi Susanto, S.Kom., M.Kom. (NIDN: 0320098606)
3. Amin Muzaeni, S.Kom., M.Kom (NIDN: 0326078904)

Untuk menjadi Narasumber dalam kegiatan yang akan dilaksanakan pada:

Hari / tanggal	: Sabtu, 21 Februari 2026
Waktu	: 10.00 WIB s.d selesai
Media	: daring (*online*)
Tema	: "*Introduction Vulnerability Assessment*."

Setelah pelaksanaan kegiatan Dosen yang ditugaskan diwajibkan membuat Laporan Pelaksanaan Kegiatan kepada pemberi tugas (LP2M Universitas IPWIJA). Mohon bantuan penanggungjawab kegiatan membantu menyediakan berkas yang diperlukan untuk pembuatan laporan pelaksanaan kegiatan.

Demikian Surat Tugas ini disampaikan untuk dapat dilaksanakan dengan penuh tanggung jawab.

Bogor, 18 Februari 2026

Drs Jayadi, M.M.
Kepala LP2M

SURAT KETERANGAN

Nomor: 08/UDN.FST-STI/I/II/2026

Assalamualaikum, Wr. Wb.

Yang bertanda tangan di bawah ini :

Nama	: Supriadi Panggabean, S.Kom., M.Pd., M.Kom.
NIP/NIDN	: - / 0323039302
Pangkat/Golongan	: Penata Muda Tk I, III/b
Jabatan Akademik	: Asisten Ahli
Jabatan	: Kaprodi Sistem dan Teknologi Informasi
Instansi	: Universitas Darunnajah Jakarta

dengan ini menerangkan bahwa:

1. Nama : Siti Sarah, M.Kom.
   NIDN : 0302129401
2. Nama : Yodi Susanto, M.Kom.
   NIDN : 0320098606
3. Nama : Amin Muzaeni, M.Kom.
   NIDN : 0326078904

Telah melaksanakan Pengabdian kepada Masyarakat (PkM) Dosen di Universitas Darunnajah Jakarta pada hari/tanggal Sabtu, 21 Februari 2026 dengan tema: " Introduction Vulnerability Assessment".

Demikian surat keterangan ini dibuat dengan sebenarnya untuk dipergunakan semestinya.

Wassalamualaikum, Wr. Wb.

Jakarta, 21 Februari 2026
Kaprodi Sistem dan Teknologi Informasi

Supriadi Panggabean, S.Kom M.Pd., M.Kom.

DIKTISAINTEK BERDAMPAK Universitas Darunnajah PUBG STI UNIVERSITAS IPWIJA

SERTIFIKAT

NOMOR : 11/UDN.FST-STI/H/II/2026

Diberikan kepada :

Siti Sarah, S.Kom., M.Kom.

Sebagai

NARASUMBER

Pada **Webinar Nasional Pengabdian Kepada Masyarakat (PKM)** Kolaborasi Univeritas Darunnajah Dan Universitas Ipwija yang dilaksanakan pada acara Pengetahuan Untuk Berbagi Gagasan Sistem dan Teknologi Informasi (PUBG STI) Part 17, dengan Tema : **"Introduction Vulnerability Assessment"**, yang diselengarakan di Jakarta pada tanggal 21 Februari 2026.

Jakarta, 21 Februari 2026

Kaprodi Sistem dan Teknologi Informasi	Ketua Pelaksana PUBG-STI
Supriadi Panggabean, M.Pd., M.Kom	**Naila Rahmah Ahadi**

DIKTISAINTEK BERDAMPAK Universitas Darunnajah PUBG STI UNIVERSITAS IPWIJA

SERTIFIKAT

NOMOR : 12/UDN.FST-STI/H/II/2026

Diberikan kepada :

Yodi Susanto, M.Kom.

Sebagai

NARASUMBER

Pada **Webinar Nasional Pengabdian Kepada Masyarakat (PKM)** Kolaborasi Univeritas Darunnajah Dan Universitas Ipwija yang dilaksanakan pada acara Pengetahuan Untuk Berbagi Gagasan Sistem dan Teknologi Informasi (PUBG STI) Part 17, dengan Tema : **"Introduction Vulnerability Assessment"**, yang diselengarakan di Jakarta pada tanggal 21 Februari 2026.

Jakarta, 21 Februari 2026

Kaprodi Sistem dan Teknologi Informasi	Ketua Pelaksana PUBG-STI
Supriadi Panggabean, M.Pd., M.Kom	**Naila Rahmah Ahadi**

DIKTISAINTEK BERDAMPAK Universitas Darunnajah PUBG STI UNIVERSITAS IPWIJA

SERTIFIKAT

NOMOR : 13/UDN.FST-STI/H/II/2026

Diberikan kepada :

Amin Muzaeni, M.Kom

Sebagai

NARASUMBER

Pada **Webinar Nasional Pengabdian Kepada Masyarakat (PKM)** Kolaborasi Univeritas Darunnajah Dan Universitas Ipwija yang dilaksanakan pada acara Pengetahuan Untuk Berbagi Gagasan Sistem dan Teknologi Informasi (PUBG STI) Part 17, dengan Tema : **"Introduction Vulnerability Assessment"**, yang diselengarakan di Jakarta pada tanggal 21 Februari 2026.

Jakarta, 21 Februari 2026

Kaprodi Sistem dan Teknologi Informasi	Ketua Pelaksana PUBG-STI
Supriadi Panggabean, M.Pd., M.Kom	**Naila Rahmah Ahadi**

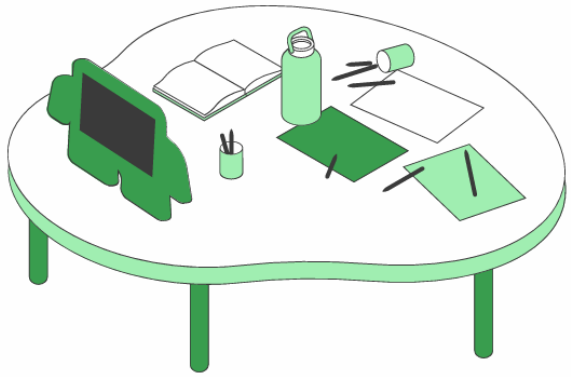
Webinar

Introduction Vulnerability Assessment

21 Februari 2026

Poin-poin

hari ini



- Apa itu Vulnerability Assesment (VA)?
- Apa itu Vulnerability Scanning?
- Apa itu Vulnerability Management?
- Jenis-Jenis alat VA
- Simulasi Vulnerability Scanning

Apa itu Vulnerability Assesment?

Merupakan proses untuk mengidentifikasi, mengevaluasi, dan melaporkan kelemahan keamanan di sistem, aplikasi, jaringan komputer dan seluruh lingkungan digital suatu organisasi.

Mengapa Vulnerability Assesment penting?

Sesuai dengan standar kepatuhan

Kelola ancaman siber secara proaktif

Memungkinkan perbaikan dan mitigasi lebih cepat

Memperkuat kepercayaan stakeholder

Security Vulnerability

Merupakan kelemahan dalam struktur, fungsi atau implementasi aset atau jaringan IT

Kelemahan pengodean

seperti aplikasi web yang rentan terhadap cross-site scripting, SQL injection

Port terbuka

dapat digunakan peretas untuk menyebarkan malware.

Kesalahan konfigurasi

dapat menyebabkan data sensitif terekspos ke internet publik

Tidak adanya patch

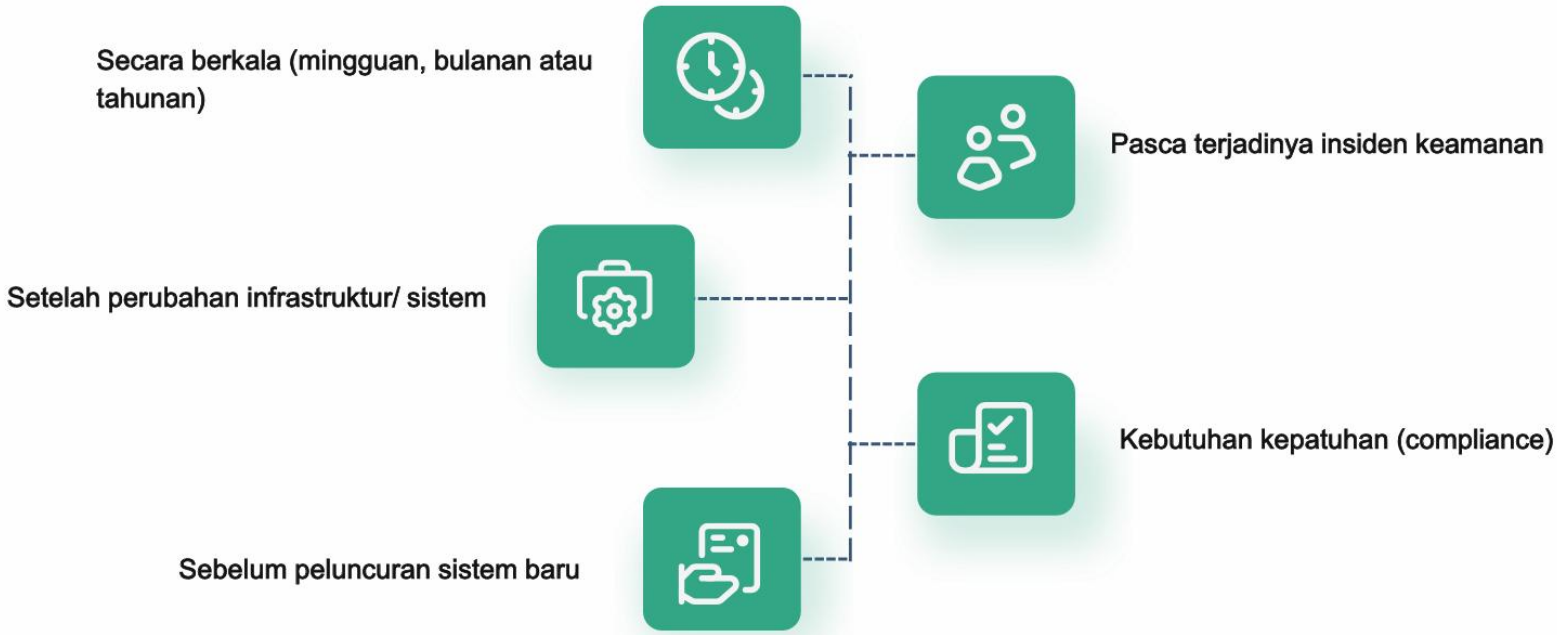
Dapat menyebabkan celah bagi threat actor atau malware masuk

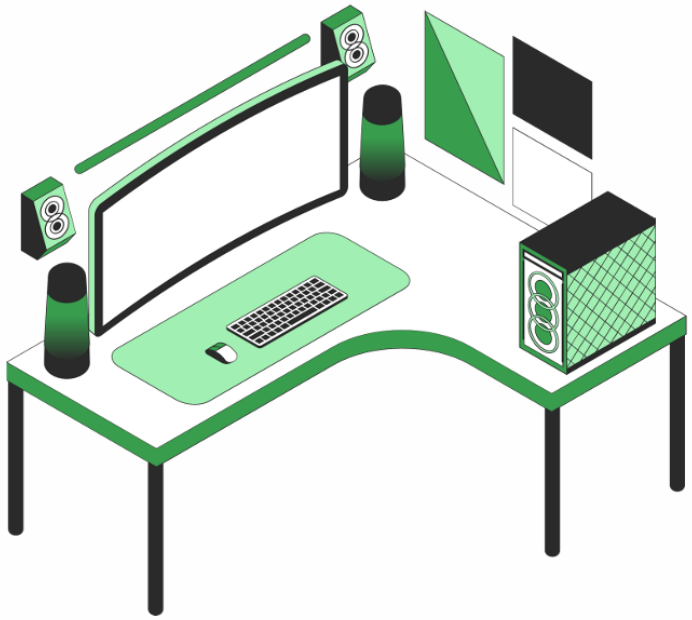
Jenis-Jenis Vulnerability Assesment

Apa itu Vulnerability Scanning?

Vulnerability Scanning , juga disebut “Vulnerability Assesment," adalah proses mengevaluasi jaringan atau aset IT untuk kerentanan keamanan, kekurangan, atau kelemahan yang dapat dieksploitasi oleh pelaku ancaman eksternal atau internal . Vulnerability Scanning adalah tahap pertama dari siklus manajemen kerentanan yang lebih luas .

Kapan Vulnerability Assessment dilakukan?





Apa itu Vulnerability Manajement?

Siklus manajemen kerentanan adalah proses berkelanjutan untuk menemukan, memprioritaskan, dan mengatasi kerentanan pada aset IT suatu perusahaan.

Perbedaan Vulnerability Assesment dan Vulnerability Management?

Vulnerability Management adalah proses mengelola kerentanan secara berkelanjutan yang menggunakan berbagai alat dan proses untuk mengidentifikasi semua aset dan kerentanan di lingkungan perusahaan. Ini juga membantu Anda merencanakan cara untuk mengurangi masalah, memperbaiki kelemahan, dan meningkatkan postur keamanan secara keseluruhan.

Vulnerability Assessment adalah bagian dari program vulnerability management yang membantu mengidentifikasi dan mengatasi risiko siber secara berkelanjutan.

Tahapan Vulnerability Manajement Lifecycle

1. Assest Discovery dan Vulnerability Assessment

Tim keamanan harus tahu apa saja yang perlu dilindungi dengan mengdentifikasi semua aset IT yang terhubung. Setelah inventaris selesai, lakukan pemindaian kerentanan.

3. Vulnerability Resolution

Tim keamanan meninjau daftar kerentanan yang diprioritaskan, dari yang paling kritis hingga yang paling tidak kritis. Organisasi memiliki tiga opsi untuk mengatasi kerentanan:

5. Reporting and Improvement

Tim keamanan mendokumentasikan aktivitas dari putaran siklus hidup terbaru, termasuk kerentanan yang ditemukan, langkah-langkah penyelesaian yang diambil, dan hasilnya.

2. Vulnerability Prioritization

Tim keamanan memprioritaskan kerentanan yang mereka temukan pada tahap penilaian. Prioritas ini memastikan bahwa tim menangani kerentanan paling kritis terlebih dahulu. Tahap ini juga membantu tim menghindari menghabiskan waktu dan sumber daya untuk kerentanan berisiko rendah.

4. Verification and Monitoring

Untuk memverifikasi bahwa upaya mitigasi dan perbaikan berhasil sesuai rencana, tim keamanan memindai ulang dan menguji ulang aset yang baru saja mereka tangani.

Common Vulnerability Scoring System (CVSS)

Apa itu CVSS?

Common Vulnerability Scoring System (CVSS) adalah kerangka kerja yang banyak digunakan untuk mengklasifikasikan dan memberi peringkat kerentanan perangkat lunak.

Score	Rating
Critical	9.0-10.0
High	7.0-8.9
Medium	4.0-6.9
Low	0.1-3.9

Common Vulnerabilities and Exposures (CVE)

Apa itu CVE?

Common Vulnerabilities and Exposures (CVE) umumnya merujuk pada daftar CVE, yaitu katalog kerentanan keamanan informasi yang diungkapkan kepada publik, yang dibuat dan dipelihara oleh MITRE Corporation.

Security Vulnerabilities, CVEs published between 2026-02-15 and 2026-02-21 CVSS score between and 10

Published in: 2026 January February

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9 In CISA KEV Catalog

Sort Results By : Publish Date Update Date CVE Number CVE Number CVSS Score EPSS Score

Page: 1 Copy

CVE-2026-27476

RustFly 2.0.0 contains a command injection vulnerability in its remote UI control mechanism that accepts hex-encoded instructions over UDP port 5005 without proper sanitization. Attackers can send crafted hex-encoded payloads containing system commands to execute arbitrary operations on the target system, including reverse shell establishment and command execution.

Source: VulnCheck

Max CVSS 9.8
EPSS Score 0.27%
Published 2026-02-19
Updated 2026-02-20

CVE-2026-27475

SPIP before 4.4.9 allows Insecure Deserialization in the public area through the table_valeur filter and the DATA iterator, which accept serialized data. An attacker who can place malicious serialized content (a pre-condition requiring prior access or another vulnerability) can trigger arbitrary object instantiation and potentially achieve code execution. The use of serialized data in these components has been deprecated and will be removed in SPIP 5. This vulnerability is not mitigated by the SPIP security screen.

Source: VulnCheck

Max CVSS 9.2
EPSS Score 0.05%
Published 2026-02-19
Updated 2026-02-20

CVE-2026-27180

MajorDoMo (aka Major Domestic Module) is vulnerable to unauthenticated remote code execution through supply chain compromise via update URL poisoning. The saverestore module exposes its admin() method through the /objects/?module=saverestore endpoint without authentication because it uses gr('mode') (which reads directly from $_REQUEST) instead of the framework's $this→mode. An attacker can poison the system update URL via the auto_update_settings mode handler, then trigger the force_update handler to initiate the update chain. The autoUpdateSystem() method fetches

Source: VulnCheck

Max CVSS 9.8
EPSS Score 0.09%
Published 2026-02-18
Updated 2026-02-20

Vulnerability scanning

proses mencari dan mengidentifikasi celah keamanan pada sistem, aplikasi, atau jaringan.

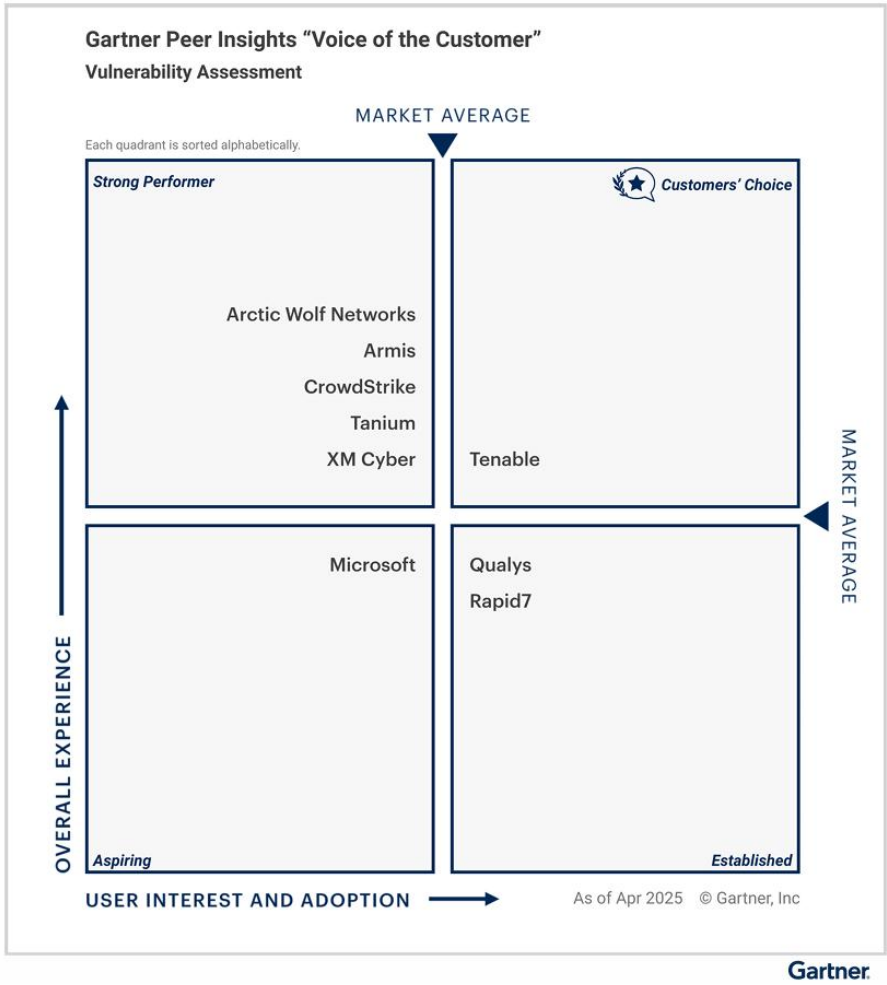
Penetration testing

proses mensimulasikan serangan nyata untuk mencoba mengeksploitasi celah keamanan.

Jenis-jenis alat Vulnerability Assessment

berdasarkan Gartner Peer “Voice of the Customer”

Voice of the Customer” adalah dokumen yang merangkum dan mengolah ulasan dari pengguna di Gartner Peer Insights menjadi informasi yang bermanfaat untuk orang atau perusahaan yang ingin membeli teknologi dan layanan.



Pekerjaan terkait VA

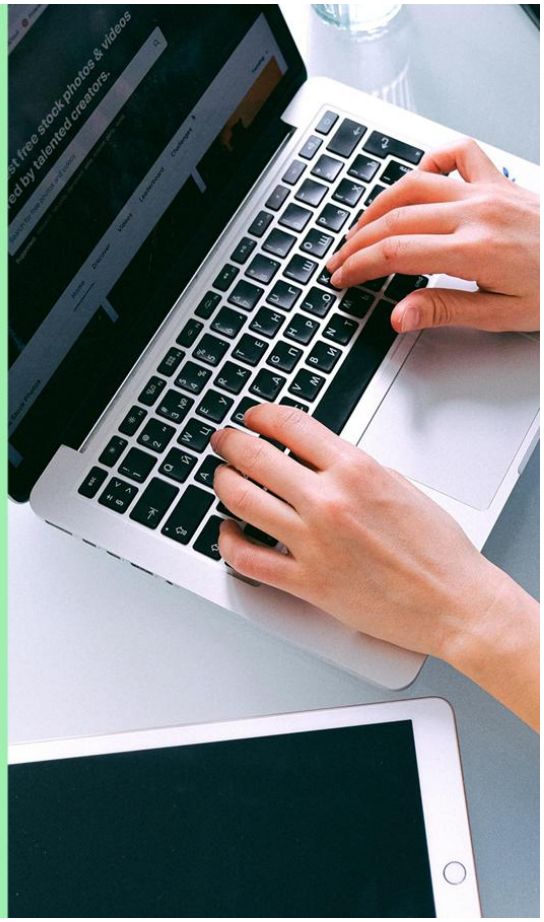
Direct Contract, IT Cyber Security, Technology
DBS Bank • Jakarta Metropolitan Area (On-site)

Responsibilities

- Develop and implement comprehensive cybersecurity strategies and policies to protect the bank's IT infrastructure and data assets
- Conduct risk assessments, vulnerability analyses, and penetration testing to identify and mitigate security threats
- Collaborate with cross-functional teams to design, deploy, and maintain secure IT systems and applications
- Investigate and respond to security incidents, implement remediation measures, and document findings
- Stay up-to-date with the latest cybersecurity trends, technologies, and best practices, and provide recommendations for continuous improvement
- Develop and deliver security awareness training programs for employees to enhance their understanding of cybersecurity risks and responsibilities
- Ensure compliance with relevant industry standards, regulations, and internal policies related to information security

Requirements

- Bachelor's degree in Computer Science, Information Technology, or a related field
- Minimum 5 years of experience in IT cybersecurity, with a strong understanding of security frameworks, protocols, and best practices
- Proven track record in designing, implementing, and managing comprehensive cybersecurity solutions
- Expertise in security monitoring, incident response, and threat management
- Proficient in using security tools and technologies, such as firewalls, intrusion detection/prevention systems, and security information and event management (SIEM) platforms
- Excellent problem-solving, analytical, and critical thinking skills
- Strong communication and collaboration skills to work effectively with cross-functional teams
- Certifications in relevant cybersecurity domains (e.g., CISSP, CISM, CISA) are preferred



Pekerjaan terkait VA

IT APPLICATION SECURITY
PT Bank KEB Hana Indonesia • Jakarta, Jakarta, Indonesia (On-site)

About the job

Requirements

- Bachelor's degree in Computer Science, Information Technology, Cybersecurity, or a related field.
- Minimum 5 years of experience in application security, cybersecurity, or software development.
- Strong understanding of OWASP Top 10 and common application vulnerabilities.
- Hands-on experience with security tools such as SAST, DAST, SCA, WAF, and penetration testing tools.
- Familiarity with secure software development practices and CI/CD pipelines.
- Knowledge of application architecture (API security, web app security, microservices, cloud apps).
- Ability to read and review code in languages such as Java, JavaScript, Python, or others.
- Experience with security incident response related to application threats.

Responsibilities

- Perform application security assessments, including code reviews, penetration testing, and vulnerability scans.
- Identify, analyze, and prioritize security vulnerabilities within applications.
- Work closely with development teams (DevOps/SRE) to implement secure coding practices and integrate security into the SDLC (Secure Development Lifecycle).
- Monitor and respond to application-related security incidents.
- Develop, review, and maintain application security policies, standards, and guidelines.
- Ensure compliance with security frameworks and regulatory requirements (e.g., ISO 27001, PCI-DSS, OWASP).
- Collaborate with product, IT, and infrastructure teams to ensure secure architecture and design principles are followed.
- Assist in implementing application-level security tools (WAF, SAST, DAST, SCA, etc.).

Pekerjaan terkait VA

Offensive Security Engineer
ParagonCorp • Jakarta, Indonesia (On-site)

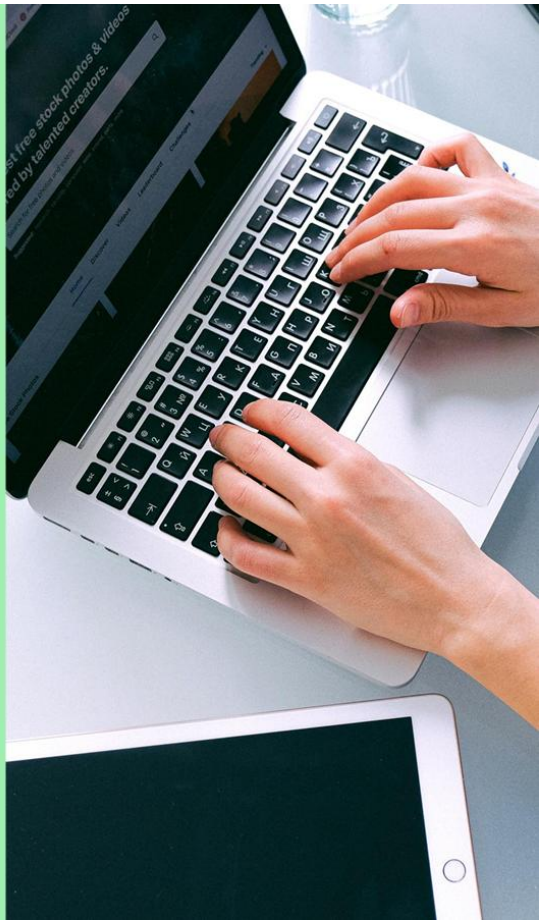
About the job

Job Description:

- Conduct covert, threat-based penetration testing to simulate real-world adversary attacks on Paragon systems
- Develop attack vectors and execute reconnaissance, enumeration, footprinting, and open-source intelligence (OSINT) gathering
- Identify, exploit, and validate security vulnerabilities across applications, infrastructure, and networks
- Develop exploit payloads, proof-of-concepts, and persistence mechanisms to demonstrate security impact
- Collaborate with engineering, infrastructure, and platform teams to remediate identified vulnerabilities
- Provide technical guidance to improve the security posture of applications, cloud environments, and infrastructure
- Document findings clearly, including attack paths, risk impact, and remediation recommendations
- Support continuous improvement of Paragon's offensive security methodologies and tooling
- Stay updated on emerging threats, attack techniques, and offensive security tools

Requirements:

- Bachelor's degree in Computer Science, Information Systems, or a related field
- 2–3 years of experience in offensive security, penetration testing, or information security engineering
- Hands-on experience performing penetration testing on applications, systems, or networks
- Experience using vulnerability scanning and offensive security tools (e.g. Burp Suite, Metasploit, Nmap, etc.)
- Understanding of common operating systems (Windows, Linux, macOS) and basic cloud environments
- Good understanding of networking concepts, configurations, and security controls
- Ability to communicate technical findings clearly to both technical and non-technical stakeholders
- Strong problem-solving skills and ability to think like an attacker
- Ability to work calmly under pressure and maintain confidentiality
- Strong sense of ownership and personal accountability



Pekerjaan terkait VA

Security Engineer, Offensive Security
Grab • Jakarta Metropolitan Area (On-site)

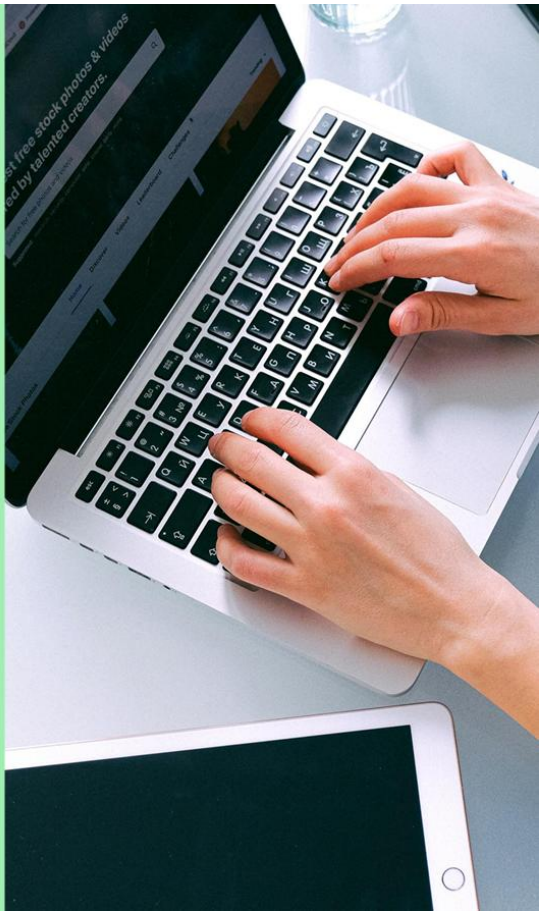
The Critical Tasks You Will Perform

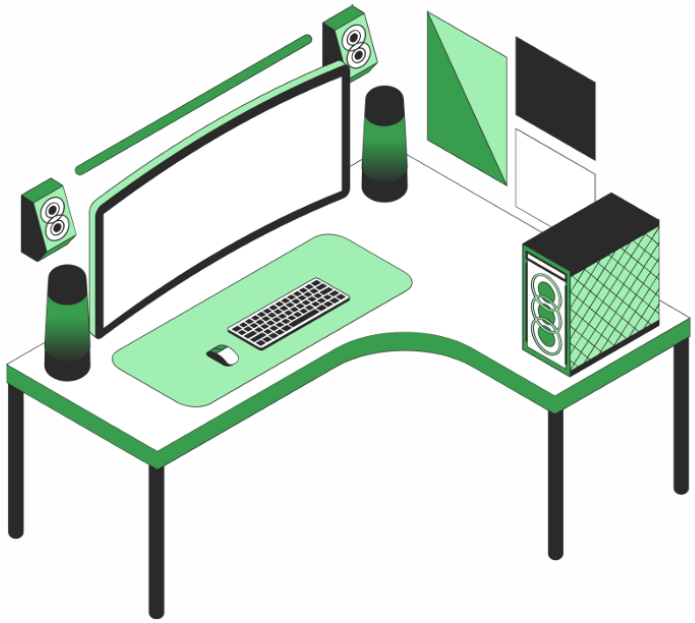
- Vulnerability Management: Drive the identification and remediation of high-priority Web/Mobile application and environment security issues, including screening, providing remediation guidance, validating fixes, and assessing the risk and impact of vulnerabilities or proposed mitigations.
- Security Expertise & Support: Provide application security expertise to other Cyber Security teams and assist the Cyber Incident Response team with investigations.
- Bug Bounty Participation: Triage security issues reported via Grab's Bug Bounty Program on HackerOne and follow up with development teams for fixes.
- Testing & Auditing: Conduct application security testing, source code auditing, and penetration testing focused on critical data, services, and environments; provide clear risk assessments and remediation guidelines.
- Research & Documentation: Research the latest cybersecurity methodologies, threats, and technology frameworks; document and disseminate security guidelines, remediation mentorship, and security technology baselines.
- Tool Development & AI Utilization: Develop tools, exploits, and AI-enhanced automation scripts/intelligent security testing frameworks to support application security reviews and penetration testing.
- AI/ML Security: Secure AI/ML applications and APIs against emerging threats (e.g., prompt injection, model poisoning, adversarial attacks) and use AI-powered tools/assistants to enhance vulnerability detection, risk assessment, testing efficiency, research, and threat analysis.

Qualifications

What Essential Skills You Will Need

- 2+ years of security industry experience, specializing in web/mobile application security and an understanding of the threat landscape; embody our core values of Heart, Hunger, Honour, and Humility.
- Technical Proficiency: Working knowledge of major cloud platforms (AWS, GCP, Alibaba, Azure), expertise in web/mobile penetration testing tools/procedures, and foundational understanding of defense-in-depth methodologies and security best practices.
- Coding & Automation: Ability to code/script in at least one language (e.g., Python, Java, GoLang, C++) to develop technical solutions, automate security testing, and mitigate vulnerabilities.
- AI Security Focus: Understanding of AI/ML security risks (e.g., OWASP Top 10 for LLMs, prompt injection, model vulnerabilities), knowledge of securing AI applications/APIs, and proficiency in using AI assistants (ChatGPT/Claude) and basic prompt engineering for security analysis.
- Communication & Collaboration: Able to point out technical solutions, advocate for cybersecurity across teams, and





Simulasi Vulnerability Scanning

Simulasi scanning menggunakan tools Tenable.SC dan nessus scanner

Thank you

Webinar “Introduction Vulnerability Assessment”
21 Februari 2026.