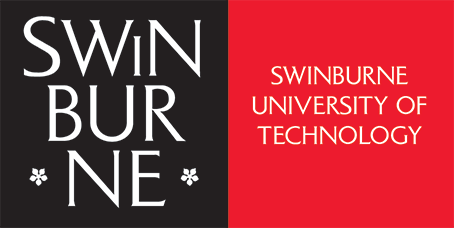
****

COS30049-Computing Technology Innovation Project

Assignment 3

Semester2 2023

Key Information

| Purpose | The main objectives of this assignment align closely with the Unit Learning Outcomes (ULOs) of the course:   * ULO1: students will apply their foundational knowledge to analyze potential cybersecurity threats, and implement software engineering skills, including code analysis, debugging, etc. * ULO4: students will need to consider the ethical, legal, and commercial dimensions, ensuring that proposed solutions don't breach any of these boundaries. * ULO5: Students must articulate their findings, suggestions, and evaluations in a manner that's coherent to both technical peers and non-technical stakeholders. * ULO7: Apply coordination skills to effectively manage team activities, ensuring timely and quality output. Demonstrate Effective Teamwork and Collaboration. |
| --- | --- |
| Assignment Description | This assignment is fundamentally report-based, designed to allow students to delve deep into practical scenarios within the realm of blockchain and cybersecurity. |
| Weight | 30% of your total marks for the unit |
| Due Date | Sunday, 05/11/2023, 11:59 pm |
| Submission | * Upload the project in a PDF file via Canvas Assignment Submission. * Turnitin will be used for similarity checking of all submissions. |
| Late Penalties | 10% deduction of the available mark per calendar day or part thereof for up to one week.  Submissions more than 7 calendar days after the due date will receive a mark of zero (0) and no assessment feedback will be provided. |

# **1 Assignment Task Description**

Assignment 3 is fundamentally report-based, designed to allow students to delve deep into practical scenarios within the realm of blockchain and cybersecurity. This assignment also aims to enhance students' understanding and capabilities in various critical areas of blockchain technology, including smart contract structure, contract auditing, and incident analysis related to cryptocurrency wallets. Students in three different group sets can focus on one of these specialized areas.

## **1.1 (for Group Set 1 students)**

**1) Objective**

The primary goal of this assessment is to enable students to understand the complex structures between smart contracts, such as the calling of external libraries and the mutual inheritance and calling between complex contracts. Meanwhile, for Solidity, this assignment hopes that students can generate call graphs, inheritance graphs, and contract structure diagrams between contracts through third-party tools, thereby better understanding the structure of the contracts. At the same time, students need to explain the specific content of the contracts and the logic between functions based on the generated diagrams.

**2) Background**

In recent years, blockchain technology has evolved from a purely cryptocurrency platform to a technology with broad application prospects. Among them, smart contracts, as a core component of blockchain technology, have demonstrated their revolutionary potential in various fields. Smart contracts allow trustworthy transactions to be executed without intermediaries, not only enhancing the transparency of the process but also significantly reducing the possibility of fraud and errors. Therefore, by analyzing the structure and call order of a contract, we can better understand the logic of the contract, thereby analyzing whether there is unreasonable business logic within the contract.

**3) Report Writing**

The report should be structured and comprehensive. The following sections are mandatory, but students are encouraged to include any other relevant sections they deem necessary:

1. **Project Information 2:** Detail pertinent information about the smart contract project:
   1. Project Name:Clearly state the name of the smart contract project.
   2. Project Description:Provide a brief overview of the project's purpose, objectives, and key functionalities.
   3. Team Information: Provide team member information and responsibilities
   4. Version Information:
      1. Smart Contract Version: Mention the current version of the smart contract.
      2. Dependencies Version: Detail the versions of any libraries or frameworks used within the project. This is especially important in the context of Ethereum where certain libraries like OpenZeppelin are frequently utilized.
2. **Executive Summary 2:** Provide a concise overview of the process, tools used, major findings, and overall understanding of the smart contract project's requirements.
3. **ABI Illustration 4**: You need to generate the corresponding ABI (Application Binary Interface) file for the contract file. Also, for each function in the ABI, describe the main logic and functionality of that function. Present a general understanding of the code, commenting on:
   1. Readability and structure.
   2. Use of comments and documentation.
   3. Elaborate on the functionality of a single function.
4. **Call Graph Discussion 5**：You need to discuss the call graph generated for the contract project. For instance, which functions are from the library, the calling logic between different functions, and which functions' interrelationships constitute a core feature in the contract.
5. **Inheritance Graph Discussion 5**: In Solidity, the inheritance diagram (or inheritance hierarchy) can reflect the following information (minimum choose three of the following topics to discuss):
   1. Inheritance Relationships: The diagram clearly shows the inheritance relationships between contracts, indicating which contract inherits from another.
   2. Code Reusability: Through inheritance, Solidity allows developers to reuse existing code. The inheritance diagram can help developers and auditors understand the origins and reuse of code.
   3. Function and State Variable Overriding: In Solidity, a derived contract can override functions and state variables of its parent contract. The inheritance diagram can help identify these overriding scenarios.
   4. Function Visibility and Access Control: The diagram can assist developers and auditors in understanding which functions remain visible in derived contracts and whether their access permissions have been altered.
   5. Modifier Application: Modifiers can be applied to functions to alter their behavior. The inheritance diagram can show which functions are affected by which modifiers.

Here is the smart contract source code:

<https://github.com/Uniswap/v3-core/tree/main/contracts>

## **1.2 Smart Contract Audit Report (for Group Set 2 students)**

**1) Objective**

The primary goal of this assessment is to demonstrate their ability to effectively audit smart contract projects. By utilizing the Slither audit tool, or the auditing platform developed in Assignment 2, students should critically evaluate, identify, and report on the vulnerabilities and overall security of a given smart contract project.

**2) Background**

As the blockchain and decentralized technology ecosystem continues to expand, the importance of secure and robust smart contract design and implementation cannot be overstated. A flaw in a smart contract can lead to significant financial and reputational losses. Professional auditing of these contracts is essential to ensure they are both secure and function as intended. In this assignment, students will emulate this professional auditing process, preparing them for real-world scenarios in the industry.

**3) Report Writing**

The report should be structured and comprehensive. The following sections are mandatory, but students are encouraged to include any other relevant sections they deem necessary:

1. **Project Information:** Detail pertinent information about the smart contract project:
   1. Project Name:Clearly state the name of the smart contract project.
   2. Project Description:Provide a brief overview of the project's purpose, objectives, and key functionalities.
   3. Auditing Team: Provide auditing team member information
   4. Version Information:
      1. Smart Contract Version: Mention the current version of the smart contract being audited. If there are multiple contracts with varying versions, list them appropriately.
      2. Dependencies Version: Detail the versions of any libraries or frameworks used within the project. This is especially important in the context of Ethereum where certain libraries like OpenZeppelin are frequently utilized.
2. **Executive Summary:** Provide a concise overview of the audit process, tools used, major findings, and overall evaluation of the smart contract project's security.
3. **Vulnerability Detection:** List and describe all vulnerabilities detected. For each vulnerability:
   1. Every vulnerability indicated by Slither must be **manually** verified by carefully inspecting the corresponding sections of code.
   2. Detail its nature and potential impact.
   3. Suggest mitigation strategies or fixes.
   4. Rate its severity (e.g., critical, high, medium, low).
4. **Contract Audit Results:** Dive deep into each smart contract in the project. For each contract:
   1. Provide a brief description of its purpose.
   2. Detail any vulnerabilities specific to that contract.
   3. Suggest improvements or optimizations.
5. **Code Review:** Present a general review of the code quality, commenting on:
   1. Readability and structure.
   2. Use of comments and documentation.
   3. Adherence to best practices.
6. **Conclusion of the Report:** Summarize the overall state of the smart contract project after your audit. Reflect on the security and robustness of the project code, highlighting areas of excellence and areas needing improvement.

**4) Auditing Project Source Code**

The auditing project (*HoldEarn.zip*) is provided. You can directly download the source code from the Canvas Assignments Page.

## **1.3 Crypto Wallet Incident Analysis Report (for Group Set 3 students)**

**1) Objective**

The objective of this assignment is to conduct a comprehensive analysis of an incident involving a crypto wallet company, with a focus on providing an in-depth understanding of the incident, scrutinizing transaction details, and proposing effective mitigation measures and remediation strategies.

**2) Background**

On November 1, 2022 (UTC), Deribit Exchange experienced a security breach. The attacker successfully compromised Deribit’s hot wallets, leading to the unauthorized withdrawal of cryptocurrencies. In response to this incident, the company requests an incident report, and the following information is provided for your reference.

Deribit’s wallet address:

* ETH: 0x58F56615180A8eeA4c462235D9e215F72484B4A3

Hackers wallet address(es):

* ETH

0xb0606F433496BF66338b8AD6b6d51fC4D84A44CD

0x8d08aAd4b2BAc2bB761aC4781CF62468C9ec47b4

* BTC

bc1q2dequzmk5vk8nmmrata8nq4y0zgqn4vc0n2h8y

bc1qw5g8lw4kzltpdcraehy2dt6dqda8080xd6vhl4kg4wwsypwerg9s3x6pvk

**3) Report Writing**

The report should contain but not limit to the following information:

1. **Incident Overview 3**
   1. Provide a concise summary of the incident.
   2. Include the date and time of the incident.
   3. Specify the main entities involved.
   4. Describe the nature of the suspicious/illegal activity.
2. **Incident Details 3** 
   1. Transaction amounts.
   2. Parties involved.
   3. Addresses relevant to the incident.
   4. Transaction hashes relevant to the incident.
   5. Tags (e.g., Exchange, Wallet Company, Hacker Wallet) for relevant addresses.
   6. Any red flags observed.
3. **Transaction Analysis and Visualisation 6**
   1. Analyze the transactions and any blockchains associated with the incident
   2. Highlight unusual patterns from typical behavior.
   3. Provide details on: a) Source of funds, b) Purpose of transactions, c) Hidden information in transaction data (e.g., information decoded from ETH ‘input’ text).
   4. Visualize path information of illicit funds:
      1. For ETH transactions, utilize the transaction analysis platform developed in your group's previous assignments.
      2. For BTC transactions, either draw the path using graphic design tools or use existing tracing platforms (e.g., OKLink) with proper referencing.

\*Note: Score deduction may apply if alternative tracing platforms, graphic design tools are used for ETH transaction visualization or the path is hand drawn. If you are unable to utilize your own tracing platform for visualizing the transaction path, please provide clarification.

1. **Mitigation Measures and Remediation: 6**
   1. Describe actions taken to mitigate risks associated with suspicious/illegal activity.
   2. Outline steps for ongoing monitoring and remediation.
   3. Provide recommendations for strengthening AML processes and controls.

# **2 Submission**

You must submit your assignment via the assignment submission link (i.e., “Assignment 3 Submission”) on the Canvas site by the deadline specified in Section 1 (Sunday, 05/11/2023, 11:59 pm).

* There will be NO hard copy submission required for this assignment.
* You are required to submit your assignment as a PDF file named with your group number. For example, if your group number is “group 1-23”, you would submit a zipped file named “group 1-23.pdf”.
* No submission is accepted via email.

# **3 Deliverables**

Your submission should contain the following files:

**Analysis Report**: The report should be at least 10 pages (excluding references). You must acknowledge all statements and information taken from other sources and adhere to the guidelines published regarding plagiarism. All ideas and material taken from references must be cited within the report itself and a full reference list and bibliography (if appropriate) must be provided at the end of the report. Diagrams and/or tables may be used if you think this will strengthen your arguments. Remember that diagrams and tables adapted from other sources must be cited (***Harvard*** style) as well.

**Contribution Form**: A form includes sections for the personal information of each team member, details of the contribution (with the upper limit set at **100% for each individual)**, and other additional information. Each team is permitted to submit only **one** such form. It's imperative that team members confer and reach a consensus before submitting the contribution form.

**Important Notes:**

* Please be careful to ensure you do not publicly post anything which includes your reasoning, logic or any part of your work to the Canvas discussion, doing so violates Swinburne plagiarism/ collusion rules and has significant academic penalties. Use email to your allocated tutor to raise questions that may reveal part of your reasoning or solution.
* You should be aware that there might be a file size limit for uploads.
* In this Assessment, you must NOT use generative artificial intelligence (AI) to generate any materials or content in relation to the assessment task.

# **4 Marking Criteria**

This assignment is worth 30% of your total mark. Your work will be marked as per the following:

| **Criterion** | **Marks** |
| --- | --- |
| **Structure**   * **Organization (2 points)**   + Logical flow and coherence among sections   + Effective use of headings and subheadings * **Formatting and Consistency (2 points)**   + Submissions must be readable by Microsoft Word or PDF/Acrobat format   + Must at least **10 pages** (excluding references), have at least 2cm margins, and use a font size no smaller than 12 point. Penalties apply for non-compliance   + Consistent formatting and style throughout the report | 4 |
| **Professional Writing**   * **Clarity and Precision (2 points)**   + Clear, concise, and precise language usage   + Absence of grammatical and syntactical errors * **Tone and Style (2 points)**   + Appropriate and consistent tone and style for an academic report   + Professional and respectful language | 4 |
| **Reference**   * **Accuracy (2 points)**   + All claims and data are accurately cited   + Full citation details provided for each source * **Consistency (2 points)**   + Uniformity in the chosen citation style (Harvard Style)   + Proper in-text citations and reference list formatting | 4 |
| **Key Requirements**   * **(for Group Set 1 students)** * **Smart Contract Audit Report (for Group Set 2 students)**   + Project Information (2)   + Executive Summary (1)   + Vulnerability Detection (7)   + Contract Audit Results (5)   + Code Review (2)   + Conclusion of the Report (1) * **Crypto Wallet Incident Analysis Report (for Group Set 3 students)** | 18 |
| TOTAL | 30 |

The marking rubric used to assess your assessment task is also available in the assignment submission folder here in the unit site. I strongly encourage you to review it while working on your assignment to ensure your work aligns with the rubric itself.

|  | | |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  | | |