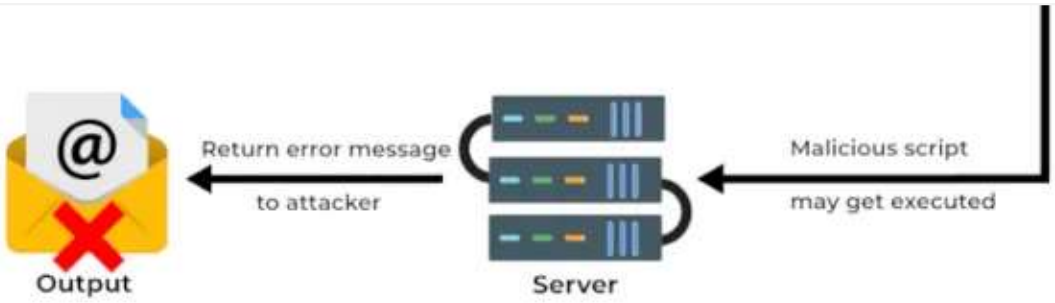
Muhamad Hidayat Follow
Feb 19 · 2 min read

OWASP API Security (Offensive Prespective) : Injection #8

Photo by Diana Polekhina on Unsplash

Assalamualaikum Wr Wb.

Apa itu Injection?



https://beaglesecurity.com/blog/vulnerability/remote-code-execution.html

Injection Flaw adalah kondisi dimana sebuah sistem / program memproses sebuah data yang tidak valid, yang mengakibatkan attacker dapat menginputkan kode tertentu kepada program lalu kode tersebut akan membuat program menjalankan perintah yang salah.

Lengkapnya ada di article saya terkait OWASP top 10 sebelumnya:

Owasp Top 10 Series — A3 (Injection Flaw) [Indonesia] | by Muhamad Hidayat | Medium

VulnLab SQL Injection — Dynamic Application Security Testing #3 | by Muhamad Hidayat | Medium

VulnLab Command Injection (Linux, PHP) — Dynamic Application Security Testing #5 | by Muhamad Hidayat | Medium

VulnLab XSS Reflected GET & POST (Basic Reflected) — Dynamic Application Security Testing #2 | by Muhamad Hidayat | Medium

Kurang lebih sama, Injection flaw yang terdapat pada web dengan yang ada pada REST API.

Meskipun serangan Injection bisa terjadi pada kedua jenis aplikasi tersebut, ada beberapa perbedaan dalam cara serangan Injection dilakukan pada aplikasi web biasa dan REST API. Perbedaan tersebut antara lain:

- **Sumber daya yang diserang**: Pa[illegible]eb biasa, serangan Injection umumnya ditujukan pada parameter URL, form input, atau cookie. Sedangkan pada REST API, serangan Injection lebih sering terjadi pada parameter URL dan body request.
- **Format input:** REST API menggunakan format data yang lebih terstruktur, seperti JSON atau XML, sedangkan aplikasi web biasa cenderung menggunakan format data yang lebih longgar dan tidak terstruktur, seperti teks mentah atau HTML. Karena format data yang terstruktur memungkinkan pengembang untuk menentukan jenis dan tipe data yang diharapkan, maka serangan Injection pada REST API dapat lebih terukur dan terdokumentasi.
- **Metode request:** Pada aplikasi web biasa, umumnya menggunakan metode GET atau POST, sedangkan pada REST API, selain GET dan POST, juga terdapat metode HTTP lainnya seperti PUT, DELETE, dan PATCH. Serangan Injection pada metode request HTTP yang berbeda dapat memerlukan teknik yang berbeda pula.
- **Response format:** REST API memberikan respons dalam format terstruktur seperti JSON atau XML. Hal ini dapat memberikan petunjuk tentang bagaimana input dari serangan Injection dapat dihasilkan dalam format yang diinginkan oleh penyerang. Sedangkan aplikasi web biasa dapat memberikan respons yang lebih tidak terstruktur, seperti halaman HTML atau pesan kesalahan mentah.

Namun, meskipun terdapat perbedaan tersebut, prinsip dasar serangan Injection tetap sama, yaitu dengan memasukkan kode berbahaya ke dalam input aplikasi untuk mencuri data atau mengambil alih kontrol dari sistem tersebut. Oleh karena itu, penting bagi pengembang untuk melindungi aplikasi mereka dari serangan Injection, baik pada aplikasi web biasa maupun REST API.

Owasp Top 10 Injection Xml Json Web Vulnerabilities