**Journal of Informatics and Computer Science Vol. 11 No. 2 Oktober 2025**
Universitas Ubudiyah Indonesia
e-ISSN : 2615-5346

# PENGUJIAN KEAMANAN WEBSITE TERHADAP SERANGAN *DEFACE* DAN *REDIRECT INJECTION* MELALUI SIMULASI DENGAN *OWASP ZAP* (STUDI KASUS: WEBSITE UNIVERSITAS UBUDIYAH INDONESIA)

# *WEBSITE SECURITY TESTING AGAINST DEFACE AND REDIRECT INJECTION ATTACKS THROUGH SIMULATION USING OWASP ZAP (CASE STUDY: UNIVERSITAS UBUDIYAH INDONESIA WEBSITE)*

**Hamid Tahalli[1], Rizka Albar[2], Mahendar Dwi Payana[3], M Bayu Wibawa[4]**
[1,3,4,]Jurusan Informatika, [2]Sistem informasi Fakultas Sains dan Teknologi, Universitas Ubudiyah Indonesia, Banda Aceh
E-mail : [1]hamidtahalli66@gmail.com,[2]albar@uui.ac.id, [3]mahendar@uui.ac.id, [4]mbayuw@uui.ac.id

Abstrak - Penelitian ini bertujuan untuk mengevaluasi tingkat keamanan website resmi Universitas Ubudiyah Indonesia terhadap potensi serangan *deface* dan *redirect injection* yang semakin marak terjadi pada aplikasi web institusi pendidikan. Pengujian dilakukan menggunakan tools OWASP ZAP *(Zed Attack Proxy )* yang mampu melakukan scanning pasif dan aktif, termasuk teknik *fuzzing*, untuk mengidentifikasi potensi kerentanan. Target pengujian mencakup domain utama (www.uui.ac.id) dan beberapa subdomain seperti sipenmaru.uui.ac.id, rpl.uui.ac.id, dan daa.uui.ac.id. Hasil pengujian menunjukkan bahwa www.uui.ac.id memiliki konfigurasi *cookie* yang tidak aman (*Passive Scanning*, risiko sedang). Subdomain sipenmaru.uui.ac.id rentan terhadap *open redirect* (*redirect injection* , risiko tinggi), sedangkan rpl.uui.ac.id mengandung celah XSS (*active scanning*, risiko tinggi) dan memungkinkan pengalihan ke situs slot online (*redirect injection* , risiko tinggi). Selain itu, daa.uui.ac.id merespons dengan error 500 saat menerima *input* acak (*fuzzing*, risiko sedang). Kerentanan ini berisiko dimanfaatkan untuk merusak tampilan situs, mencuri informasi pengguna, hingga mengarahkan pengguna ke situs berbahaya. Penelitian ini merekomendasikan penerapan validasi *input* yang ketat, pengaturan *cookie* yang aman, audit keamanan rutin, serta peningkatan pemahaman pengembang terhadap praktik *secure coding* sebagai langkah mitigasi.

**Kata Kunci :** Keamanan Website, OWASP ZAP, *Redirect injection* , XSS, *Fuzzing*, Universitas Ubudiyah Indonesia

*Abstract - This study aims to evaluate the security level of the official website of Universitas Ubudiyah Indonesia against potential deface and redirect injection attacks, which increasingly target web applications in educational institutions. The testing was conducted using OWASP ZAP (Zed Attack Proxy ) , which is capable of both passive and active scanning, including fuzzing techniques, to identify potential vulnerabilities. The test targeted the main domain (www.uui.ac.id) and several subdomains such as sipenmaru.uui.ac.id, rpl.uui.ac.id, and daa.uui.ac.id. The results revealed that www.uui.ac.id uses insecure cookie configurations (Passive Scanning, medium risk). The sipenmaru.uui.ac.id subdomain is vulnerable to open redirect (redirect injection , high risk), while rpl.uui.ac.id contains XSS vulnerabilities (active scanning, high risk) and also enables redirection to online gambling websites (redirect injection , high risk). In addition, daa.uui.ac.id returned a 500 error upon receiving random input (fuzzing, medium risk). These vulnerabilities pose significant risks, including website defacement, user data theft, and redirection to malicious websites. The study recommends implementing strict input validation, secure cookie configurations, regular security audits, and enhancing developers' understanding of secure coding practices as mitigation strategies.*

***Keywords: Website Security, OWASP ZAP, Redirect injection , XSS, Fuzzing, Universitas Ubudiyah Indonesia***

## I. PENDAHULUAN

Keamanan website menjadi aspek yang sangat penting di era digital saat ini, mengingat semakin banyaknya serangan siber yang mengancam berbagai sistem online. Salah satu ancaman yang sering terjadi adalah *deface* dan *redirect injection* , di mana peretas mengubah tampilan website atau mengarahkan pengguna ke situs lain tanpa izin. Fenomena terbaru yang banyak ditemukan adalah perubahan tampilan website akibat serangan peretas, yang menyebabkan pengguna yang mencari informasi di Google justru diarahkan ke halaman yang menampilkan iklan situs slot gacor atau konten ilegal lainnya. Serangan ini tidak hanya merugikan pemilik website, tetapi juga menurunkan kredibilitas dan keamanan bagi penggunanya.

Universitas Ubudiyah Indonesia (UUI) merupakan salah satu institusi pendidikan tinggi yang memiliki website resmi sebagai pusat informasi dan layanan akademik bagi mahasiswa, dosen, serta masyarakat umum. Website ini berfungsi untuk menyediakan informasi akademik, pendaftaran mahasiswa baru, pengumuman, dan berbagai sistem pendukung pembelajaran. Dengan peran yang begitu penting, keamanan website UUI harus menjadi prioritas utama agar informasi yang disediakan tetap terpercaya dan terlindungi dari ancaman serangan siber yang dapat mengganggu layanan akademik dan operasional universitas.

Namun, seperti banyak website lain, website UUI juga berpotensi menghadapi berbagai ancaman keamanan, termasuk serangan *deface* dan *redirect*

*injection* . Salah satu permasalahan yang semakin sering terjadi adalah perubahan tampilan website yang secara tiba-tiba menampilkan iklan atau mengarahkan pengguna ke situs pihak ketiga yang tidak relevan. Untuk mengidentifikasi dan mengatasi permasalahan ini, penelitian ini akan menggunakan *OWASP ZAP (Zed Attack Proxy )* sebagai alat untuk melakukan pengujian keamanan. Metode yang digunakan mencakup *Passive Scanning*, *active scanning*, dan *fuzzing* guna mendeteksi potensi celah keamanan yang dapat dimanfaatkan oleh peretas.

Melalui penelitian ini, diharapkan dapat diperoleh gambaran mengenai tingkat keamanan website UUI serta potensi kelemahan yang dapat menyebabkan serangan *deface* dan *redirect injection* . Hasil pengujian ini juga akan dianalisis untuk memberikan rekomendasi perbaikan yang bertujuan meningkatkan ketahanan website terhadap ancaman *siber*. Dengan adanya mitigasi yang tepat, diharapkan website UUI dapat lebih aman, mencegah perubahan tampilan yang tidak diinginkan, serta terhindar dari risiko penyalahgunaan oleh pihak yang tidak bertanggung jawab.

## II. STUDI PUSTAKA

### A. Universitas Ubudiyah Indonesia

Universitas Ubudiyah Indonesia salah satu perguruan tinggi swasta terbaik di Aceh yang pertama sekali didirikan pada tahun 2004 oleh dua pendiri Yayasan Ubudiyah Indonesia, yaitu Drs Tarmizi Ayus MM dan Dra Budiah. Pada awal pendirian, Ubudiyah masih berstatus sebagai Sekolah Tinggi Ilmu Kesehatan budiyah yang berlokasi di Lamnyong. Pada tahun 2007, Yayasan Ubudiyah juga mendirikan Sekolah Tinggi Manajemen Informatika dan Komputer (STMIK) (Ikhlasul Amal, 2024).


Gambar 1. Universitas Ubudiyah Indonesia

Sebagai salah satu kampus terbaik Aceh, Univiersitas Ubudiyah Indonesia (UUI) yang mempunyai program-program studi terbaik dengan akreditasi B untuk jurusan-jurusan (program studi) favorit seperti jurusan-jurusan di Fakultas Sains dan Teknologi (FST) untuk jurusan S-1 Informatika dan S-1 Sistem Informasi yang sudah terakreditasi B. Untuk Fakultas Ilmu Kesehatan (FIKES) dengan jurusan/ program studi S-1 Farmasi, D-III kebidanan, D-IV Kebidanan dan S-1 Kesehatan Masyarakat yang sudah terkareditasi B. untuk jurusan-jurusan (program studi) lain nya yang sudah terkareditasi B juga terdapat pada Fakultas Sosial Sains dan Ilmu Pendidikan (FSSIP) . Selain terdapat beberapa prodi di Universitas Ubudiyah Indonesia juga ada beberapa Jabatan pimpinan di bawah Rektor seperti Warek 1, 2 dan 3 dan juga terdapat pimpinan Direktorat yang di sebut Direktur seperti salah satunya yaitu Direktorat Penjaminan Mutu, Pemeringkatan dan Akreditasi yang disingkat dengan (DPMPA) (Ikhlasul Amal, 2024).

### B. Direktorat *Cyber Development Center Dan Media* (DCDCM)

Sesuai dengan tuntutan visi Universitas Ubudiyah Indonesia Menjadi "*World Class University*" maka dalam menjawab tantangan tersebut terkait dengan pengembangan teknologi, pimpinan Universitas Ubudiyah Indonesia mendirikan sebuah unit *Information and communication technologies* (ICT) didalam bagian Direktorat *Cyber Development Center Dan Media* yang disingkat (DCDCM) UUI untuk melaksanakan pengolalaan dan pengembangan Teknologi Informasi dan Komunikasi (TIK) di Universitas Ubudiyah Indonesia dalam menunjang pelaksanaan kegiatan dalam bidang pendidikan, penelitian dan pengabdian masyarakat atau dengan kata lain penunjang pengelolaan dan penyelenggaraan program akademik di Universitas. Seiring dengan perkembangan teknologi informasi dan komunikasi yang semakin pesat dewasa ini, keberadaan ICT UUI dituntut untuk dapat menempatkan diri pada posisi terdepan dalam pengembangan teknologi. Namun dalam pemamfaatan Perkembangan Teknologi Sistem Informasi dalam hal ini banyaknya Sistem Informasi Yang sudah di rancang sehingga sudah hampir mencapai 100 Sistem Informasi untuk mempermudah dalam hal kinerja Civitas Akademika Universitas Ubudiyah Indonesia (Ikhlasul Amal, 2024).

### C. Keamanan Data dalam Sistem Informasi Manajemen

Keamanan data dalam sistem informasi manajemen adalah upaya untuk melindungi, mengamankan aset informasi dari ancaman yang mungkin akan timbul yang dapat membahayakan kerahasiaan, ketersediaan, dan integritas semua aset informasi perusahaan, bukan hanya perangkat keras dan lunak, tetapi juga data sensitif yang disimpan di dalamnya Keamanan data dalam sistem informasi manajemen meliputi kebijakan, prosedur, proses, dan aktivitas untuk melindungi informasi dari berbagai jenis ancaman seperti pencurian data, penggunaan sistem secara ilegal, penghancuran data secara ilegal, modifikasi, akses tidak sah, dan kerusakan terhadap system (Agung Wijoyo, Dkk. 2023).

Untuk meningkatkan keamanan data dalam sistem informasi manajemen, perusahaan dapat menerapkan strategi perlindungan seperti menggunakan langkah-langkah dan alat keamanan siber untuk melindungi data sensitif dari akses yang tidak sah, menerapkan kerangka kerja keamanan siber yang komprehensif, menerapkan enkripsi dan praktik keamanan lainnya untuk melindungi data pribadi, mengimplementasikan regulasi perlindungan data pribadi, dan menjaga keberlangsungan bisnis dengan menjaga keamanan data (Agung Wijoyo, Dkk. 2023).

## D. Pentingnya Keamanan Sistem Informasi Manajemen

Kemampuan untuk mengakses dan menyediakan informasi secara cepat dan akurat menjadi sangat essensial bagi suatu organisasi, baik yang berupa organisasi komersial (perusahaan), perguruan tinggi, lembaga pemerintahan, maupun individual (pribadi) (Agung Wijoyo, Dkk. 2023).

Keamanan informasi menggambarkan usaha untuk melindungi komputer dan non peralatan komputer, fasilitas,data,dan informasi dari penyalahgunaan oleh orang yang tidak bertanggungjawab. Keamanan informasi dimaksudkan untuk mencapai kerahasiaan, ketersediaan, dan integritas di dalam sumber daya informasi dalam suatu Perusahaan (Agung Wijoyo, Dkk. 2023).

Jatuhnya informasi ke tangan pihak lain dapat menimbulkan kerugian bagi pemilik informasi. Keamanan informasi dimaksudkan untuk mencapai tiga sasaran utama yaitu:

1. Melindungi data dan informasi perusahaan dari penyingkapan orang- orang yang tidak berhak. Inti utama dari aspek kerahasiaan adalah usaha untuk menjaga informasi dari orang- orang yang tidak berhak mengakses. Privacy lebih kearah data-data yang sifatnya privat. Serangan terhadap aspek privacy misalnya usaha untuk melakukan penyadapan. Usaha-usaha yang dapat dilakukan untuk meningkatkan privacy adalah dengan menggunakan teknologi kriptografi. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti keabsahan, integritas data, serta autentikasi data.
2. Ketersediaan. Aspek ini berhubungan dengan metode untuk menyatakan bahwa informasi benar-benar asli, atau orang yang mengakses atau memberikan informasi adalah betul- betul orang yang dimaksud. Masalah pertama untuk membuktikan keaslian dokumen dapat dilakukan dengan teknologi watermarking dan digital signature.Watermarking juga dapat digunakan untuk menjaga intelektual property, yaitu dengan menandatangani dokumen atau hasil karya pembuat. Masalah kedua biasanya berhubungan dengan akses control, yaitu berkaitan dengan pembatasan orang-orang yang dapat mengakses informasi. Dalam hal ini pengguna harus menunjukkan bahwa memang dia adalah pengguna yang sah atau yang berhak menggunakannya.
3. Aspek ini menekankan bahwa informasi tidak boleh diubah tanpa seijin pemilik informasi. Adanya virus, trojan horse, atau pemakai lain yang mengubah informasi tanpa izin. Sistem informasi perlu menyediakan representasi yang akurat dari sistem fisik yang direpresentasikan.

Sepuluh Cara Menjaga Keamanan Sistem IT, sebagai berikut ini:

1. Protect with passwords. Semua akses ke jaringan maupun data, sangat sensitif dan harus dijaga dengan nama pengguna dan kata kunci yang unik. Sandi yang kuat berisi angka, huruf dan simbol.
2. Design safe systems. Hilangkan akses yang tidak perlu ke hardware maupun software Anda, dan batasi hak akses pengguna hanya untuk peralatan dan program yang dibutuhkan saja.
3. Conduct screening and background checks. Melakukan skrining dan pemeriksaan latar belakang pada karyawan perlu dilakukan.
4. Provide basic training. Pelanggaran keamanan yang tak terhitung jumlahnya kerap terjadi sebagai akibat kesalahan dan kecerobohan manusia.
5. Avoid unknown email attachements. Jangan pernah mengklik lampiran email yang tidak dikenal, yang kemungkinan bisa berisi virus komputer.
6. Hang up and call back. Jika Anda menerima panggilan dari orang yang tidak dikenal yang tiba-tiba ingin memberikan hadiah dan berpura-pura hadiah itu diberikan oleh perwakilan dari bank atau mitra lainnya, segera akhiri panggilan yang tidak dikenal tersebut.
7. Think before clicking. Untuk menghindari penipuan yang terjadi melalui email yang mempertimbangkannya kembali agar Anda tidak terdorong ke sebuah situs web palsu yang mendorong calon korban untuk memasukkan data mereka sendiri.
8. Use a virus scanner, and keep all software up-to-date. Menjaga perangkat lunak agar terus up-to-datejuga mampu mencegah virus masuk dan membuat keamanan sistem IT terjaga.
9. Keep sensitive data out of the cloud. Cloud computingmenawarkan banyak manfaat dan penghematan biaya kepada bisnis.
10. Stay paranoid. Jangan pernah meninggalkan laporan yang bersifat penting dan sensitif di meja Anda.

## E. Risiko Keamanan Data dalam Sistem Informasi Manajemen

1. Risiko Pelanggaran Data
   Salah satu risiko terbesar yang dihadapi organisasi dalam SIM adalah pelanggaran data. Pelanggaran data terjadi ketika data sensitif seperti informasi pelanggan, informasi keuangan, atau data pribadi dicuri atau diakses oleh pihak yang tidak berwenang. Pelanggaran

data dapat memiliki dampak serius, termasuk hilangnya kepercayaan pelanggan, kerugian finansial, dan bahkan tindakan hukum.

2. Risiko Serangan Perangkat Lunak Jahat
   Serangan perangkat lunak jahat, seperti virus, *worm*, *ransomware*, dan *trojan horse*, dapat merusak atau mencuri data dalam SIM. Serangan ini dapat terjadi melalui email *phishing*, situs web yang tidak aman, atau perangkat USB yang terinfeksi. Serangan perangkat lunak jahat merupakan ancaman konstan bagi keamanan data.
3. Risiko Serangan DDoS
   Serangan *Denial of Service* (DDoS) adalah serangan di mana penyerang mencoba membuat layanan SIM menjadi tidak tersedia dengan membanjiri sistem dengan lalu lintas internet palsu. Ini dapat mengakibatkan gangguan serius dalam operasional perusahaan, terutama jika bisnis sangat bergantung pada SIM untuk operasi sehari-hari.
4. Risiko Ancaman Insider
   Ancaman dari dalam organisasi, baik itu disengaja atau tidak, merupakan risiko lain yang signifikan. Karyawan yang tidak jujur atau kurangnya pelatihan keamanan data dapat menyebabkan pelanggaran data atau kerusakan sistem dari dalam.
5. Risiko Ketidakpatuhan Regulasi
   Organisasi sering kali harus mematuhi berbagai regulasi dan kebijakan yang berkaitan dengan keamanan data, seperti GDPR di Eropa atau HIPAA di Amerika Serikat. Pelanggaran regulasi ini dapat mengakibatkan sanksi hukum dan denda yang signifikan.

## F. *Redirect injection*

*Redirect injection* merupakan salah satu jenis serangan keamanan web yang terjadi ketika penyerang menyisipkan atau memanipulasi parameter URL dalam sebuah aplikasi web dengan tujuan untuk mengarahkan *(redirect)* pengguna ke situs web yang tidak sah atau berbahaya. Serangan ini biasanya terjadi karena kurangnya validasi terhadap *input* pengguna, khususnya pada parameter yang menangani URL tujuan setelah aksi tertentu, seperti *login* atau *logout* (Kaur, G., & Kinger, S. 2013).

Dalam praktiknya, penyerang mengeksploitasi celah ini dengan menyisipkan URL eksternal ke dalam parameter redirect. Jika sistem tidak melakukan penyaringan atau validasi dengan baik, pengguna yang mengklik tautan tersebut dapat secara otomatis dialihkan ke situs berbahaya seperti situs *phishing*, *malware*, atau situs judi online. Serangan ini tidak hanya membahayakan pengguna, tetapi juga merusak reputasi dan kepercayaan terhadap sistem atau situs yang menjadi target serangan (Kaur, G., & Kinger, S. 2013).

*Redirect injection* sering digunakan sebagai bagian dari strategi rekayasa sosial (social engineering), di mana pengguna dibuat percaya bahwa mereka sedang mengakses situs resmi, padahal sebenarnya telah diarahkan ke situs penipuan. Oleh karena itu, penting bagi pengembang sistem untuk memastikan bahwa setiap parameter URL divalidasi dan dibatasi hanya untuk redirect ke domain atau rute yang telah ditentukan Kaur, G., & Kinger, S. (2013).

## G. *Deface Attack*

*Deface attack* atau serangan *defac*ement merupakan salah satu bentuk serangan terhadap keamanan website di mana penyerang berhasil mengubah tampilan antarmuka (interface) halaman web tanpa izin pemiliknya. Serangan ini biasanya dilakukan dengan cara mengeksploitasi celah keamanan pada sistem web, seperti kerentanan pada skrip, sistem manajemen konten (CMS), atau kelemahan konfigurasi server (A. Gupta and R. Gupta, 2015).

Tujuan utama dari *deface attack* bukan untuk mencuri data, melainkan untuk menunjukkan keberhasilan penetrasi ke dalam sistem dengan cara mengubah konten visual dari halaman yang diserang. Biasanya, halaman yang sudah di*deface* akan menampilkan pesan tertentu dari penyerang, seperti propaganda, sindiran, atau simbol identitas kelompok hacker. Hal ini dapat berdampak serius terhadap reputasi, kepercayaan pengguna, serta citra lembaga atau organisasi yang websitenya menjadi target (A. Gupta and R. Gupta, 2015).

Secara teknis, *deface attack* terjadi ketika penyerang mendapatkan akses tidak sah ke file sistem atau database website, terutama file HTML, PHP, atau direktori utama tempat file website disimpan. Setelah mendapatkan akses, penyerang dapat mengganti, menghapus, atau menyisipkan file baru untuk mengganti halaman yang seharusnya ditampilkan (A. Gupta and R. Gupta, 2015).

Untuk mencegah serangan ini, penting bagi pengelola website untuk melakukan pengamanan berlapis, seperti memperbarui sistem secara berkala, menerapkan kontrol akses yang ketat, serta memantau log aktivitas dan celah keamanan secara aktif (A. Gupta and R. Gupta, 2015).

## H. *OWASP ZAP*

*Zed Attack Proxy* (ZAP) adalah aplikasi untuk melakukan pentest untuk menemukan vulnerabilities dalam suatu *web applications* dengan cara mudah, ZAP menyediakan scanner automatis sebaik bila kita menggunakan *tool* untuk menemukan *vulnerabilities* secara manual. Ketika digunakan sebagai *server proxy*, ini memungkinkan pengguna untuk memanipulasi semua lalu lintas yang melewatinya, termasuk lalu lintas menggunakan https, itu juga dapat berjalan dalam mode *daemon* yang kemudian dikontrol melalui REST API. ZAP telah ditambahkan ke dalam Radar Teknologi *ThoughtWorks* pada 30 Mei 2015 di cincin Percobaan. ZAP awalnya bercabang dari Paros, *proxy* pentesting lainnya. Simon Bennetts, pemimpin proyek, menyatakan pada tahun 2014 bahwa hanya 20% dari kode sumber ZAP masih dari Paros (Gregorius Hendita Artha Kusuma, 2022).

## III. METODE PENELITIAN

### A. Jenis Penelitian

Penelitian ini merupakan penelitian *eksperimen* yang bertujuan untuk menguji keamanan website terhadap serangan *deface* dan *redirect injection* melalui simulasi serangan menggunakan *OWASP ZAP*. Pendekatan ini dilakukan dengan melakukan serangkaian pengujian keamanan pada website Universitas Ubudiyah Indonesia (UUI) guna mengidentifikasi potensi celah keamanan yang dapat dieksploitasi oleh peretas.

Selain itu, penelitian ini juga bersifat *deskriptif*, di mana hasil pengujian akan dianalisis untuk mengetahui sejauh mana website rentan terhadap ancaman siber. Data yang diperoleh akan dikaji secara mendalam untuk memberikan rekomendasi mitigasi guna meningkatkan ketahanan website terhadap serangan siber.

### B. Teknik Pengumpulan Data

Teknik pengumpulan data dalam penelitian ini dilakukan melalui beberapa metode berikut:

1. Pengujian Keamanan dengan *OWASP ZAP*
   Pengujian dilakukan dengan menggunakan *OWASP ZAP (Zed Attack Proxy )* untuk mensimulasikan serangan terhadap website Universitas Ubudiyah Indonesia (UUI). Teknik yang digunakan mencakup:
   a. *Passive Scanning* untuk mengidentifikasi potensi celah keamanan tanpa mengganggu sistem.
   b. *Active scanning* untuk menguji kemungkinan eksploitasi celah keamanan yang ditemukan.
   c. *Fuzzing* untuk menguji berbagai *input* yang dapat menyebabkan kerentanan seperti *redirect injection* dan *deface*.
2. Observasi Langsung
   Observasi dilakukan dengan mengamati kondisi keamanan website UUI sebelum dan sesudah dilakukan pengujian. Data yang dikumpulkan meliputi tampilan website, kemungkinan adanya perubahan akibat serangan, serta respons sistem terhadap simulasi serangan yang dilakukan.
3. *Analisis Log* dan *Response Website*
   Data dikumpulkan dari log sistem yang merekam aktivitas pengujian, termasuk request-response yang terjadi selama simulasi. Log ini akan dianalisis untuk mendeteksi potensi celah keamanan yang dapat dieksploitasi oleh peretas.
4. Studi Literatur
   Penelitian ini juga menggunakan berbagai referensi dari jurnal, buku, serta laporan keamanan siber yang relevan dengan ancaman *deface* dan *redirect injection* . Studi literatur ini bertujuan untuk memperkuat analisis dan memberik an dasar teori dalam mendukung hasil pengujian.

### C. Pengujian dan Analisis

Pengujian dalam penelitian ini dilakukan untuk mengevaluasi tingkat keamanan website Universitas Ubudiyah Indonesia (UUI) terhadap serangan *deface* dan *redirect injection* . Proses pengujian menggunakan *OWASP ZAP* yang akan menganalisis berbagai celah keamanan yang dapat dimanfaatkan oleh peretas. Hasil pengujian kemudian dianalisis berdasarkan tingkat risiko serta dampak yang ditimbulkan terhadap website.

Analisis dilakukan dengan membandingkan hasil deteksi *OWASP ZAP* dengan standar keamanan yang berlaku, seperti *OWASP Top 10* dan *CWE (Common Weakness Enumeration)*. Dari hasil analisis ini, penelitian akan memberikan rekomendasi mitigasi untuk meningkatkan keamanan website UUI agar lebih tahan terhadap serangan siber.

### D. Roadmap Penelitian

Roadmap penelitian ini mencakup tahapan-tahapan yang dilakukan dalam proses pengujian keamanan website. Tahapan tersebut meliputi:

1. **Studi Pendahuluan**
   a. Identifikasi permasalahan keamanan website
   b. Studi literatur terkait ancaman *deface* dan *redirect injection*
   c. Pemilihan alat pengujian (*OWASP ZAP*)
2. **Persiapan dan Konfigurasi Pengujian**
   a. Instalasi dan konfigurasi *OWASP ZAP*
   b. Pengaturan parameter peng ujian sesuai dengan skenario serangan
   c. Pengumpulan data awal website UUI
3. **Pelaksanaan Pengujian**
   a. *Passive Scanning* untuk mengidentifikasi potensi celah keamanan
   b. *Active scanning* untuk menguji kemungkinan eksploitasi
   c. *Fuzzing* untuk mengidentifikasi *input* yang rentan terhadap serangan
4. **Analisis dan Evaluasi Hasil**
   a. Pemeriksaan hasil deteksi *OWASP ZAP*
   b. Identifikasi dan klasifikasi celah keamanan yang ditemukan
   c. Evaluasi dampak dan tingkat risiko terhadap website
5. **Rekomendasi Mitigasi dan Kesimpulan**
   a. Penyusunan strategi mitigasi untuk meningkatkan keamanan website
   b. Penyusunan laporan hasil penelitian
   c. Kesimpulan dan saran untuk pengembangan keamanan website ke depannya

### *E. Passive Scanning*

*Passive Scanning* adalah teknik pengujian yang dilakukan tanpa mengirimkan request berbahaya ke website target. Teknik ini digunakan untuk mengamati respon website terhadap permintaan biasa dan

mengidentifikasi potensi celah keamanan yang dapat dieksploitasi.

Pada penelitian ini, *Passive Scanning* dengan *OWASP ZAP* akan digunakan untuk:

a. Mendeteksi kebocoran informasi dalam header HTTP atau *cookie*.
b. Mengidentifikasi konfigurasi keamanan yang lemah.
c. Menganalisis CSP (*Content Security Policy*) dan proteksi terhadap *redirect injection* .
d. Menemukan potensi celah keamanan tanpa menyebabkan gangguan pada website.

### F. *Active scanning*

*Active scanning* adalah teknik pengujian yang lebih agresif, di mana *OWASP ZAP* akan mengirimkan berbagai *request* yang dimodifikasi untuk menguji kemungkinan eksploitasi celah keamanan.

Dalam penelitian ini, *active scanning* akan digunakan untuk:

**a.** Menguji kemungkinan *SQL Injection* dan *XSS (Cross-Site Scripting).*
**b.** Mengidentifikasi *open redirect vulnerabilities* yang memungkinkan serangan *redirect injection* .
**c.** Menguji kekuatan autentikasi dan *validasi input* pada website.
**d.** Mensimulasikan eksploitasi terhadap celah keamanan yang ditemukan dalam *Passive Scanning.*

### G. *Fuzzing*

*Fuzzing* adalah teknik pengujian keamanan yang bertujuan untuk menemukan kelemahan dalam sistem dengan memasukkan data acak atau tidak terduga ke dalam *input* website.

Dalam penelitian ini, *fuzzing* akan digunakan untuk:

a. Menguji kemungkinan eksploitasi pada *form input* dan parameter URL.
b. Mendeteksi *vulnerabilities* pada sesi pengguna atau autentikasi website.
c. Mengidentifikasi kelemahan yang dapat menyebabkan perubahan tampilan website atau pengalihan ke situs pihak ketiga.

## IV. HASIL DAN PEMBAHASAN

### A. Pengujian Keamanan Website Universitas Ubudiyah Indonesia

Penelitian ini bertujuan untuk mengidentifikasi dan menganalisis potensi kerentanan keamanan pada website Universitas Ubudiyah Indonesia (UUI) terhadap dua jenis serangan umum, yaitu ***deface*** dan ***redirect injection*** , dengan menggunakan pendekatan simulasi melalui tools *Open Web Application Security Project Zed Attack Proxy* (**OWASP ZAP**). OWASP ZAP dipilih karena merupakan salah satu alat yang diakui secara luas dalam dunia *penetration testing* berbasis web, dengan kemampuan *Passive Scanning*, *active scanning*, hingga *fuzzing* terhadap parameter *input* situs web.

Pengujian dilakukan pada saat waktu aktif pengguna (antara pukul 10.00 s.d. 13.00 WIB) guna memperoleh lalu lintas data yang optimal. Hal ini sesuai dengan pendekatan *real-traffic simulation* yang bertujuan untuk mengidentifikasi ancaman keamanan dalam kondisi aktual penggunaan.

### B. Identifikasi Target Website

Identifikasi target diawali dengan observasi terhadap domain utama dan subdomain aktif yang terasosiasi dengan layanan sistem informasi Universitas Ubudiyah Indonesia. Berdasarkan hasil pengamatan, beberapa domain dan subdomain yang dijadikan objek pengujian adalah sebagai berikut:

1. www.uui.ac.id – Website utama institusi.
2. sipenmaru.uui.ac.id – Daa penerimaan mahasiswa baru.
3. rpl.uui.ac.id – Daa penerimaan mahasiswa baru jalur RPL.
4. daa.uui.ac.id – Sistem informasi administrasi dan akademik.

Pemilihan subdomain ini didasarkan pada frekuensi akses pengguna dan potensi penyimpanan data sensitif, sehingga menjadikannya target yang relevan untuk pengujian keamanan berbasis simulasi serangan.

### C. Teknik *Passive Scanning*

Teknik *Passive Scanning* digunakan untuk memetakan informasi awal tanpa mengirimkan payload atau permintaan aktif ke server target. OWASP ZAP secara otomatis menangkap HTTP request dan response untuk mendeteksi potensi kelemahan dari sisi konfigurasi.

Beberapa temuan dari *Passive Scanning* meliputi:

1. *Cookie* Tidak Aman: Teridentifikasi penggunaan *cookie* tanpa atribut Secure dan HttpOnly. Hal ini membuka peluang bagi session hijacking atau *cookie* theft dalam koneksi yang tidak dienkripsi.
2. Pengalihan Tak Valid: Beberapa halaman diketahui melakukan pengalihan *(redirect)* ke situs eksternal tanpa validasi URL yang ketat. Ini dapat digunakan oleh penyerang untuk melakukan serangan *redirect injection* .

### D. Teknik *Active scanning*

Pada tahap ini, OWASP ZAP mengirimkan payload ke endpoint dan parameter *input* secara otomatis guna mendeteksi respons abnormal dari server.

Beberapa kerentanan ditemukan:

1. **XSS *(Cross-Site Scripting)***: Parameter *input* pada subdomain rpl.uui.ac.id rentan terhadap injeksi skrip berbahaya. Pengguna yang mengakses tautan terinfeksi berpotensi kehilangan sesi atau mengalami manipulasi tampilan.

2. ***Open redirect*** : Subdomain pmb.uui.ac.id mengandung parameter ?redirect=, yang tidak menyaring URL tujuan secara tepat, memungkinkan pengguna diarahkan ke situs *phishing*.

Temuan ini memperlihatkan kurangnya validasi *input* dan sanitasi parameter, yang merupakan rekomendasi dasar dari OWASP Top 10 kategori *Injection* dan *Broken Authentication*.

### E. Teknik *Fuzzing*

*Fuzzing* dilakukan dengan mengirimkan berbagai variasi *input* acak ke parameter situs guna melihat bagaimana sistem menangani *input* yang tak lazim.

Hasilnya:

a. Beberapa endpoint pada subdomain daa.uui.ac.id menghasilkan kode status 500 (Internal Server Error) saat menerima karakter acak atau payload spesifik. Hal ini menunjukkan adanya penanganan *input* yang lemah dan potensi terhadap serangan *Denial of Service* atau eksploitasi celah *code execution*.

### F. Implementasi dan Hasil Pengujian

Berikut adalah rekapitulasi hasil pengujian keamanan terhadap website Universitas Ubudiyah Indonesia berdasarkan domain/subdomain yang diuji, jenis kerentanan, teknik deteksi, dan tingkat risikonya:

Tabel 1. Hasil Pengujian Keamanan Website Universitas Ubudiyah Indonesia

| No | Domain/Subdomain | Kerentanan Terdeteksi | Teknik Pengujian | Tingkat Risiko |
|---|---|---|---|---|
| 1 | www.uui.ac.id | *Cookie* tidak aman | *Passive Scanning* | Sedang |
| 2 | sipenmaru.uui.ac.id | *Open redirect* URL | *Redirect injection* | Tinggi |
| 3 | rpl.uui.ac.id | XSS pada parameter *input* | *Active scanning* | Tinggi |
| 4 | daa.uui.ac.id | Error 500 pada *input* acak | *Fuzzing* | Sedang |
| 5 | rpl.uui.ac.id | Redirect ke situs slot online | *Redirect injection* | Tinggi |

### G. Pembahasan

Berdasarkan hasil pengujian, ditemukan sejumlah kerentanan kritikal yang menunjukkan bahwa website Universitas Ubudiyah Indonesia memerlukan pembenahan signifikan dalam hal keamanan aplikasi web.

Beberapa poin penting pembahasan adalah:

1. Kerentanan terhadap *Redirect injection*
   Serangan redirect memungkinkan penyerang mengalihkan pengguna dari situs resmi ke situs jahat seperti iklan judi online atau situs phising. Tanpa adanya validasi URL tujuan (*whitelist redirect*), pengguna dapat diarahkan secara diam-diam ke situs yang membahayakan.
2. *Cookie* Tidak Aman
   Tidak adanya atribut Secure dan HttpOnly pada *cookie* memungkinkan pencurian data sesi jika pengguna mengakses dari jaringan publik (misal Wi-Fi umum). Hal ini membuka peluang bagi serangan *session hijacking*.
3. Celah XSS dan Poor *Input* Handling
   Celah XSS masih menjadi masalah utama dalam banyak sistem aplikasi web. Selain XSS, hasil error 500 dari *input* acak menunjukkan server tidak memiliki sistem sanitasi dan validasi *input* yang baik.

### H. Implikasi dan Rekomendasi

Temuan penelitian ini memiliki implikasi serius terhadap:

a. Reputasi Institusi: Redirect ke situs tidak sah dapat mencoreng nama baik institusi pendidikan.
b. Keamanan Pengguna: Celah XSS dan *open redirect* dapat menyebabkan pencurian akun pengguna dan eksploitasi data pribadi.
c. Kepatuhan dan Audit: Sistem web institusi perlu mengikuti standar keamanan nasional dan internasional seperti ISO 27001.

Rekomendasi:

a. Audit keamanan sistem secara berkala.
b. Implementasi Web Application Firewall (WAF).
c. Penggunaan Content Security Policy (CSP) dan Secure Header.
d. Validasi dan sanitasi semua *input* pengguna.
e. Edukasi dan pelatihan bagi pengembang aplikasi web internal.

## V. KESIMPULAN DAN SARAN

### A. Kesimpulan

Berdasarkan hasil penelitian dan pengujian keamanan website Universitas Ubudiyah Indonesia menggunakan tools OWASP ZAP, dapat disimpulkan beberapa poin penting sebagai berikut:

1. Terdapat Kerentanan pada Beberapa Subdomain Website UUI
   Hasil pengujian menunjukkan bahwa website utama dan beberapa subdomain seperti pmb.uui.ac.id, elearning.uui.ac.id, dan daa.uui.ac.id memiliki celah keamanan signifikan, termasuk *open redirect* , *cross-site scripting* (XSS), serta penanganan *input* yang buruk (error 500), yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab.
2. Kerentanan *Redirect injection* Berisiko Tinggi
   Beberapa endpoint tidak memiliki validasi URL yang ketat, sehingga memungkinkan pengguna

dialihkan ke situs eksternal berbahaya, seperti situs perjudian online. Kondisi ini sangat membahayakan reputasi institusi dan berpotensi menyebabkan pengguna menjadi korban *phishing*.

3. Keamanan Session Rentan karena Konfigurasi *Cookie* Tidak Optimal
   Ditemukan bahwa *cookie* yang dikirimkan oleh server tidak disertai dengan atribut Secure dan HttpOnly, sehingga membuka peluang terjadinya serangan *session hijacking*, khususnya ketika pengguna mengakses melalui jaringan tidak aman.
4. Kurangnya Validasi *Input* dan Penanganan Error
   Pengujian dengan teknik *fuzzing* menghasilkan error internal server (500) saat *input* acak dikirimkan ke server. Hal ini menunjukkan belum diterapkannya mekanisme validasi dan penanganan *input* secara menyeluruh, sehingga meningkatkan risiko terhadap serangan DoS (*Denial of Service*) atau eksploitasi kode.
5. Pentingnya Audit dan Keamanan Berlapis Secara umum, pengujian ini menegaskan pentingnya penerapan *security hardening* dan audit sistem informasi secara berkala untuk menjamin keamanan data, sistem, dan pengguna.

**B. Saran**

Adapun saran yang dapat diberikan sebagai tindak lanjut dari hasil penelitian ini antara lain:

1. Melakukan Validasi dan Sanitasi *Input* secara Ketat
   Semua parameter dan *input* dari pengguna harus melalui proses validasi *(whitelisting)* dan sanitasi agar mencegah injeksi kode berbahaya seperti XSS, SQLi, atau *command injection.*
2. Mengimplementasikan Header Keamanan pada Response HTTP
   Penggunaan *heade*r seperti *Content-Security-Policy (CSP), X-Content-Type-Options, Strict-Transport-Security*, dan pengaturan *cookie* Secure dan *HttpOnly* sangat disarankan untuk meningkatkan lapisan keamanan aplikasi web.
3. Melakukan Penyesuaian pada Mekanisme Redirect
   Sistem sebaiknya hanya mengizinkan redirect ke URL internal yang telah ditentukan *(whitelisted).* Apabila harus redirect ke situs luar, maka harus disertai konfirmasi pengguna atau token validasi.
4. Melakukan Audit Keamanan Web Secara Berkala Audit atau *penetration testing* minimal dilakukan setiap 6 bulan atau setelah adanya perubahan besar pada sistem. Pengujian dapat dilakukan dengan tools seperti OWASP ZAP, *Burp Suite*, atau dengan jasa audit eksternal yang profesional.
5. Meningkatkan Literasi Keamanan Pengembang Web Internal
6. Diperlukan pelatihan keamanan (*secure coding* ) untuk tim pengembang internal guna meningkatkan pemahaman terhadap praktik pengembangan aplikasi web yang aman sesuai dengan panduan OWASP Top 10.
7. Mengaktifkan Monitoring dan Logging Insiden Keamanan Sistem monitoring real-time serta pencatatan log aktivitas harus diaktifkan agar dapat mendeteksi aktivitas mencurigakan dan merespon insiden dengan cepat.

**REFERENSI**

[1] Ikhlasul Amal, 2024. rancang bangun sistem informasi *virtual tour* campus menggunakan H5P studi kasus universitas ubudiyah indonesia. skripsi 2024.

[2] Agung Wijoyo, Dkk. 2023. Keamanan Data dalam Sistem Informasi Manajemen: Risiko dan Strategi Perlindungan. Jurnal 2023.

[3] Kaur, G., & Kinger, S. (2013). *Analysis of SQL Injection Detection and Prevention Techniques*. International Journal of Computer Applications, 77(16), 7–12. https://doi.org/10.5120/13435-1123

[4] A. Gupta and R. Gupta, "Web Application Security: Threats and Solutions," Int. J. Adv. Res. Comput. Sci. Softw. Eng., vol. 5, no. 4, pp. 646–651, 2015.

[5] Gregorius Hendita Artha Kusuma, 2022. Implementasi Owasp Zap Untuk Pengujian Keamanan Sistem Informasi Akademik. Jurnal 2022.

[6] Z. Munawar. Dkk. 2020. Keamanan Jaringan Komputer Pada Era Big Data. Vol.2 No. Juni 2020. Jurnal Sistem Informasi.

[7] Hasbullah Jamaluddin. Dkk. 2018. Analisis Keamanan Website Terhadap Sniffing Process Pada Jaringan Nirkabel Menggunakan Aplikasi Wireshark (Studi Kasus : Simak Unismuh). Skripsi, 2018.

[8] D.B. Rendro, Dkk, 2020. Analisis *Monitoring* Sistem Keamanan Jaringan Komputer Menggunakan *Software Nmap* (Studi Kasus Di Smk Negeri 1 Kota Serang). Jurnal 2018. Vol. 7 N0. 2 E-Issn 2597-9922. September 2020. Jurnal PROSISKO

[9] Edwin Mandala Putra. Dkk, 2021. Analisis Kemanan Jaringan Internet *(Wifi)* Dari Serangan Packet Data *Sniffing* Di Universitas Muhammadiyah .Jurnal, 2021