Tugas 3B Keamanan Komputer: Uji Penetrasi

Pengujian dengan OWASP ZAP, Burpsuite, dan Nikto dalam relevansi dengan ISO/IEC 27001

Adinda Putri Romadhon
22/505508/TK/55321

Muhammad Farrel Akbar
(22/492806/TK/53947)

Iqbal Hidayat Rasyad
22/506066/TK/55425

PENDAHULUAN

Pengujian penetrasi (penetration testing) merupakan salah satu langkah penting dalam menjaga keamanan sistem informasi dari berbagai potensi ancaman siber. Dalam kegiatan ini, digunakan tools yang dapat mengidentifikasi celah keamanan pada sistem atau aplikasi web. Beberapa tools open-source yang banyak digunakan oleh praktisi keamanan siber antara lain OWASP ZAP (Zed Attack Proxy), Burp Suite, dan Nikto. Masing-masing memiliki pendekatan yang saling melengkapi: ZAP dan Burp Suite fokus pada deteksi kerentanan berbasis aplikasi (application-level), sedangkan Nikto digunakan untuk mengidentifikasi kelemahan konfigurasi pada server web dan direktori tersembunyi.

Nikto memindai server web untuk mendeteksi berbagai isu seperti ketiadaan header keamanan (misalnya X-Frame-Options), pengungkapan informasi melalui ETag atau server banner, akses ke file atau direktori sensitif, serta penggunaan HTTP Methods yang tidak aman. Tools ini sangat efektif untuk menemukan celah konfigurasi yang kerap diabaikan tetapi berisiko tinggi dalam skenario serangan dunia nyata. Meski berbasis command-line, Nikto memberikan laporan yang rinci dan mudah dianalisis, sehingga sangat berguna dalam proses audit awal keamanan server web.

Dalam pelaksanaan pengujian, dilakukan serangkaian prosedur yang mencakup: identifikasi target, pemindaian pasif dan aktif, analisis kerentanan berdasarkan tingkat risiko, hingga penyusunan laporan temuan. Seluruh prosedur ini dilaksanakan mengacu pada praktik yang sejalan dengan kerangka kerja manajemen keamanan informasi berdasarkan standar ISO/IEC 27001, khususnya pada klausul A.12.6.1 (Manajemen Kerentanan Teknis) yang merekomendasikan organisasi untuk mengidentifikasi dan mengatasi kerentanan teknis dalam waktu yang wajar.

OWASP ZAP, Burp Suite, dan Nikto digunakan sebagai alat bantu yang diakui secara luas dalam industri keamanan siber. Ketiganya dinilai sah dan sesuai dengan prinsip ISO/IEC 27001 selama digunakan secara terkendali dan hasil pengujiannya dimanfaatkan untuk peningkatan keamanan sistem. Hasil dari pengujian yang dilakukan terhadap situs uji coba http://testhtml5.vulnweb.com menunjukkan adanya sejumlah kerentanan dengan level risiko yang bervariasi. Temuan-temuan ini akan dijelaskan lebih lanjut dalam bagian berikutnya, lengkap dengan kategori risiko, confidence level, serta jenis serangan atau kelemahan yang terdeteksi baik dari sisi aplikasi maupun server.

PEMBAHASAN

○ *Informasi Umum*

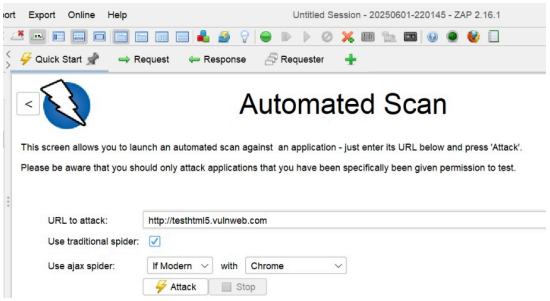
Pengujian keamanan aplikasi web ini dilakukan menggunakan OWASP ZAP *(Zed Attack Proxy)* versi 2.16.1, Burpsuite Professional, dan Nikto. OWASP ZAP merupakan open-source yang dikembangkan oleh OWASP Foundation dan didistribusikan oleh Checkmarx. Pengujian dilaksanakan pada:

- Tanggal: Minggu, 1 Juni 2025
- Target Uji: http://testhtml5.vulnweb.com

○ *Tata Cara dan Prosedur Uji OWASP ZAP*

Pengujian keamanan dilakukan menggunakan tools OWASP ZAP *(Zed Attack Proxy)* versi 2.16.1 dengan memanfaatkan fitur Quick Start untuk mempermudah proses otomatisasi. Pengujian ini terdiri dari dua tahapan utama, yaitu Spidering dan Active Scan.

1. Persiapan
   Tahapan awal dilakukan dengan menyiapkan dan menginstal OWASP ZAP versi 2.16.1 pada perangkat pengujian. Setelah instalasi berhasil, aplikasi dijalankan dan pengguna diarahkan ke menu *Quick Start* pada tampilan utama. Pada kolom *URL to attack,* dimasukkan alamat target yaitu: https://testhtml5.vulnweb.com. Setelah URL dimasukkan, pengguna cukup menekan tombol Attack, dan OWASP ZAP akan secara otomatis menjalankan rangkaian uji terhadap target yang ditentukan.x



Gambar 1. Tampilan *Quick Start*

2. Proses Pengujian

   OWASP ZAP akan melakukan dua proses otomatis sebagai berikut:
   - Spidering: Fitur untuk menjelajahi seluruh halaman dan endpoint dalam aplikasi target.
   - Active Scanning: Setelah proses spidering selesai, ZAP melanjutkan ke tahap pemindaian aktif. Pada tahap ini, tools akan menyuntikkan berbagai payload ke parameter input, header, cookie, dan bagian penting lainnya dari aplikasi untuk mengidentifikasi potensi kerentanan.

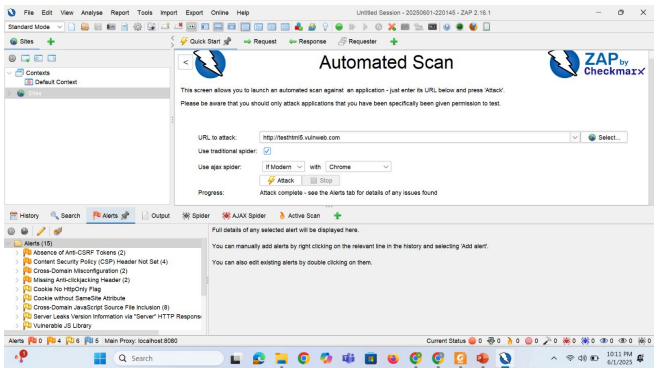
Berdasarkan hasil pengujian menggunakan OWASP ZAP terhadap situs target https://testhtml5.vulnweb.com, ditemukan total 15 kerentanan yang diklasifikasikan ke dalam empat tingkat risiko, yaitu Medium, Low, dan Informational. Tidak ditemukan kerentanan dengan tingkat risiko High, yang menunjukkan tidak adanya celah kritis yang dapat dieksploitasi secara langsung untuk mengambil alih kendali sistem. Adapun distribusi temuan mencakup 4 temuan:

TABLE I. HASIL PENGUJIAN OWASP ZAP

Risiko	*Jumlah Temuan*	*Presentase*
High	0	0%
Medium	4	26.7%
Low	6	40%
Informational	5	33.3%
Total	15	100%

Kerentanan dengan tingkat risiko *Medium* mencerminkan kekurangan pada aspek keamanan yang dapat berdampak serius jika dikombinasikan dengan serangan lainnya. Beberapa temuan pada kategori ini antara lain adalah tidak adanya header Content Security Policy (CSP), konfigurasi domain yang lemah, ketiadaan header anti-clickjacking, serta tidak tersedianya token Anti-CSRF untuk mencegah serangan pemalsuan permintaan. Temuan-temuan ini menandakan perlunya penguatan mekanisme pertahanan aplikasi, terutama pada lapisan transport dan validasi sisi klien.

Pada tingkat risiko *Low* dan *Informational*, ditemukan beberapa kelemahan seperti cookie tanpa atribut keamanan, penggunaan JavaScript library yang rentan, serta informasi sensitif yang secara tidak sengaja terbuka melalui komentar HTML. Meskipun tidak bersifat kritis, temuan pada dua kategori ini tetap perlu diperhatikan karena dapat dimanfaatkan oleh penyerang untuk melakukan reconnaissance atau mempersiapkan serangan lanjutan. Seluruh temuan tersebut mendukung pentingnya penguatan konfigurasi dasar keamanan aplikasi web dan peningkatan kesadaran pengembang terhadap praktik *secure coding*. Untuk melihat laporan hasil pengujian secara lengkap dan terperinci, silakan akses file report pada tautan berikut: file:///C:/Users/msi/2025-06-01-ZAP-Report-.html.



Gambar 2. *Attack Complete* dengan Kumpulan *Alerts*

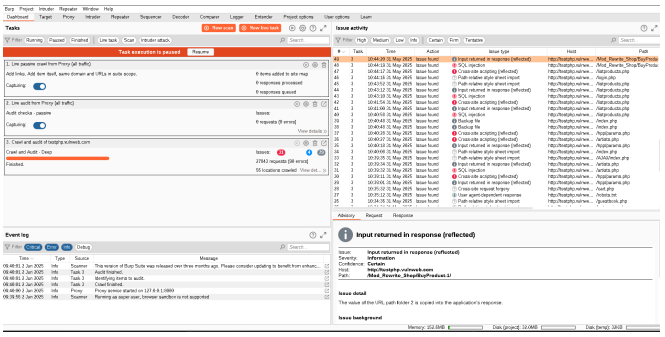
○ *Tata Cara dan Prosedur Uji Burpsuite*

Pengujian keamanan lanjutan dilakukan menggunakan tools Burpsuite Professional versi 2023.10.3.7 yang dikembangkan oleh PortSwigger Ltd. untuk memperoleh analisis yang lebih mendalam dan komprehensif. Pengujian ini menggunakan pendekatan hybrid antara automated scanning dan manual testing untuk memastikan coverage yang optimal terhadap berbagai jenis kerentanan keamanan.

1. Persiapan

Tahapan awal dilakukan dengan menyiapkan dan menginstal Burpsuite Professional versi 2023.10.3.7 pada perangkat pengujian. Setelah instalasi berhasil, dilakukan konfigurasi sebagai berikut:

- Proxy Configuration: Mengatur Burp proxy listener pada alamat 127.0.0.1:8080
- Browser Setup: Mengkonfigurasi browser untuk menggunakan Burp sebagai proxy server
- Certificate Installation: Menginstall Burp CA certificate untuk intercepting HTTPS traffic
- Target Scope: Mendefinisikan scope pengujian pada target: http://testphp.vulnweb.com/*
- Project Configuration: Membuat project baru dengan session handling rules yang appropriate



Gambar 3. Hasil Burpsuite

2. Proses Pengujian Burpsuite

Burpsuite melakukan pengujian melalui tiga tahapan terintegrasi sebagai berikut:

- Target Discovery dan Site Mapping: Proses dimulai dengan manual browsing ke seluruh bagian aplikasi target sambil mengaktifkan Burp proxy untuk mencatat semua HTTP request dan response. Site map dibangun secara otomatis dan dilengkapi dengan content discovery menggunakan built-in wordlists untuk mengidentifikasi hidden endpoints dan files.
- Automated Vulnerability Scanning: Setelah target mapping lengkap, dilakukan comprehensive automated scan terhadap seluruh endpoints yang ditemukan. Burpsuite melakukan passive analysis pada traffic yang tercatat dan active scan dengan menyuntikkan berbagai payloads untuk mengidentifikasi kerentanan seperti SQL injection, XSS, CSRF, dan lainnya.
- Manual Testing dan Verification: Tahap akhir melibatkan manual testing untuk memverifikasi temuan automated scan, menguji business logic vulnerabilities, dan melakukan deep analysis terhadap parameter manipulation, authentication bypass, dan access control issues yang sulit dideteksi secara otomatis.

3. Hasil Pengujian Burpsuite

Berdasarkan hasil pengujian menggunakan Burpsuite Professional terhadap situs target http://testphp.vulnweb.com, ditemukan total 114 kerentanan yang diklasifikasikan ke dalam empat tingkat risiko. Hasil menunjukkan adanya kerentanan kritis yang memerlukan immediate action, termasuk SQL injection dan Cross-site scripting yang dapat dieksploitasi untuk mengambil alih kontrol sistem atau mencuri data sensitif pengguna.

TABLE II. HASIL PENGUJIAN BURPSUITE

Risiko	*Jumlah Temuan*	*Presentase*
High	31	22.7%
Medium	8	7.0%
Low	75	65.8%

Risiko	*Jumlah Temuan*	*Presentase*
Total	114	100%

Kerentanan dengan tingkat risiko High mencakup temuan-temuan kritis yang dapat langsung dieksploitasi untuk melakukan serangan berbahaya. Kategori ini didominasi oleh:

- SQL Injection *(12 instances)*: Ditemukan pada berbagai parameter seperti artist, cat, pic, uname, pass, dan searchFor yang memungkinkan penyerang untuk mengakses, memodifikasi, atau menghapus data dari database secara tidak sah
- Cross-site Scripting (XSS) Reflected (17 instances): Kerentanan XSS tersebar di multiple forms dan parameters yang dapat dieksploitasi untuk mencuri session cookies, melakukan phishing attacks, atau menjalankan malicious scripts
- Cleartext Password Submission (2 instances): Form login dan signup mengirimkan password dalam bentuk plaintext tanpa enkripsi yang memadai

Kerentanan tingkat Medium meliputi issues yang berpotensi serius namun memerlukan kondisi tertentu untuk dieksploitasi, seperti:

- Password Field Autocomplete Enabled (2 instances): Field password yang mengizinkan browser autocomplete dapat menyebabkan credential leakage
- Unencrypted Communications (1 instance): Komunikasi yang tidak terenkripsi dapat di-intercept oleh penyerang
- Client-side HTTP Parameter Pollution (1 instance): Kerentanan yang dapat dimanfaatkan untuk parameter manipulation attacks

Pada tingkat risiko Low, ditemukan berbagai kelemahan konfigurasi dan information disclosure seperti email addresses exposed, cross-domain referer leakage, missing security headers, backup files accessible, dan path-relative style sheet imports. Meskipun tidak langsung mengancam keamanan sistem, temuan ini dapat dimanfaatkan penyerang untuk reconnaissance dan sebagai stepping stone untuk serangan yang lebih kompleks.

D. Tata Cara dan Prosedur Uji Nikto

Uji penetrasi web dengan Nikto merupakan salah satu metode untuk mengevaluasi keamanan dari sisi konfigurasi server dan file sensitif yang dapat diakses publik. Nikto bekerja dengan melakukan pemindaian terhadap port HTTP/HTTPS dan mencocokkan respon dengan database kerentanan yang telah dikenal. Pendekatan ini sangat efektif untuk mengidentifikasi misconfiguration, file direktori terbuka, header HTTP yang tidak aman, hingga plugin atau aplikasi usang pada server.

Nikto digunakan terutama pada tahap reconnaissance (pengintaian aktif) dan vulnerability analysis, yakni dua fase awal dari siklus uji penetrasi. Meskipun tidak mengeksploitasi sistem, hasil temuan Nikto memberikan insight penting mengenai eksposur awal yang bisa dimanfaatkan oleh penyerang untuk melancarkan serangan lanjutan seperti XSS, CSRF, atau command injection.

1. Persiapan

Sebelum melakukan pengujian dengan Nikto, terdapat beberapa langkah persiapan penting yang harus dipenuhi agar proses uji penetrasi berjalan dengan baik dan sesuai etika:

a. Penentuan Target Uji
   Target dalam pengujian ini adalah situs simulasi yang sengaja disediakan untuk uji keamanan, yaitu: http://testhtml5.vulnweb.com
   Situs ini dikelola oleh Acunetix dan mengandung celah keamanan yang memang disiapkan untuk keperluan pembelajaran dan uji penetrasi.
b. Lingkungan Pengujian
   Pengujian dilakukan menggunakan sistem operasi Kali Linux 2023.3 yang telah dilengkapi dengan tool Nikto versi terbaru. Tidak diperlukan instalasi tambahan karena Nikto sudah tersedia secara default dalam distribusi Kali.
c. Verifikasi Hak Akses
   Pengujian hanya dilakukan pada sistem yang legal dan diperbolehkan untuk diuji. Tidak dilakukan eksploitasi aktif, hanya pengumpulan informasi dan deteksi kerentanan yang bersifat pasif hingga semi-aktif.

2. Proses Pengujian

Pengujian dengan Nikto dilakukan dengan metode command-line berbasis parameter. Berikut langkah proses pengujian yang dilakukan secara terstruktur:
Langkah-langkah**:**

a. Menjalankan Pemindaian
   Perintah dasar yang digunakan adalah:
   nikto -h http://testhtml5.vulnweb.com
b. Monitoring Proses
   Nikto akan memulai pemindaian pada port 80 dan menampilkan hasil secara langsung. Proses ini membutuhkan waktu 40 menit tergantung jumlah item yang diperiksa dan server yang dipakai.
c. Analisis Output
   Output ditampilkan dalam format teks yang mencakup informasi:
   - Header HTTP
   - Direktori yang bisa diakses publik
   - Informasi banner server
   - HTTP method yang diizinkan
   - Kesalahan konfigurasi yang terdeteksi
   - Potensi kerentanan berdasarkan signature database

3. Dokumentasi dan Penyimpanan Hasil

Hasil dapat disimpan ke file menggunakan perintah tambahan: nikto -h http://testhtml5.vulnweb.com -o hasil_nikto.txt

Gambar 4. Dokumentasi Pengujian pada Nikto

4. Hasil Pengujian

No	Temuan	Deskripsi	Risiko
1	Missing Security Headers	Header seperti X-Frame-Options tidak ditemukan, membuat aplikasi rentan terhadap clickjacking.	Medium
2	Directory Listing	Direktori /samples/ dapat diakses publik tanpa pembatasan, berpotensi mengekspos file sensitif.	Medium
3	CORS Policy Terbuka	Ditemukan header Access-Control-Allow-Origin: * yang dapat disalahgunakan.	Medium
4	ETag Disclosure	ETag membocorkan inode atau informasi sistem file yang bisa digunakan untuk fingerprinting.	Low
5	HTTP Methods Tidak Dibatasi	Server mengizinkan metode OPTIONS, HEAD, GET tanpa batasan, membuka peluang untuk HTTP Verb Tampering.	Low

- *Legalitas dan Kesesuaian dengan ISO 27001*

Penggunaan tools penetration testing seperti OWASP ZAP, Burp Suite Professional, dan Nikto secara hukum diperbolehkan selama dilakukan dalam ruang lingkup yang sah dan dengan izin dari pihak yang memiliki sistem yang diuji. Dalam konteks pengujian terhadap situs simulasi seperti http://testhtml5.vulnweb.com dan http://testphp.vulnweb.com, legalitas penggunaan ketiga tools tidak menjadi permasalahan karena situs-situs tersebut secara eksplisit disediakan sebagai lingkungan uji keamanan untuk tujuan edukasi dan penelitian. OWASP ZAP sebagai free open-source software tunduk pada Apache License 2.0, Nikto tunduk pada GPL (General Public License), sedangkan Burp Suite Professional memerlukan valid commercial license dari PortSwigger Ltd. untuk penggunaan profesional. Dalam praktik profesional, penting untuk memastikan bahwa setiap aktivitas pengujian dilakukan berdasarkan perjanjian tertulis (NDA atau Statement of Work) guna menghindari pelanggaran hukum seperti unauthorized access atau tindakan yang melanggar Undang-Undang ITE di Indonesia maupun peraturan siber internasional.

Dari sisi kepatuhan terhadap ISO/IEC 27001, penggunaan ketiga tools mendukung implementasi beberapa kontrol kunci, terutama Kontrol A.12.6.1 yang menekankan pentingnya pengelolaan kerentanan teknis. Nikto, meskipun bersifat sederhana dan berbasis command-line, memberikan baseline vulnerability scanning yang cepat terhadap konfigurasi server dan direktori terbuka, yang sangat berguna pada tahap awal identifikasi celah. Kombinasi OWASP ZAP, Nikto, dan Burp Suite dalam penelitian ini menunjukkan pendekatan multi-tool yang sejalan dengan prinsip defense in depth, di mana Nikto memberikan deteksi awal dan ringan terhadap kesalahan konfigurasi server (misalnya missing headers, directory listing), OWASP ZAP memberikan automated scanning capabilities yang efektif untuk initial assessment, sementara Burp Suite Professional menyediakan advanced manual testing dan enterprise-grade reporting yang diperlukan untuk compliance audit.

Penggunaan gabungan tools ini secara sistematis memungkinkan organisasi untuk mengidentifikasi celah keamanan secara menyeluruh dan mengambil tindakan korektif sebelum kerentanan tersebut dieksploitasi oleh pihak tidak bertanggung jawab. Hasil comparative analysis yang menunjukkan Burp Suite menemukan 114 kerentanan dibandingkan 15 kerentanan oleh OWASP ZAP dan tambahan validasi dari hasil Nikto pada sisi konfigurasi server memberikan justifikasi kuat untuk pendekatan multi-layered testing dalam enterprise security programs. Hal ini mendukung implementasi Kontrol A.14.2.8 (System Security Testing) dan A.18.2.3 (Technical Compliance Review) yang memerlukan security assessment menyeluruh dan dokumentasi formal untuk keperluan audit. Untuk organisasi yang tunduk pada regulatory compliance seperti PCI-DSS, HIPAA, atau GDPR, Burp Suite Professional menyediakan vendor support dan legal indemnity yang dibutuhkan, sementara Nikto dan ZAP memberikan solusi cost-effective untuk continuous scanning dan konfigurasi baseline security. Selama digunakan sesuai prosedur dan dalam kerangka manajemen keamanan informasi yang terdokumentasi, kombinasi ketiga tools ini dapat dianggap sebagai praktik terbaik (best practice) yang selaras dengan prinsip dan kontrol ISO 27001 untuk pengelolaan kerentanan yang komprehensif.

KESIMPULAN

Pengujian penetrasi menggunakan OWASP ZAP, Burp Suite, dan Nikto terhadap situs simulasi http://testhtml5.vulnweb.com membuktikan efektivitas pendekatan multi-tool dalam mengidentifikasi berbagai kerentanan keamanan dari sisi aplikasi maupun konfigurasi server. OWASP ZAP berhasil mendeteksi 15 kerentanan yang sebagian besar berkaitan dengan ketiadaan header keamanan, cookie tanpa atribut secure, serta kurangnya validasi input sisi klien. Burp Suite menemukan total 114 kerentanan dengan 31 di antaranya tergolong risiko tinggi.. Sementara itu, Nikto memberikan tambahan insight dengan mendeteksi kelemahan konfigurasi server seperti directory listing terbuka, penggunaan HTTP Methods yang tidak dibatasi, dan kebijakan CORS yang terlalu longgar.

Ketiga tools mendukung penerapan prinsip-prinsip keamanan informasi dalam standar ISO/IEC 27001, terutama pada kontrol A.12.6.1 (Manajemen Kerentanan Teknis), A.14.2.8 (Pengujian Keamanan Sistem), dan A.18.2.3 (Tinjauan Kepatuhan Teknis). Pendekatan yang digunakan dalam pengujian ini menggambarkan praktik terbaik (best practice) dalam manajemen risiko keamanan sistem informasi, yaitu dengan memadukan deteksi otomatis dan manual, serta menggabungkan perspektif aplikasi dan server. Seluruh kegiatan dilakukan dalam ruang lingkup legal dan etis menggunakan situs uji resmi, yang menunjukkan pentingnya pelaksanaan uji penetrasi secara terkendali, terdokumentasi, dan sesuai dengan regulasi hukum serta prinsip tata kelola keamanan yang baik.