INNOVATIVE: Journal Of Social Science Research
Volume 4 Nomor 5 Tahun 2024 Page 3629-3647
E-ISSN 2807-4238 and P-ISSN 2807-4246
Website: https://j-innovative.org/index.php/Innovative

Pengujian Keamanan *Website* dengan Metode *Penetration Testing* (Studi Kasus: Universitas Esa Unggul)

Ferby Septian[1]✉, Muhamad Hadi Arfian[2], Jefry Sunupurwa Asri[3], Budi Tjahjono[4]
Universitas Esa Unggul
Email: ferbyseptian78@gmail.com[1]✉

Abstrak

Perkembangan era digital di Indonesia telah membawa manfaat dan transformasi positif, namun juga menimbulkan tantangan keamanan terkait risiko peretasan dan kebocoran data. Keamanan website menjadi sebuah komponen penting yang tidak bisa dianggap remeh, sehingga website perpustakaan Universitas Esa Unggul memerlukan perlindungan maksimal terhadap ancaman keamanan yang terus berkembang. Penelitian ini bertujuan untuk mengidentifikasi dan mengatasi risiko keamanan melalui pengujian keamanan pada website perpustakaan Universitas Esa Unggul menggunakan metode penetration testing dengan pendekatan black-box, serta memanfaatkan OWASP Top 10 2021 sebagai acuan informasi kerentanan. Pengujian keamanan website berhasil dilakukan melalui beberapa tahapan penetration testing, yaitu reconnaissance, scanning, vulnerability assessment, exploitation, dan reporting. Hasil penelitian ini menunjukkan bahwa website perpustakaan Universitas Esa Unggul memiliki kerentanan yang tercantum dalam OWASP Top 10 2021, dengan 2 jenis kerentanan berisiko tinggi yaitu broken access control dan security misconfiguration, serta 1 kerentanan berisiko rendah yaitu cryptographic failures. Berdasarkan hasil temuan tersebut, rekomendasi perbaikan yang dapat diberikan adalah dengan melakukan konfigurasi ulang terhadap akses kontrol untuk mencegah akses yang tidak sah, menambahkan secure flag pada cookie guna memperkuat enkripsi, serta menerapkan security header untuk mencegah berbagai serangan cyber. Penelitian ini diharapkan dapat meningkatkan keamanan website perpustakaan Universitas Esa Unggul, serta dapat menjadi referensi dalam melakukan pengujian kemanan.

Kata Kunci: *Peretasan dan Kebocoran Data, Keamanan Website, Pengujian Keamanan, Penetration Testing, OWASP Top 10 2021*

Abstract

The development of the digital era in Indonesia has brought benefits and positive transformations, but it has also posed security challenges related to the risks of hacking and data breaches. Website security has become an important component that cannot be underestimated, so the Esa Unggul University library website requires maximum protection against ever-increasing security threats. This research aims to identify and address security risks through security testing on the website of Esa Unggul University Library using the penetration testing method with a black-box approach, as well as utilizing the OWASP Top 10 2021 as a reference for vulnerability information. The security testing of the website was successfully carried out through several stages of penetration testing, namely reconnaissance, scanning, vulnerability assessment, exploitation, and reporting. The results of this research indicate that the library website of Esa Unggul University has vulnerabilities listed in the OWASP Top 10 2021, with 2 types of high-risk vulnerabilities: broken access control and security misconfiguration, as well as 1 low-risk vulnerability: cryptographic failures. Based on these findings, the recommended improvements include reconfiguring access control to prevent unauthorized access, adding a secure flag to cookies to strengthen encryption, and implementing security headers to prevent various cyber attacks. This research is expected to enhance the security of the website of Esa Unggul University Library and serve as a reference for conducting security testing.

Keywords: *Hacking and Data Breaches, Website Security, Security Testing, Penetration Testing, OWASP Top 10 2021*

PENDAHULUAN

Indonesia saat ini telah memasuki perkembangan era digital yang membawa berbagai manfaat dan transformasi positif dalam berbagai aspek kehidupan manusia yang menciptakan peluang baru dalam komunikasi dan akses informasi. Perkembangan era digital terhadap kemajuan teknologi telah memainkan peran penting dalam mengubah perspektif dan gaya hidup masyarakat secara keseluruhan [1]. *Website* merupakan *platform* yang dipublikasikan di internet, maka dar itu harus dijaga keamanannya agar tetap terlindung dari ancaman serangan *hacker.* [2]. Keamanan *website* merupakan komponen penting yang tidak boleh diabaikan dalam melindungi integritas, kerahasiaan, dan ketersediaan data [3].

Gambar 1. Trafik Anomali Serangan Siber di Indonesia Tahun 2022
Sumber: www.idsirtii.or.id

Menurut laporan Badan Siber dan Sandi Negara (BSSN), pada tahun 2022 Indonesia mengalami 976.429.996 serangan siber, dengan 56,84 persen di antaranya merupakan serangan malware, yang diikuti oleh kebocoran data sebesar 14,75 persen dan serangan trojan sebesar 10,9 persen. Serangan lainnya juga mencakup 17,51 persen juga mengancam keamanan siber Indonesia [4]. Serangan oleh *hacker* atau *cracker* dari berbagai negara menimbulkan kerentanan signifikan, terutama dalam pengiriman informasi intelijen melalui dunia maya [5].

Gambar 2. *Website* Perpustakaan Universitas Esa Unggul
Sumber : https://xxx.xxx.ac.id

Universitas Esa Unggul, sebagai salah satu perguruan tinggi swasta terkemuka di Indonesia, memanfaatkan *website* untuk menyebarkan informasi dan menghubungkan civitas akademika. *Website* perpustakaan universitas ini menyediakan layanan seperti sirkulasi buku, bantuan referensi, akses sumber multimedia, serta formulir online untuk berbagai keperluan akademik. Dengan direktori umum, pencarian koleksi menjadi lebih mudah, mendukung sumber daya pendidikan dan pengalaman belajar. Dengan meningkatnya kejahatan siber, pengelolaan keamanan *website* kini menjadi aspek krusial dalam menjaga integritas, kerahasiaan, dan ketersediaan data. Agar *website* tetap

berfungsi sebagai sumber daya yang terpercaya dan aman, diperlukan pengujian keamanan melalui metode *Penetration Testing*, yang memanfaatkan klasifikasi kerentanan dari OWASP Top 10 2021.

METODE PENELITIAN

Identifikasi Masalah

Identifikasi masalah menjadi elemen penting yang perlu diteliti secara menyeluruh, dalam sebuah penelitian. Celah keamanan yang terdapat pada sebuah *Website* tentunya dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab merupakan salah satu masalah yang muncul. Hal ini menjadi ancaman serius bagi pemilik *website* dan pengguna yang mengaksesnya, karena rentan terhadap serangan *cyber* seperti peretasan, pencurian data sensitif, atau bahkan diambil alih oleh orang yang tidak bertanggung jawab. Selain itu, kompleksitas dan kerentanan sistem *website* yang terus berkembang juga menjadi tantangan tersendiri dalam mengidentifikasi dan mengatasi masalah keamanan tersebut.

Pengumpulan Data

Observasi

Dalam melakukan sebuah penelitian yang melibatkan pengujian keamanan, diperlukan observasi untuk mengamati tentang bagaimana alur proses yang berjalan dari *website* perpustakaan Universitas Esa Unggul serta *framework* yang digunakan. Proses observasi ini dapat membantu dalam mengumpulkan informasi relevan dan akurat, yang nantinya dapat menjadi landasan untuk tahap analisis keamanan yang diperlukan.

Wawancara

Dalam upaya memperoleh informasi serta pemahaman yang mendalam mengenai *website* perpustakaan Universitas Esa Unggul, dilakukan wawancara tidak terstruktur terhadap Pihak BTIK Universitas Esa Unggul, khususnya Kepala Bagian BTIK. Melalui wawancara ini, data yang diperoleh diharapkan dapat memberikan gambaran keamanan dan arsitektur mengenai *website* perpustakaan Universitas Esa Unggul, agar menjadi dasar untuk mengusulkan rekomendasi perbaikan yang dapat diterapkan guna mengoptimalkan keamanan *website*.

Studi Literatur

Selain observasi dan wawancara, penelitian ini juga didasarkan pada peninjauan literatur tentang penelitian serupa. Pada tahap studi literatur ini, teknik pengumpulan data

dilakukan dengan mengumpulkan informasi dari berbagai literatur yang relevan tentang pengujian keamanan *website* dan *penetration testing*. Sumber-sumber yang digunakan mencakup buku, jurnal ilmiah, dan sumber web terkait yang telah diuji keakuratannya.

Tahapan *Penetration Testing*

Dalam Penelitian ini, metode yang akan digunakan adalah Penetration Testing yang mencakup tahapan sebagai berikut:

Gambar 3. Metode *Penetration Testing*

1. *Reconnaissance*

   Pada proses *reconnaissance*, akan dilakukan pengumpulan informasi secara aktif dengan memanfaatkan berbagai tools seperti *Nslookup, Dig*, dan *Whatweb* untuk mengumpulkan informasi secara detail mengenai *website* perpustakaan Esa Unggul. Penggunaan tools ini bertujuan untuk mendapatkan informasi yang tepat dan pemahaman secara menyeluruh mengenai sistem.

2. *Scanning*

   Pada proses *scanning*, akan dilakukan menggunakan beberapa *tools* seperti *Nmap*, *Nikto* dan *Dirb* untuk mengidentifikasi potensi kerentanan pada sistem. Penggunaan *tools* ini bertujuan untuk memastikan bahwa semua aspek keamanan sistem diperiksa secara menyeluruh dan mendalam.

3. *Vulnerability Assessment*

   Pada tahap *Vulnerability Assessment* ini, setiap kerentanan yang ditemukan akan dianalisis dan diklasifikasikan berdasarkan tingkat keparahannya menggunakan *Common Vulnerability Scoring System* (CVSS) versi 3.1.

4. *Exploitation*

   Pada tahap e*xploitation*, eksploitasi akan dilakukan berdasarkan hasil Vulnerability Assessment, namun eksploitasi yang berpotensi merusak sistem secara sengaja tidak akan dilakukan. Keputusan ini diambil berdasarkan kesepakatan terhadap pihak BTIK, yang bertujuan untuk menjaga kelancaran operasional sistem selama proses pengujian berlangsung. Meskipun kerentanan telah diidentifikasi,

tindakan eksploitasi yang dapat mengganggu atau merusak integritas sistem dihindari sepenuhnya.

5. *Reporting*

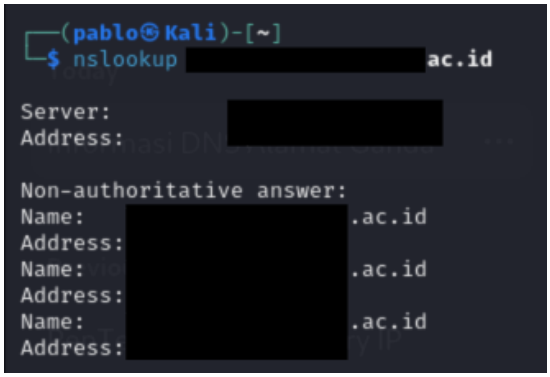
Pada tahap *reporting*, hasil pengujian keamanan disusun dalam laporan komprehensif yang mencakup rincian kerentanan, analisis keparahan, dampak potensial, serta rekomendasi perbaikan. Tujuan pelaporan ini adalah untuk memberikan dokumentasi yang jelas dalam membantu tim *developer* atau *administrator* sistem memperkuat keamanan *website* perpustakaan Esa Unggul.

HASIL DAN PEMBAHASAN

Reconnaissance

1. *Nslookup*

Dalam pencarian informasi terkait DNS menggunakan tools NsLookup, didapatkan hasil sebagai berikut:



Gambar 4. Hasil *Information Gathering* dengan tools *Nslookup*

Berdasarkan hasil Information gathering menggunakan tools NsLookup, terdapat 3 IP Address berbeda yang ditemukan yaitu ; xxx.xx.xx.127, xxx.xx.x.172, dan xxx.xx.x.172. "Non-authoritative Answer", menunjukkan bahwa informasi didapat dari cache DNS resolver yang berarti bukan dari Authoritative DNS server. DNS resolver menyimpan hasil pencarian DNS sebelumnya untuk mempersingkat waktu pencarian dan mengurangi beban pada Authoritative DNS server. Informasi yang diberikan masih dapat diandalkan, meskipun tidak diambil secara langsung dari sumber utamanya.

2. Dig

Dig *(Domain Information Groper)*, digunakan untuk mendapatkan informasi langsung dari *authoritative* DNS *server*. Untuk dapat menemukan informasi terkait *authoritative* DNS *server,* Dig mengirimkan *query* ke *server* DNS, lalu *server* akan

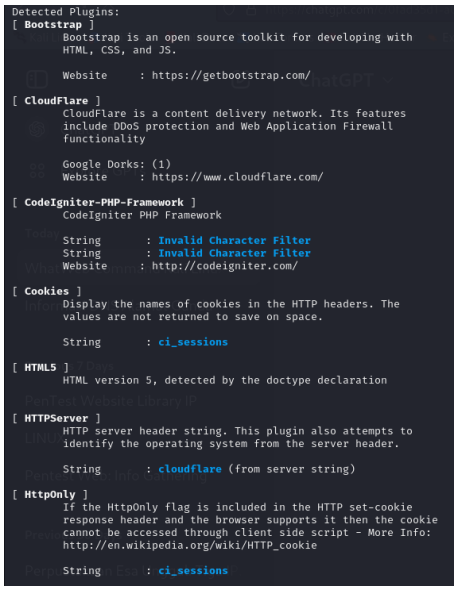
menerima respon yang berisikan informasi yang diminta.

Gambar 5. Hasil *Information Gathering dengan* tools *Dig*

Hasil *Information gathering* yang didapatkan menggunakan Dig, menunjukkan bahwa *request* DNS terhadap domain ini dijawab oleh *server* dengan status *"NOERROR"*, yang menandakan bahwa *request* berhasil diproses tanpa kesalahan dalam waktu 63 milidetik, sehingga didapatkan juga *Authoritative DNS server* dari domain xxx.xxx.ac.id yaitu "sid.ns.cloudflare.com", dengan informasi kontak administrator "dns@cloudflare.com". Selain itu ketiga *IP Address* yang terdapat pada domain xxx.xxx.ac.id ini, di-hosting oleh *Cloudflare* yang mengarah pada penggunaan layanan CDN *(Content Delivery Network)*. Cloudflare berfungsi sebagai *reverse proxy*, yang mengarahkan lalu lintas melalui jaringan global mereka untuk meningkatkan kinerja dan keamanan pada *website*.

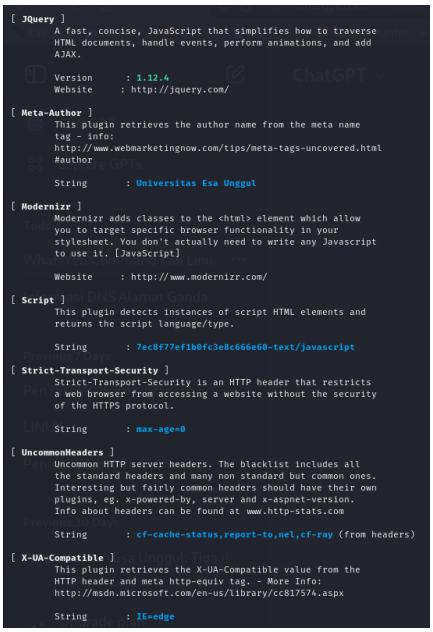
3. *Whatweb*

WhatWeb bekerja dengan mengirimkan permintaan HTTP terhadap *website* target dan menganalisis tanggapan untuk mengidentifikasi fitur dan teknologi yang digunakan. Maka dari itu, informasi yang diperoleh dari *Whatweb* sangat berguna untuk memahami arsitektur dari *website* yang sedang diuji.



Gambar 6. Hasil *Whatweb* 1

Hasil *Information Gathering* yang dilakukan menggunakan *tools WhatWeb* menunjukkan bahwa *website* ini menggunakan teknologi dan sistem keamanan yang canggih. *Website* ini menggunakan *Bootstrap* untuk pengembangan HTML, CSS, dan *JavaScrip*t, serta dilindungi oleh CloudFlare yang berfungsi mengatasi serangan DDoS dan menyediakan *Web Application Firewall* (WAF). *Framework* PHP yang digunakan adalah *CodeIgniter*, yang dilengkapi dengan deteksi string *'Invalid Character Filter'* untuk mencegah kesalahan, kerusakan data, atau serangan berbahaya seperti SQL *Injection* dan *Cross-Site Scripting* (XSS).



Gambar 7. Hasil *Whatweb* 2

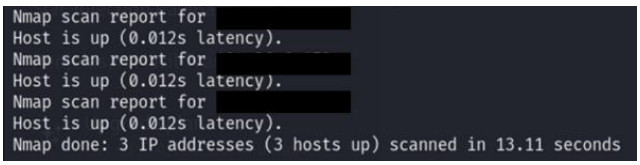
Cookie "ci_sessions", yang memiliki flag *"HttpOnly",* digunakan untuk mengelola sesi pengguna dan tidak dapat diakses melalui *scripting client-side*. Versi HTML yang digunakan adalah HTML5, yang dapat dikenali dari deklarasi *doctype-nya*. *Library JavaScript* yang digunakan adalah *Modernizr* dan *jQuery* versi 1.12.4. Header *HTTP* khusus seperti *cf-cache-status*, *report-to*, *nel*, dan *cf-ray* menunjukkan bahwa *website* ini menggunakan *Cloudflare* sebagai *Content Delivery Network* (CDN). Selain itu, protokol keamanan HTTP *Strict-Transport-Security* (HSTS) meningkatkan keamanan *website* dengan memastikan bahwa hanya protokol HTTPS yang dapat digunakan untuk mengaksesnya.

Scanning

1. *Nmap*

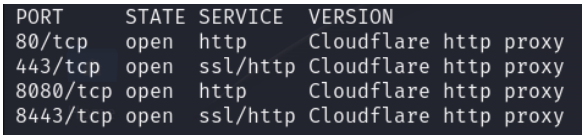
   Dengan Menggunakan *tools Nmap*, dilakukan *host scanning*. *Host scanning*

merupakan salah satu teknik dalam tahap scanning yang bertujuan untuk mengidentifikasi *host* yang aktif dalam sebuah jaringan dengan cara mengirimkan ICMP *Echo Request*.



Gambar 8. Hasil *Host Scanning* dengan Nmap

Host scanning dilakukan dengan menjalankan perintah tersebut, lalu perintah akan mengirimkan ping ke alamat IP *target* untuk memeriksa apakah *host* tersebut merespons dan aktif. Dapat dilihat pada Gambar 4.5, bahwa *Host scanning* berhasil dilakukan dan ketiga *host merespon* dengan waktu 13.11 detik. Setelah mendapatkan informasi mengenai *host* yang aktif, maka selanjutnya akan dilakukan pemindaian *port (port scanning)* untuk menemukan *port* yang terbuka pada. Proses ini dilakukan dengan cara mengirimkan paket data ke berbagai *port host* dan menunggu tanggapan host untuk menentukan apakah *port* tersebut terbuka, tertutup, atau *terfilter*. Proses ini sangat penting untuk menemukan titik masuk potensial untuk aktivitas jaringan yang sah maupun tidak sah.



Gambar 9. Hasil *Scanning Port dengan Nmap*

Berdasarkan hasil *scanning* yang dilakukan menggunakan *tools Nmap* terhadap domain xxx.xxx.ac.id, menunjukkan bahwa beberapa *port* penting ditemukan terbuka dan beroperasi sebagai layanan *proxy* Cloudflare, seperti *port* 80 (HTTP), *port* 443 (HTTPS), *port* 8080 (HTTP), dan *port* 8443 (HTTPS). Hal ini tidak menimbulkan kecurigaan terkait adanya kerentanan melalui *port-port* tersebut.

2. *Nikto*

Pada saat melakukan *scanning* dengan *tools Nikto*, *URL* target diisi dengan *URL* lengkap xxx.xxx.ac.id dan *port target* diatur pada *port* 443, yang merupakan *port* standar untuk protokol HTTPS. Pemilihan port 443 menekankan analisis pada keamanan komunikasi melalui protokol HTTPS.

Gambar 10. Hasil *Vulnerability Scanning* dengan *Nikto*

Setelah proses *scanning* selesai, ditemukan beberapa celah keamanan yang terdapat pada *website* xxx.xxx.ac.id sebagai berikut:

a. *The anti-clickjacking X-Frame-Options header is not present*
b. *The site uses TLS and the Strict-Transport-Security HTTP header is set with max-age=0*
c. *The X-Content-Type-Options header is not set*
d. *Cookie ci_sessions created without the secure flag*

Proses *scanning* yang telah dilakukan menggunakan *tools Nikto*, menunjukkan adanya beberapa celah keamanan. Langkah selanjutnya adalah melakukan analisis lebih mendalam untuk mengidentifikasi pada tahap *Vulnerability Assessment*.

Vulnerability Assessment

1. *Broken Access Control* (A01: 2021)

Berdasarkan hasil *scanning directory* yang dilakukan dengan *tools* Dirb, dicurigai terdapat beberapa kerentanan pada *URL* berikut:

a. *xxx.xxx.ac.id/git/index.html*
b. *xxx.xxx.ac.id/user*
c. *xxx.xxx.ac.id/tracer*
d. *xxx.xxx.ac.id/admin.auth.inc*
e. *xxx.xxx.ac.id/login/index*
f. *xxx.xxx.ac.id/phpmyadmin/changelog*

Url tersebut diklasifikasikan ke dalam jenis kerentanan *broken access control*. Jenis kerentanan ini terjadi karena sistem gagal membatasi akses pengguna terhadap sumber daya atau fungsi yang seharusnya tidak dimiliki. Untuk mengetahui *severity* dan *score* yang dimiliki oleh *broken access control* ini, dapat dilihat pada hasil berikut:

Gambar 11. CVSS *(Broken access control)*

Sumber: https://www.first.org/cvss/calculator/3.1

2. *Cryptographic Failures* (A02:2021)

Berdasarkan hasil *scanning* yang dilakukan dengan *tools* nikto, terdapat celah kerentanan yang teridentifikasi melalui "*Cookie ci_sessions created without the secure flag*". *Cookie "ci_sessions"* tidak memiliki *flag Secure*, sehingga *cookie* bisa dikirim melalui koneksi yang tidak aman (HTTP) untuk meningkatkan risiko pencurian *cookie*. Kerentanan ini dapat memungkinkan *threat actor* untuk mengarahkan pengguna ke *website* yang berbahaya dan menampilkan data yang tidak benar, sehingga dapat merusak kredibilitas *website*.

Gambar 12. CVSS *(Cookie Without Secure Flag Detected)*

Sumber: https://www.first.org/cvss/calculator/3.1

3. *Security Misconfiguration* (A05:2021)

Berdasarkan hasil scanning yang dilakukan menggunakan tools *Nikto*, menunjukkan bahwa terdapat kerentanan "*The anti-clickjacking X-Frame-Options header is not present*", *"The site uses TLS and the Strict*-Transport-Security *HTTP header is set with max-age=0",* dan "*The X-Content-Type-Options header is not set*". Ketiga kerentanan ini menunjukkan adanya kelemahan dalam konfigurasi keamanan *website*, yang dikenal sebagai *security misconfiguration*. Kategori ini mencakup kesalahan atau kelalaian dalam pengaturan keamanan yang seharusnya melindungi situs dari berbagai serangan, seperti *clickjacking*, *downgrade attack*, dan *MIME-type sniffing.*

Gambar 13. CVSS *(Security Misconfiguration)*

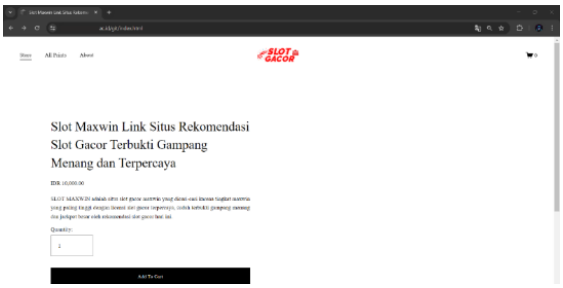
Sumber: https://www.first.org/cvss/calculator/3.1

Exploitation

Exploitation dilakukan menggunakan *tools Dirb* dengan teknik *bruteforce* dan hanya akan dilakukan terhadap jenis *vulnerability Broken access control*, untuk mengeksploitasi isi konten yang terdapat pada *website perpustakaan* esa unggul.

1. *Broken Access Control*

Pada saat mengakses *URL* : *xxx.xxx.ac.id/git/index.html*, tampilan halaman yang muncul adalah sebuah situs promosi judi *online* dengan judul "Slot *Maxwin Link* Situs Rekomendasi Slot Gacor Terbukti Gampang Menang dan Terpercaya."



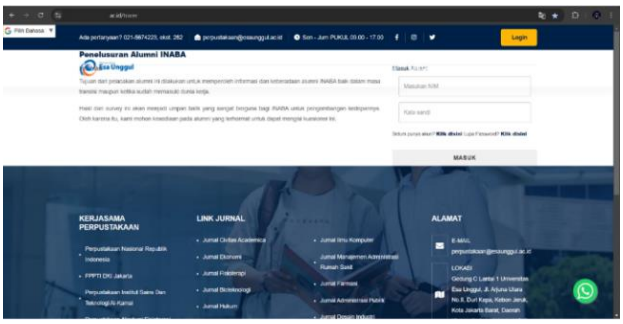
Gambar 14. Exploitation *Broken Access Control /git/*

Hal ini mengindikasikan bahwa *website xxx.xxx.ac.id* telah mengalami serangan dan terdapat penyisipan konten yang tidak sah. Serangan ini kemungkinan besar memanfaatkan kerentanan dalam kontrol akses atau kelemahan keamanan lainnya pada *web server* atau aplikasi yang di-hosting pada *website* tersebut.

Gambar 15. *Exploitation Broken Access Control User*

Pada saat mengakses *xxx.xxx.ac.id/user*, tampilan halaman yang muncul adalah promosi situs *judi* online dengan judul "*Slot Thailand* : Daftar Situs Slot *Online* Gacor Terbaru Hari Ini dan *Maxwin* Besar". Halaman ini menampilkan konten terkait perjudian online yang jelas tidak sesuai dengan tujuan dan konten asli dari *website* perpustakaan esa unggul. Hal ini mengindikasikan adanya kerentanan serius dalam kontrol akses dan

keamanan *website* tersebut, karena *url* ini dapat diakses oleh semua pengguna.



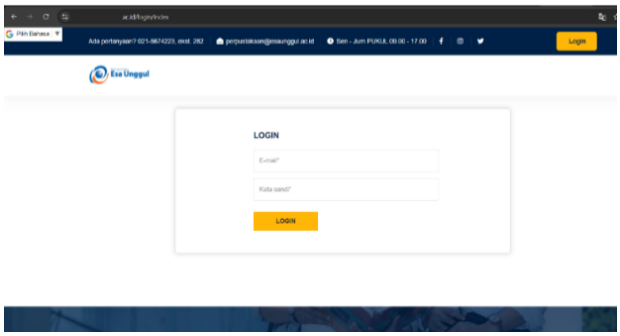
Gambar 16. *Exploitation Directory Tracer*

Halaman web xxx.xxx.ac.id/tracer yang terindikasi memiliki kerentanan Broken access control dapat dieksploitasi melalui beberapa bug. Salah satu bug ini, akan memungkinkan pengguna untuk mengakses halaman atau informasi sensitif tanpa perlu melakukan login. Bug lain memungkinkan privilege escalation, di mana pengguna dengan izin rendah dapat *mengakses* fungsi atau data administratif. Selain itu, manipulasi *Url* dan *Insecure Direct Object Reference* (IDOR) dapat memungkinkan pengguna untuk mengakses data atau objek yang bukan miliknya hanya dengan mengubah parameter dalam *Url*.

Gambar 17. *Exploitation Directory admin.auth.inc*

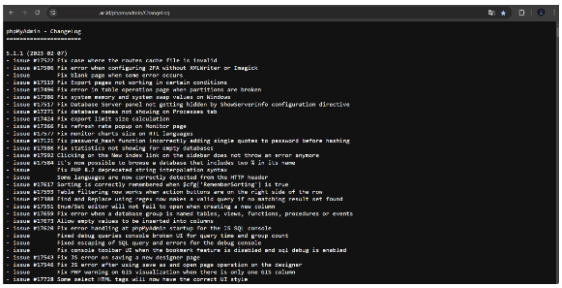
Pada saat mengakses halaman web xxx.xxx.ac.id/admin.auth.inc, pengguna diarahkan ke halaman awal selamat datang. Hal ini menunjukkan adanya beberapa bug pada halaman tersebut yang dikategorikan sebagai kerentanan Broken *access control*. Dalam kasus ini, meskipun pengguna diarahkan ke halaman awal, ada potensi bahwa kontrol akses tidak diterapkan dengan benar untuk mencegah akses ke halaman administrasi atau informasi sensitif lainnya tanpa autentikasi yang tepat.

Pada saat mengakses *URL* xxx.xxx.ac.id/login/index, halaman yang muncul adalah halaman login yang meminta untuk memasukkan *email* dan *password*.



Gambar 18. *Exploitation directory login/index*

Berdasarkan penilaian yang telah dilakukan pada tahap *vulnerability assessment*, *Url* ini dapat diakses oleh semua pengguna menunjukkan bahwa halaman ini kemungkinan merupakan pintu masuk bagi pengguna yang ingin mengakses fitur atau informasi yang dibatasi hanya untuk pengguna terautentikasi, seperti mahasiswa, staf, ataupun dosen.



Gambar 19. *Exploitation Directory Changelog*

Pada saat mengunjungi *directory* phpmyadmin/ChangeLog, berbagai informasi *penting* tentang pembaruan sistem, perbaikan kesalahan, dan perubahan konfigurasi dapat ditemukan. Informasi yang terdapat pada *web page* yaitu, perbaikan masalah seperti rute cache yang tidak valid, konfigurasi 2FA, penanganan kesalahan saat *startup*, dan berbagai perbaikan terkait fungsionalitas lainnya. Menampilkan *changelog* yang dapat diakses publik dapat memberikan banyak informasi berguna bagi *threat actor*. Maka dari itu, dengan mengamankan akses ke informasi ini sangat penting untuk menjaga keamanan keseluruhan sistem. Pastikan bahwa informasi sensitif seperti ini hanya dapat diakses oleh pihak yang berwenang dan dengan cara yang aman.

Reporting

Dari hasil pengujian yang telah dilakukan menggunakan metode *penetration testing,* ditemukan bahwa *website* perpustakaan Universitas Esa Unggul memiliki tiga kerentanan utama: *Broken Access Control, Cryptographic Failures,* dan *Security Misconfiguration*. Hasil pengujian ini telah disusun dalam bentuk tabel yang memuat informasi mengenai jenis kerentanan, deskripsi singkat, tingkat keparahan serta rekomendasi perbaikan, yang

dapat dilihat sebagai berikut:

Tabel 1. Reporting Hasil Penetration Testing

Kategori Kerentanan	Deskripsi	*Impact*	*Severity/ Score*
(A01 : 2021) *BrokenAccess Control*	a. xxx.xxx.ac.id/git/index.html b. xxx.xxx.ac.id/user c. xxx.xxx.ac.id/tracer d. xxx.xxx.ac.id/admin.auth.inc e. xxx.xxx.ac.id/login/index f. xxx.xxx.ac.id/phpmyadmin/changelog	Dapat mengakibatkan kebocoran data,sehingga rentan terhadap Serangan SQL Injection, Cross-site scripting (XSS).	*High*/ 8.8

Rekomendasi Perbaikan :

1. Akses situs *Cloudflare* dan masuk ke *dashboard*.
2. Login dan pilih *domain* yang ingin dikonfigurasi.
3. Klik tab *"Rules"* pada *dashboard*.
4. Pilih *"Page Rules"* dan klik *"Create Page Rule"*.
5. Masukkan URL yang ingin dibatasi pada *"If the URL matches"*.
6. Pilih *"Forwarding URL"* untuk mengarahkan atau "*Return a 403 Forbidden"* untuk memblokir.
7. Atur "Status Code" menjadi "302" (Temporary) atau "301" (Permanent).
8. Masukkan URL tujuan di kolom *"Destination URL"*.
9. Klik *"Save"* atau *"Deploy"* untuk menyimpan dan menerapkan aturan.

Tabel 2. Hasil reporting penetration testing 2

Kategori Kerentanan	Deskripsi	*Impact*	*Severity/ Score*
(A02 : 2021) Cryptographic Failures	*Cookie ci_sessions created without the secure flag*	Rentan terhadap serangan Man-in-the-Middle	Low/3.1

Rekomendasi Perbaikan :

1. Akses situs *Cloudflare* dan masuk ke *dashboard*.
2. login dan pilih *domain* yang ingin dikonfigurasi.
3. Klik tab *"Rules"* pada *dashboard*, lalu pilih *"Transform Rules"*.
4. Klik *"Create Transform Rule"*.
5. Pilih *Set-Cookie* sebagai field, dan tetapkan kondisi untuk cookie ci_sessions.
6. Atur *action* untuk menambahkan ; *"Secure"* pada cookie jika belum ada.
7. Klik "Save" atau *"Deploy"* untuk menyimpan dan menerapkan aturan.

Tabel 3. Hasil Reporting Penetration Testing 3

Kategori Kerentanan	Deskripsi	*Impact*	*Severity/ Score*
(A05 : 2021) Security Misconfiguration	*a) The anti-clickjacking X-Frame-Options header is not present* *b) HTTP header is set with max-age=0* *c) The X-Content-Type-Options header is not set*	Rentan terhadap serangan *clickjacking*, *downgrade attack*, *Cross-site scripting* dan *MIME-type sniffing*	High/7.8

Rekomendasi Perbaikan :

a) *The anti-clickjacking X-Frame-Options header is not present* :

1. Akses situs *Cloudflare* dan masuk ke dashboard.
2. login dan pilih *domain* yang ingin dikonfigurasi.
3. Pilih tab *"Rules"*, lalu Klik *"Transform Rules"* atau *"Page Rules"*.
4. Klik *"Create Rule"* atau *"Add Rule"*, masukkan URL yang sesuai pada *"If the URL matches"*.
5. Pilih *"Rewrite HTTP Headers"* atau *"Modify Response Headers"*.
6. Tambahkan Nilai *header* "DENY" atau "SAMEORIGIN pada "X-Frame-Options"
7. Klik *"Save"* atau *"Deploy"* untuk menyimpan dan menerapkan aturan.

b) *HTTP header is set with max-age=0* :

1. Akses situs *Cloudflare* dan masuk ke *dashboard.*
2. *Login* dan pilih *domain* yang ingin dikonfigurasi.
3. Pilih *tab* "SSL/TLS" di *dashboard Cloudflare*.
4. Pilih *sub-tab "Edge Certificates"*, lalu *Scroll* ke bawah hingga menemukan bagian "HTTP Strict Transport Security (HSTS)". Klik *"Enable HSTS"* jika belum diaktifkan.
5. *Setting max-age* menjadi *"Strict-Transport-Security: max-age*=31536000".
6. Pilih opsi "Include Subdomains" untuk mengamankan semua subdomain dengan HSTS. Centang opsi *"Preload"* untuk mendaftarkan situs ke daftar *preload* HSTS *global*.
7. Klik *"Save"* atau *"Deploy"* untuk menyimpan dan menerapkan aturan.

c) *The X-Content-Type-Options header is not set* :

1. Akses situs Cloudflare dan masuk ke dashboard.
2. Login dan pilih domain yang ingin dikonfigurasi.
3. Pilih tab "Rules" di dashboard Cloudflare, lalu pilih "Transform Rules" atau "Page Rules".
4. Klik "Create Rule" atau "Add Rule", lalu tambahkan aturan yang mencakup seluruh situs,

misalnya dengan URL "xxx.ac.id".

5. Di bagian *"Then"* atau *"Settings"*, pilih *"Rewrite HTTP Headers"* atau *"Modify Response Headers"*. Tambahkan nilai *"nosniff"* pada *header* : *X-Content-Type-Options*.
6. Klik *"Save"* atau *"Deploy"* untuk menyimpan dan menerapkan aturan.

SIMPULAN

Saran dalam penelitian ini dibagi menjadi dua bagian utama untuk memberikan arahan yang jelas bagi pihak terkait dan penelitian lanjutan:

1. Untuk BTIK Universitas Esa Unggul

   Segera terapkan langkah mitigasi yang diidentifikasi, seperti memperbaiki kontrol akses, menambahkan *secure flag* pada *cookies*, dan konfigurasi *header* keamanan. Lakukan audit keamanan rutin, perbarui sistem sesuai standar terbaru.
2. Untuk Peneliti Selanjutnya

   Peneliti selanjutnya disarankan untuk lebih mendalami aspek-aspek keamanan lain yang belum dibahas secara detail dalam penelitian ini. Selain itu, pengembangan metodologi pengujian dengan menggunakan *tools* yang lebih canggih juga dapat dilakukan untuk mendapatkan hasil yang lebih komprehensif.

DAFTAR PUSTAKA

R. B, I. P, S. S, and T. T. DS, "Globalisasi Pendidikan Berbasis Teknologi Di Indonesia," *Pros. Semin. Nas. MIPATI*, vol. 1, no. 1, pp. 71–84, 2021, [Online]. Available: https://jurnal.stkipbjm.ac.id/index.php/mipati/article/view/1528

H. Hermanto and H. Haeruddin, "Peningkatan Sistem Keamanan *Website* Menggunakan Metode OWASP," *J. Ilmu Komput. dan Bisnis*, vol. 13, no. 1, pp. 94–104, 2022, doi: 10.47927/jikb.v13i1.277.

I. P. A. E. P. I Dewa Gede Govindha Dharmawangsaa , Gusti Made Arya Sasmitaa, "Penetration Testing Berbasis OWASP Testing Guide Versi 4.2 (Studi Kasus: X *Website*) I Dewa Gede Govindha Dharmawangsa a1 , Gusti Made Arya Sasmita a2 , I Putu Agus Eka Pratama b3," *J. Ilm. Teknol. dan Komput.*, vol. 4, 2023.

S. S. Taufik Nurhidayat *et al.*, "Lanskap Keamanan Siber Indonesia," 2022. [Online]. Available: https://www.idsirtii.or.id/halaman/tentang/laporan-hasil-monitoring.html

E. Soesanto, A. Romadhon, B. D. Mardika, and M. F. Setiawan, "Analisis dan Peningkatan Keamanan Cyber: Studi Kasus Ancaman danSolusi dalam Lingkungan Digital Untuk

Mengamankan Objek Vital dan File," *SAMMAJIVA J. Penelit. Bisnis dan Manaj.*, vol. 1, no. 2, pp. 172–191, 2023.

W. Rahmadhani, "PEMANFAATAN *WEBSITE* SEBAGAI BENTUK DIGITALISASI PELAYANAN ISLAM Wulan Ayu Rahmadhani , David King , Embarina Melviyani Br Ginting , Fernandes Institut Pemerintahan Dalam Negeri A . PENDAHULUAN Pada era society 5 . 0 perkembangan teknologi sangat pesat , p," *Edukasi Islam. J. Pendidik. Islam*, vol. 11, pp. 1167–1182, 2022, doi: 10.30868/ei.v11i01.2979.

J. A. S. Siregar and K. Handoko, "Jurnal Comasie Jurnal Comasie," *J. Comasie*, vol. 6, no. 2, pp. 40–51, 2021, [Online]. Available: http://ejournal.upbatam.ac.id/index.php/comasiejournal%0AJurnal Comasie ISSN (Online) 2715-6265%0APERANCANGAN

M. B. Yel and M. K. M. Nasution, "Keamanan Informasi Data Pribadi Pada Media Sosial," *J. Inform. Kaputama*, vol. 6, no. 1, pp. 92–101, 2022, doi: 10.59697/jik.v6i1.144.

H. One, "What Is Security Testing?" https://www.hackerone.com/knowledge-center/what-security-testing (accessed Nov. 03, 2023).

R. Ashar, "Analisis Keamanan Open *Website* Menggunakan Metode OWASP dan ISSAF," *J. Inf. dan Teknol.*, vol. 4, no. 4, pp. 211–218, 2022, doi: 10.37034/jsisfotek.v4i4.233.

AWS, *Pilar Keamanan*. 2023.

G. A. Utomo, "Ethical Hacking," *Cyber Secur. dan Forensik Digit.*, vol. 2, no. 1, pp. 8–15, 2019, doi: 10.14421/csecurity.2019.2.1.1418.

C. A. Indonesia, "Mengenal Tentang Penetration Testing," 2023. https://www.cyberacademy.id/blog/mengenal-tentang-penetration-testing (accessed Nov. 02, 2023).

ITG.ID, "Penetration Testing Menyempurnakan Program Keamanan Informasi," 2023.

IBM, "Apa saja jenis serangan siber yang umum?" https://www.ibm.com/id-id/topics/cyber-attack (accessed Dec. 02, 2023).

Y. Kinza, "Penetration testing," 2022. https://www.techtarget.com/searchsecurity/definition/penetration-testing (accessed Nov. 01, 2023).

OWASP, "About the OWASP Foundation." https://owasp.org/about/ (accessed Nov. 01, 2023).

A. Burton, "Who are OWASP?," *2020*. https://privatekey.dev/who-are-owasp/ (accessed Nov. 02, 2023).

S. A. Robbani, "Analisis Kerentanan Keamanan Aplikasi Manajemen Aset Berbasis Web Menggunakan Metode OWASP (Open Web Application Security Project) Studi Kasus PT. XYZ," *Academia.Edu*, 2022, [Online]. Available:

https://www.academia.edu/download/60637761/TugasAkhir_Metpen_TI01_0110217055_AhmadFathanSyakir20190918-1361-1a1985x.pdf

g0tmi1k, "What is Kali Linux?," *Kali.org*, 2023. https://www.kali.org/docs/introduction/what-is-kali-linux/ (accessed Mar. 01, 2024).

TechMindXperts, "Exploring WhatWeb: A Versatile Tool for Web Reconnaissance and Vulnerability Scanning," *Medium*, 2023. https://medium.com/@techmindxperts/exploring-whatweb-a-versatile-tool-for-web-reconnaissance-and-vulnerability scanning-7293c43483f#:~:text=WhatWeb is a web reconnaissance,technologies that are being used. (accessed Mar. 01, 2024).

Tech Target, "What is Nslookup?," 2023. https://www.techtarget.com/searchnetworking/definition/nslookup (accessed Jan. 03, 2024).

Hazel Virdó and dbrian, "How to Retrieve DNS Information Using Dig," *Digital Ocean*, 2024. https://www.digitalocean.com/community/tutorials/how-to-retrieve-dns-information-using-dig (accessed Jan. 04, 2024).

Nmap.org, "Chapter 15. Nmap Reference Guide." https://nmap.org/book/man.html (accessed Dec. 30, 2023).

E. Litchner, "What is Dirb?," *2022*. https://zerodayhacker.com/what-is-dirb/ (accessed Jan. 01, 2024).

geeksforgeeks.org, "What is Nikto and it's usages ?" https://www.geeksforgeeks.org/what-is-nikto-and-its-usages/?ref=header_search (accessed Dec. 31, 2023).