CERTLABZ CERTIFICATION BOARD

Certified Web3 Security Specialist (CW3SS)

Ten Sample Questions

These ten questions are written at the difficulty of the live exam. Six carry a figure, a data table, a configuration or a code listing; four are plain scenario questions, as on the live paper. Every one is a scenario a working Web3 security specialist would meet, and none of them appears in the live question bank.

The live exam is multistage adaptive: how you score on one stage selects the difficulty of the next, so no two candidates sit the same paper. It is a performance-based exam: each form can carry up to 5 to 12 performance-based questions alongside the multiple-choice questions, which means you build, sequence or complete something rather than only choosing from a list. Answers and full explanations follow each question here; the live exam does not disclose item-level answers.

Question 1 — Domain 2: Smart Contract Vulnerabilities — DATA

Emma Wilson matches each vulnerability to its defense.

Vulnerability	Defense
Reentrancy	(to choose)
Missing access control	(to choose)
Oracle manipulation	(to choose)
Unchecked call result	(to choose)

Table 1.1 Vulnerabilities and defenses.

Which set of defenses is correct?

A. Role checks, checks-effects-interactions, verify return values, and a manipulation-resistant feed, so role checks fix reentrancy.

B. Checks-effects-interactions, role-based restrictions, a manipulation-resistant price feed, and verifying the call return value.

C. A price feed, verifying return values, role restrictions, and checks-effects-interactions, so a price feed fixes reentrancy here.

D. Verifying return values, a price feed, checks-effects-interactions, and role restrictions, so return checks fix reentrancy first.

Correct answer: B
Reentrancy is defended with checks-effects-interactions, missing access control with role-based restrictions, oracle manipulation with a manipulation-resistant price feed, and an unchecked call with verifying the return value. Only option B pairs each vulnerability with its defense.

Question 2

Domain 3: Wallet, Key and Infrastructure Security

CONFIG

James Carter reviews a user who nearly lost funds.

```
user received a link to "verify" a wallet
site asked to approve a token spend
spender was an unknown draining contract
unlimited allowance requested
```

Listing 2.1 The incident.

What class of attack is this, and the defense?

A. A consensus attack, defended by raising the gas limit so the malicious approval cannot be included in a block at all.

B. An approval-phishing drainer; defend by verifying sites, scrutinizing approvals, and limiting or revoking allowances.

C. A reentrancy attack, defended by adding a reentrancy guard to the user wallet before any approval can be signed.

D. A denial-of-service attack, defended by sending many small transactions to keep the drainer contract too busy to act.

Correct answer: B
A phishing site tricking the user into signing an unlimited approval to a drainer is approval phishing. The defense is verifying sites, scrutinizing what an approval grants, and limiting or revoking allowances. It is not a consensus, reentrancy or denial-of-service attack, and gas limits do not stop it.

Question 3

Domain 4: Protocol and DeFi Attacks

DATA

Olivia Davis matches each protocol attack to its description.

Attack	Description
Flash-loan attack	(to choose)
MEV	(to choose)
Bridge exploit	(to choose)
Governance attack	(to choose)

Table 3.1 Protocol attacks.

Which set of descriptions is correct?

A. Reordering for profit, borrowing to manipulate within a transaction, seizing votes to pass a proposal, and draining a bridge.

B. Borrowing large sums to manipulate within one transaction, extracting value by reordering, draining a cross-chain bridge, and seizing votes.

C. Draining a cross-chain bridge, seizing votes, borrowing to manipulate in a transaction, and reordering for profit, in the order shown.

D. Seizing votes to pass a proposal, draining a bridge, reordering for profit, and borrowing to manipulate, in the order shown here.

Correct answer: B
A flash-loan attack borrows large sums to manipulate a protocol within a single transaction, MEV extracts value by reordering transactions, a bridge exploit drains a cross-chain bridge, and a governance attack seizes votes to pass a malicious proposal. Only option B matches each attack.

Question 4

Domain 6: Incident Response and Operations

CONFIG

Liam Anderson lists the steps of an incident response, out of order.

```
A. Publish a post-mortem and harden controls
B. Detect and confirm the incident
C. Contain, for example pause the affected contract
D. Investigate scope and impact
```

Listing 4.1 Response steps.

What is the correct order?

A. A, then C, then B, then D, publishing a post-mortem and pausing before the incident is even detected or confirmed at all.

B. B, then C, then D, then A, detecting and confirming, containing, investigating scope, then publishing a post-mortem and hardening.

C. D, then A, then B, then C, investigating and publishing before the incident is detected or the affected contract is contained.

D. C, then B, then D, then A, containing before the incident has been detected or confirmed as real in the first place at all.

Correct answer: B
Incident response runs: detect and confirm, contain (for example pause the affected contract), investigate scope and impact, then publish a post-mortem and harden controls. The other orders act or publish before the incident is detected and confirmed.

Question 5

Domain 5: Testing, Auditing and Monitoring

DATA

Ava Thompson matches each practice to what it provides.

Practice	Provides
Independent audit	(to choose)
Fuzzing	(to choose)
On-chain monitoring	(to choose)
Bug bounty	(to choose)

Table 5.1 Security practices.

Which set is correct?

A. Random and edge inputs, an external expert review, an incentive for outside researchers, and live alerting on anomalies.

B. An external expert review before launch, random and edge-case input testing, live alerting on anomalies, and outside-researcher incentives.

C. Live alerting on anomalies, an incentive for outside researchers, an external review, and random and edge inputs, in the order shown.

D. An incentive for outside researchers, live alerting on anomalies, random and edge inputs, and an external review, in the order shown.

Correct answer: B
An independent audit is an external expert review before launch, fuzzing tests random and edge-case inputs, on-chain monitoring provides live alerting on anomalies, and a bug bounty incentivizes outside researchers. Only option B maps each practice to what it provides.

Question 6

Domain 1: Web3 Security Foundations

DATA

A team weighs the security implications of immutability.

Fact	Implication
Deployed code is hard to change	Bugs are costly to fix
Transactions are final	No easy reversal
Value is bearer-like	Key theft equals loss
Code is public	Attackers can study it

Table 6.1 Immutability implications.

What does this imply for how Web3 systems should be secured?

A. Security can be added later, because immutability and finality make it easy to patch and reverse any problem after launch.

B. Security must be built in before deployment, since bugs are costly, transactions are final, and stolen keys mean lost funds.

C. Only the frontend needs securing, because immutable public contracts cannot be attacked once they are deployed on chain.

D Nothing special is needed, because public code and final transactions make Web3 inherently safe from every attack by design.

Correct answer: B
Because deployed code is hard to change, transactions are final, value is bearer-like and code is public, security must be designed in before deployment rather than patched afterward. Security cannot simply be added later, contracts are attackable, and public final systems are not inherently safe.

Question 7 Domain 3: Wallet, Key and Infrastructure Security

A protocol team keeps its upgrade and treasury keys on a single person laptop for convenience. Why is this a serious risk, and the fix?

A It is fine, because keeping powerful keys on one convenient device is the recommended setup for a small protocol team.

B A single key is a single point of failure; use multisig or an HSM and separation of duties so no one device or person is enough.

C The only risk is battery life, so keeping the laptop plugged in resolves the concern about the upgrade and treasury keys.

D The fix is to email a backup of the keys to the whole team, so that anyone can recover and use them at any time.

Correct answer: B
Powerful keys on one device are a single point of failure: theft or compromise of that laptop can drain the treasury or push a malicious upgrade. The fix is multisig or an HSM with separation of duties so no single device or person suffices. Battery life is irrelevant, and emailing keys makes the exposure far worse.

Question 8 Domain 4: Protocol and DeFi Attacks

A governance token is cheap and thinly held, and any proposal that passes executes immediately with no delay. Why is this dangerous?

A It is not dangerous, because cheap tokens and instant execution make governance more efficient and harder to attack overall.

B An attacker can cheaply acquire enough votes to pass and instantly execute a malicious proposal before anyone can react.

C The only danger is that voting is slow, so instant execution actually removes the main governance risk entirely here.

D The danger is purely cosmetic, because governance outcomes never affect the funds or parameters a protocol controls.

Correct answer: B
Cheap, thinly held votes let an attacker acquire a majority inexpensively, and instant execution means a malicious proposal takes effect before anyone can respond. Mitigations include a timelock and broader token distribution. Instant execution adds risk rather than removing it, and governance does control real funds and parameters.

Question 9 Domain 5: Testing, Auditing and Monitoring

A protocol passed one audit two years ago and has shipped many changes since without further review. What is the sound guidance?

A. One audit is permanent proof of security, so no further review is ever needed regardless of how much the code changes.

B. Security is ongoing; new and changed code needs fresh review, plus monitoring and a bug bounty, not a one-time stamp.

C. Audits only matter for the first deployment, so any code shipped after launch is automatically safe and needs no review.

D. The team should remove the old audit report, because keeping it is the only real security risk the protocol now faces.

Correct answer: B
Security is continuous: code shipped after an audit needs fresh review, backed by monitoring and a bug bounty, because a two-year-old audit does not cover new or changed code. One audit is not permanent proof, later code is not automatically safe, and the risk is unreviewed changes, not the old report.

Question 10 Domain 6: Incident Response and Operations

Mid-incident, a team can pause the affected contract to stop an ongoing drain but worry it looks bad. What is the right call?

A. Do not pause, because appearances matter more than funds and pausing would signal weakness to the wider community.

B. Pause to contain the drain if a safe mechanism exists, since stopping ongoing loss takes priority over optics during an incident.

C. Wait until the drain finishes on its own, because interrupting an active exploit always makes the situation worse for users.

D. Delete the contract entirely, because removing it is the only way to stop a drain once it has already started on chain.

Correct answer: B
When a safe pause mechanism exists, containing an active drain takes priority over how it looks, because stopping ongoing loss protects users. Prioritizing optics, waiting for the drain to finish, or trying to delete a live contract all lead to greater loss.

Published by the CertLabz Certification Board, a division of CertLabz LLC. Companion to objectives document CW3SS-001. https://certlabz.com/certifications/certified-web3-security-specialist.html