# Euler Finance Exploit (2023)

**Definition:** Flash loan + donate function abuse.

**Example:** ~$197M drained; partially recovered.

**Cause:** Missing reentrancy protection.

**Prevention:** Use ReentrancyGuard and access modifiers.

# TempleDAO Hack (2022)

**Definition:** Misconfigured role enabled unauthorized withdrawal.

**Example:** ~$2.3M stolen from staking vault.

**Cause:** Insecure access control.

**Prevention:** RBAC and privileged function audit.

# Transit Swap Exploit (2022)

**Definition:** Approval hijack through internal call injection.

**Example:** ~$21M stolen; partial recovery.

**Cause:** Poor input validation.

**Prevention:** Whitelist contract calls; input sanitization.

# PancakeBunny Flash Loan Attack (2021)

**Definition:** Price manipulation using flash loans.

**Example:** ~$45M drained from BSC protocol.

**Cause:** No TWAP or price bounding.

**Prevention:** Use average price oracles and flash loan limits.

# Yam Finance Bug (2020)

**Definition:** Integer overflow in rebase logic bricked governance.

**Example:** $750K lost due to rebasing flaw.

**Cause:** Faulty math in rebasing implementation.

**Prevention:** Use SafeMath or Solidity 0.8+ and audit math-heavy logic.

# Snowdog DAO Rug Pull (2021)

**Definition:** Liquidity pulled using a hidden withdrawal script.

**Example:** $10M lost in a coded rug pull.

**Cause:** Opaque logic in migration contracts.

**Prevention:** Transparently publish and audit migration plans.

# Acala aUSD Depeg Incident (2022)

**Definition:** Pool bug allowed excessive minting of aUSD.

**Example:** 3B aUSD minted; stablecoin depegged.

**Cause:** Logic flaw in liquidity pool config.

**Prevention:** Limit mint caps and enforce access controls.