Muhamad Hidayat Follow
Feb 14 · 3 min read

OWASP API Security (Offensive Prespective) : Security Misconfiguration #7

Assalamualaikum Wr. Wb

Apa itu Security Misconfiguration

Sederhananya adalah kondisi gagalnya sistem menerapkan kontrol keamanan atau best practice baik pada aplikasi, infrastruktur atau komponen software.

Penyebabnya bisa banyak hal, mengingat banyaknya configurasi di tiap-tiap komponen software yang menjadikan Security Misconfigurasi ini menjadi Trend TOP 10 vulnerability menurut OWASP.

Berikut hal-hal yang sering terjadi pada software yang menyebabkan terjadinya Security Misconfiguration:

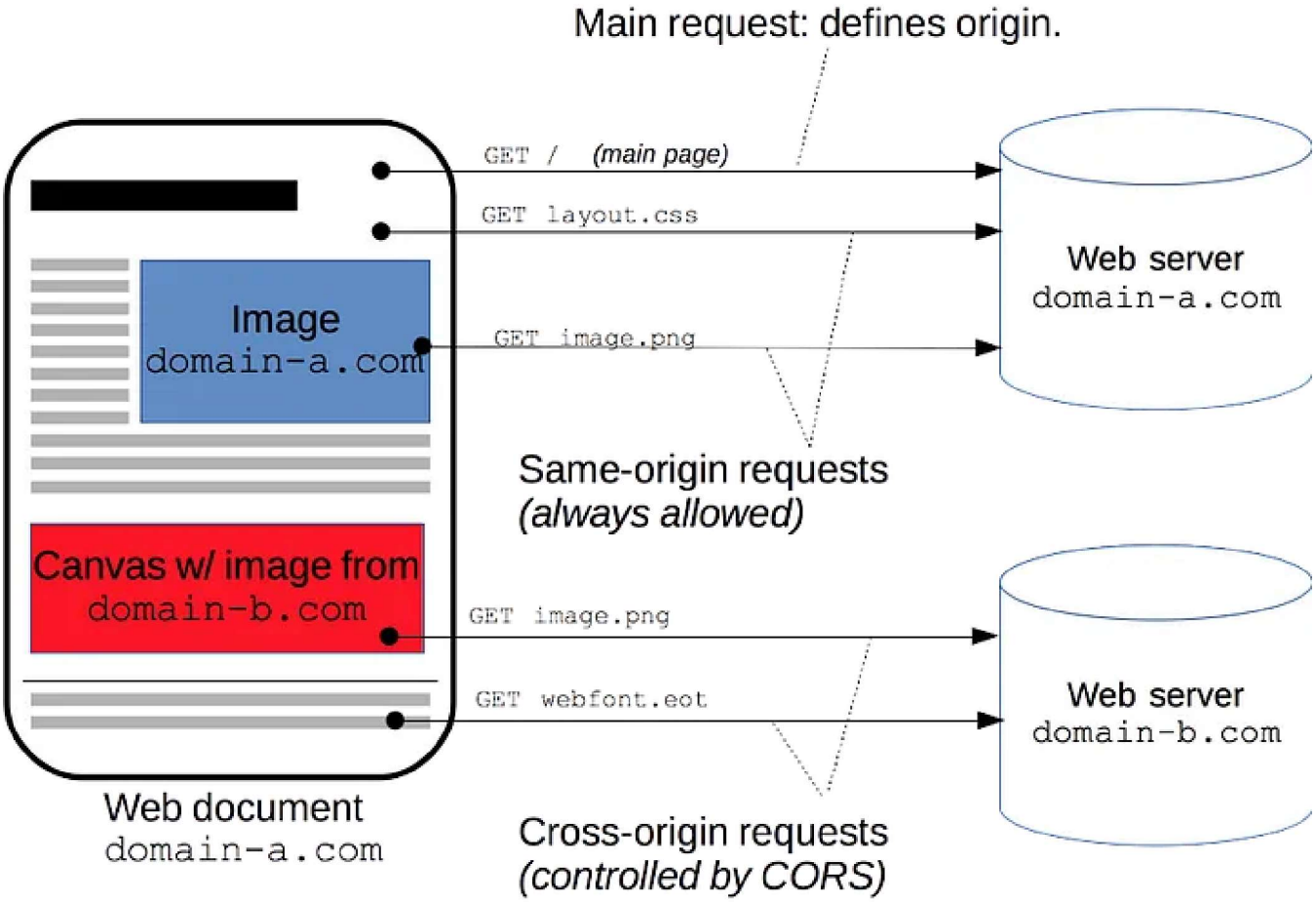
- Cross-Origin Resource Sharing (CORS) policy.
- Improper handling of errors.
- Improperly Configured permissions on cloud services.
- The latest security patches are missing.

Di atas adalah beberapa contoh yang sering terjadi terkait Security Misconfiguration.

Berikut salah satu contoh penyerangan terkait Security Misconfigurasi yang umum terjadi pada REST API.

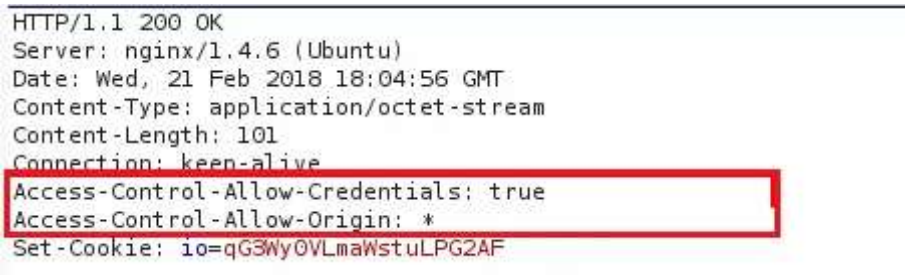
Cross-Origin Resource Sharing (CORS) policy.

Guna CORS pada REST API sederhananya agar salah satu fitur keamanan pada browser melakukan pembatasan antar origin, Origin yang dimaksud adalah merujuk pada asal domain **scheme://hostname:port (http://domain-b.com/)** pemilik sumber assets.



Cross-Origin Resource Sharing (CORS) — HTTP | MDN (mozilla.org)

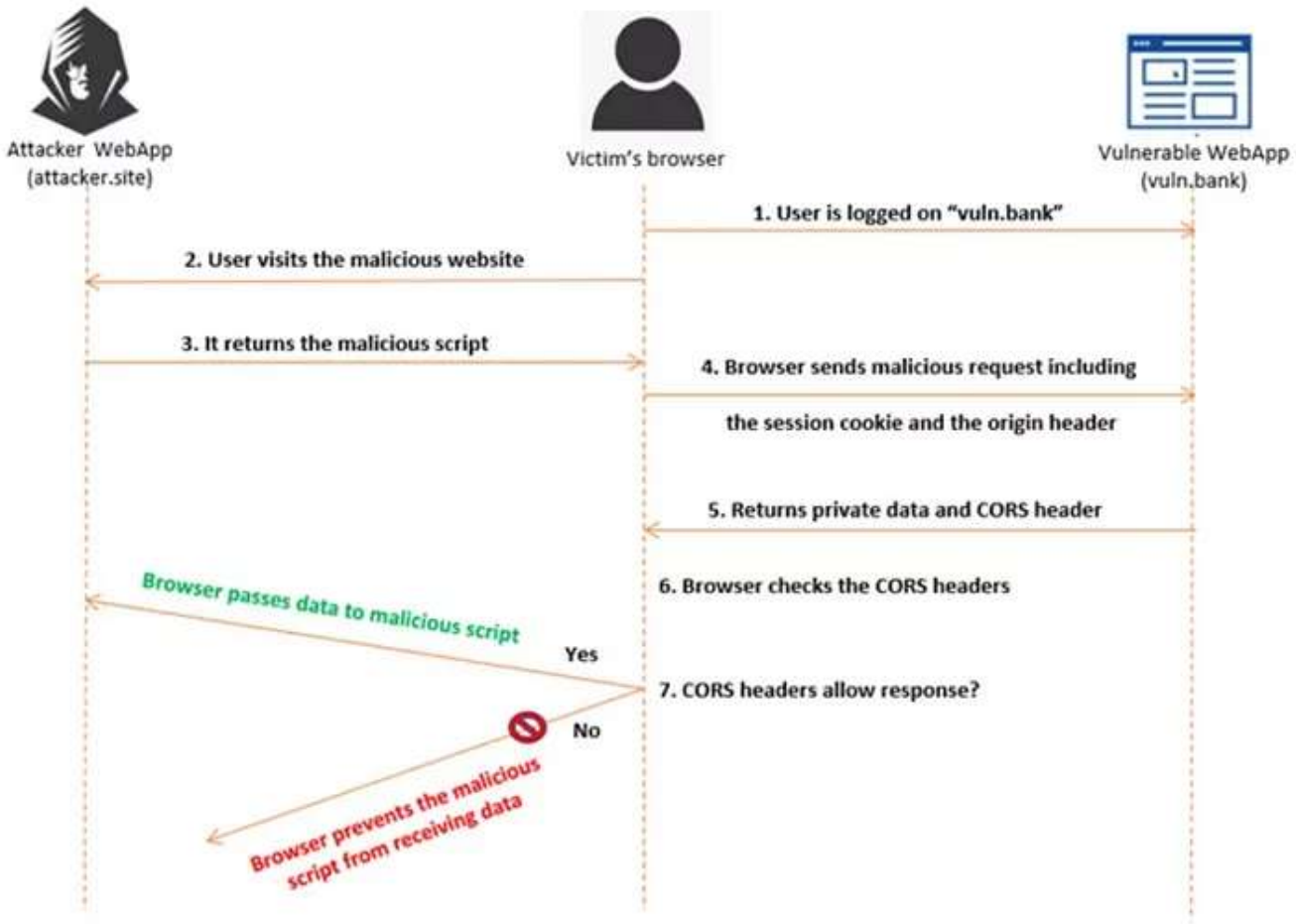
Pada ilustrasi di atas, **domain-a.com** mencoba melakukan akses pada resource atau asset yang dimiliki oleh **domain-b.com**. Apabila CORS Policy pada resource **domain-b.com** tidak di configurasi agar mengizinkan domain-a.com untuk mengakses resourcenya. Maka **domain-a.com** akan mendapatkan alert dari security browser terkait policy Same-Origin yaitu salah satu kebijakan yang hanya mengizinkan Origin satu hanya bisa mengakses origin yang sama dalam hal ini **domain-b.com** hanya bisa diakses **domain-b.com** saja.



www.we45.com

Kondisi seperti diatas adalah salah satu kondisi dimana **CORS Policy** mengalami salah satu Security Misconfiguration. yaitu ketika header CORS **“Access-Control-Allow-Origin”** diatur ke tanda bintang (“*”) atau domain yang tidak dapat dipercaya.

Ini akan memberikan izin akses domain lain ke semua situs web atau domain yang meminta sumber daya, termasuk domain yang tidak diizinkan, yang dapat mengakibatkan penyalahgunaan atau serangan keamanan yang disebabkan oleh akses domain yang tidak sah.



Misconfigured Cross-Origin Resource Sharing (CORS) Risk (varutra.com)

Salah satu contoh serangan terkait CORS Misconfiguration adalah seperti pada flow diatas. Threat Actor (Attacker) membuat sebuah web malicious berisi request endpoint private data dari web vuln.bank (http://vuln.bank/private/data).

Setelah user melakukan login pada website resmi vuln.bank, User secara sadar mengunjungi Malicious Website yang dibuat oleh attacker di browser yang sama dengan browser yang menyimpan session login vuln.bank sebelumnya.

Secara otomatis website tersebut melakukan request malicious ke endpoint milik vuln.bank atas browser yang dimiliki oleh User, Alhasil akan mengirimkan kembali response pada vuln.bank ke malicious website milik attacker, yang mana response tersebut berisi private data yang direquest atas browser yang telah berisi session milik user.

Bagaimana cara pencegahanya?

- Melakukan limitasi akses terhadap Cross-Origin hanya kepada domain yang di percaya saja.

Security Misconfiguration Owasp Top 10 Api Security Exploit Development