Analisis Keamanan *Website* PPDB dengan Pendekatan *Information System Security Assessment Framework* (ISSAF) pada Sekolah XYZ

Mochamad Evan Wiratama[*1)], Muhamad Nasrullah[2)], dan Adzanil Rachmadhi Putra[3)]
[1)]Sistem Informasi, Fakultas Teknik Informasi dan Bisnis, Institut Teknologi Telkom Surabaya, Jl. Ketintang No. 156, Surabaya, 60231, Indonesia
mochevan@student.ittelkom-sby.ac.id

Abstrak

Website saat ini menjadi keperluan bersama dengan meningkatnya pengguna yang tersambung ke jaringan internet. Yang mana hal ini dapat menimbulkan tindakan kejahatan cyber oleh pihak yang tidak bertanggung jawab. Maka diperlukannya Keamanan Sistem Informasi, yang dapat mengantisipasi adanya kejahatan cyber. Website PPDB sekolah XYZ memiliki peran penting, dimana terdapat data siswa baru hingga proses melakukan pembayaran pendaftaran. Oleh karena itu, penelitian ini melakukan analisis keamanan sistem informasi sebagai bentuk melindungi data pribadi siswa hingga financial yang ada pada website tersebut. Dalam penelitian ini, pendekatan information system security assesment framework (ISSAF) dapat digunakan untuk mengevaluasi keamanan sistem, jaringan komputer, hingga aplikasi atau website. Dalam pendekatan ISSAF terdapat 3 tahapan dalam evaluasi penilaian yaitu planning and preparation, assesment, reporting, clean up and destroy artifacts. Dari hal tersebut didapatkan beberapa hasil setelah melakukan hasil penetration testing berdasarkan framework ISSAF, yaitu teridentifikasinya profil perusahaan setelah melakukan scan whois, terdapat kerentanan pada vulnerability scan, dan adanya kerentanan XSS dan file upload user pada penetration test. Namun terdapat hasil tes yang tidak berhasil dilakukan untuk mendapatkan hak akses yaitu pada tahap gaining access and privilege escalation sehingga tidak dapat dilakukan tahap selanjutnya hingga corvering tracks karena website telah di konfigurasi dengan baik. Kemudian dilakukannya pemberian rekomendasi dan solusi untuk mengatasi celah keamanan yang ada pada website PPDB sekolah XYZ.

Kata kunci: *Keamanan, Website, PPDB, ISSAF, Penetration Testing*

1. Pendahuluan (Introduction)

Pertumbuhan teknologi saat ini semakin berkembang dan inovatif dalam penyampaian informasi hingga pengelolaan data yaitu *website*. *Website* memiliki fungsi dalam penyampaian informasi dan mengelola data secara luas sehingga masyarakat dapat dengan mudah menggunakannya. Hanya dengan jaringan internet dapat diakses oleh siapa saja melalui perangkat komputer dan *smartphone* (Eko Prasetyo & Hassanah, 2021).

Pada tahun 2018, Indonesia memiliki jumlah pengguna internet sebesar 132,7 juta pengguna dan meningkat setiap tahunnya. Pada tahun 2022, pengguna internet sudah mencapai 204,7 juta pengguna dan akan terus meningkat, dimana jumlah tersebut melonjak sebesar 54,25% dari tahun-tahun sebelumnya sehingga menjadikan Indonesia sebagai salah satu negara dengan pengguna internet terbesar di dunia (Cindy Mutia Annur, 2022). Seiring dengan meningkatnya jumlah pengguna internet, maka hal itu juga mempengaruhi peningkatan jumlah pengguna *website*. Hal tersebut dapat berdampak adanya kerentanan *website* yang memiliki resiko diserang oleh oknum tidak bertanggungjawab sebab terdapat celah keamanan *website* yang tidak diperhatikan admin *website* tersebut sehingga timbul adanya peretasan (Eko Prasetyo & Hassanah, 2021).

Website penerimaan peserta didik baru (PPDB) merupakan *website* yang menyediakan berbagai informasi terkait pendaftaran siswa baru. Dengan melakukan PPDB secara *online*, maka pendaftar dapat memanfaatkan teknologi informasi dari rumah sehingga tidak perlu datang di tempat untuk melakukan pengisian data hingga melakukan pembayaran pendaftaran (Utoro et al., 2020).Seiring dengan

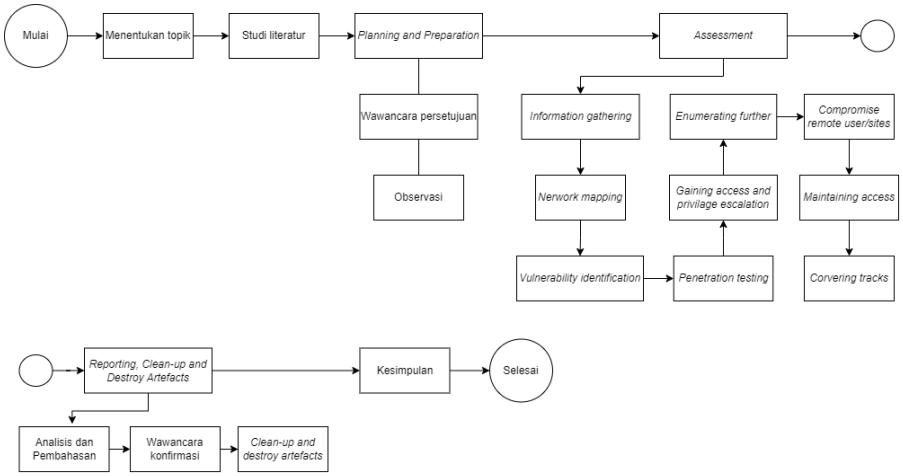
meningkatnya jumlah siswa di sekolah XYZ, maka semakin meningkat juga penggunaan *website* PPDB tersebut. Hal ini menjadi peran penting, dimana banyak data calon siswa baru hingga nomor rekening pendaftaran yang harus dijaga sedemikian rupa. Hal tersebut pernah terjadi ketika saat hilangnya data calon siswa sehingga pihak lembaga sekolah XYZ harus melakukan *back-up* data kembali. Pengujian keamanan sistem informasi perlu dilakukan untuk mengantisipasi ancaman peretasan yang diterima oleh pihak administrasi sekolah, dimana hal tersebut berdampak pada kebocoran informasi yang dapat mengakibatkan serangan *cyber* seperti *phising*, *deface*, hingga hilangnya data pribadi calon siswa (Utoro et al., 2020).

Dalam pengujian keamanan sistem informasi, terdapat dua jenis metode pengujian kerentanan pada *website* PPDB, yaitu *vulnerability testing* dan *penetration testing*. *Vulnerability testing* merupakan proses pemindaian sistem salah satunya pada *website* yang bertujuan untuk mengetahui titik kelemahan di dalam *website* tersebut. Sedangkan, *penetration testing* merupakan pengujian dengan melakukan serangan ke dalam sistem *website* tersebut yang bertujuan untuk mengetahui kemungkinan titik sistem yang mudah terdapat serangan. Dari kedua metode tersebut merupakan metode yang baik dalam menguji keamanan sistem *website*. Namun *penetration testing* memiliki peran besar dan disarankan untuk melakukan pengujian keamanan sistem (Sanjaya et al., 2020).

Information system security assesment framework (ISSAF) merupakan kerangka kerja dalam melakukan *penetration testing*, dimana memiliki beberapa fungsi terkait kontrol keamanan, struktur intuitif yang memberikan arahan melalui langkah-langkah yang kompleks. ISSAF terikat pada pedomannya menjelaskan bahwa *penetration testing* dilakukan untuk memberikan arahan pengujian secara benar, hingga menghindari adanya kesalahan dengan metode serangan yang dilakukan secara acak (Sanjaya et al., 2020). *Framework* ISSAF memiliki kelebihan yaitu penggunaan ISSAF memiliki kesesuaian untuk memenuhi persyaratan penilaian keamanan organisasi dan dapat dijadikan acuan untuk memenuhi persyaratan keamanan informasi lainnya. ISSAF mencakup aspek utama pemrosesan dan penilaian keamanan informasi, membantu mendapatkan gambaran lengkap tentang potensi kerentanan (Syarif Revolino & Jatmiko Andri, 2019).

Penelitian ini berfokus terhadap pengujian keamanan sistem *website* PPDB yang dilakukan dengan metode *penetration testing* berdasarkan *framework* ISSAF. Penelitian ini bertujuan untuk mengetahui sisi kerentanan pada *website* berdasarkan *framework* ISSAF, sehingga dalam penelitian ini dapat memberikan rekomendasi agar terjadi peningkatan keamanan pada *website* sekolah XYZ (Sanjaya et al., 2020).

2. Metode Penelitian (Methods)



Gambar 1. *Flowchart* ISSAF

2.1. Menentukan Topik

Topik ditentukan sesuai dengan acuan apa saja yang harus diteliti. Menentukan topik penelitian ini dimulai dengan mengidentifikasi kebutuhan terkait metode serta objek yang digunakan.

2.2. Studi Literatur

Setelah menemukan topik, lalu pengumpulan jurnal-jurnal terdahulu terkait dengan topik yang ditentukan untuk menyusun data pustaka yang akan dibuat.

2.3. *Planning and Preparation*

2.3.1 Wawancara Persetujuan

Sebelum melakukan eksekusi dalam uji keamanan sistem informasi *website* PPDB sekolah XYZ, maka diperlukan wawancara terlebih dahulu. Dalam wawancara ini melakukan sesi tanya jawab atas perizinan melalui *Supervisor* Sistem Informasi lembaga XYZ agar mendapat informasi dalam melakukan pendekatan sebelum melakukan *penetration testing.*

2.3.2 Observasi

Setelah mendapatkan perizinan melalui pihak Lembaga Pendidikan Sekolah XYZ, maka dilakukan observasi dengan mengamati *website* PPDB sekolah XYZ dengan cara melakukan *login* serta melihat fitur yang ada pada *website* tersebut.

2.4. *Assessment*

2.4.1 *Information Gathering*

Pada tahap *information gathering* melakukan pengumpulan informasi menggunakan internet untuk menemukan seluruh informasi pada *website* PPDB sekolah XYZ. Hal tersebut dapat dilakukan pengumpulan info mengenai info teknis seperti *IP address*, sistem, dan juga info non teknis dengan menggunakan media pendukung seperti *search engine* (Sanjaya et al., 2020). Tahap *information gathering* ini menggunakan *tools* Ping, Whois, dan Wappalyzer (Wardhana & Seta, 2021).

2.4.2 *Network Mapping*

Ketika seluruh informasi target diperoleh, maka dilakukan pendekatan secara teknis, yaitu memperoleh seluruh informasi mengenai proses *scanning* jaringan yang diperoleh yaitu *port open*, layanan yang digunakan, dan sistem operasi yang berjalan di *server website* PPDB sekolah XYZ. Tahap *network mapping* ini menggunakan *tool* yaitu Nmap (Wardhana & Seta, 2021).

2.4.3 *Vulnerability Identification*

Tahap *vulnerability identification* yaitu melakukan *scanning* untuk mengidentifikasi titik kerentanan pada *website* PPDB sekolah XYZ. Kerentanan dapat diklasifikasikan dalam tingkat tertentu, yaitu: *low, medium, high,* dan *critical*. Pada tahap *vulnerability identification* menggunakan *tool* yaitu Nessus (Wardhana & Seta, 2021).

2.4.4 *Penetration Testing*

Pada tahap *penetration testing* melakukan uji coba serangan untuk medapatkan hak akses ilegal dengan cara menghindari sistem keamanan dan mencoba mengambil akses sejauh mungkin. Tahap *penetration testing* ini menggunakan teknik serangan SQL *injection*, XSS *cross-site scripting* dan *shell upload exploitation. Tools* yang digunakan yaitu SQLmap dan *manual input* pada fitur yang ada pada *website* PPDB sekolah XYZ (Wardhana & Seta, 2021).

2.4.5 *Gaining Access and Privilage Escalation*

Setelah melakukan tahap *penetration testing*, maka dilakukan tahap *gaining access and privilages escalation*. Pada tahap ini mencoba kembali melakukan akses sejauh mungkin dengan cara mendapatkan hak akses *root* pada *server website* PPDB sekolah XYZ. Pada tahap ini melakukan jenis serangan b*rute force*, *explotation port* 80, dan PHP *shell injection*. Hal ini menggunakan *tools* Metasploit, Hydra, dan *manual input* pada *form upload* (Wardhana & Seta, 2021).

2.4.6 *Enumerating Further*

Pada tahap *enumarting further* melakukan tahapan mencari informasi lebih lanjut dari tahap sebelumnya yang meliputi *sniff traffic* dan *hijackinig session* untuk mengetahui kerentanan dalam rekam data yang berisikan *username* dan *password* dan pencurian *cookies*. *Tool* yang digunakan yaitu Wireshark, Burpsuites, dan Cookie Manager (Wardhana & Seta, 2021).

2.4.7 *Compromise Remote User/Sites*

Pada tahap *compromise remote user/sites* yaitu melakukan eksploitasi untuk mendapatkan akses ke dalam *user root* dengan menghubungkan *remote user* dan *enterprise user* (Wardhana & Seta, 2021).

2.4.8 *Maintaining Access*

Pada tahap *maintaining access* melakukan pengujian dengan mempertahankan hak akses dengan penanaman *backdoor*. Hal tersebut bertujuan untuk masuk kembali ke sistem dengan mudah tanpa memerlukan metode serangan awal yang rumit (Wardhana & Seta, 2021).

2.4.9 *Corvering Tracks*

Pada tahap *corvering tracks* merupakan tahapan terakhir dalam *penetration testing*. Setelah eksploitasi berhasil masuk ke dalam sistem, maka penyerang berusaha untuk menghapus *log* aktivitas sistem agar sulit untuk ditelusuri kembali terkait serangan atau akses yang telah dilakukan (Wardhana & Seta, 2021).

2.5. *Reporting, Clean-up and Destroy Artefacts*

2.5.1. Analisis dan Pembahasan

Setelah melakukan wawancara konfirmasi, maka dianalisis kembali hasil dari *penetration testing* sehingga menghasilkan rekomendasi yang baik kepada pihak lembaga sekolah XYZ untuk melakukan antisipasi kembali terhadap keamanan sistem *website* PPDB sekolah XYZ.

2.5.2. Wawancara Konfirmasi

Pada tahap wawancara konfirmasi merupakan tahapan untuk melakukan wawancara kembali bersama *Supervisor* Sistem Informasi lembaga sekolah XYZ mengenai pelaporan terkait hasil *penetration testing* pada *website* PPDB sekolah XYZ.

2.5.3. *Clean-up and Destroy Artefacts*

Setelah melakukan seluruh tahapan *assessment*, maka dilakukannya penghapusan seluruh jejak terkait serangan yang dilakukan. Tujuannya yaitu untuk memastikan bahwa tidak ada bukti yang digunakan untuk mengidentifikasi penyerang (Agus Rochman, Rizal Rohian Salam, 2021).

2.6. Kesimpulan

Setelah melakukan seluruh kegiatan penetration testing dengan kerangka kerja ISSAF, maka dilakukannya pembuatan kesimpulan pada penelitian ini agar mengetahui hasil secara ringkas.

3. Hasil dan Pembahasan (Results and Discussions)

Dalam *framework* ISSAF telah menunjukkan berbagai proses yang dilakukan sebelum, selama, dan setelah melakukan *penetration testing* keamanan pada institusi tertentu. Namun hal ini hanya befokus pada penetrasi keamanan pada bagian *technical control assessment* atau tidak melakukan proses *physical security assesment* dan *social engineering*. Berikut adalah tahapan yang dilakukan.

3.1. *Planning and Preparation*

3.1.1. Wawancara Persetujuan

Wawancara persetujuan merupakan hal yang sangat penting sebelum melakukan sebuah uji kerentanan pada sistem PPDB sekolah XYZ. Pada tahap ini menghasilkan sebuah diskusi berupa pendekatan yang dilakukan dengan cara izin serta melakukan sesi tanya jawab kepada pihak lembaga sekolah XYZ.

Waktu pengujian dilaksanakan sesuai dengan hasil diskusi yang dilakukan pada saat sesi persetujuan. Hal ini bertujuan untuk mengetahui waktu dilakukannya *maintenance* pada sistem *website* tersebut. Pada tahap ini bertujuan untuk menghindari adanya kesalahpahaman ketika sedang melakukan

uji kerentanan pada *website* PPDB sekolah XYZ. Adapun ruang linkgup pada pengujian ini adalah untuk mengumpulkan berbagai infomasi terkait *website* tersebut apakah pernah terjadi insiden pada *domain ppdb.xyz.sch.id.*

3.1.2. Observasi

Pada tahap observasi pentingnya dalam mengelola dan memahami sistem *website* PPDB sekolah XYZ. Hal ini merupakan proses dalam menganalisis isi dari sistem *website* tersebut. Dengan melakukan observasi, maka mendapatkan informasi mengenai isi pada *website* tersebut yang berkaitan dengan interaksi pengguna, permintaan server, dan kinerja aplikasi.

Dalam tahap ini dapat menjelajahi berbagai teknik dan *tools* apa yang dapat digunakan untuk melakukan dan memahami sistem *website* PPDB sekolah XYZ, serta praktik terbaik untuk menerapkannya.

3.2. *Assessment*

3.2.1. *Information Gathering*

Pada tahap *information gathering*, dilakukan berbagai hal untuk mendapatkan semua informasi terkait *website* pendaftaran siswa sekolah XYZ. Dalam hal ini, mencari situs utama pendaftaran siswa *website* sekolah XYZ, mengidentifikasi spesifikasi *website* pendaftaran siswa, mencari alamat IP, dan mencari informasi pribadi terkait *website* PPDB sekolah XYZ.

Dalam pencarian situs utama *website* PPDB sekolah XYZ dapat diketahui melalui pencarian *Google* bahwa situs utama yang dimilikinya adalah ppdb.xyz.sch.id. setelah mengetahui *domain website* pendaftaran siswa sekolah XYZ, berhasil mengidentifikasi spesifikasi *website* melalui *tool* Wappalyzer. Kemudian berhasil mendapatkan alamat IP *website* PPDB sekolah XYZ melalui *ping*. Kemudian berhasil mendapatkan informasi pribadi pada website pendaftaran siswa sekolah XYZ dengan menampilkan informasi perusahaan *hosting* melalui *tool* Whois. Dari beberapa hasil tersebut dapat dilihat pada tabel berikut:

Tabel 1. Hasil tahap *information gathering*

Teknik Pengujian	*Tool*	Hasil *caption*	Hasil
Mencari informasi *Domain*	Mesin pencarian *Google*	Melakukan pencarian *website* PPDB sekolah XYZ pada pencarian *google* untuk mengetahui *domain* dari *website* PPDB sekolah XYZ.	Berhasil
Identifikasi spesifikasi	Wappalyzer	Menggunakan *tool wappalyzer* untuk menemukan spesifikasi terkait *website* PPDB sekolah XYZ.	Berhasil
Pencarian *IP address*	Ping	Melakukan pencarian *IP address* menggunakan Ping.	Berhasil
Mencari data informasi tentang *domain*	Whois	Melakukan pencarian data *domain* PPDB sekolah XYZ menggunakan *tool* Whois.	Berhasil

3.2.2. *Network Mapping*

Langkah selanjutnya adalah melakukan *scan port* untuk mengetahui *port* apa saja yang ada di *website* ppdb.xyz.sch.id. Pada tahap ini menggunakan *tool* Nmap karena *tool* tersebut memiliki tingkat akurasi yang baik. Berikut hasil *scan* ppdb.xyz.sch.id menggunakan Nmap:

Tabel 2. Hasil *scan* menggunakan Nmap

Port	State	Service	Version
21/tcp	open	ftp	Pure-FTPd
80/tcp	open	http	LiteSpeed
110/tcp	open	Pop3	Dovecot pop3d
143/tcp	open	imap	Dovecot imapd
443/tcp	open	ssl/https	Litespeed
587/tcp	open	tcpwrapped	
993/tcp	open	ssl/imap	Dovecot imapd
995/tcp	open	tcpwrapped	
3306/tcp	open	mysql	MySQL 5.5.5-10.5.19-MariaDB-cll-lve

Kemudian pada tahap selanjutnya dilakukan pengujian keamanan SSL dan TLS yang digunakan pada *website* ppdb.xyz.sch.id menggunakan *tool online* bernama ssllabs.com dengan hasil *website* ppdb.xyz.sch.id didukung dengan TLS terbaru 1.3.

Berikut adalah hasil *network mapping*, versi *scanning*, dan pemindaian SSL/TLS yang bertujuan untuk memetakan jaringan yang terdapat pada sistem:

Tabel 3. Hasil pengujian *network mapping* dan SSL/TLS

Teknik Pengujian	*Tool*	Hasil *caption*	Hasil
Network mapping	Nmap	Melakukan *scanning* menggunakan *tool nmap* sekaligus mencari informasi mengenai versi yang digunakan setiap *port*.	Berhasil
Scanning SSL/TLS	Ssllabs.com	Melakukan *scanning* menggunakan *tool online* ssllabs.com agar mengetahui *overall rating* dan keamanan pada *transfer* komunikasi data.	Berhasil

3.2.3. *Vulnerability Identification*

Tahap *vulnerability identification* bertujuan untuk menemukan celah keamanan yang ada pada sistem dan *server website* ppdb.xyz.sch.id menggunakan *tool* Nessus. Pada tahap ini menggunakan fitur yang ada pada Nessus yaitu *basic network scan* dalam melakukan *vulnerability scan* dengan hasil :

Tabel 4. Hasil kategori *vulnerability*

Kerentanan	Tingkat
SSL anonymous cipher suiter supported	*Low*
DNS server spoofed request amplification DDos	*Medium*
TLS version 1.0 protocol detection	*Medium*
TLS version 1.1 protocol deprecated	*Medium*
SSL medium strength cipher suites supported (SWEET32)	*Medium*
DNS server recursive query cache poisoning weakness	*Medium*

Berikut hasil pengujian *vulnerability identification* menggunakan fitur pada *tool* Nessus yaitu *basic network scan*:

Tabel 5. Hasil pengujian *vulnerability identification*

Teknik pengujian	*Tool*	Hasil *caption*	Hasil
Vulnerability scan	Nessus	melakukan *scan* dengan menampilkan hasil kerentanan dengan kategori 1 *low* dan 4 *medium.*	Berhasil

3.2.4. *Penetration Testing*

Tahap selanjutnya adalah tahap *penetration testing*. Pada tahap ini, pengujian keamanan sistem menyeluruh dilakukan. Ini melibatkan mengidentifikasi dan mengeksplorasi berbagai jenis kerentanan yang mungkin ada dalam sistem situs web pendaftaran siswa Sekolah XYZ. Dalam hal ini, fokus pada menemukan kelemahan dan menyelidiki potensi serangan yang bisa dilakukan. Pengujian yang dilakukan pada tahap ini meliputi SQL *injection*, *cross-site scripting* (XSS), dan pengujian eksploitasi pengunggahan *shell*.

Berdasarkan hasil pengujian, hasil pengujian SQL *injection* gagal karena perangkat tidak dapat membuat koneksi SSL dan diblokir oleh *firewall Immunify360*. lalu di pengujan serangan XSS dengan mencoba memasukan *payload stored* XSS berhasil dijalankan karena *form input* pada *website* tidak mensanitasi input dengan baik. Lalu uji eksploitasi *upload shell* pada *form uploader* berhasil karena kurangnya validasi input pada *form upload user*.

Berikut adalah hasil pada tahap penetration testing berdasarkan hasil pengujian di atas, sebagai berikut:

Tabel 6. Hasil pengujian *penetration testing*

Teknik pengujian	*Tool*	Hasil *caption*	Hasil
SQL Injection form login users	Sqlmap	melakukan uji SQL *injection* pada form *login user*.	Gagal
XSS cross-site scripting	*Manual input/test*	Perform XSS test on melakukan pengujian XSS pada *form* pendaftaran menggunakan *stored* XSS.	Berhasil
Shell upload exploitation form upload users	*Manual input/test*	Melakukan *upload* pada *form upload* menggunakan *shell* PHP yang berisikan skrip *info* PHP.	Berhasil

3.2.5. *Gaining Access and Privilage Escalation*

Tahap selanjutnya adalah *gaining access and privilege escalation*. Tahapan ini memiliki proses yang berbeda-beda. Dalam proses *gaining access* yaitu berusaha mendapatkan akses ke sistem atau jaringan yang akan diserang. Kemudian pada proses *privilege escalation* yaitu berusaha untuk meningkatkan hak akses yang dimilikinya dalam sistem atau jaringan.

Pada *gaining access* pertama, melakukan serangan *brute force* pada *port* 21 menggunakan *tool* Metasploit gagal mendapatkan hak akses karena situs *web* mendeteksi batas login maksimum. kemudian *gaining access* yang kedua mencoba lagi untuk melakukan serangan *brute force* pada *port* 21 tetapi menggunakan *tool* Hydra. hasilnya gagal karena tidak ada yang cocok dengan kombinasi *username* dan *password*. kemudian pada *gaining access* yang ketiga mengeksploitasi *port* 80 menggunakan Metasploit gagal dilakukan karena diblokir oleh *firewall*. Kemudian pada *gaining access* keempat untuk melakukan serangan PHP *shell injection*. hasil ini gagal karena *shell* difilter oleh *firewall* situs *website*.

Dalam tahap *gaining access*, hasil akhir beberapa serangan yang ditentukan ini tidak berhasil mencapai tujuannya untuk mendapatkan hak akses ke *server website* PPDB sekolah XYZ. Keberhasilan di tahap ini penting karena akan mempengaruhi kemampuan untuk melanjutkan ke tahap selanjutnya, yaitu *privillage escalation*, yang membutuhkan hak akses lebih tinggi, seperti hak akses *root*. Namun, karena serangan di tahap *gaining access* tidak berhasil, tidak ada kemajuan yang dapat dilakukan pada tahap *privillage escalation*.

Berikut hasil proses *gaining access and privillage esacalation* yang diuji berdasarkan hasil percobaan diatas, sebagai berikut:

Tabel 7. Hasil pengujian *gaining access and privilege escalation*

Teknik pengujian	*Tool*	Hasil *caption*	Hasil
Brute force attack	Metasploit	Melakukan uji *brute force attack username* dan *password* pada *port* 21.	Gagal
	Hydra	Melakukan uji *brute force attack username* dan *password* pada *port* 21.	Gagal
Exploitation	Metasploit	Melakukan eksploitasi pada *Port* 80.	Gagal
PHP shell injection	Manual test	Melakukan *upload shell* yang berisikan skrip untuk menuju hak akses pada *Form upload user*.	Gagal

3.2.6. *Enumerating Further*

Tahap selanjutnya adalah *enumerating further*. Tahap ini melibatkan langkah lanjutan setelah tahap sebelumnya. *Enumerating further* memanfaatkan *session hijacking* di mana proses ini mengambil penilaian keamanan dari target yang dievaluasi. Pada tahap ini dilakukan pengujian *session hijacking* dan *sniff traffic* menggunakan *tool* Burpsuites dan Wireshark.

Pada pengujian *session hijacking* gagal karena pada saat memasukan parameter tanpa mengisi kredensial masih kembali ke halaman login. lalu uji *sniff traffic* gagal karena *website* telah dienkripsi oleh TLS 1.3 sehingga paket data yang berisi *username* dan *password* tidak diketahui.

Berikut ini daftar hasil lebih lanjut menggunakan dua jenis pengujian, yaitu *session hijacking* dan *sniff traffic*:

Tabel 8. Hasil pengujian *enumerating further*

Teknik pengujian	*Tool*	Hasil *caption*	Hasil
Session hijacking	Burpsuites dan Cookie Manager	Berhasil menyimpan *cookie* namun masih tidak dapat *login* tanpa menulis kredensial.	Gagal
Sniff traffic	Wireshark	Paket data yang diterima tidak menunjukkan paket yang berisi *username* dan *password*.	Gagal

3.2.7. *Compromise Remote User/Sites*

Pada tahap ini melakukan upaya untuk mendapatkan *gaining access* ke dalam jaringan internal dengan memanfaatkan kelemahan yang ada pada pengguna atau situs tersebut. Dengan berhasil mengontrol pengguna atau situs jarak jauh dapat merambah ke dalam jaringan internal dengan tingkat hak akses yang lebih tinggi. Namun tidak dapat sampai ke tahap ini karena gagalnya dalam tahap *gaining access and privillage escalation* dikarenakan sistem yang dimiliki oleh PPDB sekolah XYZ telah dikonfigurasi dengan baik sehingga tidak dapat diakses lebih lanjut.

3.2.8. *Maintaining Access*

Pada tahap ini melakukan berbagai teknik dan strategi untuk mempertahankan akses yang telah diperoleh, termasuk memanfaatkan kerentanan yang belum diperbaiki, membuat sistem backdoor untuk akses jangka panjang agar menghindari deteksi oleh sistem keamanan yang ada. Namun tidak dapat sampai ke tahap ini karena gagalnya dalam tahap *gaining access and privillage escalation* dikarenakan sistem yang dimiliki oleh PPDB sekolah XYZ telah dikonfigurasi dengan baik sehingga tidak dapat diakses lebih lanjut.

3.2.9. *Corvering Tracks*

Pada tahap terakhir ini yaitu melakukan serangkaian langkah untuk menghilangkan jejak aktivitas, termasuk menghapus atau mengubah *file log*, menghapus *entri log*, menghapus *file* atau *folder* yang terkait dengan serangan, serta melakukan tindakan lain yang bertujuan untuk menghapus bukti-bukti yang dapat mengungkap identitas penyerang. Namun tidak dapat sampai ke tahap ini karena gagalnya dalam tahap *gaining access and privillage escalation* dikarenakan sistem yang dimiliki oleh PPDB sekolah XYZ telah dikonfigurasi dengan baik sehingga tidak dapat diakses lebih lanjut.

3.3. *Reporting, Clean-up and Destroy Artefacts*

3.3.1. Analisis dan Pembahsan

Tabel 9. Hasil analisis dan pembahasan

Assessment	*Tool*	Hasil	*Impact*	Rekomendasi
Information gathering	Mesin pencarian *Google*, Wappalyzer, Ping, Whois	Menampilkan informasi pribadi milik penyedia layanan *hosting* melalui *tool whois*. Namun informasi ini biasanya mencakup nama perusahaan, *email*, dan kontak	Informasi yang ditampilkan oleh *scan whois* menyebabkan terjadinya aktivitas mencurigakan seperti penargetan *spam*, *phising*,	Melakukan *protect* pada informasi-informasi data privasi dengan *whois protect* agar penyerang tidak dapat mengakses serta

Assessment	*Tool*	Hasil	*Impact*	Rekomendasi
		teknis terkait *domain*.	atau serangan *cyber* lainnya (Alwi et al., 2020).	eksploitasi lebih lanjut (Alwi et al., 2020).
Network mapping	Nmap, SSLLabs	Menampilkan *port* yang terbuka pada *website* PPDB sekolah XYZ adalah *port* 21, 80, 110, 143, 443, 587, 993, 995, dan 3306. Serta mengetahui layanan yang dipakai pada *port* 80 dan 443 menggunakan *litespeed.* Namun versi dari *server* tersebut tidak terdeteksi pada hasil *nmap.*	Informasi terkait *port* terbuka yang didapatkan melalui *scan tool nmap* sangat berbahaya karena beberapa *port* tersebut merupakan celah bagi *hacker* untuk melakukan penyerangan (Sanjaya et al., 2020).	Menerapkan *intrusion detection system* (IDS) untuk mendeteksi adanya serangan seperti *port scan* (Sutarti et al., 2018).
Vulnerability identification	Nessus	*SSL anonymous cipher suiter supported (low).*	Resiko yang terjadi adalah memungkinkan *administrator* untuk menyiapkan adanya layanan yang dapat mengenkripsi lalu lintas tanpa ada sertifikat SSL. Layanan ini tidak menawarkan cara agar dapat memverifikasi identitas *host* jarak jauh. Hal ini membuat layanan rentan dengan adanya *man-in-the-middle* (Alfin Syarifuddin Syahab, Erik Iman Heri Ujianto, 2023).	Solusi yang disarankan adalah mengkonfigurasi ulang pengaturan aplikasi sedapat mungkin untuk menghindari *cipher* yang lemah (Alfin Syarifuddin Syahab, Erik Iman Heri Ujianto, 2023).
		DNS server spoofed request	Dalam hal ini penyerang bisa mendapatkan	Solusi dalam hal ini yaitu melakukan

Assessment	*Tool*	Hasil	*Impact*	Rekomendasi
		amplification DDoS (medium).	amplifikasi untuk konfirmasi serangan penolakan terhadap *host* menggunakan *remote* DNS *server* (Kamilah & Hendri Hendrawan, 2019).	batasan akses *server* DNS dari jaringan publik serta mengkonfigurasi ulang agar menolak permintaan terkait hal tersebut (Kamilah & Hendri Hendrawan, 2019).
		Suite cipher SSL dengan kekuatan sedang didukung (SWEET32) (*medium*).	Dengan layanan jarak jauh, enkripsi berkekuatan sedang lebih mudah dilewati jika penyerang berada di jaringan fisik yang sama (Alfin Syarifuddin Syahab, Erik Iman Heri Ujianto, 2023).	Solusi yang disarankan harus mengkonfigurasi ulang aplikasi jika dapat menghindari penggunaan enkripsi yang memiliki kekuatan sedang (Alfin Syarifuddin Syahab, Erik Iman Heri Ujianto, 2023).
		DNS Server Recursive Query Cache Poisoning Weakness (*medium*).	Penyerang bisa memasukkan catatan alamat *domain* palsu untuk DNS internet (Irfan Murti Raazi, Ima Dwitawati, 2023)	Batasi permintaan rekursif ke *host* yang dimana harus menggunakan nama *server* dengan mengelompokkan alamat *internal* (Irfan Murti Raazi, Ima Dwitawati, 2023)
Penetration testing	SQLMap, *manual input*	Gagal melakukan SQL *injection* pada *form user login.*	Gagal nya melakukan *SQL injection* dikarenakan	-

Assessment	*Tool*	Hasil	*Impact*	Rekomendasi
			terdeteksi oleh *firewall imunify360* (WAF) sehingga IP pengguna atau penyerang ter-*block* oleh *server*. *Stored* XSS bisa mempengaruhi semua pengguna.	
		Mencoba memasukkan *payload stored* XSS pada *form* pendaftaran *user* berhasil dilakukan. Hal ini disebabkan karena kurangnya validasi dan sanitasi pada *form input* pendaftaran *users*.	XSS dihasilkan ketika pengguna atau penyerang memasukkan data yang akan ditampilkan lagi. Penyerang memasukkan kode HTML atau klien kode lain pada halaman *web* mereka (Charly et al., 2022).	Memfilter karakter khusus, tag HTML dan *JavaScript* atau menggunakan *library* anti-XSS bawaan CI untuk memblokir serangan XSS (Jrsfaisal, 2018).
		Melakukan teknik *shell upload exploitation* dengan ekstensi PHP yang berisi mengenai informasi konfigurasi PHP pada *server* berhasil dilakukan. Hal ini disebabkan karena kurangnya validasi dan sanitasi pada *form uploader*.	Kerentanan *upload file* dalam aplikasi *website* memberikan peluang sehingga peretas dapat meng-*upload file* dengan skrip berbahaya yang kemudian dapat dieksekusi pada *server*. Namun pada hal ini dapat mengetahui aktivitas konfigurasi PHP pada *server* (Muhammad Anis Al Hilmi1*), 2022).	Melakukan *secure coding* agar dapat memfilter *file* yang di *upload* (Muhammad Anis Al Hilmi1*), 2022).

3.3.2. Wawancara Persetujuan

Setelah selesai melakukan tahap *penetration testing* berdasarkan *framework* ISSAF, maka dilanjutkan untuk melakukan konfirmasi mengenai kerentanan yang ada serta pemberian rekomendasi.

Wawancara konfirmasi ini dilakukan kepada *Supervisor* Sistem Informasi lembaga sekolah XYZ dengan menjelaskan serta memberikan buku report terkait hasil yang telah dilakukan.

3.3.3. *Clean-up and Destroy Artefacts*

Pada tahap *clean-up and destroy artefacts*, semua data yang telah dibuat atau ditambahkan ke sistem perlu dihapus. Jika menggunakan sistem jarak jauh, hal ini tidak dapat dilakukan, pihak pengujian harus diberi tahu agar personel TI di pihak tersebut dapat memusnahkan data ini saat laporan diterima. Hal tersebut dapat dilihat pada gambar dibawah ini.

3.4. Kondisi *Website* Saat Ini

Berdasarkan hasil diatas, pengujian *website* PPDB sekolah XYZ tergolong tidak aman karena pada tahap *penetration testing* didapatkan kerentanan setelah melakukan pengujian XSS dan *shell upload exploitation* yang dimana dapat berdampak pada serangan *cyber* seperti *deface* website hingga untuk langkah awal pada *gaining access and privilege escalation* untuk mendapatkan hak akses.

3.5. Kesimpulan (Conclusion)

Berdasarkan dari pembahasan yang telah dipaparkan sebelumnya maka diambil beberapa kesimpulan. Kesimpulan tersebut yaitu:

1. Kondisi keamanan sistem informasi setelah melakukan pengujian *penetration testing*. Ditemukan celah keamanan sehingga tergolong tidak aman pada *website* PPDB sekolah XYZ, yaitu: *cross-site scripting* (XSS) dan penanaman *shell PHP* pada *form upload user* pada *website* PPDB sekolah XYZ, serta ditemukan celah lain melalui hasil *vulnerability scan* mengenai DNS dan SSL, dan berhasil melakukan proses *scanning port* terbuka. Namun seluruh uji coba serangan dalam melakukan *gaining access and privilege escalation* tidak berhasil untuk mendapatkan hak akses ke server PPDB sekolah XYZ karena *website* terkonfigurasi dengan baik sehingga tidak bisa berlanjut ke tahap *compromise remote user/site, maintaining access,* dan *corvering tracks.*
2. Dalam melakukan langkah-langkah *penetration testing* pada *website* PPDB sekolah XYZ berdasarkan *framework* ISSAF, maka didapatkan hasil: tahap *information gathering* berhasil dilakukan dengan mendapatkan informasi pribadi milik *website* PPDB sekolah XYZ, *network mapping* berhasil dilakukan dengan mendapatkan informasi *port* terbuka hingga versi yang digunakan, *vulnerability identification* berhasil dilakukan dengan mendapatkan hasil kerentanan secara otomatis, *penetration testing* menggunakan tiga teknik pengujian dengan satu teknik pengujian gagal dan dua teknik pengujian berhasil dengan menemukan kerentanan secara uji teknikal, *gaining access and privilege escalation* tidak berhasil dilakukan karena pada setiap teknik tidak mendapatkan hak akses, *enumerating further* tidak berhasil dilakukan karena komunikasi data yang ada pada jaringan *website* PPDB sekolah XYZ dilindungi oleh *protocol* TLS ter-*update*.
3. Rekomendasi yang diberikan yaitu selalu memvalidasi pada *level* PHP untuk mencegah adanya serangan XSS dan penanaman shell PHP, selalu memperhatikan konfigurasi terkait DNS dan SSL pada sistem, dan menutup akses orang untuk melakukan scan terhadap *port-port* yang ada didalam sistem. Lalu dilanjutkan dalam pemberian buku report agar pihak lembaga sekolah XYZ dapat memperbaiki berdasarkan hasil rekomendasi yang ada yang sesuai dengan hasil pengujian keamanan sistem *website* PPDB.

Ucapan Terima Kasih (Acknowledgement)

Terimakasih kepada semua pihak yang terlibat dalam pengerjaan penelitian ini, yaitu Rektorat Institut Teknologi Telkom Surabaya, Bapak Muhamad Nasrullah, S.Kom., M.Kom., Selaku Dosen Pembimbing 1 dan Bapak Adzanil Rachmadhi Putra, S.Kom., M.Kom., Selaku Dosen Pembimbing 2, Staff dan Dosen Institut Teknologi Telkom Surabaya yang telah memberikan pengetahuan dan

pengalaman yang berharga selama masa studi di perguruan tinggi ini, Teman dekat yang selalu memberikan semangat, dukungan, dan doa.

Daftar Pustaka

Agus Rochman, Rizal Rohian Salam, dan S. A. M. (2021). *Analisis Keamanan Website Dengan Information System Security Assesment Framework (ISSAF) Dan Open Web Application Security Project (OWASP) Di Rumah Sakit XYZ*. *2*(4), 6.

Alfin Syarifuddin Syahab, Erik Iman Heri Ujianto, R. (2023). Penggunaan Wireshark dan Nessus untuk Analisis SSL/TLS pada Keamanan Data Pengguna Website. *JIKA (Jurnal Informatika)*, *7*(2), 183–192.

Alwi, E. I., Herdianti, H., & Umar, F. (2020). Analisis Keamanan Website Menggunakan Teknik Footprinting dan Vulnerability Scanning. *INFORMAL: Informatics Journal*, *5*(2), 43. https://doi.org/10.19184/isj.v5i2.18941

Charly, P., Diatmika, K. E., Prayoga, I. M. P., & Listartha, I. M. E. (2022). Pendeteksian Keamanan Website SMA Greenschool Menggunakan Metode Owasp dengan Pengujian XSS. *Format : Jurnal Ilmiah Teknik Informatika*, *11*(1), 77. https://doi.org/10.22441/10.22441/format.2022.v11.i1.008

Cindy Mutia Annur. (2022). *Ada 204,7 Juta Pengguna Internet di Indonesia Awal 2022*. https://databoks.katadata.co.id/datapublish/2022/03/23/ada-2047-juta-pengguna-internet-di-indonesia-awal-2022

Eko Prasetyo, S., & Hassanah, N. (2021). Analisis Keamanan Website Universitas Internasional Batam Menggunakan Metode ISSAF. *Jurnal Ilmiah Informatika*, *9*(02), 82–86. https://doi.org/10.33884/jif.v9i02.3758

Irfan Murti Raazi, Ima Dwitawati, P. N. (2023). Uji Vulnerability Assessment Dalam Mengetahui Tingkat Keamanan Web Aplikasi Sistem Informasi Laporan Diskominfo dan Sandi Aceh. *JINTECH: Journal of Information Technology*, *4*(1), 1–15.

Jrsfaisal. (2018). *[SECURITY BUG] - Reflected Cross Site Scripting (XSS) On Parameter Cari #1175*. https://github.com/OpenSID/OpenSID/issues/1175

Kamilah, I., & Hendri Hendrawan, A. (2019). Analisis Keamanan Vulnerability pada Server Absensi Kehadiran Laboratorium di Program Studi Teknik Informatika. *Prosiding Semnastek*, *16*(0), 1–9. https://jurnal.umj.ac.id/index.php/semnastek/article/view/5233

Muhammad Anis Al Hilmi1*), R. K. Y. (2022). Pengujian Keamanan Fitur Upload File Pada Sistem Aplikasi Web . *Jurnal Informatika: Jurnal Pengembangan IT (JPIT), Vol.7, No.1, Januari 2022* , *7*(keamanan), 37–43.

Sanjaya, I. G. A. S., Sasmita, G. M. A., & Arsa, D. M. S. (2020). Evaluasi Keamanan Website Lembaga X Melalui Penetration Testing Menggunakan Framework ISSAF. *Jurnal Ilmiah Merpati (Menara Penelitian Akademika Teknologi Informasi)*, *8*(2), 113. https://doi.org/10.24843/jim.2020.v08.i02.p05

Sutarti, Pancaro, A. P., & Saputra, F. I. (2018). Implementasi IDS (Intrusion Detection System) Pada Sistem Keamanan Jaringan SMAN 1 Cikeusal. *Jurnal PROSISKO*, *5*(1), 1–8.

Syarif Revolino, T., & Jatmiko Andri, D. (2019). *Analisis Perbandingan Metode Web Security PTES , ISSAF Dan OWASP Di Dinas Komunikasi Dan Informasi Kota Bandung*. 8. https://elibrary.unikom.ac.id/880/13/21.10112427_TIO REVOLINO SYARIF_JURNAL BAHASA INDONESIA.pdf

Utoro, S., Nugroho, B. A., Meinawati, M., & Widianto, S. R. (2020). Analisis Keamanan Website E-Learning SMKN 1 Cibatu Menggunakan Metode Penetration Testing Execution Standard. *Multinetics*, *6*(2), 169–178. https://doi.org/10.32722/multinetics.v6i2.3432

Wardhana, A. W., & Seta, H. B. (2021). Analisis Keamanan Sistem Pembelajaran Online Menggunakan Metode ISSAF pada Website Universitas XYZ. *Informatik : Jurnal Ilmu Komputer*, *17*(3), 226. https://doi.org/10.52958/iftk.v17i3.3653