PENETRATION TEST REPORT

SYSTEM SECURITY ASSESSMENT

CONFIDENTIAL

Daftar Isi

Laporan Penetration Testing

Lembar Persetujuan

	NAMA	POSISI	TANDA TANGAN	TANGGAL
DISIAPKAN OLEH	Satria Pamungkas	Pentester	TTD	13-11-2025
DISETUJUI OLEH				

Catatan Perubahan

Tanggal	Versi	Penulis	Deskripsi
13 November	1.0	Satria Pamungkas	Laporan Pentesting

1.Latar Belakang

Aplikasi berbasis *website* saat ini menjadi salah satu aset penting bagi kehidupan suatu bisnis, hal ini membuat perusahaan untuk melakukan transformasi untuk melakukan digitalisasi terhadap jasa atau barang yang mereka jual.

Aplikasi berbasis *website* saat ini sudah sangat berkembang pesat dari sisi pembuatan hingga sisi keamanan, namun disisi lain ancaman terhadap aplikasi juga ikut meningkat. Ancaman ini yang menjadi suatu momok mengerikan bagi pemilik bisnis, karena ancaman yang ada dapat mengakibatkan pencurian data penting bagi perusahaan, kerugian dari sisi finansial perusahaan, serta menurunnya reputasi dari bisnis tersebut dari klien mereka.

Penetration testing merupakan suatu metode untuk melakukan simulasi serangan terhadap suatu aplikasi yang dilakukan secara etis dan terkontrol. Kegiatan ini bertujuan untuk menemukan kerentanan pada aplikasi sebelum penyerang menemukan kerentanan dan memanfaatkan kerentanan tersebut, sehingga ancaman serangan dapat diminimalisir seminim mungkin.

Aplikasi yang akan dilakukan pengujian adalah owasp juice shop (https://juice-shop.herokuapp.com/#/) yang merupakan aplikasi berbasis *website* yang dibuat oleh owasp untuk tujuan edukasi dalam melakukan penetration testing. *Website* ini menggambarkan toko yang menjual produk seperti produk buah dan jus buah.

2.Metodologi

Pengujian pada *website* owasp *juice shop* ini menggunakan metode *black box*, yang mana pentester tidak diberikan informasi secara detail mengenai target yang akan diuji. Metodologi yang dilakukan pada pengujian ini adalah OWASP (*Open Web Application Security Project*). Setiap temuan dari hasil pengujian aplikasi owasp *juice shop* akan dianalisis menggunakan standar CVSS 3.1 untuk menentukan prioritas perbaikan yang harus diutamakan.

3.Scope

Ruang lingkup pada pengujian penetration testing kali ini berada pada website https://juice-shop.herokuapp.com/# hanya pada bagian fitur dari search bar dan juga login form di lingkungan production.

4. Ringkasan Eksekutif

Aplikasi juice shop yang berbasis website memiliki kerentanan SQL injection pada halaman login. Kerentanan ini dapat dimanfaatkan oleh penyerang untuk melakukan vertical privilege escalation terhadap akun admin dan menyebabkan kerusakan yang lebih parah. Kerentanan ini harus segera diatasi dengan cara menggunakan prepared statement dengan query parameter, melakukan validasi input, dan menggunakan stored procedures yang dikonfigurasi dengan benar.

Kerentanan berikutnya yang ditemukan adalah kerentanan XSS (Cross Site Scripting) yang dapat digunakan penyerang untuk melakukan pencurian data yang bersifat sensitif seperti data pengguna. Resiko dari serangan ini bisa menurunkan reputasi perusahaan bagi klien apabila data mereka berhasil dicuri. Kerentanan ini dapat diatasi menggunakan metode menghindari penggunaan sink yang berbahaya, melakukan context sensitive encoding terhadap data, menggunakan HTML sanitation dan memperketat validasi input.

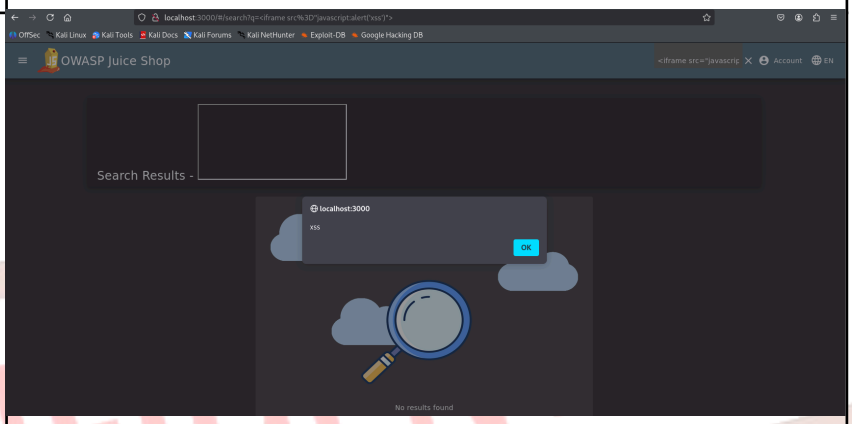
5.Temuan

Setelah dilakukan *penetration testing* terhadap *website* https://juice-shop.herokuapp.com/#, terdapat 2 temuan kerentanan pada *website* yakni SQL injection dan XSS (DOM). Prioritas utama dalam melakukan penanganan disarankan dimulai dari kerentanan dengan tingkat yang tinggi terlebih dulu.

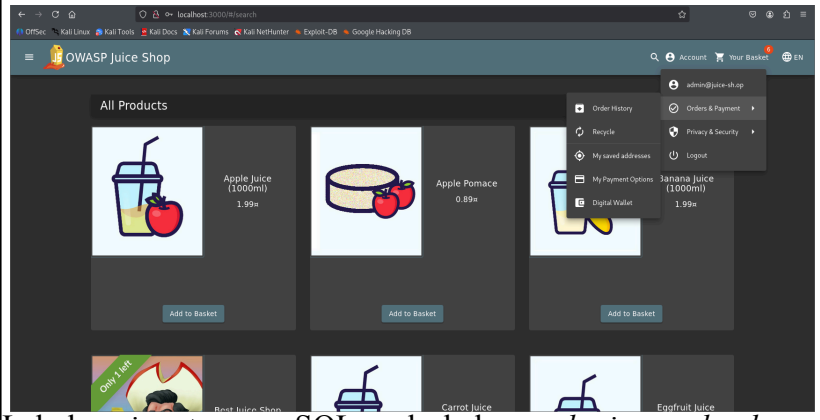
No	Name	Severity	Founded	Status
1	SQL Injection	**High**	13-11-25	Open
2	XSS (DOM)	**Medium**	13-11-25	Open

6.Detail Temuan

Berikut merupakan detail dari hasil temuan kegiatan *penetration testing* yang telah dilakukan sebelumnya pada *website.*

1. XSS (DOM)	
Severity	Medium (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)
Description	Penyerang menemukan kerentanan XSS (DOM), dimana penyerang dapat meng-injeksikan javascript berbahaya pada aplikasi yang dapat mengakibatkan pengambilan informasi sensitif seperti *cookie* dan informasi lainnya.
Hosts Affected	https://demo.owasp-juice.shop/#/
Endpoint Affected	1. /search - Parameter: q
POC	 Lakukan injeksi *form search* dengan parameter q dengan *payload* “<iframe src="javascript:alert(`xss`)">” kita dapat melihat *script* yang di-injeksikan dapat di render oleh aplikasi diproses menjadi sebuah perintah untuk memunculkan *alert*.
Recommendation	● Hindari penggunaan fungsi sink berbahaya ● Lakukan context sensitive encoding terhadap data ● Gunakan HTML Sanitization ● Perketat validasi input

2. SQL Injection	
Severity	High (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:N)
Description	Penyerang menemukan kerentanan SQL injection di *form login* website. Penyerang dapat meng-*input query* SQL untuk melakukan *vertical escalation privilege*.
Hosts Affected	https://demo.owasp-juice.shop/#/login
Endpoint Affected	1. /login - Parameter: -

POC	 Lakukan *input query* SQL pada halaman *login*, *payload* yang digunakan untuk *email* diisi dengan ‘ OR TRUE– dan password diisi dengan bebas. Maka dapat dilihat akun admin berhasil diakses.
Recommendation	• Gunakan prepared statement dengan query parameter. • Lakukan validasi input. • Gunakan stored procedures yang dikonfigurasi dengan benar.

7. Referensi

Berdasarkan hasil temuan dari kegiatan *penetration testing* yang telah dilakukan, berikut merupakan referensi yang dapat digunakan untuk melakukan remediasi atau perbaikan pada aplikasi website.

- DOM based XSS Prevention - OWASP Cheat Sheet Series
- SQL Injection Prevention - OWASP Cheat Sheet Series