Privasec | RED
RED TEAMING & ADVANCED ETHICAL HACKING

Blockchain Security and Smart Contract Audits

Fact Sheet v1.1

What is a Smart Contract Audit?

A **Smart Contract Audit (or Review)** is the process of examination of a smart contract (ie. code deployed on a blockchain) to identify security flaws that may be overlooked in the initial development phase.

Why are Smart Contract Audits Important?

With increasingly vast amounts of value transacted through or locked within smart contracts, they are attractive targets for malicious actors to act upon.

Blockchain transactions are irreversible, so making sure that a project's code is secure is of utmost importance.

The highly secure nature of the Blockchain makes it difficult to retrieve funds and resolve issues after implementation, which means that it will be better to prevent vulnerabilities at all costs.

The smart contract audit is essential in:

1. Security against hacking attacks
2. Reccommending coding best practices

OUR SMART CONTRACT AUDIT PROCESS

- We study the function, business context and environment where the code will operate in, to understand the possible risks associated with the code.
- Our next step would be a combination of automated code review and manual code assessment by our consultants.
- Our automation is aimed at filtering out "low-hanging fruits" in the initial stages. This approach results in a large amount of false positives along with vulnerabilities. All of the vulnerabilities identified in this process are verified to ensure the authenticity of the findings.
- The developer's intentions and general business logic are not taken into consideration at this juncture.
- Manual code review is the main focus of our smart contract review, with our consultants going through the code line-by-line to identify business logic flaws that would not be picked up by the automated code review process due to the logic behind the tool.

What to expect from our Audit Report

- You will receive a preliminary report, which contains an executive summary, together with a list of issues categorised by severity (e.g. critical, major, minor) and their associated status.
- The report will also contain a full breakdown of vulnerable code within the project, examples of fixes to directly remediate these items and other possible mitigation actions that can be taken.
- There will be time provided between this preliminary report and the release of a final version, during which you will be able to remediate on the findings of the first report.

Our Blockchain and Smart Contract Research Team

The Blockchain and Smart Contracts are relatively new, and testing techniques are constantly evolving. We keep ourselves apprised of movements within this space to better situate our offering.

Our team familiarises ourselves with what are considered best practices with Smart Contract security, keeping up with the community-at-large on several aspects:

- **General Design Philosophy:** What would be an optimal security mindset to adopt when programming a smart contract? Given the experimental nature of the technology, high cost of failure and difficulty of code change as development progresses, a different philosophy of development is warranted.
- **Development Recommendations:** We keep ourselves updated on good code patterns, from general precautions to more involved areas such as Solidity-specific or Token-specific practices.
- **Known Attacks:** We catalogue all classes of attacks against smart contracts to-date, together with known variants of said attacks.
- **Security Tools:** We utilise and maintain tools that help us be better at our job, be it detecting vulnerabilities or helping developers maintain a high code quality.

GET THE BALL ROLLING

Talk to your consultant or ring us today to understand your needs and provide a proposal to get started on your Smart Contract Audit.

You can call us at **6610 9597** or email us at **info@privasec.com**

Privasec

GRC GOVERNANCE AND INFORMATION SECURITY PARTNERS

RED RED TEAMING & ADVANCED ETHICAL HACKING

+61 1800 996 001 (AU)
+65 6610 9597 (SG)
+64 9 222 4725 (NZ)

info@privasec.com

www.privasec.com

New South Wales Office
Level 12, 234 George Street
Sydney 2000
NSW, Australia

Victoria Office
Level 6, 276 Flinders Street
Melbourne 3000
VIC, Australia

Queensland Office
Level 6, 200 Adelaide Street
Brisbane 4000
QLD, Australia

New Zealand Office
Level 4, 17 Albert Street
Auckland CBD 1010
New Zealand

Singapore Office
10 Anson Road
International Plaza #34-06
Singapore 079903

Malaysia Office
B-5-8 Plaza Mont Kiara
Mont Kiara 50480
Kuala Lumpur, Malaysia