InComTech: Jurnal Telekomunikasi dan Komputer
vol.12, no.2, Agustus 2022, 129-138
http://publikasi.mercubuana.ac.id/index.php/Incomtech
P-ISSN: 2085-4811 E-ISSN: 2579-6089

Penetration Testing Pada Sistem Informasi Jabatan Universitas Hayam Wuruk Perbanas

Gaguk Suprianto*

Informatika, Fakultas Teknik dan Desain, Universitas Hayam Wuruk Perbanas,
Jl. Wonorejo Utara No. 16, Rungkut, Surabaya, Jawa Timur, Indonesia
*Email Penulis Koresponden: gaguk.suprianto@perbanas.ac.id

Abstrak:
Keamanan pada sisi server merupakan salah satu upaya untuk mencegah terjadinya pembobolan sistem oleh pihak yang tidak bertanggung jawab. Pencegahan dapat dilakukan oleh sistem administrator untuk melindungi informasi pengguna dengan terlebih dahulu melakukan pengujian. Universitas Hayam Wuruk Perbanas menyimpan data-data dari pihak-pihak yang mempunyai jabatan seperti data mahasiswa, keuangan, penjaminan mutu dan lain-lain karena menjadi bagian kelangsungan proses bisnis perguruan tinggi. Sehingga data-data tersebut bersifat penting. Berbagai macam ancaman serangan yang berpotensi dihadapi seperti *Cross Site Scripting* (XSS), *Denial of Services,* SQL *Injection* dan lain sebagainya. Oleh sebab itu dilakukan pengujian untuk mengetahui kelemahan-kelemahan domain jabatan. Pihak pengelola menginginkan pengujian berfokus pada perangkat lunak dan informasi awal yang diberikan hanya alamat domain sehingga pengujian dilakukan dengan metode berjenis *black box*. Keunggulan metode tersebut berfokus pada pengujian kualitas perangkat lunak seperti untuk menemukan kesalahan pada struktur data dan fungsi sistem. Pengujian dilakukan dengan menggunakan beberapa *tools* seperti NMAP dan Acunetix. Hasil yang diperoleh ditemukan beberapa celah keamanan pada sistem seperti celah XSS yang dapat merubah tampilan. Selain itu *shell backdoor* masih dapat diunggah pada *form* dengan ekstensi pdf. Adapun domain jabatan belum mempunyai sertifikat *SSL* sehingga lalu lintas data dapat terbaca. Temuan-temuan tersebut sebagai masukan ke pengelola sistem agar dilakukan perbaikan. Penelitian selanjutnya dapat menggunakan metode *white box* yang membuat penguji dapat menguji tahapan yang belum tarcapai dengan metode *black box* dengan secara lebih dalam dan menyeluruh.

***Kata Kunci**:*
Cross Site Scripting;
Denial of Services;
SQL Injection;
Black Box;
Shell Backdoor;

Riwayat Artikel:
Diserahkan 10 Maret 2021
Direvisi 11 Juli 2022
Diterima 14 Juli 2022
Dipublikasi 18 Agustus 2022

DOI:
10.22441/incomtech.v12i2.15093

1. PENDAHULUAN

Sistem informasi merupakan aspek yang sangat penting dalam suatu institusi atau organisasi. Salah satunya adalah aspek dari sisi keamanannya. Hal tersebut seiring dengan meningkatnya jumlah volume data yang dipertukarkan melalui media internet. Saat ini penggunaan teknologi informasi menjadi keharusan bagi organisasi yang menjalankan kegiatan operasionalnya. Penerapan teknologi informasi sendiri bagi institusi menjadi sangat penting dalam peranannya sebagai kelangsungan proses bisnis. Dalam upaya mendukung tercapainya rencana staretegis suatu perusahaan atau institusi, perananan teknologi informasi menjadi hal yang penting agar perusahaan atau institusi tersebut dapat mencapai sasaran visi, misi dan tujuan yang diinginkan [1]. Namun seiring berjalannya waktu, organsasi yang menerapkan sistem informasi terpusat perlu mewaspadai aspek dari sisi keamanan informasi. Hal tersebut karena keamanan informasi adalah suatu keharusan dimana keamanan dimaksudkan untuk menjaga sistem dari ancaman [2]. Sistem keamanan yang lemah akan membuat *hacker* untuk mempunyai kesempatan merusak sistem atau memindahkan fungsi yang sudah dibuat [3].

Universitas Hayam Wuruk Perbanas Surabaya mempunyai banyak sistem informasi dalam menjalankan kegiatan operasionalnya yang mana data didalamnya harus dijaga. Seorang penyerang akan menyerang sistem keamanan jaringan dengan tujuan untuk mendapatkan data yang terdapat pada sistem informasi tersebut. Sebagai upaya meminimalisir resiko terhadap serangan yang dilakukan oleh *hacker* yang bisa datang secara tiba-tiba, maka langkah yang dapat dilakukan dengan mengevaluasi keamanan sistem informasi. Oleh karenanya perlu dilakukan pengujian berupa *penetration testing* yang dimana kegiatan tersebut dilakukan sebagai langkah untuk identifikasi dan eksploitasi kerentanan pada sistem. Pengujian sistem merupakan langka-langkah atau tahapan dalam upaya menemukan kesalahan pada sistem yang diuji sehingga dapat dilakukan perbaikan agar sistem layak untuk digunakan [4]. Selain itu dengan dilakukannya pengujian akan mengurangi resiko dari terjadinya penyalahgunaan sumber daya organisasi.

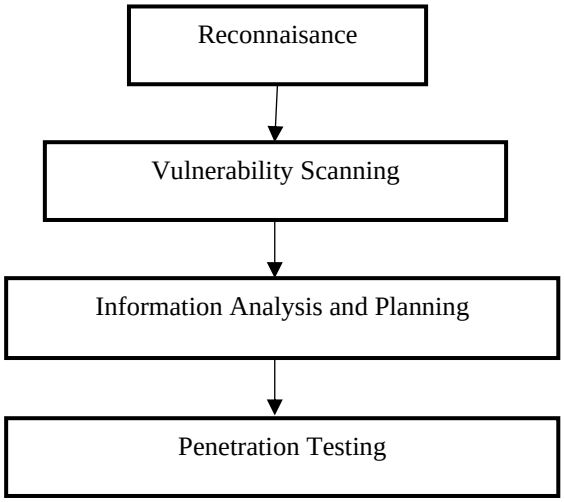
Terdapat beberapa penelitian terdahulu yang serupa yang telah dilakukan. Pada penelitian [5] melakukan *penetration testing* untuk menguji kerentanan sistem informasi manajemen dan *website* dengan langkah-langkah pengujian seperti *information gathering, webserver footprinting, vulnerability scanning* dan analisa. Sedangkan pada penelitian [6] melakukan *penetration testing* dengan menggunakan metode OWASP pada *website* kampus. Pada penelitian [7] dilakukan penelitian *penetration testing* untuk mendeteksi kelemahan *web server* Sistem Informasi Kampus dengan tahapan *Information Gatering* dan *Vulnerability Scanning*. Berdasarkan penelitian-penelitian serupa yang telah dilakukan sebelumnya, keamanan sistem informasi organisasi menjadi hal yang menarik untuk diteliti. Organisasi dapat dilihat bagaimana upayanya dalam mengamankan informasi organisasi terhadap serangan *hacker* sehingga dapat dievaluasi sikap organisasi tersebut terkait keamanan informasi, sedangkan cara terbaik yang dapat dilakukan dengan melakukan pengujian penetrasi karena dengan pengujian tersebut dimungkinkan untuk menemukan kerentanan baru [8]. Berdasarkan hal tersebut, peneliti melakukan *penetration testing* pada sistem informasi jabatan di Universitas Hayam Wuruk Perbanas. Pihak pengelola menginginkan pengujian berfokus pada kualitas perangkat lunak dan hanya memberikan alamat domain saja yang ingin

penguji seolah-olah menjadi *hacker* asli. Sehingga pengujian dilakukan menggunakan metode *black box*. Penelitian ini menggunakan beberapa *tool* seperti NMAP yang berfungsi untuk melakukan *network scanning* meliputi *port, protocol, services*. Selain itu juga menggunakan perangkat lunak Acunetix yang digunakan untuk mendeteksi kelemahan sistem informasi. Untuk memantau lalu lintas data menggunakan Wireshark dan Brutus untuk memecah kata sandi. Setelah hasil pengujian diperoleh, pengelola sistem dapat menerapkan sistem manajemen keamanan informasi atau ISO 270001 yang merupakan metode khusus terstruktur tentang pengamanan informasi yang akan berperan sebagai kontrol untuk mengendalikan dan mengelola risiko keamanan informasi.

2. METODE

Terdapat dua jenis *penetration testing* yakni *black box* dan *white box*. Ada juga yang mengombinasikan kedua jenis penetrasi tersebut. Metode pengujian *black box* merupakan jenis pengujian yang dibuat seolah-olah serangan dari *hacker* asli, karena penguji hanya diberikan informasi berupa nama organisasi dan nama domain sistem informasi atau *website* tersebut. Sehingga penguji membutuhkan waktu yang lebih banyak untuk mencari informasi lain yang terkait dengan sistem yang diuji. Selain itu dalam pengujian berjenis *black box* berfokus untuk pengujian kualitas perangkat lunak. Pengujian berjenis *black box* digunakan untuk menemukan berbagai kerentanan perangkat lunak yaitu struktur data yang tidak benar, fungsi sistem yang salah, performansi yang tidak sesuai, kesalahan antarmuka serta inisialisasi dan terminasi yang salah [9]. Sedangkan metode *white box* merupakan jenis pengujian yang dimana semua informasi secara lengkap diberitahukan diawal sebelum melakukan pengujian.

Ruang lingkup *penetration testing* adalah sistem informasi jabatan yang merupakan situs dari pihak-pihak yang mempunyai jabatan pada institusi untuk mengatur wewenangnya. Adapun langkah-langkah pengujian yang dilaksanakan adalah seperti pada Gambar 1 berikut.



Gambar 1. Langkah-langkah pengujian

Berdasarkan alur di atas, maka dapat diuraikan langkah-langkah dari masing-masing tahapan seperti berikut ini:

2.1 *Reconnaissance*

Tahapan ini dilakukan sebagai persiapan awal sebelum melakukan penyerangan. *Reconnaissance* adalah tahapan pencarian informasi yang dilakukan *hacker* dari target yang dijadikan sasaran sebelum proses penyerangan [10]. Teknik ini merupakan langkah *network scanning* yang dapat dilakukan melalui jaringan pada area internal maupun external. Dengan berbekal alamat domain yang telah diberikan, terlebih dahulu penguji mencari informasi berupa IP *Address* target dengan melakukan ping pada domain sistem informasi jabatam. IP *Address* yang telah didapatkan untuk selanjutnya dilakukan *scanning* menggunakan *tool* NMAP yang bertujuan mengumpulkan informasi dari target meliputi *port, protocol, services,* topologi dan informasi jaringan lainnya. Informasi tersebut digunakan untuk tahapan selanjutnya. *Reconnaisance* mempunyai dua jenis salah satunya *active reconnaissance* yang artinya penguji mencoba mengintai target menggunakan berbagai alat seperti Ping, Traceroute, Netcat dan lain-lain. Aktivitas atau kegiatan peretasan yang dilakukan secara langsung ke korban atau rekan korban yang mempunyai sistem yang akan diretas, hal tersebut akan sangat beresiko oleh *hacker* itu sendiri [11]. Jika pengujian tersebut diketahui korban maka dapat berakibat pidana atau ganti rugi. Selain itu ada *passive reconnaissance* yang merupakan aktivitas atau kegiatan pengumpulan informasi dari target yang akan diretas melalui berbagai media baik cetak maupun elektonik seperti koran, radio, televisi dan internet [12]. Sehingga dapat dikatakan bahwa pengujian ini merupakan *active reconnaissance* karena pengujian dilakukan langsung ke target.

2.2 *Vulnerability Scanning*

Langkah berikutnya merupakan proses *vulnerability scanning* pada domain sistem informasi jabatan menggunakan perangkat lunak *Accunetix* yang betujuan untuk untuk memperoleh informasi kelemahan target. Langkah *vulnerability scanning* adalah proses mengidentifikasi kelemahan keamanan dan kekurangan pada sistem dan perangkat lunak yang berjalan didalamnya [13]. Tujuan yang ingin dicapai adalah memperoleh informasi *vulnerability network* tersebut, misal daftar *port* yang terbuka, *bug* pada aplikasi server, dan lain-lain yang kadangkala fase ini disebut sebagai *passive attack* [14]. Tahapan ini penguji memasukkan alamat domain ke perangkat lunak tersebut kemudian secara otomatis perangkat lunak tersebut akan melakukan *scanning* terhadap domain yang telah dimasukkan. Hasil dari proses tersebut berupa laporan informasi kelemahan yang terbagi menjadi beberapa level yaitu *High Alert* yang berada pada level ke 3, *Medium Alert* yang berada pada level ke 2, *Low Alert* yang berada pada level ke 1 dan *Infomational Alert*. Level 3 merupakan kerentanan paling berbahaya seperti *XSS*, level 2 kerentanan yang disebabkan *sitecoding* yang lemah, level 1 merupakan kerentanan akibat kurangnya enkripsi atau keamanan pada lalu lintas data dan *information alert* merupakan item yang ditemukan selama *scannning* seperti pengungkapan kata sandi atau alamat internal IP. Informasi yang diperoleh pada tahap ini dipetakan untuk dianalisis dan perencanaan penyerangan.

2.3 *Information Analysis* dan *Planning*

Tahapan selanjutya melakukan analisis dan perencanaan penyerangan ke sistem berdasarkan hasil laporan *scanning vulnerability* dengan perangkat lunak Acunetix. Perangkat lunak Acunetix *Web Vulnerability Scanner* digunakan untuk kegiatan atau aktivitas *vulnerability assessment* [15]. Berdasarkan laporan informasi kelemahan target dan topologi serta informasi jaringan lainnya. Kelemahan-kelemahan tersebut dipetakan menjadi beberapa level. Untuk level *high* penguji akan menyiapkan sebuah kode berbahaya untuk menginjeksi target, level *medium* penguji menyiapkan kode yang telah disusun untuk diunggah pada sistem, level *low* penguji menyiapkan *tool* untuk memantau lalu lintas data antara *user* dengan server dan *informational alert* penguji menyiapkan *tool* untuk mendapatkan kata sandi atau infromasi lain. Persiapan ini dilakukan agar pada tahap *penetration testing* dapat berjalan dengan maksimal dan cepat.

2.4 *Penetration Testing*

Berdasarkan hasil pemetaan dari analisa dan perencanaan yang telah dilakukan, tahapan ini merupakan pengujian akhir berupa *penetration testing* pada domain jabatan. *Penetration testing* merupakan proses simulasi serangan secara nyata yang bertujuan untuk megetahui nilai risiko yang berkaitan dengan potensi dari adanya pelanggaran keamanan [16]. Tahapan *penetration testing* bertujuan untuk mengevaluasi keamanan dari sebuah sistem informasi dan jaringan komputer. Pengujian ini telah mempunyai izin atau persetujuan dari organisasi yang akan diuji. Pada pengujian level 3, penguji membagi 2 tahap yakni pengujian *Reflected* XSS dengan memasukkan kode berbahaya pada domain jabatan melalui *Address Bar* mesin pencarian dan *Stored* XSS dilakukan dengan memasukkan kode pada salah satu *form* berektensi .pdf. Sedangkan pengujian level 2, penguji mengunggah *shell backdoor* berupa kode dalam format php ke *form* berkestensi pdf. Berikutnya pada pengujian level 1, penguji memantau lalu lintas data dengan *tool Wireshark.* Selain itu pada pegujian *informational alert*, penguji menggunakan *brutus tool* untuk menguji apakah *password* bisa dipecahkan atau tidak. Segala informasi terkait ancaman keamanan aktual yang berpotensi dieksploitasi yang apabila termasuk dalam doktrin dan proses keamanan organisasi dapat disajikan pada pengujian penetrasi. Tahapan tersebut dapat membantu organisasi untuk mengidentifikasi secara cepat dan tepat baik potensi kerentanan dan kerentanan yang nyata [17].

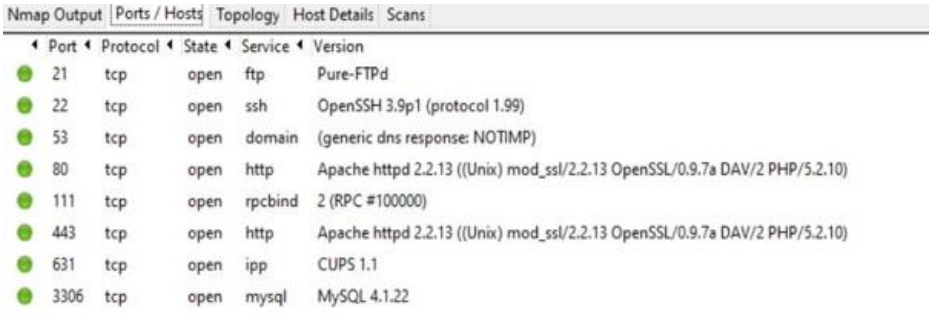
3. HASIL DAN PEMBAHASAN

Bagian yang dijelaskan dibawah ini merupakan hasil tahapan-tahapan yang seperti diuraikan pada bagian sebelumnya.

3.1 Hasil *Reconnaisance*

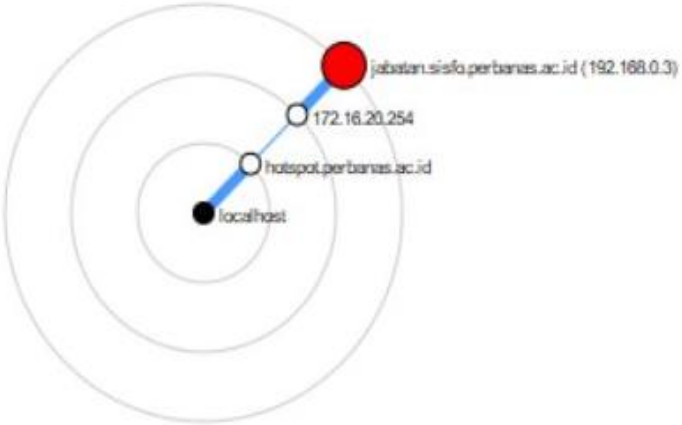
Berdasarkan hasil *scanning* pada domain sistem informasi jabatan menggunakan *tool* NMAP diperoleh hasil bahwa beberapa *port* masih berstatus *open* atau terbuka. Protokol *file transfer* FTP dan protokol jaringan SSH tampak masih berstatus *open*. Terlihat juga bahwa domain yang diuji masih menggunakan

port http (80) sehingga lalu lintas data dapat terbaca dengan bantuan *tool*. Hasil dari kegiatan tahap ke satu juga ditunjukkan sebagaimana pada Gambar 2 di bawah ini.



Gambar 2. Status *Port*

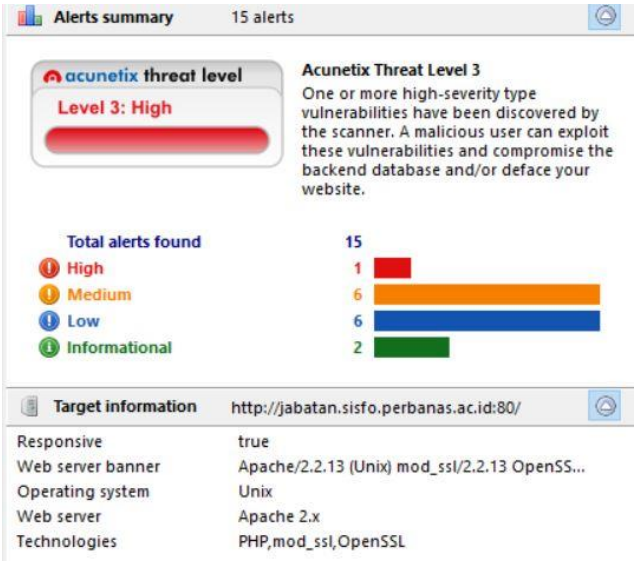
Selain informasi *port* yang terbuka seperti pada Gambar 2, juga dapat diketahui topologi yang digunakan seperti yang ditunjukkan pada Gambar 3. Penguji berstatus sebagai *local host* yang melakukan pengujian menggunakan internet pada area kampus yang dimana domain hostpot tersebut terhubung dengan *gateway* 172.16.20.254 sebelum mencapai domain yang diuji.



Gambar 3. Topologi Sistem Informasi

3.2 Pengujian *Vulnerability Scanning*

Pada pengujian ini diperoleh bahwa domain yang diuji mempunyai kerentanan dengan level 3: *High* yang berarti bahwa domain tersebut memiliki tingkat celah yang tinggi sehingga dapat berpotensi untuk dimasuki oleh *hacker*. Pada Gambar 4 ditemukan 15 *Alert* dengan rincian 1 *Alert* berstatus *High*, 6 berstatus *Medium*, 6 berstatus *Low* dan 2 berstatus *informational*.



Gambar 4. Hasil *Scanning* Perangkat lunak *Accunetix*

3.3 Pemetaan *Information Analysis* dan *Planning*

Tahapan ini berupa pemetaan dari tahapan sebelumnya. Masing-masing level dilakukan pengujian. Adapun pemetaan tersebut seperti terlihat pada Tabel 1.

Tabel 1. Pemetaan Celah Keamanan

Level	Celah	Pengujian
High	XSS	- *Reflected XSS:* memasukan kode pada *address bar* - *Stored XSS* dilakukan dengan memasukkan kode pada salah satu *form* berektensi pdf.
Medium	*Site Coding* lemah	Pengujian dilakukan dengan mengunggah *backdoor shell* dengan format php
Low	*Not Encrypted Sites*	Memantau lalu lintas data antara server dengan *user*
Informational	*User Credentials*	Melakukan serangan *brute force*

3.4 Hasil *Penetration Testing*

Setelah melakukan analisis dan perencanaan, penguji mengambil beberapa kelemahan yang mempunyai tingkat resiko yang tinggi untuk dilakukan *penetration testing*. Ada beberapa pengujian diantaranya adalah:

- Pada pengujian *Reflected* XSS penguji memasukkan kode pada *address bar* untuk menguji apakah ada dampak dari penyisipan *script*. Hasil dari kegiatan juga ditunjukkan sebagaimana pada Gambar 5. Pengujian *Reflected* XSS bersifat *non-persistent* karena hasil pengujian ini hanya dapat dilihat pada satu tab browser yang dilakukan oleh penguji. Sedangkan ketika dibuka pada tab lain, halaman *website* menampilkan tampilan sebagaimana mestinya.
- Pengujian *Stored* XSS dilakukan dengan memasukkan kode pada salah satu *form* berektensi pdf. *Script* disisipkan pada *form* pada sistem informasi tersebut. Hasil dari aktivitas ini ditunjukkan pada Gambar 6. Pengujian ini

berpengaruh pada halaman lain karena saat mengakses menggunakan browser yang berbeda, halaman menampilkan gangguan yang sama.

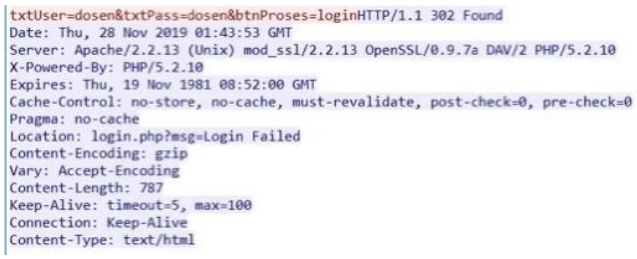
- Pengujian dilakukan dengan mengunggah *backdoor shell* dengan format php pada salah satu *form* berkekstensi pdf yang terdapat pada sistem informasi jabatan. Pada Gambar 7 dapat dilihat bahwa penguji berhasil mengunggah *backdoor shell* akan tetapi *backdoor shell shell* tersebut tidak berhasil dieksekusi atau dengan kata lain pengujian tersebut tidak berdampak ancaman terhadap sistem informasi.

Gambar 5. Pengujian *Reflected* XSS

Gambar 6. Pengujian *Stored* XSS

Gambar 7. Pengujian Unggah *Backdoor Shell*

- Saat *user* login data yang bersifat sensitif berupa *Username* dan *Password*, masih terbaca dengan *tool* Wireshark (***User*=dosen dan *Password*= dosen**) seperti yang terlihat Gambar 8. Hal tersebut karena domain yang diuji belum mempunyai sertifikat SSL sehingga lalu lintas data masih dapat terbaca atau belum terenkripsi.



Gambar 8. Hasil *scanning* dengan Wireshark

- Pengujian ini mencoba melakukan serangan *brute force* untuk memecah kata sandi dengan menggunakan *Brutus tool.* Dari beberapa percobaan diperoleh kesimpulan bahwasannya sistem informasi jabatan sudah menerapkan *user credentials* yang aman.

4. KESIMPULAN

Dari pengujian ditemukan beberapa celah keamanan. Hasil pengujian hanya dapat dilihat pada satu *tab browser* ketika pengujian *Reflexted* XSS sedangkan hasil pengujian *Stored* XSS berpengaruh pada halaman lain ketika mengakses menggunakan *browser* yang berbeda yakni halaman menampilkan gangguan yang sama. Adapun pengujian *backdoor shell* memberikan hasil bahwa *shell* berhasil diunggah walau tidak berhasil dieksekusi. Selain itu domain sistem informasi jabatan belum mempunyai sertifikat SSL sehingga lalu lintas data antara *user* dan *server* dapat terbaca. Dari serangan *brute forcé* yang telah dilakukan diperoleh hasil bahwa sistem sudah menerapkan *user credentials* secara aman. Sehingga penguji memberikan rekomendasi pada pihak pengelola untuk melakukan validasi data pada *source code* baik di sisi *user* maupun *server*, mengaktifkan *firewall* sistem dan menerapkan SSL agar koneksi antara *server* dan *user* aman. Selanjutnya penguji menyarankan di penelitian berikutnya menggunakan metode *white box* agar sistem dapat teruji pada tahapan yang belum tarcapai dengan metode *black box* dengan secara lebih dalam dan menyeluruh. Penguji juga menyarankan kepada pihak pengelola agar dapat menerapkan sistem manajemen keamanan informasi atau ISO 270001 yang merupakan metode khusus tentang pengamanan informasi.

REFERENSI

[1] I. Riadi, A. Yudhana, and M. C. F. Putra, “Forensic Tool Comparison on Instagram Digital Evidence Based on Android with The NIST Method,” *Sci. J. Inform.*, vol. 5, no. 2, pp. 235–247, 2018, doi: 10.15294/sji.v5i2.16545.

[2] E. Kurniawan and I. Riadi, "Security level analysis of academic information systems based on standard ISO 27002: 2003 using SSE-CMM," *ArXiv Prepr. ArXiv180203613*, 2018, doi: 10.48550/arXiv.1802.03613.
[3] F. Fachri, A. Fadlil, and I. Riadi, "Analisis Keamanan Webserver Menggunakan Penetration Test," *J. Inform.*, vol. 8, no. 2, pp. 183–190, 2021, doi: 10.31294/ji.v8i2.10854.
[4] M. Nurudin, W. Jayanti, R. D. Saputro, M. P. Saputra, and Y. Yulianti, "Pengujian Black Box pada Aplikasi Penjualan Berbasis Web Menggunakan Teknik Boundary Value Analysis," *J. Inform. Univ. Pamulang*, vol. 4, no. 4, pp. 143–148, 2019, doi: 10.32493/informatika.v4i4.3841.
[5] R. Pangalila, A. Noertjahyana, and J. Andjarwirawan, "Penetration Testing Server Sistem Informasi Manajemen dan Website Universitas Kristen Petra," *J. Infra*, vol. 3, no. 2, pp. 271–276, 2015.
[6] S. Hidayatulloh and D. Saptadiaji, "Penetration Testing pada Website Universitas ARS Menggunakan Open Web Application Security Project (OWASP)," *J. Algoritma*, vol. 18, no. 1, pp. 77–86, 2021, doi: 10.33364/algoritma/v.18-1.827.
[7] S. Sahren, R. A. Dalimuthe, and M. Amin, "Penetration Testing Untuk Deteksi Vulnerability Sistem Informasi Kampus," in *Prosiding Seminar Nasional Riset Information Science (SENARIS)*, 2019, vol. 1, pp. 994–1001, doi: 10.30645/senaris.v1i0.109.
[8] S. R. Zeebaree, K. Jacksi, and R. R. Zebari, "Impact analysis of SYN flood DDoS attack on HAProxy and NLB cluster-based web servers," *Indones J Electr Eng Comput Sci*, vol. 19, no. 1, pp. 510–517, 2020, doi: 10.11591/ijeecs.v19.i1.pp505-512.
[9] F. C. Ningrum, D. Suherman, S. Aryanti, H. A. Prasetya, and A. Saifudin, "Pengujian Black Box pada Aplikasi Sistem Seleksi Sales Terbaik Menggunakan Teknik Equivalence Partitions," *J. Inform. Univ. Pamulang*, vol. 4, no. 4, pp. 125–130, 2019, doi: 10.32493/informatika.v4i4.3782.
[10] R. Sahtyawan, "Penerapan zero entry hacking didalam security misconfiguration pada VAPT (vulnerability assessment and penetration testing)," *J. Inf. Syst. Manag. JOISM*, vol. 1, no. 1, pp. 18–22, 2019, doi: 10.24076/joism.2019v1i1.18.
[11] A. R. Kelrey and A. Muzaki, "Pengaruh Ethical Hacking Bagi Keamanan Data Perusahaan," *Cyber Secur. Dan Forensik Digit.*, vol. 2, no. 2, pp. 77–81, 2019, doi: 10.14421/csecurity.2019.2.2.1625.
[12] D. Wahyudi, "Keamanan Jaringan Komputer: Reconnaissance," *Keamanan Jar. Komput. Reconnaiss.*, vol. 7, no. 7, pp. 1–7, 2017.
[13] Balbix, "What is Vulnerability Scanning," *Balbix*, Jan. 24, 2020. https://www.balbix.com/insights/what-is-vulnerability-scanning/ (accessed Feb. 09, 2022).
[14] H. Herdianti and F. Umar, "Analisis Keamanan Website Menggunakan Teknik Footprinting dan Vulnerability Scanning," *INFORMAL Inform. J.*, vol. 5, no. 2, pp. 43–48, 2020 doi: 10.19184/isj.v5i2.18941.
[15] F. Wibowo, H. Harjono, and A. P. Wicaksono, "Uji Vulnerability pada Website Jurnal Ilmiah Universitas Muhammadiyah Purwokerto Menggunakan OpenVAS dan Acunetix WVS," *J. Inform.*, vol. 6, no. 2, pp. 212–217, 2019 doi: 10.31294/ji.v6i2.5925.
[16] H. Azis and F. Fattah, "Analisis Layanan Keamanan Sistem Kartu Transaksi Elektronik Menggunakan Metode Penetration Testing," *Ilk. J. Ilm.*, vol. 11, no. 2, pp. 167–174, 2019, doi: 10.33096/ilkom.v11i2.447.167-174.
[17] B. V. Tarigan, A. Kusyanti, and W. Yahya, "Analisis Perbandingan Penetration Testing Tool Untuk Aplikasi Web," *J. Pengemb. Teknol. Inf. Dan Ilmu Komput. E-ISSN*, vol. 2548, p. 964X, 2017.