WEB PENETRATION TESTING DALAM MENCARI KERENTANAN SQL INJECTION

Nico Natanael
Informatika, Universitas Pembangunan Nasional "Veteran" Jawa Timur
Jl. Rungkut Madya No.1, Gn. Anyar, Kec. Gn. Anyar, Surabaya, Jawa Timur 60294
nicnatan11@gmail.com

ABSTRAK

Di era digital yang sudah sangat maju, tidak dapat dipungkiri bahwa perkembangan digitalisasi lebih lanjut mutlak diperlukan dalam banyak hal. Contoh kebutuhan adalah website. Namun kita harus menyadari bahwa seiring dengan meningkatnya perkembangan teknologi, maka kejahatan siber di dunia maya juga meningkat, termasuk kejahatan siber di website. Seperti serangan SQL Injection, XSS, Path Traversal, dan serangan injection lainnya. Pada penelitian ini merucut pada serangan SQL Injection, dengan menyertakan metode Penetration Testing. Maksut dari penelitian ini mengetahui kerentanan SQL Injection pada website OWASP JUICE SHOP. Pendeteksian secara manual serangan SQL Injection dengan memasukkan simbol karakter pada form login. Lalu, dilanjutkan dengan penyerangan pada bagian eksploitasi. Dengan hasil pada tahapan eksploitasi mendapatkan hak akses admin, dengan payloads yang sederhana.

Kata kunci: *penetration testing, sql injection, owasp.*

1. PENDAHULUAN

Di era digital yang sudah sangat maju, tidak dapat dipungkiri bahwa perkembangan digitalisasi sangat diperlukan dalam banyak hal. Contoh kebutuhannya adalah website. Website kini sudah tersebar luas di berbagai sektor, baik itu bisnis, belanja, dan tak lupa sektor pendidikan itu sendiri. Banyak developer yang telah mempelajari berbagai bentuk kreativitas dan keterampilan dalam mendesain website. Namun kita harus memahami bahwa seiring dengan semakin berkembangnya kejahatan siber, maka kejahatan siber di dunia maya juga akan semakin meningkat, termasuk kejahatan siber di website. [1]

Perlu diketahui, jumlah domain web di dunia sudah mencapai ratusan juta. Menurut Verisign Domain Name Industry Brief 2021, Edisi ke-4, terdapat sekitar 367,3 juta nama domain yang terdaftar di seluruh dunia pada akhir Juni 2021. Dibandingkan kuartal sebelumnya, jumlah tersebut meningkat sebesar 3,8 juta atau 1,1%. Sedangkan menurut data yang dipublikasikan Verisign pada akhir kuartal I 2021, total TLD yang terdaftar di Indonesia berjumlah sekitar 775 ribu. Namun hanya mencakup top-level domain terpopuler seperti .com, .net, .org, dll, namun tidak mencakup top-level domain terpopuler di Indonesia yaitu .id. [2]

Untuk menghindari kerugian yang disebabkan oleh serangan siber, perusahaan dan organisasi harus memiliki sistem keamanan informasi yang kuat. Penetration testing adalah salah satu metode yang digunakan untuk menguji keamanan sistem informasi. Penetration testing atau pen testing adalah proses menguji sistem keamanan dengan mencoba menembus sistem tersebut dan mengidentifikasi kelemahan yang ada. Hal ini bertujuan untuk membantu mengidentifikasi risiko keamanan yang ada dalam sistem, sehingga dapat diambil tindakan pencegahan yang tepat. [3]

Berdasarkan penjelasan diatas, perlu diketahui bahwa pentingnya sadar akan pencegahan kejahatan cyber perlu ditingkatkan. Oleh karena itu pada penelitian ini menguraikan cara untuk mengetahui kerentanan celah yang ada pada website, dan melakukan penetration testing untuk membuktikan kerentanan celah. Untuk target website penelitian menggunakan lab virtual yaitu OWASP JUICE SHOP Website yang dijalankan pada localhost.

2. TINJAUAN PUSTAKA

Dalam penyusunan dan pengerjaan penelitian ini, tidak dipungkiri mengacu terhadap penelitian penelitian sebelumnya dengan topik yang sama dan dilakukan oleh pihak lain. adapun terdapat beberapa hasil hasil dari penelitian sebelumnya yang akan dijadikan sebagai referensi dalam penyusunan dan pengerjaan penelitian ini.

2.1. PENELITIAN TERDAHULU

Pada penelitian ini menggunakan pustaka hasil-hasil penelitian sebelumnya yang relevan, berupa jurnal. Berikut adalah sumber terkait penelitian sebelumnya.

Memberikan pandangan betapa jahatnya penetration testing dan dampak dari SQL Injection untuk berbagai sistem aplikasi web. Penulis menerangkan bahwa memilih beberapa website secara acak untuk dianalisis kerentanan keamanan celah pada website, termasuk dengan SQL Injection. Pada tahapan hasil dan pembahasan terdapat beberapa langkah untuk memenuhi tujuan penulis. Yang pertama, penulis mencari ruang lingkup proyek penelitian, yang disebut Scope of Project. Di dalamnya terdapat alamat domain website dan IP website. Yang kedua, penulis melakukan pengumpulan informasi terkait target Scope, yang disebut Information Gathering. Di dalamnya berisi tentang informasi

server dan services yang ada pada website menggunakan port scanning. Dan yang terakhir, penulis melakukan pengujian terhadap port yang terbuka sesuai dengan hasil Information Gathering, yang mana disebut dengan Penetration Testing. [1]
Terdapat beberapa hasil penetration testing yang dilakukan oleh penulis. Namun, disini hanya menjabarkan keberhasilan penulis dalam melakukan penetration testing saja. Yang pertama pengujian terhadap website A. Terdapat beberapa port yang terbuka pada website ini, salah satu nya yaitu port untuk ssh. Penulis menemukan user dan password menggunakan Teknik brute force dengan menggunakan tools Metaspoit dan Hydra. Yang kedua pengujian terhadap website C. Penulis melakukan bypass login menggunakan SQL Injection untuk masuk ke halaman dashboard admin dan mendapatkan hak penuh sebagai admin. Yang ketiga pengujian terhadap website D. Penulis mengatakan bahwa port 111 terbuka pada website D, yang mana port tersebut digunakan untuk Network File System(NFS). Beberapa kerentanan pada website D membuat penulis dapat mengakses ke sistem file. Namun, pada website D tidak ditemukan celah keamanan untuk SQL Injection. Yang terakhir disatukan saja pada poin ini, dikarenakan hasil yang ditemukan sama antara Website E, F, G, dan H. Penulis mendapatkan celah keamanan terhadap 4 website ini yaitu dapat dilakukannya SQL Injection, dan penulis dapat mengakses database pada keempat website ini. [1]

Mengetahui celah keamanan pada sisi web server pada studi kasus di E-Learning Universitas Negeri Padang. Pada tahapan hasil dan pembahasan di jurnal diterangkan dengan beberapa langkah tahapan. Yang pertama yaitu, mencari tahu terkait informasi domain dari target, termasuk port yang terbuka pada target domain. Penulis menyebut tahapan ini sebagai Intelegence Gathering Yang kedua, penulis melakukan proses scanning ke target domain untuk memperoleh hasil celah keamanan. Penulis menyebut tahapan ini sebagai Vulnerability Analysis.[4]
Di dapatkan lima hasil peringatan teratas.

1. HTML without Cross-site Request Forgery (CSRF/XSRF) protection
2. Development configuration file yang menampilkan informasi sensitive
3. Slow HTTP Denial of Service Attack
4. Weak password (login page passwordguessing attack)
5. TLS 1.0 Enable

Mendapatkan hasil nilai kerentanan pada sistem website dan mendeteksi kerentanan pada website. Pada tahapan hasil dan pembahasan pada jurnal, penulis menggunakan tool Nessus. Didapatkan Vulnerability Assesment yang cukup fatal. Dan penulis menyimpulkan dengan persentase yaitu, 3% kerentanan kritis, 5% tinggi, 15% sedang, dan 5% rendah. Dengan kerentanan pada PHP, JQuery, ClickJacking, User Enumeration, dan Password Auto-Completion. Setelah penulis mendapatkan hasil celah keamanan, dilakukannya laporan hasil tersebut dengan menyertakan solusi yang dapat menanggulangi celah keamanan tersebut. [5]

Analisa keamanan website pada SMKN 1 Cibatu menggunakan metode *Penetration Testnig Execution Standard* menghasilkan beberapa tingkat kerentanan pada website sistem informasi target. Dengan hasil yang paling tinggi yaitu *Cross Site Scripting, Cross Site Request Forgery* dan *Eavesdropping.* Menggunakan teknik yang sama dengan penelitian artikel ini, dapat dihasilkan beberapa tingkatan celah keamanan yang lumayan berbahaya. Tahapan yang paling penting yaitu pada *Vulnerability Testing* dan *Exploitation*. Menggunakan alat bantu Nessus dapat diketahui celah keamanan secara otomatis. Pada tahapan *Exploitation* dengan memasukkan *payloads* tidak mendapatkan hasil yang dapat mengancam kinerja website.[6]

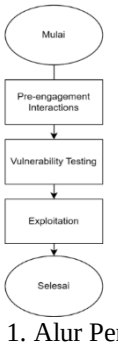
3. METODE PENELITIAN

Pada penelitian ini memanfaatkan pendekatan secara kuantitatif dan penerapan penelitian secara deskriptif. [4]

Terdapat tiga cara untuk melakukan penetration testing yaitu *White Box, Grey Box, dan Black Box.* Dengan perbedaan yang mencolok yaitu pada hak akses pada setiap cara yang berbeda. Pada penelitian ini menggunakan metode *Penetration Testing* yang mana metode ini kerap dipakai untuk pengujian keamanan website. [7]

3.1. Penetration Testing

Terdapat beberapa langkah dalam melakukan *Penetration Testing*. Seperti pada gambar 1, yang mana menggambarkan alur jalan nya metode. [4]



Gambar 1. Alur Penelitian

a. Pre-Engagement Interactions
   Serangkaian kegiatan yang dilakukan sebelum memulai sebuah tes penetrasi atau penetration testing. Interaksi ini bertujuan untuk memastikan bahwa tes penetrasi dilakukan dengan aman dan sesuai dengan persyaratan yang telah disepakati oleh kedua belah pihak.
b. Vulnerability Testing
   Pencarian celah keamaan target scooping, yang mana diperoleh dari beberapa tools secara otomatis. Dan bisa juga dilakukan secara manual

dengan menginputkan tanda petik (‘) pada form login website.[8]

c. Exploitation
Pada tahapan exploitation melakukan percobaan penyerangan terhadap hasil vulnerability testing yang mengacu pada hasil vulnerability testing.

3.2. Variabel Penelitian

Mengacu pada poin 3.1 penelitian ini. Terdapat beberapa variabel yang dipakai untuk menjalankan tahapan pada poin 3.1.

a. Pre-Engagement Interactions
   1. Scoping
      Scoping adalah target penelitian. Pada penelitian ini objek penelitian nya yaitu lab virtual OWASP JUICE SHOP Website yang dijalankan pada localhost. [9]
   2. Consent
      Consent adalah sebuah perjanjian kedua belah pihak. Namun, pada penelitian ini tidak menggunakan perjanjian consent, dikarenakan lab virtual yang dipakai bersifat Open-Source. [3]
   3. Information Gathering
      Information Gathering merupakan tahapan untuk mencari data terkait website scoping. Pada penelitian ini memanfaatkan tools whatweb pada kali linux. [3]

b. Vulnerability Testing
Pada *Vulnerability Testing* akan memanfaatkan percobaan memasukkan tanda petik (‘) pada form login website. Jika terjadi error, maka memungkinkan bisa terkena serangan SQL Injection.[8]

c. Exploitation
Pada tahapan exploitation, memanfaatkan tools BurpSuite, dan akan dilakukan secara *realtime* melalui google chrome. Yang mana, pada *exploitation* bergerak memanfaatkan hasil dari *vulnerability testing.* [10]

4. HASIL DAN PEMBAHASAN

a. Pre-Engagement Interactions

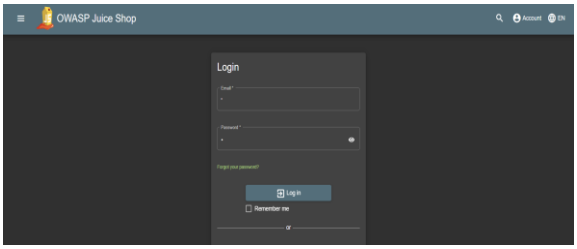
Gambar 2. Hasil Scan Whatweb

b. Pre-Engagement Interactions

Gambar 3. Hasil Scan Whatweb

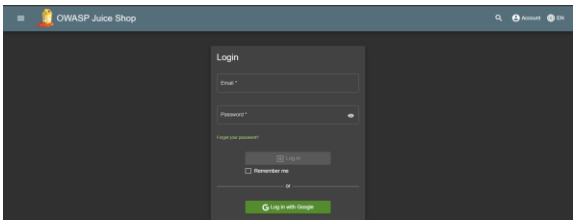
Pada gambar 2 dan 3, dapat dilihat bahwa alamat IP yang dimiliki oleh OWASP JUICE SHOP adalah 54.220.192.176. Dengan teknologi yang dipakai diantaranya yaitu Jquery versi 2.2.4.

c. Vulnerability Testing
Pada tahapan ini akan mencoba form login pada website vulnerable terhadap SQL Injection atau tidak. Akan dimasukkan tanda petik (‘) pada form login bagian email, dan akan dimasukkan ‘a’ pada form login bagian *password*. Jika, seandainya tidak terjadi *error* pada website, kemungkinan *vulnerable* terhadap SQL Injection Blind. [8]



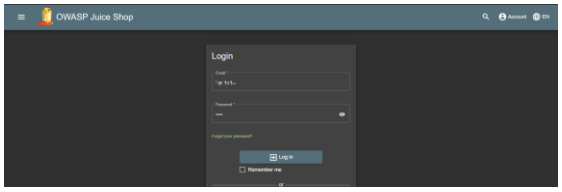
Gambar 4 Percobaan SQL Injection

d. Exploitation
Pada tahapan *Exploitation* mengacu pada hasil *Vulnerability Testing.* Terdapat salah satunya *vulnerable* SQL Injection. Yang mana akan didemonstrasikan sebagai berikut.



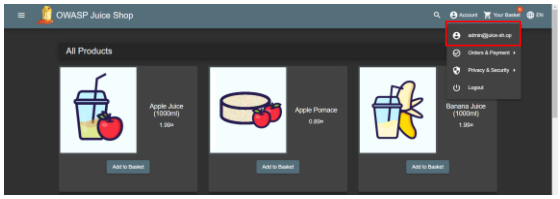
Gambar 5. Form Login OWASP JUICE SHOP

Pada gambar 4, merupakan form login yang disediakan oleh OWASP JUICE SHOP. Yang mana, pada form tersebut vulnerable terdapat SQL Injection. Selanjutnya, akan dimasukkan *payload* berikut ‘ or 1=1 –, pada bagian Email, dan ‘a’ untuk bagian password. Seperti pada gambar 5.



Gambar 6. Percobaan Memasukkan Payload

Setelah, menekan button login, disini kita mendapatkan user sebagai Admin Juice Shop seperti pada gambar 6 berikut.



Gambar 7. Mendapat akun Admin

5. KESIMPULAN DAN SARAN

Pada penelitian ini mengedepankan pencarian terhadap kerentanan SQL Injection dengan menggunakan metode *Penetration Testing*. Yang mana, sebelum memulai *Exploitation* harus mencari informasi terkait website *scoping*. Dapat dilihat pada poin hasil dan pembahasan. Bahwa website OWASP JUICE SHOP memiliki celah SQL Injection pada form login yang tersedia. Dengan payload sederhana, dapat mendapatkan akun admin milik OWASP JUICE SHOP. Terdapat sebuah saran terkait kerentanan SQL Injection yaitu perlunya mensanitasi *input* dari pada *user*, dan perlunya membatasi karakter penulisan dalam *input* dari pada *user*.

DAFTAR PUSTAKA

[1] A. Alanda, D. Satria, M. Isthofa Ardhana, A. A. Dahlan, and A. Mooduto, "INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION journal homepage: www.joiv.org/index.php/joiv INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION Web Application Penetration Testing Using SQL Injection Attack." [Online]. Available: www.joiv.org/index.php/joiv

[2] and fr, "TOP 10 LARGEST TLDs BY NUMBER OF REPORTED DOMAIN NAMES THE DOMAIN NAME INDUSTRY BRIEF EXECUTIVE SUMMARY," vol. 19, no. 1, doi: 10.5M.

[3] F. Fachri, A. Fadlil, I. Riadi, A. Dahlan, Y. Jln Soepomo, and I. Artikel, "Analisis Keamanan Webserver Menggunakan Penetration Test," *JURNAL INFORMATIKA*, vol. 8, no. 2, 2021, [Online]. Available: http://ejournal.bsi.ac.id/ejurnal/index.php/ji

[4] "Jurnal Vocational Teknik Elektronika dan Informatika", [Online]. Available: http://ejournal.unp.ac.id/index.php/voteknika/

[5] R. Armando *et al.*, "IT Support Website Security Evaluation Using Vulnerability Assessment Tools," *Journal of Information Systems and Informatics*, vol. 4, no. 4, 2022, [Online]. Available: http://journal-isi.org/index.php/isi

[6] S. Utoro *et al.*, "Analisis Keamanan Website E-Learning SMKN 1 Cibatu Menggunakan Metode Penetration Testing Execution Standard."

[7] S. Rani and R. Nagpal, "PENETRATION TESTING USING METASPLOIT FRAMEWORK: AN ETHICAL APPROACH," *International Research Journal of Engineering and Technology*, 2019, [Online]. Available: www.irjet.net

[8] O. Cheikhrouhou, H. Hamam, A. Mahfoudhi, and I. Jemal, "SQL Injection Attack Detection and Prevention Techniques Using Machine Learning," 2020. [Online]. Available: http://www.ripublication.com

[9] M. Althunayyan, N. Saxena, S. Li, and P. Gope, "Evaluation of Black-Box Web Application Security Scanners in Detecting Injection Vulnerabilities," *Electronics (Switzerland)*, vol. 11, no. 13, Jul. 2022, doi: 10.3390/electronics11132049.

[10] R. Jadhav, S. Ovhal, P. Mutyal, A. Damale, and S. Nagannawar, "Automating Security Vulnerabilities using Scanning and Exploiting," 2019.