ANALISIS CELAH KERENTANAN KEAMANAN TERHADAP ANCAMAN SERANGAN PADA *WEBSITE* SIAK.CHY.MY.ID DENGAN *VULNERABILITY ASSESSMENT*

LAPORAN SKRIPSI

LAILY RACHMI TSANI 4817050232

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN

JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER

POLITEKNIK NEGERI JAKARTA

2021

ANALISIS CELAH KERENTANAN KEAMANAN TERHADAP ANCAMAN SERANGAN PADA *WEBSITE* SIAK.CHY.MY.ID DENGAN *VULNERABILITY ASSESSMENT*

LAPORAN SKRIPSI

Dibuat untuk Melengkapi Syarat-Syarat yang Diperlukan untuk Memperoleh Diploma Empat Politeknik

LAILY RACHMI TSANI

4817050232

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN

JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER

POLITEKNIK NEGERI JAKARTA

2021

HALAMAN PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya saya sendiri, dan semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar.

Nama	**: Laily Rachmi Tsani**
NIM	**: 4817050232**
Tanggal	**: 16 Juni 2021**
Tanda Tangan	**:**

LEMBAR PENGESAHAN

Skripsi diajukan oleh:

Nama	:	Laily Rachmi Tsani
NIM	:	4817050232
Program Studi	:	Teknik Multimedia dan Jaringan
Judul Skripsi	:	Analisis Celah Kerentanan Keamanan Terhadap Ancaman Serangan Pada *Website* Siak.Chy.My.Id Dengan *Vulnerability Assessment*

Telah diuji oleh tim penguji dalam Sidang Skripsi pada hari Rabu, Tanggal 16, Bulan Juni Tahun 2021 Dan dinyatakan **LULUS**

Disahkan oleh

Pembimbing I	: Defiana Arnaldy, S.TP, M.Si.	( )
Penguji I	: Ayu Rosida Zain, S.ST, M.T.	( )
Penguji II	: Muhammad Yusuf Bagus Rasyiidin, S.Kom., M.T.I.	( )
Penguji III	: Indra Hermawan, S.Kom., M.Kom.	( )

Mengetahui:

Jurusan Teknik Informatika dan Komputer

Ketua

Mauldy Laya, S.Kom., M.Kom.

NIP. 197802112009121003

Kata Pengantar

Assalamu'alaikum Wr. Wb.

Puji syukur penulis panjatkan atas kehadirat Allah SWT karena berkat rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan perkuliahan dan skripsi ini dengan baik. Selama menjalani masa perkuliahan dan pelaksanaan penelitian skripsi, tentu banyak dukungan, bimbingan, dan saran dari berbagai pihak. Oleh karena itu, penulis mengucapkan terima kasih kepada:

1. Bapak Defiana Arnaldy, S.TP, M.Si. selaku pembimbing skripsi yang telah membimbing penulis dan memberi masukan yang sangat membantu penulis dalam menyelesaikan skripsi ini.
2. Cahya Mulyadi selaku pemilik *Website* yang dijadikan target penelitian.
3. Orang tua dan kakak Penulis yang telah menyayangi dan memberikan dukungan, bantuan yang tek terhingga bagi penulis dari kecil sampai sekarang.
4. Dita Nurhayati,Trisya Talia ,Sabrina Annisa dan Suci Rahmadhani atas waktunya mendengarkan segala keluh kesah penulis dan menemani penulis begadang untuk mengerjakan skripsi hingga larut setiap harinya.
5. Kevin, Nio, Tona dan teman-teman pada Grup bismillah yang selalu saling membantu jika ada kesulitan selama masa perkuliahan dan saat penegerjaan skripsi dilakukan.
6. Ilsya Wirasati, atas kesabarannya menghadapi dan menemani penulis sejak tk sampai sekarang serta selalu memberi masukan positf kepada penulis.
7. Deanandita dan Arindini atas kesediaan waktunya untuk menemani dan mengajak penulis untuk sejenak menghilangkan penat dan menghibur penulis dimasa sulit pengerjaan skripsi.
8. Adam fadhel terimakasih telah ada setiap hari.
9. Gabriela Warouw, Ghevira Fatihah, Dea Aryanti yang selalu memberi semangat dan energy positif kepada penulis.

10. Acil, Piko dan Upul yang selalu setia dan menemani serta menghibur penulis dengan tingkah laku yang lucu setiap hari.

Akhir kata, semoga Allah Yang Maha Esa membalas segala kebaikan dari pihak-pihak yang telah membantu penulis. Penulis memohon maaf jika terdapat kekurangan atau kesalahn dalam tugas akhir ini. Semoga tugas akhir ini dapat bermanfaat bagi pembaca dan dapat mendorong pengembangan ilmu pengetahuan. Sekian dan terima kasih.

Jakarta, 20 April 2021

Penulis

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Politeknik Negeri Jakarta, saya yang bertanda tangan dibawah ini :

Nama	: Laily Rachmi Tsani
NIM	: 4817050232
Program Studi	: Teknik Multimedia dan Jaringan
Jurusan	: Teknik Informatika dan Komputer
Jenis Karya	: Skripsi

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Politeknik Negeri Jakarta **Hak Bebas Royalti Noneksklusif (*Non-exclusive Royalty-Free Right*)** atas karya ilmiah saya yang berjudul :

Analisis Celah Kerentanan Keamanan Terhadap Ancaman Serangan Pada *Website* Siak.Chy.My.Id Dengan *Vulnerability Assessment*

Dengan Hak Bebas Royalti Noneksklusif ini Politeknik Negeri Jakarta berhak menyimpan, mengalih media/format-kan, mengelola dalam bentuk pangkalan data (*database)*, merawat, dan mempublikasikan skripsi saya selama tetap mencamtumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Jakarta Pada tanggal : 16 Juni 2021

Yang Menyatakan

Laily Rachmi Tsani

Analisis Celah Kerentanan Keamanan Terhadap Ancaman Serangan Pada *Website* Siak.Chy.My.Id Dengan *Vulnerability Assessment*

ABSTRAK

Perkembangan teknologi dan internet semakin maju. Bersamaan dengan perkembangan teknologi, *website* juga mengalami perkembangan. *Website* atau situs dapat diartikan sebagai kumpulan halaman-halaman yang digunakan untuk menampilkan informasi teks, gambar diam atau gerak, animasi, suara, dan atau gabungan dari semuanya, baik yang bersifat statis maupun dinamis yang membentuk satu rangkaian bangunan yang saling terkait. Keamanan sebuah website merupakan hal yang penting, karena untuk melindungi informasi informasi yang ada. Jika keamanan suatu *website* tidak diperhatikan, *Vulnerability* atau kerentanan tersebut dapat digunakan oleh pihak tidak bertanggung jawab untuk mengambil keuntungan. *Vulnerability* adalah suatu titik kelemahan dimana suatu sistem rentan terhadap serangan. Terdapat beberapa Jenis kerentanan yang dapat terjadi, untuk itu perlu dilakukan pencarian celah kerentanan dengan menerapkan metode *Vulnerability Assessment* dan *Penetration testing*. Dalam menerapkan metode tersebut dilakukan dengan beeberapa tahapan penelitian dan dengan memanfaatkan *tools vulnerability scanner*. Pada penelitian ini *website* yang menjadi target adalah *website* siak.chy.my.id yang merupakan *website* yang digunakan oleh mahasiswa yang memuat data mahasiswa. Pada *website* ini belum pernah dilakukan pengujian celah kerentan sebelumnya, maka dari itu dilakukan penelitian ini untuk mengetahui celah kerentanan pada web tersebut. *Vulnerability scanner tools* yang digunakan adalah Nikto, Dirb, Vega *web vulnerability* dan OWASP ZAP.

Kata Kunci: *Website*, Kerentanan, *Vulnerability Assessment*, *Penetration Testing*, *Vulnerability Scanner*, Nikto, Dirb, Vega, OWASP ZAP

Analisis Celah Kerentanan Keamanan Terhadap Ancaman Serangan Pada *Website* Siak.Chy.My.Id Dengan *Vulnerability Assessment*

ABSTRAK

The development of technology and the internet is increasingly advanced. Along with the development of technology, the website is also experiencing development. Website or site can be defined as a collection of pages that are used to display text information, still or motion pictures, animations, sounds, and or a combination of all of them, both static and dynamic which form a series of interrelated buildings. The security of a website is important, because it protects existing information. If the security of a website is not considered, the vulnerability or vulnerability can be used by irresponsible parties to take advantage. Vulnerability is a point of weakness where a system is vulnerable to attack. There are several types of vulnerabilities that can occur, for that it is necessary to search for vulnerabilities by applying the Vulnerability Assessment and Penetration testing methods. In applying this method, several stages of research are carried out and by utilizing vulnerability scanner tools. In this study, the target website is the siak.chy.my.id website which is a website used by students that contains student data. This website has never been tested for vulnerabilities before, therefore this research was conducted to find out the vulnerabilities on the web. Vulnerability scanner tools used are Nikto, Dirb, Vega web vulnerability and OWASP ZAP.

Keywords: Website, Vulnerability, Vulnerability Assessment, Penetration Testing, Vulnerability Scanner, Nikto, Dirb, Vega, OWASP ZAP

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi dan internet semakin hari semakin maju. Bersamaan dengan perkembangan teknologi, *website* juga mengalami perkembangan. *Website* atau situs dapat diartikan sebagai kumpulan halaman-halaman yang digunakan untuk menampilkan informasi teks, gambar diam atau gerak, animasi, suara, dan atau gabungan dari semuanya, baik yang bersifat statis maupun dinamis yang membentuk satu rangkaian bangunan yang saling terkait (Rusdiana, 2019). Kini *website* telah menjadi sumber informasi untuk berbagai bidang dan kalangan. Sebagai sumber informasi terbuka sebuah *website* dengan mudah dapat diakses banyak orang. Untuk itu, perkembangan dan kemudahan ini harus diikuti dengan tingkat keamanan yang tinggi.

Keamanan sebuah *website* merupakan hal yang penting, karena untuk melindungi informasi informasi yang ada. Karena, meski dapat di akses banyak orang, dalam sebuah *website* juga terdapat informasi penting yang harus di jaga seperti data pengguna, informasi pribadi dan sebagainya. Jika keamanan suatu *website* tidak diperhatikan, *vulnerability* atau kerentanan tersebut digunakan oleh pihak tidak bertanggung jawab untuk mengambil keuntungan. *Vulnerability* adalah suatu point kelemahan dimana suatu sistem rentan terhadap serangan (Kamilah, et al., 2019).Terdapat beberapa Jenis kerentanan yang dapat terjadi, untuk itu perlu dilakukan pencarian celah kerentanan dengan melakukan *vulnerability scanning*. *Vulnerability scanning* adalah Aplikasi yang menjalankan *security* scan dan penilaian kerentanan (Sirait, et al., 2018). *Vulnerability scanning* memanfaatkan *tools* pengujian yang ada seperti *Acunetix web vulnerability*, *Nessus*, Vega, *openVAS*, *tools online* dan *tools* lainnya.

Website siak.chy.my.id merupakan *website* yang digunakan oleh mahasiswa Politeknik Negeri Jakarta sebagai sarana informasi bidang akademik yang memuat data mahasiswa termasuk nilai dan data kehadiran. untuk dapat mengakses *web* ini, dibutuhkan data penting seperti NIM dan Password Mahasiswa. Sehingga

keamanan menjadi hal yang perlu diperhatikan dalam *website* tersebut. Pada *website* ini belum pernah dilakukan pengujian celah keamanannya.

Berdasarkan latar belakang permasalahan yang telah dipaparkan, maka dilakukan penelitian pada *website* tersebut yang bertujuan untuk mengetahui kelemahan dan celah kerentanan *website* dari serangan yang mungkin terjadi agar kelemahan yang ditemukan dapat diperbaiki sehingga layanan *website* semakin baik.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah diuraikan, maka rumusan masalah pada penelitian ini sebagai berikut:

a. Bagaimana menemukan celah kerentanan dan kelemahan pada *website* Siak.chy.my.id?
b. Bagaimana melakukan pengujian kerentanan yang ditemukan pada *website* Siak.chy.my.id?
c. Bagaimana menganalisis hasil pengujian kerentanan tersebut?
d. Bagaimana mengetahui solusi dari kelemahan yang ditumakan untuk *website* tersebut?

1.3 Batasan Masalah

Agar penelitian tetap terarah dan tidak menyimpang dibutuhkan adanya batasan masalah, yaitu sebagai berikut:

a. Batasan masalah dalam penelitian ini adalah *website* yang di analisa adalah *website* siak.chy.my.id.
b. Pengujian yang dilakukan pada penelitian ini dengan *vulnerability assessment* dan *Penetration testing*.
c. Data yang diperoleh peneliti dari literatur, buku referensi, atau *browsing*.
d. Penelitian ini untuk mengetahui celah keamanan pada *web* siak.chy.my.id dengan menggunakan *tools* Nikto, Dirb, Vega *web vulnerability scanner* dan OWASP ZAP
e. Pengujian celah dilakukan hanya pada celah yang berada pada tingkat ancaman *High* dan *Medium*.
f. Pada penelitian ini diberikan rekomendasi dari celah yang ditemukan tetapi tidak dilakukan perbaikan.

1.4 Tujuan dan Manfaat

1.4.1 Tujuan

Untuk mengetahui kerentanan (*vulnerability*) yang ada pada *website* siak.chy.my.id serta diharapkan dapat membantu pengelola *web* tersebut dalam mengidentifikasi celah keamanan dan menutupnya sebelum diketahui dan dimanfaatkan oleh pengguna yang tidak bertanggung

1.4.2 Manfaat

a. Dapat mengetahui kelemahan *website* siak.chy.my.id, apakah sistem rentan terhadap serangan.
b. Dapat mengetahui langkah atau tindakan pencegahan, berdasarkan hasil analisa terhadap pengujian keamanan *website* siak.chy.my.id.
c. Meningkatkan keamanan pada layanan *website* siak.chy.my.id.

1.5 Metode Penelitian

Penelitian ini dilakukan dengan beberapa metode yaitu sebagai berikut:

1) Metode Pengumpulan Data

Dalam penelitian ini penulis mengumpulkan data yang dibutuhkan dalam pengujian menggunakan dua metode, yaitu:

a. Studi Literatur

Yaitu pengumpulan data dengan mencari bahan dari internet, jurnal dan buku yang sesuai dengan topik penelitian.

b. Pengamatan (*Observation*).

Merupakan suatu pengumpulan data yang dilakukan dengan cara mengamati permasalahan pada objek yang diteliti secara langsung.

2) Metode *Vulnerability Assessment* dan *Penetration testing*

Metode penelitian yang digunakan dalam penelitian ini adalah metode *Vulnerability Assessment* dan *Penetration Testing*. Dalam penelitian ini dilakukan dengan empat tahapan, yaitu :

a. Perancangan penelitian

Merupakan tahapan awal dalam melakukan penelitian ini yaitu membuat perancangan penelitian dengan menentukan target penelitian dan menentukan batasan-batasan terhadap *website* target yang akan diuji yaitu peneliti hanya melakukan *vulnerability scanning* (kerentanan) dan uji eksploitasi teradap kerentanan dengan tingkat *high* dan *medium* tanpa merubah tampilan.

b. *Reconnaisance*

Tahapan yang dilakukan sebagai upaya pencarian informasi mengenai *website* dengan memanfaatkan *tools* yang ada.

c. *Vulnerability Scanning*

Tahapan dilakukannya *scanning website* dengan memanfaatkan beberapa *tools web scanning*. tujuan yang ingin dicapai adalah memperoleh informasi *vulnerability website* tersebut

d. Uji Kerentanan

Tahapan dilakukan uji kerentanan dari hasil *scanning* dengan *script* yang sesuai dengan kerentanan yang ditemukan

e. Analysis dan rekomendasi

Pada tahap ini peneliti akan menganalisis hasil uji dan informasi-informasi *vulnerability* yang ditemukan setelah dilakukan *scanning* dan pengujian celah terhadap target dengan beberapa *tool* serta dapat mengetahui tingkat kerentanan dari hasil tersebut.

f. Dokumentasi dan Laporan: Tahapan ini akan mendokumentasikan hasil analisa dari celah keamanan *website* target yang nantinya dapat menjadi pertimbangan pengelola *website* dalam meningkatkan keamanan *website* tersebut.

BAB V
PENUTUP

5.1 Kesimpulan

Dalam melakukan penelitian uji kemungkinan celah kerentanan pada *website* siak.chy.my.id yang bertujuan untuk menguji keamanan pada *website* tersebut berdasarkan seluruh tahapan yang telah dilakukan dapat diambil beberapa kesimpulan antara lain sebagai berikut:

a. Untuk menemukan celah kerentanan pada *website* siak.chy.my.id dilakukan dengan metode *vulnerability assessment* dan *penetration testing* dengan beberapa tahap yaitu pengintaian (*reconnasissance*), pemindaian (*scanning*), eksploitasi (*exploitation*) dan uji kerentanan.
b. Ditemukan beberapa kerentanan yang mencakup *medium risk* sampai *low risk* serta informasi. Kerentanan tersebut terdeteksi oleh ketiga *tools vulnerability scanner* yang digunakan yaitu Nikto, Vega dan OWASP ZAP.
c. Kerentanan yang terdeteksi pada website sebanyak 14 jenis kerentanan yaitu dengan 7 kerentanan berada pada tingkat informasi, 5 kerentanan pada tingkat *low* dan 2 kerentanan pada tingkat *medium*.
d. Pada jenis kerentanan *X-Frame-Options Header Not Set* dilakukan uji dengan memasukan *script* penggunaan *iframe* pada *file* html baru kemudian *file* tersebut diakses pada browser.
e. Terdapat beberapa solusi untuk kerenanan yang terdeteksi agar dilakukan perbaikan oleh pengelola *website*.

5.2 Saran

Berdasarkan penelitian yang telah dilakukan terdapat beberapa saran yang dapat diterapkan dan dikembangkan pada penelitian berikutnya. Selain itu, juga untuk *website* Siak.chy.my.id sebagai objek penelitian, antara lan:

a. Pengujian kerentanan pada *website* siak.chy.my.id dapat dilakukan dengan metode lain untuk mendapatkan hasil berbeda.
b. Menggunakan lebih banyak *tools* untuk mendeteksi jenis kerentanan lain yang belum dapat terdeteksi oleh *tools* yang digunakan dalam penelitian ini.

Untuk pengembangan penelitian, uji kerentanan tidak hanya dilakukan ada kerentanan yang berada pada tingkat *High-Medium* namun juga pada kerentanan dengan tingkat *low*.

Perbaikan pada celah kerentanan yang ditemukan perlu dilakukan untuk peningkatan keamanan pada *website* siak.chy.my.id.

DAFTAR PUSTAKA

Arbi1, A., 2020. Penetration Testing Untuk Mengetahui Kerentanan Keamanan Aplikasi Web Menggunakan Standar OWASP 10 pada domain Web Perusahaan.

Arnaldy, D. & Perdana, A. R., 2019. Implementation and Analysis of Penetration Techniques Using the Man-In-The-Middle Attack. *International Conference of Computer and Informatics Engineering (IC2IE).*

Asfihan, A., 2021. *Vulnerability Adalah.* [Online] Available at: https://adalah.co.id/vulnerability/ [Accessed 14 April 2021].

Balbix, n.d. *What to know about Vulnerability Scanners and Scanning Tools.* [Online]
Available at: https://www.balbix.com/insights/what-to-know-about-vulnerability-scanning-and-tools/
[Accessed 24 May 2021].

Constantin, L., 20. *What are vulnerability scanners and how do they work?.* [Online]
Available at: https://www.csoonline.com/article/3537230/what-are-vulnerability-scanners-and-how-do-they-work.html
[Accessed 21 May 2021].

Cunong, D. N., Saputra, M. & Puspitasari, W., 2020. ANALISIS RESIKO KEAMANAN TERHADAP WEBSITE DINAS PENANAMAN MODAN DAN PELAYANAN TERPADU SATU PINTU PEMERINTAHAN XYZYZ MENGGUNAKAN STANDAR PENETRATION TESTING EXECUTION STANDARD (PTES). *e-Proceeding of Engineering* , Volume Vol.7, p. 2091.

Fazriani, N. I. S., Cut, B. & Sanusi, 2019. Uji Keamanan Website Terhadap Serangan Path Traversal Pada Website Pendataan Warga. *KANDIDAT,* Volume 1, pp. 15-20.

Feri Wibowo, H. A. P. W., 2019. Uji Vulnerability pada Website Jurnal Ilmiah Universitas Muhammadiyah Purwokerto Menggunakan. *JURNAL INFORMATIKA*, Volume 6, pp. 212-218.

Guntoro, Costaner, L. & Musfawati, 2020. ANALISIS KEAMANAN WEB SERVER OPEN JOURNAL SYSTEM (OJS) MENGGUNAKAN METODE ISSAF DAN OWASP (STUDI KASUS OJS UNIVERSITAS LANCANG KUNING). *JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, Volume Volume 05, pp. 45-55.

Herrera, R. D. C., 21018. *Dirb is a web content scanner*. [Online] [Accessed 4 May 2021].

Inc, K., 2018. *How to start with Vega : The web security scanner?*. [Online] Available at: https://medium.com/knoldus/how-to-start-with-vega-the-web-security-scanner-f1493fbfb027 [Accessed 28 April 2021].

Joni & Assegaff, S., 2019,. ANALISIS DAN PERANCANGAN JARINGAN VIRTUAL PADA SMK NEGERI 2 KOTA JAMBI. *Jurnal Manajemen Sistem Informasi*, Volume Vol.4, p. 137.

Kamilah, I., Ritzkal & Hendrawan, A. H., 2019. Analisis Keamanan Vulnerability pada Server Absensi Kehadiran Laboratorium di Program Studi Teknik Informatika. *Seminar Nasional Sains dan Teknologi*.

Nmap.org, 2008. *Panduan Refensi Nmap (Man Page, bahasa Indonesia)*. [Online] Available at: https://nmap.org/man/id/index.html [Accessed 4 May 2021].

OnnoCenter.id, 2017. *Kali Linux: nikto cek DVWA*. [Online] Available at: https://lms.onnocenter.or.id/wiki/index.php/Kali_Linux:_nikto_cek_DVWA [Accessed 28 April 2021].

phoenixNAP, 2019. *Containers vs Virtual Machines (VMs): What's the Difference?*. [Online]

Available at: https://phoenixnap.com/kb/containers-vs-vms [Accessed 18 May 2021].

Pirsa, N. & Sumijan, 2020. Meningkatkan Keamanan Sistem Informasi Puskesmas Terpadu dengan Metode Grey-Box Penetration Test Menggunakan Computer Assisted Audit Techniques. *Jurnal Informasi dan Teknologi*, Volume 2, pp. 133-138.

Puput Dani Prasetyoadi, S. & Dr.Ir. Zulfajri B.Hasanuddin, M., 2016. Analisis Jaringan Komputer menggunakan Teknologi. *Jurnal Teknologi Informasi & Komunikasi*.

Putra, A. A., 2020. ANALISA KERENTANAN PADA SITUSWEB. *Jurnal Informanika*, Volume 6.

Putra, S. S. H., 2017. Penanggulangan Serangan XSS, CSRF, SQL Injection. *Jurnal Pendidikan dan Teknologi Informasi Menggunakan Metode Blackbox Pada Marketplace IVENMU*, Volume 4, pp. 289-300.

Rahmadani1, M. A., 2, M. F. R. & Gunamawan3, T., 2017. IMPLEMENTASI HACKING WIRELESS DENGAN KALI LINUX MENGGUNAKAN. *e-Proceeding of Applied Science*, Volume 3, p. 1767.

Rusdiana, B. C. S., 2019. Analisa Keamanan Website Terhadap Serangan Cross-Site Request Forgery (CSRF). *Cross-Site Request Forgery (CSRF)*, Volume 1, pp. 21-29.

Sirait, F., K, M. S. & Putra, 2018. Implementasi Metode Vulnerability Dan Hardening Pada Sistem Keamanan Jaringan. *Jurnal Teknologi Elektro*, Volume 9.

Sitelock, 2017. *What is a Website Vulnerability and How Can it be Exploited?*. [Online]
Available at: https://www.sitelock.com/blog/what-is-a-website-vulnerability/ [Accessed 21 may 2021].

Subgraph, 2014. *Vega Vulnerability Scanner*. [Online]
Available at: https://subgraph.com/vega/ [Accessed 28 April 2021].

Sudiharyanto Lika, R. D. P. H. ,. I. V., 2018. ANALISA SERANGAN SQL INJEKSI MENGGUNAKAN SQLMAP. *Jurnal Sistem dan Teknologi Informasi*, Volume 4, pp. 88-94.

Sullo, C. & Lodge, D., 2019. *Nikto2*. [Online] Available at: https://cirt.net/Nikto2 [Accessed 28 April 2021].

Swigger, P., 2021. *Website vulnerability scanning*. [Online] Available at: https://portswigger.net/burp/vulnerability-scanner/guide-to-vulnerability-scanning [Accessed 21 May 2021].

Yashia, 2017. *Keamanan Jaringan Internet dan Firewall*. [Online] Available at: https://aptika.kominfo.go.id/2017/06/keamanan-jaringan-internet-dan-firewall/ [Accessed 20 April 2021].

Wahyudi, 2019. ANALISA PENGUJIAN KERENTANAN TERHADAP WEB SERVER SIMAK (Studi Kasus : STMIK Kharisma Karawang). *Jurnal Teknologi Informasi*, Volume 5.

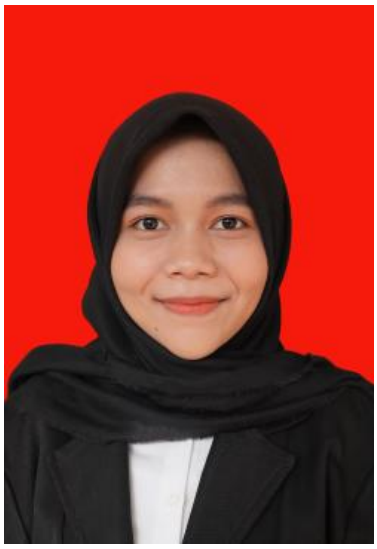
Yulianingsih, 2016. Menangkal Serangan SQL Injection dengan Parameterized Query. *Jurnal Edukasi dan Penelitian Informatika (JEPIN)*, Volume 2.

Yunus, M., 2019. ANALISIS KERENTANAN APLIKASI BERBASIS WEB MENGGUNAKAN KOMBINASI SECURITY TOOLS PROJECT BERDASARKAN FRAMEWORK OWASP VERSI 4. *Jurnal Ilmiah Informatika Komputer*, Volume Volume 24 .

Zhang, E., 2020. *What is a Website Vulnerability Scanner, and Why Should You Use One?*. [Online] Available at: https://www.zeguro.com/blog/what-is-a-website-vulnerability-scanner-and-why-should-you-use-one [Accessed 21 May 2021].

LAMPIRAN

DAFTAR RIWAYAT HIDUP PENULIS



Laily Rachmi Tsani

Lahir di Jakarta, 4 Desember 1999. Lulus dari SDIT Al-Khairaat tahun 2011, MTsN 6 Jakarta tahun 2014, SMAN 93 Jakarta pada tahun 2017 dan Diploma II program studi Network Administrator professional di CCIT-FTUI pada tahun 2019. Saat ini sedang menempuh pendidikan Diploma IV Program Studi Teknik Multimedia dan Jaringan Jurusan Teknik Informatika dan Komputer di Politeknik Negeri Jakarta.