

Approach that Integrates security practices in Devops. ← Devsecops

Devsecops ensures that security is taken care when we are deploying the projects.

- ✓✓ ① SAST (static application security testing)
- ✓✓ ② DAST (Dynamic application security testing)
- ✓✓ ③ DRCD model (Damage, Reproducibility, Exploitability, Discoverability)

DRED



app

Security risk assessment framework
which can evaluate & prioritise vulnerabilities
in web app -

It helps security teams quantify risks
systematically, allowing them to address
the most critical threats first

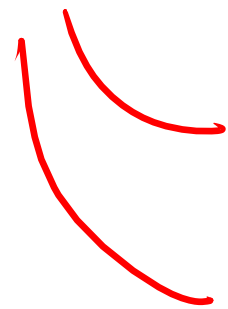
DREAD
model

Security manager

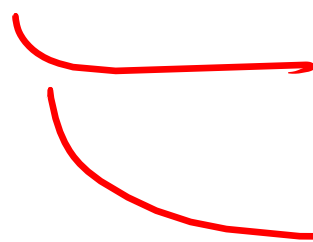
Bank

- ① Damage Potential (D) — Low damage → A minor theft
High damage → Steal million
- ② Reproducibility (R) ÷ How easy is to repeat the task?
Low reproducibility →
High

③ Exploitability (E) → How easy is to carry out the attack?

 ~~Low~~ Easy to exploit
Hard to exploit

④ Affected user (A) → How many people would be Impacted?

 Low Impact ;
High Impact

5) Discoverability (D) = How easy is it for attackers to find the weakness?

High discoverable
Low discoverable

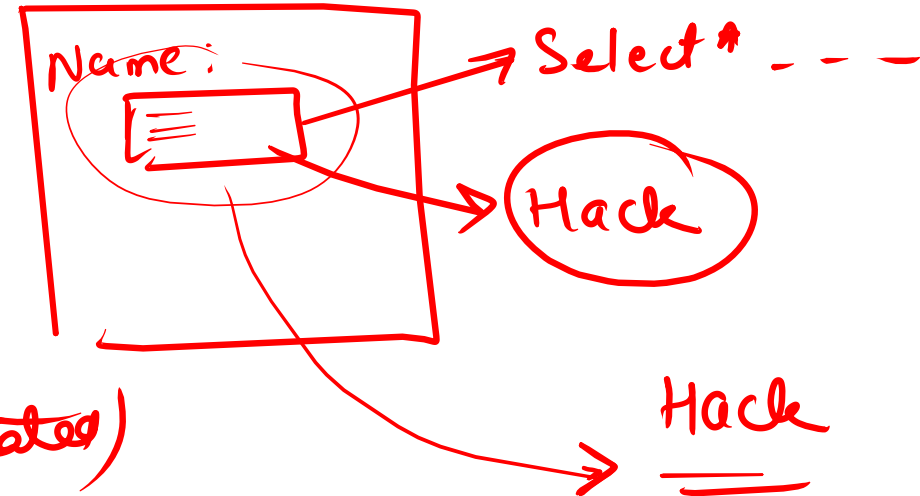
(1-10)
↑ Low ↓ High

~~10~~

$$\text{DRCAD Score} = \frac{(D + R + E + A + I)}{5}$$

SQL injection

Login



- ① Damage Potential $\rightarrow 9$ (leads to data exposure)
- ② Reproducibility $\rightarrow 10$ (can be easily repeated)
- ③ Exploitability $\rightarrow 8$ (SQL injection tools exist)
- ④ Affected user $\rightarrow 9$ (potentially all user)
- ⑤ Discoverability $\rightarrow 7$ (Moderate knowledge required)

$$\text{DREID} \rightarrow \frac{9 + 10 + 8 + 9 + 7}{5} = \underline{\underline{8.6}}$$