Jurnal Mantik, 6 (3) (2022), ISSN 2685-4236 (Online)
Published by:Institute of Computer Science (IOCS)

Jurnal Mantik

Journal homepage: www.iocscience.org/ejournal/index.php/mantik/index

Pemindai Kerentanan Terhadap Website Jago Masak Dengan Metode Pengujian Penetrasi OWASP ZAP

Reza Vidi Aditama[1], Edi Surya Negara[2]
Department of System Information, Universitas Bina Darma, Jl. Jenderal Ahmad Yani No.3, 9/10 Ulu, Kecamatan Seberang Ulu I, Kota Palembang · (0711) 515582

A R T I C L E I N F O

Article history:

Received Sept 9, 2022
Revised Sept 16, 2022
Accepted Nov 10, 2022

Keywords:

Cyber Security
Information System
OWAP ZAP
Penetration Testing

ABSTRACT

Perkembangan teknologi telah menciptakan risiko yang tak terhindarkan dalam menghadapi informasi yang dibagikan di internet, seiring dengan meningkatnya penggunaan internet dari hari ke hari, keamanan telah menjadi bagian penting dari dunia online, karena informasi yang sangat sensitif dipertukarkan melalui aplikasi online setiap hari, dan mereka telah menjadi taman bermain bagi penjahat *cyber* untuk mencuri atau memaipulasi data dan menggunakannya untuk tujuan jahat, tujuan utama dari penelitian ini adalah untuk menganalisa kelemahan dalam website jago masak menggunakan pengujian penetrasi untuk melindungi website dari ancaman dunia maya. Pada penelitian ini penulis menggunakan metode OWASP ZAP yang bertujuan untuk melakukan uji coba pemindaian kerentanan website untuk mengetahui kerentanan apa saja yang saat ini ada pada website jago masak, dari hasil penelitian ini dapat mengetahui kelemahan dari website jago masak agar dapat meningkatkan keamanan dari website tersebut.

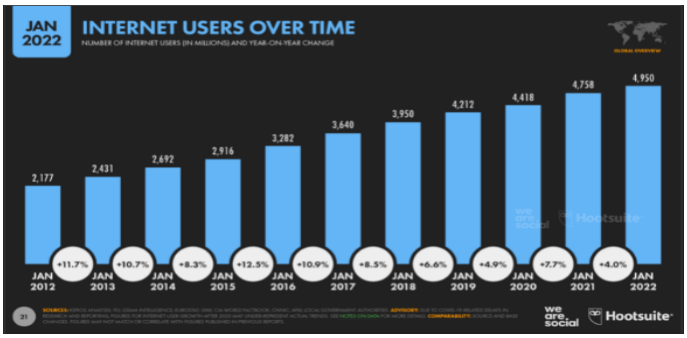
Corresponding Author:

Edi Surya Negara,
Department of System Information, Universitas Bina Darma,
Jl. Jenderal Ahmad Yani No.3, 9/10 Ulu, Kecamatan Seberang Ulu I, Kota Palembang, Sumatera Selatan 30111.
e.s.negara@binadarma.ac.id

1. PENDAHULUAN

Selama beberapa dekade terakhir, teknologi informasi telah membuat lompatan besar. memberikan dampak positif yang signifikan bagi kehidupan manusia. Internet merupakan sebuah media jaringan komputer yang memiliki akses sangat terbuka di dunia. [Ari Muzakir, A., 2022]. OWASP Zed Attack Proxy adalah alat berbasis Java yang hadir dengan antarmuka grafis intuitif, memungkinkan penguji keamanan aplikasi web untuk melakukan fuzzing, scripting, spidering, dan proxy untuk menyerang aplikasi web. [Obbayi, L. 2018]. ZAP dirilis pada 6 September 2010. Pada titik tertentu di bulan Desember, ZAP diterima sebagai proyek OWASP dan pada 1 Januari 2011 unduhan melonjak dari hampir tidak ada menjadi 433. [Simon Bennetts. 2021]. OWASP bertujuan untuk meningkatkan keamanan perangkat lunak, [BasuMallick, C. 2022]. Disini peneliti manjadikan website jamas sebagai bahan penelitian uji coba, celah keamanan dapat dijumpai dalam sebuah sistem maupun jaringan. [Dewi, B.T.K. and Setiawan, M.A., 2022]. Situs jamas merupakan website e-commerce berfokus pada masakan rumahan yang berdiri pada tahun 2021. Alasan peneliti menggunakan situs ini agar dapat membantu

website jamas untuk meningkatkan keamanan sehingga dapat beroperasi dengan lebih aman tanpa takut dengan adanya serangan dari orang yang tidak bertanggung jawab.



Gambar 1. *GLOBAL OVERVIEW REPORT*

Data terbaru menunjukkan bahwa pengguna internet tumbuh 192 juta selama 12 bulan terakhir, menghasilkan pertumbuhan tahunan hanya 4,0 persen pada tahun 2021. Namun, kami sangat menduga bahwa angka pertumbuhan yang lebih rendah ini kemungkinan besar merupakan konsekuensi dari tantangan yang terkait dengan pengumpulan dan pelaporan data selama pandemi COVID-19 yang sedang berlangsung, dan bahwa angka-angka ini tidak mencerminkan pertumbuhan aktual pengguna internet selama setahun terakhir. Akibatnya, ada peluang yang sangat bagus bahwa kami akan melaporkan angka pertumbuhan yang lebih tinggi antara tahun 2021 dan 2022 setelah data yang lebih baru tersedia. (Kemp, S. 2022).

Saat ini, aplikasi web memainkan peran penting dalam membuat hidup manusia lebih mudah. Mereka membuat kehadiran yang mulia di bidang-bidang seperti pendidikan, perbankan, hiburan, pemasaran, dan komunikasi. Beberapa contoh penting adalah belanja online, perbankan online, jejaring sosial, pengeditan dokumen online, pengeditan media online, layanan peta online, kamus online, layanan pencarian online, dan game.

Aplikasi ini memberikan layanan kepada orang-orang sesuai dengan kebutuhan mereka secara efisien dan hemat biaya. Namun, hanya menjadi efisien dan hemat biaya saja tidak cukup. Aplikasi ini harus aman dan dapat diandalkan juga. Penggunaan aplikasi yang tidak aman dan tidak dapat diandalkan mungkin selalu berdampak serius karena dapat membuat perusahaan gulung tikar. Seiring dengan meningkatnya ketergantungan hidup manusia pada layanan web. Keamanan informasi merupakan salah satu aspek penting yang harus diperhatikan oleh organisasi dan perusahaan. [Dina, D., Dedy, S. and Yesi Novaria, K., 2020]., Selama dekade terakhir, seiring dengan perkembangan teknologi web, teknik menyerang baru juga muncul. Semakin berkembangnya aplikasi berbasis web juga diiringi dengan tingginya serangan keamanan dari berbabagai teknik ancaman. [Ghozali, B., Kusrini, K. and Sudarmawan, S., 2019]. Sebelum menyerang, penyerang terlebih dahulu mencoba mengetahui kerentanan dalam aplikasi yang ingin mereka serang, dan kemudian menggunakan kemampuan kerentanan yang mereka temukan untuk melakukan serangan yang diinginkan. Hacker merupakan seseorang yang memiliki kemampuan dalam pemrograman serta jaringan computer. [Yunanri, Y., Riadi, I., & Yudhana, A. 2017]. Dalam hitungan detik, seorang pencuri virtual dapat mengakses sistem dan mencuri informasi penting, seperti password. [Ilman, Z.Y. and MM, M., 2022]. Teknologi informasi merupakan salah satu aset yang sangat berharga baik itu bagi perusahaan atau instansi yang telah menerapkan teknologi informasi dalam proses bisnisnya. [Kurnia, R. and Suryayusra, S., 2021]. Penggunaan aplikasi yang rentan selalu berbahaya bagi semua pemangku kepentingan. Hasil dari analisa kerentanan dapat membantu pengelola dan pengembang sistem untuk mencegah dan mengatasi dampak resiko yang ditemukan pada sistem. [Listartha, I.M.E., Mitha, I.M.A.P., Arta, M.W.A. and

Arimika, I.K.W.Y., 2022]. aplikasi harus selalu diuji secara menyeluruh untuk segala jenis kerentanan yang mungkin terjadi. Banyak alat tersedia untuk menguji kerentanan dalam aplikasi web. Beberapa dari mereka gratis, dan yang lainnya komersial. Mereka memindai aplikasi dengan keduanya cara otomatis dan manual. OWASP Zed Attack Proxy (ZAP), pemindai open source yang mudah digunakan untuk menemukan kerentanan dalam aplikasi web. Ini adalah salah satu proyek unggulan OWASP yang direkomendasikan oleh OWASP untuk pengujian kerentanan aplikasi web. [Mburano, B. and Si, W., 2018]. Untuk penelitian ini akan melakukan scanning dengan alat pengujian penetrasi aplikasi web dari OWASP, yang disebut Zed Attack Proxy.

2. METODE PENELITIAN

Pengujian penetrasi merupakan langkah penting dalam pengembangan sistem pertahanan berbasis komputer yang terhubung dalam suatu jaringan. [Zen, B.P., Gultom, R.A. and Reksoprodjo, A.H., 2020]. pada web jago masak hal ini di butuhkan. Karena Banyak masalah yang sering terjadi pada website salah satunya masalah keamanan yang tentunya dapat merugikan pengguna. [Pranata, D., Kunang, Y.N. and Saputri, N.A.O., 2019]. web jago masak merupakan web startup yang akan di luncurkan ke global dan seluruh orang mampu mengaksesnya. Uji coba ini dilakukan untuk mengetahui kerentanan apa saja yang saat ini terdapat pada website jago masak.

2.1 Analisis Kebutuhan

Berikut analisis perangkat yang dibutuhkan untuk melakukan penetrasi testing

Table 1. Analisis Kebutuhan

No	Perangkat	Spesifikasi
1	Laptop	processor Intel Core i5, 8GB RAM, dan VGA Nvidia GeForce MX130
2	Sistem Operasi	Windows 11 home
3	Oracle Virtual Box	Kali Linux
4	Penetrasi Tool	OWASP ZAP
5	Modem	Indihome
6	Laptop	processor Intel Core i5, 8GB RAM, dan VGA Nvidia GeForce MX130

2.1 Analisis Sistem

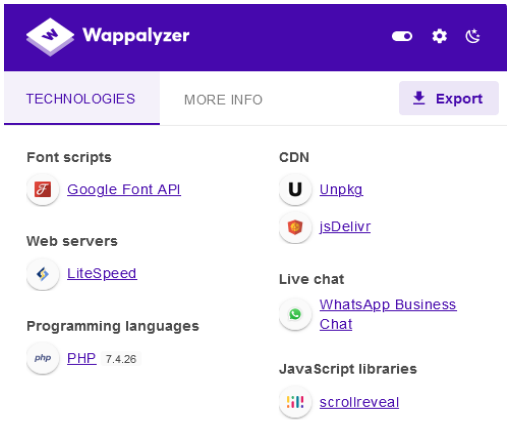
Tools yang di gunakan untuk melakukan penetrasi testing sebagai berikut:

Table 2. Analisi Sistem

No	Metode	Tools
1	Studi Literatur	Wappalyzer
2	Identifikasi Website	Who.is, Nmap
3	Exploit	Owasp ZAP, CVSS
4	Hasil Pengujian	Manual

3. HASIL DAN PEMBAHASAN

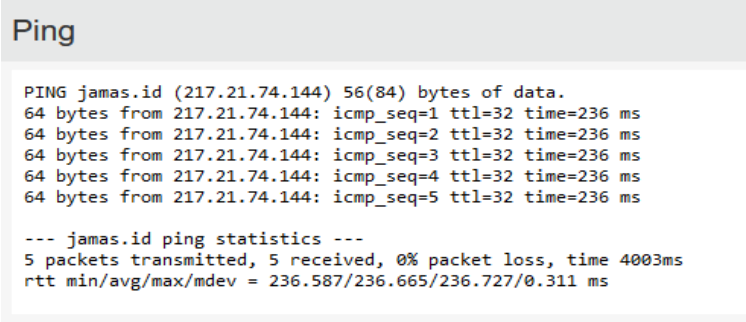
Pada bagian ini penulis berupaya untuk mendapatkan data mengenai teknologi apa saja yang di gunakan oleh website:



Gambar 2. Hasil scanning dengan wappalyzer

a. Identifikasi Website

Pada bagian ini, penulis mendefinisikan port, layanan dan host pada jaringan. Pada bagian ini menggunakan alat Who.is dan Nmap

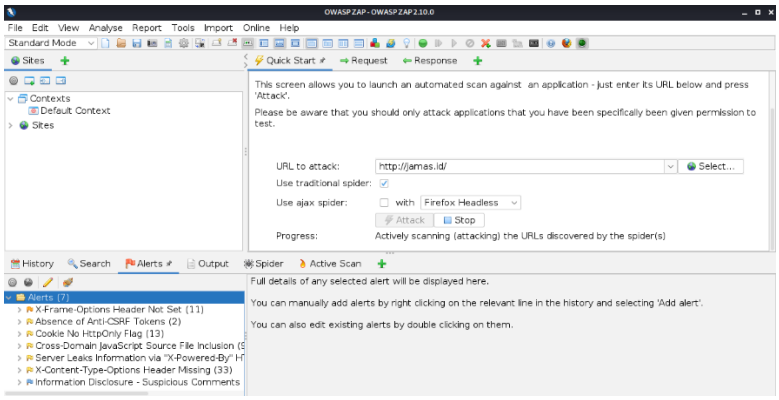


Gambar 3. Hasil Scanning dengan Who.is

Gambar 4. Hasil Scanning dengan Nmap

b. Exploit

Tahap eksploitasi merupakan tahap pengujian kelemahan keamanan, dimana data yang diperoleh sebelumnya dapat digunakan sebagai data untuk melakukan pengujian keamanan. Dari gambar dibawah terdapat beberapa kerentanan terhadap website yang di uji.

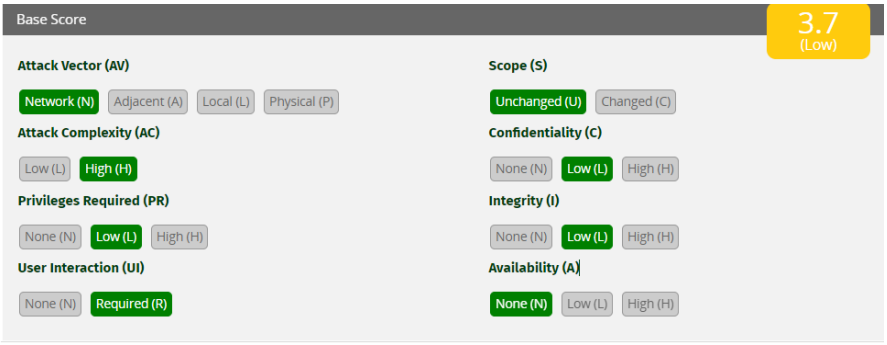


Gambar 5. Hasil Scan Menggunakan OWASP ZAP

Pada uji *scanning* menggunakan OWASP ZAP dan dari hasil yang diperoleh terdapat beberapa tingkat kerentanan antara lain:

a) X-Frame Options Header Scanner
   Setelah melakukan scaning menggunakan aplikasi OWASP ZAP pada alamat jams.id ada kerentanan yang bernama "X-Frame Options Header Not Set" dapat menyerang sistem dengan cara clickjacking.
b) Absence of Anti-CSRF Token
   Dampak yang diberikan oleh kerentanan ini penyerang dapat melakukan (XSS) *cross site scripting* memungkinkan untuk mengeksekusi kode dari jarak jauh ke jamas.id.
c) Cookie No HttpOnly Flag
   Kerentanan ini ialah membuat si penyerang dapat menggunakan *cookie* yang pernah ada dan digunakan untuk suatu Tindakan kejahatan seperti *login* sesi
d) Cross-Domain JavaScript Source File Inclusion
   Menemukan kerentanan dalam JavaScript seperti CSS, HTML, dan Web dalam struktur umum Web sebagai sistem keamanan memerlukan pembaruan referensi JavaScript secara manual setiap ada versi terbaru yang dikeluarkan**.**
e) Server Leaks Information via "X-Powered-By"
   Hal ini dapat memberikan informasi terkait dengan teknologi apa saja yang di gunakan oleh website tersebut
f) X-Content-Type-Options Header Missing
   Dampak yang dapat ditimbulkan oleh kerentanan ini ialah penyerang dapat *upload* file yang di dalamnya di taro perintah perintah jahat.

Pemberian nilai celah keamanan dengan *Common Vulnerability Scoring System* (CVSS)

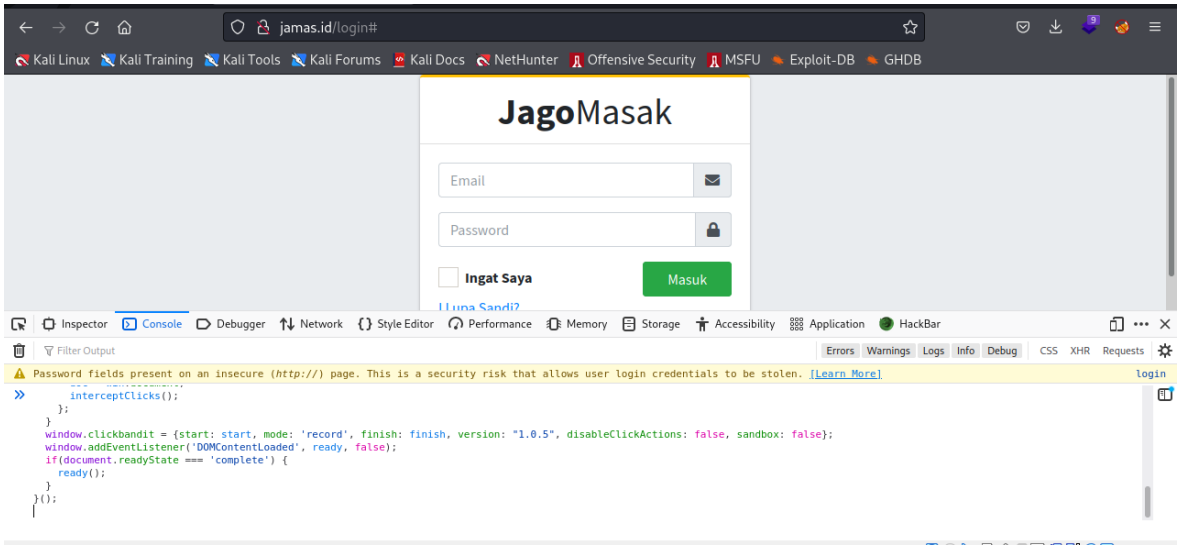


Gambar 7: CVSS

Pada hasil penilaian menggunakan *Common Vulnerability Scoring System* (CVSS) di dapat tingkat kerentanan *low* nilai 3.7 *attack vector* (AV) bagaimana cara untuk mengeksploitasi kerentanan di bagian penilain terdapat nilai (N) yang menandakan bahwa penyerang dapat melakukan serangan tanpa harus berada di jaringan yang sama kemudian *attack complexity* (AC) tingkat kesulitan dalam melakukan exploitasi di penilaian tetera (H) untuk melakukan serangan di butuhkanya persiapan dan interaksi terhadap jaringan untuk mendapatkan informasi tambahan (PR) untuk melakukan exploitasi minimal membutuhkan akses user (UI) minimal membutuhkan interaksi dengan pengguna lain agar dapat melakukan exploitasi.

c. Hasil Uji Penetrasi Testing

Setelah dilakukan proses scaning dari data yang ada di atas diketahui bahwasanya terdapat celah clikjacking yang ada pada website jago masak dan apa yang bisa di lakukan penyerang dengan melakukan clickjacking mereka dapat menanamkan tautan berbahaya yang disembunyikan di dalam tautan asli.



Gambar 8: Contoh Clickjacking

Sebagai contoh kasus penyerang akan memasukan kode jahat yang akan membuat orang lain mengakses login yang mana login itu akan mengarahkan ke suatu tempat baru yang dimana mereka tidak tau bahwa itu bukan website yang mereka tuju.

4. KESIMPULAN

Kesimpulan berdasarkan data analisis dari website jago masak dengan melakukan pemindai kerentanan dengan OWASP ZAP dapat memeriksa kelemahan yang dapat menjadi target serangan dari hacker supaya dapat merusak fungsi dari website, kemudian dengan *Common Vulnerability Scoring System* hal ini dapat di gunakan agar mengetahui tingkatan kerentanan berupa nilai yang menggambarkan tingkatan kerentanan *low,medium,high,critical* supaya dapat membantu suatu organisasi untuk memberi nilai kerentanan pada website dan tindakan apa yang harus di ambil selanjutnya. Uji coba *security* di lakukan untuk mengambil keputusan agar dapat menghindari serangan siber dengan lebih evesien berdasarkan informasi yang sudah ditemukan, dari data yang telah didapat ini melakukan penetrasi testing terbuki cukup optimal karena dapat mengetahui celah celah yang ada pada website seperti clickjacking dan semoga dari penilitian ini dapat di gunakan sebagai bahan pertimbangan untuk dapat membantu meningkatkan keamanan pada website.

DAFTAR PUSTAKA

Ari Muzakir, A., 2022. Analisis Kinerja Packet Filtering Berbasis Mikrotik Routerboard Pada Sistem Keamanan Jaringan. *Analisis Kinerja Packet Filtering Berbasis Mikrotik Routerboard pada Sistem Keamanan Jaringan*.

BasuMallick, C. (2022). *OWASP Top 10 Vulnerabilities 2022*.Www.Spiceworks.Com. https://www.spiceworks.com/it-security/vulnerability-management/articles/owasp-top-ten vulnerabilities/

Dewi, B.T.K. and Setiawan, M.A., 2022. Kajian Literatur: Metode dan Tools Pengujian Celah Keamanan Aplikasi Berbasis Web. *AUTOMATA*, *3*(1).

Dina, D., Dedy, S. and Yesi Novaria, K., 2020. *EVALUASI RESIKO KEAMANAN MENGGUNAKAN MODEL DREAD TERHADAP SISTEM INFORMASI AKADEMIK UNIVERSITAS BINA INSAN LUBUKLINGGAU* (Doctoral dissertation, Universitas Bina Darma).

Ghozali, B., Kusrini, K. and Sudarmawan, S., 2019. Mendeteksi Kerentanan Keamanan Aplikasi Website Menggunakan Metode Owasp (Open Web Application Security Project) Untuk Penilaian Risk Rating. *Creative Information Technology Journal*, *4*(4), pp.264-275.

Ilman, Z.Y. and MM, M., 2022. ANALISIS WEB VULNERABILITY UNTUK MENINGKATKAN KEAMANAN WEBSITE (STUDI KASUS: DIGITAL LIBRARY UNIVERSITAS BINA DARMA). *ANALISIS WEB VULNERABILITY UNTUK MENINGKATKAN KEAMANAN WEBSITE (STUDI KASUS: DIGITAL LIBRARY UNIVERSITAS BINA DARMA)*.

Kemp, S. (2022, January 26). *Digital 2022: Global Overview Report — DataReportal – Global Digital Insights*.Datareportal.Com.https://datareportal.com/reports/digital-2022-global-overview-report#:~:text=Global%20internet%20users%3A%20Global%20internet,of%20the%20world%27s%20total%20population.

Kurnia, R. and Suryayusra, S., 2021. ANALISIS RISIKO KEAMANAN ASET INFORMASI PADA UNIVERSITAS BINA DARMAAnalisis Risiko Keamanan Aset Informasi. In *Bina Darma Conference on Computer Science (BDCCS)* (Vol. 3, No. 4, pp. 799-808).

Listartha, I.M.E., Mitha, I.M.A.P., Arta, M.W.A. and Arimika, I.K.W.Y., 2022. Analisis Kerentanan Website SMA Negeri 2 Amlapura Menggunakan Metode OWASP (Open Web Application Security Project). *Jurnal Sistem Informasi dan Sistem Komputer*, *7*(1), pp.23-27.

Mburano, B. and Si, W., 2018, December. Evaluation of web vulnerability scanners based on owasp benchmark. In *2018 26th International Conference on Systems Engineering (ICSEng)* (pp. 1-6). IEEE.

Obbayi, L. (2018, March 30). *Introduction to OWASP ZAP for web application security assessments - InfosecResources*.Resources.Infosecinstitute.Com.https://resources.infosecinstitute.com/topic/introduction-owasp-zap-web-application-security-assessments/

Pranata, D., Kunang, Y.N. and Saputri, N.A.O., 2019. Peningkatan Keamanan Jaringan Nirkabel Dengan Pendeteksi Serangan Berbasis Kismet DD-WRT. In *Bina Darma Conference on Computer Science (BDCCS)* (Vol. 1, No. 5, pp. 1126-1132).

Simon Bennetts. (2021, April 19). *OWASP ZAP – Collecting Statistics for Open Source Projects*. https://www.zaproxy.org/blog/2021-04-19-collecting-statistics-for-open-source-projects/

Yunanri, Y., Riadi, I., & Yudhana, A. (2017). Analisis Keamanan Webserver Menggunakan Metode Penetrasi Testing (PENTEST). *Annual Research Seminar (ARS)*, *2*(1), 300–304. https://seminar.ilkom.unsri.ac.id/index.php/ars/article/view/882

Zen, B.P., Gultom, R.A. and Reksoprodjo, A.H., 2020. Analisis Security Assessment Menggunakan Metode Penetration Testing dalam Menjaga Kapabilitas Keamanan Teknologi Informasi Pertahanan Negara. *Teknologi Penginderaan*, *2*(1).

.