Aminudin Follow
Jul 26, 2022 · 3 min read

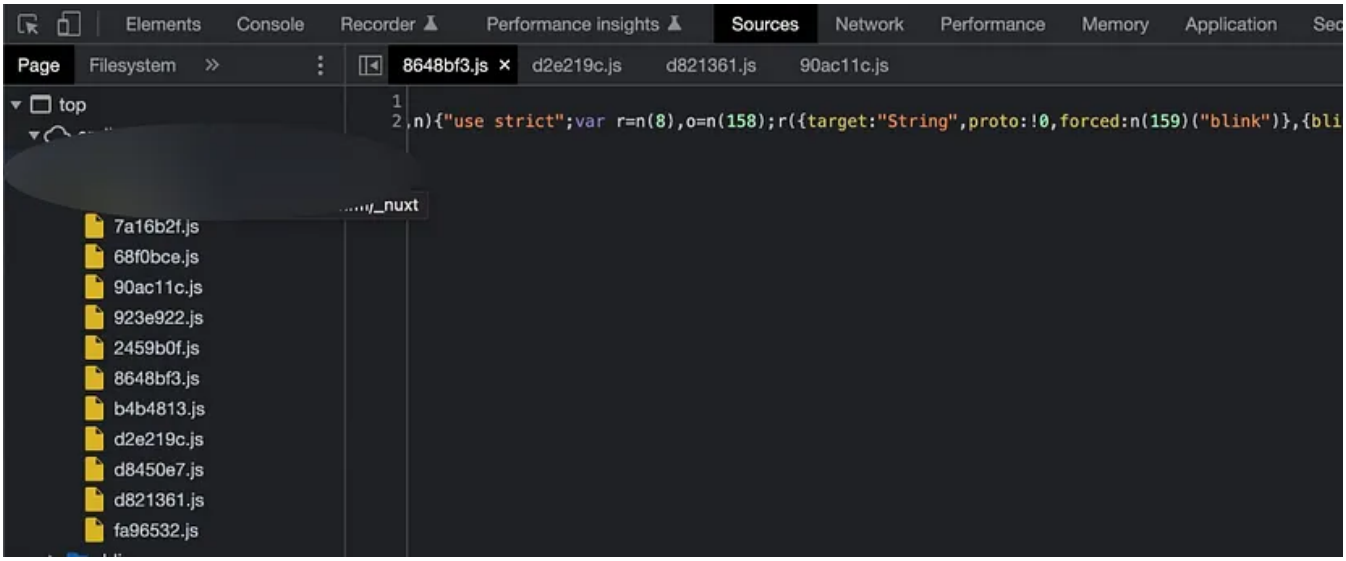
Sensitive Data Exposure: Mengambil alih semua akun, akunmu = akunku.

> *Sensitive Data Exposure vulnerabilities can occur when a web application does not adequately protect sensitive information from being disclosed to attackers. This can include information such as credit card data, medical history, session tokens, or other authentication credentials. ~ Port Swigger*

Halo semuanya,

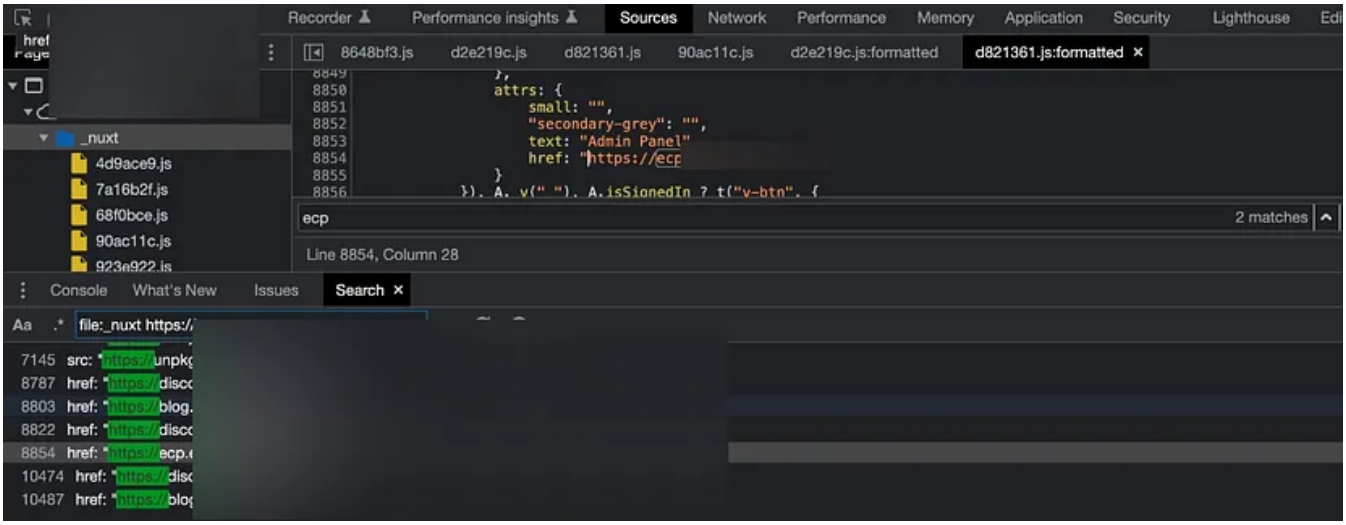
Disini saya akan membahas bagaimana cara saya mengambil alih semua data akun baik **Database** sampai dengan **API Token Digitalocean** pada sebuah website **NFT Music Marketplace.** Pertama pekerjaan saya yang utama bukan **BugBounty hunting**, tapi disini saya hanya kadang suka iseng mencari bug/pentesting diwaktu luang saya. Jadi, disini saya hanya pemula dan maaf jika ada salah salah kata.

Ok langsung saja, untuk hal pertama yang saya lakukan disini saya iseng iseng melakukan **inspect element** dan langsung menuju ke tab **sources**

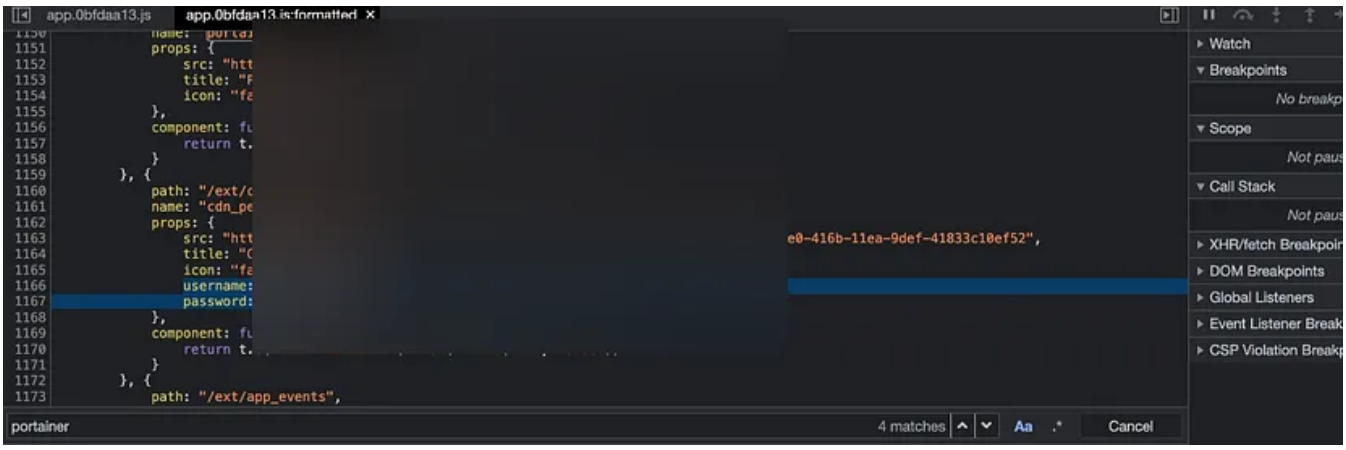


Dibagian **Sources** ini saya hanya fokus kedalam script javascript, karena yang biasanya ada data **sensitive** saya pikir dibagian javascriptnya saja. Pertama yang saya pikirkan adalah mencari kata kunci yang sekiranya adalah **variable / value** dari **sensitive** data seperti **username:, password:** atau jika mencari **halaman admin dll** bisa search dengan kata kunci **http://, https://.**

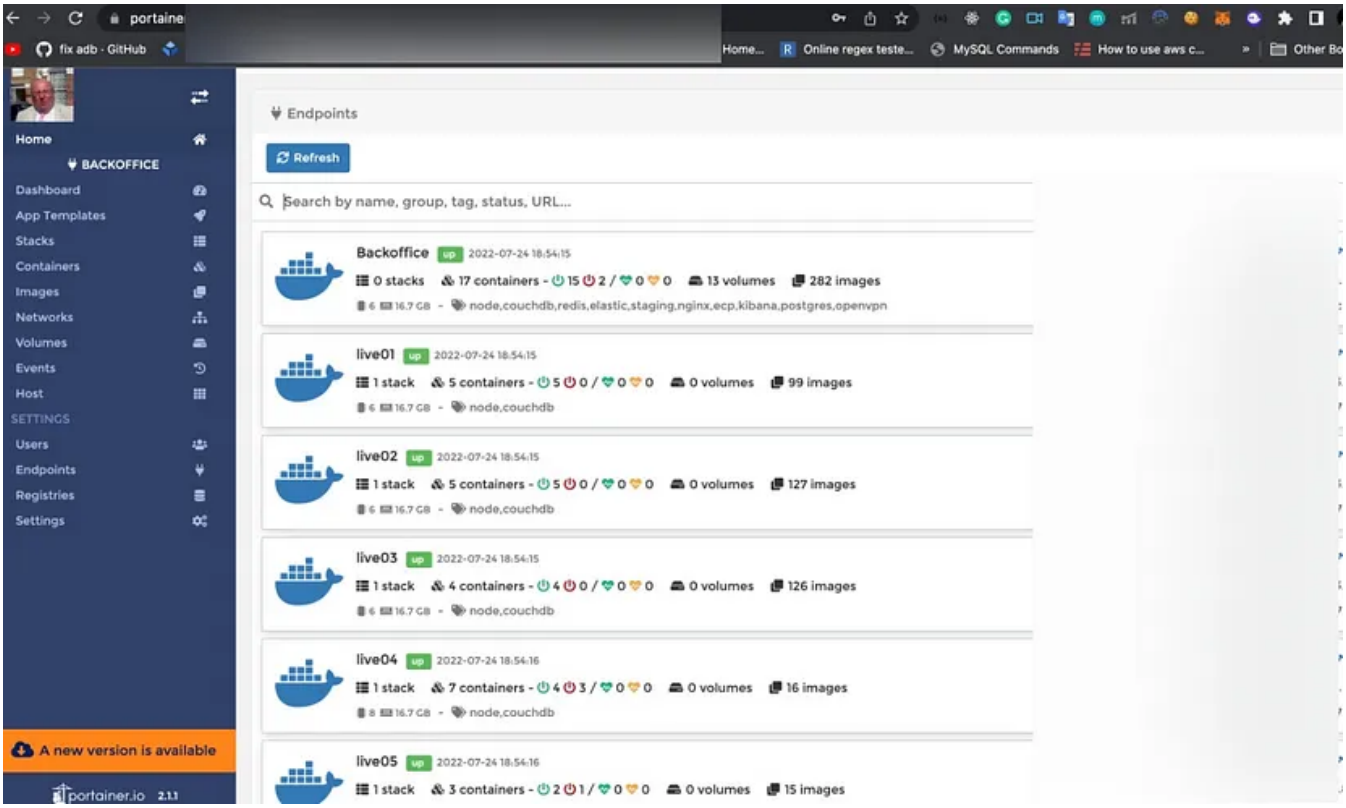
Nah, untuk case disini saya pertama cari di home websitenya terlebih dahulu dengan kata kunci seperti **username, password dll** tapi tidak ketemu, nah tapi ketika saya coba search dengan **https://** ada yang memancing mata saya



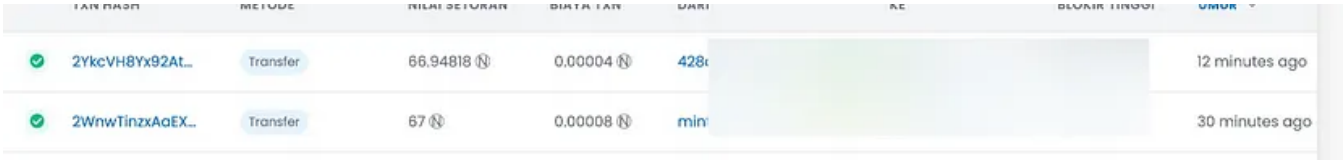
Setelah saya coba kunjungi dan boom!!! yaps bener ada halaman login untuk admin. Tapi, sampai disini bingung, mau saya apakan halaman login ini ? sedangkan saya tidak punya username dan passwordnya, **disitu saya tidak berpikir untuk coba membypass halaman login** tersebut tapi saya langsung coba untuk **inspect element** lagi dan pergi ke **sources** dengan kata kunci **username:, password:.** Dan booom!!!

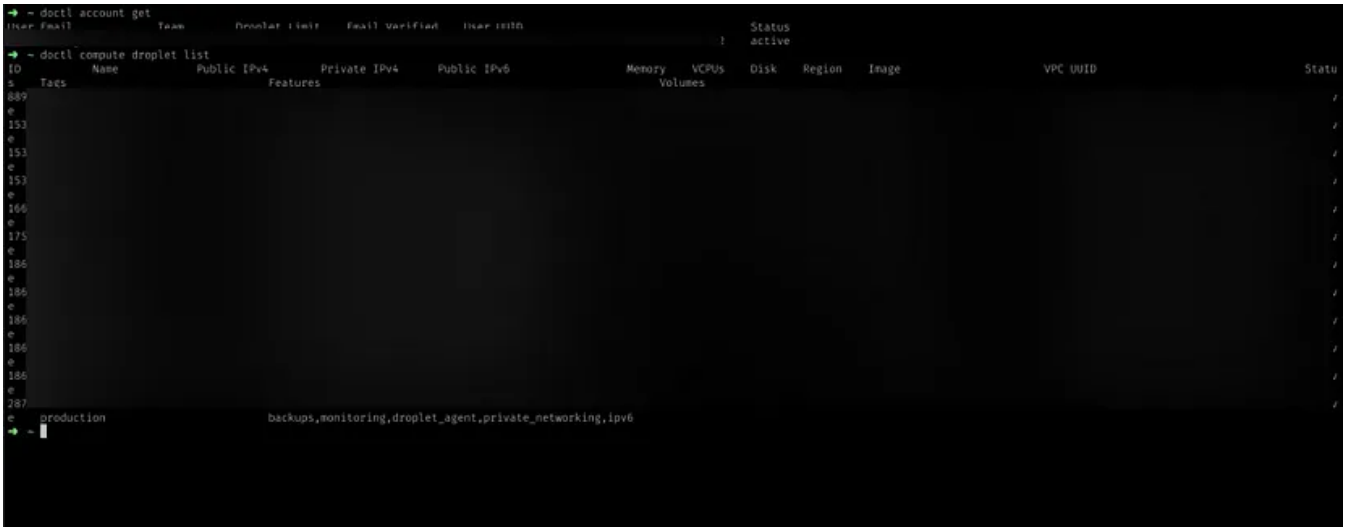


Saya dapetin source dari **kibana, couchdb dll** dan sudah tersedia **username dan passwordnya**, dari situ saya coba login ke **portainernya** yang dimana isinya adalah untuk memanage container dari semua isi websitenya dan terdapat env envnya :



Dari situ merembet saya bisa dapetin **Private Key Near account, git account** dan yang paling sensitive adalah **API Token Digitalocean**, dengan itu saya bisa memanage **droplet, projects** semuanya yang ada di **digitalocean** milik mereka :



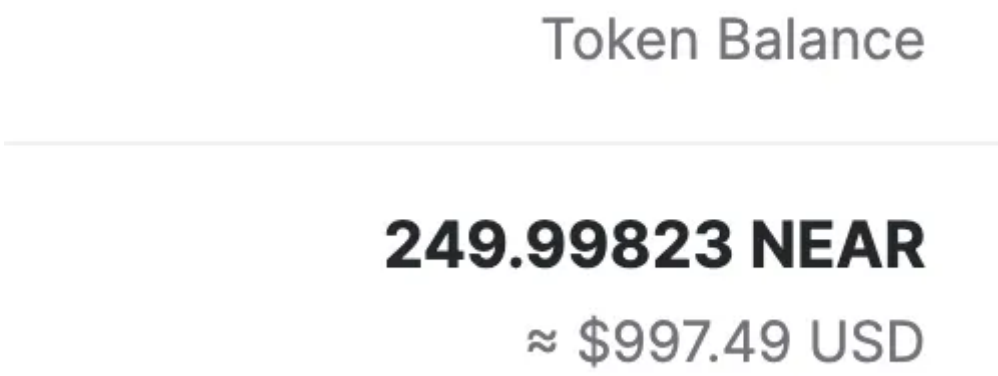


Timeline :

~ 24 July 2022 : Bug Reported

~ 24 July 2022 : Confirmed and he said I will be rewarded with 250 NEAR ($1080 rate at 24 july) after mitigations complete

~ 26 July 2022 : Bug Fixed & Reward Landed



Bug Bounty Bug Bounty Writeup Pentest Pentesting JavaScript