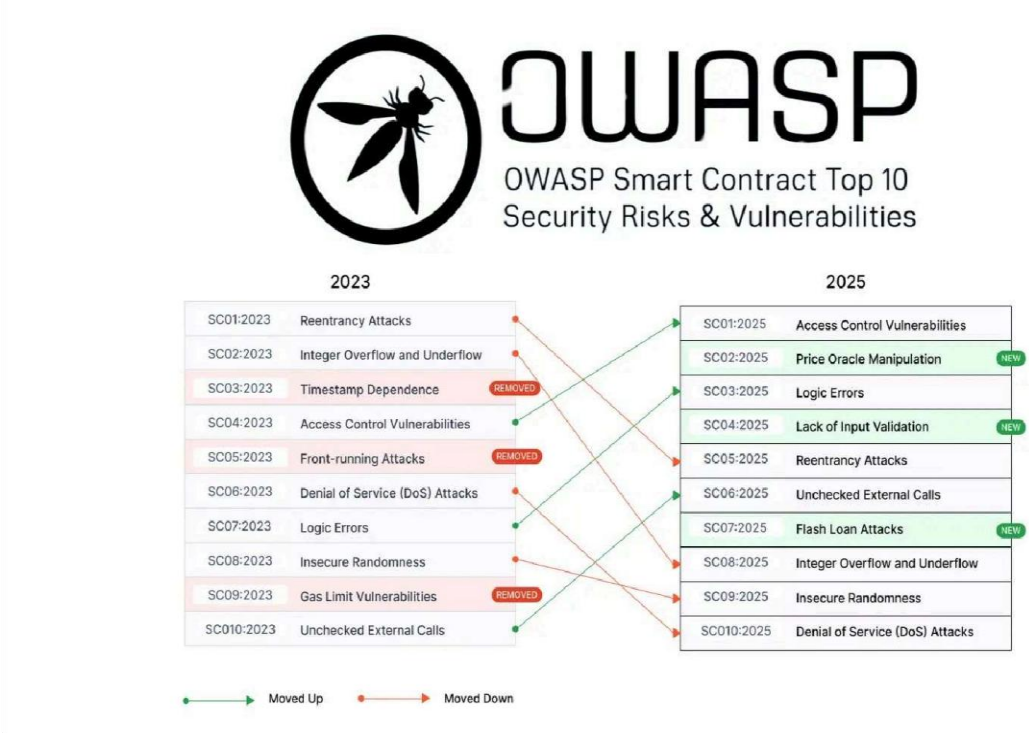


The Open Web Application Security Project (OWASP) has released its much-anticipated Smart Contract Top 10 for 2025, a comprehensive awareness document aimed at equipping Web3 developers and security teams with the knowledge to combat the most critical vulnerabilities in smart contracts.

As decentralized finance (DeFi) and blockchain technology continue to grow, the importance of robust smart contract security has never been more evident. The latest list reflects evolving attack vectors and highlights the vulnerabilities that have been most exploited or discovered in recent years.

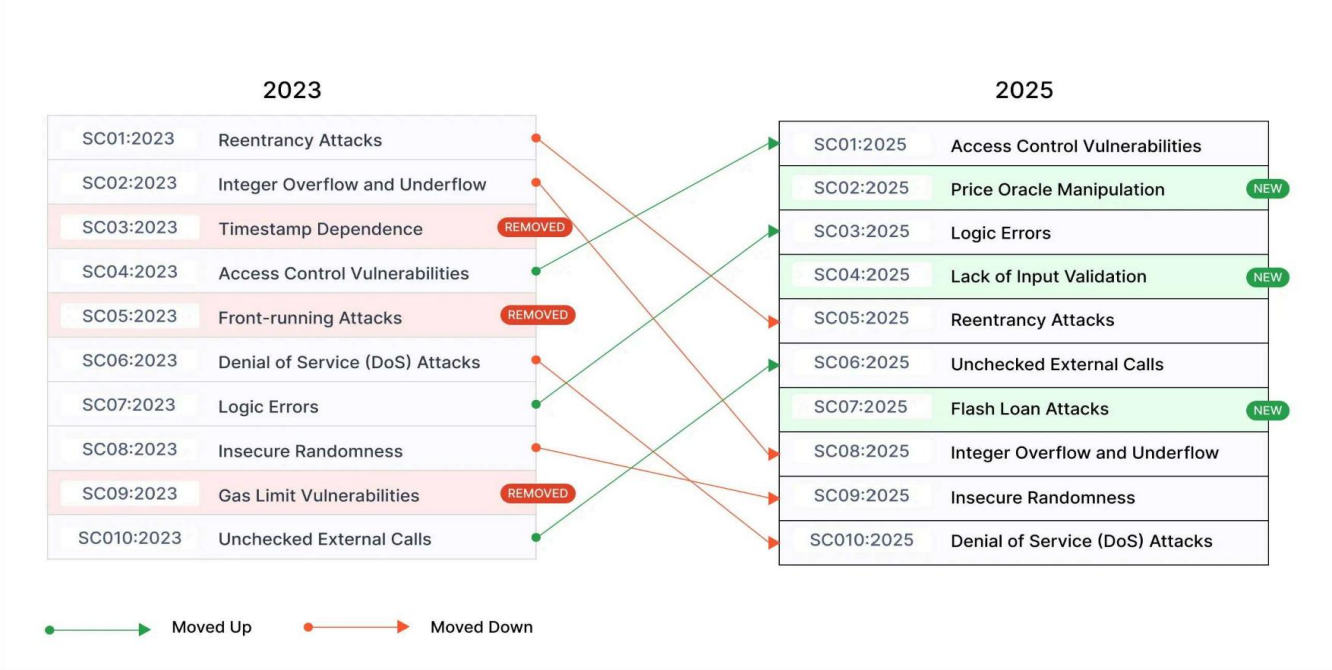
The OWASP Smart Contract Top 10 serves as a vital resource for developers, auditors, and security professionals, offering insights into common weaknesses and mitigation strategies.

It complements other OWASP projects, such as the Smart Contract Security Verification Standard (SCSVS) and Smart Contract Security Testing Guide (SCSTG), providing a holistic approach to securing blockchain ecosystems.

Key Changes from 2023 to 2025

The 2025 edition introduces updated rankings and new insights based on real-world incidents and emerging trends. Notable changes include the addition of Price Oracle Manipulation and Flash Loan Attacks as distinct categories, reflecting their growing prevalence in DeFi exploits.

Meanwhile, vulnerabilities such as Timestamp Dependence and Gas Limit Issues, prominent in earlier editions, have been replaced or integrated into broader categories like Logic Errors.



OWASP 2023 – 2025

OWASP Top 10 Vulnerabilities 2025:

1. **Access Control Vulnerabilities**
2. **Price Oracle Manipulation**
3. **Logic Errors**
4. **Lack of Input Validation**
5. **Reentrancy Attacks**
6. **Unchecked External Calls**
7. **Flash Loan Attacks**
8. **Integer Overflow and Underflow**
9. **Insecure Randomness**
10. **Denial of Service (DoS) Attacks**

Detailed Overview of the Top Vulnerabilities

SC01: Access Control Vulnerabilities

Access control flaws remain the leading cause of financial losses in smart contracts, accounting for $953.2 million in damages in 2024 alone. These vulnerabilities occur when permission checks are improperly implemented, allowing unauthorized users to access or modify critical functions or data. A notable example is the 88mph Function Initialization Bug, which allowed attackers to reinitialize contracts and gain administrative privileges.

SC02: Price Oracle Manipulation

Manipulating price oracles—external data feeds used by smart contracts—can destabilize protocols, leading to financial losses or systemic failures. Attackers often exploit poorly designed oracle mechanisms to inflate or deflate asset prices temporarily.

SC03: Logic Errors

Business logic vulnerabilities arise when contracts fail to execute their intended functions correctly. These errors can lead to improper token minting, flawed lending protocols, or incorrect reward distributions.

SC04: Lack of Input Validation

Failure to validate user inputs can allow attackers to inject malicious data into smart contracts, causing unexpected behaviors or breaking contract logic.

SC05: Reentrancy Attacks

Reentrancy attacks exploit a contract's ability to call external functions before completing its own state updates. This classic vulnerability was infamously used in the DAO hack of 2016, which drained $70 million worth of Ether.

SC06: Unchecked External Calls

When smart contracts fail to verify the success of external calls, they risk proceeding with incorrect assumptions about transaction outcomes. This can lead to inconsistencies or exploitation by malicious actors.

SC07: Flash Loan Attacks

Flash loans allow users to borrow funds without collateral within a single transaction but can be exploited to manipulate markets or drain liquidity pools.

SC08: Integer Overflow and Underflow

Arithmetic errors occur when calculations exceed data type limits, potentially allowing attackers to manipulate balances or bypass restrictions.

SC09: Insecure Randomness

Blockchain's deterministic nature makes generating secure randomness challenging. Predictable randomness can compromise lotteries, token distributions, or other functionalities relying on random outcomes.

SC10: Denial of Service (DoS) Attacks

DoS attacks target resource-intensive functions within smart contracts, rendering them unresponsive by exhausting gas limits or computational resources.

Real-World Impacts

The OWASP Smart Contract Top 10 is informed by incidents documented in resources like SolidityScan's Web3HackHub and Immunefi's Crypto Losses Report.

In 2024 alone, over $1.42 billion was lost across 149 documented incidents due to vulnerabilities such as access control flaws ($953M), logic errors ($63M), and

reentrancy attacks ($35M). These figures underscore the urgent need for robust security practices in blockchain development.

As blockchain technology matures, so do the methods employed by attackers seeking to exploit its vulnerabilities. The OWASP Smart Contract Top 10 for 2025 provides a critical roadmap for developers and security teams aiming to safeguard decentralized ecosystems against evolving threats.

By adhering to these guidelines and integrating best practices into every stage of development from design to deployment Web3 projects can bolster their resilience against potential exploits while fostering trust among users and investors alike.