Jurnal Algoritma
E-ISSN: 2302-7339 | P-ISSN: 1412-3622
INSTITUT TEKNOLOGI GARUT

https://jurnal.itg.ac.id/index.php/algoritma
DOI: 10.33364/algoritma/v.21-2.1644

Evaluasi Celah Keamanan *Website* Dana Pensiun X Melalui Penetration Testing Berdasarkan ISSAF Framework

Fransiskus Mario Hartono Tjiptabudi[1*], Ricky Imanuel Ndaumanu[2]
[1]STIKOM Uyelindo Kupang, Indonesia
[2]Universitas Widya Dharma Pontianak, Indonesia

***email:** tjiptabudifrans@gmail.com

Info Artikel
Dikirim: 14 Mei 2024
Diterima: 11 Juli 2024
Diterbitkan: 30 November 2024

Kata kunci:
Keamanan Sistem;
Kerangka Kerja ISSAF;
Penetration Testing;
Serangan Siber;
Website;

ABSTRAK

Dapen X merupakan dana pensiun penyelenggara program pensiun untuk peserta yang merupakan karyawan dari sebuah lembaga keuangan. Dalam mendukung proses bisnisnya yang berkaitan dengan pengelolaan data dan juga informasi, Dapen X telah menerapkan sebuah *website*. Mengingat bahwa data yang dikelola dan manfaat yang diberikan oleh *website* tersebut sangat krusial maka rentan menjadi sasaran serangan siber. Berkaca pada berbagai kasus serangan siber yang terjadi, maka perlu dilakukan pencegahan akan hal tersebut terhadap *website* Dapen X sehingga wajib dilakukan pengujian tingkat keamanan *website* secara menyeluruh antara lain dengan mengidentifikasi celah keamanan, memahami risiko keamanan sistem, mengkaji keamanan *server* sebagai bentuk pertahanan dari pencurian data dan pelanggaran keamanan. Oleh karena itu, penelitian ini bertujuan untuk melakukan *penetration testing* terhadap *website* Dapen X berdasarkan kerangka kerja ISSAF. Adapun hasil yang diperoleh yakni adanya temuan sebanyak 21 kerentanan yang terdiri dari 6 kerentanan Tingkat menengah (*medium*) dan 15 kerentanan tingkat rendah (*low*). Penelitian ini menghasilkan beberapa rekomendasi perbaikan yang menjadi dasar pijakan untuk meningkatkan keamanan *website* Dapen X dalam rangka mencegah terjadinya serangan siber dari pihak luar.

1. PENDAHULUAN

Internet merupakan teknologi yang perkembangannya sangat pesat saat ini, dan seiring berjalannya waktu semakin memberikan manfaat di segala bidang yang dapat dirasakan oleh masyarakat dalam kehidupan sehari-hari. Hal ini terjadi karena fungsi internet semakin meluas, yang mana tidak hanya sebagai sarana pencarian infomasi, tetapi juga dapat dimanfaatkan sebagai sarana untuk melakukan komunikasi, pendidikan, bisnis, dan lain sebagainya secara cepat dan mudah dengan memanfaatkan sebuah aplikasi bernama *website*.

Penggunaan *website* telah banyak diterapkan oleh berbagai kalangan masyarakat maupun berbagai lembaga baik yang berorientasi profit maupun non-profit untuk mendukung proses bisnisnya [1], tidak terkecuali Dapen X sebagai lembaga dengan tugas penyelenggara program pensiun manfaat pasti yang mengelola dan mengembangkan dana pensiun untuk menjamin kontinuitas pendapatan untuk para pesertanya. Dapen X menerapkan sebuah *website* sebagai media informasi dan media pengelolaan data dana pensiun karena dianggap efektif, efisien dan mendukung proses bisnis [2] dan juga dapa memberikan manfaat lain berupa peningkatan keunggulan kompetitif bisnis ssebagai nilai tambah yang signifikan [3]. Karena *website* tersebut mengelola data penting dan memberi manfaat yang krusial maka tentu hak aksesnya terbatas sehingga rentan menjadi target serangan siber.

Serangan siber menjadi momok menakutkan bagi penerapan *website* untuk mendukung proses bisnis, kasus pembobolan data pengguna Tokopedia sebagai *e-commerce* terbesar di Indonesia yang kemudian disebar ke Dark Web [4] menjadi salah satu contoh. Berkaca pada kasus tersebut maupun kasus-kasus serangan siber lainnya yang marak terjadi, maka perlu dilakukan pencegahan terhadap serangan siber atas *website* Dapen X yang tentunya dapat merugikan. Hal tersebutlah yang menjadi fokus permasalahan pada penelitian ini yang mana perlu untuk dilakukan pengujian tingkat keamanan *website* secara menyeluruh antara lain dengan mengidentifikasi area yang rentan terhadap serangan (celah keamanan), memahami risiko keamanan sistem dari serangan siber dan mengkaji keamanan *server* [5] untuk meningkatkan kemampuan keamanan agar terhindar dari pencurian data dan pelanggaran keamanan.

Pengujian tingkat keamanan *website* untuk memperoleh informasi tentang kerentanan yang berpotensi menjadi celah keamanan [6] dapat dilakukan melalui dua langkah, yaitu *vulnerability assessment* dan *penetration testing* [7] atau yang lebih dikenal dengan istilah VAPT. *Vulnerability assessment* difokuskan untuk memindai sistem atau jaringan dengan tujuan memperoleh celah kelemahan [8] yang berfungsi sebagai pintu belakang bagi penyerang untuk melakukan serangan siber [9], sedangkan *penetration testing* menjadi langkah selanjutnya yakni dengan mencoba mengeksploitasi sistem dengan cara yang sah untuk mengetahui adanya kemungkinan-kemungkinan sistem bisa tereksploitasi [10].

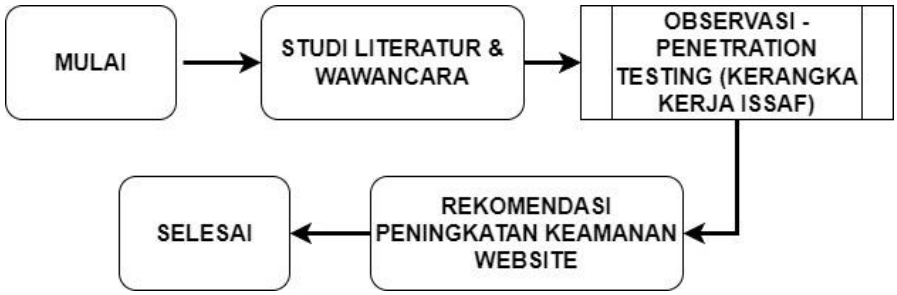
Terdapat berbagai metode atau kerangka kerja yang telah dikembangkan untuk digunakan sebagai panduan dalam pelaksanaan *penetration testing*, salah satunya yakni *Information System Security Assessment Framework* (ISSAF) yang merupakan kerangka kerja *penetration testing* dengan berbagai kelebihan dari aspek kontrol keamanan, yaitu bersifat naluriah dan memiliki struktur jelas yang memandu penguji melalui serangkaian fase yang kompleks sehingga secara optimal membantu penguji melakukan pengujian secara tepat dan lengkap serta terhindar dari kesalahan karena strategi serangan acak [11] [12].

Berbagai penelitian telah dilakukan terkait dengan pengujian keamanan *website*, antara lain dengan menggunakan *tools* OSINT untuk fase *information gathering* berdasarkan kerangka kerja OWASP [5] serta penggunaan metode VAPT dengan memanfaatkan Nessus *tools* [6]. Penelitian selanjutnya yakni pelaksanaan analisis dengan membandingkan hasil pengujian keamanan *website* menggunakan berbagai *tools* seperti Wapiti, Skipfish dan Arachni [8] serta KaliLinux, WireShark dan Zenmap [13]. Selain penelitian-penelitian tersebut, terdapat sebuah penelitian yang menggunakan kerangka kerja ISSAF namun terbatas pada fase *vulnerability identification* [14]**.** Seluruh penelitian tersebut bertujuan untuk melakukan simulasi serangan yang kemudian didokumentasikan sebagai laporan evaluasi kepada pemangku kepentingan terkait, dan dijadikan referensi untuk pemberian rekomendasi dalam meminimalisir tingkat kerentanan sistem.

Berdasarkan permasalahan yang terjadi serta berkaca pada rujukan penelitian sebelumnya, maka penelitian ini dilaksanakan dengan tujuan untuk melakukan pengujian agar dapat mengetahui celah keamanan pada *website* Dapen X, yang diperoleh melalui *penetration testing* berdasarkan kerangka kerja ISSAF, sehingga dapat memberikan informasi mengenai tingkat keamanan *website* dan memberikan rekomendasi-rekomendasi perbaikan guna meningkatkan keamanan *website* Dapen X dalam rangka mencegah terjadinya serangan siber dari pihak luar.

2. METODE PENELITIAN

Adapun metode penelitian yang diterapkan adalah metode kualitatif dengan pendekatan studi kasus, sedangkan tahapan penelitian yang akan dilakukan meliputi pengumpulan data awal, *penetration testing* pada *website* Dapen X, serta pemberian rekomendasi berdasarkan hasil pengujian seperti yang ditunjukkan pada Gambar 1:



Gambar 1. Alur penelitian

Gambar 1 menunjukkan alur tahapan yang dilakukan dalam penelitian, dimulai dengan pengumpulan data awal. Secara umum, pengumpulan data dalam penelitian ini dilakukan dengan beberapa cara yaitu:

1. Studi literatur

Proses pengumpulan data yang dilakukan dengan mencari sumber referensi yang relevan sebagai pendukung penelitian untuk dijadikan sebagai teori dasar yang menunjang penelitian sekaligus menjadi sebagai salah satu bahan penelitian. Adapun sumber referensi yang dimaksud antara lain dalam bentuk buku, artikel jurnal baik secara *offline* maupun dari internet. Dalam penelitian ini, studi literatur dilakukan dengan tujuan untuk mempelajari teori dan teknik penetrasi pada pengujian yang akan dilakukan pada *website* Dapen X.

2. Wawancara

Merupakan cara pengumpulan data melalui proses penyampaian serangkaian pertanyaan yang telah disusun sebelumnya kepada pihak yang menjadi sumber informasi, dan langsung dijawab pada saat itu juga. Dalam penelitian ini, wawancara dilakukan dengan pihak Dapen X sebagai pengelola *website* untuk memperoleh gambaran umum tentang *website* tersebut serta permasalahan dari segi keamanan yang sering terjadi, sekaligus memastikan kesepakatan dan izin untuk pelaksanaan *penetration testing*.

3. Observasi

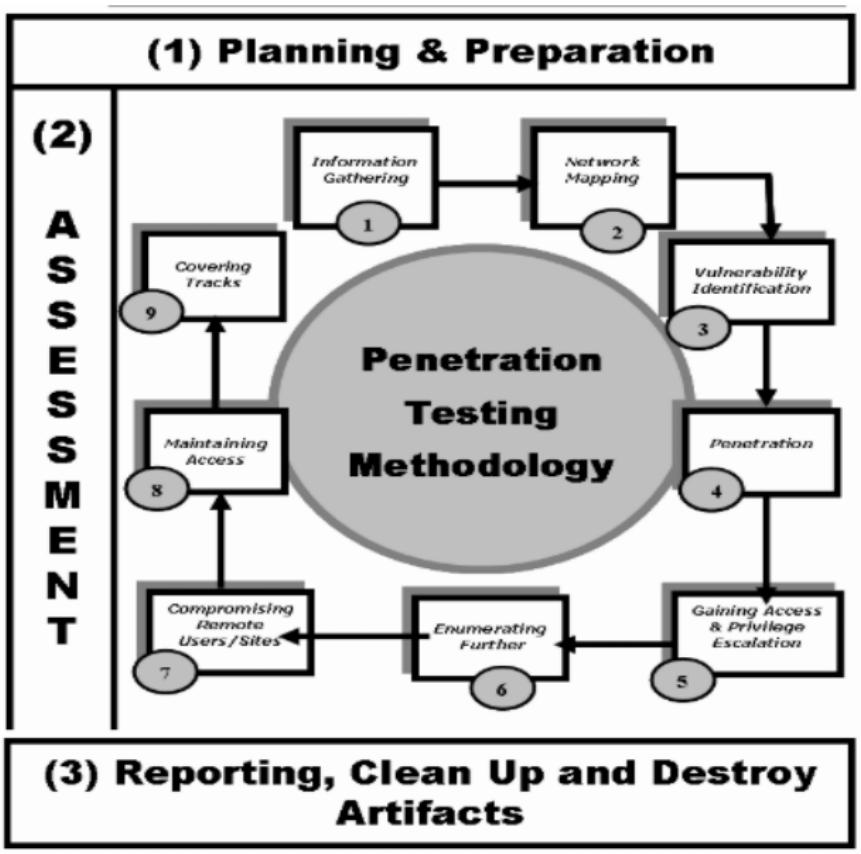
Observasi dilaksanakan untuk mengamati dan mencatat kejadian-kejadian faktual pada objek yang diamati. Observasi pada penelitian ini dilakukan secara langsung pada *website* Dapen X melalui fase *penetration* berdasarkan kerangka kerja ISAAF dengan tujuan untuk mendeteksi celah keamanan yang akan menjadi risiko pada *website* Dapen X.

ISSAF sendiri merupakan sebuah metodologi atau kerangka kerja *penetration testing* yang dikembangkan oleh OISSG (*Open Information System Security Group*) untuk mengevaluasi jaringan, sistem dan kontrol aplikasi dengan menyiapkan proses *penetration testing* secara optimal untuk membantu pelaksanaan pengujian secara lengkap dan benar. Secara umum, terdapat 3 tahapan besar dan 9 fase pengujian pada ISSAF[15]. Adapun ketiga tahapan tersebut yaitu perencanaan dan persiapan, penilaian, serta pelaporan, pembersihan, dan penghancuran artefak.

Tahapan perencanaan dan persiapan terdiri dari langkah-langkah pertukaran informasi awal, perencanaan dan persiapan ujian, yang mana terdapat perjanjian formal yang harus disepakati oleh kedua belah pihak. Dengan perjanjian tersebut akan memberikan perlindungan hukum bagi kedua belah pihak.

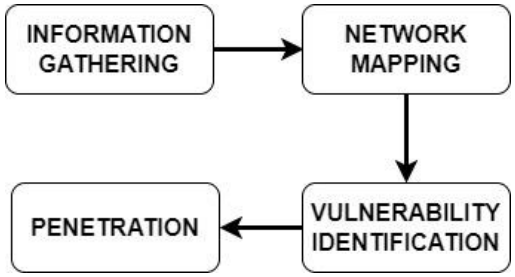
Tahapan penilaian merupakan tahapan pengujian yang dimulai dengan fase *information gathering*, yaitu fase pengumpulan informasi umum tentang *website* target. Fase kedua adalah *network mapping*, yakni pengumpulan informasi spesifik tentang jaringan *web* target. Fase ketiga adalah *vulnerability identification*, yaitu pelaksanaan *scanning* kerentanan pada *web* target. Fase keempat adalah *penetration*, yakni pelaksanaan simulasi serangan yang bertujuan untuk menemukan lubang keamanan pada *website*. Fase kelima adalah *gaining access & privilege escalation*, yang merupakan fase pengujian akses ke *website* target. Fase keenam adalah *enumerating further*, yakni fase mencari informasi terkait *password* dari *website* target. Fase ketujuh adalah *compromise remote user/sites*, yaitu fase melakukan *remote* ke *website* target. Fase kedelapan adalah *maintaning access* yakni proses penanaman *backdoor* ke dalam *website* target. Fase terakhir adalah *covering tracks* yaitu proses menghilangkan *log* serangan yang telah dilakukan pada *website* target.

Setelah tahapan penilaian dilakukan, tahapan selanjutnya adalah pelaporan, pembersihan, dan penghancuran artefak sekaligus menjadi tahapan akhir dari kerangka kerja ISSAF. Dalam tahapan ini, semua informasi yang tersimpan pada *website* target wajib dihilangkan karena dapat menjadi jalur yang bisa dimanfaatkan oleh orang lain untuk melakukan serangan. Selain itu juga dilakukan pelaporan hasil pengujian. Adapun tahapan besar serta fase-fase dalam kerangka kerja ISSAF dapat dilihat pada Gambar 2.



Gambar 2. Kerangka kerja ISSAF

Secara detail, pelaksanaan *penetration testing* berdasarkan kerangka kerja ISSAF yang akan dilakukan terhadap *website* Dapen X hanya terbatas pada 4 fase pengujian yang tampak pada Gambar 3. Hal tersebut ditetapkan pada tahapan perencanaan dan persiapan, yakni melalui proses diskusi antara pihak peneliti selaku penguji dan pihak Dapen X dengan mempertimbangkan segala risiko sehingga disepakati bahwa izin yang diberikan hanya sampai pada fase penetrasi sesuai dengan kerangka kerja ISSAF.



Gambar 3. Fase-fase *penetration testing*

Gambar 3 menunjukkan fase-fase dalam *penetration testing* yang akan dilakukan pada penelitian ini berdasarkan kerangka kerja ISSAF. *Penetration testing* diawali dengan fase pengumpulan informasi, yang mana bertujuan untuk mengumpulkan informasi umum [16] dari *website* Dapen X selaku target pengujiian. Fase kedua adalah tahap pemetaan jaringan, yakni proses pengumpulan informasi secara spesifik tentang jaringan pada *website* target melalui pemindaian *port* [17]. Fase ketiga adalah identifikasi kerentanan, yaitu

proses pemindaian *website* dengan menggunakan aplikasi sebagai alat pemindaian dengan tujuan memperoleh bagian-bagian yang rentan [13] pada *website* target. Fase terakhir adalah fase penetrasi dengan mencoba melakukan simulasi penyerangan terhadap *website* target melalui SMB *enumeration* dan FTP *enumeration* dengan tujuan untuk mendapatkan akses secara ilegal dengan cara mengakali sistem keamanan [14].

Setelah melewati tahapan *penetration testing*, maka tahap terakhir yang dilakukan adalah membuat laporan yang berisi rangkuman hasil pengujian serta rekomendasi-rekomendasi perbaikan untuk peningkatan keamanan *website* yang akan diberikan kepada pihak Dapen X dalam rangka mencegah terjadinya serangan siber dari pihak luar.

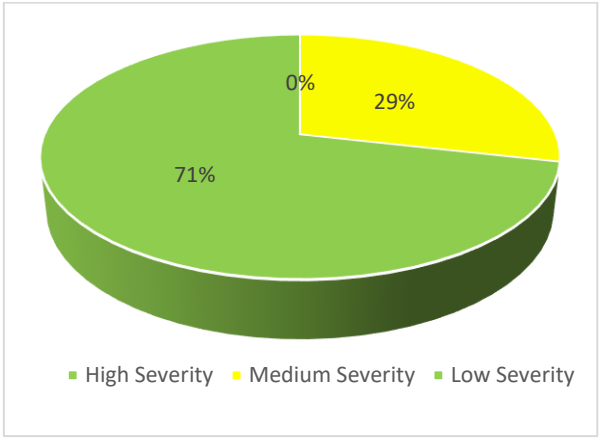
3. HASIL DAN PEMBAHASAN

3.1. Persiapan Pengujian

Fokus dari penelitian ini yakni pada proses *penetration testing* dengan tujuan untuk meperoleh celah keamanan pada *website* target, sehingga nantinya dapat dilakukan penanganan berdasarkan rekomendasi yang dihasilkan. *Penetration testing* dilaksanakan berdasarkan tahapan pada kerangka kerja ISSAF dengan menggunakan sistem operasi Windows 11 dan Kali Linux, serta beberapa aplikasi penetrasi sebagai kebutuhan perangkat lunak.

3.2. *Penetration Testing* Berdasarkan Kerangka Kerja ISSAF

Seperti yang telah dibahas sebelumnya, fase yang dilakukan pada proses *penetration testing* adalah fase *information gathering*, *network mapping*, *vulnerability identification* dan *penetration*. Gambar 4 menunjukkan grafik ringkasan total temuan celah keamanan yang dapat diperoleh melalui proses *penetration testing* dan dikelompokkan berdasarkan tingkat dan dampak terhadap *website* Dapen X.



Gambar 4. Sebaran temuan melalui *penetration testing*

Berdasarkan Gambar 4, dapat dilihat rangkuman hasil temuan sebanyak 21 kerentanan yang terdiri dari enam temuan dengan tingkat kerentanan menengah (*medium*) dan 15 temuan tingkat kerentanan rendah (*low*). Adapun temuan yang dinilai memiliki dampak yang paling besar adalah temuan tentang *port-port* yang terbuka dan juga *Cross-Site Scripting* (XSS). *Cross-Site Scripting* (XSS) merupakan salah satu model serangan berbasis injeksi *code* dan merupakan temuan yang sering ditemukan dan menjadi momok bagi *website*. Temuan ini juga sejalan dengan temuan yang diperoleh pada pengujian terhadap *website* www.stephward.co.za [14].

Information gathering merupakan fase pertama dalam proses *penetration testing* dengan aktivitas utama yakni pengumpulan informasi yang bersifat umum sebanyak mungkin tentang *website* target. Informasi-informasi tersebut berupa IP *address*, *server* dari *website* target yang berhasil terdeteksi, dan informasi lainnya yang kelak dijadikan dasar dalam melakukan penetrasi. Tabel 1 berikut menunjukkan bahwa terdapat tujuh jenis informasi yang berusaha dikumpulkan pada fase *information gathering*, yang mana lima informasi diantaranya berhasil diperoleh dan dua informasi lainnya gagal diperoleh. Adapun rincian hasil dari fase ini dapat dilihat pada Tabel 1.

Tabel 1. Hasil fase *information gathering*

Objek	Aplikasi	Hasil
Temukan keberadaan *web* target	NSLookup	√
Periksa info registrasi domain dan blok IP yang dimiliki	NSLookup	√
Periksa nama resmi server	NSLookup	√
Periksa keberadaan pencarian DNS terbalik	Dig	√
Periksa keberadaan pencarian IP terbalik	Reverse IP Lookup	x
Periksa pencarian basis data spam/penyerang	Spamhaus	x
Sistem pencarian/situs survei jaringan	Nmap	√

Setelah menemukan alamat IP dari *website* target, fase selanjutnya yang dilakukan yaitu *network mapping* yakni aktivitas menggali informasi lebih spesifik mengenai jaringan *website* target melalui pemindaian *port* dengan menggunakan aplikasi Nmap. Tabel 2 berikut menyajikan hasil pemindaian menggunakan aplikasi Nmap dan memberi informasi bahwa terdapat beberapa *port* TCP penting pada *website* target yang berada dalam status terbuka (*open*). Hasil ini memiliki kemiripan dengan hasil pemindaian pada *website* Universitas Internasional Batam [17], yang tentunya cukup berisiko karena *port-port* tersebut dapat menjadi celah bagi penyerang untuk melakukan serangan terhadap *website* [13].

Tabel 2. Hasil pemindaian *port*

Port	Status	Layanan
20	Tertutup	FTP-data
21	Terbuka	FTP
22	Tertutup	SSH
53	Terbuka	Domain
80	Terbuka	SSL
110	Tertutup	POP3
143	Tertutup	IMAP
443	Terbuka	HTTPS
445	Tertutup	SMB

Vulnerability identification merupakan fase pemindaian kerentanan yang dilakukan dengan menggunakan bantuan aplikasi ZAP. Zed Attack Proxy (ZAP) merupakan salah satu alat yang digunakan untuk melakukan pengujian keamanan dengan memindai *server* pada *website* target yang berhasil dideteksi pada fase *information gathering* sebelumnya. Hasil pemindaian dari fase ini menunjukkan bahwa *server* yang terkait dengan *website* Dapen X memiliki berbagai kerentanan, yang mana temuan-temuan kerentanan tersebut bersifat sama dan ditemukan secara berulang-ulang baik yang dikategorikan sebagai tingkat kerentanan menengah (*medium*) sebanyak enam temuan dan tingkat kerentanan rendah (*low*) sebanyak 15 temuan. Hasil temuan kerentanan tersebut dirangkum pada Tabel 3.

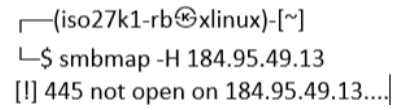
Tabel 3. Hasil identifikasi kerentanan

Kerentanan	Tingkat kerentanan
Missing 'HttpOnly' Cookie Attribute (HTTP)	*Low*
Session Cookie Without Secure Flag	*Low*
Cross-Site Scripting (XSS)	*Medium*
Cookie Without SameSite Attribute	*Low*
Missing Anti-clickjacking Header	*Medium*
Cross-Domain JavaScript Source File Inclusion	*Low*
Cookie No HttpOnly Flag	*Low*
Directory Listing Detected	*Low*
Open TCP Port: 443	*Medium*
Open TCP Port: 80	*Medium*

Temuan-temuan hasil pemindaian kerentanan umumnya memiliki perbedaan yang cukup mencolok antara satu *website* dengan *website* lainnya, misalnya hasil pada penelitian ini yang disajikan pada Tabel 3 berbeda dengan hasil dari berbagai penelitian sebelumnya [7], [9], [12]. Walaupun memperoleh hasil berbeda, namun semua

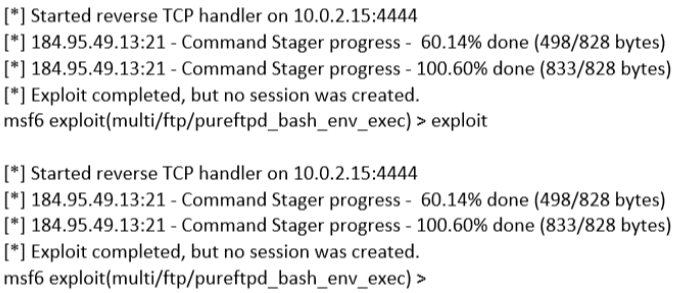
penelitian tersebut sepakat bahwa temuan kerentanan tersebut dapat menjadi celah bagi serangan siber dari pihak luar.

Fase terakhir dalam usaha *penetration testing* yang akan dilakukan dalam penelitian ini adalah fase *penetration*. Pada fase ini, penguji melakukan serangkaian jenis serangan terhadap *website* target melalui dua cara yakni SMB *enumeration* dan FTP *enumeration*. SMB *enumeration* digunakan dalam usaha penguji untuk mengakses dan mengeksploitasi *share drive* pada *server*, dan hasilnya dapat dilihat pada gambar berikut:



Gambar 5. Tangkapan layar proses SMB *enumeration*

Gambar 5 menunjukkan bahwa proses SMB *enumeration* tidak berhasil dilakukan karena *port* 445 tidak terbuka yang berarti bahwa tidak ada *share* SMB yang dapat diakses oleh penguji. Selain itu, proses FTP *enumeration* yang dilakukan juga memperoleh hasil yang sama. FTP *enumeration* sendiri digunakan sebagai cara untuk mencoba menguasai FTP *server*, yang mana pada pengujian ini *session* tidak berhasil dibuat seperti yang tampak pada Gambar 6. Walaupun pada pengujian ini tidak berhasil memperoleh informasi yang berkaitan dengan *password*, tetapi informasi *cookies* pada *website* target berhasil diperoleh dan dapat dilihat pada hasil *vulnerability identification* menggunakan ZAP yang telah dibahas sebelumnya. Hal tersebut menunjukkan bahwa *website* Dapen X masih memiliki celah yang rentan terhadap penyerangan menggunakan skrip lintas situs/*Cross-Site Scripting* (XSS).



Gambar 6. Tangkapan layar proses FTP *enumeration*

Dikarenakan *server website* target memiliki kemampuan yang cukup mumpuni maka kedua proses yang dilakukan baik SMB *enumeration* maupun FTP *enumeration* gagal memperoleh hasil yang ditargetkan seperti memperoleh hak akses admin pengelola *website* target dan akses terhadap CPanel dari *website* target. Kegagalan tersebut terjadi karena semua permintaan yang ditujukan kepada *server website* target tidak dapat melewati *firewall* [6]. Adapun hasil dari fase ini dapat dilihat pada Tabel 8.

Tabel 8. Hasil penetrasi

Jenis Akses	Target	Status	Hasil
Akses admin pengelola *website*	*Username* dan *password*	Gagal diperoleh	Gagal
Akses CPanel *website*	*Username* dan *password*	Gagal diperoleh	Gagal

3.3. Rekomendasi

Berdasarkan hasil *penetration testing* yang telah dilakukan, maka dapat dirangkum beberapa rekomendasi secara umum untuk menjadi dasar dalam proses peningkatan keamanan *website* Dapen X dalam rangka mencegah terjadinya serangan siber dari pihak luar. Rekomendasi tersebut yaitu:

1. Menerapkan pemblokiran terhadap usaha *login* yang tidak valid, misalnya dengan menerapkan *Testing for Weak Lock Out Mechanism* (OTG-AUTHN-003) guna mencegah serangan berbasis *login*.
2. Jenis serangan skrip lintas situs/*Cross-Site Scripting* (XSS) tergolong cukup membahayakan sistem. XSS dapat memanfaatkan *form* yang ada untuk mengeksekusi kode. Salah satu solusi pencegahannya adalah dengan menggunakan simbol seperti (“<>”, “/”) pada *form* sebagai validasi sehingga kode XSS tidak dapat dieksekusi.
3. *Port-port* TCP merupakan celah keamanan pada *website* yang rentan untuk dimanfaatkan, sehingga penutupan semua *port* TCP atau pembuatan *custom port* dengan mengubah *port* penting agar tidak berada pada *port default* dapat menjadi cara untuk peningkatan keamanan.
4. Atur *secure flag* menjadi '*true*' pada kode yang berfungsi sebagai *cookie.*
5. Konfigurasikan *header* HTTP "*Access-Control-Allow-Origin*" ke kumpulan domain yang lebih ketat atau hapus seluruh *header Cross Origin Resource Sharing* (CORS) agar memungkinkan *browser* menerapkan *Same Origin Policy* (SOP).
6. Aplikasi penjelajah *web* saat ini telah mendukung *header HTTP Content-Security-Policy* dan *X-Frame-Options.* Wajib mengatur salah satu dari kedua *settingan* tersebut pada semua halaman *web* yang dikembalikan oleh situs.
7. *Output* kesalahan seperti *file system path* tidak boleh dikirim melalui *remote client* karena dapat diperoleh oleh pihak lain. Oleh karena itu, *log* kesalahan (*error log*) dapat dijadikan tujuan pengiriman *output* kesalahan oleh admin.
8. Menerapkan *Intrusion Detection System* (IDS) sebagai monitoring serangan yang terjadi baik dari dalam maupun dari luar sistem.
9. Melakukan *backup* data berkala dalam rentang waktu yang pendek untuk mengantisipasi kehilangan data yang terbaru.

4. KESIMPULAN

Berdasarkan penelitian yang telah dilakukan melalui *penetration testing* berdasarkan kerangka kerja ISAAF terhadap *website* Dapen X, dapat diambil kesimpulan bahwa terdapat celah keamanan yang cukup berbahaya walaupun dalam jumlah sedikit, yakni sebanyak 21 temuan kerentanan dengan tingkat kerentanan menengah (*medium*) sebanyak 6 temuan dan tingkat kerentanan rendah (*low*) sebanyak 16 temuan. Celah yang perlu mendapat perhatian khusus yakni temuan tentang aktivitas *Cross-Site Scripting* (XSS)/skrip lintas situs serta *port* TCP yang terbuka sehingga berisiko terhadap serangan. Walaupun demikian, secara garis besar dapat dinyatakan bahwa *website* Dapen X tergolong aman, karena berdasarkan hasil pengujian tidak berhasil untuk ditembus. Untuk penelitian selanjutnya, dapat disarankan untuk menggunakan metode ataupun kerangka kerja *penetration testing* serta aplikasi penetrasi yang lain sehingga hasilnya menjadi semakin lengkap dan juga dapat dibandingkan. Selain itu, hasil penelitian *penetration testing* bisa dikombinasikan dengan manajemen risiko agar menjadi standar mitigasi.

UCAPAN TERIMA KASIH

Rasa hormat dan terima kasih disampaikan kepada pihak Dapen X dan LP3M STIKOM Uyelindo Kupang atas kesempatan yang diberikan serta dukungan penuh terhadap penelitian ini. Terima kasih juga atas sumbangsih wawasan dan pemikiran dari rekan-rekan dosen STIKOM Uyelindo Kupang.

REFERENSI

[1] T. Andreas and Tony, “Sistem Informasi Manajemen Proses Bisnis General Affairs Berbasis Web,” *JIKSI*, vol. 11, no. 1, pp. 1–8, 2023.

[2] F. M. H. Tjiptabudi and R. Bernardino, “Indonesia terrestrial border control information system and business processes alignment,” *International Journal of Business Process Integration and Management*, vol. 10, no. 1, pp. 51–61, 2020, doi: 10.1504/IJBPIM.2020.113114.

[3] F. M. H. Tjiptabudi, "Integrated Information and Communication Media Modeling Based on Organization Goal-Oriented Requirement Engineering (OGORE)," *Journal of Information System)*, vol. 19, no. 1, pp. 28–42, 2023.

[4] R. CNBC Indonesia, "Cerita Lengkap Bocornya 91 Juta Data Akun Tokopedia," CNBC.

[5] A. A. B. A. Wiradarma and G. M. A. Sasmita, "IT Risk Management Based on ISO 31000 and OWASP Framework using OSINT at the Information Gathering Stage (Case Study: X Company)," *International Journal of Computer Network and Information Security*, vol. 11, no. 12, pp. 17–29, Dec. 2019, doi: 10.5815/ijcnis.2019.12.03.

[6] C. O. N. Susanto, K. N. F. Rizko, and D. Purbohadi, "Security Assessment Using Nessus Tool to Determine Security Gaps on the Repository Web Application in Educational Institutions," *Emerging Information Science and Technology*, vol. 1, no. 2, pp. 58–62, 2020, doi: 10.18196/eist.128.

[7] Y. Thurfah Afifa Rosaliah and B. Hananto, *Pengujian Celah Keamanan Website Menggunakan Teknik Penetration Testing dan Metode OWASP TOP 10 pada Website SIM xxx*. 2021.

[8] I. P. M. Y. Pratama, A. S. Gede, K. Mahendra, I. M. E. Listartha, and D. A. J. Saskara, "Perbandingan Vulnerability Analysis Pada Website Menggunakan Tools WAPITI, SKIPFISH, DAN ARACHNI," *Jurnal Teknologi Informasi*, vol. 6, no. 2, pp. 187–193, 2022, [Online]. Available: http://testphp.vulnweb.com/.

[9] F. Y. Fauzan and Syukhri, "Analisis Metode Web Security PTES (Penetration Testing Execution And Standart) Pada Aplikasi E-Learning Universitas Negeri Padang," *Voteknika: Jurnal Vocational Teknik Elektronika dan Informatika*, vol. 9, no. 2, pp. 105–111, 2021, [Online]. Available: http://ejournal.unp.ac.id/index.php/voteknika/

[10] T. W. Hua, S. A. Ismail, and H. Abas, "Penetration Testing Process: A Preliminary Study," *Open International Journal of Informatics (OIJI*, vol. 10, no. 1, pp. 37–46, 2022.

[11] F. Mahtuf, P. Hatta, and E. Wihidiyat, "Pengembangan Laboratorium Virtual untuk Simulasi Uji Penetrasi Sistem Keamanan Jaringan," *JOINTECS) Journal of Information Technology and Computer Science*, vol. 4, no. 1, pp. 2541–3619, 2019, doi: 10.31328/jo.

[12] M. A. Nabila, P. E. Mas'udia, and R. Saptono, "Analysis and Implementation of the ISSAF Framework on OSSTMM on Website Security Vulnerabilities Testing in Polinema," *Journal of Telecommunication Network*, vol. 13, no. 1, pp. 87–95, 2023.

[13] E. P. Silmina, A. Firdonsyah, and R. A. A. Amanda, "Analisis Keamanan Jaringan Sistem Informasi Sekolah Menggunakan Penetration TEST Dan ISSAF," *Transmisi*, vol. 24, no. 3, pp. 83–91, Aug. 2022, doi: 10.14710/transmisi.24.3.83-91.

[14] H. Herman, I. Riadi, Y. Kurniawan, and I. A. Rafiq, "Analisis Keamanan Website Menggunakan Information System Security Asessment Framework(ISSAF)," *Jurnal Teknologi Informatika dan Komputer*, vol. 9, no. 1, pp. 126–136, Mar. 2023, doi: 10.37012/jtik.v9i1.1439.

[15] I. G. A. S. Sanjaya, G. M. A. Sasmita, and D. M. S. Arsa, "Information technology risk management using ISO 31000 based on issaf framework penetration testing (Case study: Election commission of x city)," *International Journal of Computer Network and Information Security*, vol. 12, no. 4, pp. 30–40, Aug. 2020, doi: 10.5815/ijcnis.2020.04.03.

[16] C. Budi Setiawan, D. Hariyadi, A. Sholeh, A. Wisnuaji, A. Yani Yogyakarta, and P. Widya Adijaya Nusantara, "Pengembangan Aplikasi Information Gathering Berbasis HybridApps," vol. 5, 2022.

[17] S. E. Prasetyo and N. Hassanah, "Analisis Keamanan Website Universitas Internasional Batam Menggunakan Metode ISSAF," *JURNAL ILMIAH INFORMATIKA*, vol. 09, no. 02, pp. 82–86, 2021.