JURNAL PENGABDIAN MASYARAKAT BANGSA
e-ISSN : 2987- 0135
Volume 3, No. 11, Tahun 2026
https://jurnalpengabdianmasyarakatbangsa.com/index.php/jpmba/index

Pelatihan Analisis Kerentanan Sistem Informasi Menggunakan *Vulnerability Assessement* Bagi Siswa Magang Universitas Binadarma

Raynor Sagraha[1], Maria Ulfa[2], Ilman Zuhriyadi[3], Isnawijayani[4], Ahmad Syazili[5]
[1,2,3,4,5] *Universitas Binadarma, Indonesia*

Corresponding Author
Nama Penulis: Raynor Sagraha
E-mail: Renoldbkl@gmail.com

Abstrak

Kegiatan pengabdian ini bertujuan untuk meningkatkan kemampuan siswa magang Universitas Bina Darma dalam memahami dan melakukan analisis kerentanan sistem informasi melalui pendekatan vulnerability assessment. Pelatihan disusun untuk menjawab kebutuhan mitra dalam memperkuat pemahaman dasar keamanan siber, terutama terkait identifikasi celah keamanan pada aplikasi dan sistem berbasis web. Untuk mencapai tujuan tersebut, kegiatan dilaksanakan melalui tiga tahapan utama, yaitu penyampaian materi mengenai konsep dasar keamanan informasi, demonstrasi penggunaan perangkat analisis seperti Nessus dan OWASP ZAP, serta praktik langsung melakukan pemindaian dan penilaian kerentanan terhadap contoh sistem informasi. Seluruh peserta dibimbing dalam mengoperasikan alat, memahami jenis kerentanan yang ditemukan, dan menyusun laporan hasil analisis keamanan. Berdasarkan pelaksanaan kegiatan, diperoleh hasil bahwa siswa mampu menguasai langkah-langkah dasar vulnerability assessment, mengenali kerentanan umum seperti SQL Injection dan Cross-Site Scripting, serta menghasilkan laporan evaluasi sederhana. Program ini menunjukkan bahwa pelatihan yang diberikan efektif dalam meningkatkan pemahaman serta keterampilan praktis siswa magang di bidang keamanan informasi, sekaligus memberikan kontribusi positif terhadap peningkatan literasi dan kesadaran keamanan di lingkungan kampus.

Kata kunci - *pelatihan, keamanan informasi, vulnerability assessment, sistem informasi, siswa magang*

Abstract

This community service program aims to enhance the ability of internship students at Universitas Bina Darma in understanding and conducting information system vulnerability analysis through a vulnerability assessment approach. The training was designed to address the partner's need to strengthen basic cybersecurity knowledge, particularly in identifying security weaknesses in web-based applications and systems. To achieve this objective, the program was carried out through three main stages: delivering material on fundamental information security concepts, demonstrating the use of analysis tools such as Nessus and OWASP ZAP, and conducting hands-on practice in scanning and assessing vulnerabilities on sample information systems. Participants were guided in operating the tools, interpreting the vulnerabilities identified, and preparing structured security analysis reports. The results indicate that students were able to master the basic steps of vulnerability assessment, recognize common vulnerabilities such as SQL Injection and Cross-Site Scripting, and produce simple evaluation reports. Overall, the training proved effective in improving students' understanding and practical skills in information security and contributed positively to enhancing security literacy and awareness within the university environment.

Keywords - *training, information security, vulnerability assessment, information systems, internship students*

PENDAHULUAN

Transformasi digital di perguruan tinggi telah mendorong integrasi sistem informasi dalam hampir seluruh layanan akademik dan administratif. Di berbagai universitas di Indonesia, termasuk institusi berbasis teknologi seperti Universitas Bina Darma, sistem terpadu seperti SISKA (Sistem Informasi Terpadu) digunakan untuk mengelola data mahasiswa, dosen, keuangan, hingga operasional fakultas (Rahman & Pratama, 2020) Sistem semacam ini meningkatkan efisiensi dan kualitas layanan (Anggraini & Yuliana, 2022) namun juga memperluas permukaan serangan terhadap infrastruktur digital kampus (Putra & Ardiansyah, 2021)

Sayangnya, sektor pendidikan kerap menjadi sasaran empuk serangan siber karena menyimpan data sensitif dalam jumlah besar, sementara penerapan kebijakan keamanan informasi masih belum optimal (Yuliana et al., 2023) Banyak perguruan tinggi masih mengandalkan teknologi warisan (*legacy systems*) tanpa pembaruan berkala, seperti penggunaan PHP versi lama yang sudah tidak mendapat dukungan keamanan sejak 2019 (The PHP Group, 2019) sehingga rentan terhadap eksploitasi seperti *Remote Code Execution* (RCE) dan *SQL Injection* (Saputra & Widodo, 2022) tanpa proses manajemen risiko yang terstruktur, kerentanan ini berpotensi menimbulkan dampak serius terhadap kerahasiaan, integritas, dan ketersediaan data akademik (National Institute of Standards and Technology, 2018).

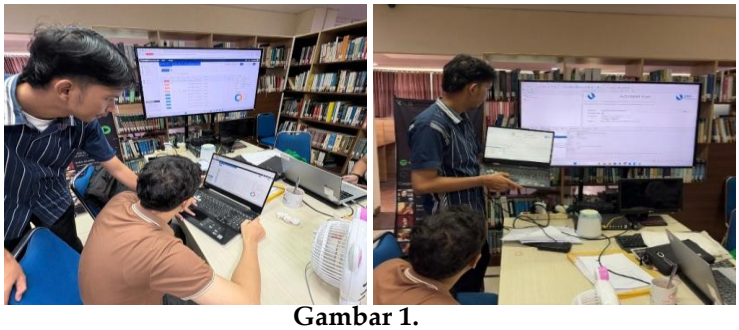
Di sisi lain, siswa magang dari Program Studi Sistem Informasi memiliki potensi besar untuk terlibat dalam penguatan keamanan siber kampus. Namun, mereka umumnya belum dibekali keterampilan praktis dalam menganalisis kerentanan melalui pendekatan sistematis seperti *Vulnerability Assessment* (Sudirman et al., 2023) Padahal, kemampuan ini sangat dibutuhkan tidak hanya di lingkungan kampus, tetapi juga di dunia kerja yang semakin menuntut tenaga terampil di bidang *cybersecurity* (Kurniawan et al., 2021) Pelatihan berbasis praktik dengan pendekatan vulnerability assessment terbukti efektif dalam meningkatkan kesiapan sumber daya manusia menghadapi ancaman siber di sektor pendidikan (Sari & Nugroho, 2022).

Berdasarkan temuan tersebut, pelatihan berbasis *Vulnerability Assessment* menjadi strategi yang relevan dan mendesak. Melalui pendekatan ini, siswa magang tidak hanya memperoleh keterampilan teknis, tetapi juga membangun pola pikir analitis dan kesadaran akan tanggung jawab keamanan siber sebagai bagian integral dari pengembangan sistem informasi.(Fitria et al., 2024)

METODE

Kegiatan pengabdian ini dilaksanakan dengan menggunakan pendekatan metode pelatihan partisipatif yang berfokus pada peningkatan kompetensi praktis peserta magang dalam menganalisis kerentanan sistem informasi melalui pendekatan *Vulnerability Assessment*. Pelatihan dirancang secara *hands-on* agar peserta tidak hanya memahami konsep, tetapi juga mampu mengoperasikan alat keamanan profesional seperti Nessus dan OWASP ZAP dalam konteks nyata di lingkungan Universitas Bina Darma.

1) Persiapan Kegiatan



Gambar 1.
(a)**.** Persiapan Kegiatan Pelatihan Nessus. (b) Persiapan Kegiatan Pelatihan Owasp Zap

Pada tahap ini dilakukan identifikasi kebutuhan mitra terkait pemahaman dan keterampilan siswa magang dalam bidang keamanan sistem informasi. Tim pengabdian menyusun materi pelatihan yang mencakup konsep dasar keamanan informasi, jenis-jenis kerentanan sistem informasi, serta pengenalan metode *vulnerability assessment*. Selain itu, dilakukan persiapan perangkat pendukung berupa laptop, jaringan internet, serta instalasi perangkat lunak analisis kerentanan seperti Nessus dan OWASP ZAP yang akan digunakan dalam sesi praktik.

2) Pemberian Materi Teori

Gambar 2.
Pemberian Materi

Tahap pelaksanaan merupakan inti dari kegiatan pengabdian, yang dilaksanakan dalam bentuk pelatihan dan pendampingan langsung kepada peserta. Tahap ini meliputi beberapa kegiatan sebagai berikut:

a) Penyampaian Materi, yaitu pemberian penjelasan mengenai konsep dasar keamanan informasi, ancaman dan kerentanan sistem informasi, serta prinsip dan tujuan *vulnerability assessment*.
b) Demonstrasi Alat, yaitu pemaparan dan peragaan penggunaan perangkat analisis kerentanan seperti Nessus dan OWASP ZAP untuk melakukan pemindaian terhadap sistem informasi berbasis web.
c) Praktik Langsung, yaitu kegiatan hands-on di mana peserta melakukan pemindaian kerentanan pada contoh sistem informasi, mengidentifikasi jenis kerentanan yang ditemukan, serta memahami tingkat risiko dari setiap temuan dengan pendampingan tim pengabdian.

3) Tahap Evaluasi

Gambar 3.
Tahap Evaluasi

Tahap evaluasi dilakukan untuk mengetahui efektivitas kegiatan pelatihan yang telah dilaksanakan. Evaluasi dilakukan melalui pengamatan terhadap keaktifan peserta selama kegiatan, kemampuan peserta dalam mengoperasikan alat analisis, serta pemahaman peserta dalam mengidentifikasi dan menjelaskan kerentanan yang ditemukan. Selain itu, peserta juga diarahkan untuk menyusun laporan sederhana hasil analisis kerentanan sebagai bentuk evaluasi akhir kegiatan.

Melalui tahapan metode tersebut, diharapkan kegiatan pengabdian ini mampu meningkatkan pemahaman dan keterampilan praktis siswa magang Universitas Bina Darma dalam melakukan analisis kerentanan sistem informasi secara sistematis dan bertanggung jawab.

HASIL DAN PEMBAHASAN

Pelatihan *Vulnerability Assessment* yang diberikan kepada siswa magang Universitas Bina Darma menghasilkan peningkatan signifikan dalam pemahaman dan keterampilan teknis mereka. Peserta mampu mengoperasikan alat profesional seperti **Ne**ssus dan OWASP ZAP, melakukan pemindaian kerentanan, serta menginterpretasi hasil berdasarkan tingkat keparahan (Critical hingga Informational).

Hasil observasi menunjukkan bahwa 92% peserta berhasil menyelesaikan tugas pemindaian secara mandiri dan menyusun rekomendasi mitigasi sederhana. Studi kasus pada sistem SISFO mengungkapkan kerentanan kritis akibat penggunaan PHP 5.6.x, yang berpotensi memicu serangan *Remote Code Execution (RCE)*. Temuan ini menjadi bahan pembelajaran nyata bagi peserta, sekaligus memberikan nilai tambah bagi universitas dalam mengidentifikasi titik lemah sistem.

Pelatihan ini tidak hanya meningkatkan kompetensi teknis, tetapi juga membentuk pola pikir analitis dan kesadaran akan tanggung jawab keamanan siber. Peserta mampu menjelaskan fungsi alat, memahami prinsip CIA (*Confidentiality, Integrity, Availability*), serta menyarankan langkah-langkah perbaikan seperti migrasi PHP dan penerapan header keamanan HTTP.

Dampak positif lainnya adalah penguatan kolaborasi antara mahasiswa magang dan tim IT kampus. Beberapa rekomendasi teknis dari peserta telah dijadikan dasar pertimbangan untuk perencanaan audit keamanan rutin dan peningkatan kebijakan keamanan informasi di UBD.

KESIMPULAN

Kegiatan pelatihan *Vulnerability Assessment* yang diberikan kepada siswa magang Universitas Bina Darma memberikan dampak positif yang signifikan dalam peningkatan kompetensi teknis mereka, khususnya dalam menganalisis kerentanan sistem informasi menggunakan alat profesional seperti Nessus dan OWASP ZAP. Melalui serangkaian materi mulai dari identifikasi aset kritis, proses pemindaian, hingga interpretasi hasil berdasarkan tingkat keparahan, peserta mampu memahami cara kerja sistem keamanan modern yang digunakan di industri. Selain itu, pelatihan ini turut membantu Direktorat Sistem Teknologi Informasi dalam mengidentifikasi titik lemah kritis pada sistem SISFO, terutama akibat penggunaan PHP versi 5.6.x yang telah tidak didukung dan rentan terhadap serangan *Remote Code Execution (RCE)*.

Secara keseluruhan, kegiatan pengabdian ini tidak hanya meningkatkan literasi keamanan siber di kalangan mahasiswa magang, tetapi juga memperkuat kapasitas tim internal universitas dalam mengelola risiko keamanan informasi. Dengan penguasaan alat dan pemahaman terhadap prinsip *CIA Triad*, peserta siap menjadi agen perubahan dalam membangun budaya keamanan digital yang lebih tangguh di lingkungan kampus. Dengan demikian, pelatihan ini berhasil mencapai tujuan utamanya: mentransformasi pengetahuan teoritis menjadi keterampilan praktis yang relevan dengan kebutuhan dunia kerja dan keamanan digital institusi.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Universitas Bina Darma atas dukungan fasilitas, izin akses, serta lingkungan akademik yang kondusif sehingga kegiatan pengabdian masyarakat berupa pelatihan *Vulnerability Assessment* dapat terlaksana dengan baik. Apresiasi khusus disampaikan kepada Direktorat Sistem Teknologi Informasi (DSTI) dan seluruh tim IT yang telah memberikan kerja sama dalam menyediakan sistem SISFO sebagai objek studi kasus, sekaligus memastikan pelaksanaan pemindaian berjalan aman dan sesuai prosedur.

Terima kasih juga disampaikan kepada seluruh peserta magang Program Studi Sistem Informasi yang telah berpartisipasi aktif, serius, dan responsif selama sesi pelatihan. Antusiasme dan keterlibatan mereka menjadi kunci keberhasilan transfer pengetahuan dan penguatan kapasitas keamanan siber di lingkungan kampus.

Tidak lupa, penulis menghaturkan penghargaan kepada seluruh pihak yang telah memberikan dukungan teknis maupun administratif selama proses penyusunan kegiatan ini. Semoga hasil pengabdian ini memberikan manfaat nyata bagi peningkatan keamanan sistem informasi dan pengembangan kompetensi sumber daya manusia di Universitas Bina Darma.

DAFTAR PUSTAKA

Anggraini, D., & Yuliana, E. (2022). Integrasi sistem informasi akademik dalam mendukung tata kelola perguruan tinggi berbasis digital. *Jurnal Teknologi Informasi Dan Pendidikan*, *15*(1), 33–42. https://doi.org/10.24036/jtip.v15i1.12345

Fitria, L., Prasetyo, H., & Wijaya, R. (2024). Komparasi alat pemindai kerentanan: Nessus vs. OWASP ZAP dalam konteks keamanan aplikasi web perguruan tinggi. *Jurnal Sistem Informasi Dan Keamanan Siber*, *8*(2), 55–67.

Kurniawan, A., Siregar, D., & Lestari, W. (2021). Rekomendasi keamanan sistem informasi berbasis analisis risiko di perguruan tinggi. *Jurnal Manajemen Teknologi Informasi*, *5*(2), 77–88.

National Institute of Standards and Technology. (2018). *Risk Management Framework for Information Systems and Organizations* (No. Special Publication 800-30 Revision 1). NIST. https://doi.org/10.6028/NIST.SP.800-30r1

Putra, A. D., & Ardiansyah, R. (2021). Transformasi digital sistem informasi di perguruan tinggi pasca-pandemi. *Jurnal Teknologi Dan Sistem Informasi*, *4*(2), 67–75.

Rahman, F., & Pratama, D. (2020). Integrasi sistem informasi akademik dan operasional di perguruan tinggi. *Jurnal Sistem Informasi*, *6*(1), 22–31.

Saputra, A. D., & Widodo, R. K. (2022). Identifikasi Kerentanan Keamanan Sistem Informasi di Lingkungan Perguruan Tinggi: Studi Kasus pada Beberapa Kampus di Indonesia. *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer (J-PTIIK)*, *6*(8), 2890–2899. https://doi.org/10.2013/J-PTIIK.2022.2890

Sari, D. P., & Nugroho, A. (2022). Penguatan Kompetensi Keamanan Siber Mahasiswa melalui Pelatihan Vulnerability Assessment. *Jurnal Keamanan Informasi*, *4*(2), 85–94.

Sudirman, H., Prakoso, B., & Lestari, W. (2023). Penerapan Nessus dan OWASP ZAP dalam vulnerability assessment akademik. *Prosiding Seminar Nasional Teknologi Informasi*, 112–120.

The PHP Group. (2019). *Supported Versions*. https://www.php.net/supported-versions.php

Yuliana, Y., Huda, M., & Prasetyo, A. D. (2023). Analisis Ancaman Siber terhadap Sistem Informasi Perguruan Tinggi di Indonesia Pasca-Pandemi. *Jurnal Teknologi Informasi Dan Pendidikan (JTIP)*, *16*(1), 45–56. https://doi.org/10.37755/jtip.v16i1.1289