Penetrasi Testing Aplikasi Website Udacoding

Nur Cahyono Kushardianto[1], Festy Winda Sari[1], Antoni Haikal[1], Muhammad Idris[1]

[1] Politeknik Negeri Batam, Jl. Ahmad Yani, Teluk Tering, Batam, Indonesia

***Abstract*—The rapid advancement of technology, particularly the internet, has propelled humanity into a modern world where digitalization is essential. Consequently, system security has become paramount in the utilization of information systems, including websites and desktop/mobile applications. According to the National Cyber and Crypto Agency (BSSN), Indonesia remains the top target for cyberattacks. Penetration testing is a lawful practice employed to identify vulnerabilities within a system and enhance its overall security. This penetration testing exercise was conducted on the website Udacoding, following a four-phase approach: planning, information gathering, attack simulation, and reporting. The findings and proposed solutions will be comprehensively documented in a final report.**

Keywords— cyber security, penetration testing, udacoding, web security

***Abstrak*— Perkembangan teknologi, khususnya internet saat ini, membawa manusia ke dunia modern yang menuntut digitalisasi. Oleh karena itu, keamanan sistem menjadi hal yang sangat penting dalam penggunaan sistem informasi, baik website maupun aplikasi desktop/mobile. Menurut Badan Siber dan Sandi Negara, Indonesia masih menjadi urutan pertama negara tujuan serangan oleh para peretas. Penetration testing merupakan upaya legal yang dilakukan untuk mencari celah keamanan suatu sistem, serta meningkatkan keamanan sistem. Kegiatan penyerangan dilakukan pada website Udacoding dengan 4 tahapan, yaitu perencanaan (planning), pengumpulan informasi (information gathering), serangan (attack), dan pelaporan (reporting). Hasil yang ditemukan dalam pelaksanaan penetration testing akan dituangkan ke dalam laporan beserta solusinya.**

***Kata Kunci*— keamanan siber, keamanan web, pengujian penetrasi, udacoding**

I. PENDAHULUAN

Tidak dipungkiri lagi bahwa berkembangnya teknologi saat ini membawa manusia kepada era aplikasi, dimana setiap lini kehidupan membutuhkan sistem atau perangkat lunak, baik berupa website maupun aplikasi berbasis multi-platform. Dengan munculnya website- website yang terhubung ke jaringan internet saat ini, dibutuhkan pula sumber daya yang mumpuni baik sumber daya manusia, maupun sumber daya perangkat lunak dan perangkat keras agar tercipta website yang aman bagi penggunanya. Keamanan sistem menjadi penting karena hal ini berurusan dengan Kerahasiaan (Confidentiality), Integritas (Integrity), dan Ketersediaan (Availability).

Badan Siber dan Sandi Negara mencatat bahwa selama tahun 2022 total trafik anomali sebanyak 976.429.996 dengan diantaranya adalah kasus web defacement. Selain itu, sektor administrasi pemerintahan merupakan sektor aduan siber terbanyak yang dilaporkan. Bulan Januari 2022 merupakan puncak trafik anomali terbesar, sebanyak 272.962.734 terdeteksi trafik anomali. Data tersebut menunjukan bahwa keadaan web server yang ada di indonesia masih

jauh dari keadaan aman dari ancaman dan serangan (Fachri, Fadlil, Riadi, 2021, p. 183-190). Hal yang dikemukan tersebut membuktikan data yang dimiliki oleh OWASP (lembaga non-profit yang berfokus pada keamanan sistem) bahwa pada tahun 2021 posisi tiga besar risiko keamanan pada aplikasi web secara berurutan adalah Broken Access Control, Cryptographic Failures, dan Injection.

Udacoding merupakan salah satu perusahaan yang bergerak di bidang software development dan Traning IT. Perusahaan ini didirikan pada tahun 2019 dengan nama PT. Koding Teknologi Asia. Sebagai perusahaan yang relatif masih muda, Udacoding belum memiliki sumber daya manusia yang fokus pada masalah keamanan siber. Tenaga ahli yang ada lebih difokuskan kepada pengembangan aplikasi web maupun mobile. Sementara itu perusahaan tersebut sudah menerima banyak penawaran baik dari segi pembuatan aplikasi dan training IT, tidak hanya dalam negeri akan tetapi juga dari luar negeri. Dengan kondisi infrastruktur website yang masih belum terjamin keamanannya, maka hal ini berpotensi untuk menghambat kemajuan perusahaan anak bangsa ini. Dalam masalah lain, perusahaan yang masih merintis ini beberapa kali merasakan pencobaan peretasan oleh orang-orang yang tidak bertanggung jawab. Kerentanan ini telah menimbulkan keresahan terhadap perusahaan dan juga pengguna terhadap aplikasi website tersebut.

Dalam mengidentifikasi kerentanan dalam suatu sistem atau jaringan dapat dilakukan uji penetrasi (Penetration Testing) untuk nantinya ketika ditemukan celah, maka dapat diberikan solusi atau perbaikan terhadap sistem. Penetration Testing saat ini merupakan metode yang popular dalam mengevaluasi keamanan sistem dan komputer dengan menerapkan beberapa langkah-langkah, lebih tepatnya merupakan kegiatan simulasi serangan yang berpotensi rentan terhadap suatu sistem. Tujuan penetration testing diantaranya adalah untuk meningkatkan pengelolaan keamanan atau kemampuan merespon terhadap ancaman, serta dapat membantu pihak manajemen dalam pengambilan keputusan.

Maka untuk membantu Udacoding dalam hal menerapkan dan mengimplementasikan Perpres Nomor 82 tahun 2022 tentang Perlindungan Informasi Vital dan Undang-undang Perlindungan Data Pribadi, dilakukan Penetrasi Testing (Pentest) terhadap salah satu aplikasi website Udacoding. Kegiatan ini bertujuan untuk menemukan celah kerentanan yang dimiliki oleh website tersebut sehingga membantu pihak Udacoding dalam membuat kebijakan dan regulasi yang berkaitan dengan penggunaan website, serta menyebarkan kesadaran keamanan dalam berteknologi baik terhadap pegawainya melalui presentasi hasil pentest yang didapatkan. Selain itu, akan tercipta rasa aman dan tidak khawatir terhadap data pribadinya yang dirasakan oleh pengguna.

II. TINJAUAN PUSTAKA

Beberapa karya ilmiah yang relevan sebagai acuan dalam kegiatan pengabdian ini ditunjukkan pada Tabel 1.

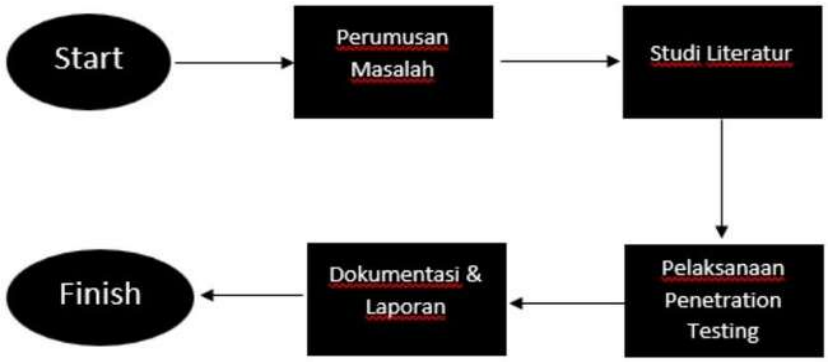
Tabel 1. Tinjauan Pustaka

Penulis	Judul	Tahun	Pembahasan
Dirgahayu et. al	Penelitian Penerapan Metode ISSAF dan OWASP versi 4 Untuk Uji Kerentanan Web Server	2015	Pemilik sistem harus melakukan pengujian mandiri terhadap server mereka untuk melindungi sistem dari serangan peretas.
Dewanto, Adetya	Penetration Testing Pada Domain uii.ac.id Menggunakan OWASP 10	2018	Penulis menggunakan metode OWASP Top 10 tahun 2013. Metode ini dipilih karena selalu dilakukan pembaruan terhadap informasi yang berisi 10 serangan terhadap web yang sering ditemukan menggunakan tool otomasi yaitu OWASP ZAP.
Mushlih et. al	Penetration Testing Tool Untuk Menguji Kerentanan Sql Injection Secara Otomatis Berbasis Web	2019	Penulis membahas tentang pengembangan alat uji penetrasi untuk menguji kerentanan SQL Injection yang merupakan salah satu jenis kerentanan teratas dalam daftar OWASP Top 10. Dalam prosesnya, pengujian keamanan dilakukan secara otomatis menggunakan aplikasi SQLMagic terhadap salah satu aplikasi subdomain di Politeknik Manufaktur Negeri Bangka Belitung.
Alanda et. al.	Web Application Penetration Testing Using SQL Injection Attack	2021	Penulis melakukan pengujian keamanan menggunakan metode Penetration Execution Execution Standard (PTES). 10 Target digunakan sebagai target percobaan untuk mengecek apakah kerentanan SQL injection dapat ditemukan pada masing-masing web. Dari hasil yang didapatkan melalui perangkat seperti hydra dan metsploit. 80% dari target uji dapat dikatan rentan terhadap SQL injection.

Penulis	Judul	Tahun	Pembahasan
Gunawan et. al	Penetration Testing Terhadap Website Universitas Pasundan Dengan Metode Zero Entry Hacking (Studi kasus: http://www.unpas.ac.id)	2022	Penulis melakukan pengujian kerentanan terhadap salah satu web di Universitas Pasundan menggunakan metode "*Zero Entry Hacking"*. Dari metode ini, penulis melakukan pengujian kerentanan yang difokuskan pada kerentantan *Sensitive Data Exposure* dan *Security Misconfiguration* yang ada di dalam daftar OWASP Top 10 2017. Dari jenis metode ini pula, karena tidak adanya akses menuju halaman admin dari web target, maka penulis tidak dapat menerapkan pengujian terhadap kerentantan *Broken Access Control*.
Hasibuan, Elhanafi	Penetration testing Sistem Jaringan Komputer Menggunakan Kali Linux Untuk Mengetahui Kerentanan Keamanan server dengan metode black box	2022	Pengujian kerentanan sistem dengan memanfaatkan sistem operasi Kali Linux menggunakan metode black-box ini ditargetkan pada sebuah web server divakaraoke.ac.id. Dari hasil pengujian dengan OWASP ZAP, penulis berhasil menemukan 2 celah serangan utama yaitu clickjacking dan sniffing. Dari proses scanning pula didapatkan port TCP yang terbuka di sisi server.

III. METODE

Kerangka bekerja pada gambar 1 merupakan serangkaian alur proses kegiatan pengabdian Penetration Testing Terhadap Website Udacoding.



Gambar 1. Kerangka Kerja Kegiatan Pengabadian

Dari proses yang ditunjukkan pada gambar 1, maka dapat dideskripsikan masing-masing proses secara berurutan seperti berikut ini:

1. Perumusan Masalah

Perumusan masalah adalah tahap awal kegiatan pengabdian ini. Pertemuan dan diskusi dengan mitra menjadi awal mula ide dari kegiatan ini, hingga diputuskan judul serta pembuatan proposal ini.

2. Studi Literatur

Pencarian pengetahuan dasar yang didapat dari buku, jurnal, artikel, serta media lain yang mendukung dalam kegiatan pengabdian ini.

3. Pelaksanaan Penetration Testing

Pada tahap ini, dilakukan penetration testing terhadap website Udacoding dengan empat tahapan utama, yaitu:

- ***Planning***: Menentukan tujuan dari penetration testing seperti sasaran utama, dan metode yang akan digunakan.
- ***Information Gathering***: Mengumpulkan informasi tentang target, misalnya nama domain, alamat IP, port yang terbuka, layanan yang berjalan, dan konfigurasi system dan melakukan analisis terhadap informasi yang dikumpulkan untuk mengidentifikasi kerentanan yang ada.
- ***Attack***: Pada tahap ini, pentester akan melakukan serangan terhadap target untuk mengeksploitasi kerentanan yang ditemukan. Serangan dapat dilakukan secara manual atau menggunakan tools penetration testing.
- ***Reporting***: Mendokumentasikan dan melaporkan hasil penetration testing, termasuk temuan kerentanan, rekomendasi perbaikan, dan bukti serangan.

Alat perangkat lunak yang digunakan dalam masing-masing tahapan diatas pun beragam, diantaranya seperti yang ditunjukkan pada Tabel 2.

Tabel 2. Alat pengujian keamanan

Nama alat	Kegunaan
Nmap	mengetahui perangkat apa saja yang terhubung ke jaringan, port apa saja yang terbuka, dan layanan apa saja yang berjalan di port tersebut
Wireshark	melihat dan menganalisis paket data yang dikirim dan diterima oleh perangkat di jaringan
Netcat	membuat koneksi TCP, UDP, atau raw socket serta menguji keamanan jaringan seperti *buffer overflow*, *denial of service*, dan lain-lain.
Metasploit	mengeksploitasi berbagai kerentanan keamanan dengan modul-modul yang tersedia pada *framework*-nya

Nama alat	Kegunaan
Burp Suite	Melakukan intersepsi dan inspeksi permintaan dan respons HTTP, melakukan *fuzzing* dan serangan lainnya terhadap aplikasi web serta melakukan pengujian keamanan web secara otomatis melalui *plugin-plugin* yang tersedia.

4. Dokumentasi & Laporan

Temuan yang dihasilkan pada tahap pelaksanaan penetration testing akan dituangkan kedalam laporan lengkap beserta solusi yang dapat dilakukan oleh pemilik website/perusahaan.

IV. HASIL DAN PEMBAHASAN

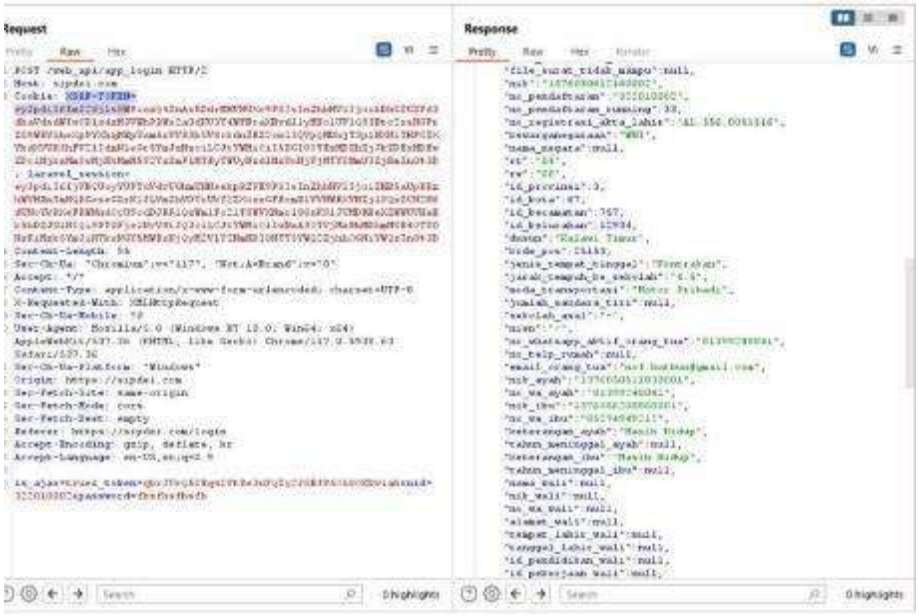
4.1 Hasil dan Pembahasan

Lingkup kegiatan pengabdian ini adalah untuk melakukan penilaian kerentanan terhadap aplikasi Udacoding berdasarkan CVSS dan melakukan uji penetrasi dengan fokus terhadap kerentanan yang ada pada OWASP TOP 10 tahun 2021.

Dalam menguji kerentanan aplikasi web ini, digunakan 2 pendekatan utama, yaitu:

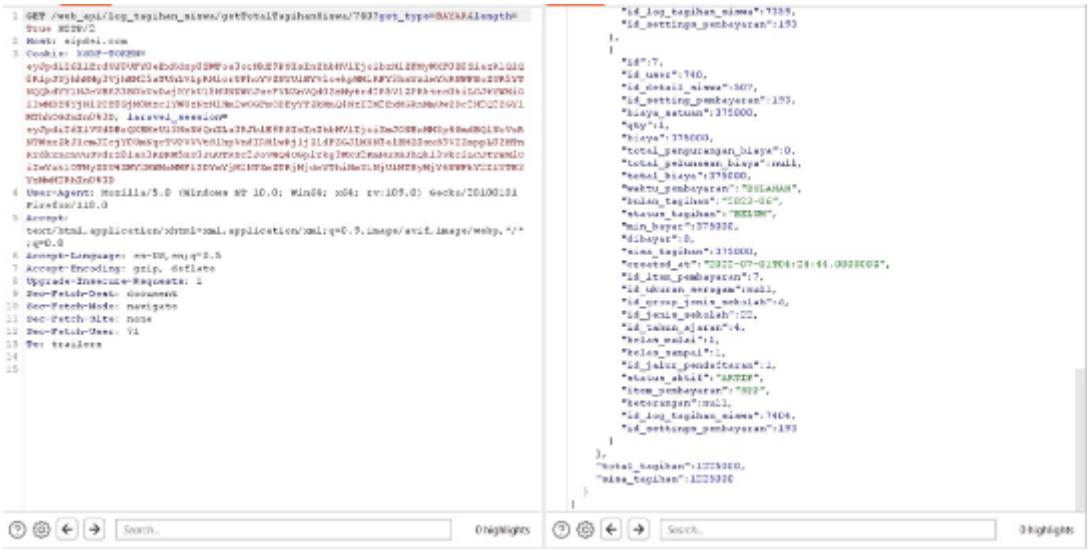
- **Otomatis**: Memindai kerentanan menggunakan aplikasi pemindai keamanan untuk mencari celah keamanan.
- **Manual**: Melakukan pengujian keamanan secara manual dengan mengeksploitasi kerentanan dan melihat dampaknya.

Dari hasil uji penetrasi yang dilakukan, kerentanan utama ditemukan pada halaman login pada URL *web_api/app_login?email=&password*. Ketika melakukan login menggunakan ID yang terdaftar dan menggunakan password yang salah, respon dari server akan menampilkan data dari ID yang digunakan untuk login meskipun menggunakan password yang salah. Dapat dilihat dari hasil yang ditunjukkan pada Gambar 2, bahwa respon yang didapatkan dari Burp Suite ini berhasil menampilkan data sensitif seperti nomor induk kependudukan dan alamat.



Gambar 2. Hasil uji kerentanan halaman login

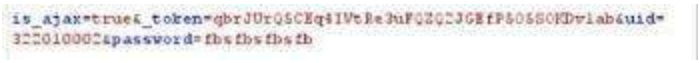
Kerentanan selanjutnya pada kategori *broken access control* adalah ditemukannya celah pada API *endpoint web_api/log_tagihan_siswa/*. dengan memanfaatkan teknik serangan IDOR (*Insecure Direct Object Reference*) melalui aplikasi Burp Suite**,** manipulasi parameter get dapat dilakukan untuk mendapatkan ID dari pengguna seperti yang ditunjukkan pada gambar 3**.**



Gambar 3. Celah keamanan pada endpoint tagihan mahasiswa

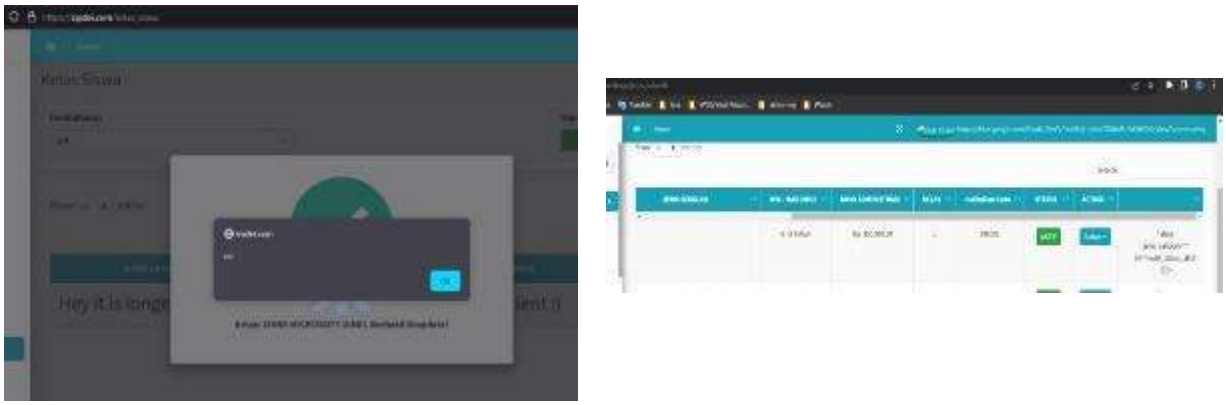
Selain dari kategori *broken access control*, celah keamanan pun ditemukan pada penerapan kriptografi yang buruk. Ketika pengguna masuk ke dalam sistem, intersepsi trafik dengan Burp

Suite berhasil mendapatkan ID dan password pengguna dalam bentuk *plain-text* seperti yang dapat dilihat pada Gambar 4. Seharusnya, penerapan kriptografi seperti algoritma hashing yang kuat dan direkomendasikan harus dilakukan pada pada bagian password pengguna.



Gambar 4. Password plain-text pengguna pada response

Selanjutnya, ditemukan pula celah keamanan injection khususnya *XSS injection* pada URL */Seting/Jenis_sekolah*. ketika memasukkan kode Javascript ke dalam formulir, maka data akan tersimpan ke database dan menampilkan data sensitif pada kolom deskripsi pada tabel seperti yang ditunjukkan pada Gambar 5.



Gambar 5. Hasil uji XSS injection pada Endpoint Jenis Sekolah

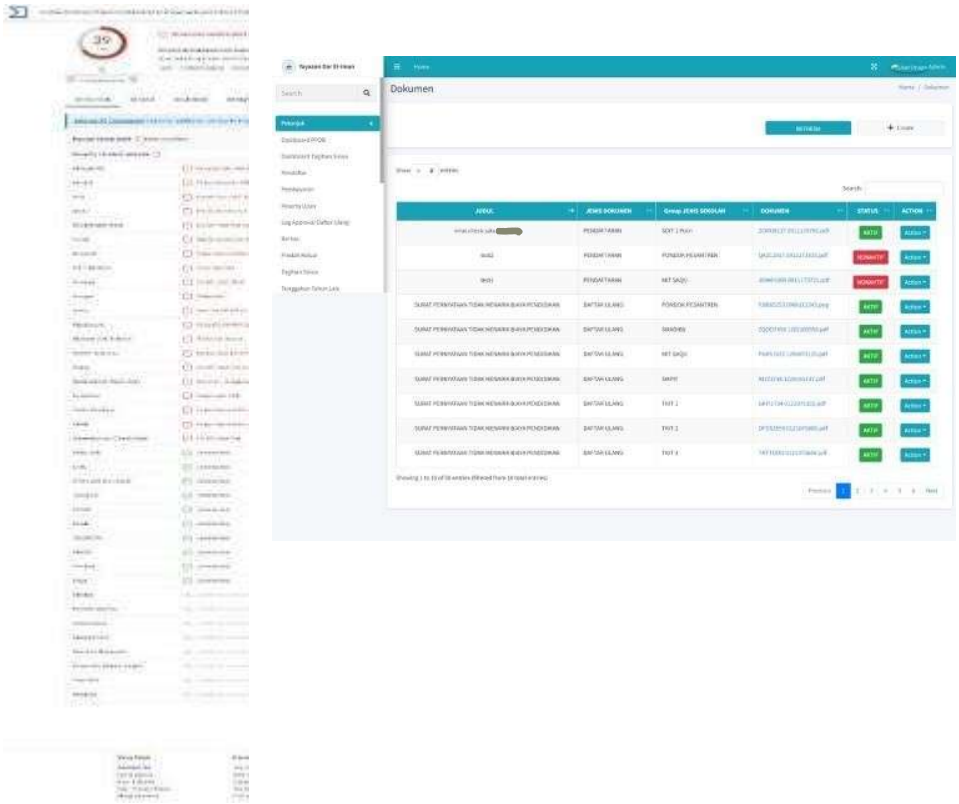
Celah keamanan selanjutnya, muncul dari *security misconfiguration* terhadap XSRF token dan implementasi session token pada parameter URL. Pada bagian XSRF token, kerentanan dapat diuji dengan memanipulasi metode get pada request, dengan perpaduan teknik IDOR dan celah token XSRF yang memiliki periode aktif lama, pengujian berhasil memperoleh kode HTTP error 500. Karena tidak adanya mekanisme error handling yang baik, data sensitif sistem meliputi data seperti nama tabel yang digunakan serta kolomnya, kueri SQL, jenis framework yang digunakan dan path dari web seperti yang ditunjukkan berhasil didapatkan seperti yang ditunjukkan pada Gambar 6.

Gambar 6. Pesan stack error dari sistem

Kerentanan kedua dari *security misconfiguration* timbul karena penempatan informasi sensitif session token dengan metode GET pada API endpoint track peserta ujian seperti yang ditunjukkan pada Gambar 7. Pengaturan token dengan mekanisme seperti ini meningkatkan risiko terhadap kerentanan karena bentuknya yang terlalu terekspos. Token session ini dapat di-*bookmark*, tersimpan di history dan log server, serta dibagi dalam bentuk tautan yang memiliki session token di dalamnya.

Gambar 7. Proses request dengan metode GET dan session token pengguna

Kerentanan selanjutnya ditemukan pada fitur unggah yang terdapat pada URL /Dokumen. Karena tidak adanya validasi input terhadap inputan file baik ekstensi dan tipe MIME-nya, proses penyerangan berhasil mengunggah atau mentransfer file berjenis berbahaya seperti kode PHP yang dapat diproses secara otomatis dalam lingkungan projek seperti yang ditunjukkan pada Gambar 8.



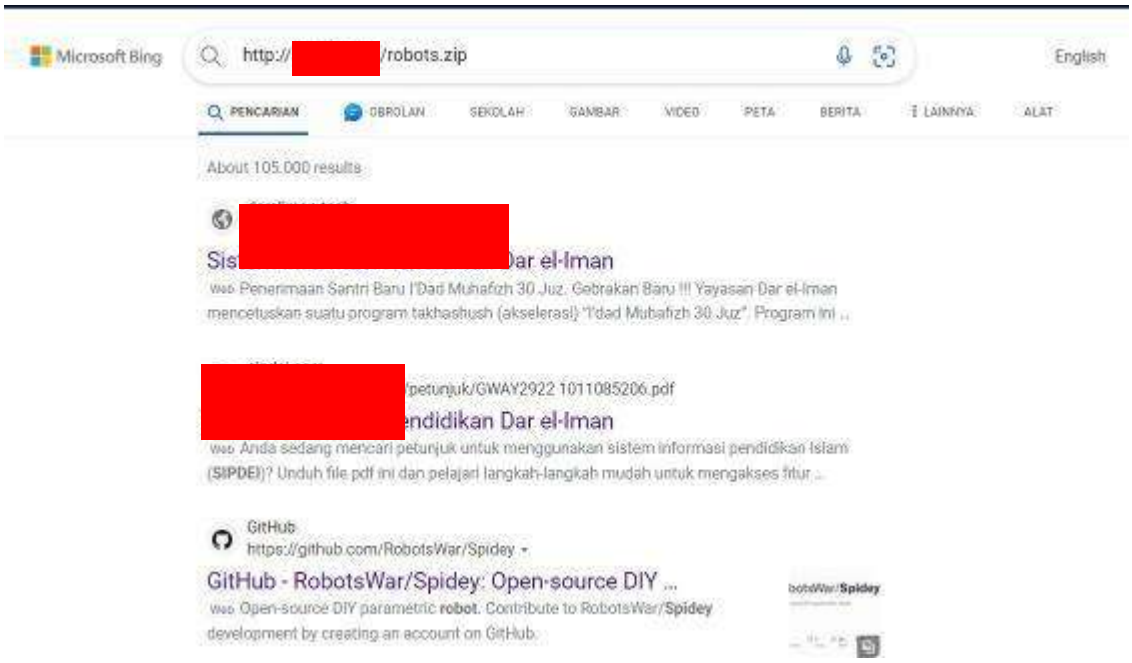
Gambar 8. Pengujian kerentanan unggah file di dokumen

Dari sisi server, web ini juga dapat dikatakan rentan dari serangan *memory exhaustion* yang dapat memperlambat kinerja aplikasi hingga bahkan menghentikan proses sistem seperti yang ditunjukkan pada percobaan nmap dan skrip slowloris pada Gambar 9.

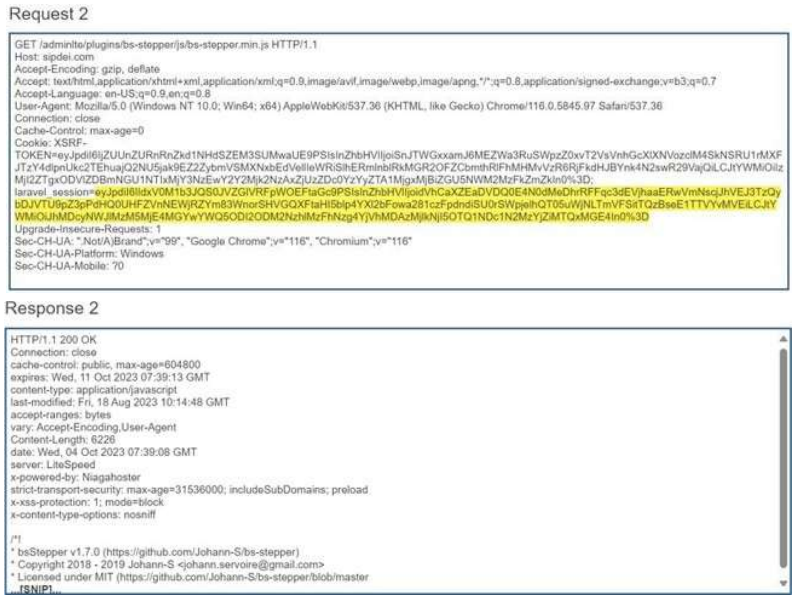
Gambar 9. Serangan memory exhaustion dengan NMAP dan Slowloris

Sebagai tambahan, 3 kerentanan potensial juga berhasil diidentifikasi seperti *frameable response* yang dapat menimbulkan serangan *clickjacking* (Gambar. 10) yang dapat terjadi akibat halaman gagal menyetel header HTTP X-Frame-Options atau Content-Security-Policy yang sesuai, file atau folder lama dan tidak dikelola dengan baik namun terekspos di publik (Gambar. 11) dan penerapan base64 encoding yang terdapat pada laravel_session (Gambar. 12). Untuk penggunaan data yang lebih sensitif, penerapan enkripsi selain base64 lebih aman dan direkomendasikan untuk melindungi data pengguna. Ketiga poin kerentanan ini dapat menjadi pintu dari kerentanan lainnya dapat menjadi masalah di kemudian hari jika tidak diperbaiki.

Gambar 10. Clickjacking di iframe



Gambar 11. File dan folder lama yang terekspos ke publik



Gambar 12. Laravel session dalam bentuk base64

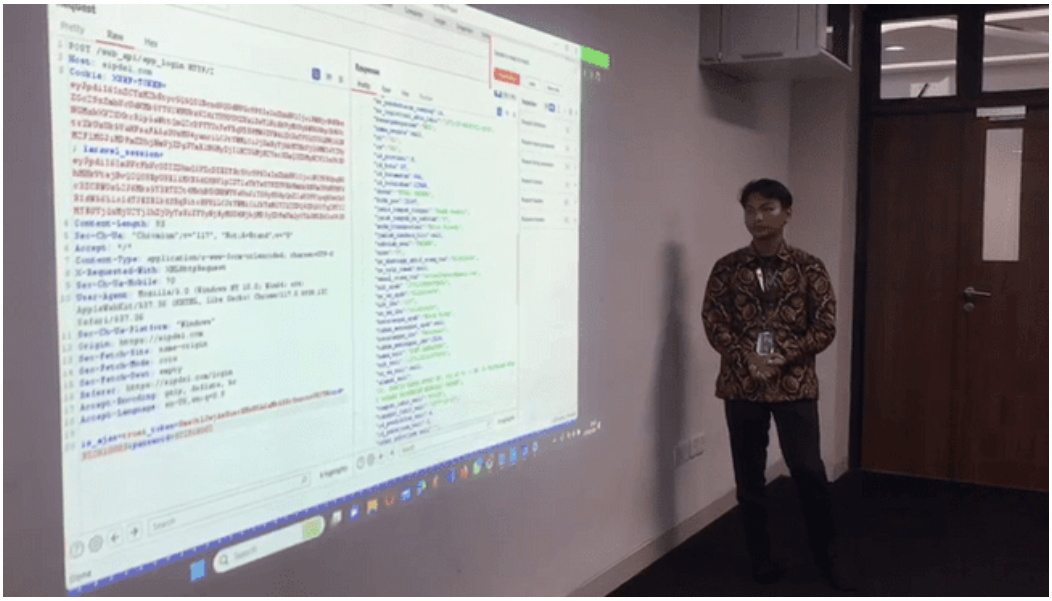
Dari hasil temuan-temuan dari uji penetrasi yang telah dilakukan, maka dapat diidentifikasikan hasil dari pengujian dalam bentuk *severity level* melalui metode penilaian CVSS (Common Vulnerability Scoring System) seperti yang ditunjukkan pada Tabel 3.

Tabel 3. Penilaian risiko keamanan dengan CVSS 3.1

No	Kerentanan	Severity Level	Base Score	CVSS Vector String
1	*Broken Access Control*	High	7.5	*CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N*
2	*Broken Access Control*	Medium	6.5	*CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N*
3	*Cryptographic Failures*	High	7.5	*CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N*
4	*Injection*	High	8.5	*CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:H/A:N*
5	*Security Misconfiguration*	Medium	6.5	*CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N*
6	*Security Misconfiguration*	Medium	6.5	*CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N*
7	*Unrestricted Upload of File with Dangerous*	High	8.8	*CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H*
8	*Uncontrolled Resource Consumption*	High	7.5	*CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H*
9	*Frameable response*	Informatif	0.0	*CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N*
10	*Publicly available of outdated file or folder*	Informatif	0.0	*CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N*
11	*Base64-encoded data in parameter*	Informatif	0.0	*CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N*

Pada akhirnya, seluruh temuan kerentanan dari proses uji penetrasi pun dipresentasikan secara langsung oleh anggota tim pengabdian seperti yang ditunjukkan pada Gambar 13, 14, dan 15.

Gambar 13. Ketua tim memberikan pengarahan kepada tim Udacoding



Gambar 14. Anggota tim mendemonstrasikan kerentanan web

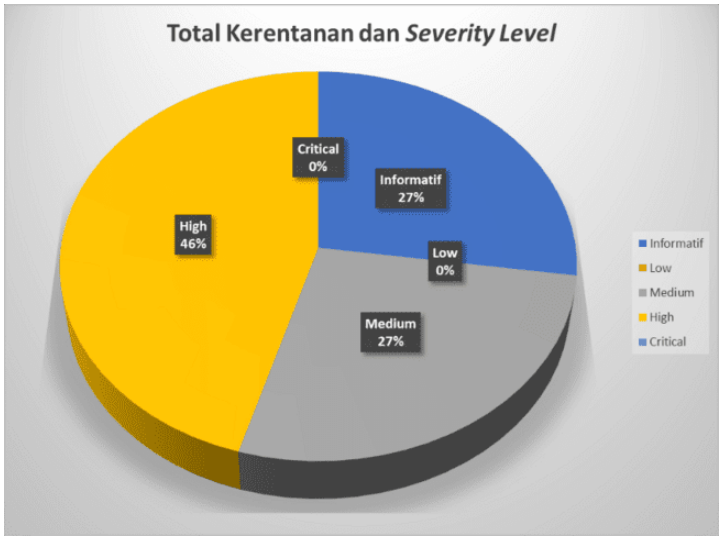
Gambar 15. Foto bersaam tim pengabdian dan tim Udacoding

4.2 Kendala dan Tantangan

Kendala dan tantangan yang dihadapi selama pelaksanaan kegiatan yaitu pelaksanaan penetration testing. Berkaitan dengan Non-disclosure Agreement yang telah disepakati bersama, server harus di-*backup* agar tidak menimbulkan kekacauan pada web server asli. Proses ini memakan waktu yang cukup lama, namun dapat dimanfaatkan oleh tim untuk latihan dan mempelajari lebih lanjut server yang akan diretas.

V. KESIMPULAN

Kegiatan pengabdian masyarakat Penetrasi Testing Aplikasi Website Udacoding telah berjalan dengan baik melalui serangkaian proses uji penetrasi yang dibagi menjadi 4 tahapan. Tingkat keamanan dan hasil kerentanan yang terdapat pada web Udacoding ini berhasil ditemukan dan diuji. Terdapat 10 kerentanan utama dengan beberapa severity level yang dihitung menggunakan kalkulasi CVSS 3.1 menggunakan beberapa alat pengujian seperti yang ditunjukkan pada Gambar 16.



Gambar 16. Total temuan kerentanan dan levelnya

Dari gambar 3, dapat dilihat bahwa jenis kerentanan yang paling dominan adalah terletak pada kerentanan dengan severity level high dimana jika dilihat dari kategori OWASP 2021 termasuk dalam kategori *broken access control, security misconfiguration* dan *injection*.

Berdasarkan temuan dan rekomendasi perbaikan keamanan yang diberikan, tim Udacoding dapat segera memperbaiki celah keamanan yang ditemukan. Prioritas perbaikan dapat dilakukan berdasarkan tingkat keparahan (severity level) yang telah diidentifikasi. Penerapan rekomendasi perbaikan yang diberikan oleh tim pengujian dapat membantu aplikasi web yang diuji maupun yang akan dikembangkan selanjutnya untuk terhindar dari segala bentuk serangan siber yang dapat menimbulkan kerugian di masa mendatang. Penyebaran kesadaran keamanan dalam berteknologi juga telah dilakukan pada saat presentasi hasil uji kepada para pegawai Udacoding dan diterima secara baik.

UCAPAN TERIMA KASIH

Ucapan terimakasih kami ucapkan kepada P3M Politeknik Negeri Batam atas dana dan hal-hal lainnya yang diberikan untuk memfasilitasi kegiatan pengabdian ini. Kepada seluruh anggota tim pengabdian baik dosen maupun anggota mahasiswa yang terlibat, dan juga kepada tim Udacoding yang telah memberikan kesempatan dan kerjasamanya yang baik selama proses pelaksanaan kegiatan pengabdian. Diharapkan dari kegiatan ini agar tim Udacoding agar terus mengembangkan teknologi informasi yang baik dan aman bagi seluruh entitas yang menggunakannya.

DAFTAR PUSTAKA

A. Alanda, D. Satria, M. I. Ardhana, A. A. Dahlan, & H. A. Mooduto. (2021). Web application penetration testing using SQL injection attack. *JOIV : International Journal on Informatics Visualization*, vol. 5, no. 3, p. 320, 2021. doi:10.30630/joiv.5.3.470.

Dewanto, A. P. (2018). *Penetration Testing Pada Domain uii.ac.id Menggunakan OWASP 10*. Yogyakarta: Universitas Islam Indonesia.

Dirgahayu, R. T., Prayudi, Yudi., Fajaryanto, Adi. (2015). *Penerapan Metode ISSAF dan OWASP versi 4 Untuk Uji Kerentanan Web Server*.

Fachri, F., Fadlil, A., & Riadi, I. (2021). Analisis Keamanan Webserver Menggunakan Penetration Test. *Jurnal Informatika*, Vol. 8 No. 2, 183-190.

Gunawan, Oman and Ferdiansyah, Doddy. (2022). *Penetration Testing Terhadap Website Universitas Pasundan Dengan Metode Zeto Entry Hacking (Studi Kasus: http://www.unpas.ac.id)*. Fakultas Teknik Unpas.

M. Hasibuan and A. M. Elhanafi (2022). Penetration testing Sistem Jaringan Komputer Menggunakan Kali Linux Untuk Mengetahui Kerentanan Keamanan server dengan metode black box. *Jurnal Teknik Informatika* Vol. 1, No. 4, 171–177.

Mushlih, M., Fitri, R., & Wardiah, I. (2019). Penetration Testing Tool Untuk Menguji Kerentanan Sql Injection Secara Otomatis Berbasis Web. *Prosiding SNRT (Seminar Nasional Riset Terapan).*

OWASP Top 10:2021, https://owasp.org/Top10/ (Diakses pada 2 Desember 2023).