BAB I
PENDAHULUAN

A. Latar Belakang

Dalam beberapa tahun terakhir, perkembangan dan penggunaan website telah meningkat dalam berbagai sektor organisasi, baik itu publik maupun swasta, termasuk pemerintahan, dan infrastruktur penting lainnya (Tudela et al., 2020). Salah satu cara yang paling umum digunakan oleh perusahaan atau organisasi untuk memberikan layanan mereka kepada pelanggan adalah dengan memanfaatkan website (Albahar et al., 2022). Namun, di tengah perkembangan tersebut, keamanan website menjadi perhatian utama karena celah keamanan yang tidak tertangani dapat menyebabkan kerugian besar, baik dari segi finansial, reputasi, hingga kehilangan data sensitif penggunanya (Wicaksono et al., 2020).

Pengujian sistem keamanan aplikasi berbasis website adalah hal yang penting untuk dilakukan, mengingat pesatnya perkembangan teknologi yang melaju dengan pesat. Semakin berkembangnya aplikasi berbasis website berbanding lurus dengan meningkatnya ancaman keamanan yang muncul dengan berbagai teknik serangan (Aryanti et al., 2021). Seiring bertambahnya jumlah penggunaan aplikasi berbasis web yang digunakan dalam berbagai sektor, potensi serangan kemanan juga semakin besar (Prasetyo & Hassanah, 2021). Kemajuan teknologi saat ini membuat para *hacker* semakin pintar dalam menggunakan berbagai teknik peretasan demi meraih keuntungan pribadi dari aksi pembobolan yang mereka lakukan. Berbagai metode serangan baru terus berkembang, menuntut sistem aplikasi web untuk memiliki perlindungan yang lebih baik agar dapat menangkal ancaman-ancaman tersebut. Laporan *Data Breach Investigations Report* (DBIR) 2024 dari Verizon, mencatat serangan siber terhadap aplikasi web, tetap yang menjadi ancaman utama bagi perusahaan.

Ancaman atau masalah keamanan web adalah aktivitas berpotensi berbahaya yang ditargetkan khusus pada satu atau beberapa komponen arsitektur aplikasi web, seperti *browser* pengguna atau *server* tempat aplikasi

web di-host (Sadqi & Yassine, 2022). Kerentanan seperti SQL Injection (SQLi) dan Cross-site Scripting (XSS) masih menjadi kerentanan yang paling sering dan paling banyak dihadapi pada aplikasi web (Tudela et al., 2020).

Website jurnalnasional.ump.ac.id merupakan portal jurnal online resmi milik Universitas Muhammadiyah Purwokerto. Portal ini menyediakan akses ke berbagai jurnal ilmiah yang diterbitkan oleh Universitas Muhammadiyah Purwokerto, mencakup berbagai disiplin ilmu. Setiap jurnal memiliki fokus dan ruang lingkup yang spesifik, menyediakan platform bagi peneliti, akademisi, dan praktisi untuk mempublikasikan hasil penelitian mereka. Portal ini memfasilitasi akses terbuka ke artikel-artikel ilmiah, mendukung penyebaran pengetahuan dan inovasi di berbagai bidang.

Menurut Bapak Eko Purwanto, selaku kepala Biro Sistem Informasi Universitas Muhammadiyah Purwokerto, website yang di kelola oleh pihak Biro Sistem Informasi seringkali menjadi target serangan oleh orang yang tidak bertanggung jawab. Oleh karena itu penting untuk meminimalkan potensi serangan keamanan guna menjaga privasi pengguna seperti data login atau data pribadi.

Metode pengujian keamanan *Dynamic Application Security Testing* (DAST) memungkinkan deteksi kerentanan pada aplikasi web yang sedang berjalan untuk mengidentifikasi kerentanan keamanan dengan mensimulasikan skenario serangan di dunia nyata. DAST menggunakan pendekatan *black-box testing,* artinya berinteraksi dengan aplikasi seperti yang dilakukan oleh pengguna atau penyerang, tanpa perlu memahami atau mengakses kode sumber (*source code*) yang mendasarinya. DAST dirancang untuk mengidentifikasi kelemahan keamanan pada aplikasi web dan *Application Programming Interface* (API) yang dapat dieksploitasi oleh penyerang, seperti *SQL injection*, *cross-site scripting* (XSS), *misconfigured* HTTP *security headers*, dan lain-lain.

Dengan metode ini, organisasi dapat memeriksa keamanan aplikasi dalam kondisi nyata dan mengidentifikasi potensi celah yang bisa dimanfaatkan oleh penyerang (Alviansyah & Ramadhani, 2021). Meski

demikian, penelitian terkait penerapan metode DAST pada berbagai jenis aplikasi web masih terbatas. Sebagian besar penelitian yang ada lebih banyak berfokus pada metode pengujian lain atau hanya pada aplikasi yang berskala besar. Hal ini mengindikasikan perlunya penelitian lebih lanjut terkait penerapan dari metode *Dynamic Application Security Testing* (DAST) pada aplikasi web dengan skala atau struktur yang berbeda, khususnya dalam konteks organisasi kecil hingga menengah yang seringkali tidak memiliki sumber daya keamanan yang memadai.

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk menganalisis website jurnalnasional.ump.ac.id dengan menggunakan metode *Dynamic Application Security Testing* (DAST) dalam mendeteksi dan mengidentifikasi kerentanan. Penelitian ini tidak hanya bertujuan untuk menemukan kerentanan, tetapi juga memberikan rekomendasi perbaikan keamanan bagi website tersebut.

B. Perumusan Masalah

Berdasarkan uraian latar belakang di atas, maka dapat di ambil perumusan masalah dalam penelitian ini yaitu, bagaimana cara menguji, menganalisis, dan kemudian melakukan validasi manual terhadap kerentanan yang telah di temukan oleh *tools* DAST untuk memeriksa keamanan website jurnalnasional.ump.ac.id dengan menggunakan metode *Dynamic Application Security Testing* (DAST)

C. Batasan Masalah

Batasan masalah pada penelitian ini adalah sebagai berikut:

1. Penelitian yang dilakukan hanya sebatas pada pengujian, menganalisis, dan melakukan validasi manual terhadap kerentanan yang telah di temukan oleh *tools*.
2. Metode yang digunakan pada penelitian ini adalah Dynamic Application Security Testing (DAST) dengan 3 tahapan, yaitu scanning, attack, dan report.

3. Tools atau alat yang digunakan yaitu OWASP ZAP, dan Codename SCNR.

D. Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah untuk mendapatkan hasil analisis yang dapat mengetahui apakah website jurnalnasional.ump.ac.id memiliki celah kerentanan keamanan di dalam websitenya.

E. Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan kontribusi dalam pengembangan ilmu pengetahuan di bidang keamanan siber, khususnya dalam hal penerapan metode DAST pada aplikasi web. Hasil penelitian ini dapat digunakan oleh pengembang website untuk mengidentifikasi dan memperbaiki kerentanan keamanan pada aplikasi yang sedang dikembangkan.