

BAB I

PENDAHULUAN

1.1 Latar Belakang

Keamanan website saat ini menjadi salah satu fokus utama, karena website berisi informasi dan data yang sensitif dan berharga bagi pemilik website. Jika website memiliki tingkat keamanan yang buruk, maka website akan menjadi sasaran empuk para peretas yang tidak bertanggung jawab dan informasi serta data yang ada di dalamnya dapat digunakan secara tidak semestinya. Saat ini banyak instansi pendidikan seperti universitas, maupun sekolah-sekolah, yang menjadi sasaran para peretas, seperti Website SMAN 1 Kota Sukabumi Sempat Diretas, Jadi Iklan Judi Online, Website yang semula berisikan informasi seputar SMAN 1 Kota Sukabumi, dijadikan iklan promosi judi online [1]. Sebelumnya Website Sekolah Vokasi Universitas Gadjah Mada (UGM) mengalami peretasan, sang *hacker* juga meninggalkan pesan di situs sekolah vokasi UGM [2]. Isinya juga masih menyuarakan soal pelecehan seksual. Hal tersebut dapat terjadi karena masih kurangnya keamanan pada website yang digunakan sebagai sarana informasi di dunia pendidikan, salah satunya adalah SDN 9 Bantan yang menggunakan teknologi informasi seperti website, website SDN 9 Bantan adalah sebuah website yang menyajikan informasi seputar kegiatan belajar-mengajar di SDN 9 Bantan.

Berdasarkan permasalahan tersebut beberapa peneliti telah melakukan penelitian sebelumnya yang berjudul Analisis Keamanan Website Sistem Informasi Administrasi Kependudukan Menggunakan Metode *Vulnerability Assesment*. Penelitian ini bertujuan untuk merekomendasikan perbaikan kerentanan untuk meminimalkan lubang keamanan yang dimanfaatkan oleh peretas. Pengujian dilakukan menggunakan *kali linux* dan OWASP ZAP. Berdasarkan Hasil pengujian kerentanan pada website tersebut ditemukan adanya 14 kerentanan atau celah diantaranya : 3 *Medium risk* dan 11 *low Risk*, Dan menghasilkan alert diantaranya: *Vulnerability Library*, *X-Frame-Option HeaderNot Set*, *Absence of anti- CSRF Token*, *Cookie Without Samesite Attribute*, *Cookie Without HttpOnly flag*, *Cross-*

Domain java Scrip Source File inclusion, Incomplete or no cache and pragma HTTP Header Set, Secure pages Mixed Content, Server leaks Information Via, X-content-Type-Options Header Missing, Charset mismatch, Information Discosure, Timetamp Discover-Unix. Dan ada 4 level Kerentanan yaitu : *medium, low, high, informational* [3].

Berdasarkan penelitian yang berjudul “Analisis Keamanan Website SMA Negeri 2 Sumbawa Besar Menggunakan Metode *Penetration Testing* (Pentest)”. Pada penelitian tersebut di lakukan beberapa tahapan pengujian yakni *Footprinting, Scanning Fingerprinting, Exploit dan Reporting*. Proses pengujian keamanan website SMA Negeri 2 Sumbawa didapatkan beberapa celah yaitu *Vulnerable JS libraries, missing X-Frame-Options headers, absence of anti-CSRF tokens, cookies without the HttpOnly flag or SameSite attribute, cross-domain JavaScript source file inclusion, incomplete or missing cache-control headers, secure pages containing mixed content, Unix timestamp disclosure, missing X-Content-Type-Options headers, charset mismatches, and information disclosure through sensitive data in URLs or suspicious comments all pose significant security risks that can lead to vulnerabilities such as cross-site scripting (XSS), cross-site request forgery (CSRF), session hijacking, clickjacking, and information leakage*, yang mendeteksi 13 *sub file vulnerability* dengan status *low* dan *medium* . Hasil penelitian tersebut berupa daftar celah kerentanan yang dapat menjadi rekomendasi bagi pihak sekolah dalam perbaikan keamanan website [4] .

Berdasarkan penelitian yang berjudul “Audit Web E-Government Dengan *Acunetix Web Vulnerability* Guna Menganalisis Dan Perbaikan Celah Keamanan Website”, pada penelitian tersebut menggunakan *tools acunetix web vulnerability*. Penelitian ini bertujuan untuk melakukan audit *web e- government*, langkah-langkah analisis keamanan *e-government* dan memberikan rekomendasi perbaikan dari hasil analisis keamanan menggunakan *acunetix web vulnerability* pada website DPMPTSP Kota Padang. Dari penelitian tersebut diperoleh dengan menggunakan *tools acunetix web vulnerability* memperoleh laporan dari proses uji penetrasi yang berisi informasi tentang kerentanan keamanan yang ditemukan pada website SINOPEN <https://nonperizinan.web.dpmpptsp.padang.go.id/sinopen>. Temuan

kerentanan sebanyak 148 data berada pada level high, 107 data berada pada level medium, 16 data berada pada level low. Beberapa diantaranya serangan yang ditemukan sebanyak 11 serangan yaitu Blind sql injection, Cross site scripting (xss), Sql injection, Application error message, HTML form without CSRF protection, Clickjacking: X-Frame-Option Header Missing, Cookie Without Secure Flag Set, File Upload, Login Page Password-Guessing Attack, Broken Links, Password Type Input With Auto-Complete Enabled [5].

Berdasarkan penelitian yang telah dilakukan sebelumnya masih ada beberapa faktor yang dapat mempengaruhi keamanan dari sebuah website. Oleh sebab itu penelitian terkait analisa dan perbaikan keamanan pada website SDN 9 Bantan menjadi satu hal yang penting dan harus dilakukan. Penelitian ini bertujuan untuk mengetahui tingkat keamanan website dan memberikan perbaikan pada celah-celah keamanan pada website yang telah ditemukan.

1.2 Permasalahan

Keamanan website saat ini menjadi salah satu fokus utama, karena website berisi informasi dan data yang sensitif dan berharga bagi pemilik website. Jika website memiliki tingkat keamanan yang buruk, maka website akan menjadi sasaran empuk para peretas yang tidak bertanggung jawab dan informasi serta data yang ada di dalamnya dapat digunakan secara tidak semestinya. Saat ini banyak instansi pendidikan seperti universitas, maupun sekolah-sekolah, yang menjadi sasaran para peretas, seperti Website SMAN 1 Kota Sukabumi Sempat Diretas, Jadi Iklan Judi Online, Website yang semula berisikan informasi seputar SMAN 1 Kota Sukabumi, dijadikan iklan promosi judi online [1]. Sebelumnya Website Sekolah Vokasi Universitas Gadjah Mada (UGM) mengalami peretasan, sang hacker juga meninggalkan pesan di situs sekolah vokasi UGM [2]. Isinya juga masih menyuarakan soal pelecehan seksual. Hal tersebut dapat terjadi karena masih kurangnya keamanan pada website yang digunakan sebagai sarana informasi di dunia pendidikan, salah satunya adalah SDN 9 Bantan yang menggunakan teknologi informasi seperti website, website SDN 9 Bantan adalah sebuah website yang menyajikan informasi seputar kegiatan belajar-mengajar di SDN 9 Bantan.

1.3 Batasan Masalah

Batasan masalah dari penelitian ini adalah analisa dan perbaikan keamanan berdasarkan daftar perbaikan celah keamanan, setelah melakukan analisa kerentanan menggunakan *tools OWASP ZAP dan Mozilla Observatory*.

1.4 Tujuan

Tujuan dari penelitian ini adalah untuk melakukan analisa dan perbaikan dari sisi keamanan website agar dapat mengetahui tingkat keamanan website dan memberikan perbaikan pada celah-celah keamanan yang ditemukan pada website SDN 9 Bantan.

1.5 Manfaat

Adapun manfaat dari penelitian ini adalah sebagai berikut:

1. Dapat mengetahui tingkat keamanan website: Pada Saat penelitian ini dilakukan diharapkan dapat mengetahui tingkat keamanan atau seberapa aman website tersebut.
2. Dapat memperbaiki celah keamanan: Pada saat penelitian ini dilakukan diharapkan dapat memperbaiki celah keamanan yang ditemukan pada saat menganalisa keamanan website.

1.6 Sistematika Penulisan

Sistematika penulisan dalam skripsi ini yaitu meliputi:

Bab 1 Pendahuluan

Pada Bab 1 membahas tentang latar belakang, permasalahan, tujuan, manfaat dan sistematika penulisan skripsi ini.

Bab 2 Kajian Pustaka

Pada Bab 2 membahas tentang deskripsi masalah, teori penunjang, dan penelitian terkait mengenai penelitian ini.

Bab 3 Desain Sistem

Pada Bab 3 membahas desain solusi, desain sistem, dari tahapan penelitian yang akan dilakukan.

Bab 4 Eksperimen dan Analisis

Pada Bab 4 berisi eksperimen atau percobaan dan analisis hasil eksperimen dari penelitian yang dilakukan.

Bab 5 Penutup

Pada Bab 5 yaitu berisi penutup kesimpulan dan saran dari hasil penelitian.