Analisis Keamanan Sistem Informasi Berdasarkan Pendekatan ISSAF Pada Website XYZ

1st Yulia Wahyu Ningsih
Sistem Informasi
Telkom University
Surabaya, Indonesia
yuliawahyuningsih@student.telkomuniversity.ac.id

2nd Muhammad Nasrullah
Sistem Informasi
Telkom University
Surabaya, Indonesia
emnasrul@telkomuniversity.ac.id

3rd Purnama Anaking
Sistem Informasi
Telkom University
Surabaya, Indonesia
purnamaanaking@telkomuniversity.ac.id

***Abstrak* — Perkembangan teknologi informasi pada saat ini telah menjadi suatu kebutuhan dalam meningkatkan efisiensi kinerja suatu organisasi, terutama aspek keamanan merupakan kunci penting yang perlu diperhatikan pada pengembangan *website* XYZ sebagai pintu utama bagi calon mahasiswa baru untuk mendaftar masuk dan mengakses informasi yang berkaitan dengan kegiatan mahasiswa baru seperti jadwal tes, pendaftaran, pengisian formulir data diri, jadwal seleksi dan kegiatan lainnya. Dengan banyaknya calon pendaftar yang masuk melalui *website*, maka akan semakin tinggi potensi terhadap risiko celah keamanan terhadap *website.* XYZ pernah mendapatkan laporan bahwa *website* XYZ masih rentan terhadap serangan *phising.* Hal ini juga menjadi ancaman yang serius sehingga dapat merugikan kepercayaan pengguna terhadap kredibilitas Universitas XYZ. Dengan semakin bertambahnya calon mahasiswa yang akan mendaftar masuk, maka keamanan sistem harus mendapatkan perhatian khusus sebagai langkah untuk pencegahan potensi kerentanan. Pada penelitian ini dilakukan *penetration testing* melalui pendekatan *Information System Security Assessment Framework* (ISSAF). Hasil *penetration testing* pada penelitian menemukan bahwa *website* XYZ terdapat celah keamanan *Local File Inclusion* melalui *path traversal* yang telah ditemukan serta memiliki 16 celah kerentanan dengan 4 tingkat *medium,* 8 tingkat *low* dan 4 tingkat *informational.* Pada prioritas perbaikan akan difokuskan menuju celah *Local File Inclusion,* dengan penerapan *whitelist,* membatasi akses pada *directory /etc, ssh/, home,* terapkan *deploy waf* seperti *modsecurity Apache.* Hal ini bertujuan ntuk menjaga kepercayaan masyarakat terhadap Universitas XYZ dan menjaga *website* dari serangan di masa yang akan datang.**

***Kata kunci*— Keamanan Sistem Informasi, Penetration Testing, Website, ISSAF**

I. PENDAHULUAN

Dalam penggunaan aktivitas media sosial serta layanan *internet* saat ini, dapat dilihat dari hasil survey laporan Asosiasi Penyelenggara Jasa Internet Indonesia di tahun 2012 terdapat 63 juta pengguna *internet* di Indonesia yang terus meningkat sebesar 24,23 dari tahun sebelumnya. Hingga pada tahun 2019-2020 jumlah pengguna *internet* di Indonesia sebanyak 196,71 juta jiwa atau 73,7% dari keseluruhan penduduk Indonesia [1].

Menurut Badan Siber dan Sandi Negara (BSSN) 361 juta serangan siber yang masuk ke Indonesia dalam kurung waktu 1 Januari-26 Oktober 2023. Telah tercatat tiga jenis serangan siber dengan *traffic* tertinggi, yaitu *malware activity* dengan jumlah 42,79%, kemudian *trojan activity* dengan jumlah 35,40%, dan yang terakhir *information leak* sebesar 9,35%. Data kerugian akibat serangan siber mencapai RP 14,5 triliun pada tahun 2023 [2]. Salah satu *website* yang perlu dilindungi dari serangan siber adalah *website* XYZ yang dimiliki oleh Universitas XYZ. *Website* XYZ digunakan sebagai pintu utama yang menyediakan layanan terkait proses seleksi penerimaan mahasiswa baru di Universitas XYZ. Namun, berdasarkan wawancara dengan Kepada Divivi IT XYZ bahwa pihak Universitas XYZ pernah mendapatkan laporan adanya indikasi potensi serangan *phising* terhadap *website* XYZ dan belum pernah dilakukan kegiatan *maintenance* sejak diterima dari pihak ketiga pada tahun 2013. Hal ini dapat menimbulkan potensi serangan pencurian data yang dilakukan oleh pihak yang tidak berkepentingan.

Oleh karena itu, penelititan ini bertujuan untuk untuk menganalisis sistem keamanan yang terdapat pada situs *website* XYZ tersebut melalui pendekatan *Information Systems Security Assessment Framework* (ISSAF). Hal ini perlu dilakukan untuk mengembangkan strategi yang matang dalam pengelolaan dan pemeliharaan sistem teknologi informasi agar tetap terjaga, aman, dan sesuai dengan norma hukum yang berlaku. Hasil dari penelitian ini berupa dokumen rekomendasi perbaikan yang bertujuan untuk pengembangan sistem *website* XYZ.

II. KAJIAN TEORI

Kajian teori menekankan betapa krusialnya pengujian keamanan sistem untuk mencegah potensi serangan siber yang dapat merugikan Universitas. Dalam pengujian ini dipilih kerangka kerja ISSAF karena dalam melakukan identifikasi kelemahan pada sistem informasi. Dengan menggunakan beragam alat pendukung uji penetrasi,

pengujian keamanan dilakukan secara menyeluruh untuk meningkatkan perlindungan sistem tetap aman dari ancaman serangan eksternal.

A. Keamanan Sistem Informasi

Keamanan sistem informasi merupakan upaya tindakan dalam menjaga informasi dan sistem informasi akses ilegal, penggunaan, pengungkapan, perubahan atau penghancuran oleh pihak yang tidak memiliki kewenangan untuk memastikan terjaganya kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan data (*availability*) [3].

B. Black Box

Pada *black box testing* penguji hanya memiliki akses terbatas terhadap sistem target yang akan diuji. Dalam proses pengujian akan mencari dan memeriksa pada tiap celah sistem berdasarkan pengalaman, keahlian, serta pemahaman teknis dengan tujuan untuk mengevaluasi tingkat keamanan dari perspektif luar sistem dengan cara bertindak menempatkan diri dari posisi penyerang [4].

C. Uji Penetrasi

Uji penetrasi digunakan untuk menilai kemampuan sistem dalam melindungi jaringan, aplikasi, *end point* serta pengguna dari ancaman kejahatan siber eksternal atau internal. Tujuan dari uji penetrasi dilakukan adalah untuk menemukan risiko potensi celah keamanan yang mungkin timbul dalam sistem [5].

D. *Information System Security Assessment* (ISSAF)

Information System Security Assessment (ISSAF) membantu organisasi dalam mengidentifikasi dan mengelola risiko ancaman keamanan secara terpadu dan komperehensif, ISSAF memiliki fleksibilitas dan skalabilitas yang memungkinkan untuk diterapkan secara efektif oleh berbagai jenis lingkup organisasi dengan kebutuhan keamanan yang beragam, sehingga dapat disesuaikan dengan karakteristik dan kebutuhan setiap organisasi [6]. ISSAF memiliki sembilan tahap pengujian, yaitu:

1. *Information Gathering* tahap pengumpulan semua informasi dasar mengenai sistem target
2. *Network Mapping* tahap identifikasi jaringan, arsitektur sistem dan pemetaan *port* terhadap sistem target
3. *Vulnerability Identification* tahap identifikasi potensi celah keamanan yang terdapat dalam sistem
4. *Penetration Testing* tahap simulasi uji serangan terhadap sistem
5. *Gaining Access and Privilege Escalation* tahap mendapatkan akses labih dalam
6. *Enumerating Further* tahap pencarian akses yang memungkinkan untuk mendapatkan *password* dan *username* sistem
7. *Compromise Remote User/Sites* tahap pengujian sistem secara *remote* atau dari jarak jauh
8. *Maintaining Access* tahap simulasi mempertahankan akses dari serangan *backdoor*
9. *Covering Tracks* tahap penghapusan jejak serangan yang telah dilakukan agar tidak terdeteksi [7]

E. *Common Vulerability Scoring System* (CVSS)

Common Vulnerability Scoring System (CVSS) merupakan sistem standar penilaian yang digunakan untuk mengukur tingkat suatu kerentanan pada sistem informasi. Pada setiap nilai terdapat kategori keparahan dalam sistem [8]. Dapat dilihat pada Tabel 1

TABEL 1
(Skala Penliaian CVSS) (Sumber: [8])

Skor	Tingkat Keparahan
0.0	*None*
0.1 – 3.9	*Low*
4.0 – 6.9	*Medium*
7.0 – 8.9	*High*
9.0 – 10.0	*Critical*

F. VMWare

VMWare merupakan mesin virtualisasi yang memungkinkan untuk melakukan pengujian, pengembangan serta implementasi dalam lingkungan terpisah tanpa harus mengubah sistem operasi utama. Hal ini menjadi solusi penting dalam keamanan sistem informasi yang efektif dna relevan. VMWare yang dikembangkan oleh Wmware, Inc juga memiliki kemampuan migrasi melalui *virtual machine* sehingga dapat digunakan pada perangkat komputer yang memiliki spesifikasi rendah

G. Alat-Alat Uji Penetrasi

Dalam pengujian keamanan *website* XYZ, dibutuhkan alat-alat pengujian yang membantu menemukan celah kerentanan selama berlangsungnya pengujian. Berikut alat-alat yang digunakan:

1. Wappalyzer digunakan untuk mengidentifikasi teknologi pada suatu situs [9]
2. Nslookup digunakan untuk pengumpulan informasi tekait dengan *Domain Name System* (DNS) dari suati sistem [10]
3. Whois untuk mengidentifikasi informasi *register* suatu *website* [11]
4. Nmap untuk mengidentifikasi suatu jaringan dan pemindaian *port* terbuka [12]
5. Ssllabs.com digunakan untuk pemindaian keamanan pada *secure Sockets Layer* (SSL) dan *Transport Layer Security* (TLS) sistem target [13]
6. Nikto untuk pemindaian celah kerentanan jaringan sistem melalui pengujian secara kompehensif [14]
7. OWASP ZAP digunakan untuk mengidentifikasi potensi celah kerentanan dalam sistem [15]
8. SQL *Map* digunakan untuk mendeteksi titik potensial pada *website* dan melakukan eksploitasi kerentanan melalui SQL *injection* [16]
9. Burp Suite digunakan untuk mendeteksi dan mengeksploitasi kerentanan dalam sistem [17]
10. Netcat digunakan untuk *remote admnistration* sebagai eksplorasi jaringan melalui *back end* menuju sistem target dari jarak jauh [18]

III. METODE

A. Metode Penelitian

Penelitian ini menggunakan pendekatan ISSAF dan metode *black box testing* dengan pengujian pada fugsionalitas sistem dengan melakukan identifikasi

kelemahan pada fitur dan menu, yang bertujuan untuk melakukan audit keamanan eksternal melalui skenario penyerangan dari luar. Peneliti juga melakukan wawancara yang bertujuan untuk mendapatkan data dan informasi yang digunakan untuk mengidentifikasi, mendiskusikan temuan, serta merumuskan rekomendasi perbaikan.

B. Bahan Penelitian

Bahan Penelitian menjadi salah satu faktor pendukung pada keberhasilan penelitian. Bahan pengujian digunakan selama uji celah keamanan berlangsung, bahan penelitian dapat dilihat pada Tabel 2

TABEL 2
(BAHAN PENELITIAN)

No	Tahap	Tools	Fungsi
1.	Sistem Operasi	VMWare, Kali Linux	Sistem operasi yang digunakan selama uji penetrasi
2.	*Information Gathering*	Search Engine, Wappalyzer dan Whois	Mengumpulkan informasi dasar terkait *website*
3.	*Network Mapping*	Nmap dan Ssllabs	Melakukan pemindaian dan pemetaan pada *port*
4.	*Vulnerability Assessment*	Owasp Zap, Nikto dan Manual Test	Melakan pemindain terhadap potensi celah kerentanan pada *domain*
5.	*Penetration Testing*	Burp Site, SQL Map dan Manual Test	Melakukan uji serangan XSS, SQL *injection* dan LFI
6.	*Gaining Access and Privilege Escalation*	Burp Suite	Melakukan hak akses lebih dalam
7.	*Enumerating Further*	Burp Suite	Melakukan pencarian mengenai *password* dan *username database*
8.	*Compromise Remote User/Sites*	Manual Test	Melakukan pengambilan hak akses jarak jauh terhadap *website*
9.	*Maintaining Access*	-	Melakukan penanaman *backdoor*
10.	*Covering Tracks*	-	Penghapusan *log* serangan

C. Alur Penelitian

Alur Penelitian ini berdasarkan pendekatan ISSAF Dapat dilihat pada Gambar 1

GAMBAR 1
(ALUR PENELITIAN)

Penelitian ini diawali dengan studi literatur terkait jurnal yang relevan mengenai pengujian, kemudian melakukan perizinan pengujian dan wawancara mengenai pengumpulan informasi dengan divisi IT Universitas XYZ. Uji penetrasi dilakukan pada tahap *assessment* dengan pendekatan ISSAF yang dimulai dengan *planning and preparation* dimana akan mengumpulkan dan informasi dasar terhadap *website* XYZ melaui wawancara. Selanjutnya pada tahap *assessment* dilakukan pengujian yang mencakup *information gathering* yaitu pengumpulan informasi dasar *website* XYZ, *network mapping* identifikasi dan pemetaan *port* jaringan, *vulnerability identification* identifikasi potensi celah kerentanan, *penetration* pengujian celah serangan, *gaining access and privilege escalation* untuk mendapatkan seberapa dalam akses yang bisa didapatkan, *enumerating further* tahap untuk mendapatkan *username* dan *password* sistem, *compromise remote user/sites* untuk mengambil alih hak akses kontrol dari jarak jauh, *maintaining access* penanaman *backdoor* pada sistem, dan *covering tracks* digunakan untuk menghilangkan jejak serangan. Kemudian akan dilakukan tahap *reporting, clean up and destroy artefacts* untuk menghapus segala kegiatan pengujian yang telah dilakukan.

IV. HASIL DAN PEMBAHASAN

A. ***Information Gathering***

Pada tahap ini dilakukan pencarian dan pengumpulan terhadap *website* XYZ untuk mengidentifikasi teknologi yang diterapkan oleh *website* XYZ melalui *tools* wappalyzer, selanjutnya dilakukan identifikasi mengenai informasi dasar seperti IP *address* melalui perintah nslookup XYZ, serta pencarian melalui whois yang menampilkan informasi sensitif seoerti *domain, data register,* URL, dan data *administrator website* XYZ. Pada tahap ini pengujian

menggunakan *tools search engine,* wappalyzer, nslookup dan whois dapat dilihat pada Tabel 3

TABEL 3
(HASIL *INFORMATION GATHERING*)

Teknik Pengujian	*Tools*	Hasil
Pencarian informasi *domain*	*Search Engine*	Mengidentifikasi *domain website* XYZ https;//XYZ
Melakukan *scan*	Wappalyzer	Mengidentifikasi teknologi yang digunakan dalam perancangan *website* XYZ
Pencarian IP *address*	Nslookup	Mendapatkan IP *address* XXX.XXX.XX.XXX dan DNS *server* XXX.XXX.XXX.X
Pencarian informasi *website*	Whois	Mendapatkan IP *adddress* XXX.XXX.XX.XXX dan informasi sensitif seperti *e-mail,* nomor telepon, nama administrator sehingga dapat memicu serangan *phising*

B. ***Network Mapping***

Pada tahap ini dilakukan pengumpulan informasi mengenai jaringan *website* XYZ dan pemetaan *port* melalui perintah nmap xxx.xxx.xx.xxx, hasil menunjukkan pemindaian *port* yang terbuka yaitu terdapat 851 *port* TCP yang terfilter, 147 *port* yang tertutup, 80/tcp *open* melayani HTTP dan 443/tcp *open* melayani HTTPS. Selanjutnya dilakukan identifikasi keamanan dengan ssllabs.com pada *Secure Socket Layer* (SSL) dan *Transport Layer Security* (TLS) dengan hasil menunjukkan *hwebsite* XYZ mendapatkan tingkat keamanan B, hal ini dikarenakan kurangnya keamanan yang memadai pada aspek *forward secrecy.* Pengujian ini menggunakan *tools* nmap dan ssllabs dapat dilihat pada Tabel 4

TABEL 4
(HASIL *NETWORK MAPPING*)

Teknik Pengujian	*Tools*	Hasil
Melakukan *scan port*	Nmap	Hasil dari pemidaian *port website* XYZ yang terbuka yaitu: • 80/tcp *open http* • 443/tcp *open https*
Melakukan *scan* SSL/TLS	Ssllabs	Aspek SSL TLS *website* XYZ mendapatkan rating B, hal ini terjadi karena kurangnya keamanan pada aspek *forward secrecy*

C. ***Vulnerability Identification***

Pada tahap ini dilakukan identifikasi potensi celah keamanan menggunakan *tools* OWASP yang menunjukkan terdapat 16 celah kerentanan. Celah kerentanan tersebut meliputi 3 *level* yaitu *medium, low* dan *informational,* diantaranya yaitu empat *medium,* depalan *low* dan empat *informational.* Selanjutnya identifikasi dilakukan melalu nikto dengan menunjukkan beberapa celah kerentanan. Dan dilakukan identifikasi melalui perintah *echo "XYZ" | tee url.tx* dan *waybackurls* untuk melihat arsip URL yang tersimpan dalam *website* XYZ. Pengujian tahap ini menggunakan *tools* OWASP ZAP, nikto dan *manual test* dapat dilihat pada Tabel 5

TABEL 5
(HASIL *VULNERABILITY IDENTIFICATION)*

Teknik Pengujian	*Tools*	Hasil
Melakukan identifikasi celah keamanan pada *website* XYZ	OWASP ZAP	Mengidentifikasi pada *website* XYZ melalui *tools* OWASP ZAP dan menemukan celah 16 celah keamanan berdasarkan *level* 4 *medium,* 8 *low,* dan 4 *informational*
Melakukan *scan*	Nikto	Risiko celah keamanan pada *website* yaitu *server* Apache versi 2.4.52, terdapat celah pada *x-frame-options* dan tidak ada konfigurasi *x-content-type-options* serta tidak ada direktori *Common Gateway Interface* (CGI)
Manual test	Echo	Perintah untuk melakukan permintaan akses pada *domain website XYZ* melalu perintah *echo "XYZ" | tee url.txt*
	Waybackurls	Perintah untuk pencarian arsip URL dalam *website* XYZ melalui *waybackurls*

D. ***Penetration Testing***

Pada tahap ini dilakukan pengujian keamananan *website* XYZ melalui serangan *Cross-Site Scripting* (XSS), SQL *injection* dan celah kerentanan *Local File Incluison* (LFI). Pengujian melalui serangan XSS dilakukan melalui *input form login* pada *website* XYZ dengan XSS *payload*, namun pengujian gagal dilakukan karena terblokir oleh sistem keamanan *website* XYZ. Pengujian kedua dilakukan melalui serangan SQL *injection* pada *form login* https://XYZ, namun hasil pengujian gagal dilakukan karena sistem keamanan pada *website* XYZ aman dari serangan SQL *injection.* Pada pengujian sebelumnya ditemukan potensi kerentanan *Local File Inclusion* (LFI) yang terletak pada URL *http://XYZ:80/index.php?page=download&subdir=pengumuman&file=BROSUR_XYZ_GEL_3_2020.pdf,* selanjutnya dilakukan pengujian terhadap kerentanan *Local File Inclusion* (LFI) menggunakan *tools* burp suite, sistem merespon permintaan dengan menampilkan lokasi direktori *script <? Php header('location: ../index.php');?>* dapat dilihat pada Tabel 6

TABEL 6
(HASIL *PENETRATION TESTING)*

Teknik Serangan	*Tools*	Hasil
XSS	Burp Suite	Melakukan pengujian melalui *input* pada *form* "No. Pendaftaran" dan "*Password*" menggunakan *payload stored* XSS

Teknik Serangan	*Tools*	Hasil
		dan gagal memperoleh akses celah keamanan dengan XSS
SQL *injection*	SQL *map*	Melakukan uji serangan melalui URL https://XYZ dan gagal diperoleh akses celah keamanan dengan SQL *injection.*
Local File Inclusion (LFI)	Burp Suite	Melakukan modifikasi URL direktori menjadi */index.php?page=downloadXYZ= index.php HTTP/1.1.* Berhasil memperoleh respon dan akses dari *server linux configuration* dengan menampilkan *script <? Php header('location: ../index.php');?>*

E. ***Gaining Access and Privilege Escalation***

Pada tahap ini dilakukan untuk memperoleh akses lebih mendalam pada sistem *website* XYZ dengan meningkatkan hak akses melalui *path traversal "../"* untuk mengakses *file* pada sistem *website* XYZ. Hasil menunjukkan sistem meberi respon rengan menampilkan file direktori konfigurasi linux sistem XYZ. Pengujian dilakukan menggunakan *tools* burp suite dapat dilihat pada Tabel 7

TABEL 7
(HASIL *GAINING ACCESS AND PRIVILEGE ESCALATION)*

Teknik Serangan	*Tools*	Hasil
Local File Inclusion (LFI)	Burp Suite	Menggunakan *path traversal* pada URL */index.php?page=downloadX YZ* dan HTTP *request* melalui perintah GET *".../"* sehingga *server* merespon dengan menunjukkan direktori *server* konfigurasi linux XYZ

F. ***Enumerating Further***

Pada tahap ini dilakukan pencarian informasi direktori yang mencakup *password* dan *username* melaluii perintah *path traversal,* hasil menunjukkan bahwa terdapat 2 *user* aktif, layanan berjalan, serta mendapatkan *username* dan *password database.* Selanjutnya dilakukan pemindaian terhadapr *port postgeSQL* 5432 melalui perintah nmap -p 5432 dengan hasil *filtered.* Tahap pengujian inni menggunakan *tools* burp suite dan Nmap dapat dilihat pada Tabel 8

TABEL 8
(HASIL *ENUMERATING FURTHER)*

Teknik Serangan	*Tools*	Hasil
Local File Inclusion (LFI)	*Burp Suite*	Pengujian celah keamanan sistem *website* menggunakan HTTP *request* melalui perintah GET, *path traversal "../"* menuju file sensitif *"/etc/passwd".* Mendapatkan akses menuju konfigurasi *database* dengan mendapatkan dua *user* aktif, *username* dan *password database*
	Nmap	Melakukan *scanning* menggunakan perintah -p terhadap *port* 5432 yang didapatkan dalam direktori linux. Mendapatkan hasil *scanning port* 5432 milik *PostgreSQL* berstatus *filtered*

G. ***Compromising Remote User/Sites***

Pada tahap ini dilakukan pengujian keamanan untuk mendapatkan kontrol akses dari jarak jauh dengan menggunakan perintah psql -h XXX.XXX.XX.XXX -p 5432 postgres -d XYZ. Hasil menunjukkan bahwa pengujian untuk memperoleh hak akses jarak jauh tidak dapat dilakukan karena ditolak, hal ini terjadi karena pengaturan pada *firewall* yang hanya mengizinkan IP *address* tertentu yang dapat mengakses. Kemudian dilanjutkan upaya pengambilan hak akses dari jarak jauh melalui perintah netcat nc XXX.XXX.XX.XXX hasil menunjukkan bawah *firewall* pada sistem XYZ memblokir akses permintaan dan hanya mengizinkan IP *address* yang terdaftar untuk masuk. Pada tahap ini pengujian menggunakan perintah psql -h dan netcat nc XXX.XXX.XX.XXX dapat dilihat pada Tabel 9

TABEL 9
(HASIL *COMPROMISING REMOTE USER/SITES)*

Teknik Serangan	*Tools*	Hasil
Manual test	*manual test* psql -h	Melakukan penyerangan hak akses jarak jauh melalui *database postgreSQL.* Gagal mendapatkan hak akses jarak jauh dalam sistem *database* hal ini terjadi karena terblokir oleh *firewall* dan hanya mengizinkan IP *address* tertentu yang dapat mengakses
	Netcat nc XXX.XX X.XX.X XX	Melakukan penyerangan hak akses jarak jauh l pada sistem melalui IP *address.* Gagal mendapatkan akses dikarenakan *firewall* XYZ hanya mengizinkan IP *address* terdaftar

H. ***Maintaining Access***

Pada tahap ini dilakukan upaya untuk mempertahankan akses yang telah diperoleh dengan memanfaatkan celah kerentanan pada tahap sebelumnya, termasuk melakukan penanaman *backdoor* serta mempertahankan akses jangka panjang sehingga terhindar dari deteksi sistem keamanan pada *website* XYZ Namun pada tahap uji penetrasi ini tidak dapat dilanjutkan karena terbatasnya akses masuk lebih dalam menuju sistem.

I. ***Covering Tracks***

Pada tahap ini, dilakukan tindakan untuk menghapus jejak serangan pada berbagai tahap sebelumnya, termasuk menghapus dan mengubah data file *log,* menghapus file, dan folder yang berkaitan dengan serangan. Namun, dalam pengujian ini langkah tersebut tidak dilakukan karena pada tahap *maintaining access* tidak berjalan. Oleh karena itu, pada penelitian ini tidak terdapat jejak aktivitas yang perlu dihapus. Fokus pada pengujian ini tetap pada evaluasi kerentanan dan penentuan skala prioritas perbaikan, tanpa melakukan tindakan pengujian yang dapat melanggar kebijakan keamanan atau merusak data pada sistem.

V. KESIMPULAN

Berdasarkan penelitian yang telah dilakuan melalui pendekatan ISSAF pada *website* XYZ ditemukan total 16 temuan kerentanan yang terbagi menjadi 6 pada tingkat tertinggi, yaitu *Local File Inclusion* (LFI) dengan tingkat skor 7.5 *high* hal ini terjadi karena kurangnya validasi *input* yang dapat dilakukan eksploitasi melalui *path traversal.* Risiko tingkat skor 4.2 *medium* meliputi *Absence of Anti-CSRF Tokens* yang tidak menyisipkan *token anti*-CSRF pada *form* HTML*, Content Security Policy (CSP) Header Not Set, Missing Anti clickjacking Header* tidak ditemukan *Anti-Clickjacking* dalam *respons* HTTP*, Vulnerability jS Library.* Selanjutnya pada tingkat *low* terdapat *Charset Mismatch (Header Versus Meta Content-Type Charset).* Sementara itu terdapat 4 kerentanan pada tingkat *informational* yaitu *Charset Mismatch (Header Versus Meta Content-Type Charset), Information Disclosure – Suspicious Comments, Modern Web Application, Session Management Response Identified.*

REFERENSI

[1] APJII, "Survei Internet APJII," https://survei.apjii.or.id.

[2] Y. A. Pohan, Y. Yunus, and Sumijan, "Meningkatkan Keamanan Webserver Aplikasi Pelaporan Pajak Daerah Menggunakan Metode Penetration Testing Execution Standar," *Jurnal Sistim Informasi dan Teknologi*, vol. 3, pp. 1–6, Mar. 2021, doi: 10.37034/jsisfotek.v3i1.36.

[3] W. R. H. Nasution, M. I. P. Nasution, and Sundari Sri Suci Ayu, "9 Pendapat Ahli Mengenai Sistem Informasi Manajemen," *Jurnal Inovasi Penelitian*, vol. 3, no. 4, pp. 5893–5896, Sep. 2022.

[4] D. W. Yahya and M. W. Astuti, "Pengujian Black Box Sistem Informasi Penilaian Kinerja Karyawan PT Inka (Persero) Berbasis Equivalence Partitions," *Jurnal Digital Teknologi Informasi*, vol. 4, no. 1, pp. 22–26, 2021.

[5] I. G. A. S. Sanjaya, G. M. A. Sasmita, and D. M. S. Arsa, "Evaluasi Keamanan Website Lembaga X Melalui Penetration Testing Menggunakan Framework ISSAF," *Jurnal Ilmiah Merpati*, vol. 8, no. 2, pp. 113–124, Aug. 2020.

[6] A. W. Wardhana and H. B. Seta, "Analisis Keamanan Sistem Pembelajaran Online Menggunakan Metode ISSAF Pada Website Universitas XYZ," *Jurnal Informatik*, vol. 3, no. 17, p. 2021, 2021.

[7] L. Kestina, Yuhandri, and W. G. Nurcahyo, "Penanganan Celah Keamanan Website dengan Ethical Hacking dan Issaf Menggunakan Acunetix Vulnerability (Studi Kasus di BKPSDMD Kabupaten Kerinci)," *INNOVATIVE: Journal Of Social Science Research*, vol. 3, no. 4, pp. 9192–9203, 2023, Accessed: Jul. 11, 2023. [Online]. Available: : https://j-innovative.org/index.php/Innovative

[8] FIRST, "Common Vulnerability Scoring System," https://www.first.org/cvss/v3-1/specification-document .

[9] Wappalyzer, "About Us," https://www.wappalyzer.com/about/.

[10] T. Rizkayanti and Y. W, "Analisis Keamanan Website Sistem Informasi Administrasi Kependudukan Menggunakan Metode Vulnerability Assesment," *Jurnal Teknologi Informatika Dan Komputer*, vol. 1, no. 1, pp. 1–9, 2023, doi: 10.xxxxx.

[11] A. Rochman, R. Ro. Salam, and S. A. Maulana, "Analisis Keamanan Website Dengan Information System Security Assessment Framework (ISSAF) Dan Open Web Application Security Project (OWASP) Di Rumah Sakit XYZ," *Jurnal Indonesia Sosial Teknologi*, vol. 2, no. 4, p. 506, 2021.

[12] G. "Fyodor" Lyon, "Nmap Network Scanning," https://nmap.org/book/.

[13] I. Ristic, "About SSL Labs," https://www.ssllabs.com/.

[14] M. Dewi, Budiono. Avon, and U. Y. K. S. Hediyanto, "Vulnerability Assessment pada Website Rekruitasi Asisten (IRIS) Fakultas Rekayasa Industri menggunakan Nikto dan Nessus," vol. 10, no. 2, pp. 1631–1636, 2023.

[15] Zap Dev Team, "Getting Started," https://www.zaproxy.org/getting-started/.

[16] A. M. N. Rizky, M. Tahir, T. A. Sapitri, and M. F. Islam, "Implementasi SQL Injection Dalam Penetration Testing Untuk Deteksi Celah Keamanan Web," *Jurnal Mahasiswa Teknik Informatika*, vol. 9, no. 4, pp. 6964–6968, 2025.

[17] I. M. Lina and G. R. Fernandes, "Anticipate Password Security with Burp Suite Using the Brute Force Attack Method," *Jurnal Elektro Komputer Teknik*, vol. 7, no. 1, pp. 118–127, Jun. 2023, doi: 10.37339/e-komtek.v7i1.1162.

[18] D. Kurniawan and Y. M. Saputra, "Implementasi Ansible pada Otomasi Honeypot Deployment Berbasis Web," *Journal of Internet and Software Engineering*, vol. 5, no. 2, 2024.