Jurnal Sistem dan Teknologi Informasi (JSTI)

https://journalpedia.com/1/index.php/jsti Vol. 06, No. 3 Agustus 2024

PENETRATION TESTING UNTUK MENGUJI KERENTANAN SISTEM INFORMASI PEMERINTAH DAERAH

Merry Dian Khoiroh[1]
Email: 210631100118@student.trunojoyo.ac.id

Muhlis Tahir[2]
Email: muhlis.tahir@trunojoyo.ac.id

M. Ainul Yaqin Asmorodono[3]
Email: 210631100132@student.trunojoyo.ac.id

Iksan Dwi Rahmawan[4]
Email: 210631100140@student.trunojoyo.ac.id

Diniyatul Fatma[5]
Email: 210631100124@student.trunojoyo.ac.id

Maulana Pramudigdo[6]
Email: 210631100141@student.trunojoyo.ac.id

M. Rosul[7]
Email: 210631100135@student.trunojoyo.ac.id

[1,2,3,4,5,6,7]Universitas Trunojoyo Madura

ABSTRAK

Teknologi internet dapat dirasakan dalam berbagai bidang kehidupan, banyak media internet yang menjadi tempat penyaluran informasi secara resmi dan sebagai media interaksi antar manusia. Salah satunya yang sering digunakan adalah *website*. Karena menjadi media penyaluran informasi banyak pihak yang kini membutuhkan akan perlindungan terhadap informasi sensitif yang tersimpan dalam suatu *website*. Dalam hal ini jika suatu instansi pemerintah yang memiliki berbagai macam sistem informasi *website* dalam menjalankan kegiatan operasionalnya dan server yang menyimpan berbagai data rahasia dan informasi masih rentan dalam keamanan sistemnya maka akibat dari hal ini dapat memicu terjadinya ancaman-ancaman tindak kejahatan *cyber* oleh pihak yang tidak bertanggung jawab. Untuk mengatasi masalah tersebut, dibutuhkan evaluasi kerentanan (*Vulnerabilty*) dengan menggunakan metode *Penetration Testing* dengan mencoba menggunakan teknik SQLmap untuk menganalisa celah keamanan pada website tersebut melalui Kali Linux. Agar nantinya dapat mengetahui kelemahan dan kerentanan dari *website* tersebut yang dapat dievaluasi dan diperbaiki dikemudian hari. Hasil uji coba yang diperoleh pada penelitian ini yaitu *vulnerability level hight, level medium, level low*, dan *informational* dan setelah di eksploitasi menggunakan teknik SQLmap dengan menerapkan SQL *injection* berhasil melakukan penetrasi kedalam sistem dan diperoleh file *database* yang disimpan pada server yang berisikan informasi penting

dan rahasia yang sangat rentan untuk disalah gunakan oleh pihak yang tidak bertanggung jawab.

Kata Kunci: *Penetration Testing, Vulnerability, Kali Linux, SQLmap*

ABSTRACT

With the rapid development of technology, many internet media have become a place for official distribution of information and as a medium for interaction between people. One of them that is often used is a website. Because it is a medium for distributing information, many parties now need protection for sensitive information stored on a website. In this case, if a government agency has various kinds of website information systems in carrying out its operational activities and servers that store various confidential data and information are still vulnerable in terms of system security then the consequences of this can trigger threats of cyber crime by unauthorized parties. responsible. To overcome this problem, a vulnerability evaluation is needed using the Penetration Testing method by trying to use the SQLmap technique to analyze security gaps on the website via Kali Linux. So that later you can find out the weaknesses and vulnerabilities of the website which can be evaluated and corrected at a later date. The test results obtained in this research are high level, medium level, low level, and informational vulnerability and after being exploited using the SQLmap technique by applying SQL injection, they succeeded in penetrating the system and obtained a database file stored on the server containing important information and secrets that are very vulnerable to misuse by irresponsible parties.

Keywords: *Penetration Testing, Vulnerability, Kali Linux, SQLmap.*

1. PENDAHULUAN

Pada era digital ini, mayoritas setiap masyarakat mencari informasi melalui website, sehingga website menjadi platform yang paling sering diakses oleh setiap masyarakat. Oleh sebab itu penggunaan website pada suatu instansi pemerintah sangat penting yang digunakan sebagai media penyaluran informasi secara resmi dari suatu pemerintahan yang ditujukan kepada masyarakat setempat, selain itu website tersebut juga dapat digunakan sebagai media interaksi dengan masyarakat seperti tempat penyampaian aspirasi masyarakat. Dengan adanya website tersebut, aliran informasi dan komunikasi antara masyarakat dan pemerintah dapat dilakukan dengan mudah dan efisien.

Dibalik banyaknya manfaat dan kelebihan penggunaan website tidak menutup kemungkinan terdapat kelemahan yang membahayakan, salah satunya yaitu pada celah keamanan yang lemah yang bisa diretas oleh pihak yang tidak bertanggung jawab. Hal ini

merupakan salah satu jenis tindak kejahatan cyber dikarenakan data dan informasi yang dimiliki suatu instansi pemerintahan tidak semua bersifat terbuka. Jika tidak segera ditanggulangi, akan mengakibatkan kerusakan data bahkan hilangnya data pada website tersebut.

Indonesia menduduki peringkat ke-2 dengan jumlah serangan 39.957 server dalam laporan survey BSSN (Badan Siber dan Sandi Negara).

Gambar 1. Data Skala Nasional Serangan Webserver Sumber : (Salsabila, 2020)

Menurut data di atas yang telah dihimpun oleh Badan Siber dan Sandi Negara (BSSN). menjelasakan bahwa terdapat 190 juta serangan terhadap webserver yang ada di indonesia dari mulai bulan januari hingga agustus 2020. Data diatas menunjukan bahwa keadaan web server yang ada di indonesia masih jauh dari keadaan aman dari ancaman dan serangan.

Begitu pula pada tahun ini, juru biacara BSSN mengungkapkan bahwasanya pemerintah mengalami kebocoran data. "BSSN sudah mendeteksi ada 207 dugaan pelanggaran data base sepanjang 2023. Terbanyak di situs administrasi pemerintahan sebanyak 55 persen. Ini wajar, kenapa? Karena sistem elektronik pemerintah banyak sekali, Ada ribuan sistem elektronik sehingga data breach paling banyak terjadi di pemerintahan. Di sektor teknologi dan informasi hanya 3 persen"(Ariandi, 2023)

Untuk mengatasi permasalahan seperti ini digunakan metode *penetration testing* untuk menganalisa celah keamanan pada *website* tersebut melalui kali linux yang telah mendapatkan izin oleh pihak terkait, agar nantinya ditemukan solusi yang tepat untuk meningkatkan sistem keamanan yang dapat disarankan kepada administrator jaringan pemerintah ataupun pihak terkait.

2. TINJAUAN PUSTAKA

Penetration Testing

Pengujian penetrasi (juga dikenal sebagai pentesting atau PT) adalah praktik umum untuk secara aktif menilai pertahanan jaringan komputer atau (Web Server) dengan

merencanakan dan mengeksekusi semua kemungkinan serangan untuk menemukan dan mengeksploitasi kerentanan yang ada. (Ghanem & Chen, 2020).

Penetration testing pada *website* merupakan langkah krusial dalam menjaga keamanan digital sebuah entitas dalam ranah daring. pengujian ini telah mendapatkan izin dari pihak terkait. Pengujian penetrasi menggunakan metode dan cara yang digunakan oleh penjahat dunia maya untuk menemukan kerentanan ini, tetapi diizinkan untuk melakukannya. Ini berarti tidak seperti penjahat dunia maya penguji penetrasi memiliki persetujuan / izin dari organisasi yang sedang diuji (Kelrey & Muzaki, 2019)

Kali Linux

Kali Linux merupakan suatu sistem operasi berbasis linux debian yang dapat digunakan untuk memenuhi keperluan dalam melakukan penetration testing disebuah keamanann pada komputer. Kali linux memiliki tamppilan yang sederhana dan penggunaan yang cukup mudah.

Vulnerability Assesment

Vulnerability Assessment adalah analisa keamanan yang menyeluruh serta mendalam terhadap berbagai dokumen terkait keamanan informasi, hasil scanning jaringan, konfigurasi pada sistem, cara pengelolaan, cara kesadaraan orang-orang yang terlibat dan keamanan fisik, untuk mengetahui seluruh kelamahan kristis yang ada. *Vulnerability Assessemnt* bukan sekedar melakukan scanning dari jaringan menggunakan *Vulnerability Assessemnt tools*. Hasil *Vulnerability Assessment* jauh berbeda dengan pentest *balckbox* dan *greybox*. Kedua jenis pentest ini tidak mampu memberikan hasil yang komprehensif karena tidak seluruh potensi kerentanan kritis akan terindentifikasi. Bahkan ditemukan dalam banyak kasus, hasil pentest *blackbox* melaporkan tidak adanya kelemahan kritis, namun saat dilakukan *Vulnerability Assessment* terdapat kelemahan kritis (Lumy, Majalah Infokomputer, April 2010).

SQLmap

SQLmap adalah alat sumber terbuka yang secara otomatis menemukan dan mengeksploitasi kerentanan injeksi SQL. Kita dapat menggunakannya untuk menguji aplikasi web untuk mengetahui kerentanan injeksi SQL dan mendapatkan akses ke database yang rentan. Kita dapat menggunakan SQLmap untuk melakukan berbagai macam serangan. Ini termasuk sidik jari basis data, ekstraksi data, dan bahkan pengambilalihan seluruh basis data. Kita juga dapat menggunakannya untuk melewati formulir login dan menjalankan perintah sewenang-wenang pada sistem operasi yang mendasarinya.

3. METODE PENELITIAN

Penetration testing pada penelitian ini menggunakan metode *experimental*. Penelitian ini menggunakan laptop dengan menggunakan *virtual machine* yaitu *virtualbox* yang menggunakan sistem operasi kali linux dan beberapa *tools* untuk simulasi serangan sistem dalam melakukan *penetration testing* dan telah mendapatkan izin dari pengelola *website* yang akan di uci coba.

Teknik pengujian *penestrationn testing* yang digunakan dalam demo simulasi serangan terdapat beberapa tahapan yaitu :

1) Planning

Tahapan dari *planning* ini yang pertama adalah *Executive summar* dan *Scope Of Testing* (mendefinisikan ruang lingkup dan tujuan pengujian serta mengumpulkan jaringan, nama *domain*, hingga server *email*)

2) Scanning

Pada tahapan *scanning* ini menggunakan beberapa *tools* salah satunya adalah *arachni* kemudian disajikan dengan *Graphical Summary* dan *List Of Vulnerability* yang telah ditemukan **(**pengecekan kode aplikasi untuk memperkirakan perilaku saat suatu sistem jaringan berjalan)

3) Gaining Access

Tahapan ini berupa *Vulnerability Assesment* menggunakan SQL injection (menggunakan serangan aplikasi web seperti SQL injection untuk mengungkap kerentanan target dan mengeksploitasi kerentanan tersebut dengan tujuan pencurian data dan yang lainnya dengan tujuan untuk memahami kerusakan yang ditimbulkannya)

4) *Maintaining Access* (Menggunakan kerentanan untuk melihat apakah kerentanan tersebut bersifat pemanen dalam sistem)

5) *Analisys* (pada tahap ini terdapat reporting yang berupa dokumentasi tentang kerentanan suatu sistem jaringan komputer dan juga terdapat analisa dan melaporkan risiko yang ditimbulkan dari kerentanan dan memberikan saran untuk peningkatan keamanan jaringan)

4. HASIL DAN PEMBAHASAN

1. Executive Sumary

a. Scope Of Testing

Pengujian akan fokus pada identifikasi kerentanan keamanan pada aplikasi web dan infrastruktur yang terkait. Ini termasuk analisis mendalam terhadap konfigurasi server, pengecekan terhadap kerentanan umum seperti SQL injection, *cross-site scripting* (XSS), serta pemeriksaan terhadap kontrol keamanan sesuai dengan standar terkini. Pengujian akan mencakup fase pencitraan *(reconnaissance)*, penetrasi aktif, dan pengujian eksplorasi terhadap kerentanan yang ditemukan. *Report penetration testing* ini akan mencakup hasil-hasil uji penetrasi dan rekomendasi perbaikan untuk memperkuat tingkat keamanan situs website ini.

b. Grapichal Summary

Menampilkan grafik yang menggambarkan hasil secara visual dan termasuk grafik lingkaran yang memperlihatkan distribusi kerentanan berdasarkan jenisnya seperti SQL injection, XSS, atau kerentanan lainnya. Grafik-grafik ini akan memberikan gambaran cepat dan mudah dipahami mengenai status keamanan *website*, memungkinkan kepentingan untuk dengan cepat mengidentifikasi area-area yang memerlukan perhatian lebih lanjut dan langkah-langkah perbaikan yang harus diambil pada *website* tersebut.

Digaram berikut adalah hasil dari scanning menggunakan arachni.

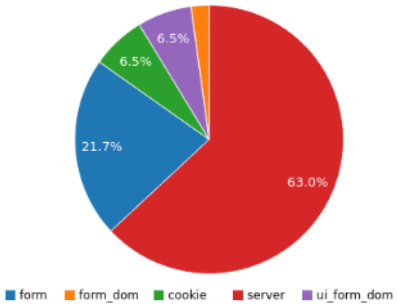


Diagram 1. Issue Website

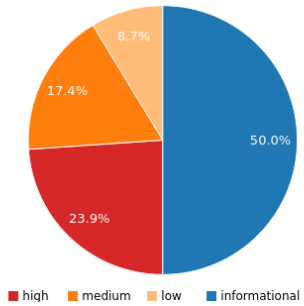


Diagram 2. Severity Website

c. List Of Vulnerabilities

No.	*Vulnerability*	*Severity*
1	*Cross-Site Request Forgery*	*High*
2	*Cross-Site Scripting (XSS)*	*High*
3	*DOM-based Cross-Site Scripting (XSS)*	*High*
4	*Blind SQL Injection (timing attack)*	*High*
5	*Common directory*	*Medium*
6	*Unencrypted password form*	*Medium*
7	*HTTP TRACE*	*Medium*
8	*Missing 'Strict-Transport-Security' header*	*Medium*
9	*Common sensitive file*	*Low*
10	*Password field with auto-complete*	*Low*
11	*Interesting response*	*Informational*

2. Detail Vulnerability yang ditemukan

a. Cross-Stie Request Forgery (Hight)

Setelah melakukan scan *Vulnerability* terhadap website, kali ini telah berhasil mengidentifikasi kerentanan tingkat tinggi berupa *Cross-Site Request Forgery* (CSRF) pada fitur yang memungkinkan serangan CSRF terjadi tanpa validasi yang memadai. CSRF memberikan potensi bagi penyerang untuk melakukan tindakan yang tidak diinginkan atas nama pengguna yang sudah terautentikasi, tanpa pengetahuan atau persetujuan mereka. Hal ini dapat membahayakan keamanan pengguna yang telah masuk ke dalam sistem. Untuk mengeksploitasi kerentanan ini, penyerang dapat memanfaatkan celah pada sistem validasi permintaan, memaksa pengguna yang sudah terautentikasi melakukan aksi tertentu tanpa persetujuan mereka.

b. Cross-Stie Scripting XSS (Hight)

Setelah melakukan *scan Vulnerability* terhadap *website*, ditemukan kerentanan tingkat tinggi yang terkait dengan *Cross-Site Scripting* (XSS) dalam konteks skrip *(script context).* Kerentanan ini terletak *website* dan dapat memungkinkan serangan XSS, di mana penyerang dapat menyisipkan skrip berbahaya ke dalam halaman web. Hal ini membuka celah bagi penyerang untuk mencuri data pengguna, menjalankan aksi yang tidak diinginkan atas nama *pengguna, atau memanipulasi tampilan website secara keseluruhan.*

c. Dom-Based Cross-Site Scripting XSS (Hight)

Setelah melakukan *scan Vulnerability* terhadap *website*, ditemukan kerentanan tingkat tinggi yang terkait dengan *DOM-based Cross-Site Scripting* (XSS). Kerentanan ini terletak pada mekanisme DOM *(Document Object Model) website* yang memungkinkan serangan XSS, di mana penyerang dapat menyisipkan skrip berbahaya ke dalam DOM yang kemudian dieksekusi di sisi klien, menjadikan pengguna rentan terhadap eksploitasi.

d. Blind SQL Injection Timing Attack (Hight)

Setelah melakukan scan *Vulnerability* terhadap *website*, teridentifikasi sebuah kerentanan tingkat tinggi yang terkait dengan *Blind SQL Injection*, khususnya pada metode serangan timing. Kerentanan ini memungkinkan penyerang untuk melakukan serangan SQL Injection yang secara tidak langsung memungkinkan mereka mendapatkan akses atau informasi sensitif dari database dengan menggunakan teknik timing attack. Melalui teknik ini, penyerang dapat

memanfaatkan waktu yang dibutuhkan untuk melakukan perintah SQL yang memungkinkan mereka mengungkapkan informasi sensitif.

e. Common Directory (Medium)

Setelah melakukan scan *Vulnerability* terhadap website ditemukan sebuah kerentanan pada direktori umum *(common directory)* yang dapat diakses publik. memungkinkan akses terhadap file dan informasi yang seharusnya tidak diperuntukkan untuk umum. Kehadiran direktori umum meningkatkan risiko keamanan dengan potensi akses tidak sah terhadap data sensitif, potensialnya penyebaran informasi yang seharusnya terbatas, dan penyalahgunaan data oleh pihak yang tidak berwenang.

f. HTPP Trace (Medium)

Setelah melakukan *scan Vulnerability* keamanan terhadap *website,* ditemukan kerentanan pada metode HTTP *Trace* yang masih aktif. Kehadiran fitur HTTP *Trace* dapat memberikan informasi sensitif kepada penyerang, memungkinkan mereka untuk melakukan serangan *Cross-Site Tracing* dan mendapatkan data rahasia seperti token otentikasi dari server. Hal ini meningkatkan risiko keamanan karena dapat mengekspos informasi penting kepada pihak yang tidak berwenang.

3. Vulnerability Assesment

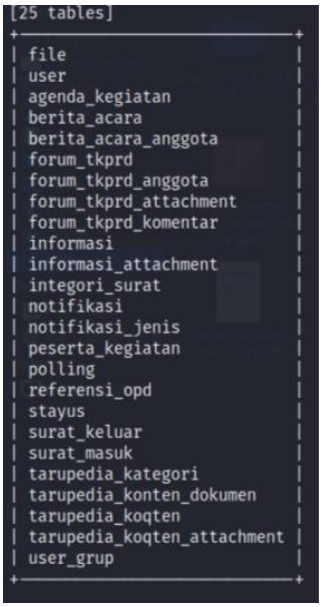
a. SQL Injection

Setelah melakukan penelusuran keamanan pada *website* tersebut dan berhasil mengidentifikasi celah keamanan berupa kerentanan SQL *injection.* Dengan menggunakan teknik sqlmap, berhasil melakukan penetrasi ke dalam sistem dan memperoleh akses ke 4 *database* yang terdapat pada website tersebut. Hasil dari penelusuran ini telah kami dokumentasikan secara rinci untuk keperluan analisis lebih lanjut untuk memperkuat keamanan sistem dan memberikan rekomendasi perbaikan kepada pihak terkait, dengan harapan dapat segera dilakukan perbaikan untuk mencegah potensi serangan yang lebih luas dan melindungi data yang ada.

Berikut merupakan dokumentasi SQL injection yang dilakukan dan dihasilkan 4 database.

Gambar 2. SQL injection temuan database

Setelah berhasil mengidentifikasi celah keamanan berupa SQL injection pada *website* tersebut, tim kami berhasil melakukan penetrasi ke dalam sistem dan memperoleh akses ke empat database yang tersedia. Dari salah satu database, kami berhasil mengekstraksi informasi dari 25 tabel yang beraneka ragam, mengandung data informasi penting. Selanjutnya, dari database MySQL, kami juga berhasil mengekstraksi informasi dari 22 tabel yang mengandung data informasi penting. Temuan ini telah kami dokumentasikan secara rinci untuk melakukan analisis mendalam terkait kerentanan sistem dan menyusun rekomendasi perbaikan yang tepat.



Gambar 3. SQL injection isi Database pertama

Gambar 4. SQL injection isi database mysql

4. Analisa dan Saran Perbaikan

Setelah analisis yang disampaikan disetiap kerentanan yang ditemukan terhadap temuan tersebut, terdapat kerentanan dan kelemahann pada website tersebut yang dapat diretas data penting di dalamnya. jenis kerentanan pada website tersebut. jika peretasan ini dilakukan oleh pihak yang tidak bertanggung jawab dapat menyebabkan kerusakan pada data - data yang ada didalamnya dan bahkan dapat kehilangan beberapa database tersebut. Bahwa disarankan sejumlah perbaikan yang perlu segera dilakukan untuk meningkatkan keamanan sistem:

1. Pembaruan Keamanan *Database*: Perlu dilakukan pembaruan sistem keamanan database untuk mengatasi celah SQL injection yang ada. Implementasi *parameterized queries* atau penggunaan *prepared statements* akan membantu mencegah serangan SQL injection di masa mendatang.
2. Peninjauan Kebijakan Akses: Mengevaluasi ulang terhadap kebijakan akses ke database. Peninjauan hak akses, pengelolaan kata sandi yang lebih kuat, serta pembaruan rutin kata sandi dapat membantu mengurangi risiko akses tidak sah.
3. Monitoring Keamanan Aktif: Diperlukan penerapan sistem monitoring keamanan aktif yang dapat mendeteksi dan memberikan peringatan atas aktivitas yang mencurigakan atau serangan yang sedang terjadi.
4. Kami merekomendasikan bahwa tindakan perbaikan ini segera dilakukan untuk mengurangi risiko serangan dan melindungi data sensitif yang tersimpan dalam database.

Terima kasih atas perhatiannya terhadap temuan ini. Kami berharap rekomendasi ini dapat menjadi landasan untuk meningkatkan keamanan sistem secara keseluruhan

5. KESIMPULAN

Berdasarkan penelitian yang telah dilakukan mengenai keamanan web server maka kesimpulan yang didapat adalah terdapat kerentanan dan kelemahann pada *website* tersebut yang dapat diretas data penting di dalamnya. jenis kerentanan pada *website* tersebut didapatkan empat kategori *level* yaitu *hight, medium, low,* dan *informational*. simulasi serangan menggunakan SQL injection dengan menggunakan teknik SQLmap yang menghasilkan didapatkannya 4 *database* dan disetiap *database* terdapat data yang bersifat penting yang berada didalam *website* tersebut. jika peretasan ini dilakukan oleh pihak yang tidak bertanggung jawab dapat menyebabkan kerusakan pada data - data yang ada didalamnya dan bahkan dapat kehilangan beberapa database tersebut. Maka saran dan masukan tehadap pihak terkait agar melakukan sejumlah perbaikan yang perlu segera dilakukan untuk meningkatkan keamanan sistem yaitu dengan pembaruan keamanan *database* untuk mengatasi celah SQL injection yang ada dengan cara bisa mengimplementasikan *parameterized queris* atau penggunaan *prepared statements*, cara tersebut dapat membantu mencegah serangan SQL *injection* di masa mendatang. Selain itu perlu adanya peinjauan kebijakan akses dengan mengevalusi ulang terhadap kebijakan akses database, peninjauan hak akse, pengelolaan kata sandi yang lebih kuat, serta pembaharuan rutin kata sandi dapat membantu mengurangi risiko akses tidak sah, dan selalu memonitoring keamanan aktif yang dapat mendeteksi aktivitaas yang mencurigakan.

DAFTAR PUSTAKA

Andrian, (2023) Situs administrasi pemerintaah jadi yang terbanyak dibobol hacker. *CNNindonesia.com* *https://www.cnnindonesia.com/teknologi/20231024152212-192-1015287/situs-administrasi-pemerintah-jadi-yang-terbanyak-dibobol-hacker*

Bin Ibrahim, A., & Kant, S. (2018). Penetration Testing Using SQL Injection to Recognize Bin Ibrahim, A., & Kant, S. (2018). Penetration Testing Using SQL Injection to Recognize the Vulnerable Point on Web Pages. International *Journal of Applied Engineering Research, 13*(8), 5935–5942. http://www.ripublication.com

Fauzan, R. H. (2019). Pengujian Keamanan Sistem Informasi Akademik Menggunakan Metode Penetration Testing. *Studi Kasus: Institut Pertanian Stiper Yogyakarta*

Ghanem, M. C., & Chen, T. M. (2020). Reinforcement learning for efficient network penetration

testing. *Information (Switzerland)*, *11*(1), 1–23. https://doi.org/10.3390/info11010006

I Gede Ary Suta Sanjaya, Gusti Made Arya Sasmita, D. M. S. A. (2020). Evaluasi Keamanan Website Lembaga X Melalui Penetration Testing Menggunakan Framework ISSAF. *Jurnal Ilmiah Merpati, Vol. 8, No (2), 113–124.*

Kelrey, A. R., & Muzaki, A. (2019). Pengaruh Ethical Hacking Bagi Keamanan Data Perusahaan. *CyberSeccurity Dan Forensik Digital*, *2*(2), 77–81.

Lumy, Gildas Deograt. 2010, *Ilusi Test Penetrasi Bagian 1*, InfoKomputer.

S. Hidayatulloh and D. Saptadiaji, "Penetration Testing pada Website Universitas ARS Menggunakan Open Web Application Security Project (OWASP)," 2021. [Online]. *Available: http://jurnal.itg.ac.id/*

Salsabila, P. Z. (2020, October 12). Kejahatan Siber di Indonesia Naik 4 Kali Lipat Selama Pandemi. *Kompas.Com*, *1*. *https://tekno.kompas.com/read/2020/10/1 2/07020007/kejahatan-siber-di indonesianaik-4-kali-lipat-selama-pandemi*