Vulnerability Assessment Website E-Government dengan NIST SP 800-115 dan OWASP Menggunakan *Web Vulnerability Scanner*

Esti Zakia Darojat[a*], Eko Sediyono[b], Irwan Sembiring[c]

[a] Magister Sistem Informasi, Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana
[b,c] Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana

Naskah Diterima : 20 Juli 2022; Diterima Publikasi : 22 September 2022

DOI: 10.21456/vol12iss1pp36-44

Abstract

E-Government is one of the local government's means of implementing service-oriented values and public information disclosure by providing the local government's official website. Vulnerability Assessment (VA) is a vulnerability assessment method by testing security vulnerabilities to find out all potential critical weaknesses of e-government websites, the aims is to support convenience and service improvement when using e-government websites. The method is using descriptive quantitative to analyze and evaluate security level of both e-government websites based on the NIST SP 800-115 method regarding technical guidelines for testing and assessing information security parameters and OWASP using two web vulnerability scanners. This study is to analyze and evaluate the results of vulnerability scanning on two different types of e-government web, namely the e-government web belonging to the local government and village government, the sample assessment using the semarangkab.go.id website belonging to the local government of Semarang Regency, Central Java Province. and gunungtumpeng.id which is the official e-government website owned by the Gunung Tumpeng Village Government, Suruh District, Semarang Regency, Central Java Province, Indonesia. Hasil penelitian menunjukkan ditemukan persamaan penilaian dalam hal kategori level ancaman dan jumlah kerentanan menggunakan kedua alat *web vulnerability scanner*, dan hasil yang berbeda terdapat pada durasi, kecepatan pemindaian, dan jenis temuan kerentanan. Kedua parameter OWASP dapat memberikan petunjuk dan penjelasan kompleks untuk membantu pengembang atau pihak pemerintah daerah melakukan pengambilan keputusan mengenai keamanan informasi pada web *e-government* yang dikelola.

Keywords: *Vulnerability Assessment; E- Government Website; Web Vulnerability Scanner;* NIST SP 800-115, OWASP

Abstrak

E-Government adalah salah satu sarana pemerintah daerah dalam mengimplementasikan nilai berorientasi pelayanan dan keterbukaan informasi publik dengan menyediakan *website* resmi pemerintah daerah. *Vulnerability Assessment* (VA) merupakan sebuah cara penilaian kerentanan dengan melakukan pengujian celah keamanan untuk mengetahui seluruh potensi kelemahan kritis dari *website e-government*, hal ini dilakukan guna mendukung kenyamanan dan peningkatan pelayanan ketika menggunakan *website e-government* tersebut. Metode yang digunakan yaitu kuantitatif deskriptif untuk menganalisis dan mengevaluasi tingkat keamanan kedua *website e-government* berdasarkan metode NIST SP 800-115 mengenai panduan teknis untuk pengujian dan penilaian keamanan informasi dan parameter OWASP yang dilakukan menggunakan dua alat *web vulnerability scanner*. Penilaian ini adalah untuk menganalisis dan mengevaluasi hasil pemindaian kerentanan pada dua jenis *web e-government* yang berbeda, yaitu *web e-government* milik pemerintah daerah dan milik pemerintah desa, penilaian sampel menggunakan *website* semarangkab.go.id milik pemerintah daerah Kabupaten Semarang Provinsi Jawa Tengah dan gunungtumpeng.id yaitu website e-government resmi milik Pemerintah Desa Gunung Tumpeng, Kecamatan Suruh, Kabupaten Semarang, Provinsi Jawa Tengah Indonesia. The results showed that there were similar assessments in terms of threat level categories and number of vulnerabilities using both web vulnerability scanning tools, and different results were found on duration, scanning speed, and types of vulnerability findings. Both OWASP parameters can provide complex instructions and explanations to help developers or local governments make decisions about information security on managed e-government webs.

Kata Kunci: *Vulnerability Assessment; E- Government Website; Web Vulnerability Scanner;* NIST SP 800-115, OWASP

*) Penulis korespondensi: 972020005@student.uksw.edu

1. Pendahuluan

E-government merupakan sebuah mekanisme baru dari interaksi antara pemerintah dengan masyarakat memanfaatkan teknologi komunikasi sehingga dapat meningkatkan kualitas layanan public (Andoyo *et al.,* 2015). Sistem Pemerintahan Berbasis Elektronik (SPBE) atau selanjutnya disebut *e-government* adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada Pengguna (Al-fajri *et al.,* 2020). Manajemen SPBE meliputi: manajemen risiko, manajemen keamanan informasi, manajemen data, manajemen aset teknologi informasi dan komunikasi, manajemen sumber daya manusia, manajemen pengetahuan, manajemen perubahan, dan manajemen Layanan SPBE. Amanat Inpres No. 6 tahun 2001 tentang telematika dalam pemerintahan dan Inpres No. 3 tahun 2003 tentang Penyelenggaraan Tata Kelola Pemerintahan Secara Elektronis di Indonesia menyebutkan implementasi dari *e-government* salah satunya adalah pengembangan Sistem Informasi Desa merupakan alat bantu perangkat desa untuk melayani masyarakat (Mustanir, 2020). Tahapan metode siklus hidup pengembangan perangkat lunak diharapkan mampu menginovasi pemerintahan desa untuk meningkatkan kualitas pelayanan masyarakat, responsivitas, responsibilitas dan produktivitas (Fitri *et al.,* 2017).

Penilaian kerentanan menggunakan alat pemindaian pada dua jenis *web e-government* yang berbeda, yaitu *web* pemerintah daerah dan *web* pemerintah desa. Pemilihan kedua jenis web tersebut bertujuan untuk mengetahui keandalan masing-masing *web e-government* pada tingkat keamanannya. Dengan alamat *domain* semarangkab.go.id sebagai *web* pemerintah daerah dan gunungtumpeng.id sebagai *web* pemerintah desa. *Web* semarangkab.go.id merupakan *website e-government* milik pemerintah daerah Kabupaten Semarang Provinsi Jawa Tengah yang menggunakan *domain* go.id, sebuah situs *web* resmi yang hanya dapat digunakan untuk lembaga pemerintahan pusat dan daerah. Kabupaten Semarang dipilih karena pada tahun 2022 ini pihak pemerintah kabupaten sedang menjalankan koordinasi terkait pelaksanaan SPBE yang salah satunya terdapat kegiatan pemantauan dan evaluasi SPBE, sehingga hasil penilaian kerentanan dapat menjadi referensi dalam evaluasi. Sedangkan gunungtumpeng.id adalah *website* milik Pemerintah Desa Gunung Tumpeng Kecamatan Suruh Kabupaten Semarang dimana *website* ini sebelumnya pernah dilakukan penelitian oleh penulis dengan kerangka PIECES (*Performance, Information, Control and Security, Efficiency, and Services*). Hasilnya pada aspek *Economics, Control and Security, Eficiency*, dan *Services*, tergolong negatif sehingga dari hasil tersebut *website* gunungtumpeng.id direkomendasikan untuk diteliti celah sistem keamanannya.

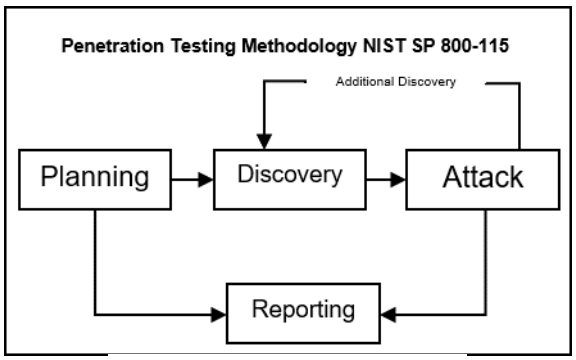
Hasil *scan* akan menampilkan *score* akhir dari hasil *Vulnerability Assessments* (VA) dengan pedoman NIST (*National Institute of Standards and Technology*) khususnya standar NIST SP 800-115 mengenai Panduan Teknis untuk Pengujian dan Penilaian Keamanan Informasi. Penilaian menggunakan alat *web vulnerability scanner* yaitu Acunetix dan Pentest-Tools dengan parameter OWASP (*Open Web Application Security Project*). Penelitian ini menggunakan dua dokumen yang disediakan OWASP. OWASP Top 10 merupakan 10 daftar teratas kerentanan yang menjadi ancaman pada suatu *website* dan bertujuan supaya keamanan perangkat lunak dapat ditinjau oleh individu maupun organisasi sehingga dapat dilakukan pengambilan keputusan terkait resikonya (Hidayatulloh *et al.,* 2021). Penelitian ini berfokus pada penilaian kerentanan (VA) (Dewi Laksmiati, 2020) menggunakan kombinasi metode antara NIST dan OWASP dengan tahapan menggunakan panduan NIST SP 800-115 dan parameter temuan menggunakan OWASP Top 10 (Yudiana *et al.,* 2021) yang telah terimplementasi dalam kedua alat *web vulnerability scanner*, kemudian memakai dua sampel *web e-government* dengan spesifikasi yang berbeda yaitu *website* Pemerintah Kabupaten (Pemkab) dan *website* Pemerintah Desa (Pemdes), sehingga dapat dilakukan perbandingan lalu ditarik hasil analisis dan evaluasi dari kedua *website* memakai kedua alat tersebut.

2. Kerangka Teori

Vulnerability Assessment (VA) merupakan analisa keamanan menyeluruh dan mendalam seperti pada keamanan informasi, hasil *scanning* jaringan, cara pengelolaan, konfigurasi pada sistem, kesadaran keamanan aktor yang terlibat dan keamanan fisik, untuk mengetahui seluruh potensi kelemahan kritis yang ada (Tarigan *et al.,* 2017). Empat bidang utama yang ditangani NIST (*National Institute of Standards and Technology*) antara lain bioteknologi, nanoteknologi, teknologi informasi dan manufakturing *modern*.(Silaban *et al.,* 2018) Pada bidang teknologi informasi terdapat NIST SP 800-115 yang merupakan panduan teknis untuk pengujian dan penilaian keamanan informasi, metodologi yang dikhususkan untuk membantu organisasi dalam melakukan perencanaan tes keamanan informasi (Silaban *et al.,* 2018). Bagan proses metode NIST SP 800-115 dapat dilihat pada Gambar 1.

OWASP (*Open Web Application Security Project*) merupakan komunitas riset lembaga nirlaba beranggotakan para ilmuwan, peneliti, dan sektor swasta yang menerbitkan laporan artikel, alat/peralatan, dan dokumen yang bersifat *open source*. (Kurniawan, 2019) OWASP menjadi

rekomendasi dalam pemanfaatannya karena menurut pendapat para peneliti keamanan, OWASP merupakan perangkat lunak *open source*. Disamping itu OWASP menyediakan beberapa dokumen untuk menjaga keamanan *website* sehingga dapat dijadikan panduan penting bagi para *developer*. Dalam penelitian ini terdapat dua dokumen OWASP yang dijadikan acuan parameter, yaitu *Developer Cheat Sheet Series* dan OWASP *Top* 10.



Gambar 1. Metode NIST SP 800-115

Alat *Web Vulnerability Scanner* yang pertama yaitu sebuah perangkat lunak yang dibangun untuk melakukan *scanning* disebut Acunetix. Alat ini memberi rekomendasi solusi dari kerentanan yang ditemukan, dan mampu mengelola *traceability* dari setiap kerentanan *website* yang diuji. Disamping itu menyediakan beberapa fungsi tambahan untuk dapat melakukan pengujian lanjutan.(Maharani *et al.*, 2017) Alat kedua adalah Pentest-Tools *Website Vulnerability Scanner* yaitu alat yang dapat menemukan kerentanan pada aplikasi *web* umum dilengkapi dengan temuan masalah konfigurasi server. Layanan *Light Scan* mampu menemukan beberapa aspek *website* yang dapat diperiksa atara lain versi *software server*, HTTP *headers*, miskonfigurasi pada *server*, *cookies*, dan status SSL. (Alwi *et al.*, 2020)

3. Metode

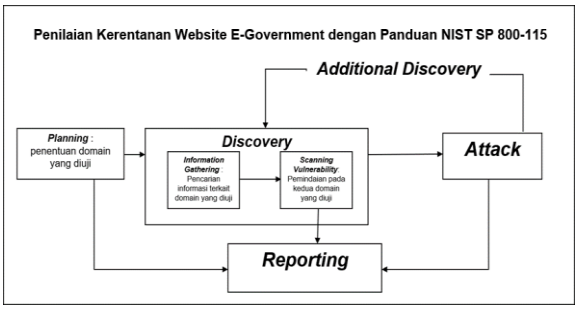
Pada penelitian ini menggunakan metode kuantitatif deskriptif dengan pedoman NIST SP 800-115 penelitian dilakukan untuk mengetahui tingkat keamanan *website e-government* pemerintah daerah semarangkab.go.id dan pemerintah desa gunungtumpeng.id. Kegiatan terbatas pada tahap pemindaian menggunakan aplikasi Acunetix *Web Vulnerability Scanner* dan Pentest-Tools *Website Vulnerability Scanner* dengan parameter OWASP.

3.1 Tahapan Penelitian

Pada panduan NIST SP 800-115 terdapat beberapa tahapan seperti *Planning, Discovery, Attack* dan *Report*. Tahapan ini berfungsi membantu proses pengujian *website*.(*Hanifah et al., 2021*) Empat fase pada metode NIST SP 800-115 akan dijelaskan sebagai berikut:

a. *Planning*: pada fase ini dilakukan penentuan *domain* yang diuji, persetujuan dengan pihak pemerintah kabupaten dan desa, penjelasan mengenai ruang lingkup penelitian yang dalam hal ini hanya sebatas pengukuran *scanning*, metode pengujian dengan NIST SP 800-115 dengan parameter OWASP, dimana pelaksanaan fase tersebut telah dijabarkan pada bagian pendahuluan dan metodologi penelitian.
b. *Discovery*: terdiri dari dua tahap yaitu *information gathering* dan *vulnerability scanning*, dimana untuk *information gathering* dilakukan pencarian informasi mengenai kondisi kerentanan *website* yang telah dijabarkan pada bagian hasil dan pembahasan khususnya sub bagian struktur dan fungsi *website*, kemudian pada *vulnerability scanning* dilakukan pemindaian kerentanan pada kedua *website* tersebut yang penjelasannya terdapat pada sub bagian pemindaian *website*.
c. *Attack*: dilakukan analisis dari hasil pemindaian kedua *website* yang menggunakan dua alat *web vulnerability scanner* bedasarkan frekuensi serangannya dan dijelaskan pada sub bagian pembahasan.
d. *Reporting*: penyampaian hasil penelitian dan penjelasan mengenai kesimpulan dari hasil pengujian dan penilaian keamanan, hal ini dipaparkan pada bagian kesimpulan.

Tahapan penilaian kerentanan website *e-government* dengan panduan NIST SP 800-115 dideskripsikan pada Gambar 2.

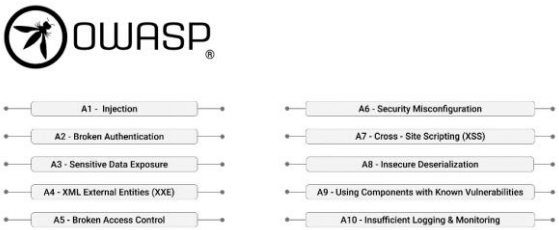


Gambar 2. Analisis Metode Penelitian dengan NIST SP 800-115

Parameter OWASP yang digunakan disini yang pertama dokumen *Developer Cheat Sheet Series* yang terdiri dari 78 *points* yang menjelaskan mengenai berbagai macam kelemahan, protokol keamanan, serta bagaimana melakukan keamanan menggunakan bahasa pemrograman yang popular yang pada penelitian ini hanya akan diambil beberapa acuan yang relevan dengan hasil temuan. Parameter selanjutnya adalah OWASP *Top* 10 2017 sebagai acuan pengujian kerentanan *website e-government*, kesepuluh parameter tersebut terdiri dari:

a. *Injection*: serangan yang dilakukan dengan cara menginjeksi *script* ke suatu *website*.
b. *Broken Authentication* : celah keamanan bagi seorang *hacker* melakukan akses ke dalam akun pengguna karena adanya kelemahan pada sistem login.
c. *Sensitive Data Exposure*: *website* tidak melindungi dengan baik terkait informasi sensitif.
d. XML *External Entities* (XEE) : jenis serangan terhadap *website* dengan mem-*parsing input* XML.
e. *Broken Access Control*: mengacu kepada sistem kontrol yang mengakses informasi dan fungsionalitasnya.
f. *Security Misconfiguration* : terdapat kesalahan konfigurasi keamanan sehingga dapat didefinisikan sebagai kegagalan untuk mengimplementasikan semua kontrol keamanan untuk sebuah *website*.
g. *Cross-Site Scripting* (XSS) : serangan jenis injeksi yaitu *malicious code* di injeksikan ke *website*.
h. *Insecure Deserialization* : kerentanan terhadap data yang tidak dapat dipercaya yang digunakan untuk melakukan serangan *Denial of Service* (DOS), *execute code, bypass authentication*.
i. *Using Components with Known Vulnerabilities*: kelemahan pada komponen seperti *libraries* dan *framework* yang digunakan pada *website* yang ditemukan *hacker* sehingga berpotensi diserang.
j. *Insufficient Logging & Monitoring*: kerentanan akibat serangan tidak dicatat dengan benar dan sistem tidak memantau kejadian.(Hidayatulloh *et al.*, 2021)

Parameter OWASP Top 10 dan kode kerentanannya dapat dilihat pada Gambar 3.



Gambar 3. Parameter OWASP *Top* 10

Pada penelitian ini untuk mengukur tingkat keparahan ancaman pada *website* semarangkab.go.id dan gunungtumpeng.id terdapat *level* peringatan kerentanan. Ditemukan kesamaan dalam *level* kerentanan pada Acunetix *Web Vulnerability Scanner* dan *Pentest Tools Website Vulnerability Scanner,* 4 *level* kerentanan tersebut diantaranya *High Risk Alert Level* 3, *Medium Risk Alert Level* 2, *Low Risk Alert Level* 1, dan, *Informational Alert* seperti peringatan kerentanan pada Tabel 1 berikut ini.

Tabel 1. Peringatan kerentanan

Peringatan Kerentanan		
Kategori Level Acunetix	Kategori Level Pentest-Tools	Tingkatan
High Risk Alert	High	Level 3
Medium Risk Alert	Medium	Level 2
Low Risk Alert	Low	Level 1
Informational Alert	Information	-

Peringatan kerentanan yang pertama yaitu *High Risk Alert* dan *High* dengan *Level* 3 merupakan kategori kerentanan yang paling berbahaya sehingga target pemindaian memiliki resiko maksimum apabila terjadi peretasan dan pencurian data. Kedua pada *Medium Risk Alert* dan *Medium* dengan *Level* 2 penyebab kerentanan yaitu kelemahan pengkodean situs dan kesalahan konfigurasi *server*, hal ini berakibat mampu memfasilitasi gangguan dan penyusupan *server.* Peringatan ketiga yaitu *Low Risk Alert* dan *Low* dengan *Level* 1 penemuan kerentanan karena pengungkapan jalur direktori atau kurang enkripsi lalu lintas data. Kemudian pada *Informational Alert* dan *Information* merupakan informasi mengenai penemuan beberapa *item* yang dianggap menarik selama proses pemindaian, misalnya penemuan informasi layanan selama pemindaian, penemuan pencocokan *string* pencarian pada *Google Hacking Database*, kemungkinan pengungkapan alamat *email* maupun IP internal.

4. Hasil dan Pembahasan

Sesuai panduan pada NIST SP 800-115 maka beberapa tahapan yang telah disampaikan sebelumnya mulai dijabarkan pada bagian ini. Hasil pemindaian *website e-government* pemkab Semarang yaitu semarangkab.go.id menggunakan Acunetix *Web Vulnerability Scanner* didapati kerentanan tingkat menengah atau *Medium Risk Alert Level* 2 dan hasil yang sama dengan pemindaian menggunakan Pentest-Tools *Website Vulnerability Scanner* yaitu ditemukan kerentanan tingkat menengah (*Medium*). Pada *website e-government* pemdes Gunung Tumpeng yaitu gunungtumpeng.id dengan kerentanan tingkat menengah atau *Medium Risk Alert Level* 2 dan temuan pemindaian menggunakan Pentest-Tools *Website Vulnerability Scanner* ditemukan pula kerentanan tingkat menengah (*Medium*).

4.1. Struktur dan Fitur Website

4.1.1. Website semarangkab.go.id

Struktur *Website* Pemkab Semarang yaitu semarangkab.go.id diawali *Homepage* (halaman utama) yang terdiri dari beberapa bagian yang diarahkan ke *link website subdomain* OPD (Organisasi Perangkat Daerah)(Nugraha, 2018) antara lain *Website* Utama, Lapor Bupati, Produk

Hukum, *Open Data*, LPSE, PPID, SIMPEDA, Aset Digital, SIRUP, SIPENDUK *Online*, SIMMISKIN, SIMTARU, SIPP, SME, E-SAKIP, PATEN, *Dashboard*, WBS KPK, SIPARTO, dan Lapor!. *Website* Utama terdiri dari Profil, Informasi Publik, Lapor Bupati, Perangkat Daerah, Aksi PPK, APBD, Publikasi Statistik, Tanggap COVID-19.

Fitur yang dimiliki *Website* Pemkab semarangkab.go.id antara lain:

a. Kontak: berisi layanan untuk menghubungi pihak pemerintah kabupaten dengan terdapat *form* pada halaman Lapor Bupati, alamat *email*, nomor whatsapp, dan nomor telepon.
b. *Blog*: berisi artikel maupun berita sebagai bukti keterbukaan informasi, seperti Kabar Kabupaten Semarang, Pengumuman, Ruang Anak,
c. *Bar* Pencarian: terdapat bilah pencarian untuk memudahkan penelusuran.
d. *Secure Socket Layers* (SSL): terdapat sertifikat keamanan pada alamat *web*.

4.1.2. Website gunungtumpeng.id

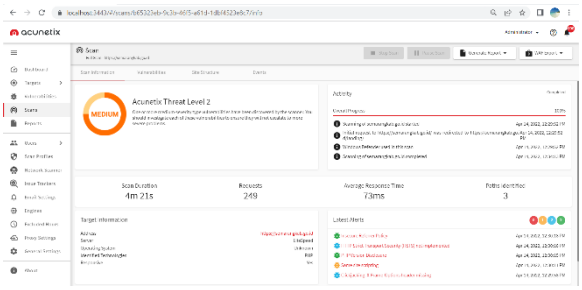
Struktur *Website* Desa gunungtumpeng.id dimulai dari halaman *Homepage* (halaman utama) yang berisi Profil Desa, Kependudukan, *Marketplace*, dan Perpustakaan. Halaman pertama adalah Profil Desa memiliki gambaran umum tentang desa dan disamping itu terdapat *Home*, Profil Desa, Monografi, Berita, Produk Hukum, Galeri, dan Hubungi. Halaman kedua yaitu Kependudukan berisi berbagai *form* layanan dokumen-dokumen kependudukan contohnya Permohonan Akta, Permohonan KTP, Surat Keterangan, Surat Kelahiran, Surat Kematian, dan lainnya. Halaman ketiga adalah *Marketplace* merupakan layanan pasar *online* untuk masyarakat desa dimana terdapat *Home*, Kategori Produk, Cara Beli, Cara Bayar, Jadi Penjual. Keempat yaitu halaman Perpustakaan yang menyediakan layanan informasi perpustakaan yang diarahkan untuk dapat mengakses *e-book digital* yang dihubungkan dengan *link* Dinas Perpustakaan Kabupaten.

Fitur yang dimiliki *Website* Desa gunungtumpeng.id antara lain:

a. *Contact Us*: berisi layanan untuk menghubungi administrator atau pihak Pemerintah Desa Gunung Tumpeng, tersedia *form*, email dan nomor telepon.
b. *Blog*: berisi artikel maupun berita sebagai bukti keterbukaan informasi, seperti Monografi, Sejarah Desa, artikel produk pasar *online*, dan lainnya.
c. *Marketplace*: berisi layanan jual beli *online* produk merupakan hasil produksi warga desa dan UMKM.(Singgalen *et al.*, 2020)

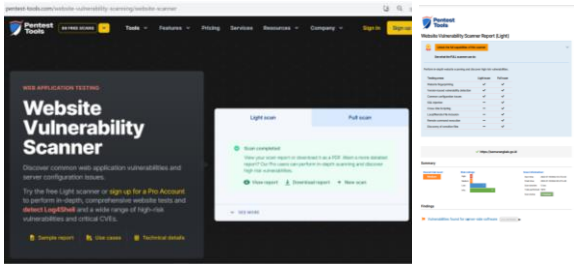
4.2. Hasil Pemindaian Website https://semarangkab.go.id

Uji menggunakan alat Acunetix *Web Vulnerability Scanner* berlangsung selama 4 menit 21 detik, kecepatan rata-rata waktu respon 73 m/s, waktu respon maksimum 296 m/s, jumlah permintaan sebanyak 249. Tampilan hasil pemindaian *website* Pemkab Semarang menggunakan Acunetix adalah seperti pada Gambar 4.



Gambar 4. Hasil Pemindaian https://semarangkab.go.id dengan Acunetix

Uji menggunakan alat Pentest-Tools *Website Vulnerability Scanner* berlangsung selama 12 detik, waktu persiapan selama 30 menit dan menghasilkan 19 temuan kerentanan. Tampilan hasil pemindaian *website* Pemkab Semarang menggunakan Pentest-Tools adalah seperti pada Gambar 5.



Gambar 5. Hasil Pemindaian https://semarangkab.go.id dengan Pentest-Tools

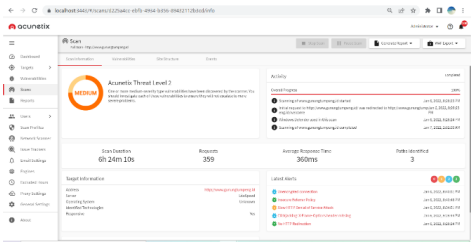
Tabel perbadingan hasil pemindaian *website* Pemkab Semarang menggunakan kedua alat penilaian kerentanan yaitu Acunetix dan Pentest-Tools berdasarkan panduan dokumen pada NIST dan OWASP adalah seperti pada Tabel 2.

4.3. Hasil Pemindaian Website http://www.gunungtumpeng.id

Dengan alat Acunetix *Web Vulnerability Scanner* berlangsung selama 6 jam 24 menit, kecepatan rata-rata waktu respon 360 m/s, waktu respon maksimum 7522 m/s, jumlah permintaan sebanyak 359. Tampilan hasil pemindaian *website* Pemdes Gunung Tumpeng menggunakan Acunetix adalah seperti pada Gambar 6.

Tabel 2. Hasil pemindaian https://semarangkab.go.id

	Hasil Pemindaian					
	Kategori	Jumlah Kerentanan	Dampak	Dokumen *Developer Cheat Sheet Series*	Dampak	Dokumen OWASP *Top* 10
Acunetix	*Medium Risk Alert*	1			▪ *Same Site Scripting*	▪ A07:2017 *Cross-Site Scripting* (XSS)
	Low Risk Alert	2	▪ *Clickjacking: header X-Frame-Options* hilang ▪ HTTP *Strict Transport Security* (HSTS) tidak dilaksanakan	▪ *Clickjacking Defense Cheat Sheet* ▪ HTTP *Strict Transport Security Cheat Sheet*		
	Informational Alert	2	▪ *Referrer Policy* Tidak Aman	▪ *HTTP Headers*	▪ Pengungkapan Versi PHP	▪ A3:2017-*Sensitive Data Exposure*
Pentest-Tools	*Medium*	1			▪ Ditemukan kerentanan untuk *server-side software*	▪ A09:2017 *Using Components with Known Vulnerabilities*
	Low	7	▪ *Header* keamanan tidak ada: *Content-Security-Policy* ▪ *Header* keamanan tidak ada: X-*Frame-Options* ▪ *Header* keamanan tidak ada: X-XSS-*Protection* ▪ *Header* keamanan tidak ada: X-*Content-Type-Options* ▪ *Header* keamanan tidak ada: *Referrer- Policy* ▪ Header keamanan tidak ada: *Strict-Transport-Security*	▪ *Content Security Policy* ▪ *Clickjacking Defense* ▪ *HTTP Headers* ▪ *HTTP Headers* ▪ *HTTP Headers* ▪ *HTTP Strict Transport Security*	▪ Ditemukan perangkat lunak dan teknologi *server*	▪ A06:2017 *Security Misconfiguration* ▪ A06:2017 *Security Misconfiguration* ▪ A06:2017 *Security Misconfiguration* ▪ A06:2017 *Security Misconfiguration* ▪ A06:2017 *Security Misconfiguration* ▪ A06:2017 *Security Misconfiguration*
	Info	11	▪ *File Security*.txt hilang ▪ Situs *web* dapat diakses ▪ Tidak ditemukan apapun untuk daftar direktori ▪ Tidak ditemukan apapun untuk Http*Only flag of cookie* ▪ Tidak ditemukan apapun untuk domain yang terlalu longgar untuk *cookie*. ▪ Tidak ditemukan apapun untuk kebijakan akses klien. ▪ Tidak ditemukan apapun untuk komunikasi yang aman ▪ Tidak ditemukan apapun untuk metode *debug* HTTP yang diaktifkan ▪ Tidak ditemukan apapun untuk penggunaan sertifikat yang tidak dipercaya ▪ *File robots*.txt tidak ada ▪ Tidak ada yang ditemukan untuk *Secure flag of cookie*			▪ A06:2017 *Security Misconfiguration*



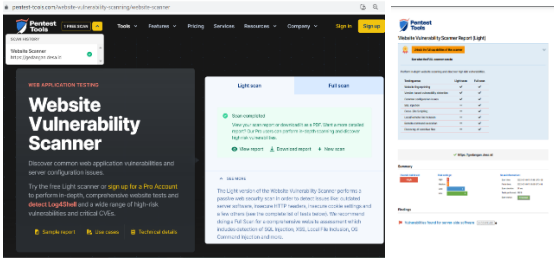
Gambar 6. Hasil Pemindaian http://www.gunungtumpeng.id dengan Acunetix

Uji menggunakan alat Pentest-Tools *Website Vulnerability Scanner* berlangsung selama 18 detik, waktu persiapan selama 45 menit dan menghasilkan 19 temuan kerentanan. Tampilan hasil pemindaian *website* Pemdes Gunung Tumpeng menggunakan Pentest-Tools adalah seperti pada Gambar 7.

Hasil pemindaian *website* Pemdes Gunung Tumpeng panduan dokumen pada NIST dan OWASP adalah seperti pada Tabel 3

Tabel 3. Hasil Pemindaian http://www.gunungtumpeng.id

	Hasil Pemindaian					
	Kategori	Jumlah Kerentanan	Dampak	Dokumen *Developer Cheat Sheet Series*	Dampak	Dokumen OWASP *Top* 10
Acunetix	*Medium Risk Alert*	1	▪ Serangan *Denial of Service* HTTP Lambat	▪ *Denial of Service*		
	Low Risk Alert	2	▪ *Clickjacking: header* X-*Frame-Options* hilang ▪ Koneksi tidak terenkripsi	▪ *Clickjacking Defense Cheat Sheet* ▪ *Password and Cryptographic Storage*		▪ A3:2017-*Sensitive Data Exposure*
	Informational Alert	2	▪ *Referrer Policy* Tidak Aman ▪ Tidak ada Pengalihan HTTP	▪ HTTP *Headers* ▪ *Unvalidated Redirects and Forwards Cheat Sheet*	▪	▪
Pentest-Tools	*Medium*	4			▪ Pengaturan *cookie* tidak aman: tidak ada *HttpOnly flag* ▪ Pengaturan *cookie* tidak aman: tidak ada *Secure flag* ▪ Komunikasi dilakukan melalui HTTP yang tidak aman dan tidak terenkripsi ▪ Kerentanan ditemukan untuk *server-side software*	▪ A06:2017 *Security Misconfiguration* ▪ A06:2017 *Security Misconfiguration* ▪ A3:2017-*Sensitive Data Exposure* ▪ A09:2017 *Using Components with Known Vulnerabilities*
	Low	6	▪ Header keamanan tidak ada: *Content-Security-Policy* ▪ Header keamanan tidak ada: X-*Frame-Options* ▪ Header keamanan tidak ada: X-XSS-*Protection* ▪ Header keamanan tidak ada: X-*Content-Type-Options* ▪ Header keamanan tidak ada: *Referrer-Policy* ▪ Perangkat lunak dan teknologi *server* ditemukan	▪ *Content Security Policy Cheat Sheet* ▪ *Clickjacking Defense Cheat Sheet*		▪ A06:2017 *Security Misconfiguration* ▪ A06:2017 *Security Misconfiguration* ▪ A06:2017 *Security Misconfiguration* ▪ A06:2017 *Security Misconfiguration* ▪ A06:2017 *Security Misconfiguration* ▪ A06:2017 *Security Misconfiguration*
	Info	9	▪ *File security*.txt tidak ada ▪ Tidak ada yang ditemukan untuk metode *debug* HTTP yang diaktifkan ▪ Tidak ada yang ditemukan untuk HTTP *header - Strict-Transport-Security* yang hilang ▪ Tidak ada yang ditemukan untuk daftar direktori ▪ Situs *web* dapat diakses ▪ Tidak ada yang ditemukan untuk penggunaan sertifikat yang tidak dipercaya ▪ Tidak ada yang ditemukan untuk *file robots*.txt ▪ Tidak ada yang ditemukan untuk *client access policies* ▪ Tidak ada yang ditemukan untuk *domain* yang terlalu longgar untuk *cookie*			▪ A06:2017 *Security Misconfiguration*



Gambar 7. Hasil pemindaian http://www.gunungtumpeng.id dengan Pentest-Tools

4.4. Pembahasan

Penilaian kerentanan (VA) pada kedua *website e-government* dengan kedua alat *web vulnerability scanner* berada pada tahapan *discovery* dalam proses *vulnerability scanning* sesuai panduan NIST SP 800-115. Kemudian pada tahap *attack* mulai dilakukan analisis dan ditemukan persamaan dalam kategori level ancaman, keduanya memiliki tingkat kerentanan menengah, *medium risk alert* pada alat Acunetix dan *medium* pada alat Pentest-Tools. Persamaan selanjutnya ditemukan pada jumlah kerentanan, kedua *web e-government* memiliki jumlah kerentanan yang sama yaitu 5 temuan pada Acunetix dan 19 temuan pada Pentest-Tools hal ini dapat terjadi karena kedua website memiliki kemiripan fungsi yaitu sebagai portal, yaitu wadah bagi beberapa *link* lainnya, seperti *link* Sipenduk *Online* dan Perpustakaan Digital yang menghubumgkan ke alamat berikutnya. Isi dari website itu sendiri tidak terlalu kompleks dan menggunakan kapasitas yang tidak terlalu besar. Akan tetapi, persamaan jumlah temuan tidak diikuti dengan durasi dan kecepatan pemindaian antara kedua *website e-government*, perbandingan waktu *web* Pemkab dengan Pemdes adalah 1:88 bila dipindai menggunakan Acunetix dan 2:3 saat dipindai menggunakan Pentest-Tools.

Dalam temuan terjadi *gap* jarak waktu antara kedua alat pemindai kerentanan meskipun ditemukan beberapa persamaan pada hasil. Hal ini terjadi karena Pemkab memiliki lebih sedikit *request* pemindaian dibandingkan dengan Pemdes, sehingga proses dapat dilakukan secara lebih singkat. Perbedaan juga didapati dari jenis temuan kerentanan yang dihasilkan. Pada *web* semarangkab.go.id parameter temuan pada resiko ancaman menengah menggunakan OWASP *Top* 10 dengan indeks A07:2017 *Cross-Site Scripting* (XSS) untuk Acunetix dan A09:2017 *Using Components with Known Vulnerabilities* untuk Pentest-Tools. Sedangkan pada *web* gunungtumpeng.id parameter temuan pada resiko ancaman menengah menggunakan dokumen *Developer Cheat Sheet Series* pada point *Denial of Service* untuk Acunetix dan menggunakan OWASP *Top* 10 berindeks A06:2017 *Security Misconfiguration*, A3:2017-*Sensitive Data Exposure*, A09:2017 *Using Components with Known Vulnerabilities* pada Pentest-Tools. Pada resiko keamanan rendah kedua dokumen OWASP menjadi parameter untuk kedua alat *web vulnerability scanner*.

5. Kesimpulan

Berdasarkan hasil pembahasan dengan adanya beberapa persamaan hasil *vulnerability assessment* pada kedua *web e-government* yang telah dijalankan sesuai panduan NIST SP 800-115, maka dapat disimpulkan bahwa akuntabilitas kedua alat *web vulnerability scanner* yang digunakan dapat terbukti. Meskipun terdapat perbedaan resiko yang kemudian dapat saling melengkapi referensi dalam pemberian rekomendasi keamanan. Jenis temuan yang didapatkan pada setiap level kerentanan mengacu pada kedua parameter OWASP, dan kedua dokumen yang disediakan OWASP yaitu OWASP *Top* 10 dan *Developer Cheat Sheet Series* memberikan petunjuk dan penjelasan kompleks untuk membantu pengembang atau pihak pemerintah daerah dalam menentukan langkah preventif selanjutnya melakukan pengambilan keputusan mengenai keamanan informasi pada web e-government yang dikelola. Kualitas konten dari kedua *web e-government* masih terdapat kesenjangan, khususnya pada *web* pemerintah desa, dikarenakan *e-government* pada pemerintah desa belum terdapat acuan resmi mengenai pelaksanaan SPBE. Diharapkan kedepan *web e-government* baik pemkab maupun pemdes dapat sama-sama meningkatkan standar pelayanan dan keamanan informasi.

Saran untuk penelitian selanjutnya dilakukan penelitian selain kerentanan *website*, seperti *web server*, sistem informasi, jaringan, *email*, dan lain sebagainya. Dapat dilakukan pula lanjutan tahap penilaian kerentanan atau *vulnerability assessment* ke tahap pengujian, dan menggunakan standar metode yang lebih bervariasi. Untuk parameter OWASP dapat dicoba menggunakan alat yang dapat bekerja dengan pengembangan OWASP *Top* 10 yang terkini yaitu OWASP *Top* 10 2021. Penggunaan panduan NIST dapat pula mencoba panduan NIST SP 800-55 mengenai Panduan Pengukuran Kinerja untuk Keamanan Informasi maupun NIST SP 800-44 mengenai Pedoman Mengamankan *Server Web* Publik, dengan pemilihan panduan yang lebih relevan dan spesifik dengan tema penelitian.

Daftar Pustaka

Al-fajri, B. H., Fauzi, R., & Mulyana, R., 2020. Perancangan manajemen risiko operasional Spbe / E-Gov Pada kategori risiko infrastruktur, aplikasi, layanan, data dan informasi Berdasarkan Permen Panrb Nomor 5 Tahun 2020 (Studi Kasus : Pemerintah Kota Bandung). Proceeding of Engineering, 7(2), 7364–7372.

Alwi, E.I., Herdianti, H., & Umar, F., 2020. Analisis

keamanan website menggunakan teknik footprinting dan vulnerability scanning. INFORMAL: Informatics Journal, 5(2): 43.

Andoyo, A & Sujarwadi, A., 2015. Sistem informasi berbasis web pada Desa Tresnomaju Kecamatan Negerikaton Kab. Pesawaran. Jurnal TAM (Technology Acceptance Model), 3(1), 1–9.

Dewi, L., 2020. Vulnerability assessment pada situs www.hatsehat.com menggunakan Openvas. Jurnal Akrab Juara, 5(3), 240–246.

Fitri, R., Asyikin, A.N., & Nugroho, A.S.B., 2017. Pengembangan sistem informasi desa untuk menuju tata kelola desa yang baik (good governance) berbasis TIK. POSITIF : Jurnal Sistem dan Teknologi Informasi, 3(2), 99–105.

Hanifah, F., Budiyono, A., Widjajarto, A., 2021. Analisa kerentanan pada Vulnerable Docker menggunakan alienvault dan docker bench for security dengan acuan framework Cis Control, Proceeding of Engineering, 8(5).

Hidayatulloh, S & Saptadiaji, D., 2021. Penetration Testing pada website universitas ARS menggunakan Open Web Application Security Project (OWASP). Jurnal Algoritma, 18(1), 77–86. doi: 10.33364/algoritma/v.18-1.827

Kurniawan, A., 2019. Penerapan Framework OWASP dan Network Forensics untuk analisis, deteksi, dan pencegahan serangan injeksi di sisi Host-Based. Jurnal Telematika, 14(1), 9–18.

Maharani, M.Z., Andrian, H.R. & Ismail, S.J.I., 2017. Analisis keamanan website menggunakan metode scanning dan perhitungan security metriks. E-Proceeding of Applied Science, 3(3), 1775–1782.

Mustanir, A., 2020. Implementasi e government pemerintahan Desa dalam administrasi pelayanan publik (studi kasus web site Desa Kanie Kecamatan Maritengngae Kabupaten Sidenreng Rappang). OSF Preprints,

Nugraha, J.T., 2018. E-Government dan pelayanan publik (studi tentang elemen sukses pengembangan e-government di Pemerintah Kabupaten Sleman). Jurnal Komunikasi dan Kajian Media, 2(1), 32–42.

Silaban, R.C. & Wijaya, E., 2018. Analisis kerentanan website menggunakan metode NIST SP 800-115 dan OWASP di Diskominfo Kabupaten Bandung. Jurnal Ilmiah Komputer dan Informatika.

Singgalen, Y.A., Darojat, E.Z., Wowor, E.F.P., & Sediyono, E., 2020. Perancangan sistem informasi berbasis website menggunakan System Development Life Cycle Waterfall : E-Marketplace Seminar Nasional: Kualitas Sumberdaya Manusia (KUSUMA). Seminar Nasional : Kualitas Sumberdaya Manusia (KUSUMA), 1–15.

Tarigan, B.V., Kusyanti, A. & Yahya, W., 2017. Analisis perbandingan penetration testing tool untuk aplikasi web. Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, 1(3), 206–214.

Yudiana, Y., Elanda, A., & Buana, R.L., 2021. Analisis Kualitas Keamanan Sistem Informasi E-Office Berbasis Website Pada STMIK Rosma dengan Menggunakan OWASP Top 10. CESS (Journal of Computer Engineering, System and Science), 6(2), 185.