VULNERABILITY ASSESSMENT DAN PENETRATION TEST PADA WEBSITE MA/MTS HUSNUL KHATIMAH KUNINGAN

Mohamad Fathurahman[1)], Zulhelman[2)], dan Abdul Aziz[3)]

[1,2]Jurusan Teknik Elektro, Politeknik Negeri Jakarta
[3]Jurusan Teknik Informatika dan Komputer, Politeknik Negeri Jakarta
E-mail: mohamad.fathurahman@elektro.pnj.ac.id

Abstract

The internet facility employed almost every field of work and people have become dependent on it. Concerns about information security have increased including the world of education especially during this pandemic, is done via the internet. That's why the element of security is so important for any website. Attention to web security is very high carried out by government agencies, educational institutions, and the financial sector. If the stored data can be hacked then hackers can use the data illegally and can lead to crime. It is important to test the security of web applications by conducting penetration tests to identify web application vulnerabilities and actions taken by hackers. This research will focus on web application security. The output of the vulnerability test is in the form of a report that contains a description of the vulnerabilities that exist on the website. Through the analysis of the output of the vulnerability assessment, it is possible to improve the security of the site and then test it again with a penetration test. Through the identification of web security vulnerabilities, improvements had been made to increase the security level of the application website until it reaches a low level.

Keywords: *security, hacking, Penetration Test, website, Vulnerability Assessment*

PENDAHULUAN

Berdasarkan riset platform manajemen media sosial HootSuite dan agensi marketing sosial We Are Social bertajuk Global Digital Reports 2020, yang dirilis akhir Januari lalu, sudah lebih dari setengah jumlah populasi, yaitu sebesar 64 persen penduduk Indonesia terkoneksi dengan internet(We Are Social, 2021). Bahkan, situasi pandemi korona diyakini menjadi salah satu pendorong adopsi penggunaan internet nasional mengalami pertumbuhan yang lebih masif lagi dalam 6 bulan terakhir. Tak heran jika potensi kebocoran data juga semakin membesar.

Di dunia pendidikan pun tak lepas dari penggunaan internet. Sejak dimulai pandemi Covid 19 tahun lalu, metode pembelajaran di sekolah, kampus maupun di pondok pesantren beralih ke pembelajaran jarak jauh (PJJ). Metode PJJ ini sangat mengandalkan penggunaan internet sebagai sarana utama. Beberapa sekolah dan pondok pesantren banyak juga yang menggunakan aplikasi *Learning Management*

System (LMS) untuk aplikasi pembelajaran jarak jauhnya. Disamping memudahkan dalam proses belajar mengajar, meode PJJ ini juga menimbulkan celah baru dalam hal aksi kejahatan siber. Selain diretas untuk konten pornografi (Dio Prasasti, 2020), data yang diinput oleh user juga berpotensi diretas dan disalahgunakan salah satunya yang menimpa Edmodo, salah satu aplikasi LMS yang terkenal, pada tahun 2017 mereka menjadi korban peretasan. Data milik 77 juta pengguna bocor, termasuk username, password dan alamat email. Karena semua password di-hash dan dienkripsi menggunakan algoritma bcrypt, upaya untuk mendekripsi semua password akan membutuhkan kerja yang sangat besar. Berdasarkan audit eksternal yang dilakukan oleh Edmodo, tidak ada laporan tentang data sekolah atau identitas yang terkena dampak (Maulita Putri, 2019).

Pondok Pesantren Husnul Khotimah Kuningan yang menaungi MTs dan MA Husnul Khotimah, dalam proses belajar mengajar juga menerapkan metode PJJ di masa pandemi saat ini. Aplikasi PJJ yang digunakan adalah e-learnng berbasis website. Pada hari Rabu 24 Maret 2021 lalu, website elearning MTs dan MA Husnul Khotimah mengalami peretasan dan proses PJJ sempat terganggu selama 4 hari. Jenis serangan yang dialami adalah defacement website, yakni serangan di mana pihak jahat meretas situs web dan mengganti konten di situs dengan pesan mereka sendiri. Pesan tersebut dapat menyampaikan pesan politik atau agama, sumpah serapah, atau konten tidak pantas lainnya yang akan mempermalukan pemilik situs web, atau pemberitahuan bahwa situs web telah diretas oleh grup peretas tertentu (Imperva, 2021). Oleh karena itu, saat ini sangat mendesak untuk dilakukan vulnerability assessment dan penetration testing terhadap website aplikasi khususnya elearning MTs/MA Husnul Khotimah guna mengetahui celah-celah apa saja yang dapat ditembus oleh peretas untuk selanjutnya diperbaiki agar supaya serangan peretas dapat dicegah dan ditanggulangi.

Tujuan Program

Program Kegiatan kepada Masyarakat yang dilaksanakan bertujuan untuk:

1. Menganalisa hasil *vulnerability assessment dan penetration test* (VAPT) yang dituangkan ke dalam *report* hasil pengujian;
2. Mengidentikasi celah-celah keamanan apa saja yang ada hasil dari Analisa *report* VAPT;

3. Memberi saran dan melakukan perbaikan atau menutup seoptimal mungkin celah-celah keamanan yang ada guna meningkatkan keamanan website aplikasi pondok pesantren dan elearning MTs dan MA Husnul Khotimah, dan menurunkan *security risk* dari website aplikasi menjadi rendah (*low*).

Gambar 1 Pondok Pesantren Khusnul Khotimah

Deskripsi Program

Program pengabdian kepada masyarakat ini dilaksanakan karena ada kejadian peretasan website elearning MTs dan MA Husnul Khotimah yang sangat mengganggu proses PJJ yakni pada hari Rabu 24 Maret 2021. Guna mencegah kejadian serupa terjadi lagi dimasa yang akan datang, maka perlu dilakukan pengujian terhadap website aplikasi dengan menggunakan metode Penetration Testing Execution Standard, atau dikenal juga dengan VAPT. Luaran dari pengujian VAPT ini adalah berupa reporting yang berisi tentang konfigurasi dan tingkat kerentanan dari website. Dalam kegiatan pengabdian kali ini, dari report yang dihasilkan dari proses assessmen (VAPT) akan dianalisa kemudian diidentifikasi celah-celah keamanan apa saja yang ada untuk kemudian dibemberikan saran dan dilakukan perbaikan atau menutup seoptimal mungkin celah-celah keamanan yang ada guna meningkatkan keamanan website aplikasi pondok pesantren dan elearning MTs dan MA Husnul Khotimah. Kegiatan ini seiring dengan regulasi Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik pasal 25 mengatur tentang hak kekayaan intelektual, termasuk diantaranya website aplikasi, dan dilindungi oleh undang-undang. Pemilik hak kekayaan

intelektual ini dapat mengajukan gugatan atas kerugian yang ditimbulkan sesuai pasal 26 ayat 2 (RI, 2008).

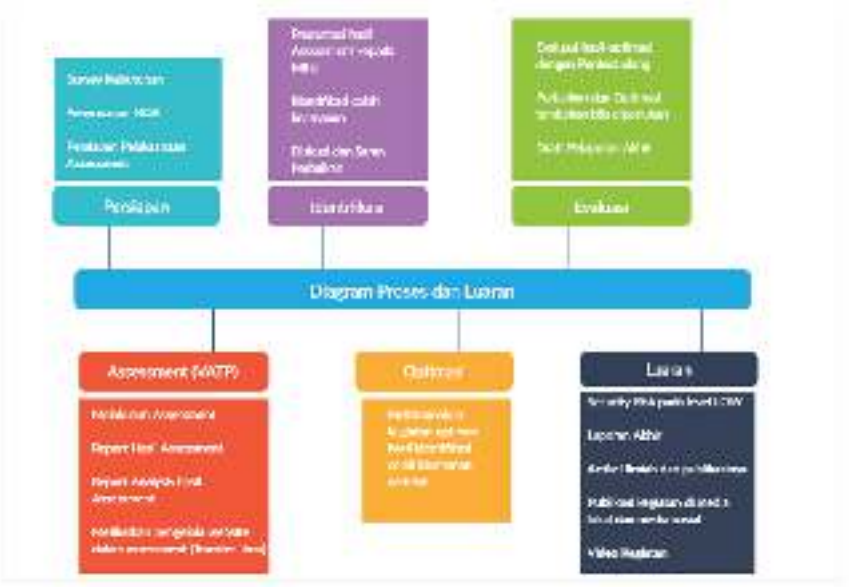
METODE PENELITIAN

Penilaian Kerentatan keamanan (*vulnerability assessment*) adalah proses utama perbaikan menuju kepada kematangan dan intergrasi sistem keamanan informasi. Sedangkan Pengujian Penetrasi (*penetration testing*) hanya potret efektifitas sistem keamanan informasi yang sudah diterapkan saat potret dilakukan. Karena dasar inilah, tanpa bermaksud mengesampingkan Pengujian Penetrasi, Penilaian Kerentanan dapat memberikan nilai tambah lebih kepada organisasi dibandingkan dengan Pengujian Penetrasi atas pentingnya Sistem Manajemen yang efisien (Itg.id, 2021).

Sepuluh risiko keamanan telah diidentifikasi oleh *Open Web Application Security Project* (OWASP) sebagai risiko keamanan paling kritis yang terkait dengan aplikasi web. Risiko ini dikenal sebagai bentuk serangan yang umum. Selain dapat dieksploitasi dan dapat berdampak negatif pada situs web saat dijalankan, maka mereka dimasukan sebagai peringkat 10 besar risiko teratas yang dipublikasikan oleh OWASP yaitu, (Appiah et al., 2019):

- *Injection flaws*
- *Broken authentication and session management*
- *Cross site scripting*
- *Insecure direct object references*
- *Security misconfiguration*
- *Sensitive data exposure*
- *Missing level access control*
- *Cross Site Request Forgery (CSRF)*
- *Using components with known vulnerabilities*
- *Unvalidated redirects and forwards*

Melalui identifikasi kerentanan keamanan web dari hasil reporting VAPT, akan dilakukan perbaikan guna meningkatkan tingkat keamanan website aplikasi sampai mencapai level rendah (low). Secara umum solusi pemacahan masalahnya dideskripsikan pada bagan teori dasar program berikut:



Gambar 2. Diagram Proses dan Luaran Kegiatan Pengabdian Masyarakat

Hasil kajian yang dilakukan tim telah menghasilkan serangkaian kegiatan yang meliputi:

1. Menganalisa hasil *vulnerability assessment dan penetration test* (VAPT) yang dituangkan ke dalam report hasil pengujian;
2. Mengidentikasi celah-celah keamanan apa saja yang ada hasil dari Analisa report VAPT;
3. Memberi saran dan melakukan perbaikan atau menutup seoptimal mungkin celah-celah keamanan yang ada guna menurunkan *security risk* dari website aplikasi menjadi rendah (*low*) dan meningkatkan keamanan website aplikasi pondok pesantren dan elearning MTs dan MA Husnul Khotimah.

Gambar 3. Situs web Pondok Pesantren Husnul Khotimah

HASIL DAN PEMBAHASAN

Dalam pelaksanaan kegiatan pengabdian ini, tahap-tahap berikut:

- Pengumpulan informasi

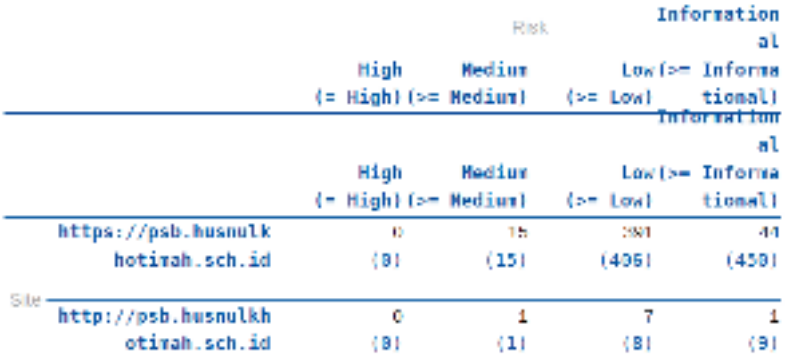
Dari hasil pengumpulan informasi melalui tool yang digunakan diperoleh data:

Tabel 1.
Web Target

No	Web Target	IP Address
1.	husnulkhotimah.sch.id	xx.xx.xxx.xxx
2.	psb.husnulkhotimah.sch.id	xx.xx.xxx.xxx

- Pada tahap ini pengujian akan lebih fokus berinteraksi langsung dengan perangkat atau sistem jaringan dari 2 web target yang berdomain husnulkhotimah.sch.id. Pada kasus ini beberapa target memiliki IP yang sama dikarenakan berupa Virtual Host. Tahap selanjutnya adalah melakukan port scanning untuk mengetahui port TCP dan UDP apa saja yang terdapat pada server target. Pengujian dilakukan dengan beberapa tools yaitu nmap dan zenmap untuk mengetahui informasi port scanning.

Masih ada beberapa port yang terbuka yang bisa dijadikan celah dalam penyerangan web. Untuk lebih melihat celah yang ada, dengan menggunakan tools vulnerability seperti OWASP Zap, diperoleh hasil,



	Risk			
	High (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informational)
Site				
https://psb.husnulkhotimah.sch.id	0 (0)	15 (15)	431 (436)	44 (459)
http://psb.husnulkhotimah.sch.id	0 (0)	1 (1)	7 (8)	1 (9)

Gambar 4 Hasil Pengujian Menggunakan OWASP Zap

Dari Gambar 4 terlihat bahwa level keamanan terhadap serangan siber masih pada level medium yang tertinggi meskipun pengujian ini baru untuk mode standar.

SIMPULAN

Dari hasil pengumpulan informasi dan hasil pengujian diperoleh hasil bahwa masih ada beberapa port yang terbuka dan tidak terlindungi dengan firewall misalnya sehingga masih ada celah serangan siber. Dengan mode standar dalam pengujian penetrasi diperoleh hasil level securitynya berada pada level medium.

DAFTAR PUSTAKA

Appiah, V., Asante, M., Nti, I. K., & Nyarko-Boateng, O. (2019). Survey of websites and web application security threats using vulnerability assessment. *Journal of Computer Science*, *15*(10), 1341–1354. https://doi.org/10.3844/jcssp.2019.1341.1354

Dio Prasasti, G. (2020). *Ada Konten Porno di Situs Belajar, KPAI Minta Orangtua Dampingi Anak Saat PJJ dengan Internet*. Https://Www.Liputan6.Com/Health/Read/4331039/Ada-Konten-Porno-Di-Situs-Belajar-Kpai-Minta-Orangtua-Dampingi-Anak-Saat-Pjj-Dengan-Internet. https://www.liputan6.com/health/read/4331039/ada-konten-porno-di-situs-belajar-kpai-minta-orangtua-dampingi-anak-saat-pjj-dengan-internet

Imperva. (2021). Website Defacement Attack. *Https://Www.Imperva.Com/Learn/Application-Security/Website-Defacement-Attack/*, https://www.imperva.com/learn/application-security. https://www.imperva.com/learn/application-security/website-defacement-attack/

Itg.id. (2021). *Pemahaman Metodologi Vulnerability Assessment dan Pengujian Penetrasi*. https://itgid.org/pemahaman-metodologi-vulnerability-assessment-dan-pengujian-penetrasi/

Maulita Putri, V. (2019). 6 Fakta soal Edmodo, Aplikasi Kelas Sekolah Online yang Populer di AS. *1 Juli 2019*. https://inet.detik.com/cyberlife/d-4607260/6-fakta-soal-edmodo-aplikasi-kelas-sekolah-online-yang-populer-di-as

RI. (2008). Uu-2008-11 Informasi Dan Transaksi Elektronik. *Undang-Undang*, *11*, 1–18. papers3://publication/uuid/8C845E4E-CD67-4476-BB4F-7123C56F0449

We Are Social. (2021). Digital 2021: the latest insights into the 'state of digital' - We Are Social UK. *We Are Social*, 9–25. https://wearesocial.com/uk/blog/2021/01/digital-2021-the-latest-insights-into-the-state-of-digital/.