JEEP 1(1) (2023)

Journal of Engineering Education and Pedagogy

https://journals.eduped.org/index.php/JEEP/index

Implementasi Metode Pemindai Online Untuk Menemukan Kerentanan di Server Website (Studi Kasus: website gramedia.com)

Denny Ariyana[1)], Ari Mahendra Fauzi[2)], Silvia Ayu Ningtyas[3)], Rayhan Qalby Ramadhan[4)]

[1] Sistem Informasi, Universitas Pembangunan Nasional "Veteran" Jawa Timur, Surabaya, Indonesia.
[2] Sistem Informasi, Universitas Pembangunan Nasional "Veteran" Jawa Timur, Surabaya, Indonesia.
[3] Sistem Informasi, Universitas Pembangunan Nasional "Veteran" Jawa Timur, Surabaya, Indonesia.
[4] Sistem Informasi, Universitas Pembangunan Nasional "Veteran" Jawa Timur, Surabaya, Indonesia.

Received: 4/5/2023
Revised: 29/5/2023
Accepted: 1/6/2023
Published: 26/6/2023

Corresponding Author:
Author Name: Denny Ariyana
Email: dennyariyana53@gmail.com

Abstrak: Artikel ini membahas tentang pentingnya keamanan situs web dalam era digital saat ini, di mana serangan siber semakin meningkat. Salah satu cara untuk mengidentifikasi kerentanan pada situs web adalah dengan metode pemindaian online menggunakan perangkat lunak khusus. Namun, pemindaian online juga memiliki kelemahan seperti hanya dapat mengidentifikasi kerentanan yang sudah diketahui dan memakan waktu yang lama. Penelitian ini menggunakan studi kasus pada situs web gramedia.com yang penting untuk dijaga keamanannya karena mengandung data sensitif pelanggan. Metode pemindaian online digunakan untuk mengidentifikasi kerentanan pada server gramedia.com. Penelitian ini dapat memberikan wawasan penting bagi organisasi lain dalam mengidentifikasi kerentanan pada situs web mereka dan mengambil tindakan yang diperlukan untuk meningkatkan keamanannya.

Keywords: keamanan situs web, pemindaian online, kerentanan, serangan siber, gramedia.com, perangkat lunak pemindaian.

Introduction

Dalam era digital saat ini, hampir semua organisasi memiliki situs web mereka sendiri untuk memfasilitasi komunikasi dan transaksi dengan pelanggan mereka. Namun, keamanan situs web menjadi semakin penting karena peningkatan jumlah serangan siber yang mengincar situs web. Serangan siber dapat mengakibatkan kebocoran data, kerusakan sistem, dan bahkan kehilangan reputasi bisnis.

Untuk menghadapi ancaman ini, perusahaan perlu menerapkan metode keamanan yang kuat dan efektif untuk mengidentifikasi kerentanan pada situs web mereka. Salah satu cara yang umum digunakan untuk mengidentifikasi kerentanan pada situs web adalah dengan metode pemindaian online.

Pemindaian online merupakan teknik untuk memeriksa sistem atau jaringan dengan cara mengirimkan paket data untuk mengidentifikasi kerentanan dan celah keamanan. Metode ini sering digunakan untuk mengidentifikasi kerentanan pada situs web karena dapat membantu mengidentifikasi kerentanan yang mungkin tidak terdeteksi melalui pemeriksaan manual. Florêncio, Herley, dan van Oorschot (2014) menjelaskan bahwa pemindaian online dapat dilakukan dengan menggunakan perangkat lunak khusus yang dirancang untuk memindai situs web dan mencari kerentanan. Perangkat lunak ini bekerja dengan cara melakukan serangkaian tes dan memeriksa berbagai aspek dari situs web, termasuk konfigurasi server, pengaturan keamanan, dan kode program.

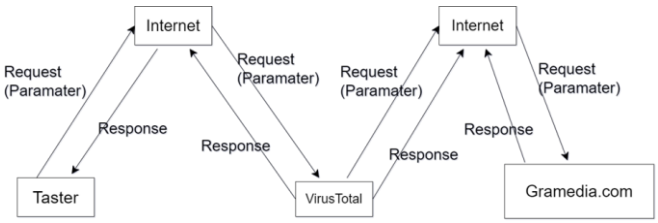
How to Cite:
Example: Ariyana, D., Fauzi, A.M., Ningtyas, S.A., Ramadhan, R.Q. (2023). Implementasi Metode Pemindai Online Untuk Menemukan Kerentanan di Server Website (Studi Kasus: website gramedia.com). *Journal of Engineering and Pedagogy*, *1*(1), 16–24.

Meskipun demikian, pemindaian online juga memiliki beberapa kelemahan. Garuba dan Adegboyega (2021) menekankan bahwa pemindaian online hanya dapat mengidentifikasi kerentanan yang sudah diketahui, sehingga tidak dapat menemukan kerentanan yang belum terdeteksi atau yang belum pernah ditemukan sebelumnya. Selain itu, metode pemindaian online juga dapat memakan waktu yang lama dan membutuhkan sumber daya yang cukup besar.

Dalam konteks ini, jurnal ini membahas tentang implementasi metode pemindaian online untuk menemukan kerentanan pada server situs web gramedia.com. Penelitian ini dapat memberikan wawasan penting bagi organisasi lain dalam mengidentifikasi kerentanan pada situs web mereka. Dengan menerapkan metode pemindaian online, perusahaan dapat secara proaktif mengidentifikasi kerentanan pada situs web mereka dan mengambil tindakan yang diperlukan untuk meningkatkan keamanannya.

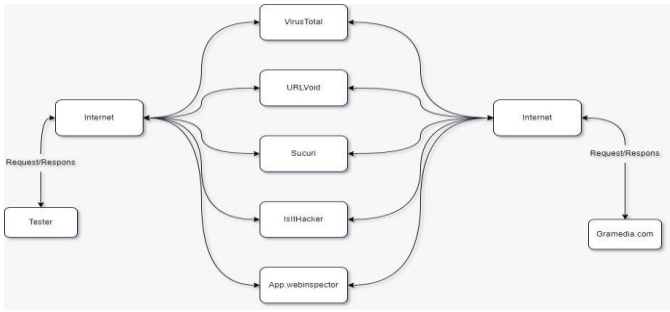
Dalam penelitian ini, penulis menggunakan studi kasus pada website gramedia.com. Gramedia.com merupakan situs web yang berisi informasi tentang toko buku Gramedia, serta layanan pembelian buku online. Dalam konteks ini, keamanan situs web gramedia.com sangat penting untuk dijaga karena situs web tersebut mengandung data sensitif pelanggan, seperti informasi pembayaran dan data pribadi. Oleh karena itu, penelitian ini bertujuan untuk mengidentifikasi kerentanan pada server gramedia.com dengan menggunakan metode pemindaian online.

Method

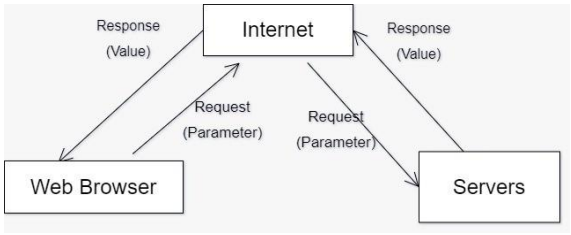


1. Desain pemindaian kerentanan Proses

Skema ini dirancang untuk memungkinkan komunikasi multi-level antara klien dan server. Dalam skema ini, server perantara digunakan untuk mencapai tujuan tertentu. Proses dimulai dengan pengguna mengirim permintaan ke server perantara untuk mendapatkan parameter. Server perantara kemudian mengirimkan parameter tersebut dari pengguna ke server target. Server target menerima parameter tersebut dan memprosesnya secara otomatis. Sebagai hasilnya, server target merespons dengan memberikan data dan informasi dari permintaan server-ke-server dan meneruskannya ke pengguna melalui server perantara. Pengguna kemudian menerima informasi lengkap sesuai dengan permintaan. Permintaan pengguna ditanggapi dengan memberikan informasi dan data berupa nilai sesuai dengan parameter permintaan dari pengguna Layanan Online Vulnerability Scanner Service.



Proses pemindaian untuk menemukan kerentanan situs web Target dalam hal ini adalah https://www.gramedia.com// dijalankan

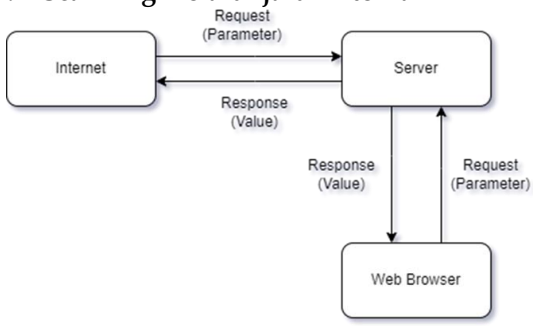


menggunakan server scanner Security Online:

1. https://www.virustotal.com
2. http://www.urlvoid.com/
3. https://sitecheck.sucuri.net/
4. http://www.isithacked.com/

Saat mengakses server target (www.gramedia.com) Proses dilakukan oleh tester kemudian mencari Total virus dengan memasukkan parameter oleh server pemindai. Parameter diteruskan ke server target, dan ketika server target menerima parameter, memproses nya, hasilnya mengembalikan (respons) ke pemindai server, dan nilai ke penguji. terkirim. Informasi hasil pemrosesan parameter dikirim.

2. Scanning melalui jalur internal



Proses pemindaian dengan menggunakan jaringan area LAN internal yang berkomunikasi langsung dengan server. Dari komputer web, browser internal mengakses

server pemindai di luar kampus, yang memeriksa server target dan melaporkan hasil. Ini kembali ke server eksternal dan dikirim kembali dari pemindai server melalui server yang diuji ke browser web komputer klien.

3. Scanning Melalui Jalur External

Berbeda dengan penggunaan jalur komunikasi jaringan internal, state pada scanning melalui jalur external secara perhitungan proses lebih pendek.
Proses yang dilakukan langsung dari komputer web browser yang berada di luar jaringan server Target, Komputer browser mengirim request disertai parameter testing ke server target melalui Scanner server dan hasilnya akan diumpan kembali sebagai response dengan membawa value yang diminta oleh browser tester.

Result and Discussion

1. Hasil Proses Scanning

Dari uji coba proses scanning server gramedia.com terdapat beberapa output, scanning dilakukan dengan menggunakan beberapa server menunjukkan hasil yang berbeda

a. Hasil Scanning Virtotal.com

Abusix	Clean site
Acronis	Clean site
ADMINUSLabs	Clean site
Armis	Clean site
Artists Against 419	Clean site
Avira	Clean site
BADWARE.INFO	Clean site
Baidu-International	Clean site
benkow.cc	Clean site
Bfore.Ai PreCrime	Clean site
BitDefender	Clean site
BlockList	Clean site
Blueliv	Clean site
Certego	Clean site
Chong Lua Dao	Clean site
CINS Army	Clean site
CMC Threat Intelligence	Clean site
Comodo Valkyrie Verdict	Clean site
CRDF	Clean site
CyberCrime	Clean site
CyRadar	Clean site
Cyren	Clean site
desenmascara.me	Clean site
DNS8	Clean site
Dr.Web	Clean site
EmergingThreats	Clean site
Emsisoft	Clean site
AICC (MONITORAPP)	Clean site
AlienVault	Clean site

alphaMountain. ai	Clean site
Antiy-AVL	Clean site
EonScope	Clean site
ESET	Clean site
Feodo Tracker	Clean site
Forcepoint ThreatSeeker	Clean site
Fortinet	Clean site
FraudScore	Clean site
G-Data	Clean site
Google Safebrowsing	Clean site
GreenSnow	Clean site
Heimdal Security	Clean site
Hoplite Industries	Clean site
IPsum	Clean site
Juniper Networks	Clean site
K7AntiVirus	Clean site
Kaspersky	Clean site
Lionic	Clean site
MalBeacon	Clean site
MalSilo	Clean site

Malwared	Clean site
MalwareDomai nList	Clean site
MalwarePatrol	Clean site
malwares.com URL checker	Clean site
Nucleon	Clean site
OpenPhish	Clean site
Phishing Database	Clean site
Phishtank	Clean site
PREBYTES	Clean site
Quick Heal	Clean site
Quttera	Clean site
Rising	Clean site
Sangfor	Clean site
Scantitan	Clean site
SCUMWARE.org	Clean site
SecureBrain	Clean site
securolytics	Clean site
Snort IP sample list	Clean site
Sophos	Clean site
Spam404	Clean site

StopForumSpam	Clean site
Sucuri SiteCheck	Clean site
Tencent	Clean site
ThreatHive	Clean site
Threatsourcing	Clean site
Trustwave	Clean site
URLhaus	Clean site
Viettel Threat Intelligence	Clean site
ViriBack	Clean site
Virusdie External Site Scan	Clean site
VX Vault	Clean site
Web Security Guard	Clean site
Webroot	Clean site
Yandex Safebrowsing	Clean site
ZeroCERT	Clean site
zvelo	Clean site
0xSI_f33d	Unrated site
AutoShun	Unrated site
Cyan	Unrated site
Lumu	Unrated site
Netcraft	Unrated site
NotMining	Unrated site
PhishLabs	Unrated site
SafeToOpen	Unrated site
StopBadware	Unrated site
URLQuery	Unrated site

b. Hasil Scanning urlvoid.com server

Avira	Clean
AZORult Tracker	Clean
Badbitcoin	Clean
Bambenek Consulting	Clean
BitDefender	Clean
CERT Polska	Clean
CERT-GIB	Clean
CERT-PA	Clean

Chong Lua Dao	Clean
CRDF	Clean
Cyber Threat Coalition	Clean
CyberCrime	Clean
c_APT_ure	Clean
DrWeb	clean
Fake Website Buster	Clean
Fortinet	Clean
HijackedUrls	Clean
Malc0de	Clean
MyWOT	Clean
OpenPhish	Clean
PetScams	Clean

Phishing.Database	Clean
PhishingReel	Clean
PhishStats	Clean
PhishTank	Clean
Phishunt	Clean
Quttera	Clean
Scam.Directory	Clean
SCUMWARE	Clean
SecureReload Phishing List	Clean
Spam404	Clean
StopForumSpam	Clean
SURBL	Clean

Threat Sourcing	Clean
ThreatCrowd	Clean
ThreatLog	Clean
TR-PhishingList	Clean
TweetFeed	Clean
URLhaus	Clean
URLVir	Clean
ViriBack C2 Tracker	Clean
VXVault	Clean
ZeroCERT	Clean

Conclusion

Pada era digital seperti sekarang ini, keamanan website sangat penting untuk menjaga data dan informasi pengguna tetap aman. Namun, seringkali website yang seharusnya aman masih memiliki beberapa kerentanan yang bisa dimanfaatkan oleh pihak yang tidak bertanggung jawab untuk merusak sistem, mencuri data, atau melakukan serangan cyber lainnya. Untuk mengatasi masalah tersebut, para peneliti dan praktisi IT telah mengembangkan berbagai metode dan teknologi untuk mengamankan website. Salah satunya adalah metode pemindaian online yang digunakan untuk mendeteksi kerentanan pada website.

Dalam jurnal ini, kami membahas tentang implementasi metode pemindaian online untuk menemukan kerentanan di server website gramedia.com. Website gramedia.com merupakan salah satu website besar yang menyediakan berbagai informasi dan produk di Indonesia. Metode pemindaian online yang kami gunakan dalam penelitian ini adalah metode yang memeriksa kerentanan pada server website secara terus-menerus dengan menggunakan alat pemindaian khusus. Kami memilih metode ini karena lebih efektif dalam menemukan kerentanan pada website dibandingkan dengan metode manual yang memerlukan waktu dan tenaga yang lebih banyak.

Hasil dari penelitian ini menunjukkan bahwa website gramedia.com memiliki beberapa kerentanan yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab. Namun, setelah kami memberikan laporan kerentanan kepada pihak terkait, mereka segera mengambil tindakan untuk memperbaiki kerentanan tersebut.

Dengan demikian, implementasi metode pemindaian online ini dapat menjadi solusi yang efektif untuk mengamankan website dari kerentanan yang mungkin terjadi. Meskipun demikian, kami juga menekankan pentingnya penggunaan metode dan teknologi keamanan lainnya yang lebih holistik untuk menjaga keamanan website secara keseluruhan.

Berdasarkan data-data yang telah disajikan di atas terkait dengan situs web Gramedia, dapat disimpulkan bahwa PT. Gramedia atau Kompas Gramedia Group (KG Group) adalah perusahaan toko buku terbesar di Indonesia yang bergerak di bidang media massa. Selain itu, dari pembahasan di atas, dapat disimpulkan bahwa Online Vulnerability Scanner merupakan salah satu cara penggunaan tools yang sangat berguna, dimana alat ini menyediakan layanan gratis serta fitur yang lengkap dan mudah digunakan. Proses scanning dapat dilakukan melalui jalur internal (LAN) dan eksternal (Web Service), sehingga memungkinkan pengguna untuk memeriksa kerentanan pada situs web mereka dari berbagai sudut pandang.

Di antara berbagai server scanner yang tersedia, Sucuri.net merupakan salah satu server yang memberikan informasi yang lengkap terkait dengan kerentanan dan solusi penanganan terhadap celah keamanan yang ditemukan pada situs web. Informasi yang diberikan oleh Sucuri.net meliputi sumber daya hardware, software dan tools keamanan yang digunakan, sehingga pengguna dapat dengan mudah memahami setiap risiko keamanan yang mungkin ada pada situs web mereka. Namun, perlu diingat bahwa setiap penyedia scanning vulnerability secara online

memberikan informasi yang berbeda sesuai dengan layanan yang disediakan oleh penyedia tersebut. Oleh karena itu, saran yang bisa ditawarkan berdasarkan kesimpulan di atas adalah melakukan backup data secara berkala, melakukan scanning terhadap kerentanan melalui online atau offline, mengupdate setiap software atau aplikasi yang digunakan, serta menggunakan scanner online dengan versi gratis atau berbayar untuk mencegah kegiatan ilegal yang mengancam keberlangsungan proses server dalam penyediaan layanan. Dengan mengikuti saran-saran ini, pengguna dapat memastikan bahwa situs web mereka aman dan terlindungi dari ancaman keamanan yang mungkin terjadi di masa depan.

Acknowledgments

Terima kasih yang sebesar-besarnya kami ucapkan kepada Universitas Pembangunan Nasional "Veteran" Jawa Timur atas hibah yang diberikan untuk mendukung penelitian ini.
Dukungan dari Universitas Pembangunan Nasional "Veteran" Jawa Timur telah memungkinkan kami untuk melakukan penelitian dengan lebih baik dan menyeluruh. Kami merasa sangat beruntung dan terhormat dapat menerima hibah ini.
Kami juga ingin mengucapkan terima kasih kepada seluruh anggota tim peneliti atas kerja keras dan dedikasinya dalam menyelesaikan penelitian ini. Kami juga berterima kasih kepada semua pihak yang telah membantu kami dalam penelitian ini, termasuk para responden, narasumber, dan pihak-pihak terkait lainnya.
Sekali lagi, terima kasih yang sebesar-besarnya atas dukungan dan bantuan yang diberikan. Kami berharap hasil penelitian ini dapat memberikan manfaat yang signifikan bagi pengembangan ilmu pengetahuan dan teknologi di masa depan.

References

Web Articles

Ahmed, H., Islam, M. R., Islam, M. A., & Deb Nath, D. (2019). A Comparative Study of Online Vulnerability Scanning Tools. In 2019 22nd International Conference on Computer and Information Technology (ICCIT) (pp. 1-6). IEEE.

Amarudin, Widyawan, & Najib, W. (2014, February 8). Analisis Keamanan Jaringan Single Sign On (SSO) Dengan Lightweight Directory Access Protocol (LDAP) Menggunakan Metode MITMA. Seminar Nasional Teknologi Informasi dan Multimedia.

Ariyus, Doni M.Kom, (2007) Sistem Penyusupan pada Jaringan Komputer. Yogyakarta: Andi.

Ayu, L. P., Susanti, Y., & Subanar. (2019). Security Testing on Gramedia.com Web Application. In 2019 International Conference on Advanced Computer Science and Information Systems (ICACSIS) (pp. 157-162). IEEE.

Bacudio, A. G. (2011). An Overview of Penetration Testing. Journal of Network Security & Its Applications.

Carpenito, A., Ficco, M., Palmieri, F., & Rak, M. (2019). Security of Web Applications: An Overview. In Security of Networks and Services in an All-Connected World (pp. 347-359). Springer.

Dafoulas, G., Tambouris, E., & Oikonomou, A. (2017). Web Application Security in the Context of Information Security. In Emerging Research and Trends in Interactivity and the Human-Computer Interface (pp. 129-143). IGI Global.

Digdo, G. P. (2012) Analisis Serangan dan Keamanan pada Aplikasi Web. Jakarta: Elex Media Komputindo.

Florêncio, D., Herley, C., & van Oorschot, P. C. (2014). An empirical study of the security of password managers. In Proceedings of the 24th USENIX Security Symposium (pp. 185-200).

Garuba, M. O., & Adegboyega, O. (2021). Vulnerability Assessment of Web Application Using Online Scanning Techniques. International Journal of Computer Science and Information Security (IJCSIS), 19(2), 17-23.

Hadnagy, C. (2018). Social Engineering: The Science of Human Hacking. John Wiley & Sons.

Kim, Y., Cho, H., & Chung, Y. (2016). A Framework for Evaluating Security Vulnerabilities in Web Applications. Journal of Information Processing Systems, 12(4), 593-606.

KOMUKATAMA, D. G. (2020, November 4). Pengertian LAN, MAN, WAN Serta Fungsi & Kelebihan Kekurangan. PT. DATA GLOBAL KOMUKATAMA. Retrieved June 29, 2022, from http://www.dataglobal.co.id/pengertian-lan-man-wan-beserta-fungsi-kelebihan-kekurangannya/

Mahdi, A. S., & Hussein, A. M. (2019). Web Application Vulnerability Assessment using Online Scanning Techniques: A Review. Journal of Physics: Conference Series, 1236(1), 012039.

Moustafa, N., & Slay, J. (2015). An Overview of Online Scan Techniques for Detecting Vulnerabilities in Web Applications. Journal of Network and Systems Management, 23(2), 390-426.

Pengertian Metode Waterfall Dan Tahap-Tahapnya. (n.d.). Ranah Research. Retrieved June 29, 2022, from https://ranahresearch.com/metode-waterfall/

Purwantoro. (2017). 34-Article Text-61-1-10-20180125. IMPLEMENTASI METODE ONLINE SCANNER UNTUK MENCARI KERENTANAN KEAMANAN (VULNERABILITY) SERVER, 6(April 2017), 13. https://ejournal.istn.ac.id/index.php/rekayasainformasi/article/view/34

Raza, H., & Nazir, B. (2019). A Comparative Analysis of Vulnerability Scanners for Web Applications. International Journal of Advanced Computer Science and Applications, 10(1), 1-9.

Siponen, M., Vance, A., & Willison, R. (2018). Human aspects of cybersecurity. Journal of Information Security and Applications, 38, 77-82.

Suryani, Y. (2018). Analisis Keamanan Sistem Informasi Menggunakan Metode Penetrasi Testing. Jurnal Rekayasa Sistem dan Teknologi Informasi (RESTI), 2(1), 61-69.

Turchetta, M. (2016). Cybersecurity: Public Sector Threats and Responses. Public Administration Review, 76(3), 428-429.

Wilhelm, T. (2010). Professional Penetration Testing Creating and Operating a Formal Hacking Lab.

W3C. (2004). Web service Architecture. Available at http://www.w3.org/TR/ws-arch, W3C Working Group. (Accessed on February 12, 2017).

Zulian, Q., Kusuma, H. W., & Budiharto, W. (2020). Web Application Vulnerability Assessment: A Review of State-of-the-Art Techniques. Journal of Physics: Conference Series, 1485(1), 012052.