E-ISSN : 2988-1986
https://ejournal.warunayama.org/kohesi

Kohesi: Jurnal Multidisiplin Saintek
Volume 01, No. 06 2023, pp. 81-90

PENGUJIAN KEAMANAN WEB JUICE SHOP DENGAN METODE PENTESTING BERBASIS OWASP TOP 10

Mochammad Dzaki Al Vriano
E-mail : 19081010138@student.upnjatim.ac.id

Informatika, Ilmu Komputer, UPN "Veteran" Jawa Timur

Abstrak

Seiring dengan perkembangan teknologi informasi keamanan merupakan suatu faktor vital yang harus ada dan terjamin dalam penerapan dan penggunaannya. Aplikasi berbasis web merupakan salah satu platform yang memiliki kerentanan dalam keamanan siber. Kerentan ini dapat terhadap bebagai ancaman maupun serangan maupun eksploitasi seperti *SQL injection, DoS, CSRF, Cross Site Scripting (XSS),* dan lain-lain yang tercantum dalam OWASP Top 10. Hal ini merupakan landasan dari terbentuknya *Open Web Application Security Project* (OWASP) yang merupakan organisasi yang bertujuan untuk meningkatkan keamanan perangkat lunak. OWASP menentukan standar keamanan perangkat lunak yang digunakan secara *universal*. Metode *penetration testing* ini berfungsi untuk menganalisis kerentanan dengan mengidentifikasi dan eksploitasi dari pengujian keamanan yang dapat dijadikan sebagai laporan pengembangan keamanan pada OWASP Juice Shop . *Penetration testing* akan dilakukan melalui 5 tahapan *ethical hacking* yaitu *Reconnaisance, scanning & enumeration, gaining access (exploitation), maintaining access, dan covering tracks*.

Kata kunci: Kerentanan, *penetration testing*, OWASP, *ethical hacking*

1. PENDAHULUAN

1.1 Latar Belakang

Perkembangan dalam teknologi informasi yang pesat hingga kini menjadi bagian dari lini kehidupan masyarakat merupakan salah satu fenomena yang luar biasa[1]. Hal ini dapat dirasakan salah satunya dengan terintegrasinya segala aspek kehidupan masyarakat dengan bentuk sistem informasi maupun aplikasi yang memudahkan pekerjaan dan kebutuhan[2]. Dengan kemajuan ini juga terdapat beberapa keresahan yang dirasakan baik dari sisi pengguna maupun pengembang suatu sistem informasi.

Keresahan dalam teknologi informasi ini dapat berupa kerentanan keamanan yang dapat menimbulkan ancaman untuk mencari keuntungan finansial, merusak nama baik perusahaan tertentu dan lain sebagainya apabila ditemukan oleh para pelaku kriminal *cyber/cracker*. Namun pada umumnya tidak semua yang dapat menemukan celah keamanan ini adalah pelaku kriminal, adapun ethical hacker yang merupakan peretas yang bertujuan untuk memperkuat keamanan suatu sistem.

Penetration testing atau *pentest* adalah kegiatan di mana seseorang mencoba untuk melakukan serangan terhadap suatu jaringan organisasi/perusahaan untuk menemukan kelemahan pada sistem tersebut. Hal ini juga umum dilakukan oleh seorang ethical hacker untuk memperkuat keamanan suatu sistem. Dalam penelitian ini akan dilakukan sebuah *penetration testing* terhadap aplikasi berbasis web yang bertujuan untuk menemukan celah keamanan sebelum titik tersebut dieksploitasi para *cracker* serta membantu meningkatkan keamanan sistem. Pentesting dalam penelitian ini juga akan menerapkan 5 tahapan dari ethical hacking yaitu *teconnaisance, scanning & enumeration, gaining access (exploitation), maintaining access,* dan *covering tracks*[2].

Prefix DOI : 10.3785/kjst.v1i6.347

Sebuah sistem pada umumnya memliki mekanisme keamanan yang diterapkan oleh pihak pengembang[3]. Namun pada kenyataannya terdapat banyak informasi penting dan critical yang dapat diakses tanpa izin akibat dari celah keamanan oleh sistem tersebut. OWASP Juice Shop merupakan web yang dirancang untuk menguji developer maupun pentester dalam cyber security tentang kerentanannya yang umum terjadi pada aplikasi web. Web ini menggabungkan aspek keamanan dalam dunia nyata dengan pengalaman berbelanja online dengan model online shop. Juice Shop menawarkan beberapa pertanyaan keamanan yang mengajarkan pengguna bagaimana membuat, menemukan, dan melindungi aplikasi web dari potensi serangan cyber.

Adapun tujuan yang diharapkan dari penelitian pengujian celah keamanan ini adalah menguji keamanan sistem aplikasi berbasis web terhadap serangan eksternal oleh pelaku kriminal, melakukan pengujian terhadap sistem yang telah dikembangkan, dan membuat laporan hasil pentest/*pentest report*. *Pentest report* ini akan terdiri temuan yang didapat dari tahapan *reconnaisance* hingga *post exploitation*. Tujuannya laporan ini akan digunakan untuk menyajikan laporan dan hasil dari pentest yang telah dilakukan dengan tujuan untuk membantu perusahaan/instansi pengguna sistem[4]. Dengan begitu saat melihat laporan pentest, klien dapat sepenuhnya menyadari seberapa aman produk dan area apa yang perlu ditingkatkan.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, berikut adalah rumusan masalah yang didapat:

a. Bagaimana cara menguji keamanan domain dan subdomain yang dapat merugikan perusahaan/instansi pengguna sistem?
b. Bagaimana solusi pencegahan preventif dalam keamanan w*ebsite* OWASP Juice Shop?

1.3 Tujuan Penelitian

Tujuan yang diharapkan dari penilitan pengujian celah keamanan ini adalah:

a. Melakukan pengujian celah keamanan dari website dengan yang ada terhadap kemungkinan serangan eksternal.
b. Mengidentifikasi hasil temuan dari pengujian pentest dan kemungkinan solusi preventif yang dapat digunakan.

2. TINJAUAN PUSTAKA

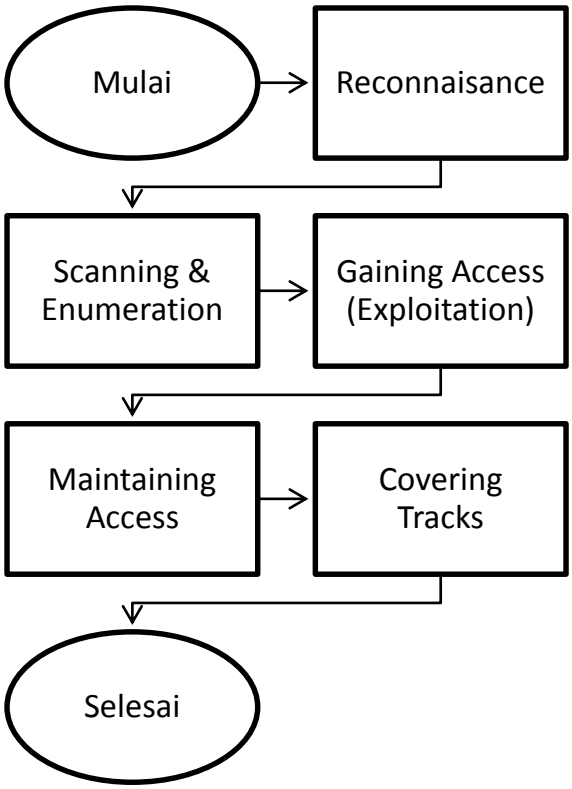
Syarif Hidayatulloh dan Desky Saptadiaji dalam penelitiannya [2] menjelaskan bahwa pengujian *penetration testing* yang dilakukan pada Website Universitas ARS berbasis pada OWASP TOP 10 2017. Adapun metode pengujian yang dilakukan melalui 4 tahapan yakni *planning, discovery, attack,* dan *reporting.*Hasil yang didaptkan dari penelitian ini adalah keamanan pada website Universitas ARS sudah sesuai dengan prinsip CIA TRIAD.

Olajide Ojagbule, Hayden Wimmer, dan Rami J. Haddad dalam penelitiannya [3] melakukan analisis kerentanan terhadap 3 web CMS yaitu Wordpress, Drupal, dan Joomla dengan metode penyerangan SQL injection melalui SQLMAP. Mereka mengemukakan 3 metode yang digunakan dalam proses pengujian yakni *information gathering, exploitation,* dan *mitigation*. Hasil yang didapatkan adalah ketiga website sudah terlindungi oleh Web App Firewall (WAF).

Fauzan Rum. Dalam penelitiannya [4] memaparkan pengujian *penetration testing* yang dilakukan tidak berbasis pada OWASP TOP 10. Adapun pengujian yang dilakukan melalui 5 tahapan *yaitu information gathering, enumeration, vulnerability assessment, gaining access, dan escalating privelages*. Target/studi kasus dari penilitian ketiga yang telah dilakukan ini adalah sistem akademik INSTIPER Yogyakarta.

Pada penelitian selanjutnya

Prefix DOI : 10.3785/kjst.v1i6.347



Gambar 1 5 Tahapan Dari Ethical Hacking

3. METODOLOGI

Penetration testing pada umumnya dilakukan dalam beberapa tahapan. Tahapan ini bersifat universal di mana sebagian besar *pentester* menggunakan metode yang sama. Metodologi *pentest* ada untuk mengidentifikasi kerentanan keamanan dalam suatu organisasi[5]. Metode ini memiliki 5 tahapan dalam penerapannya seperti yang terdapat pada gambar 1.

A. *Reconnaisance*

Reconnaisance merupakan tahap di mana pencarian mengenai informasi target dilakukan. Pencarian ini juga biasa disebut dengan *open source intelligence* (OSINT). *Reconnaisance* dapat dilakukan secara aktif maupun pasif[6]. Berikut adalah penjelasan dari kedua jenis tahap *reconnaisance* yang umum dilakukan.

1) *Active reconnaisance* adalah ketika seorang *pentester* berinteraksi langsung dengan sistem komputer untuk mengumpulkan informasi spesifik sistem tentang target. Pengintaian aktif dapat digunakan untuk mengetahui informasi seperti port terbuka/tertutup, OS mesin, layanan yang sedang berjalan, *banner grabbing*, menemukan *host* baru, atau menemukan aplikasi rentan pada *host*.

2) *Passive reconnaisance* adalah ketika seorang *pentester* dapat menggali informasi tanpa berinteraksi secara langsung dengan target. Umumnya *passive reconnaisance* menggunakan

Prefix DOI : 10.3785/kjst.v1i6.347

sumber daya publik yang memiliki informasi tentang target tersebut. Hal ini biasa disebut dengan *Open source intelligence* (OSINT). Dengan OSINT seseorang dapat menumpulkan informasi penting seperti IP *address*, *domain name, email, dns*, dsb.

B. *Scanning & Enumeration*

Tahap *scanning & enumeration* merupakan tahap yang dilakukan untuk menggali informasi atau *scanning* nama pengguna, nama mesin, sumber daya jaringan, dan layanan lain dari suatu sistem[7]. Semua informasi yang dikumpulkan digunakan untuk mengidentifikasi kerentanan atau titik lemah dalam keamanan sistem dan kemudian mencoba untuk mengeksploitasinya. *Vulnerabilty scanning & enumeration* dapat dilakukan dengan menggunakan beberapa *open source tools* seperti nessus, nmap, burp suite, dll.

C. *Gaining Access*

Gaining access merupakan proses untuk mendapatkan akses ke dalam sistem melalui eksploitasi dari temuan yang telah didapatkan. Tujuannya adalah agar seorang pentester mendapatkan akses mutlak/*root* maupun akses informasi berharga dan rahasia. Contoh paling umum dalam *web app exploitation* menurut OWASP Top 10 2021 adalah :

1) A01:Broken Access Control
2) A02:Cryptographic Failures
3) A03:Injection
4) A04:Insecure Design
5) A05:Security Misconfiguration
6) A06:Vulnerable and Outdated Components
7) A07:Identification and Authentication Failures
8) A08:Software and Data Integrity Failures
9) A09:Security Logging and Monitoring Failures
10) A10:Server-Side Request Forgery

D. *Maintaining Access*

Setelah berhasil mendapatkan akses dari host, jika *rules of engagement* mengizinkannya, lebih baik untuk memastikan bahwa *pentester* akan dapat mempertahankan akses untuk pemeriksaan lebih lanjut atau penetrasi jaringan target. Hal ini juga untuk memastikan bahwa *pentester* akan dapat terhubung kembali ke korban/target meskipun terdapat hambatan yang terjadi contohnya seperti jaringan maupun infrastruktur target yang telah *direset*[8]. *Maintaining access* dapat dilakukan melalui penggunaan *backdoor* maupun virus/malware. Namun pada umumnya dalam *pentesting* maintaining access dapat dicapai hanya dengan add user.

E. *Covering Tracks*

Covering tracks merupakan tahap di mana seorang *pentester* mengembalikan kondisi sistem/jaringan target kembali pada posisi konfigurasi awal yang sesuai saat sebelum dilakukannya *pentesting*. Hal ini bertujuan untuk menghilangkan jejak sedalam mungkin sehingga *pentester* sulit untuk dilacak.

4. HASIL DAN PEMBAHASAN

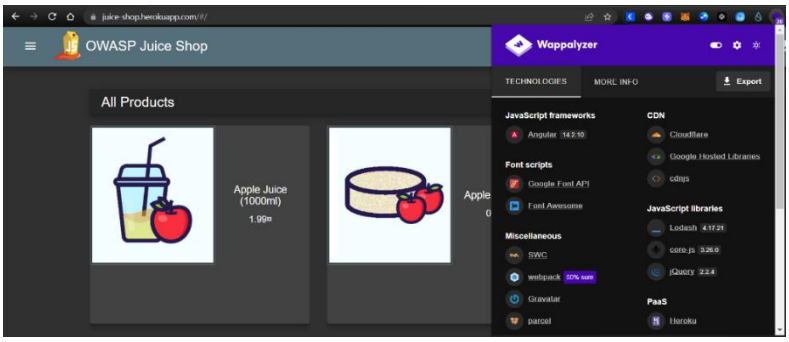
Berikut adalah hasil dan pembahasan pengujian celah keamanan website yang sesuai dengan metode *ethical hacking*.

A. Tahap *Reconnaisance*

Pada tahap ini dilakukan pencarian informasi mengenai target dengan cara aktif maupun

Prefix DOI : 10.3785/kjst.v1i6.347

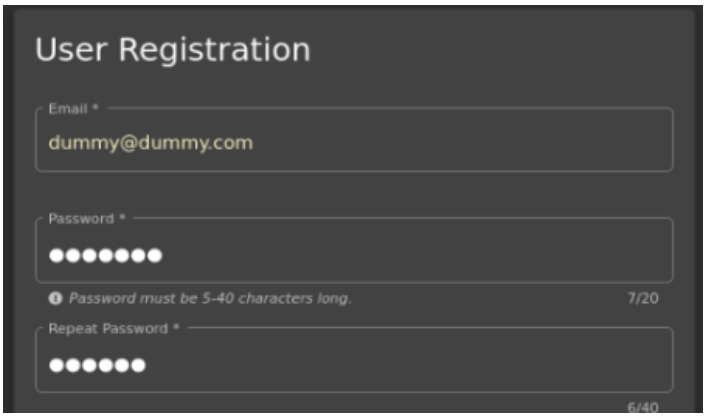
pasif. Dalam implementasinya, hal ini dapat dilakukan dengan mengunjungi website target yaitu juice-shop.herokuapp.com maupun pencarian informasi melalui media sosial dan sebagainya. Temuan yang didapatkan berupa informasi front-end dan back-end yang merupakan bersifat penting. Beberapa *tools* yang dapat digunakan dalam proses ini antara lain adalah website who.is dan wappalyzer.



Gambar 2 Tampilan Front-end Halaman dan Detilnya

B. Tahap *Scanning & Enumeration*

Tahap *Scanning & Enumeration* adalah proses mengumpulkan semua informasi yang didapat pada tahap sebelumnya, kemudian diolah untuk mencari kelemahan yang ada. Hal ini dapat dilakukan dengan menggunakan beberapa tools yang sudah tersedia dalam Kali Linux seperti Burpsuite dan Nmap[9]. Pada tahapan ini metode scanning & enumeration yang dilakukan adalah dengan mengunjungi website sebagai user. Pada saat pendaftaran pengguna baru didapatkan bahwa kolom *password* dan pengulangan *password* yang disediakan tidak mengikuti standar prinsip DRY (Don't Repeat Yourself). Di mana pengguna dapat mengganti password yang berbeda dengan repeat password pada saat munculnya error '*Passwords do not match*'.
Selain itu dengan melihat salah satu review produk penulis mendapatkan informasi email beberapa pengurus website dengan domain @juice-sh.op. Data ini dapat digunakan dalam login info yang dapat diexploit dengan SQL injection dan broken authentication.



Gambar 3 Password Field yang Tidak Sesuai dengan Prinsip DRY

Prefix DOI : 10.3785/kjst.v1i6.347

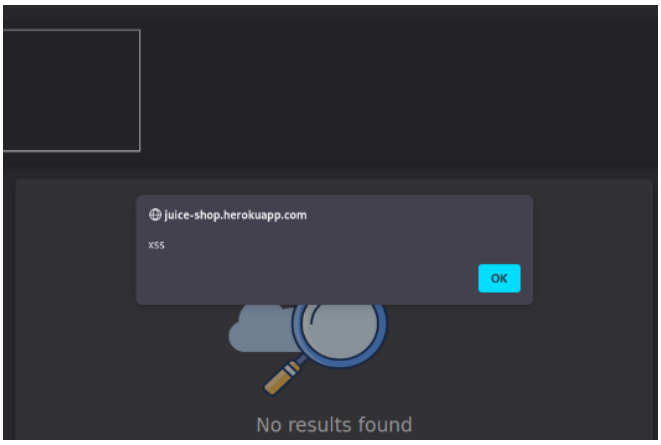
E-ISSN : 2988-1986
https://ejournal.warunayama.org/kohesi

Kohesi: Jurnal Multidisiplin Saintek
Volume 01, No. 06 2023, pp. 81-90

Prefix DOI : 10.3785/kjst.v1i6.347

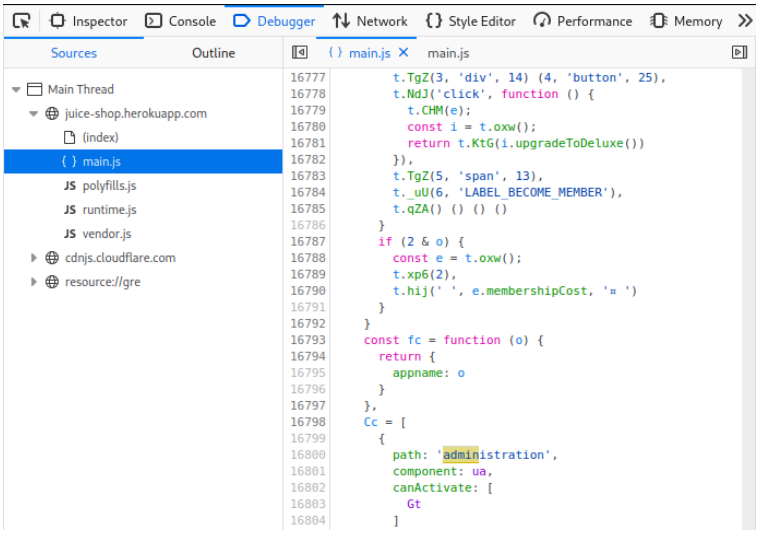
Gambar 4 Temuan email berdomain @juice-sh.op

Selanjutnya website ini juga rawan akan DOM XSS (Cross Site Scripting) di mana pada saat memberikan input code <iframe src="javascript:alert(`xss`)"> dalam *search field* akan berhasil memunculkan pop-up XSS yang artinya *vuln*/rentan terhadap XSS.



Gambar 5 Pop-up DOM XSS

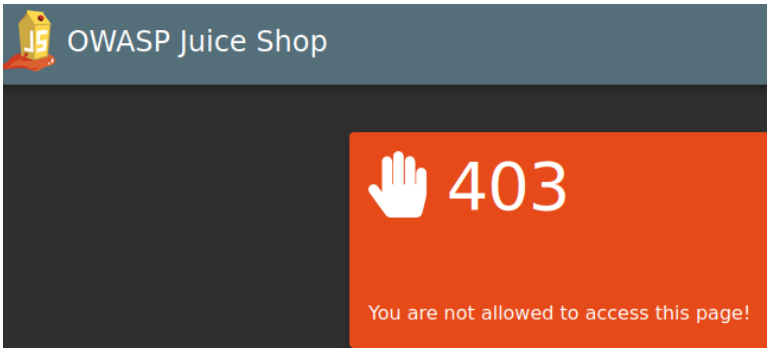
Dengan menggunakan fitur dev tools pada browser Firefox penulis dapat melihat directory



Gambar 6 Dev Tools Menampilkan Admin Directory

Prefix DOI : 10.3785/kjst.v1i6.347

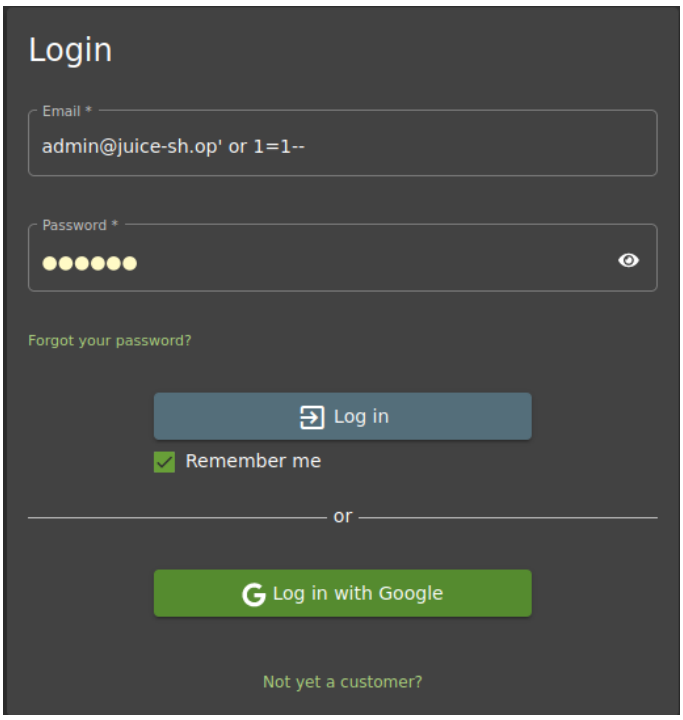
'administration' dalam main.js yang tidak dapat diakses kecuali dengan memiliki *permission admin login*.



Gambar 7 Error Code 403 Forbidden Access

C. Tahap *Gaining Access*
Pada tahap ini dilakukan eksploitasi untuk mendapatkan akses dengan menggunakan temuan yang didapat. Dengan menggunakan SQL *injection* di dalam *login form* kita dapat menggunakan *email* admin yang telah didapatkan dalam proses *scanning & enumeration* dan *password* yang asal[10]. Input SQL yang diberikan dalam *username field* adalah *email* admin dan *injection* yang sudah umum. Hal ini dapat dilakukan dengan email berdomain @juice-sh.op yang berbeda yang menyebabkan selain rentan dengan SQL *injection* website ini juga rentan dengan *broken authentication.* Dengan memiliki akses admin pentester dapat memiliki akses penuh pada *website juice shop*.

D. Tahap *Maintaining Access*
Proses ini dapat dilakukan dengan membuat *embeded* XSS *payload* ke dalam video promotion

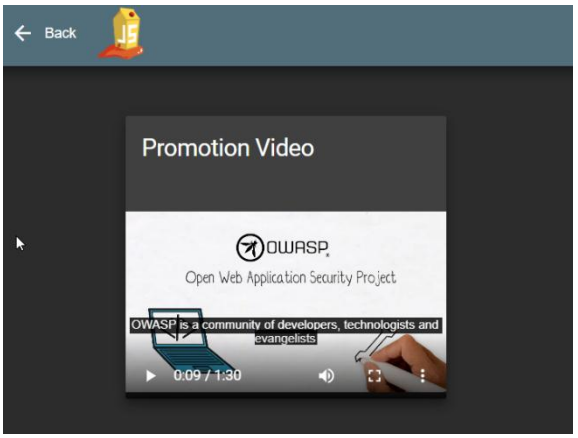


Gambar 8 Proses SQL Injection

yang berada pada assets/public/videos/owasp_promo.mp4. Dengan menggunakan kerentanan zip

Prefix DOI : 10.3785/kjst.v1i6.347

slip dapat memungkinkan kita menanam *embeded XSS payload* dengan menguunggah file zip dalam '#/complain' dan dapat terpicu dengan mengunjungi '/promotion ' namun tanpa keuntungan yang signifikan dalam mempertahankan akses dalam *website*.



Gambar 9 OWASP Promotion Video

E. Tahap Covering Tracks
Proses ini dapat dilakukan dengan menghapus jejak dalam website namun pada umumnya proses ini lebih sering dilakukan dalam proses *pentesting* terhadapa target jaringan, aplikasi mobile, dan *active directory*[11]. Pada proses pentesting *website* Juice Shop proses *covering tracks* dapat dilakukan dengan menghapus komentar yang telah ditinggalkan dalam review produk, keranjang belanja, dan sebagainya. Tujuannya adalah untuk menghilangkan jejak sedalam mungkin sehingga pentester sulit untuk dilacak.

4. KESIMPULAN DAN SARAN

4.1 KESIMPULAN

1. Dengan melakukan pengujian menggunakan metode *penetration testing* berbasis OWASP TOP 10 pada *website Juice Shop* dapat diidentifikasi temuan kerentanan yang dapat berpengaruh pada keamanan web. Pengujian dilakukan sesuai dengan etika dalam ethical hacking. Adapun temuan yang didapat menunjukkan bahwa terdapat celah keamanan seperti XSS, SQL *injection*, dan *broken authentiaction*. Celah keamanan tersebut dapat menyebabkan serangan yang sangat berpengaruh terhadap website. Adapun temuan berupa information disclosure yang sangat perlu diperhatikan karena ditemukan beberapa email berdomain juice-sh.op dan email milik admin dan staff website. Pada tahap *gaining access* menggunakan eksploitasi dengan SQL *injection* dengan kode yang cukup umum didapatkan *admin acces* secara penuh pada *website Juice Shop*. SQL *injection* yang sama juga dapat dilakukan dengan *email* berdomain @juice-sh.op. Hal ini dapat dikategorikan dalam *vulnerability*/kerentanan *broken authentication*. Besar kemungkinan juga bahwa *email* admin@juice-sh.op berada pada *email* dalam SQL *database* dengan urutan paling atas/pertama.
2. Berdasarkan temuan yang telah didapat dalam pengujian ini, beberapa langkah pencegahan secara preventif yang dapat dilakukan terhadap potensi serangan pada web juice shop adalah dengan menerapkan *information disclosure* yang sesuai dengan C dalam CIA TRIAD. CIA TRIAD sendiri merupakan confidentiality, integrity, dan availibity. Adapun sanitasi dalam batasan input character yang diperbolehkan terhadap input field terutama pada login form. Oleh karena itu pemeliharaan dan perhatian terhadap web yang dikelola secara berkala merupakan salah satu faktor yang penting dalam keamanan web yang terus berkembang.

4.2 SARAN

Setelah melalui rangkain proses dalam *pentesting* yang telah dimulai dari tahap information

Prefix DOI : 10.3785/kjst.v1i6.347

gathering hingga *covering tracks* dapat diketahui bahwa *information disclosure* merupakan informasi awal yang sensitif untuk kemudian dapat digunakan dalam proses eksploitasi. Metode penetration testing dengan berbasis pada OWASP TOP 10 masih dapat ditingkatkan lagi dengan pengujian yang lebih mendalam dan agresif. Penggunaan metode penyerangan dan *tools* pendukung juga dapat memungkinkan untuk memperoleh hasil uji yang lebih detail.

5. DAFTAR RUJUKAN

[1] A. Bastian, H. Sujadi and L. Abror, "ANALISIS KEAMANAN APLIKASI DATA POKOK PENDIDIKAN (DAPODIK) MENGGUNAKAN PENETRATION TESTING DAN SQL INJECTION," INFOTECH Journal, vol. 6, no. 2, pp. 65-70, 2020.

[2] S. Hidayatulloh and D. Saptadiaji, "Penetration Testing pada Website Universitas ARS Menggunakan Open Web Application Security Project (OWASP)," Jurnal Algoritma, vol. 18, no. 1, pp. 77-86, 2021.

[3] O. Ojagbule, H. Wimmer and R. J. Haddad, "Vulnerability Analysis of Content Management Systems to SQL Injection Using SQLMAP," SoutheastCon, Vols. 978-1-5386-6133-8, no. 18, pp. 1-7, 2018.

[4] Fauzan, Rum. "PENGUJIAN KEAMANAN SISTEM INFORMASI AKADEMIK MENGGUNAKAN METODE PENETRATION TESTING (Studi Kasus: Institut Pertanian Stiper Yogyakarta)." PhD diss., University of Technology Yogyakarta, 2019.

[5] Sahren, Sahren, Ruri Ashari Dalimuthe, and Muhammad Amin. "Penetration Testing Untuk Deteksi Vulnerability Sistem Informasi Kampus." Prosiding Seminar Nasional Riset Information Science (SENARIS), vol. 1, pp. 994-1001. 2019.

[6] Fauzan, F. Y., & Syukhri, S. (2021). Analisis Metode Web Security PTES (Penetration Testing Execution And Standart) Pada Aplikasi E-Learning Universitas Negeri Padang. Voteteknika (Vocational Teknik Elektronika dan Informatika), 9(2), 105-111.

[7] Wardaya, M. S. S. Penetration testing terhadap website asosiasi pekerja professional informasi sekolah Indonesia (Bachelor's thesis, Fakultas Sains dan Teknologi Universitas Islam Negeri Syarif Hidayatullah Jakarta).

[8] Sholeh, A. N., & Wardaya, M. S. S. (2019). ANALISIS DAN PENGUJIAN KERENTANAN SISTEM INFORMASI PERPUSTAKAAN. Jurnal Mandiri: Ilmu Pengetahuan, Seni, dan Teknologi, 3(1), 116-131.

[9] Dewanto, A. P. (2018). PENETRATION TESTING PADA DOMAIN UII. AC. ID MENGGUNAKAN OWASP 10.

[10] Fachri, F., Fadlil, A., & Riadi, I. (2021). Analisis Keamanan Webserver Menggunakan Penetration Test. Jurnal Informatika, 8(2), 183-190.

[11] Nagpure, S., & Kurkure, S. (2017, August). Vulnerability assessment and penetration testing of web application. In 2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA) (pp. 1-6). IEEE.

Prefix DOI : 10.3785/kjst.v1i6.347