EVALUASI KEAMANAN SISTEM INFORMASI BERBASIS WEB MENGGUNAKAN METODE SQL INJECTION

(Web-Based Information System Security Evaluation Using SQL Injection Method)

Ramadya Wahyu Dwinanto[1*], Azkiyatun Nadroh[2]
[1]Program Studi Informatika, Fakultas Sains dan Teknologi, Universitas Harapan Bangsa Purwokerto
[2]Program Studi Sistem Infromasi, Fakultas Sains dan Teknologi, Universitas Harapan Bangsa Purwokerto
, Jl. Raden Patah No.100, Kedunglongsir, Ledug, Kec. Kembaran, Kabupaten Banyumas, Jawa Tengah 53182
[1]ramadyawahyudwinanto1208@gmail.com*, [2]azkiyatunnadroh56@gmail.com

ABSTRACT

Nowadays, various media can be accessed to obtain information, with the internet and smartphones being the main sources of information for people around the world. The internet has opened up access to information to anyone, regardless of geographic location, time of day, or age of the user. This allows individuals around the world to easily access public information. However, the existence of web applications that facilitate this kind of access is also an attractive target for attackers. Unfortunately, currently, more than 90% of these applications have exploitable vulnerabilities, with an average of 13 vulnerabilities per application. This research focuses on penetration testing to test the security level of the pmb.uhb.ac.id website. The purpose of this research is to identify security vulnerabilities that may exist on the pmb.uhb.ac.id website using the SQL injection method. The results of testing the pmb.uhb.ac.id website showed that the site was not affected by SQL Injection. However, the gap scan results show that some of the highest medium level gaps were found in the Nessus and Acunetix scan results. The most frequently found gaps come from gaps that depend on Cross Site Scripting.

Keywords : Website, Penetration Testing, SQL Injection

ABSTRAK

Saat ini, berbagai media dapat diakses untuk mendapatkan informasi, dengan internet dan ponsel pintar menjadi sumber utama informasi bagi masyarakat di seluruh dunia. Internet telah membuka akses informasi kepada siapa saja, tanpa memandang lokasi geografis, waktu, atau usia pengguna. Ini memungkinkan individu di seluruh dunia untuk mengakses informasi publik dengan mudah. Namun, keberadaan aplikasi web yang memfasilitasi akses seperti ini juga menjadi target menarik bagi para penyerang. Sayangnya, saat ini, lebih dari 90% dari aplikasi-aplikasi tersebut memiliki kerentanan yang dapat dieksploitasi, dengan rata-rata 13 kerentanan per aplikasi. Penelitian ini difokuskan pada penetration testing untuk menguji tingkat keamanan situs web pmb.uhb.ac.id. Tujuan dari penelitian ini adalah untuk mengidentifikasi kerentanan keamanan yang mungkin ada di situs web pmb.uhb.ac.id dengan menggunakan metode SQL injection. Hasil dari pengujian terhadap situs web pmb.uhb.ac.id menunjukkan bahwa situs tersebut tidak terkena efek SQL Injection. Namun, hasil pemindaian celah menunjukkan bahwa beberapa celah dengan tingkat sedang tertinggi ditemukan dalam hasil pemindaian Nessus dan Acunetix. Celah yang paling banyak ditemukan berasal dari celah yang bergantung pada Cross Site Scripting.

Kata kunci : Website, Penetration Testing, SQL Injection

*** Ramadya Wahyu Dwinanto**
Email:ramadyawahyudwinanto1208@gmail.com

PENDAHULUAN

Saat ini, teknologi informasi dan digital berkembang dengan sangat cepat. Membuat informasi tersedia dengan menggunakan berbagai media. Internet *website* dan *mobile* saat ini menjadi andalan dalam memberikan informasi kepada masyarakat global karena membuat informasi tersedia untuk semua orang, tanpa memandang waktu, wilayah, atau usia. Hal ini memungkinkan orang-orang di seluruh dunia mengakses informasi publik sebagai sumber informasi(Zech et al., 2019). Keamanan data dan informasi semakin penting untuk menjaga validitas dan integritas data. Serangan dan upaya penyusupan atau pemindaian yang tidak berwenang harus mencegah sistem, jaringan komunikasi, dan data(Noman et al., 2020). Akibatnya, keamanan jaringan, *website*, *server*, dan database harus dipantau dan ditingkatkan secara berkala. Semakin banyak *tools* penetrasi yang tersedia di internet dan pengetahuan tentang *hacking* semakin memudahkan para penyusup dan penyerang untuk melakukan penyusupan dan penyerangan(Ahmed & Junaid, 2019).

Dalam beberapa tahun terakhir, aplikasi *website* telah menjadi bagian utama kehidupan kita, baik secara komersial maupun pribadi. Aplikasi ini berbagi dan memproses data pengguna sensitif yang harus dilindungi dengan segala cara. Dengan demikian, aplikasi multi-pengguna seperti itu adalah target yang menarik bagi penyerang. Sayangnya, saat ini lebih dari 90% aplikasi ini rentan, dengan jumlah rata-rata 13 kerentanan per aplikasi. Keamanan karenanya memainkan peran penting untuk aplikasi *website*(Ula, 2019).

Server web adalah salah satu target penyerang yang paling umum dan rentan. Menyerang server *website* adalah langkah pertama untuk terus menyerang *database*. *Web server* adalah inti dari *World Wide Web* (WWW), yang berfungsi untuk mengirimkan data melalui protokol HTTP (*Hyper Text Transfer Protocol*), yang dapat dikirimkan pengguna melalui *web browser* untuk ditampilkan di halaman *web*(Chowdhary et al., 2020).

Ada banyak jenis teknik untuk menguji sebuah keamanan pada *website*. Salah satu teknik yang sangat populer dalam Penetration Testing adalah *SQL Injection. SQL Injection* adalah serangan basis data menggunakan SQL (*Structure Query Language*) untuk mendapatkan informasi atau melakukan aktivitas yang biasanya memerlukan akun pengguna yang diautentikasi. Dengan perkiraan kejadian maksimum 19%, tingkat kejadian rata-rata 3% dan 274.000 kasus, 94% aplikasi disaring untuk injeksi. Sehingga *Injection* menjadi urutan ke 3 dalam *OWASP Top 10 Vulnerabilities for 2022*(Lika et al., 2018).

Andria dan Ridho Pamungkas (2021) dalam penelitiannya tentang *penetration testing database* menggunakan metode *SQL injection* via *SQLMap* di *termux* menggunakan metode *SQL Injection* aplikasi *Termux* pada *smartphone* memiliki hasil bahwa terdapat celah keamanan atau kerentanan yang dapat dieksploitasi oleh pencuri atau peretas. Kerentanan ini memungkinkan mereka untuk melihat dan mengakses struktur *database* yang ada di *web server*. Mengingat betapa pentingnya *database* sebagai media penyimpanan data, itu pasti sangat berbahaya. Dengan demikian, hasilnya menunjukkan bahwa perlu dilakukan upaya untuk mencegah dan mencegah akses yang tidak semestinya atau tidak sah. Akses ini harus diminimalkan agar kerugian yang serius seperti penyalahgunaan data oleh pihak yang tidak bertanggung jawab dapat dihindari(Andria & Pamungkas, 2021).

Sedangkan dalam penelitian tentang pengujian pengumpulan informasi menggunakan panduan pengujian OWASP v4 pada studi kasus aplikasi SIMAK-NG Universitas Udayana oleh Rasendriya Revo Daniswara, Gusti Made Arya Sasmita dan I Putu Agus Eka Pratama (2020) yang menggunakan metode OWASP Testing Guide Version 4 memiliki hasil bahwa dilakukan sepuluh tes, tiga di antaranya menghasilkan hasil negative dan tidak ada informasi *sensitive* yang ditemukan dari beberapa pengujian yang telah dilakukan(Revo et al., 2020).

Kemudian berdasarkan penelitian dari Richard Pangalila, Agustinus Noertjahyana, Justinus Andjarwirawan mengenai *penetration testing* server sistem informasi manajemen dan *website* Universitas Kristen Petra yang menggunakan metode *Penetration Testing* menunjukkan bahwa hasil keamanan sistem baik situs maupun administrasi yang diuji dalam penelitian ini secara keseluruhan tergolong buruk karena kurangnya perawatan sistem, seperti pembaruan berkala, yang menyebabkan beberapa kasus yang seharusnya tidak terjadi tetapi akhirnya

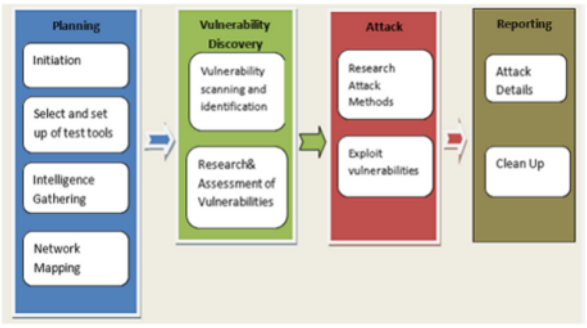
menyebabkan kerusakan. Hasil pemindaian celah menunjukkan bahwa celah pada tingkat sedang terbesar berasal dari celah yang bergantung pada SSL dan *Cross Site Scripting*. Selain itu, hasil pemindaian *OpenVAS* dan *Acunetix* menunjukkan bahwa celah pada tingkat sedang juga berasal dari jenis ini. Selain itu, adanya dominasi *Denial of Service* yang signifikan pada keempat situs yang diuji menunjukkan bahwa situs tersebut mungkin rentan terhadap *overloading*, yang menyebabkan mereka tidak dapat memberikan layanan kepada pengguna(Pangalila et al., 2015).

Pertumbuhan Universitas Harapan Bangsa Purwokerto semakin besar. Bersamaan dengan berkembangnya teknologi yang juga semakin pesat, Universitas Harapan Bangsa Purwokerto memiliki berbagai *website* sistem informasi yang mempunyai fungsi berbeda-beda.

Penelitian ini membahas tentang penetration testing untuk menguji keamanan *website* pmb.uhb.ac.id menggunakan *SQL injection*, yaitu teknik hacking yang berfokus pada pengujian database sebagai sistem penyimpanan data dengan memasukkan perintah SQL (*Structured Query Language*) melalui URL (*Uniform Resource Locator*) *Address* untuk kemudian di eksekusi oleh basis data yang terdapat pada *web server*. Penelitian ini menggunakan SQLMap, sebuah alat *open source* yang dapat menganalisa, mendeteksi, dan melakukan *exploit bug SQL Injection*(Astrida et al., 2022).

METODE PENELITIAN

Metode yang digunakan dalam penelitian ini menggunakan frame yang diusulkan oleh Rajiv Kumar dan Katlego Tlhagadikgora (Kumar & Tlhagadikgora, 2019) yang meliputi :



Gambar 1. Metodologi pengujian penetrasi

1. *Planning* (Rencana)
   a. *Initiation*
      Tahapan dimulai dengan mengidentifikasi masalah yang ada pada objek penelitian(Chowdhary et al., 2020).
   b. *Select and set up of test tools*
      Proses memilih dan menyiapkan alat uji yang digunakan pada penelitian(Lika et al., 2018).
   c. *Intelligence Gathering*
      Proses mengumpulkan informasi sebanyak banyaknya untuk digunakan dalam menguji.
   d. *Network Mapping*
      Proses *Network mapping* atau NMap ini digunakan untuk mengecek keamanan aplikasi(Hermawan, 2021).
2. *Vulnerability Discovery*
   a. *Vulnerability scanning and identification*
      Tahapan ini dengan melakukan pemindaian dan mengidentifikasi keamanan dan memahami kelemahan dalam sistem atau aplikasi(Revo et al., 2020).
   b. *Research & Assessment of vulnerabilities*
      Proses penelitian kerentanan untuk menemukan kerentanan dan penilaian kerentanan untuk mengidentifikasi, mengevaluasi, dan mengklasifikasikan tingkat risiko pada kerentanan keamanan pada aplikasi.
3. *Attack*
   a. *Research attack methods*
      Tahapan ini mencari metode yang digunakan untuk penyerangan(Aydos et al., 2022).
   b. *Exploit vulnerabilities*
      Proses dimana mengeksploitasi celah kerentanan pada aplikasi(Kade et al., 2020).
4. *Reporting*
   a. *Attack details*
      Proses pelaporan informasi rincian hasil serangan(Andria & Pamungkas, 2021).
   b. *Clean up*
      Membersihkan apa yang telah kita uji dan telah kita laporkan(Andria & Pamungkas, 2021).

HASIL DAN PEMBAHASAN

Information Gathering

Pengumpulan informasi dalam penelitian ini menggunakan *tools Whatweb*.

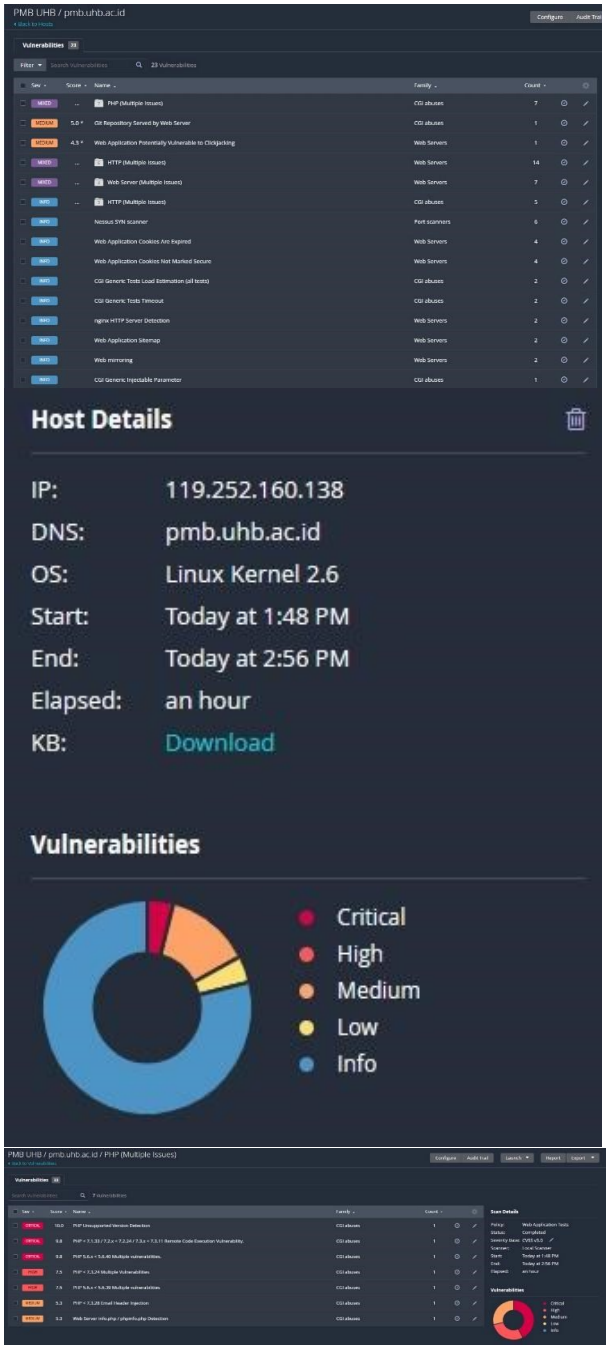
Gambar 2. Hasil pengumpulan informasi menggunakan Whatweb

Dengan menggunakan *Whatweb* ini kita menemukan banyak sekali informasi pada *website*. Seperti pada *website* yang telah kita uji menggunakan *whatweb website* tersebut memiliki *IP address* 119.252.160.138, dengan keamanan server menggunakan *Nginx* dan email yang terhubung dengan *website* adalah info@uhb.ac.id dan pmb@uhb.ac.id. Dan masih banyak sekali informasi yang didapatkan melalui *whatweb*.

Vulnerability Test

Vulnerability test digunakan untuk mengidentifikasi dan mengidentifikasi serangan yang dapat terjadi terhadap kerentanan sistem yang ada, dan untuk mengevaluasi dampak ekpoitasi yang dilakukan oleh penyerang terhadap bisnis(EC-Council, 2012). Penilaian kerentanan pada tahap ini menggunakan 2 *tools* yaitu *Nessus* dan *Acunnetix*.

1. *Nessus*

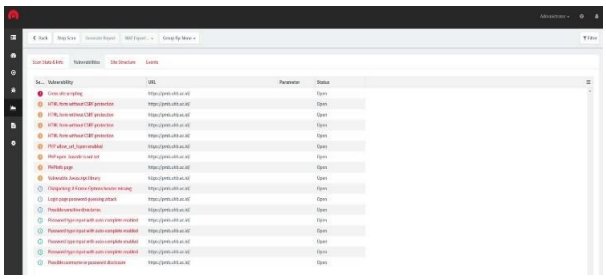


Gambar 3. Hasil pemindaian website menggunakan Nessus

Dengan menggunakan *Nessus* kita menemukan celah keamanan *critical* sebanyak 3 atau 8%, *hight* sebanyak 2 atau 5%, *medium* sebanyak 5 atau 13%, *low* sebanyak 3 atau 5%, dan memberikan informasi sebanyak 55 atau 69%.

Berdasarkan rangkuman pemindaian website melalui *Nessus* ini yang digolongkan menjadi 5 tingkatan. *Website* tersebut cukup memiliki banyak celah keamanan yang nantinya dapat berakibat fatal jika tidak segera dilakukan perbaikan atau pembaruan.

2. *Acunnetix*



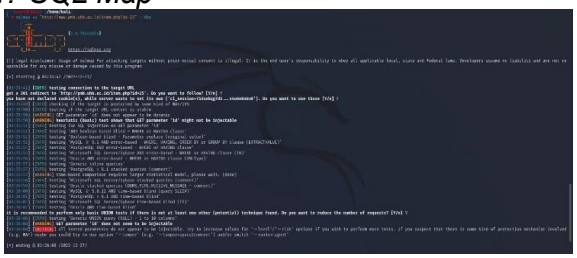
Gambar 4 Hasil pemindaian menggunakan tools Accunetix

Berdasarkan pemindaian yang telah dilakukan menggunakan *accunetix* bahwa terdapat banyak sekali celah keamanan yang terdeteksi. Terutama yang sangat rentan adalah dengan menggunakan *Cross Site Script*. Dengan adanya hal tersebut sangat sekali dibutuhkan perbaikan *website*.

Attack

Proses penyerangan menggunakan Teknik *SQL Injection* menggunakan *SQL Map* dan *Login Bypass*.

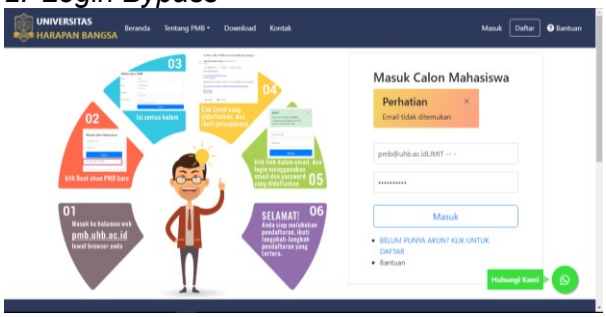
1. SQL Map



Gambar 5. Hasil penyerangan website menggunakan SQL Map

Website tersebut sudah dilakukan *SQL Injection* dengan menggunakan *SQL Map*. Banyak sekali informasi yang di informasikan oleh *SQL Map*, tetapi hasilnya *website* tersebut tidak bisa di serang menggunakan *SQL Injection*. Meskipun demikian, *website* tersebut masih perlu adanya perbaikan atau pembaruan. Karena yang telah di uji *vulnerability* masih banyak sekali celah keamanan yang lalai diperhatikan.

2. Login Bypass



Gambar 6. Hasil penyerangan website menggunakan Login Bypass dengan username

Login menggunakan *email* yang telah ditemukan pada proses *scanning* dan menambahkan kode 'LIMIT -- -'. Hasilnya tidak dapat *login*, karena server membaca itu bukan jenis *email*.

Gambar 7. Hasil penyerangan website menggunakan Login Bypass tidak dengan username

Hasil dari *login* dengan tidak menggunakan *email* namun dengan kode ‘or 1=1 LIMIT 1 -- -’ menunjukan bahwa tidak dapat *login*, karena server membaca itu bukan jenis *email*.

SIMPULAN

Hasil pengujian menunjukkan bahwa situs pmb.uhb.ac.id aman dari *SQL Injection*. Namun, ada kekurangan dalam pemeliharaan sistem, seperti pembaruan yang tidak diberikan secara berkala. Untuk saat ini, situs ini masih dapat dianggap baik karena celah dengan tingkat tinggi sudah cukup sedikit. Namun, dengan menjaga sistem yang diperbarui dengan baik, celah dapat dikurangi hingga tingkat yang paling rendah. *SQL Injection* tidak berdampak pada mereka. Namun, hasil pemindaian celah menunjukkan bahwa celah yang paling banyak pada tingkat sedang berasal dari celah yang bergantung pada *Cross Site Scripting*.

SARAN

Dengan demikian, untuk meningkatkan keamanan dan pemeliharaan website pmb.uhb.ac.id adalah dengan memperbarui sistem secara berkala. Penting untuk memastikan bahwa semua komponen perangkat lunak, platform, dan bahkan plugin pihak ketiga diperbarui secara teratur. Ini akan membantu mengatasi kerentanannya terhadap serangan dan memperbaiki bug yang mungkin ada. Keamanan web harus selalu menjadi prioritas utama untuk melindungi data dan reputasi situs website.

DAFTAR PUSTAKA

Ahmed, S., & Junaid, M. (2019). – Optimized

Port Scanning With Nmap Tool. *2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (ICoMET)*, *March 2020*, 1–6.

Andria, A., & Pamungkas, R. (2021). Penetration Testing Database Menggunakan Metode SQL Injection Via SQLMap di Termux. In *Indonesian Journal of Applied Informatics* (Vol. 5, Issue 1, p. 1). https://doi.org/10.20961/ijai.v5i1.40845

Astrida, D. N., Saputra, A. R., & Assaufi, A. I. (2022). Analysis and Evaluation of Wireless Network Security with the Penetration Testing Execution Standard (PTES). *Sinkron*, *7*(1), 147–154. https://doi.org/10.33395/sinkron.v7i1.11249

Aydos, M., Aldan, Ç., Coşkun, E., & Soydan, A. (2022). Security testing of web applications: A systematic mapping of the literature. *Journal of King Saud University - Computer and Information Sciences*, *34*(9), 6775–6792. https://doi.org/10.1016/j.jksuci.2021.09.018

Chowdhary, A., Huang, D., Mahendran, J. S., Romo, D., Deng, Y., & Sabur, A. (2020). Autonomous security analysis and penetration testing. *Proceedings - 2020 16th International Conference on Mobility, Sensing and Networking, MSN 2020*, *September*, 508–515. https://doi.org/10.1109/MSN50589.2020.00086

EC-Council. (2012). *Certified Ethical Hacker v8: Module 20 Penetration Testing*.

Hermawan, R. (2021). Teknik Uji Penetrasi Web Server Menggunakan SQL Injection dengan SQLmap di Kalilinux. *STRING (Satuan Tulisan Riset Dan Inovasi Teknologi)*, *6*(2), 210. https://doi.org/10.30998/string.v6i2.11477

Kade, N., Handayani, M., Made, G., Sasmita, A., Agung, A., & Agung, K. (2020). Evaluation Security Web-Based Information System Application Using ISSAF Framework (Case Study : SIMAK-NG Udayana University). *JITTER - Jurnal Ilmiah Teknologi Dan Komputer*, *1*(2).

Kumar, R., & Tlhagadikgora, K. (2019). Internal Network Penetration Testing Using Free/Open Source Tools: Network and System Administration Approach. In *Communications in Computer and Information Science* (Vol. 956). Springer Singapore. https://doi.org/10.1007/978-981-13-3143-5_22

Lika, S., Halim, R. D. P., & Verdian, I. (2018). Analisa Serangan Sql Injeksi Menggunakan Sqlmap. *POSITIF : Jurnal Sistem Dan Teknologi Informasi*, *4*(2), 88.

Noman, M., Iqbal, M., & Manzoor, A. (2020). A survey on detection and prevention of web vulnerabilities. *International Journal of Advanced Computer Science and Applications*, *11*(6), 521–540. https://doi.org/10.14569/IJACSA.2020.0110665

Pangalila, R., Neortjahyana, A., & Andjarwirawan, J. (2015). Penetration Testing Server Sistem Informasi Manajemen Dan Website Universitas Kristen Petra. *Jurnal Teknologi Informasi*, *3*(2), pp.271-p.276. http://publication.petra.ac.id/index.php/teknik-informatika/article/view/3145

Revo, R., Made, G., Sasmita, A., Agus, I. P., & Pratama, E. (2020). Testing for Information Gathering Using OWASP Testing Guide v4 (Case Study : Udayana University SIMAK-NG Application). *Jurnal Ilmiah Teknologi Dan Komputer*, *1*(1).

Ula, M. (2019). Evaluasi Kinerja Software Web Penetration Testing. *TECHSI - Jurnal Teknik Informatika*, *11*(3), 336. https://doi.org/10.29103/techsi.v11i3.1996

Zech, P., Felderer, M., & Breu, R. (2019). Knowledge-based security testing of web applications by logic programming. *International Journal on Software Tools for Technology Transfer*, *21*(2), 221–246. https://doi.org/10.1007/s10009-017-0472-3