Back end vulnerabilities

Thursday, January 18, 2024 8:36 PM

Common web vulnerabilities

if no vulns found in public-facing web app then we can find some manually usually due to poor configurations

Broken authentication/Access control

most common and dangerous

Broken authentication - vulnerabilities that allow attackers to bypass auth functions

Broken access control - access pages and features that you shouldn't have access to

Malicious file upload

Malicious file upload

uploading malicious scripts

can bypass checks by doing things like:

shell.php.jpg

Command injection

many web apps perform local OS commands to perform processes

ex: install plugin by doing OS command

SQLi

app executes SQL query from user input