Section A: EVM Smart Contract Security Vulnerability Checklist (see Solana list in section B)

1. General Smart Contract Vulnerabilities

- Reentrancy
- Cross-function reentrancy
- Cross-contract reentrancy
- Read-only reentrancy
- Integer overflow
- Integer underflow
- Precision loss
- Rounding errors
- Division by zero
- Incorrect arithmetic
- Unchecked return values
- Unchecked external calls
- Unsafe low-level calls
- delegatecall vulnerabilities
- call injection
- Denial of Service (DoS)
- Gas exhaustion
- Gas griefing
- Block gas limit issues
- Transaction-order dependence
- Front-running
- Back-running
- Sandwich attacks
- MEV exploitation
- Flash-loan attacks
- Oracle manipulation
- Price manipulation
- Timestamp manipulation
- Block-number dependence
- Weak randomness
- Signature replay
- Cross-chain replay

- Missing nonce validation
- Improper access control
- Privilege escalation
- Missing authorization
- Unauthorized function execution
- Default/admin privilege abuse
- Centralization risks
- Single point of failure
- Improper initialization
- Re-initialization
- Unprotected upgradeability
- Proxy vulnerabilities
- Storage collision
- Function selector collision
- Self-destruct vulnerabilities
- Forced ETH/BNB/Native-token transfer
- Unexpected token behavior
- Malicious token interactions
- ERC-20 compatibility issues
- ERC-721 compatibility issues
- ERC-1155 compatibility issues
- Fee-on-transfer token issues
- Rebasing token issues
- Deflationary token issues
- Blacklist/whitelist abuse
- Honeypot mechanisms
- Hidden minting
- Hidden burning
- Hidden transfer restrictions
- Hidden owner privileges
- Emergency-function abuse
- Incorrect state validation
- State manipulation
- Invariant violations
- Logic flaws
- Business-logic vulnerabilities

2. Token Contract

- Unauthorized minting
- Unlimited minting
- Unauthorized burning
- Unauthorized pausing
- Unauthorized unpausing
- Unauthorized blacklist modification
- Unauthorized whitelist modification
- Transfer restriction bypass
- Trading restriction bypass
- Max-wallet bypass
- Max-transaction bypass
- Anti-bot bypass
- Tax/fee manipulation
- Buy-tax manipulation
- Sell-tax manipulation
- Transfer-tax manipulation
- Fee exemption abuse
- Supply manipulation
- Balance manipulation
- Allowance manipulation
- Approval race conditions
- Infinite approval risks
- approve() vulnerabilities
- transferFrom() vulnerabilities
- Zero-address handling
- Ownership takeover
- Ownership renouncement flaws
- Hidden privileged functions
- Honeypot behavior
- Sell restriction
- Buy restriction
- Liquidity removal privileges
- Hidden trading controls

3. Token Locker

- Unauthorized unlock

- Early unlock
- Lock bypass
- Lock-period manipulation
- Unlock timestamp manipulation
- Owner impersonation
- Unauthorized withdrawal
- Unauthorized token recovery
- Unauthorized emergency withdrawal
- Lock ownership takeover
- Lock ID manipulation
- Lock amount manipulation
- Locked-balance manipulation
- Duplicate withdrawal
- Double claim
- Reentrancy
- Token substitution
- Fee manipulation
- Lock creation manipulation
- Lock deletion
- Lock modification
- Incorrect unlock calculations
- Incorrect remaining-balance calculations
- Privilege escalation
- Admin abuse
- Upgradeability vulnerabilities

4. Liquidity Locker

- Unauthorized LP withdrawal
- Early LP unlock
- LP ownership takeover
- LP token substitution
- LP amount manipulation
- Liquidity amount manipulation
- Lock bypass
- Unlock-time manipulation
- Duplicate LP withdrawal
- Double claim

- Unauthorized emergency withdrawal
- Unauthorized LP recovery
- Reentrancy
- Pair manipulation
- Pool manipulation
- DEX compatibility issues
- LP token validation failure
- Wrong LP-token handling
- Fee manipulation
- Admin privilege abuse
- Upgradeability vulnerabilities

5. MEV Contract

- Sandwich vulnerability
- Front-running
- Back-running
- Transaction-order dependence
- Flash-loan manipulation
- Oracle manipulation
- Price manipulation
- Slippage bypass
- Minimum-output bypass
- Maximum-input bypass
- Arbitrage manipulation
- Callback exploitation
- Reentrancy
- Malicious router interaction
- Malicious pool interaction
- Untrusted external calls
- Gas griefing
- Block timestamp dependence
- Block-number dependence
- Signature replay
- Nonce manipulation
- Access-control bypass
- Profit-accounting errors
- Incorrect reserve calculations

- Incorrect swap calculations
- Path manipulation
- Token approval abuse
- Allowance theft
- Native-token handling errors

6. Auto-Trading Smart Contract

- Unauthorized trading
- Unauthorized withdrawal
- Unauthorized fund transfer
- Wallet takeover
- Strategy manipulation
- Parameter manipulation
- Trading-pair manipulation
- Router manipulation
- Oracle manipulation
- Price manipulation
- Slippage attacks
- Sandwich attacks
- Front-running
- Back-running
- Flash-loan attacks
- Reentrancy
- Callback attacks
- Token approval abuse
- Allowance abuse
- Unlimited approval risks
- Malicious token interaction
- Honeypot-token interaction
- Fee-on-transfer incompatibility
- Rebasing-token incompatibility
- Gas griefing
- DoS
- Incorrect profit calculation
- Incorrect balance calculation
- Incorrect PnL calculation
- Incorrect fee calculation

- Duplicate execution
- Replay attacks
- Nonce issues
- Timestamp manipulation
- Block-number manipulation
- Access-control vulnerabilities
- Admin privilege abuse
- Emergency-function abuse
- Upgradeability vulnerabilities

7. Wallet / Wallet-Related Contracts

- Private-key exposure
- Seed-phrase exposure
- Signature forgery
- Signature replay
- Transaction replay
- EIP-712 validation flaws
- Domain-separator flaws
- Nonce manipulation
- Signature malleability
- Unauthorized transaction execution
- Unauthorized withdrawals
- Unauthorized approvals
- Delegatecall exploitation
- Multisig bypass
- Owner takeover
- Guardian bypass
- Recovery-function abuse
- Social-recovery manipulation
- Access-control bypass
- Arbitrary external call
- Arbitrary contract execution
- Arbitrary token transfer
- Arbitrary native-token transfer
- Spending-limit bypass
- Allowance abuse
- Phishing/signature authorization risks

- Upgradeability vulnerabilities
- Storage collision

8. Staking / Farming Contracts

- Reward manipulation
- Reward inflation
- Reward calculation errors
- Reward-token manipulation
- Unauthorized reward withdrawal
- Double claiming
- Claim replay
- Stake manipulation
- Unstake bypass
- Early withdrawal bypass
- Lock-period bypass
- Precision loss
- Rounding errors
- Flash-loan staking
- Flash-loan reward manipulation
- Pool manipulation
- Share-price manipulation
- Reentrancy
- DoS
- Access-control vulnerabilities

9. Presale / ICO Contracts

- Unauthorized token allocation
- Unauthorized withdrawals
- Price manipulation
- Contribution manipulation
- Purchase-limit bypass
- Max-wallet bypass
- Whitelist bypass
- Allocation manipulation
- Claim manipulation
- Double claiming
- Refund manipulation

- Hard-cap bypass
- Soft-cap calculation errors
- Incorrect token-price calculation
- Incorrect USD/ETH/BNB conversion
- Oracle manipulation
- Flash-loan exploitation
- Reentrancy
- Front-running
- MEV exploitation
- Timestamp manipulation
- Access-control vulnerabilities
- Admin privilege abuse

10. Bridge / Cross-Chain Contracts

- Cross-chain replay
- Message replay
- Fake message injection
- Invalid message verification
- Proof verification bypass
- Validator compromise
- Signer threshold bypass
- Chain-ID confusion
- Nonce manipulation
- Token minting manipulation
- Token burning manipulation
- Wrapped-token manipulation
- Decimal mismatch
- Cross-chain accounting errors
- Message-order manipulation
- Finality assumptions
- Oracle manipulation
- Access-control bypass
- Upgradeability vulnerabilities

11. NFT Contracts

- Unauthorized minting
- Unauthorized burning

- Token-ID manipulation
- Metadata manipulation
- URI manipulation
- Royalty manipulation
- Approval vulnerabilities
- setApprovalForAll() abuse
- Ownership manipulation
- Reentrancy
- Signature replay
- Marketplace callback attacks
- Unsafe receiver handling
- Enumeration inconsistencies
- Supply manipulation
- Access-control vulnerabilities

12. Oracle / Price Feed Integration

- Stale price
- Incorrect price validation
- Price manipulation
- Decimal mismatch
- Feed-address manipulation
- Oracle substitution
- Missing heartbeat validation
- Missing deviation checks
- Zero/negative price handling
- Flash-loan price manipulation
- TWAP manipulation
- Spot-price manipulation
- Oracle fallback manipulation
- Oracle availability DoS

13. Upgradeable / Proxy Contracts

- Unauthorized upgrades
- Proxy takeover
- Implementation takeover
- Uninitialized implementation
- Re-initialization

- Storage collision
- Storage-layout corruption
- Function-selector collision
- Admin-slot manipulation
- Proxy-admin vulnerabilities
- UUPS authorization flaws
- Transparent-proxy mistakes
- Upgrade bypass
- Malicious implementation
- Delegatecall vulnerabilities

14. Access Control / Governance

- Missing onlyOwner
- Incorrect role assignment
- Role escalation
- Role revocation failure
- Unauthorized admin
- Owner takeover
- Governance takeover
- Flash-loan governance attack
- Voting manipulation
- Quorum manipulation
- Proposal manipulation
- Timelock bypass
- Timelock manipulation
- Emergency-admin abuse
- Multisig bypass
- Centralization risk

15. Solana / Anchor-Specific

- Missing account validation
- Missing signer validation
- Missing owner validation
- Account substitution
- PDA seed collision
- PDA validation failure
- Incorrect PDA derivation

- Missing PDA bump validation
- Arbitrary CPI
- CPI privilege escalation
- Account type confusion
- Account closing vulnerabilities
- Closed-account reuse
- Lamport manipulation
- Rent-exemption issues
- Sysvar spoofing
- Program-ID validation failure
- Duplicate mutable accounts
- Remaining-accounts abuse
- Token-account substitution
- Mint-account substitution
- Authority validation failure
- Constraint bypass
- Arithmetic overflow/underflow
- Serialization/deserialization issues
- Initialization vulnerabilities
- Reinitialization
- Upgrade authority abuse
- Upgrade authority not secured
- Missing freeze/mint authority validation
- SPL Token / Token-2022 compatibility issues

16. EVM-Specific

- Reentrancy
- delegatecall
- call
- staticcall
- tx.origin authentication
- msg.value manipulation
- block.timestamp dependence
- block.number dependence
- blockhash dependence
- Selfdestruct-related issues
- CREATE/CREATE2 address manipulation

- Storage collision
- ABI encoding/decoding errors
- Function-selector collision
- Proxy vulnerabilities
- ERC-20 incompatibility
- ERC-777 callback attacks
- ERC-4626 vault vulnerabilities
- Permit/signature vulnerabilities
- EIP-712 vulnerabilities
- Gas-related vulnerabilities
- Return-data validation failures

17. Economic / DeFi Vulnerabilities

- Liquidity manipulation
- Reserve manipulation
- Share-price manipulation
- Exchange-rate manipulation
- Collateral manipulation
- Liquidation manipulation
- Interest-rate manipulation
- Fee manipulation
- Yield manipulation
- Flash-loan attacks
- Oracle manipulation
- Price manipulation
- Economic griefing
- Bank-run scenarios
- Insolvency
- Bad-debt accumulation
- Unbounded exposure
- Economic denial of service
- MEV extraction
- Incentive manipulation

18. General Audit / Code-Quality Checks

- Logic errors
- Business-logic flaws

- Incorrect assumptions
- Missing validation
- Missing input sanitization
- Unsafe external dependencies
- Deprecated dependencies
- Incorrect compiler version
- Known compiler vulnerabilities
- Unused privileged functions
- Dead code
- Shadowed variables
- Incorrect visibility
- Unsafe type conversions
- Unsafe casting
- Precision errors
- Rounding errors
- Inconsistent state updates
- Incorrect event emission
- Missing events
- Inconsistent accounting
- Invariant violations
- Unexpected edge cases
- Denial-of-service conditions
- Gas inefficiencies
- Centralization risks
- Trust assumptions
- Upgrade risks
- Admin-key risks
- Emergency-control risks
- Third-party dependency risks

Section B: Solana Smart Contract Security Vulnerability Checklist

1. Account Validation

- Missing account validation
- Missing owner validation
- Missing signer validation

- Missing writable-account validation
- Incorrect account ownership
- Account substitution
- Account confusion
- Account type confusion
- Type cosplay
- Incorrect account relationship
- Missing has_one validation
- Missing address validation
- Unchecked AccountInfo
- Unchecked UncheckedAccount
- Duplicate mutable accounts
- Duplicate account references
- Missing account existence validation
- Incorrect executable-account validation
- Incorrect system-program validation
- Incorrect token-program validation
- Incorrect associated-token-program validation

2. Signer / Authority Security

- Missing signer checks
- Fake authority
- Authority impersonation
- Incorrect signer validation
- Signer substitution
- Unauthorized signer
- Missing authority relationship checks
- Authority takeover
- Authority replacement
- Unauthorized authority transfer
- Missing multisignature validation
- Insufficient signer threshold
- Privilege escalation

3. PDA Security

- PDA seed collision
- Incorrect PDA seeds

- Missing PDA validation
- Incorrect PDA derivation
- Incorrect program ID
- Missing bump validation
- Non-canonical bump
- User-controlled bump
- PDA substitution
- PDA account confusion
- PDA authority confusion
- PDA seed manipulation
- Cross-instance PDA collision
- Missing seeds constraint
- Incorrect seeds::program
- PDA privilege misuse

Solana PDAs are particularly important because programs can authorize actions on behalf of their PDAs through invoke_signed.

4. Cross-Program Invocation (CPI)

- Arbitrary CPI
- Unverified CPI target
- Malicious CPI program
- Incorrect program ID
- CPI account substitution
- CPI signer privilege abuse
- CPI writable privilege abuse
- Unauthorized invoke
- Unauthorized invoke_signed
- Incorrect PDA signer seeds
- CPI privilege escalation
- CPI recursion issues
- Malicious callback
- CPI-induced state manipulation
- Untrusted external program interaction
- Missing CPI account validation

CPIs are a major Solana-specific attack surface because programs can invoke other programs and PDA signatures can be supplied through invoke_signed.

5. Account Initialization

- Reinitialization attack
- Missing initialization check
- Double initialization
- Initialization takeover
- Uninitialized account usage
- Incorrect initialization authority
- Initialization parameter manipulation
- Initialization front-running
- Account creation DoS
- Incorrect account size
- Incorrect rent handling

6. Account Closing / Revival

- Account revival
- Closed-account reuse
- Improper account closure
- Unauthorized account closure
- Incorrect close authority
- State persistence after closure
- Lamport manipulation
- Close-account race conditions
- Reinitialization after closure

7. remaining_accounts

- Unvalidated remaining accounts
- Arbitrary remaining accounts
- Incorrect remaining-account count
- Account substitution
- Duplicate remaining accounts
- Unverified ownership
- Unverified PDA
- Unverified token account
- Unverified mint
- Unverified authority
- Malicious remaining-account ordering

- Remaining-account CPI abuse

8. Anchor-Specific

- Incorrect #[account] constraints
- Missing Signer
- Incorrect Account
- Unsafe UncheckedAccount
- Missing has_one
- Missing constraint
- Incorrect seeds
- Incorrect bump
- Incorrect init
- Incorrect init_if_needed
- Unsafe realloc
- Incorrect close
- Account reload issues
- Account discriminator bypass
- Manual deserialization flaws
- Type cosplay
- Constraint bypass
- Anchor version vulnerabilities
- Incorrect account relationships

Anchor's account constraints provide important security checks, but unsafe use of unchecked accounts or manual validation can bypass those protections.

9. SPL Token / Token Account

- Incorrect mint validation
- Incorrect token-account validation
- Incorrect token authority
- Token-account substitution
- Mint substitution
- Freeze-authority abuse
- Mint-authority abuse
- Unauthorized minting
- Unauthorized burning
- Unauthorized transfer

- Unauthorized freeze
- Unauthorized thaw
- Token decimal mismatch
- Token amount manipulation
- Token-account ownership errors
- Token-program substitution
- Token-2022 incompatibility
- Transfer-hook exploitation
- Transfer-fee manipulation
- Permanent-delegate abuse
- Token extension misuse

10. Token-2022

- Transfer-hook vulnerabilities
- Transfer-fee vulnerabilities
- Permanent-delegate abuse
- Default-account-state manipulation
- Non-transferable-token assumptions
- Confidential-transfer assumptions
- Metadata-extension manipulation
- Interest-bearing-token manipulation
- Extension compatibility failures
- Incorrect extension validation
- Incorrect mint-extension assumptions
- Incorrect token-account extension assumptions

Token-2022 extensions need specific validation because token behavior can differ materially from standard SPL Token behavior.

11. Arithmetic / Numerical

- Integer overflow
- Integer underflow
- Division by zero
- Integer truncation
- Precision loss
- Rounding errors
- Decimal mismatch

- Unsafe casting
- Casting truncation
- Signed/unsigned conversion errors
- Incorrect percentage calculations
- Incorrect fee calculations
- Incorrect reward calculations
- Incorrect token amount calculations
- Incorrect share calculations
- Incorrect price calculations

12. Solana Native Program Security

- Unsafe AccountInfo handling
- Missing owner checks
- Missing signer checks
- Missing executable checks
- Incorrect account data parsing
- Unsafe serialization
- Unsafe deserialization
- Borsh parsing issues
- Account-data corruption
- Incorrect account-size assumptions
- Manual discriminator errors
- Incorrect program-ID validation
- Incorrect sysvar validation

13. Sysvar / Instruction Introspection

- Sysvar spoofing
- Incorrect sysvar validation
- Instructions sysvar manipulation
- Transaction introspection flaws
- Missing instruction-index validation
- Ed25519 verification bypass
- Secp256k1 verification bypass
- Signature verification logic errors
- Cross-instruction authorization bypass
- Missing transaction-level constraints

14. Reentrancy / Recursive Execution

- Reentrancy
- CPI recursion
- Cross-program recursive execution
- State inconsistency during CPI
- Callback exploitation
- State-update-after-CPI vulnerabilities
- Read-before-write inconsistencies

Solana's execution model differs from EVM reentrancy; direct self-recursion is possible, while indirect reentrancy through another program is restricted by the runtime.

15. SOL / Lamport Handling

- Unauthorized SOL withdrawal
- Lamport manipulation
- Incorrect lamport accounting
- Forced SOL transfers
- Incorrect rent handling
- Rent-exemption failures
- Unauthorized account funding
- Balance manipulation
- Incorrect SOL transfer authority
- System-program substitution

16. Transaction / Instruction Security

- Transaction-order dependence
- Front-running
- Back-running
- Sandwich attacks
- Transaction replay
- Instruction replay
- Duplicate instruction execution
- Instruction-order manipulation
- Missing nonce protection
- Missing expiration
- Stale transaction execution

- Blockhash expiration handling
- Transaction simulation assumptions

17. Oracle / Price Security

- Oracle manipulation
- Stale oracle data
- Invalid oracle account
- Oracle account substitution
- Incorrect price-feed validation
- Price-feed decimal mismatch
- Price manipulation
- TWAP manipulation
- Spot-price manipulation
- Flash-loan price manipulation
- Missing confidence validation
- Missing freshness validation
- Oracle fallback manipulation

18. DeFi / Liquidity

- Liquidity manipulation
- Pool manipulation
- Reserve manipulation
- Share-price manipulation
- Exchange-rate manipulation
- Flash-loan attacks
- Economic manipulation
- Liquidation manipulation
- Collateral manipulation
- Reward manipulation
- Yield manipulation
- Fee manipulation
- LP-token manipulation
- LP-account substitution
- Incorrect liquidity accounting

19. Token Locker

- Unauthorized unlock
- Early unlock
- Lock bypass
- Lock-time manipulation
- Unlock timestamp manipulation
- Lock amount manipulation
- Locked-balance manipulation
- Lock-account substitution
- PDA lock-account substitution
- Unauthorized withdrawal
- Unauthorized token recovery
- Unauthorized emergency withdrawal
- Duplicate withdrawal
- Double claim
- Token-account substitution
- Mint substitution
- Lock ownership takeover
- Lock authority takeover
- Reinitialization
- CPI abuse
- Token-2022 compatibility issues

20. Liquidity Locker

- Unauthorized LP withdrawal
- Early LP unlock
- LP ownership takeover
- LP-token substitution
- LP amount manipulation
- Pool substitution
- Pair/account substitution
- Liquidity manipulation
- Lock bypass
- Unlock-time manipulation
- Duplicate LP withdrawal
- Double claim
- Unauthorized recovery

- Unauthorized emergency withdrawal
- PDA manipulation
- CPI abuse
- Token-program substitution
- Token-2022 compatibility issues

21. MEV / Trading

- Sandwich attacks
- Front-running
- Back-running
- Transaction-order manipulation
- Slippage manipulation
- Minimum-output bypass
- Maximum-input bypass
- Price manipulation
- Oracle manipulation
- Pool manipulation
- Reserve manipulation
- Arbitrage manipulation
- Flash-loan attacks
- Router/program substitution
- CPI manipulation
- Token-account substitution
- Malicious pool interaction
- Malicious token interaction

22. Auto-Trading

- Unauthorized trading
- Unauthorized withdrawal
- Unauthorized transfer
- Strategy manipulation
- Parameter manipulation
- Trading-pair substitution
- Pool substitution
- Program substitution
- Router substitution
- Oracle manipulation

- Price manipulation
- Slippage attacks
- Sandwich attacks
- Front-running
- Back-running
- Flash-loan attacks
- Token approval/authority abuse
- Incorrect PnL calculation
- Incorrect fee calculation
- Incorrect balance calculation
- Duplicate execution
- Replay attacks
- CPI abuse

23. Wallet / Treasury Programs

- Unauthorized withdrawal
- Unauthorized SOL transfer
- Unauthorized token transfer
- Unauthorized CPI
- Authority takeover
- PDA authority takeover
- Signer bypass
- Multisig bypass
- Spending-limit bypass
- Recovery-function abuse
- Owner replacement
- Guardian bypass
- Transaction replay
- Signature replay
- Ed25519 verification flaws
- Arbitrary program execution
- Arbitrary CPI
- Token-account substitution
- Mint substitution

24. Staking / Farming

- Stake-account substitution

- Unauthorized staking
- Unauthorized unstaking
- Early withdrawal
- Lock-period bypass
- Reward manipulation
- Reward inflation
- Double claiming
- Claim replay
- Reward-account substitution
- Pool manipulation
- Share manipulation
- Precision loss
- Rounding errors
- Flash-loan staking
- Reentrancy/CPI issues
- Unauthorized reward withdrawal

25. Presale / Token Sale

- Unauthorized purchase
- Unauthorized withdrawal
- Price manipulation
- Allocation manipulation
- Contribution manipulation
- Whitelist bypass
- Purchase-limit bypass
- Max-wallet bypass
- Hard-cap bypass
- Soft-cap manipulation
- Claim manipulation
- Double claiming
- Refund manipulation
- Token-account substitution
- Treasury substitution
- Oracle manipulation
- SOL/USDC price manipulation
- Front-running
- MEV exploitation

- PDA manipulation

26. Upgrade / Program Authority

- Unauthorized program upgrade
- Upgrade-authority takeover
- Unprotected upgrade authority
- Upgrade authority not revoked
- Malicious upgrade
- Upgrade bypass
- Program-ID mismatch
- Incorrect deployment address
- Redeployment confusion
- Cross-instance confusion
- Initialization after upgrade
- State-layout incompatibility
- Migration vulnerabilities

27. DoS / Resource Exhaustion

- Account creation DoS
- Compute-unit exhaustion
- Excessive CPI
- Excessive account loading
- Excessive account allocation
- Reallocation DoS
- Transaction-size exhaustion
- Stack exhaustion
- Heap exhaustion
- Loop-based DoS
- Unbounded iteration
- Malicious remaining accounts
- Rent-related DoS
- Account-lock contention

28. Business Logic / Economic

- Incorrect state transitions
- Broken invariants

- Incorrect accounting
- Unauthorized state modification
- Missing state validation
- State desynchronization
- Incorrect fee logic
- Incorrect reward logic
- Incorrect ownership logic
- Incorrect lock logic
- Incorrect withdrawal logic
- Incorrect liquidity accounting
- Economic exploits
- Incentive manipulation
- Centralization risks
- Admin abuse
- Emergency-function abuse

29. Deployment / Configuration

- Incorrect program ID
- Incorrect PDA seeds
- Incorrect deployment configuration
- Wrong upgrade authority
- Wrong token mint
- Wrong token program
- Wrong treasury address
- Wrong oracle address
- Wrong DEX/program address
- Incorrect production configuration
- Debug/test configuration in production
- Uninitialized production accounts
- Missing authority revocation

30. Solana-Specific Code Review

- Unsafe unsafe Rust
- Panic conditions
- unwrap() abuse
- expect() abuse
- Unchecked arithmetic

- Unchecked casts
- Manual account parsing
- Manual PDA derivation
- Manual signer verification
- Manual owner verification
- Manual token validation
- Unsafe CPI construction
- Hard-coded addresses
- Hard-coded authorities
- Missing error handling
- Incomplete error handling
- Incorrect error propagation
- Unchecked return values
- Inconsistent state updates

The Solana checklist put much greater emphasis on account validation, signer validation, PDA security, CPI security, account lifecycle, remaining accounts, SPL Token/Token-2022 validation, and Anchor constraints. These are repeatedly identified as core Solana-specific security areas.