Jurnal FORISTEK, Volume 13, No.1, Maret 2023, Hal. 1-12
p-ISSN 2087-8729, e-ISSN 2579-7174
Akreditasi (**SINTA 5**), SK. No. 225/E/KPT/2022
DOI: 10.54757/fs.v14i1.238

ANALISIS PENGUJIAN PENETRASI PADA LAYANAN *HOSTING* MENGGUNAKAN METODE *BLACK BOX* (Studi kasus : *Blogspot, Wordpress* dan *Shared Hosting)*

Aditya Bimandaru[1], Alamsyah[2,], Aryo Nugroho[3]

Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Narotama[1,3]
Jurusan Teknik Elektro Fakultas Teknik Universitas Tadulako[2]
adityabima265@gmail.com[1], alamsyah.zakaria74@gmail.com[2], aryo.nugroho@narotama.ac.id[3]

ABSTRACT

Analyzing the security of hosting services is important to ensure website security. This research was conducted to test the security level of the Village website. By using 15 samples with 5 websites each, on each Hosting service such as Wordpress, Blogspot, and Shared Hosting. With the Black Box method and Google dork to find the target website to be tested. Open Web Application Security Project (OWASP) Zed Attack Proxy (ZAP) to find security holes by scanning websites. The results obtained are usually 3 types of vulnerabilities, namely Cross Site Scripting (XSS), Cross-Site Request Forgery (CSRF) Tokens, and Clickjacking. After that, analyze the results by seeing how many warnings you get from the scanning process to find out which hosting service has the highest level of security.

This research aims to help the village government build a secure village website. By choosing a safe hosting service and knowing how to find security holes on the website that has been made, so that you can fix these security holes.

Keywords : Hosting, OWASP, ZAP, XSS, CSRF.

INTISARI

Menganalisa keamanan layanan hosting merupakan hal penting untuk menjamin keamanan website. Penelitian ini dilakukan untuk menguji tingkat keamanan website Desa. Dengan menggunakan 15 sampel dengan masing-masing 5 website, pada setiap layanan Hosting seperti Wordpress, Blogspot, dan Shared Hosting. Dengan metode Black Box serta Google dork Untuk menemukan target website yang akan diuji. Open Web Application Security Project (OWASP) Zed Attack Proxy (ZAP) untuk menemukan celah keamanan dengan memindai website. Hasil yang didapat biasanya terdapat 3 jenis kerentanan yaitu Cross Site Scripting (XSS), Cross-Site Request Forgery (CSRF) Tokens, dan Clickjacking. Setelah itu, menganalisa hasil dengan cara melihat seberapa banyak peringatan yang didapat dari proses pemindaian untuk mengetahui layanan hosting manakah yang mempunyai tingkat keamanan yang paling tinggi.

Peneltian ini bertujuan untuk membantu pemerintah Desa membangun website Desa yang aman. Dengan memilih layanan hosting yang aman serta mengetahui cara menemukan celah keamanan pada website yang telah dibuat, sehingga dapat memperbaiki celah keaman tersebut.

Kata kunci: *Hosting, OWASP, ZAP, XSS, CSRF.*

I. PENDAHULUAN

Perkembangan Teknologi semakin berkembang [1]. Dahulu orang menyalurkan informasi menggunakan media cetak seperti koran dan majalah [2]. Sehingga memerlukan kertas untuk dicetak dengan tinta, hal ini mengakibatkan, gangguan pada lingkungan dan tidak efisien, tetapi sekarang bisa menggunakan *Website* dengan berbagai macam layanan *hosting* untuk menyimpan data informasi lalu disalurkan ke semua orang yang mengaksesnya melalui internet.

Dengan pesatnya perkembangan teknologi [3]. Mengakibatkan semua layanan *hosting* memperkuat pertahanan keamanan dari adanya serangan *Hacker,* yaitu seseorang yang mempunyai kemampuan untuk memasuki celah keamanan dengan bahasa pemrograman tertentu serta jaringan komputer, sehingga bisa mengambil data informasi yang ada didalamnya [4]. Melihat

Jurnal FORISTEK, Volume 13, No.1, Maret 2023, Hal. 1-12
p-ISSN 2087-8729, e-ISSN 2579-7174
Akreditasi (**SINTA 5**), SK. No. 225/E/KPT/2022
DOI: 10.54757/fs.v14i1.238

kasus seperti itu, Kita juga harus pintar memilih layanan *hosting* apa yang paling aman untuk menyimpan data informasi kita. karena jika data informasi, Kita telah diambil dapat disalahgunakan dan menyebabkan kerugian, Indonesia juga tercatat sebagai negara yang masihlambat dalam mengikuti perkembangan teknologi komunikasi modern [5]. Sehingga Indonesia sangat rentan terhadap serangan siber [6].

Celah keamanan ada berbagai macam, yaitu melalui jaringan komputer maupun internet, *syntax* pemrograman, protokol jaringan, dan domain atau subdomain yang telah digunakan [7]. Yang semua itu sudah disediakan oleh layanan *hosting*, jika layanan *hosting* yang kita pakai keamanannya lemah, serta mempunyai banyak celah keamanan mengakibatkan mudahnya data diambil oleh *Hacker* [8].

Tujuan penelitian ini dilakukan untuk menemukan celah keamanan [9]. *Website* yang menggunakan layanan hosting yang berbeda, dengan cara yang mudah menggunakan OWASP ZAP, agar dapat memperbaiki celah keamanan tersebut [10]. Berdasarkan studi kasus di beberapa layanan hosting seperti *blogspot*, *wordpress*, dan *shared hosting*. Akan diambil beberapa *website* pemerintahan yang ada di Desa, untuk dilakukan pengujian, dengan kriteria, *website* menyediakan banyak informasi di dalamnya, seperti agenda kegiatan, Berita,dan layanan sosial yang ada di Desa, serta selalu memberikan informasi terbaru [11]. Penelitian ini dilakukan karena masih banyaknya orang yang tidak mengerti cara menemukan celah keamanan *website* dan memilih layanan *hosting* yang mempunyai tingkat keamanan yang tinggi.

Metode yang digunakan juga mudah, karena hanya melakukan pemindaian URL pada *website* menggunakan *OWASP ZAP* [12]. Penelitian ini juga terdapat langkah-langkah untuk menemukan celah keamanan pada *website* beserta penjelasannya [13].

Tujuan yang akan dicapai penelitian ini adalah memberikan edukasi bagaimana memilih layanan *hosting* yang aman dan bagaimana menemukan celah keamanan pada *Website* [14].

II. LANDASAN TEORI

A. Pengujian Penetrasi

Penetrasi adalah pengujian keamanan untuk menentukan kerentanan yang terdapat pada sistem. Kerentanan yaitu suatu kelemahan yang dapat diserang sehingga mengganggu atau mendapatkan akses ke sistem dan data informasi didalamnya. Pengujian penetrasi juga mempunyai 3 metode pengujian yaitu, black box pengujian yang dilakukan untuk mengamati hasil input dan output dari sistem tanpa mengetahui struktur dari sistem yang ada, white box pengujian sistem dengan cara menganalisa dan meneliti struktur internal dan kode, serta grey box pengujian untuk mengetahui permasalahan dan kekurangan dalam sebuah sistem dengan hanya menguji fungsi-fungsi komponen.

B. Hosting

Tempat untuk menyimpan semua data informasi yang ada di website berupa video, gambar, email, kode pemrograman, aplikasi, dan database. Yang dapat diakses banyak orang dengan internet. Cara kerja hosting adalah pada saat mengakses atau membuka alamat situs web, internet akan mengirim permintaan akses ke server hosting. Kemudian server akan merespon dengan mengirim kembali data informasi dari alamat website yang dicari dalam bentuk tulisan maupun gambar.

III. METODE PENELITIAN

Pada penelitian ini menggunakan metode *black box* [15] yaitu pengujian pada *website* yang telah menggunakan layanan *hosting* tanpa dibekali informasi apapun tentang sistem, infrastruktur, maupun *source code* yang terdapat di dalamnya agar tau layanan *hosting* mana yang mempunyai tingkat keamanan yang tinggi pada studi kasus.

Berikut alur metode penelitian atau langkah - langkah yang akan dilakukan pada penelitian ini :

Jurnal FORISTEK, Volume 13, No.1, Maret 2023, Hal. 1-12
p-ISSN 2087-8729, e-ISSN 2579-7174
Akreditasi (**SINTA 5**), SK. No. 225/E/KPT/2022
DOI: 10.54757/fs.v14i1.238

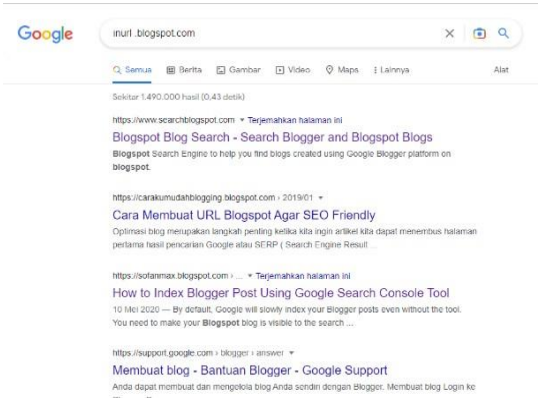
.

A. Alur Atau Langkah - Langkah Metodologi Penelitian

Gambar 1. Alur Atau Langkah – Langkah Metodologi Penelitian.

Gambar 1 penjelasan alur metode penelitian pada gambar 2.1 Alur atau langkah - langkah metodologi penelitian berdasar urutannya.

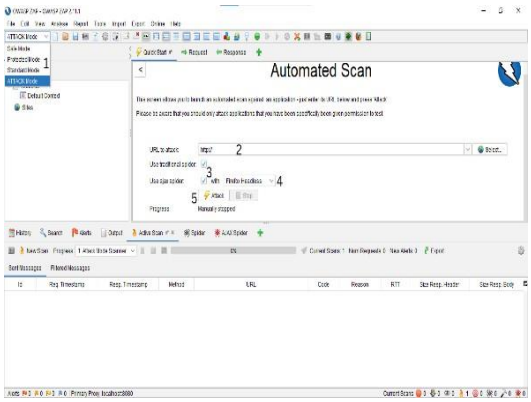
B. Analisa Menggunakan Google Dork



Gambar 2. Analisa Menggunakan Google Dork

Gambar 2 menunjukan tahap awal yang dilakukan adalah melakukan analisa dengan menggunakan *google dork* untuk menemukan *website* yang menggunakan layanan *hosting*, seperti pada studi kasus yang akan dilakukan pengujian. *Inurl* yaitu menyematkan pencarian *URL* didalamnya dan dan *site* untuk mencari alamat domain *website* yang lebih spesifik.. dengan *google dork* membantu melakukan pencarian dengan akurat [16].

C. Pemilihan Input



Gambar 3. Pemilihan Input

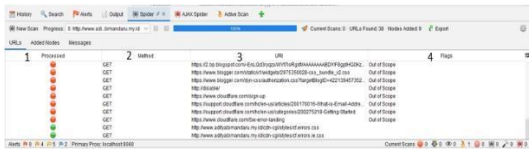
Gambar 3 menunjukan cara pemilihan input, seperti berikut :

1. Pilih metode *attack mode*.
2. Masukan alamat *website* di kolom *URL to attack*.
3. Centang *traditional spider* dan *ajax spider*, *traditional spider* [17]. Merupakan fitur untuk mengidentifikasi semua halaman maupun *URL* yang terhubung pada *website* yang biasa disebut *hyperlink* sedangkan ajax spider fitur untuk mengumpulkan konten dari situs *web* ke indeks yang dapat diakses.
4. Pilih *browser* sebagai pendukung selama proses pemindaian, Saya menggunakan *firefox Headless* dikarenakan lebih ringan.
5. Tekan *Attack* untuk memulai pemindaian.

D. Pemilihan Output

Setelah selesai maka akan keluar hasil dari pemindaian dari *traditional spider* dan ajax *spider*, serta peringatan yang muncul karena terdapat celah keamanan di dalamnya meliputi risiko ancaman tingkat rendah menengah dan tinggi.

E. Traditional Spider



Gambar 4. *Traditional Spider*

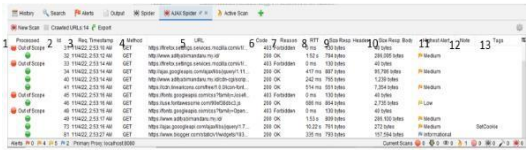
Gamabar 4 menunjukan fitur yang digunakan untuk memindai *URL* yang terkait pada *website*

Jurnal FORISTEK, Volume 13, No.1, Maret 2023, Hal. 1-12
p-ISSN 2087-8729, e-ISSN 2579-7174
Akreditasi (**SINTA 5**), SK. No. 225/E/KPT/2022
DOI: 10.54757/fs.v14i1.238

untuk menemukan celah keamanan. Berikut Gambar dan penjelasannya :

1. *Processed* Jika berwarna merah maka *URL* yang dipindai gagal seperti respon tidak diterima, terjadi kesalahan saat merespon, serta tidak diberikan akses, dan jika hijau *URL* tersebut berhasil dipindai.
2. *Method* adalah cara pemindaian *URL* terkait, dengan menggunakan *GET* yaitu, akan menampilkan data pada *URL* dan *POST* yaitu, mengirimkan data langsung ke *action* untuk ditampung.
3. *URL* singkatan dari *Uniform Resource Locator* atau yang biasa disebut alamat atau *link* dalam *website.*
4. Flags yaitu informasi tentang *URL*, jika *Out of Scope* maka URL yang dipindai tidak termasuk dari *website* tetapi terkait, dan jika *Seed* artinya *URL* tersebut berasal dari *website* yang diuji.

F. Ajax Spider

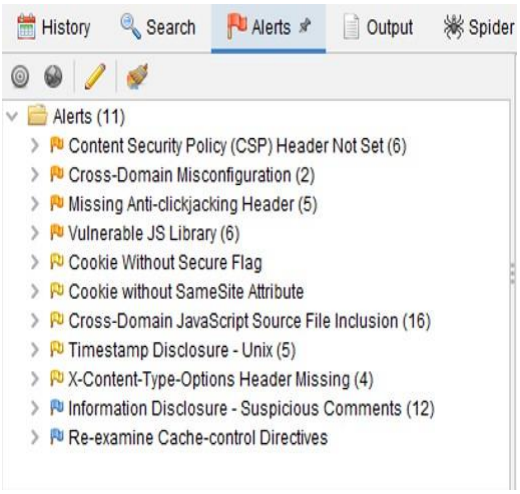


Gambar 5. *Ajax Spider*

Gambar 5 menunjukkan fitur memindai *URL website*terkait dengan mengekstrak *javascript* di dalamnya hingga menemukan celah keamanan. Berikut gambar dan penjelasannya :

1. *Processed* jika berwarna hijau berhasil dan merah gagal sama seperti *traditional spider.*
2. *Id* adalah urutan nomor pemindaian, terkadang tidak urut karena tergantung koneksi internet dan berapa lama proses pemindaian.
3. *Req. Timestamp* adalah permintaan waktu pemindaian *URL* dilakukan.
4. *Method* sama dengan *traditional spider* menggunakan *GET* dan *POST.*
5. *URL* sama seperti *traditional spider* yaitu *link* atau alamat *website* terkait.
6. *Code* adalah kode respon dari pemindaian, jika 403 artinya gagal dan 200 artinya berhasil.
7. *Reason* adalah alasan dari hasil pemindaian yang telah dilakukan jika berhasil mendapat akses maka akan OK dan jika gagal Forbidden.
8. *RTT* juga disebut *Round Trip Time* yaitu ukuran dalam waktu milidetik saat memulai permintaan jaringan dan menerima respon.
9. *Size resp. Header* adalah ukuran respon data *header* yang diterima, saat memindai *URL* dalam *website* terkait.
10. *Size resp. Body* adalah ukuran respon data *body* yang diterima, saat memindai *URL* dalam *website* terkait.
11. *Highest Alert* adalah tanda peringatan bahwa telah ditemukan celah keamanan pada saat pemindaian *URL website*, dari tingkat resiko rendah, menengah, dan tinggi.
12. *Note* adalah catatan yang akan didapat jika, ditemukan celah keamanan dengan tingkat resiko yang tinggi.
13. *Tags* adalah tanda dimana letak kesalahan yang didapat mudah diperbaiki.

G. Seleksi Output



Gambar 6. Seleksi *Output*

Gambar 6 menunjukan pemilihan celah keamanan hasil dari proses pemindaian seperti :

1. *Cross Site Scripting (XSS)* merupakan salah satu jenis serangan dengan memasukan kode bahasa pemrograman dengan tujuan untuk

Jurnal FORISTEK, Volume 13, No.1, Maret 2023, Hal. 1-12
p-ISSN 2087-8729, e-ISSN 2579-7174
Akreditasi (**SINTA 5**), SK. No. 225/E/KPT/2022
DOI: 10.54757/fs.v14i1.238

mengambil data penting, mengambil *cookie* dari user atau mengirimkan suatu program yang dapat merusak pengguna, tetapi penyebabnya seperti dari *web* itu sendiri [18].

2. *Cross-Site Request Forgery (CSRF)* adalah serangan eksploitasi *web* yang membuat pengguna tanpa sadar mengirim sebuah permintaan atau *request* ke *website* yang sedang digunakan, dengan cara menyematkan link pada gambar atau yang lainnya [19]. Apabila setelah di klik, akan diarahkan ke sebuah *web* yang mengandung kode berbahaya. Kode tersebut dibuat agar pengguna dapat langsung terkena serangan dengan satu kali klik. Maka *CSRF* juga sering disebut *one click attack.* Jenis serangan *CSRF* ada 2 yaitu :
   a. *Stored*

Yaitu serangan dengan memanfaatkan aplikasi *website* yang akan diserang untuk menyalurkan *exploit URL* sehingga akan dianggap *request* atau permintaan tersebut asli dari pengguna internet.

   b. *Reflected*

Serangan dengan memanfaatkan sistem di luar aplikasi *website* target untuk menyalurkan *exploit URL* menggunakan email, konten serta kolom komentar.

3. Clickjacking merupakan serangan pada aplikasi *web* yang membuat korbannya tidak sengaja mengklik dengan menumpangkan konten berbahaya pada elemen asli seperti tombol dengan dibuat tidak terlihat [20]. Contohnya pada sebuah *website* terdapat pilihan tombol *"Download"* tetapi di atas tombol ditumpangkan konten tidak terlihat sehingga saat klik tombol tersebut penyerang menghubungkan halaman email kita dengan sebuah tombol "hapus semua pesan" tanpa disadari. Sehingga serangan ini juga disebut jebakan klik.

H. Pengujian

Dalam pengujian menggunakan beberapa serangan seperti, *XSS,CSRF*, dan *Clickjacking*.

I. Review Hasil

Hasil dari pengujian dengan melakukan serangan dari celah keamanan yang sudah ditemukan selama proses pemindaian dengan *OWASP ZAP* [21].

IV. HASIL PENELITIAN DAN PEMBAHASAN

Penelitian yang telah dilakukan pada tahap ini menggunakan metode *black box*. Data yang digunakan merupakan data yang telah melalui tahap pemindaian menggunakan OWASP ZAP. Pada proses pemindaian *website* menggunakan *Spider* untuk memindai *URL* yang ada dalam *website,* menggunakan *ajax spider* untuk mengekstrak *java script* di dalam *URL,* hingga *Active Scan* mencapai 100%. Sedangkan untuk mendapatkan data alamat *website* menggunakan *google dork.*

A. Hasil Analisis

Hasil analisis untuk mencari target *website* yang menggunakan layanan yang berbeda seperti *wordpress, blogspot* dan *shared hosting* yang dikhususkan mencari *website* Desa dengan menggunakan *google dork*. Sehingga mendapatkan masing-masing 5 *website* dengan penggunaan layanan yang berbeda. Berikut hasilnya :

B. Blogspot

Berdasarkan hasil pencarian *google dork* menggunakan :
[situs desa *inurl*:*blogspot*] telah ditemukan 5 alamat *website* yang menggunakan layanan *blogspot*. Berikut hasil yang telah didapat :

1. http://www.bantarjaya.web.id/
2. https://www.desakahayya.id/
3. https://www.santur.desa.id/
4. https://tanjungtelang.kotaprabumulih.go.id/
5. https://wingkoharjo.blogspot.com/

C. Wordpress

Berdasarkan hasil pencarian *google dork* menggunakan :

Jurnal FORISTEK, Volume 13, No.1, Maret 2023, Hal. 1-12
p-ISSN 2087-8729, e-ISSN 2579-7174
Akreditasi (**SINTA 5**), SK. No. 225/E/KPT/2022
DOI: 10.54757/fs.v14i1.238

.

- [situs desa *inurl*:*admistrator*]
- [situs desa *site*:*wordpress.com*]
- [situs desa *inurl*:*admin*]
- [situs desa *site*:desa.id]
- [situs desa *inurl*: tanjung agung-seluma]

telah ditemukan 5 alamat *website* yang menggunakan layanan *wordpress*. Berikut hasil yang telah didapat :

1. https://desapesanggrahan.id/
2. https://jatiandesa.wordpress.com/
3. https://lipatkainselatan.desa.id/
4. https://www.panggungharjo.desa.id/
5. https://tanjungagung-selbar.desa.id/

D. Shared Hosting

Berdasarkan hasil pencarian *google dork* menggunakan

- [situs desa *inurl*:*login*]
- [situs desa *inurl*:*admin*]
- [situs desa *site*:*.com*]
- [situs desa *inurl*:kopo]
- [situs desa *inurl*:turungan]

telah ditemukan 5 alamat *website* yang menggunakan layanan *shared hosting*. Berikut hasil yang telah didapat :

1. https://desalamunretengah.co.id/
2. https://desasidomulyo.com/
3. https://www.jembayantengah.com/
4. https://kopo.desa.id/
5. https://turunganbaji.desa.id/

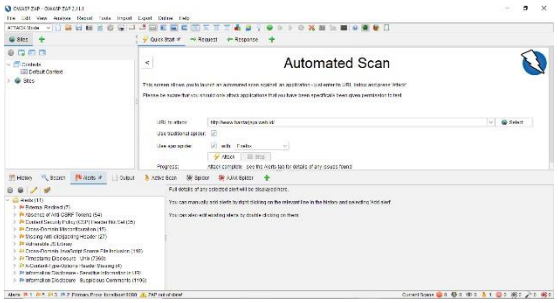
E. Hasil Pemindaian Website

Website yang sudah ditemukan menggunakan *google dork* dan sesuai kriteria akan dipindai atau *attack*, serta pengujian menggunakan *OWASP ZAP* dengan memilih *attack* mode, *spider* dan *ajax spider* sebagai pendukung. Jumlah tingkat kerentanan keamanan bisa dilihat di bawah pojok kiri. Pertama gambar bendera warna merah menandakan kerentanan keamanan tingkat tinggi, warna oranye tingkat menengah dan kuning tingkat rendah. Berikut hasil pemindaiannya :

F. Blogspot

Pada hasil pemindaian *website* Desa, yang menggunakan layanan *Blogspot*. Dengan *OWASP ZAP*, telah menemukan kerentanan keamanan. Tingkat tinggi, menengah dan rendah pada fitur *alerts* yang ada di *OWASP ZAP*. Berikut hasilnya:

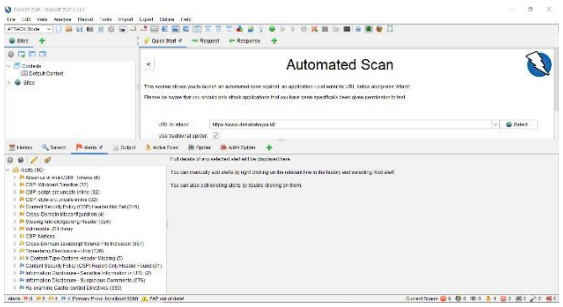
G. Website Desa Bantarjaya Bogor



Gambar 7. *Alerts* Desa Bantarjaya Bogor

Gambar 7 menunjukan *website* Desa Bantarjaya Bogor telah ditemukan kerentanan keamanan. Tingkat tinggi dengan jumlah 1, tingkat menengah 5 dan tingkat rendah 3.

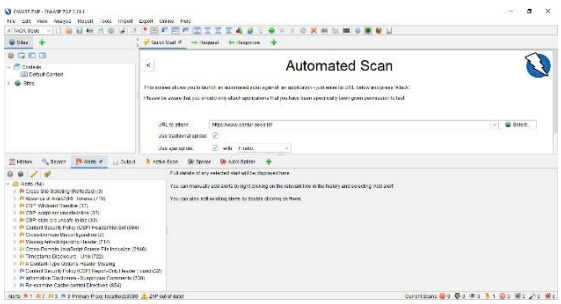
H. Website Desa Kahayya



Gambar 8. *Alerts* Desa Kahayya

Gambar 8 menunjukan *website* Desa Kahayya telah ditemukan kerentanan keamanan. Tingkat menengah dengan jumlah 8 dan tingkat rendah 4.

I. Website Desa Santur



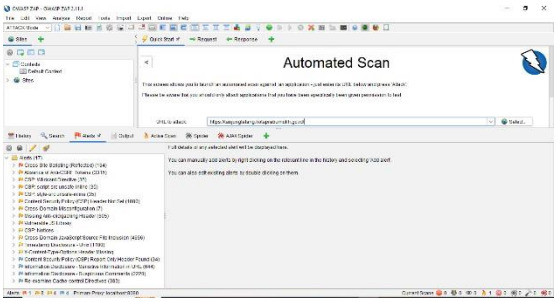
Jurnal FORISTEK, Volume 13, No.1, Maret 2023, Hal. 1-12
p-ISSN 2087-8729, e-ISSN 2579-7174
Akreditasi (**SINTA 5**), SK. No. 225/E/KPT/2022
DOI: 10.54757/fs.v14i1.238

.

Gambar 9. *Alerts* Desa Santur

Gambar 9 menunjukan *website* Desa Santur telah ditemukan kerentanan keamanan. Tingkat tinggi dengan jumlah 1, tingkat menengah 7 dan tingkat rendah 3.

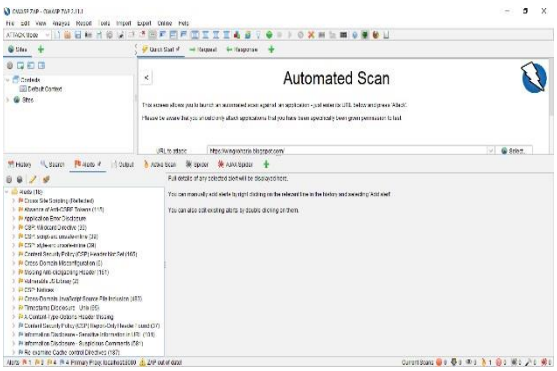
J. Website Desa Tanjung Telang



Gambar 10. *Alerts* Desa Tanjung Telang

Gambar 10 menunjukan *website* Desa Tanjung Telang telah ditemukan kerentanan keamanan. Tingkat tinggi dengan jumlah 1, tingkat menengah 8 dan tingkat rendah 4.

K. Website Desa Wingkoharjo



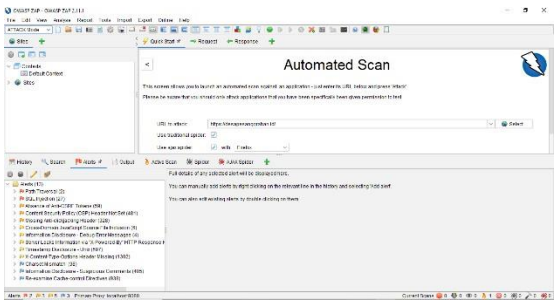
Gambar 11. *Alerts* Desa Wingkoharjo

Gambar 11 menunjukan *website* Desa Wingkoharjo telah ditemukan kerentanan keamanan. Tingkat tinggi dengan jumlah 1, tingkat menengah 9 dan tingkat rendah 4.

L. Wordpress

Pada hasil pemindaian website Desa, yang menggunakan layanan *wordpress*. Dengan *OWASP ZAP*, telah menemukan kerentanan keamanan. Tingkat tinggi, menengah dan rendah pada fitur *alerts* yang ada di *OWASP ZAP*. Berikut hasilnya:

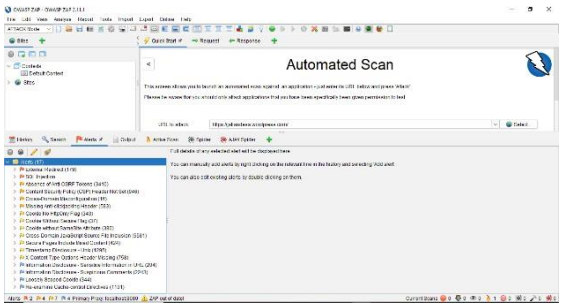
M. Website Desa Pesanggrahan



Gambar 12. *Alerts* Desa Pesanggrahan

Gambar 12 menunjukan *website* Desa Pesanggrahan telah ditemukan kerentanan keamanan. Tingkat tinggi dengan jumlah 2, tingkat menengah 3 dan tingkat rendah 5.

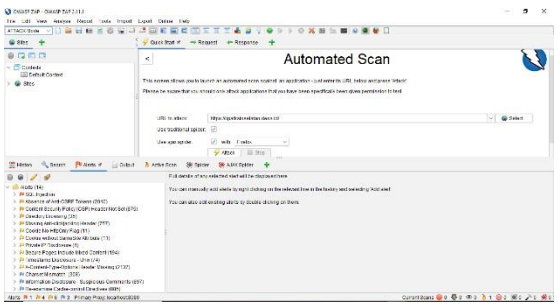
N. Website Desa Jatian



Gambar 13. *Alerts* Desa Jatian

Gambar 13 menunjukan *website* Desa jatian telah ditemukan kerentanan keamanan. Tingkat tinggi dengan jumlah 2, tingkat menengah 4 dan tingkat rendah 7.

O. Website Desa Lipatkain Selatan



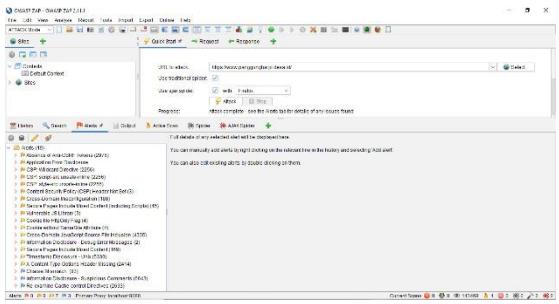
Gambar 14. *Alerts* Desa Lipatkain Selatan

Gambar 14 menunjukan *website* Desa Lipatkain Selatan telah ditemukan kerentanan keamanan. Tingkat tinggi dengan jumlah 1, tingkat menengah 4 dan tingkat rendah 6.

Jurnal FORISTEK, Volume 13, No.1, Maret 2023, Hal. 1-12
p-ISSN 2087-8729, e-ISSN 2579-7174
Akreditasi (**SINTA 5**), SK. No. 225/E/KPT/2022
DOI: 10.54757/fs.v14i1.238

.

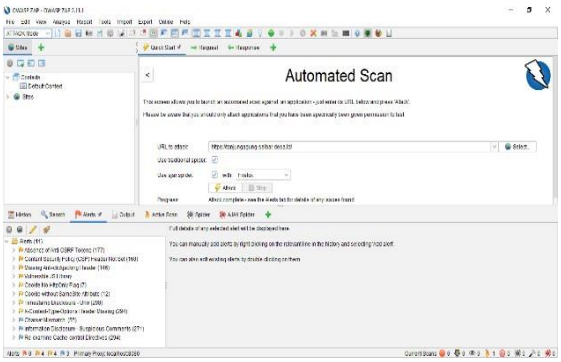
P. Website Desa Panggungharjo



Gambar 15. *Alerts* Desa Panggungharjo

Gambar 15 menunjukan *website* Desa Panggungharjo telah ditemukan kerentanan keamanan. Tingkat menengah dengan jumlah 9 dan tingkat rendah 7.

Q. Website Desa Tanjung Agung



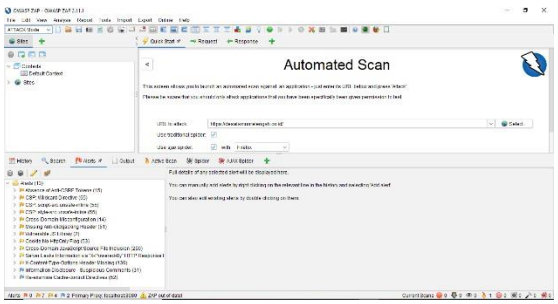
Gambar 16. *Alerts* Desa Tanjung Agung

Gambar 16 menunjukan *website* Desa Tanjung Agung telah ditemukan kerentanan keamanan. Tingkat menengah dengan jumlah 4 dan tingkat rendah 4.

R. Shared Hosting

Pada hasil pemindaian website Desa, yang menggunakan layanan *shared hosting*. Dengan *OWASP ZAP*, telah menemukan kerentanan keamanan. Tingkat tinggi, menengah dan rendah pada fitur *alerts* yang ada di *OWASP ZAP*. Berikut hasilnya :

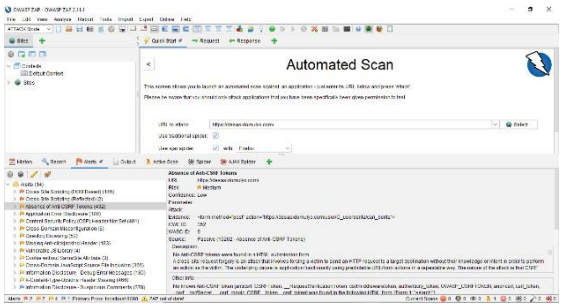
S. Website Desa Lamunre Tengah



Gambar 17. *Alerts* Desa Lamunre Tengah

Gambar 17 menunjukan *website* Desa Lamunre Tengah telah ditemukan kerentanan keamanan. Tingkat menengah 7 dan tingkat rendah 4.

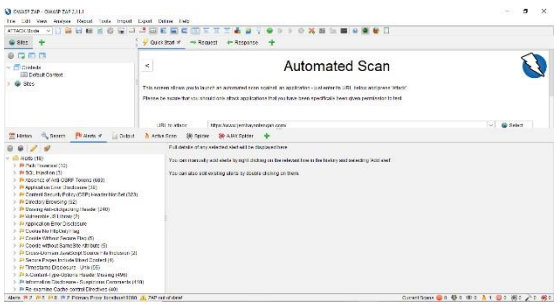
T. Website Desa Sidomulyo



Gambar 18. *Alerts* Desa Sidomulyo

Gambar 18 menunjukan *website* Desa Sidomulyo telah ditemukan kerentanan keamanan. Tingkat tinggi dengan jumlah 2, tingkat menengah 7 dan tingkat rendah 4.

U. Website Desa Jembayan Tengah



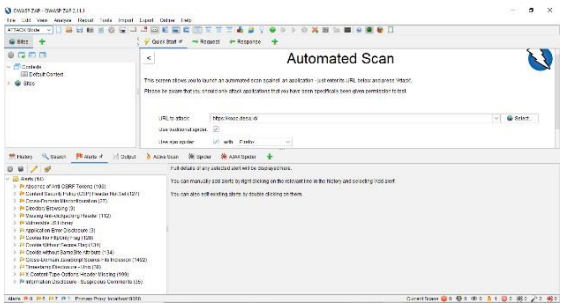
Gambar 19. *Alerts* Desa Jembayan Tengah

Gambar 19 menunjukan *website* Desa Jembayan Tengah telah ditemukan kerentanan keamanan. Tingkat tinggi dengan jumlah 2, tingkat menengah 6 dan tingkat rendah 8.

Jurnal FORISTEK, Volume 13, No.1, Maret 2023, Hal. 1-12
p-ISSN 2087-8729, e-ISSN 2579-7174
Akreditasi (**SINTA 5**), SK. No. 225/E/KPT/2022
DOI: 10.54757/fs.v14i1.238

.

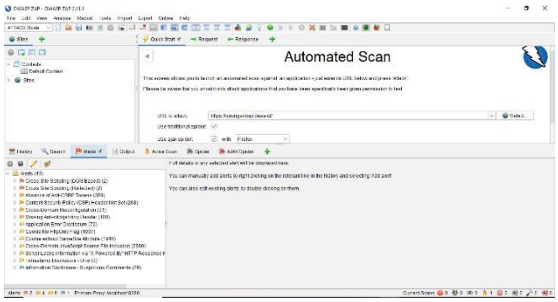
V. Website Desa Kopo



Gambar 20. *Alerts* Desa Kopo

Gambar 20 menunjukan *website* Desa Kopo telah ditemukan kerentanan keamanan. Tingkat menengah 6 dan tingkat rendah 7.

W. Website Desa Turungan Baji



Gambar 21. *Alerts* Desa Turungan baji

Gambar 21 menunjukan *website* Desa Turungan Baji telah ditemukan kerentanan keamanan. Tingkat tinggi dengan jumlah 2, tingkat menengah 4 dan tingkat rendah 6.

X. Review Hasil

Hasil yang sudah didapatkan dari pemindaian serta pengujian menggunakan *OWASP ZAP* berupa, beberapa kerentanan keamanan dengan tingkat rendah, menengah, dan tinggi. Hasil akan di total, berapa jumlah kerentanan keamanan yang ditemukan pada *website*, yang telah dikelompokan jenis layanan dan tingkat kerentanan keamanan. Hasil akan dibuatkan pada tabel 1 seperti berikut:
T = Tinggi
M = Menengah
R = Rendah
Berikut Alamat *Website*(W) sesuai abjad :

A. http://www.bantarjaya.web.id/
B. https://www.desakahayya.id/
C. https://www.santur.desa.id/
D. https://tanjungtelang.kotaprabumulih.go.d
E. https://wingkoharjo.blogspot.com/
F. https://desapesanggrahan.id/
G. https://jatiandesa.*wordpress*.com/
H. https://lipatkainselatan.desa.id/
I. https://www.panggungharjo.desa.id/
J. https://tanjungagung-selbar.desa.id/
K. https://desalamunretengah.co.id/
L. https://desasidomulyo.com/
M. https://www.jembayantengah.com/
N. https://kopo.desa.id/
O. https://turunganbaji.desa.id/

Tabel 1. Jumlah Data Kerentanan Keamanan

Tabulasi	Kerentanan Keamanan				
BLOGSPOT	NO	W	T	M	R
	1	A	1	5	3
	2	B		8	4
	3	C	1	7	3
	4	D	1	8	4
	5	E	1	9	4
TOTAL			4	37	18
WORDPRESS	1	F	2	3	5
	2	G	2	4	7
	3	H	1	4	6
	4	I		9	7
	5	J		4	4
TOTAL			5	24	29
SHARHOST	1	K		7	4
	2	L	2	7	4
	3	M	2	6	8

Jurnal FORISTEK, Volume 13, No.1, Maret 2023, Hal. 1-12
p-ISSN 2087-8729, e-ISSN 2579-7174
Akreditasi (**SINTA 5**), SK. No. 225/E/KPT/2022
DOI: 10.54757/fs.v14i1.238

E I D N G	4	N		6	7
	5	O	2	4	6
TOTAL			6	30	29

Pada Tabel 1 menunjukkan hasil jumlah data kerentanan keamanan *website* Desa, pada masing-masing layanan. Dengan 3 tingkat kerentanan keamanan. Yaitu, tinggi, menengah dan rendah. Kerentanan keamanan tingkat tinggi yang paling sedikit ditemukan pada layanan *blogspot* dengan jumlah total 4, lalu kerentanan keamanan tingkat tinggi paling banyak ditemukan pada layanan *shared hosting* dengan jumlah total 6. Untuk tingkat menengah paling sedikit pada layanan *wordpress* dengan jumlah total 24, dan paling banyak pada layanan *blogspot* dengan jumlah total

37. Serta kerentanan keamanan tingkat rendah paling sedikit pada layanan *blogspot* dengan total

18 dan paling banyak pada layanan *wordpress* serta *shared hosting* yaitu, 29 kerentanan keamanan.

Y. Pembahasan

Setelah mendapatkan data dari *review* hasil dengan menjumlah total kerentanan keamanan pada semua target *website*, lalu akan diberi nilai yaitu, kerentanan keamanan tingkat tinggi 3 poin, menengah 2 poin dan rendah 1 poin.

T = Tinggi

M = Menengah

R = Rendah

BL = *Blogspot*.

WO = *Wordpress*

SH = *Shared Hosting*

TO = Total

LA = Layanan

Tabel 2. Total Nilai Data Kerentanan Keamanan

NO	LA	T	M	R	TO
1	BL	12	74	18	104
2	WO	15	48	29	92
3	SH	18	60	29	107

Pada tabel 2 menunjukan hasil nilai atau poin yang telah diberikan pada masing-masing layanan, yang telah dikelompokan dengan tingkat kerentanan keamanan yang berbeda. Total nilai atau poin yang telah diberikan, dari jumlah total kerentanan keamanan tingkat Tingkat tinggi, menengah dan rendah. Ditemukan paling sedikit pada layanan *wordpress* yaitu, 92 poin dan paling banyak pada layanan *shared hosting* dengan total 107 poin.

V. KESIMPULAN

Penelitian telah dilakukan tentang analis layanan *hosting*, dengan memilih beberapa target *Website* Desa. Dengan metode *black box* menggunakan alat *OWASP ZAP*, untuk memindai target *website*, bahwa telah ditemukan beberapa kerentanan keamanan. Kemudian dijumlahkan dan diberi nilai pada setiap tingkat kerentanan keamanan, serta dikelompokan pada masing-masing layanan. Ditemukan layanan *wordpress* yang telah digunakan untuk membangun *website* Desa memiliki tingkat kerentanan keamanan paling sedikit.

DAFTAR PUSTAKA

[1] L. P. Simarmata, “Perkembangan Teknologi Terhadap Desa Terpencil,” *J. Lex Justitia*, vol. 1, no. 1, Art. no. 1, Jul. 2019, doi: 10.22303/lex.

[2] “Surat Kabar Dan Perkembangan Teknologi: Sebuah Tinjauan Komunikatif | Jurnal Ilmu Politik dan Komunikasi.” https://ojs.unikom.ac.id/index.php/jipsi/article/vie w/3086 (accessed Oct. 12, 2022).

[3] S. E. D. Kurniawan, A. Widodo, and A. Nugroho, “Meningkatkan Sistem Layanan Pelanggan Dengan Pendekatan Framework ITIL,” *JOINTECS J. Inf. Technol. Comput.*

.

Sci., vol. 7, no. 1, Art. no. 1, Feb. 2022, doi: 10.31328/jointecs.v7i1.2550.

[4] M. Y. Dm, V. Yola, D. Maiharani, and E. Dwi, "Analisis Terhadap Modus-Modus Dalam Hukum Cyber Crime," *J. Huk. Polit. DAN ILMU Sos.*, vol. 1, no. 2, Art. no. 2, Jun. 2022, doi: 10.55606/jhpis.v1i2.725.

[5] I. Rosydi, A. Nugroho, and A. Ambarwati, "Sistem Monitoring BTS Pada Perusahaan Telekomunikasi Seluler Berbasis Aplikasi Mobile," *JOINTECS J. Inf. Technol. Comput. Sci.*, vol. 7, no. 3, Art. no. 3, Oct. 2022, doi: 10.31328/jointecs.v7i3.3782.

[6] S. A. M. Babys, "Ancaman Perang Siber Di Era Digital Dan Solusi Keamanan Nasional Indonesia," *Oratio Directa*, vol. 3, no. 1, Art. no. 1, Nov. 2021, Accessed: Oct. 12, 2022. [Online]. Available: https://www.ejurnal.ubk.ac.id/index.php/oratio/ar ticle/view/163

[7] S. F. Maulana and H. Suhendi, "Pengujian Celah Keamanan Jaringan Komputer Pt. Jiona Sejati Dengan Network Penetration Testing," *EProsiding Tek. Inform. Prot.*, vol. 2, no. 1, Art. no. 1, Jul. 2021.

[8] Zulkifli, Samsir, and A. Sirait, "Implementasi Max Length dan Input Type Number Pada Form Login Website Untuk Mencegah Penetrasi SQL Injeksi Secara Paksa," *U-NET J. Tek. Inform.*, vol. 4, no. 1, Art. no. 1, 2020, doi: 10.52332/u-net.v4i1.223.

[9] A. P. Habibi And A. Nugroho, "Audit Keamanan Sistem Informasi Berdasarkan Standar Iso/Iec 27001: 2005 (Studi Kasus: Pt. Aplikanusa Lintasarta)".

[10] E. I. Alwi, H. Herdianti, and F. Umar, "Analisis Keamanan Website Menggunakan Teknik Footprinting dan Vulnerability Scanning," *INFORMAL Inform. J.*, vol. 5, no. 2, pp. 43–48, Aug. 2020, doi: 10.19184/isj.v5i2.18941.

[11] A. Jimi, "Rancang Bangun Sistem Informasi Desa Berbasis Website (Studi Kasus Desa Netpala)," *J. Pendidik. Teknol. Inf. JUKANTI*, vol. 2, no. 1, Art. no. 1, May 2019, doi: 10.37792/jukanti.v2i1.17.

[12] N. Singh, V. Meherhomji, and B. R. Chandavarkar, "Automated versus Manual Approach of Web Application Penetration Testing," in *2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, Jul. 2020, pp. 1–6. doi: 10.1109/ICCCNT49239.2020.9225385.

[13] Y. W, R. Anto, D. T. Yuwono, and Y. Yuliadi, "Deteksi Serangan Vulnerability Pada Open Jurnal System Menggunakan Metode Black-Box," *J. Inform. Dan Rekayasa Elektron.*, vol. 4, no. 1, pp. 68–77, Apr. 2021, doi: 10.36595/jire.v4i1.365.

[14] M. I. Kurniansyah and S. Sinurat, "Sistem Pendukung Keputusan Pemilihan Server Hosting Dan Domain Terbaik Untuk WEB Server Menerapkan Metode VIKOR," *J. Sist. Komput. Dan Inform. JSON*, vol. 2, no. 1, Art. no. 1, Sep. 2020, doi: 10.30865/json.v2i1.2450.

[15] M. Hasibuan and A. M. Elhanafi, "Penetration Testing Sistem Jaringan Komputer Menggunakan Kali Linux untuk Mengetahui Kerentanan Keamanan Server dengan Metode Black Box: Studi Kasus Web Server Diva Karaoke.co.id," *Sudo J. Tek. Inform.*, vol. 1, no. 4, Art. no. 4, Dec. 2022, doi: 10.56211/sudo.v1i4.160.

[16] A. O. Bryushinin, A. V. Dushkin, and M. A. Melshiyan, "Automation of the Information Collection Process by Osint Methods for Penetration Testing During Information Security Audit," in *2022 Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus)*, Jan. 2022, pp. 242–246. doi: 10.1109/ElConRus54750.2022.9755812.

[17] Nurbojatmiko, A. Lathifah, F. Bil Amri, and A. Rosidah, "Security Vulnerability Analysis of the Sharia Crowdfunding Website Using OWASP-ZAP," in *2022 10th International Conference on Cyber and IT Service Management (CITSM)*, Sep. 2022, pp. 1–5. doi: 10.1109/CITSM56380.2022.9935837.

.

[18] Y. Putra, Y. Yuhandri, and S. Sumijan, "Meningkatkan Keamanan Web Menggunakan Algoritma Advanced Encryption Standard (AES) terhadap Seragan Cross Site Scripting," *J. Sistim Inf. Dan Teknol.*, pp. 56–63, Sep. 2021, doi: 10.37034/jsisfotek.v3i2.44.

[19] M. Z. Zakaria and R. Kadir, "Risk Assessment of Web Application Penetration Testing on Cross-Site Request Forgery (CSRF) Attacks and Server-Side Includes (SSI) Injections," in *2021 International Conference on Data Science and Its Applications (ICoDSA)*, Oct. 2021, pp. 85–90. doi: 10.1109/ICoDSA53588.2021.9617554.

[20] L. E. Nilwanda, N. P. J. Maharani, A. N. Cahyani, and A. R. I. S, "Kesadaran Ancaman Privasi Serta Perilaku Perlindungan Privasi Dalam menggunakan Sosial Media:," *Pros. Semin. Nas. Teknol. Dan Sist. Inf.*, vol. 1, no. 1, Art. no. 1, 2021.

[21] F. Ö. Sönmez and B. G. Kiliç, "Holistic Web Application Security Visualization for Multi-Project and Multi-Phase Dynamic Application Security Test Results," *IEEE Access*, vol. 9, pp. 25858–25884, 2021, doi: 10.1109/ACCESS.2021.3057044.