ANALISIS KEAMANAN APLIKASI BERBASIS WEB DI UNIVERSITAS HARAPAN BANGSA MENGGUNAKAN PTES

Anggit Wirasto[1], Dinar Mustofa[2]

[1]Universitas Harapan Bangsa, Jl. Raden Patah No. 100, Kedunglongsir, Ledug, Kembaran, Banyumas
[2]Universitas Amikom Purwokerto, Jl. Letjen Pol Soemarto Watumas, Purwanegara, Purwokerto Utara, Banyumas

Email: [1]anggitwirasto@uhb.ac.id, [2]dinar.mustofa@amikompurwokerto.ac.id

ABSTRAK

Instansi pemerintahan dan institusi pendidikan telah menjadi target utama dari serangan siber. Serangan yang berhasil dapat memberikan kerugian bagi instansi yang menjadi target. Perlu dilakukan suatu tindakan analisis keamanan aplikasi berbasis web secara rutin sebagai wujud tindakan pencegahan. Penelitian ini melakukan tindakan analisis keamanan aplikasi berbasis web pada institusi pendidikan menggunakan metode *Penetration Testing Execution Standard* dan aplikasi *free and open source* Amass, Sudomy, dan OWASP ZAP. Hasil penelitian adalah ditemukannya potensi celah keamanan pada sistem informasi yang terpasang di Universitas Harapan Bangsa, serta tindakan yang dapat dilakukan sebagai upaya pencegahan.

Keywords: *web defacement, penetration testing, vulnerability identification, information gathering, PTES*

ABSTRACT

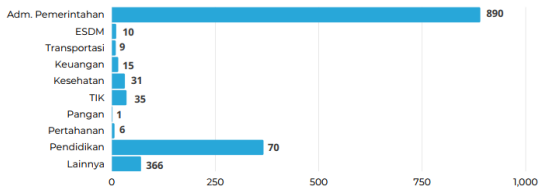
Government agencies and educational institutions have become the primary targets of cyberattacks. Successful attacks can lead to significant losses for the targeted entities. It is necessary to conduct routine security analysis of web-based applications as a preventive measure. This research undertakes a security analysis of web-based applications in educational institutions using the Penetration Testing Execution Standard method and the free and open-source applications Amass, Sudomy, and OWASP ZAP. The research findings reveal potential security vulnerabilities in the information systems deployed at Universitas Harapan Bangsa, along with recommended preventive measures..

Keywords: *web defacement, penetration testing, vulnerability identification, information gathering, PTES*

1. PENDAHULUAN

Seiring dengan semakin tingginya tingkat pemanfaatan Teknologi Informasi dan Komunikasi (TIK), jumlah serangan siber juga akan semakin meningkat. Badan Siber dan Sandi Negara (BSSN) melaporkan sepanjang 2022 telah menerima sebanyak total 1.433 notifikasi indikasi insdiden. Sektor terbanyak adalah administrasi pemerintahan sejumlah 890 kasus dan sektor pendidikan sebanyak 70 kasus, dan jenis serangan terbanyak adalah pada aplikasi web dengan jumlah 933 kasus seperti ditunjukkan pada Gambar 1 [1].

Salah satu bentuk serangan terhadap aplikasi web adalah *web defacement*, yaitu penggantian konten website dengan gambar dan teks yang disiapkan oleh penyerang [2]. Serangan *web defacement* umumnya tidak sampai merusak atau menghilangkan data penting, meskipun demikian *web defacement* dapat menyebabkan kerugian karena biaya yang ditimbulkan untuk memulihkan situs web, layanan yang terhenti sementara situs web mengalami *downtime*, dan penurunan reputasi [3].



Gambar 1. Sektor yang mendapat serangan siber sepanjang tahun 2022

Serangan *web defacement* pada suatu situs menjadi indikasi adanya celah kerentanan pada situs. Celah tersebut memungkinkan untuk terjadinya bentuk serangan lain seperti pencurian data, penyisipan *MiningPool*, *Trojan*, *Ransomware*, sampai penghapusan data [4].

Universitas Harapan Bangsa (UHB) yang terletak di Kabupaten Banyumas, Jawa Tengah, tidak luput dari serangan kepada aplikasi web yang dimilikinya. Divisi Teknologi dan Sistem Informasi (DTSI) UHB melaporkan bahwa di tahun 2023 telah terjadi dua kali serangan yang cukup masif pada bulan Maret dan Juni. Serangan pada bulan Juni berupa penyisipan halaman judi slot pada semua aplikasi web. Kejadian ini menyebabkan aplikasi-aplikasi web tersebut terpakasa di-*takedown* untuk sementara untuk memudahkan penanganan dan mengurangi risiko serangan lanjutan [5].

Pendeteksian celah keamanan sangat diperlukan untuk mencegah terjadinya serangan di masa mendatang, agar layanan yang diberikan tidak sampai terhenti dan terhindar dari risiko kehilangan data. Penelitian ini berfokus pada pengujian aplikasi berbasis web di UHB menggunakan panduan yang mengadopsi metode *Penetration Testing Execution Standard* (PTES).

2. TINJAUAN PUSTAKA

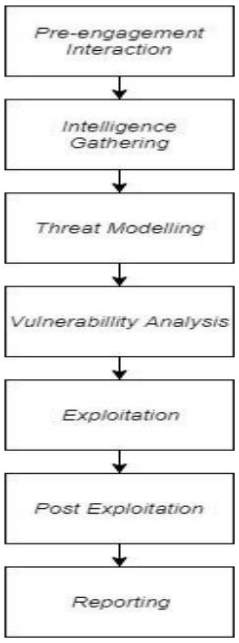
Terdapat beberapa penelitian terkait yang membahas mengenai analisis keamanan aplikasi web dan metodologinya. Penelitian yang dilakukan oleh Sanjaya dkk [6] bertujuan untuk mengetahui celah keamanan website lembaga X menggunakan metode *penetration testing* dengan menggunakan kerangka pengujian *The Information System Seurity Assessment Framework* (ISSAF).

Penelitian berikutnya oleh Hariyadi dan Nastiti [7] melakukan analisis keamanan sistem informasi di Universitas Duta Bangsa Surakarta dengan menggunakan Sudomy dan OWASP ZAP. Fauzan dan Syukhri [8] melakukan analisis metode PTES pada aplikasi *e-Learning* di Universitas Negeri Padang. Nurbojatmiko dkk melakukan analisis kerentanan website *crowdfunding* syariah menggunakan OWASP ZAP [9].

2.1 *Penetration Testing Execution Standard*

Penetration testing merupakan pendekatan yang umum digunakan dalam mengidentifikasi potensi kerentanan dan celah keamanan dalam sistem komputer dan jaringan. *Penetration Testing Execution Standard* (PTES) adalah suatu kerangka kerja yang digunakan dalam dunia keamanan komputer untuk mengarahkan dan mengatur pelaksanaan *penetration testing* dengan metode yang terstruktur dan komprehensif.

PTES pertama kali diperkenalkan pada tahun 2010 oleh sekelompok pakar keamanan yang bertujuan untuk mengatasi kebutuhan akan panduan yang lebih terstruktur dalam melaksanakan *penetration testing.* PTES membantu praktisi keamanan untuk mengidentifikasi dan mengevaluasi potensi kerentanan dalam sistem komputer dan jaringan, serta memberikan rekomendasi mitigasi yang sesuai. PTES memiliki tujuh fase yaitu: *pre-engagement interactions, intelligence gathering, threat modeling, vulnerability analysis, exploitation, post exploitation,* dan *reporting* [10].



Gambar 2. Fase dalam PTES

2.2 OWASP ZAP

OWASP *Zed Attack Proxy* (OWASP ZAP) adalah alat *penetration testing open-source* yang dirancang untuk membantu praktisi keamanan dalam mengidentifikasi dan mengatasi potensi kerentanan keamanan dalam aplikasi web. OWASP ZAP pertama kali diperkenalkan oleh *Open Worldwide Application Security Project* (OWASP) sebagai proyek *open source* untuk membantu pengembang dan praktisi keamanan dalam menguji keamanan aplikasi web. Tujuan utama

dari OWASP ZAP adalah untuk memudahkan identifikasi dan mitigasi kerentanan keamanan pada aplikasi web sejak tahap pengembangan awal hingga tahap produksi [11].

3. METODE PENELITIAN

Analisis keamanan aplikasi web dalam penelitian ini diawali dengan studi literatur mengenai pengujian yang akan dilakukan, serta melakukan diskusi dengan pihak pengelola aplikasi. Selanjutnya *penetration testing* dilakukan menggunakan langkah-langkah dari PTES. Secara lengkap PTES terdiri dari tujuh fase yaitu:

a. *Pre-engagement Interactions*: Langkah ini melibatkan komunikasi antara peneliti sebagai tim *penetration testing* dan DTSI UHB sebagai klien untuk memahami tujuan uji, jangkauan, batasan, dan ekspektasi hasil.
b. *Intelligence Gathering*: Pada langkah ini, peneliti akan mengumpulkan informasi tentang target, termasuk informasi publik, data WHOIS, alamat IP, dan lainnya.
c. *Threat Modeling*: Proses ini melibatkan analisis tentang bagaimana serangan mungkin terjadi dan dampaknya terhadap target.
d. *Vulnerability Analysis*: Tahap ini melibatkan identifikasi dan analisis potensi kerentanan dalam sistem.
e. *Exploitation*: Pada tahap ini, peneliti mencoba mengeksploitasi kerentanan yang ditemukan untuk memvalidasi apakah celah tersebut dapat dimanfaatkan oleh penyerang.
f. *Post Exploitation*: Setelah penetrasi berhasil, tahap ini melibatkan eksplorasi lebih lanjut untuk mencari informasi sensitif dan akses ke sistem lain.
g. *Reporting*: Hasil *penetration testing* akan dirangkum dalam laporan yang mencakup temuan, rekomendasi perbaikan, dan bukti pendukung.

Perangkat yang digunakan dalam penelitian ini adalah sebagai berikut:

- Laptop dengan OS Kali Linux
- Aplikasi Amass
- Aplikasi Sudomy
- Aplikasi OWASP ZAP

4. PEMBAHASAN

4.1 *Pre-engagement Interactions*

Fase ini merupakan fase persiapan dengan kegiatan berupa diskusi antara peneliti dan DTSI UHB. Hal-hal yang didiskusikan adalah kesepakatan mengenai tujuan pengujian, jangkauan dan batasan pengujian, serta hasil yang diharapkan. Karena menyangkut keamanan sistem, pada fase ini juga dilakukan kesepakatan mengenai batasan detail informasi yang boleh disampaikan secara terbuka sebagai artikel laporan hasil penelitian.

4.2 *Intelligence Gathering*

Fase kedua merupakan pencarian informasi tentang domain yang diteliti, yaitu uhb.ac.id. Berikut adalah hasil pencarian menggunakan WHOIS:

Tabel 1. Hasil pencarian WHOIS uhb.ac.id

Domain ID	PANDI-DO1026356
Nama Domain	uhb.ac.id
Dibuat	2018-10-04 05:11:55
Terakhir Diperbarui	2022-09-25 09:41:15
Tanggal Kadaluarsa	2024-10-04 23:59:59
Status	*server transfer prohibited* *client transfer prohibited*

Tahapan selanjutnya adalah melakukan penelusuran sub-domain yang dikelola UHB menggunakan aplikasi Amass. Hasil pemindaian berupa daftar sub-domain beserta alamat IP dengan status aktif berdasarkan *ping sweep* dan HTTP Status dengan kode 200.

Tabel 2. Daftar sub-domain hasil pemindaian Amass

IP Address	Domain/Sub-domain
119.252.160.138	api.uhb.ac.id
	inventaris.uhb.ac.id
	icch.uhb.ac.id
	cbt.uhb.ac.id
	helpdesk.uhb.ac.id
	khip.uhb.ac.id
	alumni.uhb.ac.id
	ejournal.uhb.ac.id
	library.uhb.ac.id
	komite.lppm.uhb.ac.id
	jurnal.uhb.ac.id
	invertaris.uhb.ac.id

	kemahasiswaan.uhb.ac.id
	cbt-dashboard.uhb.ac.id
	lppm.uhb.ac.id
	konsultasi-jurusan.uhb.ac.id
	lpm.uhb.ac.id
	p2b.uhb.ac.id
	pkkmb.uhb.ac.id
	prosiding.uhb.ac.id
	presensi.uhb.ac.id
	penerbit.uhb.ac.id
	perpustakaan.uhb.ac.id
	pmdk.uhb.ac.id
	seminar.uhb.ac.id
	semnas.uhb.ac.id
	repository.uhb.ac.id
	sertifikat.uhb.ac.id
	siska.uhb.ac.id
	sisiran.uhb.ac.id
	uhb.ac.id
	sso.uhb.ac.id
	sipmas2.uhb.ac.id
	sipmas.uhb.ac.id
	yahoomail.uhb.ac.id
	sisterdikti.uhb.ac.id
	uhbpress.uhb.ac.id
	siwalan.uhb.ac.id
119.252.160.140	akuntansi.scalsa.uhb.ac.id
	ilkom.scalsa.uhb.ac.id
	hukum.scalsa.uhb.ac.id
	manajemen.scalsa.uhb.ac.id
	sisinfo.scalsa.uhb.ac.id
	tekinfo.scalsa.uhb.ac.id
119.252.160.142	fis.scalsa.uhb.ac.id
	fst.scalsa.uhb.ac.id
128.199.226.204	eprints.uhb.ac.id
202.162.209.227	helper.siakad.uhb.ac.id
	siakad.uhb.ac.id
202.162.209.228	pbi.scalsa.uhb.ac.id
	scalsa.uhb.ac.id
104.21.82.207	www.uhb.ac.id
139.59.117.244	pmb.uhb.ac.id

4.3 *Threat Modeling*

Fase berikutnya adalah menganalisis serangan yang mungkin terjadi dan memperkirakan dampaknya terhadap target. Analisis ini memanfaatkan info aplikasi yang disediakan pihak UHB, seperti info bahasa pemrograman, *framework* pemrograman, dan fitur aplikasi. Hasil analisis adalah sebagai berikut:

Tabel 3. Jenis serangan dan dampak yang mungkin terjadi

Jenis Serangan	Dampak
Cross-Site Scripting (XSS)	Pencurian informasi, manipulasi tampilan halaman, pencurian sesi pengguna
SQL Injection	Akses data, perubahan data, penghapusan data, pencurian informasi, kerusakan sistem
Cross-Site Request Forgery	Perubahan data, penghapusan data
Broken Authentication	Pencurian kredensial, akses tidak sah, manipulasi data

4.4 *Vulnerability Analysis*

Fase ini merupakan pengidentifikasian kerentanan pada sistem menggunakan OWASP ZAP dengan sumber data yang telah diperoleh pada tahap sebelumnya. Pemindaian target menggunakan aturan OWASP ZAP yang mendasar (*default scan policy*) yaitu: *Cross-Site Scripting, HTTAccess Information Leak, Directory Browsing, ELMAH Information Leak, Source Code Disclosure, Buffer Overflow, CLRF Injection, Cross Site Scripting, Forma String Error, Parameter Tampering, Remote OS Command Injection, Server Side Code Injection, SQL Injection, External Redirect, Script Active Scan Rules, SOAP Action Spoofing, SOAP XML Injection, Path Traversal,* dan *Remote File Inclusion.* Hasil dari analisis menunjukkan beberapa celah kerentanan terhadap sejumlah aplikasi yang ada di UHB.

4.5 *Exploitation dan Post Exploitation*

Fase berikutnya merupakan percobaan eksploitasi terhadap kerentanan yang ditemukan dari fase *vulnerability analysis* untuk memvalidasi apakah celah tersebut dapat dimanfaatkan oleh penyerang. Hasil percobaan

menunjukkan sebagian besar celah kerentanan dapat dieksploitasi dengan teknik yang sesuai. Salah satunya adalah peneliti berhasil masuk ke dalam sistem server dan melakukan eksplorasi lebih lanjut dengan melakukan *privilege escalation* sebagai *root user*.

4.6 *Reporting*

Hasil dari keseluruhan tahapan *penetration testing* disampaikan dalam bentuk laporan tertulis yang mencakup detail temuan, rekomendasi perbaikan dan pencegahan, serta bukti pendukung dalam bentuk *screenshot*. Secara keseluruhan aplikasi web di UHB sudah cukup aman, dengan hanya tiga aplikasi yang memiliki risiko kemanan tinggi, 14 aplikasi dengan risiko keamanan sedang, dan 46 aplikasi dengan risiko rendah.

Tabel 4. Tingkat risiko keamanan aplikasi di UHB

Tingkat Risiko Keamanan	Jumlah Aplikasi
Tinggi	3
Sedang	14
Rendah	46

Aplikasi yang dibuat sebagian besar menggunakan *framework* pemrograman yang populer sehingga sudah memiliki fitur keamanan yang cukup bagus dan bisa mencegah upaya XSS, *SQL Injection*, CSRF, dan *Broken Authentication*. Namun yang perlu diperhatikan adalah pemasangan aplikasi harus sudah dalam mode *production* bukan *development* sehingga apabila terjadi *error* tidak menampilkan *credentials* yang umumnya muncul dalam mode *debugging*. Di sisi lain terkadang *framework* populer masih memiliki celah keamanan yang informasinya dapat tersebar dengan cepat, sehignga pengelola program harus selalu memantau berita terbaru dan melakukan *update* secara berkala.

Faktor kelemahan terbesar yang ditemukan adalah penggunaan *password* yang mudah ditebak (*easily guessable credentials*) sehingga rentan terhadap serangan *brute force*. Hal ini dapat dicegah dengan menerapkan aturan pembuatan *password* yang kompleks dan menambahkan validasi pada saat pembuatan *password* di aplikasi sehingga memaksa pengguna membuat *password* yang kompleks.

Celah kelemahan lain yang ditemukan adalah satu server yang dipasang hingga 41 aplikasi. Apabila ada satu aplikasi yang berhasil dibobol dan penyerang dapat masuk ke dalam server serta melakukan *privilege escalation* maka aplikasi-aplikasi lainnya dalam blok server yang sama menjadi terancam juga. Pihak UHB perlu mengembangkan skema *backup* kode sumber dan data di tempat yang terpisah sebagai langkah antisipasi apabila terjadi serangan yang menyebabkan hilangnya data-data penting.

5. KESIMPULAN

Berdasarkan data dari BSSN instansi pemerintahan dan institusi pendidikan telah menjadi target utama dari serangan siber. Hal ini perlu menjadi perhatian utama dari para pengelola sistem informasi di institusi tersebut. Sebab serangan terhadap sistem informasi dapat menyebabkan kerugian dari skala ringan sampai berat seperti hilangnya data. Analisis terhadap keamanan sistem informasi wajib dilakukan secara rutin untuk mencegah serangan yang dapat terjadi.

Metode PTES telah berhasil digunakan untuk menganalisis keamanan aplikasi berbasis web di Universitas Harapan Bangsa. Perangkat yang digunakan, yakni OS Kali Linux dengan aplikasi Amass, Sudomy, dan OWASP ZAP cukup dapat dihandalkan dalam melakukan tahapan-tahapan yang ada dalam metode PTES. Aplikasi-aplikasi tersebut bersifat gratis dan *open source* sehingga dapat menekan biaya yang perlu dikeluarkan dalam melakukan analisis keamanan sistem informasi.

DAFTAR PUSTAKA

[1] BSSN, “Lanskap Keamanan Siber Indonesia 2022,” Jakarta, 2022.

[2] M. Albalawi, R. Aloufi, N. Alamrani, N. Albalawi, A. Aljaedi, and A. R. Alharbi, “Website Defacement Detection and Monitoring Methods: A Review,” *Electronics*, vol. 11, no. 21, p. 3573, 2022, doi: https://doi.org/10.3390/electronics11213573.

[3] S. G. A. van de Weijer, T. J. Holt, and E. R. Leukfeldt, “Heterogeneity in trajectories of cybercriminals: A longitudinal analyses of web defacements,” *Comput. Hum. Behav. Reports*, vol. 4, p. 100113, Aug. 2021, doi: 10.1016/J.CHBR.2021.100113.

[4] H. Abusaimeh, “Security Attacks in Cloud Computing and Corresponding Defending

Mechanisms," *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 9, no. 3, pp. 4141–4148, 2020, doi: https://doi.org/10.30534/ijatcse/2020/243932020.

[5] DTSIUHB, "Laporan Kinerja Tahunan DTSI UHB 2022/2023," 2023.

[6] I. G. A. S. Sanjaya, G. M. A. Sasmita, and D. M. S. Arsa, "Evaluasi Keamanan Website Lembaga X Melalui Penetration Testing Menggunakan Framework ISSAF," *J. Ilm. Merpati (Menara Penelit. Akad. Teknol. Informasi)*, vol. 8, no. 2, pp. 113–124, Jul. 2020, doi: 10.24843/JIM.2020.V08.I02.P05.

[7] D. Hariyadi, F. Ely Nastiti, A. Yani Yogyakarta, and P. Widya Adijaya Nusantara, "Analisis Keamanan Sistem Informasi Menggunakan Sudomy dan OWASP ZAP di Universitas Duta Bangsa Surakarta," *J. Komtika (Komputasi dan Inform.*, vol. 5, no. 1, pp. 35–42, Jul. 2021, doi: 10.31603/KOMTIKA.V5I1.5134.

[8] F. Y. Fauzan and S. Syukhri, "Analisis Metode Web Security PTES (Penetration Testing Execution And Standart) Pada Aplikasi E-Learning Universitas Negeri Padang," *Voteteknika (Vocational Tek. Elektron. dan Inform.*, vol. 9, no. 2, pp. 105–111, Jun. 2021, doi: 10.24036/VOTETEKNIKA.V9I2.111778.

[9] Nurbojatmiko, A. Lathifah, F. Bil Amri, and A. Rosidah, "Security Vulnerability Analysis of the Sharia Crowdfunding Website Using OWASP-ZAP," *2022 10th Int. Conf. Cyber IT Serv. Manag. CITSM 2022*, 2022, doi: 10.1109/CITSM56380.2022.9935837.

[10] PTES, "PTES Technical Guidelines." http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines (accessed Aug. 19, 2023).

[11] D. Sagar, S. Kukreja, J. Brahma, S. Tyagi, and P. Jain, "STUDYING OPEN SOURCE VULNERABILITY SCANNERS FOR VULNERABILITIES IN WEB APPLICATIONS," *IIOAB J.*, vol. 9, pp. 43–49, 2018, Accessed: Aug. 20, 2023. [Online]. Available: www.iioab.org

.