ANALISIS *WEB SECURITY HOLE* MENGGUNAKAN METODE *PENETRATION TESTING EXECUTION AND STANDARD* (STUDI KASUS : UNIVERSITAS SINGAPERBANGSA KARAWANG)

Zidan Faizi[1], Puwantoro [2], Azhari Ali Ridha [3]
Universitas Singaperbangsa Karawang[123]
Jl. HS.Ronggo Waluyo, Puseurjaya, Telukjambe Timur, Karawang, Jawa Barat 41361
E-mail : zidan.kato19058@student.unsika.ac.id[1], purwantoro.masbro@staff.unsika.ac.id[2], azhari.ali@staff.unsika.ac.id[3]

ABSTRAK

Keamanan web adalah salah satu masalah utama di era digital saat ini. Dalam menghadapi ancaman keamanan, Universitas Singaperbangsa Karawang (Unsika) perlu memperhatikan keamanan sistem informasi mereka, terutama di *website*. Oleh karena itu, penelitian ini dilakukan untuk menganalisis kerentanan keamanan website Unsika dengan menggunakan metode *Penetration Testing Execution and Standard* (PTES). Penelitian ini bertujuan untuk menemukan dan menganalisis kerentanan keamanan pada *website* Unsika dan memberikan rekomendasi untuk memperbaiki keamanan website. Metode PTES digunakan untuk menguji dan menganalisis *website* dari segi keamanan, termasuk identifikasi kerentanan, penetrasi, dan pengujian keamanan lainnya. Hasil penelitian menunjukkan bahwa terdapat beberapa kerentanan keamanan pada website Unsika yang dapat dimanfaatkan oleh penyerang, Setelah pemindaian dilakukan, ditemukan bahwa ada satu kerentanan yang memiliki risiko tinggi, lima kerentanan dengan risiko sedang, lima kerentanan dengan risiko rendah, dan enam kerentanan dengan risiko informasional. Rekomendasi yang diberikan adalah meningkatkan keamanan *website* Unsika dengan memperbaiki kerentanan yang telah diidentifikasi. Selain itu, penting juga untuk mengupdate dan memperbarui perangkat lunak serta meningkatkan kesadaran pengguna dalam mengelola dan menggunakan sistem informasi secara aman. Dalam kesimpulannya, penelitian ini membuktikan bahwa metode PTES dapat digunakan untuk menemukan dan menganalisis kerentanan keamanan pada *website*. Diharapkan hasil penelitian ini dapat membantu Unsika dalam meningkatkan keamanan sistem informasi mereka, terutama di website.
Kata kunci : *Penetration Testing* Execution and Standard (*PTES), SQL Injection*, Keamanan *Website*, Kerentanan *Website, Cross-site scripting (XSS)*

ABSTRACTS

Web security is one of the main problems in today's digital era. In the face of security threats, Singaperbangsa University of Karawang (Unsika) needs to pay attention to the security of their information systems, especially on the website. Therefore, this research was conducted to analyze the security vulnerabilities of Unsika's website using the Penetration Testing Execution and Standard (PTES) method. This research aims to find and analyze security vulnerabilities on the Unsika website and provide recommendations for improving website security. The PTES method is used to test and analyze websites in terms of security, including vulnerability identification, penetration, and other security testing. The results showed that there were several security vulnerabilities on the Unsika website that could be exploited by attackers, After the scan was carried out, it was found that there was one vulnerability that had a high risk, five vulnerabilities with moderate risk, five vulnerabilities with low risk, and six vulnerabilities with informational risk. The recommendation given is to improve the security of the Unsika website by fixing the vulnerabilities that have been identified. In addition, it is also important to update and renew software and increase user awareness in managing and using information systems safely. In conclusion, this research proves that the PTES method can be used to find and analyze security vulnerabilities on the website. It is hoped that the results of this research can help Unsika in improving the security of their information systems, especially on the website.
Keywords: Penetration Testing Execution and Standard (PTES), SQL Injection, Website Security, Website Vulnerability, Cross-Site Scripting (XSS

1. PENDAHULUAN

Pada lajunya zaman, perkembangan teknologi informasi (TI) membawa banyak perubahan serta dampak besar pada setiap orang dalam kehidupan sehari-hari mereka, hampir seluruh sektor, mulai dari kesehatan, pendidikan, dan lainnya.Dengan berbagai fasilitas penggunaan IT sebagai alat atau sarana bukanlah hal yang tidak biasa. Sederhana namun membantu menyelesaikan pekerjaan dalam pekerjaan yang cukup padat dan kompleks. Pada titik ini kebutuhan akan keamanan menjadi syarat menjalankan berbagai bisnis dan aspek lainnya menggunakan IT, sistempun memiliki keamanan yang

berbeda tergantung pada kebutuhan yang diperlukan dari sistem itu sendiri (Syarifudin, 2020)

Hal ini memperlihatkan laporan kejahatan dunia maya yang disponsori oleh McAfee menelan biaya US$445 miliar per tahun. Namun, menurut laporan Microsoft Studi semacam itu 'sangat tidak lengkap' dan melebih- lebihkan kerugian apa yang ada dalam kenyataan. Hampir $1,5 miliar hilang karena potensi penipuan pada tahun 2012 Kartu kredit dan debit online AS. survei 2016 Juniper Research memperkirakan biaya kejahatan dunia maya bisa meningkat 2,1 kali lipat. Triliun pada 2008 (Gani, 2018).

Tentu saja, kejahatan menjadi kasus baru di dunia komputer yang seharusnya menjadi perhatian semua pengguna. Seperti jaringan internet dalam menghadapi virus, worm, DOS, dan gangguan web serta laporan digital tentang pencurian kartu kredit. Dibuat oleh We Are Social (HootSuite) dan saat ini menggunakan internet di Indonesia Ini akan mencapai 202,6 juta pada awal 2021, dimana terjadi peningkatan sebanyak 15,5% atau 27 juta pengguna dibandingkan awal tahun 2020. Jumlah Keseluruhan Penduduk Indonesia saat ini adalah sebanyak 274,9 juta yang artinya penetrasi internet di Indonesia meraih 73,7% pengguna di awal tahun 2021 (Ramadhan, 2020).

Dengan meningkatnya jumlah pengguna internet di Indonesia, ini berarti:

Orang Indonesia sekarang lebih mudah dalam mendapatkan informasi dari internet. Situs web adalah cara untuk menghadirkan informasi internet berupa teks, gambar, video dan suara. Ada sebuah keuntungan ketika dokumen yang kita punya dapat dihubungkan satu sama lain seperti halnya (hypertext) yang dapat diakses dari browser web.

Universitas Singaperbangsa Karawang telah lama menggunakan teknologi website untuk memproses dan menyimpan data terkait aktivitas akademik. Seluruh informasi yang berhubungan dengan kegiatan perkuliahan telah dimuat di dalam website dengan sistem yang cukup kompleks. Hal ini tentunya sangat membantu dalam memenuhi segala kebutuhan terkait pengolahan data, baik bagi mahasiswa maupun dosen, karena informasi dapat dengan mudah diakses dan diperoleh. Namun, risiko keamanan website menjadi sangat penting karena bila website yang digunakan oleh Universitas Singaperbangsa Karawang tidak dilengkapi dengan sistem keamanan yang memadai, maka dapat terjadi ancaman dari pihak yang tidak bertanggung jawab yang memanfaatkan celah keamanan untuk merugikan baik individu maupun institusi Universitas Singaperbangsa Karawang.

Keamanan perangkat lunak memiliki fungsi cukup esensial dalam banyak posisi pada aspek keamanan siber. Pengujian web server dengan melaksanakan selftest menggunakan metode penetration testing pada system web server itu sendiri perlu dilakukan untuk melindungi web server dari serangan pihak asing.

Pengujian penetrasi adalah prosedur dan teknik untuk mendapatkan kesimpulan seberapa baik keamanan suatu jaringan atau sistem komputer dengan menjalankan simulasi serangan untuk melihat dimana sistem rentan, lalu memperbaiki celah tersebut. Melakukan pengujian penetrasi adalah bentuk daritindakan preventif untuk terjadinya peretasan pada sistem (Mulyadi, 2018).

2. METODE PENELITIAN

PTES atau Penetration Testing Execution Standard adalah sebuah standar yang digunakan untuk melakukan uji penetrasi atau pengujian keamanan pada sistem informasi. Tujuan utama PTES adalah untuk memberikan panduan dan prosedur yang sistematis dan terstruktur dalam melakukan uji penetrasi agar hasilnya dapat diandalkan dan bermanfaat bagi pelanggan.

PTES dikembangkan oleh sekelompok praktisi keamanan informasi pada tahun 2010, dan sejak itu telah menjadi standar yang diakui di dunia industri keamanan informasi. PTES terdiri dari beberapa rangkaian diantaranya yaitu tahap *pre-engagement interactions* yang terdiri dari studi lapangan *(field reserach)* dan wawancara langsung *(interview)*, tahap *intelligence gathering*, tahap *exploitation*, tahap *post exploitation*, serta tahap *reporting* yang merupakan tahap terakhir dimana penguji harus membuat laporan dan mendokumentasikan seluruh proses analisis keamanan yang dilakukan, termasuk hasil dari setiap tahap, temuan celah keamanan yang ditemukan, dan rekomendasi penyelesaiannya. Dalam penerapannya PTES terbagi menjadi enam langkah utama, langkah-langkahnya adalah sebagai berikut:

Gambar 2.1 Metode PTES

3. HASIL DAN PEMBAHASAN

Proses pencarian kelemahan keamanan pada suatu situs web melibatkan beberapa tahap, di antaranya pre-engagement interaction, intelligence gathering, threat modelling, vulnerability analysis, exploitation, post exploitation, dan reporting. Dalam tahap intelligence gathering, menggunakan alat The Harvester dan dilanjutkan dengan tahap threat modelling dan vulnerability analysis yang cermat untuk mengidentifikasi kemungkinan kelemahan keamanan pada situs web unsika.ac.id.

Tahap exploitation kemudian dilakukan berdasarkan kelemahan yang ditemukan pada tahap intelligence gathering dan vulnerability analysis, dan diikuti dengan tahap post exploitation untuk mengamankan akses yang berhasil didapatkan. Hasil akhir dari penelitian ini adalah laporan tentang temuan yang ditemukan pada tahap exploitation dengan menggunakan metode PTES.

3.1 *Pre Engagement Interaction*

Pre Engagement Interaction merupakan tahapan awal yang dilakukan untuk memulai pengujian. Tahapan perencanaan juga mencakup penentuan objek dan ruang lingkup pengujian. Objek yang akan diuji adalah website unsika.ac.id yang merupakan situs yang menampilkan informasi yang telah dipublikasikan oleh Universitas Singaperbangsa Karawang.

3.2 *Intelligence Gathering*

Dalam fase ini hasil yang diharapkan adalah mengetahui informasi sebanyak-banyaknya untuk Langkah awal yang sangat penting dalam proses mencari bugs yang akan dilakukan pada website unsika.ac.id. Karena Intelligance Gathering adalah suatu aksi dimana peneliti mencari informasi terhadap target dengan menggunakan beberapa tools seperti Nmap dan The Harvester :

a. *Pin*g

Dalam melakukan scanning, perlu dilakukan pengujian apakah website dapat diakses dari luar atau tidak, pengujian ini dilakukan menggunakan perintah ping pada command prompt atau terminal serta nama domain yang akan di uji.

b. *Port Scanning*

Dalam melakukan *port scanning*, digunakan t*oo*l NMAP v.7.9, pada objek domain unsika.ac.id. dengan menuliskan perintah nmap -v -sT unsika.ac.id. Hasil informasi yang diperoleh setelah melakukan pemindaian dengan menggunakan NMAP kemudian diringkas dan tercatat bahwa informasi tersebut mencakup port yang terbuka dan layanan yang sedang berjalan.

c. Pemindaian Menggunakan *tool Intelligence Gathering*

Pada proses *intelligence gathering*, dilakukan scanning menggunakan tools Nikto pada sistem Kali Linux untuk mencari informasi mengenai website unsika.ac.id. Perintah yang dijalankan adalah nikto -h unsika.ac.id -o result.html. . Dari hasil *scanning* tersebut dapat diketahui bahwa *website* unsika.ac.id menggunakan *server LiteSpeed* dengan alamat IP 151.106.119.31. Selain itu ditemukan juga *retrieved x-powered-by header* menggunakan *Niagahoster, anti-clickjacking X- Frame-Options is not present* yaitu *header* opsi *anti clickjacking* tidak aktif. Sehingga, mengindikasikan bahwa *website* unsika.ac.id mempunyai celah keamanan yang dapat dilakukan dengan *penetration testing.*

3.3 *Vulnerability Analysis*

Langkah berikutnya adalah melakukan analisis kerentanan pada domain unsika.ac.id. Tujuan dari analisis ini adalah untuk menemukan kelemahan yang ada dalam sistem. Untuk melakukan analisis, digunakan alat pemindai kerentanan yang secara otomatis memindai aplikasi untuk menemukan celah keamanan yang mungkin bisa dimanfaatkan untuk pengembangan sistem atau tujuan yang tidak baik.

Dalam mencari celah keamanan, digunakan aplikasi pemindai kerentanan bernama Owasp Zap

a. Hasil Pencarian Celah *Owasp Zap*

Setelah pemindaian dilakukan, ditemukan bahwa ada satu kerentanan yang memiliki risiko tinggi, lima kerentanan dengan risiko sedang, lima kerentanan dengan risiko rendah, dan enam kerentanan dengan risiko informasional.

b. Analisis dan Perancangan Pengujian

Setelah dilakukan analisis kerentanan sebelumnya, langkah selanjutnya dalam upaya meningkatkan keamanan situs *web* adalah melakukan analisis dan perencanaan pengujian keamanan yang lebih terperinci. Hal ini meliputi menentukan skenario pengujian, menentukan jenis pengujian yang akan dilakukan, menyiapkan lingkungan pengujian yang sesuai, dan menentukan metode pengujian yang tepat.

Dalam melakukan analisis dan perencanaan pengujian keamanan, perlu mempertimbangkan faktor-faktor seperti sumber daya yang tersedia, waktu yang diperlukan, dan prioritas kerentanan yang ditemukan. Tujuan utama dari pengujian keamanan adalah untuk mengidentifikasi dan mengevaluasi kerentanan yang ada pada situs k*web*, sehingga dapat diambil tindakan yang tepat untuk meningkatkan keamanan dan melindungi situs *web* dari serangan yang dapat membahayakan keamanan dan privasi pengguna.

Setelah melakukan analisis kerentanan (*vulnerability analysis)* menggunakan *tools OWASP ZAP* maka menghasilkan beberapa faktor-faktor kelemahan yang akan diuji menggunakan metode, yaitu: *Cross-site Request Forgery (CSRF), Cross-site Scripting (XSS), X-Frame-Option Header Not Set, SQL Injection, Remote OS Command Injection, Broken Access Control,* dan *Application Error Disclosure.*

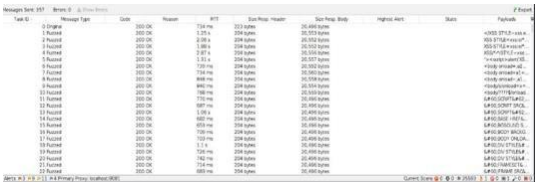
3.4 *Exploitation*

Pada tahap ini, akan dilakukan pengujian celah keamanan yang sebelumnya telah ditemukan pada aplikasi web unsika.ac.id.

Pengujian ini bertujuan untuk memvalidasi kebenaran kerentanan yang telah ditemukan pada tahap sebelumnya.

a. Cross-site Scripting (XSS)

Cross-site scripting (XSS) adalah jenis serangan keamanan yang memanfaatkan kelemahan pada aplikasi web yang memungkinkan penyerang menyisipkan script berbahaya ke dalam halaman web yang dilihat oleh pengguna akhir. Serangan ini biasanya terjadi ketika aplikasi web tidak memvalidasi atau membersihkan masukan pengguna yang diterima sebelum memasukkannya ke dalam halaman web.



Gambar 3.1 *Payload XSS* pada *OWASP ZAP*

Pengujian ini menggunakan payload XSS yang dimiliki OWASP ZAP dengan total 570 payload. Respon yang diberikan website dari 570 payload pengujian menampilkan pesan 200 OK, yang berarti website tidak menampilkan pesan error.

b. ***Cross Site Request Forgery (CSRF)***

Pengujian yang akan dilakukan dengan menggunakan script CSRF POC, dimana pengujian memanfaatkan fitur form email untuk mengubah alamat email dari akun pengguna. Pengujian ini menggunakan bantuan *tools* BurpSuite untuk menangkap parameter pada *email* apabila *email* diubah dan *Visual Studio Code* sebagai *text editor* untuk CSRF POC. Hasil dari pengujian Cross-site Request Forgery tidak berhasil. Email yang telah diinputkan pada form CSRF POC tidak berubah pada akun email yang ada pada website. Sehingga hasil pengujian ini tidak ditemukan celah keamanan *Cross-site Request Forgery.*

c. ***Application Error Disclosure***

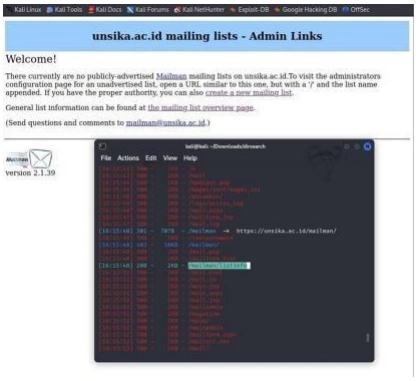
Halaman ini berisi pesan kesalahan atau peringatan yang Tampilnya informasi yang mungkin mengungkapkan informasi sensitif yang seharusnya tidak terlihat. Adapun payload yang digunakan berasal dari api sehingga di dapatkan *error disclosure* melalui url https://unsika.ac.id/wp-json/tribe/events/v1/ dan menampilkan kerentanan *Possible Server Path Disclosure.X-Frame-Option Header Not Set*

Untuk menguji celah keamanan tersebut, dilakukan pengujian dengan menggunakan sebuah file HTML yang sederhana dan berisikan sebuah iframe dengan URL tujuan yang akan diuji yaitu https://unsika.ac.id/wplogin.php?reauth=1&redirect _to=https%3A%2F%2Funsika.ac.id%2Fwp-admin%2F. Halaman yang dimaksud adalah halaman login yang memuat sebuah formulir untuk melakukan login ke situs web tersebut.

X-Frame-Options adalah salah satu tindakan keamanan *web* yang digunakan untuk melindungi situs *web* dari serangan clickjacking atau UI r*edress attack.* Ketika *header X-Frame-Option*s dikonfigurasi pada sebuah situs *web*, hal itu membatasi bagaimana situs tersebut dapat dimuat di dalam sebuah iframe atau frame di situs *web* lain. Hasil dari pengujian berhasil dilakukan *clickjacking* ada halaman https://unsika.ac.id/wp-login.php?reauth=1&redirect_to=https%3A%2F%2 Funsika.ac.id%2Fwp-admin%2F, maka hasilnya menunjukkan bahwa halaman tersebut rentan terhadap serangan *clickjacking,*

d. Broken Access Control

Broken Access Control adalah keadaan dimana sistem kontrol yang tidak memerlukan proses autorisasi untuk mengakses informasi, yang dapat menyebabkan bocornya informasi yang sensitif. Pada pengujian *broken access contro*l terhadap website unsika.ac.id, digunakan *tool* dirsearch dengan cara mengetik perintah dirsearch -u https://unsika.ac.id -e <extensions> untuk mengecek keberadaan celah tersebut.



Gambar 3.2 Pengujian *Broken Access Control*

Hasil dari proses scanning menggunakan *tools* Diresearch. Ditemukan 7 url yang bisa dilewati tanpa adanya proses autorisasi. Pengujian ini

dilanjutkan dengan mengakses url yang telah didapatkan. Hasil dari pengujian ini berhasil dilakukan, namun hanya menampilkan informasi yang tidak terlalu sensitif, hanya informasi berupa plugins yang digunakan pada website.

e. SQL Injection

Injection adalah jenis serangan yang mengambil keuntungan dari kekurangan validasi input suatu aplikasi, baik dalam *method* POST atau GET. Teknik *sql injection* mampu mencuri informasi rahasia seperti *username* dan *password*, mengubah database, dan memasukkan konten berbahaya. Serangan ini dapat mengekspos database, menampilkan informasi yang tidak seharusnya, dan memberikan akses sewenang-wenang pada penyerang untuk memanipulasi *database.* Pengujian ini menggunakan tools Sqlmap di Kali Linux. Pengujian menginjeksi melewati parameter dalam bentuk serangan S*QL Injection.*

f. Remote OS Command Injection

Dalam upaya untuk menguji keberadaan celah *Remote OS Command Injection*, dilakukan pengujian dengan menggunakan *payload* berupa query';start- sleep -s 15. *Payload* tersebut dimasukkan pada parameter query sehingga url menjadi https://unsika.ac.id/?s= query';start-sleep -s 15. Namun, setelah dilakukan pengujian, tidak terjadi perubahan apapun pada tampilan *website*, yang menandakan bahwa tidak ditemukan adanya kerentanan pada *Remote OS Command Injection*.

3.5 *Post Exploitation*

Pada tahap *Post Exploitation*, dilakukan tindakan untuk mengganggu lalu lintas *server* yang bertujuan untuk menghalangi pengguna lain dari memperoleh akses ke layanan *website*. Tindakan tersebut dilakukan untuk menjaga agar pengendalian sistem tetap berada di tangan penyerang yang telah mendapatkan akses sebelumnya.

a. Bomb Mail

Jika dilakukan *Email Bomb* pada alamat email admin upt.tik@unsika.ac.id, email tersebut akan dianggap sebagai Email Spam dan akan mengalami flooding. Artinya, kotak email akan diisi oleh banyak email yang sama sehingga jumlahnya melebihi batas alokasi kotak email. Hal ini dapat mengakibatkan email penting tidak dapat diterima atau bahkan hilang, dan dapat memicu terjadinya DOS *(denial of service)* pada *server email* sehingga server tidak memberikan respon saat diberi perintah. Jika terjadi hal tersebut, *mail serve*r ISP dapat mengalami crash atau down sehingga tidak dapat menerima atau mengirimkan email.

b. DDOS *(Denial Distributed of Services) tools Golden Eye)*

DDOS *Attack* adalah serangan yang dapat menghabiskan sumber daya pada *website* atau *server*, sehingga membuatnya tidak dapat beroperasi dengan baik. Serangan ini dapat menghalangi pengguna lain untuk memperoleh akses layanan dari website atau server yang terkena dampak DDOS karena adanya peningkatan lalu lintas kinerja pada *server* atau *website*tersebut.

3.6 *Reporting*

Tahap terakhir dalam melakukan *penetration testing* adalah *reporting.* Berdasarkan hasil pengujian pada tahap *penetration testing website* unsika.ac.id memiliki
7 kerentanan yang telah diuji. 3 dari 4 kerentanan tersebut berhasil ditemukan celah keamanan pada website http://unsika.ac.id./

4. KESIMPULAN DAN SARAN

Kesimpulan yang diperoleh dari pelaksanaan pengujian kerentanan pada website Universitas Singaperbangsa Karawang menggunakan metode penetration testing dan vulnerability analysis dengan domain unsika.ac.id. Terdapat beberapa kesimpulan yaitu pada pengujian domain unsika.ac.id, dilakukan *scanning* menggunakan *tools* OWASP-ZAP untuk melakukan *vulnerability analysis* guna menemukan kerentanan yang mungkin ada pada *website*. Hasil scanning menunjukkan bahwa terdapat satu kerentanan dengan tingkat risiko tinggi, lima kerentanan dengan tingkat risiko sedang, lima kerentanan dengan tingkat risiko rendah, dan enam kerentanan dengan tingkat risiko informasional. 1. Berdasarkan hasil analisis kerentanan, dilakukan pengujian terhadap beberapa celah keamanan seperti *Cross-site Request Forgery* (CSRF), *Cross-site Scripting* (XSS), *X-Frame-Options Header Not Set, SQL Injection, Remote OS Command Injection, Broken Access Control,* dan *Application Error Disclosure*. Hasil pengujian berhasil menemukan tiga celah keamanan, yaitu *X-Frame-Options Header Not Set* yang dapat dimanfaatkan untuk membuat iframe pada halaman *web* lain, *Application Error Disclosure* pada url https://unsika.ac.id/wp-json/tribe/events/v1/ yang mengandung pesan error yang mungkin mengungkapkan informasi sensitif, serta *Broken Access Control* yang menemukan 7 url yang dapat diakses tanpa adanya proses autorisasi, meskipun hanya menampilkan informasi yang tidak terlalu sensitif seperti plugin yang digunakan pada *website.*

Berdasarkan parameter kerentanan yang tercantum pada OWASP Top 10-2021, tidak ditemukan adanya kerentanan berisiko tinggi pada website Universitas Singaperbangsa Karawang. Meskipun demikian, ditemukan adanya kerentanan pada celah *Broken Access Control,* namun hanya menampilkan

informasi yang kurang sensitif, yakni informasi mengenai plugin yang digunakan pada website. 1. Penulis juga menyarankan agar pihak Universitas Singaperbangsa Karawang melakukan pemantauan secara rutin terhadap keamanan *website* unsika.ac.id. Pemantauan ini dapat dilakukan dengan melakukan vulnerability analysis secara berkala dan melakukan tindakan pencegahan terhadap celah-celah keamanan yang ditemukan. Selain itu, perlu dilakukan pula pelatihan atau edukasi terhadap para pengelola *website* mengenai praktik-praktik keamanan informasi yang baik agar dapat mencegah terjadinya celah keamanan di masa mendatang.

DAFTAR PUSTAKA

[1] Gani, A. (2018). CYBERCRIME (KEJAHATAN BERBASIS KOMPUTER). Logo Header Halamanjsi (Jurnal Sistem Informasi) Universitas Suryadarma, 5(1), 16–29. Https://Doi.Org/Https://Doi.Org/10.35968/Jsi.V5i1.18

[2] Gontar, P., & Kamisiński, J. (2020). Security Testing Of Web Applications – A Survey Of Current Approaches. International Journal Of Network Security, 22(6), 1033-1053.

[3] Hadzic, F., & Maric, J. (2018). Penetration Testing Of Web Applications - A Review Of Current Techniques And Tools. 2018 International Conference On Smart Systems And Technologies (SST), Sarajevo, Bosnia And Herzegovina, 1-6. Doi: 10.1109/SST.2018.8467647

[4] Khan, Z., & Li, S. (2020). A Review Of Web Application Security Testing Methodologies. International Journal Of Web Information Systems, 16(2), 146-166. Doi: 10.1108/IJWIS-02-2019-0017

[5] Mulyadi. (2018). Bagaimana Melakukan "Penetration Test"? Retrieved From Www.Kompasiana.Com Website: Https://Www.Kompasiana.Com/Moengil/5a4ae2655e13736b135dd7e3/Bagaim

[6] Ramadhan, B. (2020). Data Internet Di Indonesia Dan Perilakunya Tahun 2020. Retrieved From Teknoia.Com Website: Https://Teknoia.Com/Data-Internet-Di-Indonesia-Dan-Perilakunya-880c7bc7cd19

[7] Taneski, N., & Madevska-Bogdanova, A. (2019). A Systematic Review Of Web Application Penetration Testing Methodologies. International Journal Of Advanced Computer Science And Applications, 10(6), 70-78. Doi: 10.14569/IJACSA.2019.0100609

[8] Stallings, W. (2021). Cryptography And Network Security: Principles And Practice (8th Ed.). Pearson.

[9] Tanenbaum, A. S., Wetherall, D. (2019). Computer Networks (5th Ed.). Pearson.

[10] Tania, A. M., Setiyadi, D., & Khasanah, F. N. (2018). Keamanan Website Menggunakan Vulnerability Assessment. INFORMATICS FOR EDUCATORS AND PROFESSIONALS, 2(2), 171–180. Retrieved From Http://Download.Garuda.Kemdikbud.Go.Id/Article.Php?Article=718152&Val=11042&Title=K Eamanan Website Menggunakan Vulnerability Assessment

[9] Utoro, S., Nugroho, B. A., Meinawati, & Widianto, S. R. (2020). Analisis Keamanan Website E- Learning SMKN 1 Cibatu Menggunakan Metode Penetration Testing Execution Standard. JURNAL MULTINETICS, 6(2), 169–178. Retrieved From Https://Www.Researchgate.Net/Publication/348303165_Analisis_Keamanan_Website_E-Learning_SMKN_1_Cibatu_Menggunakan_Metode_Penetration_Testing_Execution_Sta Ndard

[10] Yahya, A. S. A., & Alnaim, A. (2019). Penetration Testing Methodology: A Review Of The State Of The Art. 2019 15th International Conference On Innovations In Information Technology (IIT), Abu Dhabi, United Arab Emirates, 22- 24. Doi: 10.1109/INNOVATIONS.2019.8710634