Jurnal Informasi dan Teknologi

http://www.jidt.org

2022 Vol. 4 No. 4 Hal: 211-218 e-ISSN: 2714-9730

Analisis Keamanan Open Website Menggunakan Metode OWASP dan ISSAF

Rahmad Ashar[1]✉

[1]Independent Researcher

rahmadasr@gmail.com

Abstract

Diskominfo Kerinci is an agency responsible for the management of information media within the Kerinci Regency Government. The existence of a website as a medium of information is a very important need to convey information to the public. This managed website is public (open website) so that information security principles must be applied so as not to get cyber attacks. This study conducted a security analysis on an open website owned by Diskominfo Kerinci using two methods, namely the Open Web Application Security Project (OWASP) method and the Information Systems Security Assessment Framework (ISSAF) method. Research related to the use of the OWASP and ISSAF methods in system security testing has been carried out, several tests state that this method greatly influences the steps and results of system security testing. The results of the security analysis from these two methods will be compared to make recommendations for improvements to the website.

Keywords: Website Security, Attack, OWASP, ISSAF, Penetration Testing.

Abstrak

Diskominfo Kerinci merupakan sebuah instansi yang bertanggung jawab atas pengelolaan media informasi di lingkup Pemerintahan Kabupaten Kerinci. Keberadaan *website* sebagai media informasi menjadi kebutuhan yang sangat penting untuk menyampaikan informasi kepada masyarakat. *Website* yang dikelola ini bersifat publik (*open website*) sehingga prinsip keamanan informasi harus diterapkan agar tidak mendapat serangan *cyber*. Penelitian ini melakukan analisis keamanan pada *open website* milik Diskominfo Kerinci dengan menggunakan dua metode yaitu metode *Open Web Application Security Project* (OWASP) dan metode *Information Systems Security Assessment Framework* (ISSAF). Penelitian terkait penggunaan metode OWASP dan ISSAF dalam pengujian keamanan sistem telah banyak dilakukan, beberapa pengujian menyebutkan bahwa metode ini sangat berpengaruh terhadap langkah dan hasil dari pengujian keamanan system. Hasil analisis keamanan dari dua metode ini akan dibandingkan untuk dijadikan rekomendasi perbaikan pada *website*.

Kata kunci: Keamanan Website, Serangan, OWASP, ISSAF, Penetration Testing.

JIDT is licensed under a Creative Commons 4.0 International License.

1. Pendahuluan

Keamanan siber telah muncul sebagai salah satu masalah paling kritis belakangan ini karena fakta bahwa hampir semua orang di dunia tersentuh oleh pengaruh Internet. Data pribadi orang-orang yang dibagikan melalui *World Wide Web* sangat besar berkat formulir yang mereka isi saat memanfaatkan layanan apa pun yang ditawarkan oleh pemerintah, perusahaan, atau organisasi amal. Ancaman keamanan siber tampak besar baik dari penjaga data pribadi pengguna dan peretas yang ada di luar sana untuk memanfaatkan celah dalam sistem dan proses untuk mencuri informasi penting dan merusak kekayaan dan ketenangan pikiran orang-orang melalui kegiatan peretasan [1].

Ancaman yang timbul dalam suatu sistem disebabkan oleh kesalahan yang muncul pada saat mendesain dan mengembangkan sistem. Beberapa pihak yang tidak bertanggung jawab memanfaatkan kerentanan sistem tersebut untuk melakukan serangan seperti defacing, phising, denial of service, bruteforce attack dan lain sebagainya. Pada awal tahun 2020 lalu berdasarkan data dari kaspersky, terdapat beberapa fasilitas dan situs vital yang menangani covid-19 menjadi target serangan di Indonesia. Menurut Badan Siber dan Sandi Negara (BSSN) mencatat bahwa pada awal tahun 2020 terdapat 88 juta serangan siber yang menyerang fasilitas negara dan non negara seperti industri dan kesehatan. Jumlah ini meningkat dari tahun sebelumnya yaitu 1,9 juta serangan [2].

Perubahan yang sangat cepat, kadang meluputkan developer dalam melakukan pengujian keamanan terhadap aplikasi yang dibangun. Pengujian merupakan proses yang sangat penting didalam pengembangan perangkat lunak yang berkualitas tinggi, karena dari beberapa kesalahan yang dianggap tidak penting beresiko sangat berbahaya hal ini menjadi celah bagi attacker untuk memanfaatkan informasi yang di curi melalui serangan kepada sistem [3].

Diterima: 07-09-2022 | Revisi: 07-10-2022 | Diterbitkan: 31-12-2022 | doi: 10.37034/jsisfotek.v4i4.233

Dinas Komunikasi dan Informatika (Diskominfo) Kabupaten Kerinci adalah sebuah instansi yang bertanggung jawab atas pengelolaan media informasi di lingkup Pemerintahan Kabupaten Kerinci. Keberadaan website sebagai media informasi menjadi kebutuhan yang sangat penting untuk menyampaikan informasi kepada masyarakat.

Dengan adanya website, informasi dan komunikasi antara pemerintah dengan masyarakat bisa dilakukan via internet. Banyak manfaat dari website yang digunakan di bidang pemerintahan diantaranya: sebagai media penyampaian informasi resmi, memudahkan penyampaian aspirasi masyarakat, mempermudah masyarakat mendapatkan akses pelayanan publik, memudahkan sistem administrasi, menjadi media promosi, mendukung keterbukaan informasi, dan sebagainya.

Namun dengan semakin banyaknya fasilitas website yang disediakan untuk mendukung program kerja Diskominfo Kabupaten Kerinci dalam melayani masyarakat, ancaman akan kejahatan dunia maya pun menjadi salah-satu masalah yang harus dihadapi secara seksama. Website memiliki kerentanan yang bervarian. Kerentanan ini cukup berbahaya berhubung informasi dan data yang dimiliki suatu instansi pemerintah khususnya Diskominfo Kabupaten Kerinci tidak semuanya bersifat terbuka.

Penggunaan sistem informasi terkadang memiliki kelemahan pada aspek keamanan yang dapat dimanfaatkan oleh oknum tertentu. Keamanan informasi menjadi tantangan utama di era perkembangan informasi seperti saat ini. Mencegah hal tersebut terjadi, perlu dilakukan evaluasi keamanan sebagai upaya menemukan kelemahan dan celah keamanan dari suatu sistem yang dapat menjadi bahan rekomendasi perbaikan sistem itu sendiri [4].

Berdasarkan hasil wawancara dengan Kepala Seksi Persandian dan Keamanan Informasi Diskominfo Kabupaten Kerinci, beliau menyatakan bahwa sudah pernah terjadi Cyber Attack yang dilakukan terhadap website Pemerintahan Kabupaten Kerinci. Penyerangan ini terjadi di tahun 2020 dengan tipe penyerangan berupa web deface, diduga penyerangan ini dilakukan individual yang melakukan eksploitasi dan menampilkan skill yang dimiliki, sehingga dibutuhkannya analisis kerentanan pada website-website yang dikelola oleh Diskominfo Kabupaten Kerinci, dengan tujuan agar dapat mengetahui kerentanan yang terdapat pada website-website tersebut, sehingga dapat mengurangi penyerangan terhadap website yang dikelola Diskominfo.

Penelitian ini akan melakukan analisis keamanan pada open website milik Diskominfo Kabupaten Kerinci dengan menggunakan dua metode yaitu metrode Open Web Application Security Project (OWASP) dan metode Information Systems Security Assessment Framework (ISSAF). Hasil analisis keamanan dari dua metode ini akan dibandingkan untuk dijadikan rekomendasi perbaikan pada sistem tersebut [5].

Penelitian terkait penggunaan metode OWASP dan ISSAF dalam pengujian keamanan sistem telah banyak dilakukan, beberapa pengujian menyebutkan bahwa metode ini sangat berpengaruh terhadap langkah dan hasil dari pengujian keamanan sistem. Objek pengujiannya beragam, alat dan metodenya beragam. Setiap metode dan alat yang digunakan memiliki perbedaan, mulai dari tahapannya hingga hasil baik analisis maupun rekomendasinya.

2. Metodologi Penelitian

2.1. Subjek Penelitian

Subjek penelitian ini adalah website Pemerintah Kabupaten Kerinci, dengan domain https://kerincikab.go.id. Penelitian dilakukan dengan melakukan pengujian terhadap website dengan menggunakan metode OWASP dan ISSAF.

2.2. Metode OWASP

Tahapan dalam metode OWASP adalah [6] :

a. Reconaissannce

Tahap ini dilakukan pengumpulan data informasi mengenai target, seperti jenis komputer, alamat, yang semuanya bisa berguna untuk tahap selanjutnya.

b. Scanning

Tahap ini dilakukan pengumpulan berbagai informasi mengenai vulnerability (kerentanan) yang terdapat pada sebuah website dan mencari berbagai kemungkinan mengenai adanya vulnerability yang bisa digunakan oleh attacker untuk merusak dan memanipulasi data yang ada pada website.

c. Exploitation

Tahap ini merupakan kegiatan lanjutan untuk masuk kedalam sistem keamanan komputer setelah diketahui adanya bugs (cela) dan vulnerability (kerentanan) yang didapatkan dalam proses Scanning.

d. Maintaining Access

e. Reporting

Pada tahap ini, seluruh data yang ditemukan berupa vulnerability (kerentanan) yang diperoleh dari hasil evaluasi akan dibuatkan laporan secara terstruktur dari kegiatan penetrasi dari tahap awal sampai akhir sebagai solusi penanganan sistem keamanan pada aplikasi web agar lebih baik lagi.

2.3. Metode ISSAF

Tahapan dalam metode ISSAF adalah [7]:

a. Information Gathering

Tahap ini digunakan Internet untuk mendapatkan informasi sebanyak-banyaknya dari target (Perusahaan atau Orang) dengan menggunakan metode teknikal

(DNS/WHOIS) dan non-teknikal (Search Engine, list E-mail, dan lain-lain).

b. Network Mapping

Setelah informasi berhasil didapatkan, pendekatan teknikal yang dapat dilakukan ialah meletakkan "Footprint" ke sistem ataupun jaringan yang diinginkan. Untuk lebih efektif.

c. Vulnerability Identification

Tahap ini akan dilakukan beberapa aktifitas untuk mendapatkan kerentanan yang ada pada sistem.

d. Penetration

Tahap ini dilakukan percobaan untuk mendapatkan akses secara illegal dengan cara mengakali sistem keamanan dan mencoba untuk mencapai akses level seluas-luasnya.

e. Gaining Access & Privilege Escalation

Di beberapa situasi, sebuah sistem dapat dinilai lebih jauh, dalam fase ini mengizinkan penguji untuk memastikan dan mendokumentasikan kemungkinan gangguan, dan penyebaran serangan otomatis. Hal ini memungkinkan hasil dari pengujian yang lebih baik kepada target secara menyeluruh.

f. Enumerate Further

Tahap ini memungkinkan untuk mendapatkan informasi tambahan berdasarkan proses pada sistem.

g. Compromise Remote User/Sites

Sebuah kerentanan sudah cukup untuk membuka seluruh network, sebagaimanapun amannya sebuah jaringan. Penguji dapat mencoba untuk menggunakan remote user. Hal ini dapat memudahkan untuk mendapatkan hak akses untuk ke jaringan yang lebih dalam.

h. Maintaining Access

Dengan menggunakan sesuatu seperti Backdoor, penguji dapat kembali ke dalam sebuah sistem, bahkan jika sistem yang diuji sudah tidak lagi ada. Backdoor dapat dibuat dengan beberapa cara, baik dengan menggunakan root-kit, dengan mengizinkan sistem target terkoneksi dengan server penguji dan lain-lain.

i. Covering the Track

Tahap ini akan menghapus jejak-jejak yang ada dengan cara menyembunyikan file, dan juga menghapus log files.

j. Reporting

Tahap ini akan dilakukan penulisan laporan yang mendeskripsikan hasil pengujian dengan rekomendasi dan penyelesaiannya.

k. Clean And Destroy Artifacts

Semua informasi yang telah dibuat atau diletakkan di sistem sudah harus dihapus pada tahap ini. Jika tidak dapat dilakukan, dengan remote system, hal ini harus diberitahukan kepada pihak yang diuji agar para staff IT pada pihak tersebut dapat menghapus informasi ini setelah laporan diterima.

2.4. Kerangka Kerja Penelitian

Kerangka kerja dibutuhkan agar penelitian memiliki pedoman dan arah yang jelas dalam melakukan penelitian. KErangka kerja disajikan pada Gamabr 1.

Gambar 1 Kerangka Kerja Penelitian

Kerangka kerja penelitian tiap tahapnya memiliki keterkaitan dengan tahap berikutnya. Penelitian dimulai dengan mengidentifikasi masalah, menentukan tujuan, studi literatur, menerapkan metode yang digunakan, melakukan analisis ancaman, melakukan hasil dan pembahasan serta membuat kesimpulan dan saran.

3. Hasil dan Pembahasan

3.2. Penerapan OWASP (*Open Web Application Security Project*)

3.2.1. *Reconaissance*

Pada tahap Reconaissance dilakukan pencarian informasi terkait website yang diteliti, Berikut adalah hasil pencarian menggunakan aplikasi Whois Domain terlihat pada Gambar 2.


Raw Whois Data

```
ID ccTLD whois server
Please see 'whois -h whois.id help' for usage.

Domain ID: PANDI-DO198016
Domain Name: kerincikab.go.id
Created On: 2007-07-09 13:09:07
Last Updated On: 2022-08-10 07:09:08
Expiration Date: 2024-08-02 00:09:08
Status: autoRenewPeriod

==================================================
Sponsoring Registrar Organization: Kementerian Komunikasi dan Informatika
Sponsoring Registrar URL:
Sponsoring Registrar Street: Jl. Medan Merdeka Barat No. 9
Sponsoring Registrar City: Jakarta Pusat
Sponsoring Registrar State/Province: Jakarta
Sponsoring Registrar Postal Code: 10110
Sponsoring Registrar Country: ID
Sponsoring Registrar Phone: 622138433507
Sponsoring Registrar Email: hostmaster@pandi.id
Name Server: rita.ns.cloudflare.com
Name Server: woz.ns.cloudflare.com
DNSSEC: Unsigned

Abuse Domain Report https://pandi.id/domain-abuse-form/?lang=en
For more information on Whois status codes, please visit https://www.icann.o
```

Gambar 2. Hasil Whois kominfo.kerincikab.go.id

Tabel 1 merupakan hasil whois website kominfo.kerincikab.go.id

Tabel 1. Whois Website kominfo.kerincikab.go.id

Domain ID	Domain Name	Created On	Expiration Date	Status
PANDI-DO198016	KERINCIKAB.GO.ID	09-07-2007	02-08-2007	Ok

Pada tahapan ini juga dilakukan pencarian port-port yang terbuka dengan menggunakan tool Nmap. Dengan mengetahui port-port yang terbuka maka bisa diketahui celah-celah yang bisa digunakan atau dimanfaatkan oleh Attacker. Berikut merupakan hasil scanning port terhadap website kominfo.kerincikab.go.id disajikan pada Tabel 2.

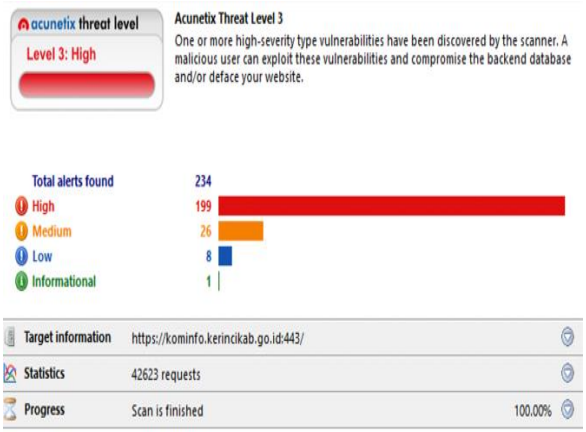
Tabel 2. Hasil Nmap kominfo.kerincikab.go.id

PORT	STATUS	SERVICE
80	Open	http
443	Open	http
8080	Open	http
8443	Open	http

Berdasarkan pada tabel 2, dapat dilihat bahwa hasil pemindaian dengan menggunakan *tool Nmap* didapatkan informasi mengenai *port-port* yang terbuka (*open*), yaitu *port* 80, 443, 8080, dan 8443. Jika terdapat *port* yang terbuka maka menandakan ada aplikasi yang dapat menerima paket data dari pengirim dan port tersebut dapat diakses. Jika terlalu banyak *port* yang terbuka maka seorang *Attacker* akan lebih mudah untuk melakukan *Remote Host* atau mengendalikan komputer dari jarak jauh.

3.2.2. *Scanning*

Tahap scanning ini dilakukan untuk mencari celah atau kerentanan dengan melakukan pemindaian aplikasi dengan menggunakan tool Acunetix. Jika terdapat kerentanan maka penguji akan menggunakan kerentanan tersebut untuk melakukan langkah pengujian yang selanjutnya.



Gambar 3 Hasil Scanning Acunetix

Gambar 3 diatas merupakan hasil dari scanning menggunakan tools Acunetix, hasil ini menunjukkan kerentanan-kerentanan yang ada pada website kominfo.kerincikab.go.id berada pada Level 3 dengan tingkat risiko HIGH yang disajikan pada Tabel 3.

Tabel 3. Hasil Kerentanan Website kominfo.kerincikab.go.id

No	Jenis Kerentanan	Risiko	Tingkat Risiko
1	*Cross site scripting (verified)*	Penyerang dapat suntikkan *JavaScript, VBScript, ActiveX, HTML*, atau *Flash* ke dalam aplikasi yang rentan untuk menipu pengguna agar mengumpulkan data dari mereka. Penyerang dapat mencuri *cookie* sesi dan mengambil alih akun, menyamar sebagai pengguna. Dimungkinkan juga untuk memodifikasi konten halaman yang disajikan kepada pengguna.	*High*
2	*SQL Injection*	Penyerang dapat mengeksekusi pernyataan SQL sewenang-wenang pada sistem yang rentan. Ini dapat membahayakan integritas database Anda dan/atau mengekspos informasi sensitif.	*High*
3	*Application error message*	*Error message* dapat mengungkapkan informasi sensitif. Informasi ini dapat digunakan untuk melancarkan serangan lebih lanjut.	*Medium*
4	*Clickjacking X-Frame-Options header missing*	Berisiko terkena serangan *clickjacking*	*Low*
5	*Cookie without HttpOnly flag set*	Informasi yang terdapat pada *cookie* seperti *username* dan *password* dapat disalahgunakan oleh penyerang.	*Low*
6	*Possible sensitive directories*	Direktori ini dapat mengekspos informasi sensitif yang dapat membantu penyerang untuk mempersiapkan serangan lebih lanjut.	*Low*
7	*Possible sensitive files*	File ini dapat mengekspos informasi sensitif yang dapat membantu penyerang untuk mempersiapkan serangan lebih lanjut	*Low*

Berdasarkan hasil scanning yang dilakukan dengan menggunakan tool Acunetix menghasilkan bahwa website kominfo.kerincikab.go.id mempunyai 7 jenis kerentanan dengan tingkat risiko berada pada level 3 yaitu High.

3.2.3. *Exploitation*

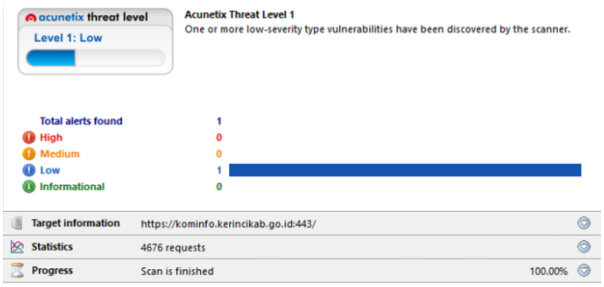
Exploitation adalah tahapan akan dilakukan pengujian terhadap hasil kerentanan dengan melakukan exploitasi. Pada tahapan ini dilakukan perbaikan berdasarkan solusi untuk mengatasi kerentanan yang disajikan pada Tabel 4.

Tabel 4. Solusi Perbaikan Terhadap Jenis Kerentanan

No	Jenis Kerentanan	Rekomendasi Perbaikan	Hasil
1	*Cross site scripting (verified)*	Script harus memfilter metakarakter dari input pengguna.	*Berhasil*
2	SQL Injection	Script harus memfilter metakarakter dari input pengguna	*Berhasil*
3	Application error message	Tinjau source code untuk script ini.	*Berhasil*
4	*Clickjacking X-Frame-Options header missing*	Konfigurasikan *server web* untuk menyertakan *header X-Frame-Options.*	*Gagal*
5	*Cookie without HttpOnly flag set*	Mengkonfigurasi session cookies dengan HttpOnly flag set .	*Berhasil*
6	*Possible sensitive directories*	Batasi akses ke direktori ini atau hapus dari situs web.	*Berhasil*
7	*Possible sensitive files*	Batasi akses ke file ini atau hapus dari situs web	*Berhasil*

3.2.4. *Reporting*

Tahapan terakhir dari Metode OWASP adalah membuat reporting pengujian kerentanan. Hasil penerapan solusi terhadap jenis kerentanan terbukti dapat meningkatkan keamanan website yang diuji dari yang sebelumnya berkategori HIGH turun menjadi kategori LOW, seperti yang terlihat pada Gambar 4.

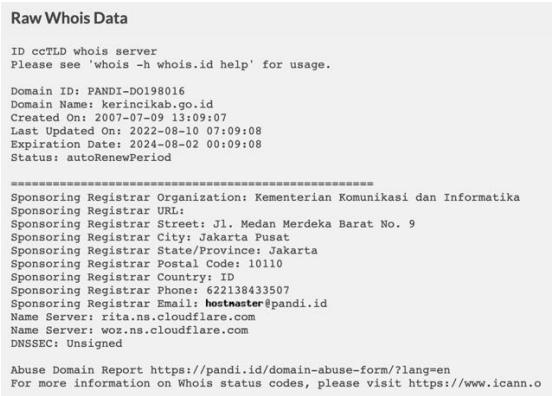


Gambar 4. Hasil kerentanan setelah dilakukan perbaikan

3.3. Penerapan Metode ISSAF (*Information Systems Security Assessment Framework*)

3.3.1. *Information Gathering*

Pada tahap *information gathering* akan dilakukan pencarian informasi terkait *Website* yang akan diteliti, berikut merupakan hasil dari pencarian tersebut dengan menggunakan Whois Domain disajikan pada Gamabr 5.



Gambar 5. Hasil Whois Domain kominfo.kerincikab.go.id

Hasil whois website kominfo.kerincikab.go.id disajikan pada Tabel 5.

Tabel 5. Whois Website kominfo.kerincikab.go.id

Domain ID	Domain Name	Created On	Expiration Date	Status
PANDI-DO198016	KERINCIKAB.GO.ID	09-07-2007	02-08-2007	Ok

Pada Tabel 5 dapat diketahui bahwa setelah dilakukan pencarian pada *Whois Domain* untuk *sub domain* kominfo.kerincikab.go.id data yang dihasilkan mengarah pada *domain* utama yaitu *domain Website* dengan nama kerincikab.go.id. Hal ini disebabkan *domain* kominfo.kerincikab.go.id masih merupakan satu kesatuan dengan *domain* kerincikab.go.id sehingga *domain* yang muncul dalam hasil *Whois Domain* ialah kerincikab.go.id. KOMINFO Kabupaten Kerinci menggunakan *Domain* ID: PANDI-DO198016, yang merupakan sebuah layanan Pengelola Nama Domain Internet Indonesia (PANDI), *domain* ini dibuat pada 09 Juli 2007 dan akan *expired* pada tanggal 02 Agustus 2024.

3.3.2. *Network Mapping*

Setelah informasi terkait website berhasil didapatkan, pendekatan teknikal yang bisa dilakukan adalah meletakkan "Footprint" ke sistem ataupun jaringan yang diinginkan. Untuk lebih efektif, Network Mapping sebaiknya dilakukan dengan sesuai dengan rencana. Rencana ini mencakup kemungkinan titik terlemah atau hal-hal yang paling penting dari perusahaan yang akan di nilai. Network mapping akan dilakukan dengan bantuan tool Zenmap, Berikut merupakan hasil dari penelusuran port-port dengan menggunakan Zenmap disajikan pada Tabel 6.

Tabel 6. Hasil Nmap kominfo.kerincikab.go.id

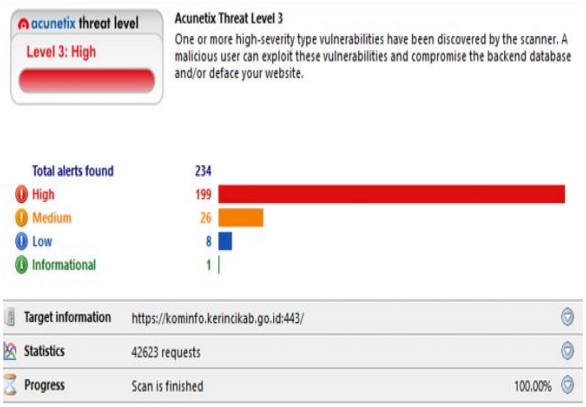
Port	Status	Service
80	Open	http
443	Open	http
8080	Open	http
8443	Open	http

Berdasarkan pada tabel 6, dapat dilihat bahwa hasil pemindaian dengan menggunakan *tool Nmap* didapatkan informasi mengenai *port-port* yang terbuka (*open*), yaitu *port* 80, 443, 8080, dan 8443. Jika terdapat port yang terbuka maka menandakan ada aplikasi yang dapat menerima paket data dari pengirim dan port tersebut dapat diakses. Jika terlalu banyak *port* yang terbuka maka seorang *Attacker* akan lebih mudah untuk melakukan *Remote Host* atau mengendalikan komputer dari jarak jauh.

3.3.3. *Vulnerabillity Identification*

Setelah dilakukan tahapan *Information Gathering* dan *Network Mapping*, tahapan selanjutnya ialah *Vulnerability Identification*, pada tahapan ini akan dilakukan pemindaian terhadap *website* untuk dilihat celah atau kerentanan yang ada pada website tersebut. Jika terdapat kerentanan maka akan digunakan kerentanan tersebut untuk melakukan langkah pengujian yang selanjutnya.

Berikut merupakan hasil dari pengujian menggunakan *tools Acunetix*, hasil ini menunjukkan kerentanan yang ada pada website **kominfo.kerincikab.go.id** berada pada Level 3 dengan tingkat risiko HIGH disajikan pada Gambar 6.



Gambar 6. Hasil Scanning Vulnerabillity

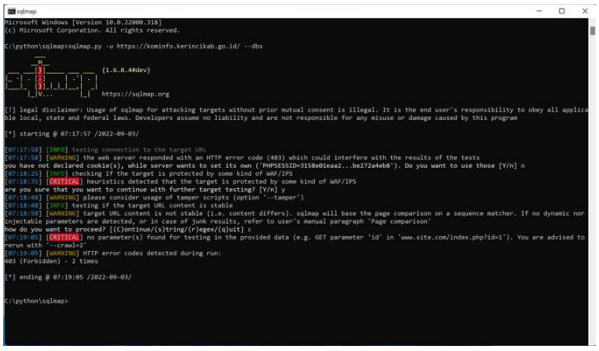
Berdasarkan hasil scanning dengan menggunakan tool Acunetix menghasilkan bahwa website kominfo.kerincikab.go.id mempunyai 7 jenis kerentanan dengan tingkat risiko berada pada level 3 yaitu High disajikan pada Tabel 7.

Gambar 7. Hasil Kerentanan Website kominfo.kerincikab.go.id

No	Jenis Kerentanan	Risiko	Tingkat Risiko
1	*Cross site scripting (verified)*	Penyerang dapat suntikkan *JavaScript, VBScript, ActiveX, HTML*, atau *Flash* ke dalam aplikasi yang rentan untuk menipu pengguna agar mengumpulkan data dari mereka. Penyerang dapat mencuri *cookie* sesi dan mengambil alih akun, menyamar sebagai pengguna. Dimungkinkan juga untuk memodifikasi konten halaman yang disajikan kepada pengguna.	*High*
2	*SQL Injection*	Penyerang dapat mengeksekusi pernyataan SQL sewenang-wenang pada sistem yang rentan. Ini dapat membahayakan integritas database Anda dan/atau mengekspos informasi sensitif.	*High*
3	*Application error message*	*Error message* dapat mengungkapkan informasi sensitif. Informasi ini dapat digunakan untuk melancarkan serangan lebih lanjut.	*Medium*
4	*Clickjacking X-Frame-Options header missing*	Berisiko terkena serangan *clickjacking*	*Low*
5	*Cookie without HttpOnly flag set*	Informasi yang terdapat pada *cookie* seperti *username* dan *password* dapat disalahgunakan oleh penyerang.	*Low*
6	*Possible sensitive directories*	Direktori ini dapat mengekspos informasi sensitif yang dapat membantu penyerang untuk mempersiapkan serangan lebih lanjut.	*Low*
7	*Possible sensitive files*	File ini dapat mengekspos informasi sensitif yang dapat membantu penyerang untuk mempersiapkan serangan lebih lanjut	*Low*

3.3.4. *Penetration*

Penetration merupakan salah satu tahapan pada metode ISSAF dimana pada tahapan ini akan dilakukan penetrasi terhadap website yang diuji untuk melihat apakah kerentanan yang ditemukan pada tahap Vulnerability Identification dapat dieksploitasi dan dapatkah penguji mendapatkan hak akses website dari hasil uji penetrasi tersebut. Dalam tahap ini akan diuji apakah website ini terdapat kerentanan kepada SQL Injection dengan menggunakan tool yaitu SQLmap. Berikut merupakan screenshot hasil dari pengujian menggunakan SQLmap. Berdasarkan dari Gambar 8, dapat dilihat bahwa Website kominfo.kerincikab.go.id tidak memiliki kerentanan SQL Injection yang disajikan pada Gamabr 8.



Gambar 8. Hasil SQLmap

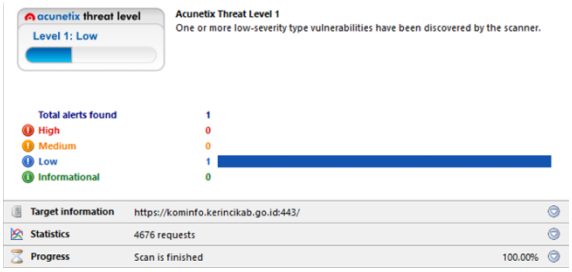
3.3.5. *Reporting*

Tahapan terakhir dari Metode ISSAF adalah membuat *reporting* pengujian kerentanan dimana tahapan ini akan dilakukan perbaikan berdasarkan solusi yang tepat untuk mengatasi kerentanan. Hasil perbaikan terhadap kerentanan yang terdapat pada website kominfo.kerincikab.go.id dapat dilihat pada Tabel 8.

Tabel 8. Hasil perbaikan terhadap kerentanan website

No	Jenis Kerentanan	Rekomendasi Perbaikan	Hasil
1	*Cross site scripting (verified)*	Script harus memfilter metakarakter dari input pengguna.	*Berhasil*
2	SQL Injection	Script harus memfilter metakarakter dari input pengguna	*Berhasil*
3	Application error message	Tinjau source code untuk script ini.	*Berhasil*
4	*Clickjacking X-Frame-Options header missing*	Konfigurasikan *server web* untuk menyertakan *header X-Frame-Options.*	*Gagal*
5	*Cookie without HttpOnly flag set*	Mengkonfigurasi session cookies dengan HttpOnly flag set .	*Berhasil*
6	*Possible sensitive directories*	Batasi akses ke direktori ini atau hapus dari situs web.	*Berhasil*
7	*Possible sensitive files*	Batasi akses ke file ini atau hapus dari situs web	*Berhasil*

Berdasarkan hasil penerapan solusi terhadap jenis kerentanan terbukti dapat meningkatkan keamanan website yang diuji dari yang sebelumnya berkategori HIGH menjadi kategori LOW, seperti yang terlihat pada Gambar 9.



Gambar 9. Hasil Scanning setelah dilakukan perbaikan

4. Kesimpulan

Dalam kesimpulan tidak boleh ada referensi. Kesimpulan berisi fakta yang didapatkan. Nyatakan kemungkinan aplikasi, implikasi dan spekulasi yang sesuai. Jika diperlukan, berikan saran untuk penelitian selajutnya.

Daftar Rujukan

[1] Zulfia, A., Ruskan, E. L., & Putra, P. (2021). Penilaian Risiko Aset Informasi dengan Metode OCTAVE Allegro: Studi Kasus ICT Fakultas Ilmu Komputer Universitas Sriwijaya. *JOINS(Journal of Information System)*, *6*(1), 40-47. https://doi.org/10.33633/joins.v6i1.4088

[2] Harahap, B. (2021). Penerapan Keamanan Owasp Terhadap Aplikasi GTFW Pada Website Universitas Battuta. *Jurnal Informatika dan Teknologi Pendidikan*, *1*(2), 80-86. https://doi.org/10.25008/jitp.v1i2.15

[3] Zirwan, A. (2022). Pengujian dan Analisis Keamanan Website Menggunakan Acunetix Vulnerability Scanner. *Jurnal Informasi dan Teknologi*, 70-75. https://doi.org/10.37034/jidt.v4i1.190

[4] Handayani, N. K. M., Sasmita, G. M. A., & Wiranath, A. A. K. A. C. Evaluation Security Web-Based Information System Application Using ISSAF Framework (Case Study: SIMAK-NG Udayana University), (2020). https://doi.org/10.24843/jitter.v1i2.65651

[5] Lala, S. K., Kumar, A., & Subbulakshmi, T. (2021). Secure web development using owasp guidelines, 2021. https://doi.org/10.1109/ICICCS51141.2021.9432179

[6] Kellezi, D., Boegelund, C., & Meng, W. (2021). Securing Open Banking with Model-View-Controller Architecture and OWASP. *Wireless Communications and Mobile Computing*, *2021*. https://doi.org/10.1155/2021/8028073

[7] Hassanah, N. (2021). *Analisis Keamanan Website Universitas Internasional Batam Menggunakan Metode Issaf* (Doctoral dissertation, Universitas Internasional Batam). https://doi.org/10.33884/jif.v9i02.3758

[8] Aminudin, Aminudin, and Eko Budi Cahyono. A practical analysis of the fermat factorization and pollard rho method for factoring integers, 2021. https://doi.org/10.24843/LKJITI.2021.v12.I01.p04

[9] Aryanti, D., & Utamajaya, J. N. (2021). Analisis Kerentanan Keamanan Website Menggunakan Metode OWASP (Open Web Application Security Project) Pada Dinas Tenaga Kerja. *Jurnal Syntax Fusion*, *1*(03), 15-25. https://doi.org/10.54543/fusion.v1i03.53

[10] Fahmi, M. I., Kifti, W. M., & Marpaung, N. PEMANFAATAN WEBSITE SEBAGAI MEDIA INFORMASI PADA POLSEK PORSEA KABUPATEN TOBA SAMOSIR, 2020. https://doi.org/10.33330/jurdimas.v3i1.494

[11] Herdianti, H., & Umar, F. (2020). Analisis Keamanan Website Menggunakan Teknik Footprinting dan Vulnerability Scanning. *INFORMAL: Informatics Journal*, *5*(2), 43-48. https://doi.org/10.19184/isj.v5i2.18941

[12] Jha, S. K., & Kumar, S. S. (2022). Cybersecurity in the Age of the Internet of Things: An Assessment of the Users' Privacy and Data Security, 2022. https://doi.org/10.1007/978-981-16-2126-0_5

[13] Maharani, D., Helmiah, F., & Rahmadani, N. (2021). Penyuluhan Manfaat Menggunakan Internet dan Website Pada Masa Pandemi Covid-19. *Abdiformatika: Jurnal Pengabdian Masyarakat Informatika*, *1*(1), 1-7. https://doi.org/10.25008/abdiformatika.v1i1.130

[14] Mardayatmi, S., Defit, S., & Nurcahyo, G. W. (2021). Sistem Pendukung Keputusan bagi Penerima Bantuan Komite Sekolah

Menggunakan Metode Topsis. *Jurnal Sistim Informasi dan Teknologi*, 134-141. https://doi.org/10.37034/jsisfotek.v3i3.56

[15] Maulana, S. A. (2021). Analisis Keamanan Website dengan Information System Security Assessment Framework (Issaf) dan Open Web Application Security Project (Owasp) di Rumah Sakit Xyz. *Jurnal Indonesia Sosial Teknologi*, *2*(4), 506-519. https://doi.org/10.36418/jist.v2i4.124

[16] Muhyidin, Y., Totohendarto, M. H., & Undamayanti, E. (2022). Perbandingan Tingkat Keamanan Website Menggunakan Nmap Dan Nikto Dengan Metode Ethical Hacking. *Jurnal Teknologika*, *12*(1), 80-89. https://doi.org/10.51132/teknologika.v12i1.143

[17] Ningsih, S. W., Almaarif, A., & Widjajarto, A. (2021). Analisis Pengujian Kerentanan Situs Pemerintahan XYZ dengan PTES. *JATISI (Jurnal Teknik Informatika dan Sistem Informasi)*, *8*(3), 1543-1556. https://doi.org/10.35957/jatisi.v8i3.1224

[18] Pohan, Y. A., Yuhandri, Y., & Sumijan, S. (2021). Meningkatkan Keamanan Webserver Aplikasi Pelaporan Pajak Daerah Menggunakan Metode Penetration Testing Execution Standar. *Jurnal Sistim Informasi dan Teknologi*, 1-6. https://doi.org/10.37034/jsisfotek.v3i1.36Cv

[19] Riadi, I., Yudhana, A., & Yunanri, W. (2020). Analisis Keamanan Website Open Journal System Menggunakan Metode Vulnerability Assessment. *Jurnal Teknologi Informasi Dan Ilmu Komputer*, *7*(4), 853-860. http://dx.doi.org/10.25126/jtiik.2020701928Cxv

[20] Sanjaya, I. G. A. S., Sasmita, G. M. A., & Arsa, D. M. S. Evaluasi Keamanan Website Lembaga X Melalui Penetration Testing Menggunakan Framework ISSAF , (2020). https://doi.org/10.24843/JIM.2020.v08.i02.p05