ANALISIS KEAMANAN *WEBSITE* DENGAN *INFORMATION SYSTEM SECURITY ASSESSMENT FRAMEWORK* (ISSAF) DAN *OPEN WEB APPLICATION SECURITY PROJECT* (OWASP)

WEBSITE SECURITY ANALYSIS WITH INFORMATION SYSTEM SECURITY ASSESSMENT FRAMEWORK (ISSAF) AND OPEN WEB APPLICATION SECURITY PROJECT (OWASP)

Verseveranda Setyo Nugroho [1], Febrian Wahyu Christanto [2]*

[1] [2] Program Studi Teknik Informatika, Universitas Semarang
Jl Soekarno Hatta Semarang
Email : verseverandasn@gmail.com [1], febrian.wahyu.christanto@*usm.ac.id* [2]

Abstrak

Meningkatnya penggunaan platform digital dalam setiap kegiatan manusia memunculkan kembali perhatian yang pada dasarnya diperlukan di setiap aktifitas atau hal yang dikerjakan manusia, seperti keamanan. Keamanan juga tentu saja hadir dalam kegiatan yang sudah terdigitalisasi atau dapat disebut juga sebagai Cybersecurity. Keamanan dalam Cybersecurity penting karena berkaitan dengan data pribadi (Privacy), integritas (Integrity), akses atau verifikasi (Authentication), kerahasiaan (Confidentiality) dan ketersediaan (Availability). DiamantePro Digital Creative bertempat di Jakarta adalah perusahaan platform digital yang menyediakan jasa undangan atau Invitation seperti undangan pernikahan, meeting internal maupun seminar. Pada dasarnya undangan memerlukan adanya identitas pribadi dari individu yang akan diundang. Maka dari itu untuk melindungi data pengguna dari kebocoran data identitas, DiamantePro Digital Creative memerlukan adanya pengujian penetrasi melalui website mereka. Metode penetrasi tingkat keamanan website dapat menggunakan Information Systems Security Assessment Framework (ISSAF) dan Open Web Application Security Project (OWASP). Hasil pengujian membuktikan bahwa website diaundangkamu.com tidak dapat ditembus karena memiliki fitur security yang mumpuni seperti Naga Cyber Defense dari hostingan rumahweb.com.

Kata kunci: *Pengujian Penetrasi, ISSAF, OWASP*

Abstract

The increasing usage of digital platform in every aspects of humans activities reemerged the fundamental concerns which needed in every actions or human's works, such as security. Security also present in the digital version of activities which could be called by Cybersecurity. The importance of security in Cybersecurity is connected to privacy, integrity, authentication, confidentiality, and availability. DiamantePro Digital Creative located at Jakarta is a digital platform company who provide invitation service such as wedding invitation, internal meeting or seminaries. In the basic concept of invitation, it needed private identity from the invited individu. Therefore to protect user's data from identity data leaks, DiamantePro Digital Creative needs to conduct a penetration test through their websites. Penetration methods of website security level may use Information Systems Security Assessment Framework (ISSAF) and Open Web Application Security Project (OWASP) The test results prove that diaundangkamu.com website is impenetrable because it has qualified security features such as Naga Cyber Defense from hosting rumahweb.com.

Keywords : *Penetration Testing, ISSAF, OWASP*

1. PENDAHULUAN

Di era teknologi yang semakin pesat, membuat banyak kemudahan bagi masyarakat umum. Teknologi *Website* adalah salah satu alternatif yang paling banyak digunakan, untuk membantu bisnis atau mendapatkan informasi yang orang butuhkan [1]. Jumlah pengguna internet yang semakin meningkat namun tidak diimbangi dengan adanya sumber daya manusia atau administrator jaringan yang mumpuni di bidangnya akan menjadi ancaman kejahatan dunia maya [2][3]. Keamanan teknologi informasi penting karena berkaitan dengan data pribadi (*privacy*) integritas (*integrity*) akses atau verifikasi (*authentication*), kerahasiaan (*confidentiality*), dan ketersediaan (*availability*) [4][5].

Pengujian penetrasi adalah proses pengujian dari sebuah organisasi atau instansi dengan tujuan untuk mencari celah keamanan dan kelemahan yang disetujui oleh pihak organisasi tersebut [6]. Terdapat beberapa metode pengujian penetrasi yang memenuhi kebutuhan pengujian peretasan *website*, diantaranya adalah metode ISSAF (*Information System Security Assessment Framework*), OSSTMM (*Open Source Security Testing Methodology Manual*) , NIST SP 800-115, OISSG *(Open Informaftion System Security Group*), yang dikeluarkan oleh owasp.org sebuah organisasi nonprofit yang berdedikasi pada keamanan aplikasi berbasis *web* [7][8]. Metode-metode tersebut digunakan untuk pengujian keamanan suatu *website* [9].

Saat pandemi tahun 2020, DiamantePro Creative ingin mengikuti pekembangan jaman teknologi yaitu membangun *website* undangan digital bernama diaundangkamu.com. Undangan tersebut memiliki bermacam-macam tujuan antara lain pernikahan, seminar, rapat internal, maupun sidang. *Platform website* diaundangkamu.com memiliki *database* yang memuat informasi mengenai tamu undangan diantaranya nama, alamat, dan nomor telepon genggam sehingga dapat menjadi incaran para oknum yang tidak bertanggung jawab.

Untuk mengetahui hal tersebut dibutuhkan pengujian penetrasi celah keamanan berupa *External Network Penetration Testing* pada *website* milik DiamantePro Digital Creative. *External Network Penetration Testing* mengacu pada penyerangan atau peretasan batasan terluar jaringan organisasi melalui *internet* atau *extranet* menggunakan tidak adanya informasi ataupun adanya informasi penuh mengenai *website* yang akan diuji [10][11]. Pengujian penetrasi ini menggunakan metode penetrasi *Information Systems Security Assessment Framework* (ISSAF) dan *Open Web Application Security Project* (OWASP) sebagai bentuk analisa dalam mencari dan mengetahui kekurangan serta meningkatkan sistem keamanan pada *website* diaundangkamu.com.

2. DASAR TEORI

2.1 Analisa Keamanan *Website*

Pengertian dari Analisa Keamanan *Website* yang menjadi judul dari penelitian ini adalah kegiatan mengurai, membedakan dan memilah sistem keamanan digital dari teknologi sebuah aplikasi *web* atau *website*. Hal ini perlu dilakukan agar *website* yang rilis nantinya dapat berjalan dengan baik dan meminimalisasikan isu terhadap peretasan suatu *website*.

2.2 Metode ISSAF

Information System Security Assessment Framework atau ISSAF adalah kerangka kerja pengujian penetrasi yang dikembangkan oleh lembaga *Open Information System Security Group* (OISSG) [12] [13]. Fase dalam metode ini meliputi *Information Gathering* yang merupakan proses mendapatkan informasi dari suatu *website* yang akan diperiksa keamanannya. Kemudian dilanjutkan pada fase *Assessment* yang merupakan pemeriksaan terhadap lubang-lubang keamanan *website* yang rentan terhadap isu peretasan. Fase terakhir dari metode ini adalah *Clean-Up and Destroy* merupakan tahapan dalam mengakomodasi lubang-lubang keamanan yang terindikasi lemah terhadapan peretasan [14].

Informasi yang terkumpul dari fase-fase dalam metode ISSAF ini dapat menjadi rekomendasi *programmer website* dalam membuat keamanan yang lebih baik terhadap *website* yang akan dirilis.

2.3 Metode OWASP

Open Web Application Security Project atau OWASP adalah pendekatan sederhana untuk menghitung dan menilai resiko yang terkait dengan aplikasi [15]. Metode ini memiliki tahapan yang antara lain adalah *footprinting*, *scanning fingerprinting and enumeration*, *exploit*, dan *reporting*. Tahapan-tahapan tersebut dilakukan untuk mengetahui tingkat keamanan dari suatu *website* yang akan dirilis.

2.4 OWASP *Top* 10

OWASP *Top* 10 merupakan projek keamanan digital dengan OWASP sebagai sponsor utamanya [16]. Projek keamanan digital ini menyajikan tren celah kerentanan dari apa yang dianggap sebagai sepuluh serangan aplikasi *website* pada tiap-tiap tahun. OWASP Top 10 adalah standar keamanan untuk *website* baru ataupun lama yang menyediakan daftar *checklist* keamanan. Data serangan yang didapatkan adalah data dari perusahaan mitra OWASP. OWASP atau *pen testing* mampu mengidentifikasi dan mengatasi kerentanan sebelum terjadi peretasan. Uji penetrasi OWASP dapat membantu mengurangi pelanggaran data, meningkatkan pengembangan perangkat lunak, dan metodologi yang berkualitas [17]. Metode ini membantu perusahaan atau *programmer* mengembangkan *website* yang berorientasi pada masa depan dan aman. Beberapa standar dari OWASP Top 10 pada tahun 2021 antara lain adalah :

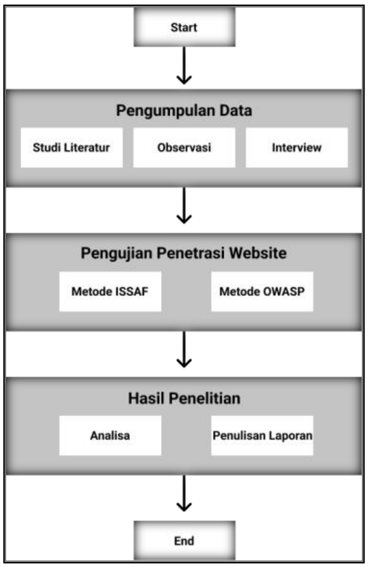
a) A01:2021 *Broken Access Control* (Kelemahan Access Control)
b) A02:2021 *Cryptographic Failures* (Kegagalan Kriptografi)
c) A03:2021 *Injection* (Injeksi)
d) A04:2021 *Insecure Design* (Kekurangan pada Desain)
e) A05:2021 *Security Misconfiguration* (Kelemahan Konfigurasi Keamanan)
f) A06:2021 *Vulnerable and Outdated Components* (Komponen yang rentan dan kadaluarsa)
g) A07:2021 *Identification and Authentication Failures* (Kegagalan Identifikasi dan Autentikasi)
h) A08:2021 *Software and Data Integrity Failures* (Kegagalan Perangkat Lunak dan Keutuhan Data)
i) A09:2021 *Security Logging and Monitoring Failures* (Kegagalan pada Keamanan *Logging* dan *Monitoring* Data)
j) A10:2021 *Server-Side Request Forgery* (SSRF)

2.5 *Black Box Penetration Testing*

Teknik *Black Box Penetration Testing* adalah pengujian penetrasi dimana penguji penetrasi tersebut tidak memiliki informasi atau ide apapun mengenai target yang berupa sistem [18]. Teknik ini dilakukan dengan mencoba seluruh menu ataupun fitur di dalam *website*. Fitur-fitur yang berhasil dan bermasalah menimbulkan kerentanan suatu *website* akan dicatat dan dilaporkan menjadi suatu data yang dapat digunakan *programmer* dalam memperbaiki *website*.

3. METODOLOGI PENELITIAN

Penelitian ini yang berjudul "Analisis Keamanan *Website* dengan *Information System Security Assesment Framework* (ISSAF) dan *Open Web Application Security Project* (OWASP)" dilaksanakan dengan menggunakan alur dan rincian sebagai berikut dalam Gambar 1 :



Gambar 1. Alur Penelitian

Penjelasan alur penelitian yang ditunjukkan pada Gambar 1 adalah sebagai berikut :

3.1 Pengumpulan Data

Dalam penelitian ini, penulis menggunakan beberapa metode dalam mengumpulkan data yang rinciannya sebagai berikut :

3.1.1 Observasi

Observasi dilakukan ke *website* diaundangkamu.com milik DiamantePro Digital Creative untuk dapat menganalisa kebutuhan data yang diperlukan dalam pengujian sistem keamanan. Data yang didapatkan meliputi IP *address*, *platform* penyedia jasa, dan *hosting website*.

3.1.2 *Interview*

Wawancara dilakukan kepada pemilik perusahaan DiamantePro Digital Creative dengan tujuan untuk mendapatkan informasi lebih lanjut mengenai kebutuhan data informasi yang sensitif pada *website* diaundangkamu.com.

3.1.3 Studi Literatur

Studi literatur terhadap pustaka-pustaka membantu kebutuhan untuk penelitian analisa *website* diaundangkamu.com milik DiamantePro Digital Creative diantaranya buku ilmiah, jurnal penelitian, artikel penelitian, dan dokumentasi teknologi.

3.1.4 Perolehan Data

Penelitian ini mengumpulkan data dari masing-masing teknik yaitu observasi, *interview*, dan Studi Literatur. Data tersebut dibagi jenisnya menjadi 2 (dua) yaitu:

a. Data Primer

Data primer adalah data yang dibutuhkan dalam penelitian ini untuk keperluan analisis dan penetrasi *website*. Data Primer didapatkan dari Diamante Pro Digital Creative diantaranya alamat dari *website* Diamante Pro Digital Creative. Dari alamat itu penulis mencari informasi dengan bantuan alat Nmap atau *whois* untuk mendapatkan IP *address, DNS,* serta *Web Framework* yang digunakan pada sistem *web* diaundangkamu.com.

b. Data Sekunder

Data sekunder adalah data yang dibutuhkan penulis dalam keperluan penulisan laporan. Data sekunder didapatkan dari jurnal penelitian, buku pedoman, serta artikel teknologi berupa pedoman dalam pengujian penetrasi *website*, langkah-langkah dalam penggunaan metode ISSAF dan OWASP serta referensi penelitian hingga metode penelitian.

3.2 Pengujian Penetrasi *Website*

Alur dalam melakukan pengujian penetrasi ini menggunakan 2 (dua) metode yaitu ISSAF dan OWASP yang didalamnya terdapat beberapa tahap yang akan dilakukan dengan metode-metode tersebut. *Tools* yang digunakan akan dijabarkan dibawah ini :

3.2.1 Metode ISSAF

Penulis menggunakan metode ISSAF dengan kerangka kerja pengujian penetrasi dan tools yang dijelaskan melalui tahapan metode ISSAF, diperlihatkan pada Tabel 1 :

Tabel 1. *Tahapan Metode ISSAF*

No.	Tahapan	*Act*	*Tools*
1.	*Information Gathering*	*Network Mapping, Information Gathering*	*Whois, SSLlabs, Nmap*

2.	*Assessment*	*Vulnerability Scanning, Penetration, SQL Injection*	*Nikto, SQLmap*
3.	*Clean-Up and Destroy*	*Analysis, Reporting, Log Clearing*	*Word, Auto Generated (HTML)*

3.2.2 Metode OWASP

Pengujian penetrasi kedua dilakukan dengan menggunakan tahapan metode OWASP. Adapun parameter celah kerentanan berdasarkan OWASP *Top* 10 tahun 2021 terdapat pada Tabel 2 dibawah ini:

Tabel 2. *OWASP Top 10 2021*

No.	Kode Nama	Nama Celah
1.	A01:2021	*Broken Access Control*
2.	A02:2021	*Cryptographic Failures*
3.	A03:2021	*Injection*
4.	A04:2021	*Insecure Design*
5.	A05:2021	*Security Misconfiguration*
6.	A06:2021	*Vunerable and Outdated Components*
7.	A07:2021	*Identification and Authentication Failures*
8.	A08:2021	*Software and Data Integrity Failures*
9.	A09:2021	*Security Logging and Monitoring Failures*
10.	A10:2021	*Server-Side Request Forgery* (SSRF)

Tahapan dan *tools* yang digunakan dalam masing-masing tahapan diperlihatkan pada Tabel 3 :

Tabel 3. *Tahapan OWASP dan Tools yang Digunakan*

No.	Tahapan	*Tools*
1.	*Foot Printing*	*Whois, netcraft, owaspzap*
2.	*Scanning Finger Printing and Enumeration*	Owaspzap
3.	*Exploit*	Owaspzap
4.	*Reporting*	Manual, *screenshot*

3.3 Hasil Penelitian

Tahap terakhir adalah menganalisa hasil dari pengujian penetrasi *website* yang terletak pada bagian pengujian dan pembahasan.

4. PENGUJIAN DAN PEMBAHASAN

4.1 Metode ISSAF

a. *Planning and Preparation*

Pada tahap ini dilakukan pencarian informasi terhadap *website* yang akan diteliti yaitu diaundangkamu.com menggunakan aplikasi *whois.domaintools* terlihat pada Gambar 2 :

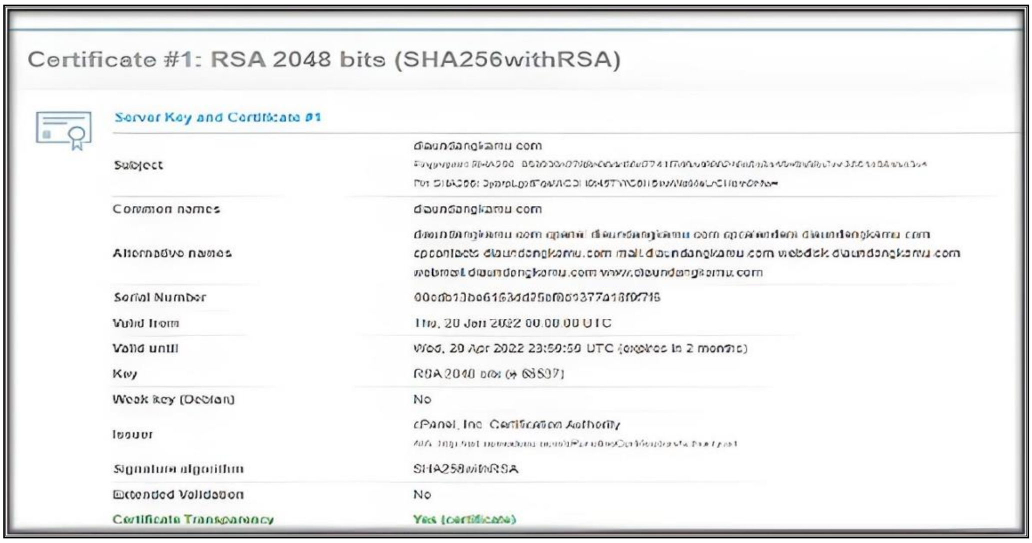
WhoIs Record for DiaUndangKamu.com

— Domain Profile

Registrant	Domain Data Guard
Registrant Org	Domain Data Guard
Registrant Country	id
Registrar	CV. Rumahweb Indonesia IANA ID: 1675 URL: https://www.rumahweb.com,http://www.rumahweb.com Whois Server: whois.rumahweb.com abuse@rumahweb.co.id (p) 62274082257
Registrar Status	ok
Dates	336 days old Created on 2021-02-19 Expires on 2022-02-19 Updated on 2021-02-20
Name Servers	NS1.RUMAHWEB.COM (has 133,062 domains) NS2.RUMAHWEB.COM (has 133,062 domains) NS3.RUMAHWEB.NET (has 435 domains) NS4.RUMAHWEB.NET (has 435 domains)
Tech Contact	Domain Data Guard PO Box 404 Yogyakarta - Visit domaindataguard.com to contact the domain registrant/owner, Yogyakarta, Yogyakarta, 55000, id noreply@domaindataguard.com (p) 6282242220053
IP Address	103.253.212.243 - 536 other sites hosted on this server
IP Location	- Jakarta Raya - Jakarta - Pt Digital Registra Indonesia
ASN	AS58487 RUMAHWEB-AS-ID Rumahweb Indonesia CV., ID (registered Dec 21, 2011)
Domain Status	Registered And Active Website
IP History	3 changes on 3 unique IP addresses over 1 years
Registrar History	1 registrar
Hosting History	1 change on 2 unique name servers over 1 year

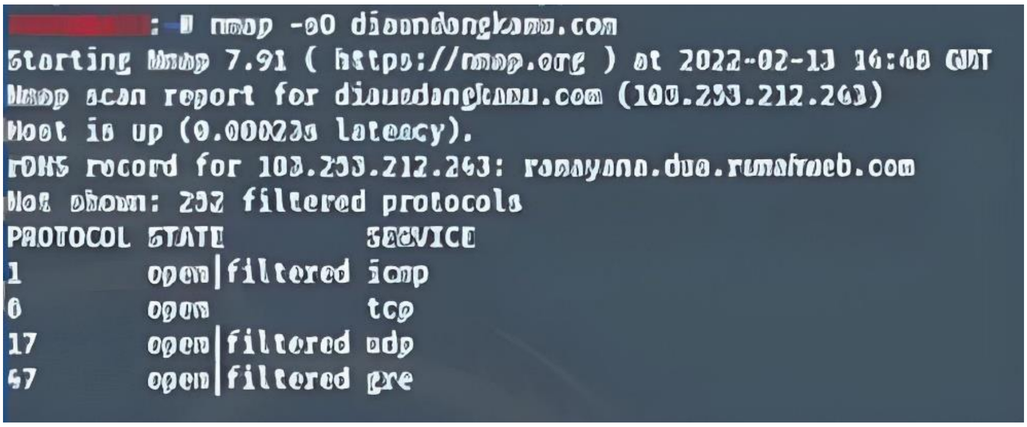
Gambar 2. *Information Gathering dengan Whois*

Pada Gambar 2 bagian registrant dilindungi oleh *Domain Data Guard*. Pada Tahap ini peneliti mencari sertifikat *Secure Socket Layer* (SSL*)* dan *Transport Layer Security* (TLS) yang dimiliki oleh *website* diaundangkamu.com berikut hasi dari pencari peneliti dengan menggunakan *sslabs* yang terlihat pada Gambar 3 :



Gambar 3. *SSL Ceritifcate diaundangkamu.com*

Pada Gambar 3, dapat terlihat *fingerprint* pada *website* diaundangkamu.com. Pada Tahap ini peneliti melihat *port* TCP yang terbuka pada *web* diaundangkamu.com dengan menggunakan *tool* Nmap. Berikut hasil *scan* dengan Nmap pada Gambar 4 :



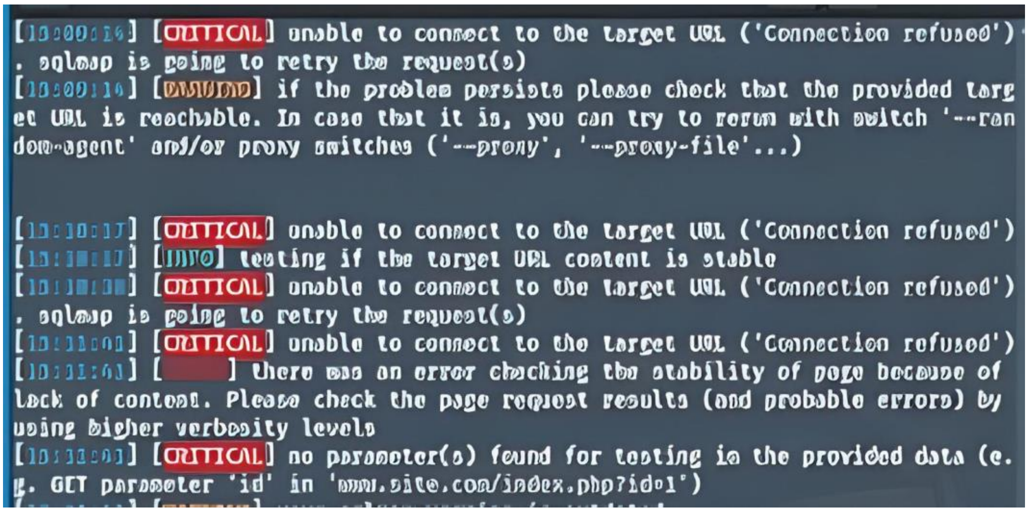
Gambar 4. *Network Mapping dengan Nmap*

b. *Assessment*

Pada tahap ini peneliti menggunakan *tool nikto* yang berfungsi sebagai *scanning* celah keamanan pada *website* diaundangkamu.com. akan tetapi peneliti tidak bisa meninjau lebih lanjut dikarenakan jaringan *internet* terblokir oleh *firewall* yang dimiliki oleh diaundangkamu.com. Berikut hasil *scanning* dengan *tool* Nikto pada Gambar 5 :

Gambar 5. *Vulnerability Scanning dengan Nikto*

Dalam tahap ini dilakukan pengujian apakah *website* ini terdapat kerentanan kepada *SQL Injection* dengan menggunakan *tool* yaitu *SQLmap*. Akan tetapi peneliti tidak bisa mendapatkan *database* dari diaundangkamu.com disebabkan jaringan peneliti sudah terblokir dengan *Firewall* yang dimiliki diaundangkamu.com. Berikut dijelaskan pada Gambar 6 :



Gambar 6. *Hasil Scanning dengan SQL Map*

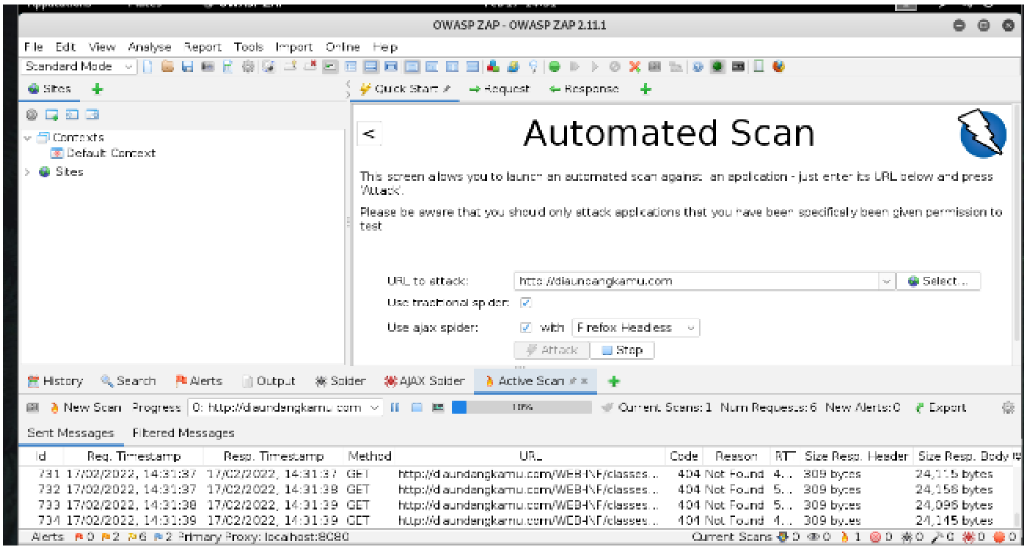
Hasil *scanning* yang telah dilakukan pada Gambar 6 berisi tentang beberapa akses yang berhasil ditolak oleh *website* yang diuji, dari hasil *scanning* dengan SQL Map didapatkan hasil bahwa *website* diaundangkamu.com tidak memiliki kerentanan dalam pencurian *database* sehingga bisa dijelaskan bahwa *website* ini termasuk dalam kategori aman terhadap peretasan.

c. *Clean-Up and Destroy*

Pada saat laporan dari peneliti sudah diterima dan dikonfirmasi oleh pemilik, semua data *log* pencarian dan temuan akan dihapus.

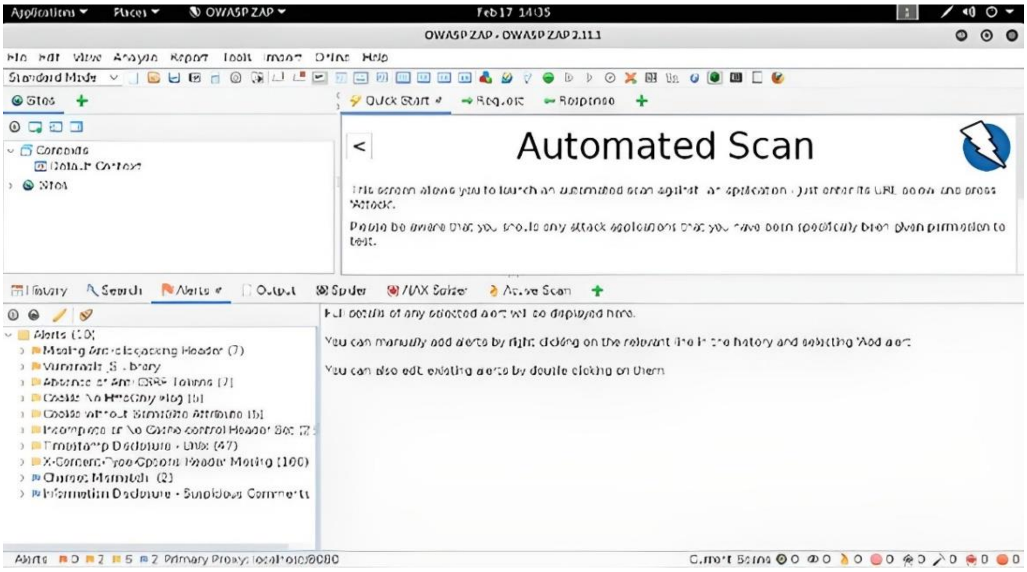
4.2 Metode OWASP

OWASPZAP secara otomatisasi meninjau kerentanan dan melakukan Ajax *Attack* terhadap *website* yang sedang diuji. Dikarenakan bagian *foot printing* peninjauan dan *tools* sama dengan menggunakan metode ISSAF, peneliti tidak menyantumkan lagi di tahap ini. Berikut Gambar 7 proses *scanning* dengan OWASPZAP :



Gambar 7. *Proses Scanning OWASPZAP*

Setelah berhasil mendapatkan informasi melalui proses *scanning* pada Gambar 7, dilanjutkan dengan proses menyerang dengan OWASPZAP yang ditunjukkan pada Gambar 8.



Gambar 8. *Attack dengan OWASPZAP*

Berdasarkan Gambar 7 dan Gambar 8 tentang hasil pengujian OWASPZAP terdapat kerentanan pada *Broken Access Control* yang memiliki kerentanan sedang, *Software and Data Integrity Failures* yang memiliki kerentanan rendah, *Vulnerable and Outdated Components* yang memiliki kerentanan rendah, dan *Security Misconfiguration* yang memiliki kerentanan sedang.

4.3 *Black Box Penetration Testing*

Implementasi *Black Box Penetration Testing* pada metode ISSAF ditunjukkan pada Tabel 4 dibawah ini:

Tabel 4. *Black Box Pentest ISSAF*

No.	Tahapan	*Tools*	Hasil
1.	*Information Gathering*	*Whois, Netcraft*	Berhasil
2.	*Network Mapping*	*Nmap*	Berhasil
3.	*Vulnerability Scanning*	*Nikto*	Berhasil
4.	*Injection*	*SQLmap*	Berhasil

Sedangkan implementasi *Black Box Penetration Testing* pada metode *OWASP* ditunjukkan pada Tabel 5:

Tabel 5. *Black Box Pentest OWASP*

No.	*Alerts*	Kode Nama	Hasil
1.	*Missing Anti-Clickjacking Header*	OWASP _2021_ A05	Berhasil
2.	*Vulnerable Js Library*	OWASP _2021_ A06	Berhasil

No.	*Alerts*	Kode Nama	Hasil
3.	*Absence of Anti-CSRF Tokens*	OWASP _2021_ A01	Berhasil
4.	*Cookie No HTTP Only Flag*	OWASP _2021_ A05	Berhasil
5.	*Cookie Without Samesite Attribute*	OWASP _2021_ A01	Berhasil
6.	*Incomplete or No Cache-Header Set*	-	Berhasil
7.	*Timestamp Disclouser Unix*	OWASP _2021_ A01	Berhasil
8.	*X-Content-Type-Options Header Missing*	OWASP _2021_ A05	Berhasil
9.	*Charset Mismatch*	-	Berhasil
10.	*Information Disclosure-Suspicious Comments*	OWASP _2021_ A01	Berhasil
11.	*SQL Injection*	OWASP _2021_ A03	Tidak Berhasil

Berdasarkan aspek keamanan *CIA TRIAD* yaitu kerahasiaan, integrasi, dan ketersediaan menunjukkan bahwa *website* diundangkamu.com memiliki keamanan yang baik di ketiga aspek tersebut, namun hanya aspek keamanan integrasi yang sedikit kurang terpenuhi karena adanya *X-Frame Option Header* yang ditemukan oleh alat *Nikto* dan *OWASPZAP* tidak diatur sedemikian rupa sehingga memungkinkan *iframe* dimuat dengan mudah di situs *web* lain yang dapat merusak integritas informasi. Keamanan *website* diaundangkamu.com sangat baik karena menggunakan *hosting* berbayar yang dimana memiliki banyak keunggulan. *Cyber Defense* fitur yang disediakan perusahaan penyedia layanan *hosting* dapat pula digunakan karena sangat mumpuni memberikan proteksi keamanan *cyber* seperti serangan virus, *malware*, *ransomware*, dan berbagai bentuk ancaman baru. *LiteSpeed server* yang dimiliki diaundangkamu.com sangatlah responsif dan cepat untuk diakses dibuktikan dari hasil uji penetrasi yang telah dilakukan hal ini dapat diperiksa pada *website* https://openlitespeed.org/. Untuk *Injection* dengan menggunakan *tools SQLmap* tidak bisa dilakukan bahkan pada bagian *Vulnerability Scanning* dengan *Nikto*. Kemudian dengan OWASPZAP didapatkan informasi untuk melihat celah keamanan yang dimiliki *website* diaundangkamu.com walaupun hanya sebatas *level medium – informational* yang memiliki pengaruh sedikit untuk menembus *database* dari *website* diundangkamu.com.

5. KESIMPULAN

Berdasarkan hasil pengujian penetrasi pada *website* diaundangkamu.com, maka dapat mengambil kesimpulan berdasarkan pengujian menggunakan metode ISSAF dan OWASP bahwa *website* diaundangkamu.com tergolong sangat aman karena tidak mampu untuk ditembus dengan beberapa serangan *cyber*. Fitur *Cyber Defense* yang disediakan penyedia layanan *hosting* memberikan proteksi keamanan *cyber* seperti serangan virus, *malware*, *ransomware*, dan berbagai bentuk ancaman baru. Kerentanan yang sama dilihat dengan metode ISSAF dan OWASP yaitu *Missing Anti-clickjacking Header* yang berdampak pada munculnya tombol atau *link* dari pihak lain yang berisi *trigger* untuk peretasan atau penipuan dan *X-Content-Type-Options Header Missing* yang berdampak pada terjadinya serangan *sniffing* konten hasil dari respon dari *server*. Dengan adanya uji penetrasi ini dapat digunakan sebagai referensi dalam menguji kerentanan suatu *website* terhadap serangan-serangan *cyber* yang sering terjadi sehingga dapat menambah standar keamanan pada *website* yang akan dirilis.

Adapun saran yang dapat diberikan adalah melakukan uji penetrasi tingkat lanjut dengan seorang *pen-tester*. Menggunakan *tools* yang mempunyai tingkat jelajah yang tinggi agar dapat terlihat kerentanan lebih detail lagi dari *website* tersebut.

DAFTAR PUSTAKA

[1] N. A. Mufida, Sudarmiatin, and W. Agung, “The Effectiveness of using the Web for the Promotion of a Car Repair Business to Increase Purchasing Decisions,” *South East Asia J. Contemp. Business, Econ. Law*, vol. 24, no. 4, pp. 35–42, 2021.

[2] M. Muttaqin, “Internet Usage Behavior of the ICT Young Workforce in the Border Region,” *J. Pekommas*, vol. 4, no. 1, p. 11, 2019, doi: 10.30818/jpkm.2019.2040102.

[3] M. Azrour, J. Mabrouki, A. Guezzaz, and A. Kanwal, “Internet of Things Security: Challenges and Key Issues,” *Secur. Commun. Networks*, vol. 2021, no. 5533843, pp. 1–11, 2021, doi: 10.1155/2021/5533843.

[4] A. Rochman, R. R. Salam, and S. A. Maulana, “Analisis Keamanan Website dengan Information System Security Assessment Framework (ISSAF) dan Open Web Application Security Project (OWASP) di Rumah Sakit XYZ,” *J. Indones. Sos. Teknol.*, vol. 2, no. 4, pp. 506–519, 2021.

[5] N. Tariq, F. A. Khan, and M. Asim, “Security Challenges and Requirements for Smart Internet of Things Applications: A Comprehensive Analysis,” *Procedia Comput. Sci.*, vol. 191, pp. 425–430, 2021, doi: 10.1016/j.procs.2021.07.053.

[6] M. Alhamed and M. M. H. Rahman, “A Systematic Literature Review on Penetration Testing in Networks: Future Research Directions,” *Appl. Sci.*, vol. 13, no. 6986, pp. 1–24, 2023, doi: 10.3390/app13126986.

[7] S. U. Sunaringtyas and D. S. Prayoga, “Implementasi Penetration Testing Execution Standard Untuk Uji Penetrasi Pada Layanan Single Sign-On,” *Edu Komputika J.*, vol. 8, no. 1, pp. 48–56, 2021.

[8] S. S. Anelia, Jayanta, and B. Hananto, “Uji Penetrasi Server Universitas PQR Menggunakan Metode National Institute Of Standards And Technology (NIST SP 800-115),” *J. Ilmu Tek. dan Komput.*, vol. 7, no. 1, pp. 35–43, 2023, doi: 10.22441/jitkom.2023.v7i1.005.

[9] D. Dalalana Bertoglio and A. F. Zorzo, “Overview and Open Issues on Penetration Test,” *J. Brazilian Comput. Soc.*, vol. 23, no. 1, pp. 1–16, 2017, doi: 10.1186/s13173-017-0051-1.

[10] I. G. A. S. Sanjaya, G. M. A. Sasmita, and D. M. S. Arsa, “Evaluasi Keamanan Website Lembaga X Melalui Penetration Testing Menggunakan Framework ISSAF,” *J. Ilm. Merpati (Menara Penelit. Akad. Teknol. Informasi)*, vol. 8, no. 2, pp. 113–124, 2020, doi: 10.24843/jim.2020.v08.i02.p05.

[11] A.-D. Tudosi, A. Graur, D. G. Balan, and A. D. Potorac, “Research on Security Weakness

Using Penetration Testing in a Distributed Firewall," *Sensors (MDPI)*, vol. 23, no. 2683, pp. 1–18, 2023.
[12] R. T. Dirgahayu, Y. Prayudi, and A. Fajaryanto, "Penerapan Metode ISSAF dan OWASP versi 4 Untuk Uji Kerentanan Web Server," *J. Ilm. NERO*, vol. 1, no. 3, pp. 190–197, 2015, [Online]. Available: http://nero.trunojoyo.ac.id/index.php/nero/article/download/29/27
[13] I. O. Riandhanu, "Analisis Metode Open Web Application Security Project (OWASP) Menggunakan Penetration Testing pada Keamanan Website Absensi," *J. Inf. dan Teknol.*, vol. 4, no. 3, pp. 160–165, 2022, doi: 10.37034/jidt.v4i3.236.
[14] M. A. Nabila, P. E. Mas'udia, and R. Saptono, "Analysis and Implementation of the ISSAF Framework on OSSTMM on Website Security Vulnerabilities Testing in Polinema," *J. Telecommun. Netw. (Jurnal Jar. Telekomun.*, vol. 13, no. 1, pp. 87–95, 2023, doi: 10.33795/jartel.v13i1.511.
[15] B. Ghozali, K. Kusrini, and S. Sudarmawan, "Mendeteksi Kerentanan Keamanan Aplikasi Website Menggunakan Metode Owasp (Open Web Application Security Project) untuk Penilaian Risk Rating," *Creat. Inf. Technol. J.*, vol. 4, no. 4, p. 264, 2019, doi: 10.24076/citec.2017v4i4.119.
[16] G. H. A. Kusuma, "Implementasi OWASP ZAP Untuk Pengujian Keamanan Sistem Informasi Akademik," *J. Teknol. Inf. J. Keilmuan dan Apl. Bid. Tek. Inform.*, vol. 16, no. 2, pp. 178–186, 2022, doi: 10.47111/jti.v16i2.3995.
[17] Sunardi, I. Riadi, and P. A. Raharja, "Vulnerability Analysis of E-voting Application using Open Web Application Security Project (OWASP) Framework," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 11, pp. 135–143, 2019, doi: 10.14569/IJACSA.2019.0101118.
[18] P. Vats, M. Mandot, and A. Gosain, "A Comprehensive Literature Review of Penetration Testing Its Applications," *ICRITO 2020 - IEEE 8th Int. Conf. Reliab. Infocom Technol. Optim. (Trends Futur. Dir.*, pp. 674–680, 2020, doi: 10.1109/ICRITO48877.2020.9197961.