Analisis Keamanan Sistem Pembelajaran *Online* Menggunakan Metode ISSAF pada *Website* Universitas XYZ

Andhika Wisnu Wardhana[1], Henki Bayu Seta[2]
Informatika / Fakultas Ilmu Komputer
Universitas Pembangunan Nasional Veteran Jakarta
Jl. RS. Fatmawati Raya, Pd. Labu, Kec. Cilandak, Kota Depok, Jawa Barat 12450
email: [1]andhikawisnu6@gmail.com, [2]henkiseta@upnvj.ac.id

Abstrak. *Website e-learning* Universitas XYZ adalah suatu aplikasi yang mudah digunakan dimanapun dan kapanpun hanya dengan menggunakan browser, baik melalui *smartphone* maupun komputer. *E-learning* menyimpan data-data mahasiswa berupa tugas, *quiz*, dan lain-lain. Dikarenakan krusialnya penggunaan *website* tersebut, untuk mengantisipasi ancaman-ancaman terhadap *website e-learning* Universitas XYZ, maka peneliti akan melakukan pengujian terhadap keamanan *website e-learning* Universitas XYZ. Pengujian keamanan *website* dilakukan dengan menggunakan metode *Web Penetration Testing*. *Framework* yang digunakan dalam pengujian *penetration testing* terhadap *website e-learning* Universitas XYZ adalah *framework* ISSAF. Tujuan penelitian ini adalah untuk mengetahui apakah terdapat celah keamanan pada *website e-learning* Universitas XYZ. Dari hasil pengujian ini, ditemukan beberapa kerentanan yakni, *Brute-force Attack*, *Cross-Site Request Forgery* (CSRF) *Attack*, *Session Hijacking* melalui *Cookie*, maupun *IDOR (Insecure Direct Object Reference).* Hasil *report* dan pemberian rekomendasi akan diberikan kepada pihak administrator IT Universitas XYZ. Penelitian ini diharapkan dapat membantu administrator IT Universitas XYZ untuk melakukan pengembangan atau peningkatan terhadap keamanan *website.*

Kata kunci: *Website*, *Penetration testing*, *ISSAF*, *E-learning*

1 Pendahuluan

Perkembangan teknologi yang semakin canggih menciptakan kemudahan dalam berbagai kegiatan manusia. Dengan berkembangnya teknologi dan ditemukannya jaringan internet, manusia menjadi lebih mudah dalam mengakses informasi dan membagikan informasi ke seluruh penjuru dunia. Kemudahan yang ditawarkan tentunya selaras dengan bahaya yang dapat disisipkan melalui berbagai hal. Ancaman dalam bidang digital tentunya dapat berpengaruh pada sistem secara keseluruhan, terlebih lagi *website*.

Website adalah dokumen yang berisi banyak tautan untuk menghubungkan satu dokumen dengan dokumen-dokumen lainnya [1]. *Website* dapat diakses dimanapun dan kapanpun hanya dengan menggunakan browser, baik melalui *smartphone* maupun komputer. Oleh karena kemudahan tersebut, *website* menjadi pilihan terbaik untuk memudahkan pekerjaan manusia sehari-hari.

Website E-learning Universitas XYZ merupakan *website* yang digunakan untuk sistem pembelajaran *online* pada Universitas XYZ. *Website* ini digunakan oleh mahasiswa untuk mengunduh materi dari dosen, melihat tugas, mengerjakan quiz dan mengunggah tugas yang diberikan oleh dosen. Selain digunakan oleh mahasiswa, *website* ini juga digunakan oleh dosen untuk memeriksa dan menilai tugas-tugas yang sudah diunggah oleh mahasiswa.

Di tengah pandemi covid-19 ini, penetrasi pengguna internet di Indonesia semakin meningkat. Asosiasi Penyelanggara Jasa Internet Indonesia (APJII) menjelaskan terdapat kenaikan trafik pengguna internet sekitar 20-25% dibandingkan pada tahun 2018 yang mana pengguna internet di Indonesia mencapai 171,17 juta dari total populasi sebanyak 264,14 juta orang pada saat itu (Asosiasi Penyelanggara Jasa Internet Indonesia, 2020). Peningkatan tersebut terjadi dikarenakan terjadi perubahan pola perilaku masyarakat yang biasanya dilakukan di perkantoran dan di sekolah, sekarang di lakukan di rumah. Oleh karena peningkatan jumlah pengguna internet tersebut, maka perlu diperhatikan mengenai keamanan dalam *website* untuk mencegah ancaman terhadap sistem yang berpotensi merusak sistem.

ISSN : 2655-139X (ONLINE)
ISSN : 0216-4221 (PRINT)

Berdasarkan informasi dari portal berita sky news [2], pada September 2020 telah terjadi serangan siber yang menimpa Newcastle University. Peretas berhasil membobol jaringan komputer Newcastle University yang berakibat pada lumpuhnya *website* Newcastle University selama berminggu-minggu. Selain itu, peretas berhasil mencuri data dan mengenkripsi mesin menggunakan Malware DoppelPaymer. Peretas mengancam akan membocorkan data pribadi mahasiswa apabila tidak diberikan tebusan.

Kasus tersebut membuktikan bahwa data penting yang diletakkan di *web server* bisa saja diretas oleh seseorang yang tidak berwenang. Dikarenakan sangat krusialnya penggunaan *website* tersebut, maka peneliti ingin melakukan *Web Penetration Testing* untuk mengetahui tingkat keamanan sistem pembelajaran *online* yang ada di Universitas XYZ. *Penetration testing* ini perlu dilakukan karena pada sistem pembelajaran *online* Universitas XYZ mengandung materi-materi dan tugas-tugas yang penting bagi mahasiswa dan dosen, selain itu sistem pembelajaran *online* Universitas XYZ ini terhubung dengan SIAKAD dan juga subdomain Universitas XYZ lainnya, sehingga dirasa perlu untuk dilakukan pengecekan terhadap keamanan *website* ini.

Penelitian ini dilakukan untuk meminimalisir dan mengantisipasi kejahatan *hacking* yang dilakukan para *hacker*. Terdapat tiga penelitian terdahulu yang digunakan sebagai acuan untuk mengerjakan penelitian ini, penelitian [3] melakukan penelitian untuk menguji ketahanan *website* akademik pada Sistem Informasi Akademik Universitas XYZ. Pada penelitian tersebut, peneliti menggunakan metode *Information Systems Security Assessment Framework* (ISSAF) pada saat melakukan *penetration testing.* Namun penelitian tersebut hanya menguji ketahanan *website* dari serangan *Sql Injection*, peneliti tidak menguji ketahanan website dari jenis serangan selain *Sql Injection.* Penelitian [4] melakukan penelitian untuk menguji ketahanan *website* Lembaga X. Lembaga X adalah lembaga pemilihan umum yang memiliki situs *web* sebagai media penyampaian informasi dan penataan data pemilih. Pada penelitian tersebut, peneliti menggunakan metode *Information Systems Security Assessment Framework* (ISSAF) pada saat melakukan *penetration testing.* Peneliti melakukan tahapan *Information gathering, Network mapping, Vulnerability identification, Penetration, Gaining access and privilege escalation, Enumerating further, Compromising remote users/sites, Maintaining access, Covering the tracks.* Uji penetrasi yang dilakukan adalah dengan melakukan serangan S*ql Injection* dan *XSS Cross Scripting*. Penelitian [5] melakukan penelitian untuk menguji ketahanan suatu *website* dengan menggunakan beberapa serangan, antara lain adalah *Sql Injection, Cross site Scripting, Directory Traversal, Broken Authentication and session management, Parameter / Form tampering, Denial of Service, dan Http request header injection.*

Metode *Penetration Testing* yang digunakan pada penelitian ini adalah dengan menggunakan metodologi *Information Systems Security Assessment Framework* (ISSAF). ISSAF dipilih karena penetration testing dilakukan pada aplikasi *website*, selain itu ISSAF bersifat *opensource* dan ISSAF memiliki pedoman yang terstruktur sehingga pengujian mendapatkan arahan yang lengkap dan jelas. Dari hasil pengujian ini, laporan atau hasilnya akan diberikan kepada pihak administrator IT agar pengembangan terhadap keamanan sistem bisa dapat dipertahankan atau ditingkatkan kembali.

2 Kajian Pustaka

Studi literatur yang direferensikan dalam penulisan ini adalah hasil dari penelitian yang telah dibuat sebelumnya sebagai bahan referensi dari penulisan, yaitu mengenai *penetration testing* menggunakan framework ISSAF.

2.1 *Penetration Testing*

Pengujian penetrasi atau *pentesting* melibatkan simulasi serangan untuk menilai risiko yang terkait dengan potensi pelanggaran keamanan. Dalam pengujian penetrasi, penguji tidak hanya menemukan kerentanan yang dapat digunakan *penyerang* tetapi juga mengeksploitasinya, untuk mencari tahu apa yang mungkin penyerang akan dapatkan setelah berhasil melakukan eksploitasi sistem [6]. Secara garis besar terdapat 6 tahapan pada *penetration testing*, yaitu *Information Gathering*, *Threat Modeling*, *Vulnerability Analysis*, *Exploitation*, *Post Exploitation*, dan *Reporting.*

ISSN : 2655-139X (ONLINE)
ISSN : 0216-4221 (PRINT)

2.2 *Framework* ISSAF

Information Systems Security Assessment Framework (ISSAF) dikembangkan oleh OISSG (Open Information System Security Group). ISSAF adalah metodologi dimana *penetration tester* meniru langkah-langkah peretasan dengan *beberapa* fase tambahan [7].

Fase pertama merupakan fase *Information Gathering***.** Fase *information gathering* merupakan tahap awal yang berupa pengumpulan informasi dengan menggunakan Internet untuk menemukan semua informasi tentang domain target. Fase kedua merupakan fase *Network Mapping*, mengikuti bagian pertama, ketika semua informasi yang mungkin tentang target telah diperoleh, pendekatan yang lebih teknis diambil untuk "*footprint*" jaringan.. Informasi mengenai jaringan yang dikumpulkan meliputi *port* dan *service* yang digunakan. Fase ketiga merupakan fase *Vulnerability identification, pentester* melakukan berbagai kegiatan untuk mengidentifikasi kelemahan yang dapat dieksploitasi. Fase keempat merupakan fase *Penetration,* penguji mencoba untuk mendapatkan akses tidak sah dengan menghindari keamanan dan mencoba untuk mencapai tingkat akses seluas mungkin. Fase kelima merupakan fase *Gaining access and privilege escalation.* Fase *gaining access and privilege escalation* merupakan tahapan mendapatkan akses hak istimewa dengan mendapatkan akses ke akun melalui beberapa cara, yaitu mencoba kombinasi *username* dan *password*, misal *Brute-force attacks* atau *Dictionary Attacks* dan mencoba *blank password* atau *default password*. Fase keenam merupakan fase *Enumerating further.* Fase *enumerating further* merupakan tahapan lanjutan dari tahap sebelumnya meliputi *decrypt password*, *sniff traffic*, mengambil *cookie* untuk *exploit session* dan *password attack*, dan memperoleh *email address*. Fase ketujuh merupakan fase *Compromising remote users/sites,* fase ini memungkinkan pengujian dengan melakukan eksploitasi untuk mendapatkan akses ke dalam *user root* melalui hubungan jarak jauh/*remote* pada *web*. Fase kedelapan merupakan fase *Maintaining access,* fase ini memungkinkan pengujian dengan melakukan penanaman *backdoor* ke dalam sistem *website* target. *Backdoor* dimaksudkan untuk selalu dapat kembali ke sistem target, bahkan jika akun yang Anda gunakan untuk meretas sistem tidak lagi tersedia. Fase kesembilan merupakan fase *Covering the tracks.* Fase *covering tracks* merupakan tahapan terakhir dari pengujian *penetration testing*, fase ini dilakukan dengan cara menghapus *log* serangan yang telah dilakukan sebelumnya. Setelah semua fase dilakukan maka dapat dilakukan *Reporting* dan pemberian rekomendasi untuk menutup celah yang telah ditemukan sebelumnya.

3 Metodologi Penelitian

Tahapan *penetration testing* diawali dengan studi literatur, observasi dan wawancara. Studi literatur dilakukan dengan membaca jurnal terkait *penetration testing* pada suatu *website* yang telah dilakukan oleh peneliti terdahulu.

Observasi dilakukan dengan cara mengunjungi laman sistem pembelajaran *online* dari Universitas XYZ. Pengamatan dilakukan dengan melihat dan mencoba fitur-fitur yang tersedia di laman sistem pembelajaran *online* Universitas XYZ.

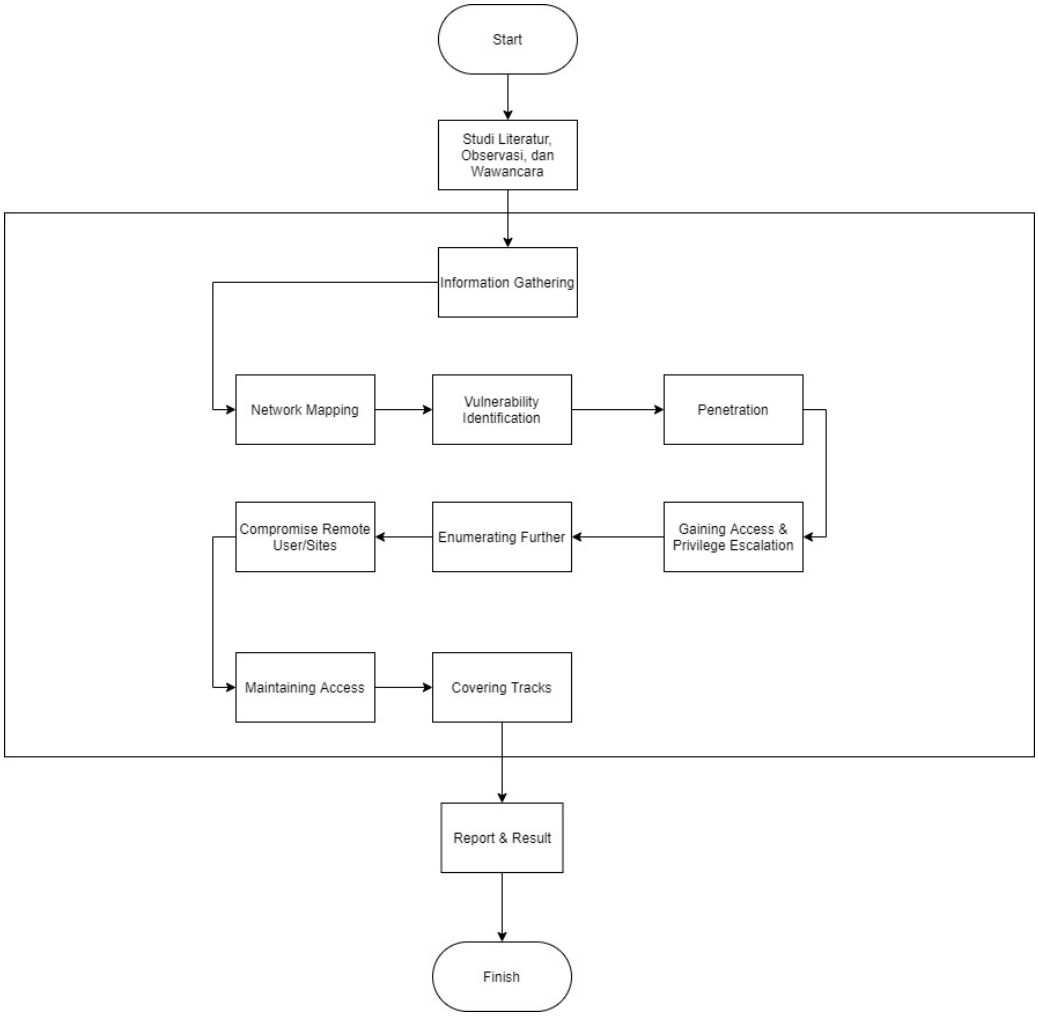
Wawancara dilakukan dengan datang secara langsung ke Ruang Teknologi Informasi dan Komunikasi Universitas XYZ, untuk bertemu langsung dengan Kepala UPT Teknologi Informasi dan Komunikasi Universitas XYZ. Tujuan wawancara tersebut adalah untuk meminta perijinan mengenai riset *penetration testing* terhadap laman sistem pembelajaran *online* Universitas XYZ serta mengetahui batasan-batasan apa saja yang boleh dan tidak boleh dilakukan terhadap *website* sistem pembelajaran *online* Universitas XYZ.

Selanjutnya, dilakukan pengujian *penetration testing* menggunakan 9 tahapan pada Framework ISSAF. Setelah semua pengujian selesai dilakukan, maka dilakukan tahap *Reporting*, yaitu merangkum celah yang ditemukan selama *penetration testing* dan memberikan rekomendasi untuk menutup celah yang ditemukan pada *website* sistem pembelajaran *online* Universitas XYZ. Tahapan penelitian yang dilakukan dapat dilihat pada Gambar 1.

ISSN : 2655-139X (ONLINE)
ISSN : 0216-4221 (PRINT)

3.1 Information Gathering

Tahap *information gathering* merupakan tahap awal yang berupa pengumpulan informasi dengan menggunakan Internet untuk menemukan semua informasi tentang domain target (perusahaan dan/atau orang) menggunakan kedua teknis (DNS/WHOIS) dan metode non-teknis (*search engines, news groups, mailing lists*, dll).



Gambar 1. *Flowchart* Alur Penelitian

3.2 Network Mapping

Mengikuti bagian pertama, ketika semua informasi yang mungkin tentang target telah diperoleh, pendekatan yang lebih teknis diambil untuk "*footprint*" jaringan. Informasi mengenai jaringan yang dikumpulkan meliputi *port* dan *service* yang digunakan, dan sistem operasi yang digunakan pada *server*. *Tool* yang digunakan pada tahap ini yaitu *Nmap*.

3.3 Vulnerability Identification

Pada tahap *Vulnerability Scanning*, penguji melakukan berbagai kegiatan untuk mengidentifikasi kelemahan yang dapat dieksploitasi. Kerentanan biasanya diklasifikasikan menurut tingkat tertentu, yaitu: low, *medium*, *high*, dan *critical*. *Tool* yang digunakan pada tahap ini yaitu *Acunetix*.

ISSN : 2655-139X (ONLINE)
ISSN : 0216-4221 (PRINT)

3.4 Penetration

Penguji mencoba untuk mendapatkan akses tidak sah dengan menghindari keamanan dan mencoba untuk mencapai tingkat akses seluas mungkin. Tahapan ini bisa menggunakan serangan *Sql Injection, XSS Cross Script,* dan *Broken Access Control*. *Tool* yang digunakan pada tahap ini yaitu *Sqlmap*.

3.5 Gaining Access & Privilege Escalation

Tahap *gaining access and privilege escalation* merupakan tahapan mendapatkan akses hak istimewa dengan mendapatkan akses ke akun melalui beberapa cara, yaitu mencoba kombinasi *username* dan *password*, misal *Brute-force attacks* atau *Dictionary Attacks* dan mencoba *blank password* atau *default password*. *Tool* yang digunakan pada tahap ini yaitu *Hydra*.

3.6 Enumerating Further

Tahap *enumerating further* merupakan tahapan lanjutan dari tahap sebelumnya meliputi *decrypt password*, *sniff* traffic, mengambil *cookie* untuk *exploit session* dan *password attack*, dan memperoleh *email address*. *Tools* yang digunakan pada tahap ini yaitu *Burp Suite* dan *Wireshark*.

3.7 Compromise Remote User / Sites

Tahap ini memungkinkan pengujian dengan melakukan eksploitasi untuk mendapatkan akses ke dalam *user root* melalui hubungan jarak jauh/*remote* pada *web*. *Tool* yang digunakan pada tahap ini yaitu *Metasploit*.

3.8 Maintaining Access

Tahap ini memungkinkan pengujian dengan melakukan penanaman *backdoor* dan RCE (*Remote Code Execution)* ke dalam sistem *website* target. *Backdoor* dimaksudkan untuk selalu dapat kembali ke sistem target, bahkan jika akun yang Anda gunakan untuk meretas sistem tidak lagi tersedia (misalnya, telah dihentikan). *Backdoor* dapat ditanamkan dengan memanfaatkan fitur *file upload* yang tersedia pada *website* target. *Tools* yang digunakan pada tahap ini yaitu *Marijuana* dan *Weevely*.

3.9 Covering Tracks

Tahap *covering tracks* merupakan tahapan terakhir dari pengujian *penetration testing*. Tahap ini mudah dipahami tetapi biasanya diremehkan. Setelah penyerang telah berhasil mengkompromikan sistem, dia ingin menyimpannya tanpa memperingatkan administrator, untuk alasan yang jelas. Semakin lama penyerang tinggal di sistem yang dikompromikan, semakin baik kemungkinan dia akan dapat mencapai tujuannya lebih lanjut dalam jaringan. Selama proses kompromi sistem, beberapa hal yang mencurigakan dan/atau salah aktivitas dicatat. Seorang penyerang yang terampil tahu bahwa *log* perlu diolah. Dia memodifikasinya untuk menutupi jejaknya dan menipu kehadirannya.

3.10 Report & Result

Tahap *report & result* merupakan tahapan untuk melaporkan hasil pengujian penetrasi, yaitu hasil kerentanan apa saja yang ditemukan pada *website* dan juga pemberian solusi terhadap kerentanan yang ditemukan pada *website. Reporting* diberikan kepada IT Administrator Universitas XYZ untuk kedepannya dilakukan perbaikan terhadap celah keamanan yang telah ditemukan.

4 Hasil dan Pembahasan

Hasil dan pembahasan pada penelitian ini meliputi hasil pengujian menggunakan kesembilan tahapan Framework ISSAF dan rekomendasi yang diberikan berdasarkan hasil pengujian.

4.1 Information Gathering

Pengumpulan informasi dilakukan pada tanggal 11 Maret 2021 20:45:00 dengan menggunakan *tools Whois*, didapatkan informasi mengenai nama domain, id domain*, IP location,* informasi mengenai *registrar*, dan nama *server.*

ISSN : 2655-139X (ONLINE)
ISSN : 0216-4221 (PRINT)

Tabel 1. Hasil Scanning Whois.

Information Gathering Result	
Domain ID	PANDI-DO152311
Domain Name	xxxxx.ac.id
Create On	07/10/1999 13:32
Expiration Date	31/10/2021 23:59
IP Location	Jakarta Selatan
Name Server	elmo.ns.cloudflare.com
	leah.ns.cloudflare.com
Registrar Organization	PT INDOSAT MEGA MEDIA
Registrar Street	JL. KEBAGUSAN RAYA NO. 36 RAGUNAN PASAR MINGGU
Registrar City	Jakarta Selatan
Registrar State/Province	DKI Jakarta
Registrar Postal Code	12550
Registrar Country	ID
Registrar Phone	02178546969
Registrar Contact	Email : optech@indosat.net.id
Admin ID	-
Admin Name	-
Admin Organization	-

Berdasarkan Tabel 1, dapat dilihat bahwa pada hasil pemindaian *tool Whois* diperoleh informasi mengenai Domain ID, Nama Domain, Lokasi Server, Nama *Server*, dan Informasi mengenai Registrar, namun informasi mengenai *admin* gagal diperoleh karena disembunyikan (*hide*) oleh *whois*. Selanjutnya dilakukan pemindaian dengan menggunakan *tool dig* untuk mengetahui *IP address website*.

```
; <<>> DiG 9.16.12-Debian <<>> demoxxxxx.xxxxx.ac.id
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18064
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;demoxxxxx.xxxxx.ac.id.       IN    A

;; ANSWER SECTION:
demoxxxxx.xxxxx.ac.id.  300   IN    A     xxx.xxx.92.26
```

ISSN : 2655-139X (ONLINE)
ISSN : 0216-4221 (PRINT)

```
;; Query time: 120 msec
;; SERVER: 118.136.64.5#53(118.136.64.5)
;; WHEN: Tue Mar 23 00:45:13 WIB 2021
;; MSG SIZE  rcvd: 66
```

Dari pemindaian menggunakan *tool dig* diatas, maka didapatkan *IP Address website* demoxxxxx.xxxxx.ac.id adalah xxx.xxx.92.26.

Pemindaian berikutnya yaitu dengan melakukan *enumerate subdomain* untuk mengetahui *subdomain website* yang berkaitan dengan target. *Enumerate subdomain* dilakukan dengan menggunakan *tool Sublist3r*. Berdasarkan hasil IP lookup menggunakan *tool Sublist3r* terdapat 67 *link* yang merupakan *subdomain* dari *domain* xxxxx.ac.id.

4.2 Network Mapping

Pengumpulan informasi mengenai *port* dan *service*, begitu pula dengan *software version* dilakukan pada tanggal 15 Maret 2021 22:56:00 dengan menggunakan *tool Nmap,* didapatkan informasi sebagai berikut.

Tabel 2. Hasil Scanning Nmap

PORT	STATE	SERVICE	VERSION
22/tcp	open	ssh	OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
80/tcp	open	http	nginx 1.19.2
135/tcp	filtered	msrpc	
139/tcp	filtered	netbios-ssn	
443/tcp	open	https	nginx 1.19.2
444/tcp	open	snpp	Cherokee httpd 1.2.104
445/tcp	filtered	microsoft-ds	
593/tcp	filtered	http-rpc-epmap	
1433/tcp	filtered	ms-sql-s	
1434/tcp	filtered	ms-sql-m	
1900/tcp	filtered	upnp	
3128/tcp	filtered	squid-http	
4444/tcp	filtered	krb524	
4899/tcp	filtered	radmin	
5678/tcp	filtered	rrac	
9898/tcp	filtered	monkeycom	

Berdasarkan Tabel 2 dapat dilihat bahwa hasil pemindaian dengan menggunakan *tool Nmap* diperoleh informasi mengenai beberapa *port* yang terbuka (*open*), yaitu *port* 22, 80, 443, dan 444. Dari Tabel 3 juga terlihat bahwa *port* yang ada pada *website* demoxxxxx.xxxxx.ac.id hanya terdapat *port* TCP dan tidak ditemukan adanya *port* UDP.

4.3 Vulnerability Identification

Pada tahap ini dilakukan pemindaian terhadap *website* sistem pembelajaran *online* untuk mengetahui kerentanan keamanan yang dimiliki *website* target. *Tool* yang digunakan pada pengujian ini menggunakan *Acunetix* sebagai proses *scanning* untuk mengetahui kerentanan keamanan pada *website*. Hasil pemindaian *tool Acunetix* dapat dilihat pada Tabel 3.

ISSN : 2655-139X (ONLINE)
ISSN : 0216-4221 (PRINT)

Tabel 3. Hasil Pengujian Vulnerability Identification

Domain	Kerentanan	Level
https://demoxxxxx.xxxxx.ac.id/search/index.php	*HTML form without CSRF protection*	*Medium*
https://demoxxxxx.xxxxx.ac.id/mod/forum/view.php?id=11	*HTML form without CSRF protection*	*Medium*
https://demoxxxxx.xxxxx.ac.id/mod/jitsi/viewpriv.php?user=1235	*Sensitive page could be cached*	*Low*
https://demoxxxxx.xxxxx.ac.id/login/index.php	*Login page password-guessing attack*	*Low*
https://demoxxxxx.xxxxx.ac.id/repository/draftfiles_manager.php	*Broken links*	*Informational*
https://demoxxxxx.xxxxx.ac.id/my/index.php	*Broken links*	*Informational*
https://demoxxxxx.xxxxx.ac.id/blog/edit.php	*Broken links*	*Informational*

Berdasarkan Tabel 3, dapat dilihat bahwa Acunetix menemukan celah CSRF pada *website* dengan *level medium*, *sensitive page cached* dengan *level low, password-guessing attack* dengan *level low* dan *broken links* dengan *level informational*.

4.4 Penetration

Pada tahap *penetration* ini dimulailah simulasi serangan yang dilakukan pada *website* target yang bertujuan untuk memperoleh celah pada keamanan *website*. Pengujian yang dilakukan pada tahap ini yaitu uji *SQL Injection, Cross-Site Scripting* (*XSS*), dan *Broken Access Control* yang dilakukan pada *website* target. Kesimpulan hasil pengujian *Penetration* dapat dilihat pada Tabel 4.

Tabel 4. Kesimpulan tahap Penetration

Pengujian		Domain	Hasil
SQL Injection		https://demoxxxxx.xxxxx.ac.id/course/index.php?categoryid=1	Gagal
		https://demoxxxxx.xxxxx.ac.id/user/profile.php?id=2225	Gagal
		https://demoxxxxx.xxxxx.ac.id/mod/customcert/my_certificates.php?userid=2225	Gagal
		https://demoxxxxx.xxxxx.ac.id/user/course.php?course=1	Gagal
		https://demoxxxxx.xxxxx.ac.id/calendar/view.php?view=month	Gagal
		https://demoxxxxx.xxxxx.ac.id ?lang=en	Gagal
		https://demoxxxxx.xxxxx.ac.id/login/logout.php?sesskey=Ce6qFISVGS	Gagal
		https://demoxxxxx.xxxxx.ac.id/admin/index.php?cache=1	Gagal
		https://demoxxxxx.xxxxx.ac.id/login/index.php	Gagal
		https://demoxxxxx.xxxxx.ac.id/search/index.php?q=%3Cscript%3Ealert%28%22test%22%29%3B%3C%2Fscript%3E&context=2	Gagal
XSS Cross Scripting		https://demoxxxxx.xxxxx.ac.id/search/index.php?q=%3Cscript%3Ealert%28%22test%22%29%3B%3C%2Fscript%3E&context=2	Gagal
		https://demoxxxxx.xxxxx.ac.id/mod/forum/discuss.php?d=39841	Gagal
		https://demoxxxxx.xxxxx.ac.id/admin/tool/lp/user_evidence_list.php?userid=1283	Gagal
Broken Access Control	Bypass Login	https://demoxxxxx.xxxxx.ac.id/login/index.php	Gagal
	CSRF	https://demoxxxxx.xxxxx.ac.id/search/index.php	Berhasil
	IDOR	https://demoxxxxx.xxxxx.ac.id/user/profile.php?id=1283	Berhasil

ISSN : 2655-139X (ONLINE)
ISSN : 0216-4221 (PRINT)

Berdasarkan Tabel 4, dapat dilihat bahwa pengujian *SQL Injection* dan *XSS Cross Scripting* gagal dilakukan. Pada *Broken Access Control* pada saat pengujian *Bypass Login* juga gagal dilakukan. Namun pada saat pengujian *Cross-Site Request Forgery*, ternyata terdapat celah CSRF pada kolom *search website* demoxxxxx.xxxxx.ac.id. Dan pada saat pengujian *Insecure Direct Object Reference* juga terdapat celah pada URL *parameter* id yang memungkinkan *attacker* untuk memperoleh informasi *user* lain.

4.5 *Gaining Access and Privilege Escalation*

Tahap *gaining access and privilege escalation* merupakan tahapan mendapatkan akses hak istimewa dengan mendapatkan akses ke akun melalui beberapa cara, yaitu mencoba kombinasi *username* dan *password*, misal *Brute-force attacks* atau *Dictionary Attacks* dan mencoba *blank password* atau *default password*. Pengujian akan dilakukan dengan menggunakan metode *Brute-force Attacks* dengan menggunakan *tool Hydra*. Kesimpulan hasil pengujian *Enumerating Further* dapat dilihat pada Tabel 5.

Tabel 5. Kesimpulan tahap Gaining Access & Privilege Escalation

Pengujian	Status	Hasil
Brute-force Attacks	Terdapat celah Brute-force Attacks secara manual pada *login page*, namun tidak ditemukan *username* & *password* yang cocok	Gagal

Berdasarkan Tabel 5, dapat dilihat bahwa terdapat celah *Brute-force Attacks* pada *login page website* demoxxxxx.xxxxx.ac.id secara manual, karena login page tidak dilindungi dengan *account lockout* atau *limit login attempt.* Namun pengujian tahap ini gagal karena tidak menemukan *username* & *password* yang cocok.

4.6 Enumerating Further

Tahap *enumerating further* merupakan tahapan lanjutan dari tahap sebelumnya meliputi *sniff traffic* menggunakan *tool Wireshark* dan mengambil *cookie* untuk *exploit session* yang diperoleh dari *website* demoxxxxx.xxxxx.ac.id. Kesimpulan hasil pengujian *Enumerating Further* dapat dilihat pada Tabel 6.

Tabel 6. Kesimpulan Enumerating Further

Pengujian	Status	Hasil
Session Hijacking dengan *Cookie*	Berhasil *login* hanya dengan menggunakan *Cookie*	Berhasil
Sniffing Traffic	Gagal men-*capture* paket data berisi *username* dan*password* dalam jaringan, karena paket data di enkripsi dengan TLS 1.2	Gagal

Berdasarkan Tabel 6, dapat dilihat bahwa pengujian *Session Hijacking* dengan menggunakan *Cookies* berhasil, celah ini cukup berbahaya karena peretas dapat *login* ke *website* tanpa menggunakan *username* dan *password*. Sementara untuk *Sniffing Traffic*, *website* demoxxxxx.xxxxx.ac.id sudah aman karena pengiriman paket data nya sudah di enkripsi dengan TLS 1.2.

4.7 *Compromise Remote User/Sites*

Tahap ini memungkinkan pengujian dengan melakukan eksploitasi untuk mendapatkan akses ke dalam *user root* melalui hubungan jarak jauh/*remote* pada *web*. Pada tahap ini, pengujian dilakukan dengan menggunakan *tools Metasploit* dengan melakukan serangan ke *port-port* terbuka yang sudah didapatkan dari tahap *Network Mapping*. Kesimpulan hasil pengujian *Compromise Remote User/Sites* dapat dilihat pada Tabel 7.

Tabel 7. Kesimpulan tahap Compromise Remote User/Sites

Pengujian	Metode	Status	Hasil
SSH Port 22	Brute-force Key Attacks	Berhasil dilakukan *Brute-force Attacks*, namun tidak ditemukan *keys* yang cocok	Gagal
	Brute-force	Berhasil dilakukan *Brute-force Attacks*, namun tidak	Gagal

ISSN : 2655-139X (ONLINE)
ISSN : 0216-4221 (PRINT)

	Wordlists Attacks	ditemukan *username* & *password* yang cocok	
HTTP Port 80	Brute-force Wordlists Attacks	Gagal dilakukan *Brute-force Attacks*	Gagal
HTTPS Port 443	HeartBleed Attacks	Tidak ditemukan celah *HeartBleed*	Gagal
SNPP Port 444	Cross-site Script Attacks	Tidak ditemukan celah *Cross-site Script*	Gagal

Berdasarkan Tabel 7, dapat dilihat bahwa pengujian tahap *Compromise Remote User/Sites* gagal dilakukan. Namun ditemukan celah *Brute-force Attacks* pada *service* SSH *port* 22. Pengujian gagal dilakukan karena tidak ditemukan *keys*, *username* dan *password* yang cocok, sehingga gagal memperoleh akses *root* ke *server*.

4.8 Maintaining Access

Tahap ini memungkinkan pengujian dengan melakukan penanaman *backdoor* dan RCE (*Remote Code Execution)* ke dalam *website* target. *Backdoor* dan RCE dapat ditanamkan dengan memanfaatkan fitur *file upload* yang tersedia pada *website* target. *Tools* yang digunakan adalah Marijuana.php dan *Weevely*. Kesimpulan hasil pengujian *Maintaining Access* dapat dilihat pada Tabel 8.

Tabel 8. Kesimpulan tahap Maintaining Access

Pengujian	Status	Hasil
Penanaman *Backdoor* Marijuana	Berhasil ter-*upload*, namun tidak dapat di eksekusi, karena file .htaccess pada *server* dikonfigurasi untuk *force download*	Gagal
Penanaman *Backdoor* Weevely	Berhasil ter-*upload,* namun tidak dapat di eksekusi, karena *server* melakukan *filtering* terhadap *script*	Gagal
Penanaman RCE (*Remote Control Execution*)	Berhasil ter-*upload*, namun tidak dapat di eksekusi, karena *server* menonaktifkan fungsi *execution shell command*	Gagal

Berdasarkan Tabel 8, dapat dilihat bahwa pengujian tahap *Maintaining Access* ini gagal dilakukan. Semua file *backdoor* dapat ter-*upload* ke server, namun tidak ada yang tereksekusi karena *server* telah melakukan pengamanan dengan melakukan *force download, filtering script* dan *disable execution shell command.*

4.9 Covering the Tracks

Tahap *covering the tracks* merupakan tahapan untuk menutupi jejak agar tidak terdeteksi oleh administrator sistem dengan cara menghapus *log* pada sistem. Dengan penghapusan *log* tersebut maka serangan yang telah dilakukan pada tahapan-tahapan sebelumnya tidak diketahui oleh administrator. Kesimpulan hasil pengujian *Covering the Tracks* dapat dilihat pada Tabel 9.

Tabel 9. Kesimpulan tahap Covering Tracks

Pengujian	Status	Hasil
Penghapusan *log* file	Gagal, karena tidak memperoleh akses ke *root server.*	Gagal

Berdasarkan Tabel 9, dapat dilihat bahwa pengujian tahap *Covering the Tracks* ini gagal dilakukan. Hal ini karena akses ke *root server* tidak berhasil diperoleh, sehingga *log* serangan sebelumnya tidak dapat dihapus.

ISSN : 2655-139X (ONLINE)
ISSN : 0216-4221 (PRINT)

4.10 Report & Result

Tahap *report & result* merupakan tahapan untuk melaporkan hasil pengujian penetrasi, yaitu hasil kerentanan apa saja yang ditemukan pada *website* dan juga pemberian solusi terhadap kerentanan yang ditemukan pada *website.* Kesimpulan hasil *Report & Result* dapat dilihat pada Tabel 10.

Tabel 10. Kesimpulan tahap Report & Result

Kerentanan	Solusi	CVSS
Session Hijacking melalui *Cookie*	*Menerapkan regenerate Cookie value* pada setiap *request* Menambahkan *cookie* berupa *auth_token* yang unik setelah melakukan *login*	9.1
Brute-force Attack di *page login*	*Menerapkan account lockout* atau *limit login attempt*	7.5
Brute-force Attack di *port* 22	Menerapkan *limit login attempt*	7.5
Cross-Site Request Forgery (CSRF) di kolom *search*	Menerapkan *CSRF Token*	6.8
IDOR (Insecure Direct Object Reference)	*Menerapkan hide URL parameter* Menerapkan *Indirect Reference Map*	6.5
Unrestricted File Upload	Memberikan batasan mengenai ekstensi file yang boleh diunggah, seperti docx, xlsx, pptx, pdf dan rar saja.	6.5

Berdasarkan Tabel 10, dapat dilihat bahwa dari seluruh tahapan *penetration testing* yang telah dilakukan, terdapat 6 kerentanan yang telah diurutkan dari yang paling *critical* sampai *medium* pada *website* demoxxxxx.xxxxx.ac.id. Karena kerentanan yang ditemukan merupakan kerentanan *critical-medium* maka dapat disimpulkan *website* demoxxxxx.xxxxx.ac.id tidak cukup aman. Diharapkan pihak administrator IT *website* tersebut segera menutup kerentanan tersebut agar *website* menjadi lebih aman.

5 Kesimpulan

Setelah dilakukan penelitian terhadap keamanan *website* sistem pembelajaran *online* dengan metode ISSAF sehingga dapat disimpulkan bahwa berdasarkan sembilan tahapan tersebut diperoleh hasil bahwa *website* demoxxxxx.xxxxx.ac.id tidak aman dari serangan seperti *Brute-force Attack*, *Cross-Site Request Forgery* (CSRF) *Attack*, *Session Hijacking* melalui *Cookie*, maupun *IDOR (Insecure Direct Object Reference).*

Rekomendasi yang dapat diberikan adalah *limit login attempt* untuk mencegah *Brute-force Attack*, penerapan *CSRF token* pada *hidden field* untuk mencegah *CSRF Attack,* penerapan *hide parameter URL* atau *Indirect Reference Map* untuk mencegah celah pada *IDOR (Insecure Direct Object Reference)*, dan penerapan *Regenerate Cookie* pada setiap *request* untuk mencegah *Session Hijacking* melalui *Cookie.*

Referensi

[1] J. Enterprise, *Otodidak desain dan pemrograman website / Jubilee Enterprise*. Jakarta: Elex Media Komputindo, 2017.
[2] A. Martin, "Coronavirus: Newcastle Uni 'completely crippled' by pandemic and cyber attack," 2020. https://news.sky.com/story/coronavirus-newcastle-uni-completely-crippled-by-pandemic-and-cyber-attack-12067971 (accessed Jan. 06, 2020).

ISSN : 2655-139X (ONLINE)
ISSN : 0216-4221 (PRINT)

[3] A. I. Rosadi, "Analisis Keamanan Sistem Informasi Akademik Dengan Web Penetraion Testing," pp. 1–12, 2016.
[4] 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," *J. Ilm. MERPATI*, vol. 8 No. 2, pp. 1–12, 2020.
[5] K. S. Prasad, D. . K. R. Sekhar, and D. . P. Rajarajeswari, "An Integrated Approach Towards Vulnerability Assessment & Penetration Testing for a Web Application," *Int. J. Eng. Technol.*, 2018.
[6] G. Weidman, *Penetration Testing: A Hands-On Introduction to Hacking*. 2014.
[7] OISSG, *Information Systems Security Assessment Framework (ISSAF) Draft 0.2.1 B*. 2006.

ISSN : 2655-139X (ONLINE)
ISSN : 0216-4221 (PRINT)