ThoughtWorks®

ELEVATION OF PRIVILEGE

Can an unprivileged user gain more access to the system than they should have? Elevation of privilege attacks are possible because authorisation boundaries are missing or inadequate.

An example of elevation of privilege is where a user can manipulate the URL string to gain access to sensitive records they should not be able to see.

KEY CONCEPTS:

- Authorisation
- Isolation
- Blast radius
- Remote Code Execution

Known vulnerabilities

- A known vulnerability in infrastructure component is exploited due to failure to apply patches in production
- A known vulnerability in application component is exploited due failure to apply patching in production

Lack of isolation in architecture

- Service which do not need to be exposed to Internet are
- Possible to escalate privilege from another system
- Possible to mount attack on other system components via network

Lack of hardening of infrastructure

- Developer mode tools or default admin credentials are enabled
- Unnecessary services exposed by underlying infrastructure
- Able to escalate privilege via cloud vendor side channel attack

Absence of authorisation in web UI

- Failure to check authorisation to more sensitive resources
- Fails to prevent clickjacking
- Lack of Client Security Policy (CSP) configuration allows loading of untrusted resources

Implementation weakness

- A security enforcing function, such as authentication, authorisation or session management has been coded from scratch

And what else?

ThoughtWorks®

thoughtworks.com