SOLIDProof

Bring trust into your projects

Blockchain Security | Smart Contract Audits | KYC

MADE IN GERMANY

Audit

Security Assessment

17. августа 2021 г.

For

DYNAMIS

Отказ от ответственности

Отчеты SolidProof.io не являются и не должны рассматриваться как «одобрение» или «неодобрение» какого-либо конкретного проекта или команды. Эти отчеты не являются и не должны рассматриваться как указание на экономику или ценность любого «продукта» или «актива», созданного какой-либо командой. SolidProof.io не покрывает тестирование или аудит интеграции с внешним контрактом или услугами (такими как Unicrypt, Uniswap, PancakeSwap и т. Д. ...)

SolidProof.io Audits не предоставляет никаких гарантий относительно абсолютного отсутствия ошибок в анализируемой технологии, а также не дает никаких указаний на владельцев технологий. SolidProof Audits ни в коем случае не должен использоваться для принятия решений об инвестициях или участии в каком-либо конкретном проекте. Эти отчеты никоим образом не содержат рекомендаций по инвестициям и не должны использоваться в качестве рекомендаций по инвестициям.

Отчеты SolidProof.io представляют собой обширный процесс аудита, призванный помочь нашим клиентам повысить качество своего кода при одновременном снижении высокого уровня риска, связанного с криптографическими токенами и технологией блокчейн. Технология блокчейн и криптографические активы представляют собой постоянный высокий уровень риска. Позиция SolidProof заключается в том, что каждая компания и каждое отдельное лицо несут ответственность за свою должную осмотрительность и постоянную безопасность. SolidProof никоим образом не претендует на какие-либо гарантии безопасности или функциональность технологии, которую мы согласны анализировать.

Сеть

Многоугольник (PoS-цепочка)

Веб-сайт

https: // Dynamis. fnance /

Телеграмма

https://t.me/Dynamis_Finance

Твиттер

https://twitter.com/Dynamis_Finance

Github

https://github.com/Dynamis-Finance

Середина

https://medium.com/@DynamisFinance

Описание

Dynamis Finance - это децентрализованная биржа, работающая в сети Polygon, которая сама по себе является сайдчейном, работающим в сети Ethereum. Платформа обеспечивает кросс-совместимость с другими экосистемами.

Название Dynamis было выбрано, потому что оно воплощает три ключевых принципа - сила, потенциал и способности. Эти принципы лежат в основе нашего основного видения платформы - места, которое позволяет нашим пользователям достичь финансовой свободы, исследуя весь потенциал децентрализованных финансов.

На платформе Dynamis пользователи могут создавать пулы ликвидности и взаимодействовать со смарт-контрактами, получая вознаграждения. Изучив потребности и желания наших пользователей, мы улучшили платформу с помощью стимулируемых утилитарных функций с помощью нескольких функций, которые будут подробно описаны в следующих разделах.

Участие в проекте

29 июля 2021 г. **Команда DYNAToken** привлекли Solidproof.io для аудита созданных ими смарт-контрактов. Задание носило технический характер и было направлено на выявление недостатков безопасности при разработке и выполнении контрактов.**Команда DYNAToken** предоставили Solidproof.io доступ к своему репозиторию кода и техническому документу.

Логотип

Ссылка на контракт

https://polygonscan.com/address/0x15b74087e37d3168e25E127f02000D1A4aF2288f # code

Уязвимость и уровень риска

Риск представляет собой вероятность того, что определенный источник-угроза воспользуется уязвимостью, и влияние этого события на организацию или систему. Уровень риска рассчитывается на основе CVSS версии 3.0.

Уровень	Ценить	Уязвимость	Риск (необходимое действие)
Критический	9 - 10	Уязвимость, которая может нарушить функционирование контракта в ряде сценариев или создает риск того, что контракт может быть разорван.	Немедленное действие снизить уровень риска.
Высокий	7 - 8,9	Уязвимость, которая влияет на желаемый результат при использовании договор или предоставляет возможность использовать контракт непреднамеренным образом.	Реализация корректирующие действия как как можно скорее.
Середина	4 - 6,9	Уязвимость, которая может повлиять на желаемый результат выполнение контракт по конкретному сценарию.	Реализация корректирующие действия в определенный период.
Низкий	2–3,9	Уязвимость, которая не имеет значительное влияние на возможные сценарии для использование контракт и наверное субъективно.	Реализация определенные корректирующие действия или принятие риск.
Информационная	0 - 1,9	Уязвимость, которая иметь информационный символ, но не влияет на код.	Наблюдение, что не определяет уровень риска

Стратегия и применяемые методы аудита

На протяжении всего процесса проверки было уделено внимание оценке репозитория на предмет проблем, связанных с безопасностью, качества кода и соответствия спецификациям и лучшим практикам. Для этого мы проводим построчную проверку нашей командой опытных пентестеров и разработчиков смарт-контрактов, документируя все обнаруженные проблемы.

Методология

Процесс аудита состоит из рутинной серии шагов:

1. Проверка кода, которая включает в себя следующее:
    я) Ознакомьтесь со спецификациями, источниками и инструкциями, предоставленными SolidProof, чтобы убедиться, что мы понимаем размер, объем и функциональность смарт-контракта.
    II) Ручная проверка кода, которая представляет собой процесс чтения исходного кода построчно в попытке определить потенциальные уязвимости.
    iii) Сравнение со спецификацией, то есть процесс проверки того, выполняет ли код то, что описывают спецификации, источники и инструкции, предоставленные SolidProof.

2. Тестирование и автоматический анализ, который включает в себя следующее:
    я) Анализ покрытия тестами, который представляет собой процесс определения того, действительно ли тестовые примеры покрывают код и сколько кода выполняется, когда мы запускаем эти тестовые примеры.
    II) Символьное выполнение, которое анализирует программу, чтобы определить, какие входные данные вызывают выполнение каждой части программы.

3. Обзор передового опыта, который представляет собой обзор смарт-контрактов с целью повышения эффективности, действенности, уточнения, ремонтопригодности, безопасности и контроля на основе установленных отраслевых и академических практик, рекомендаций и исследований.

4. Конкретные, детализированные и действенные рекомендации, которые помогут вам предпринять шаги для защиты ваших смарт-контрактов.

Использованный код из других фреймворков / смарт-контрактов (прямой импорт)

Импортированные пакеты:

- OpenZeppelin
  - Адрес
    - Собственный
  - SafeMatch
- Uniswap
  - UniswapV2Factory
  - UniswapV2Pair
  - UniswapV2Router01
  - UniswapV2Router02

Протестированные файлы контрактов

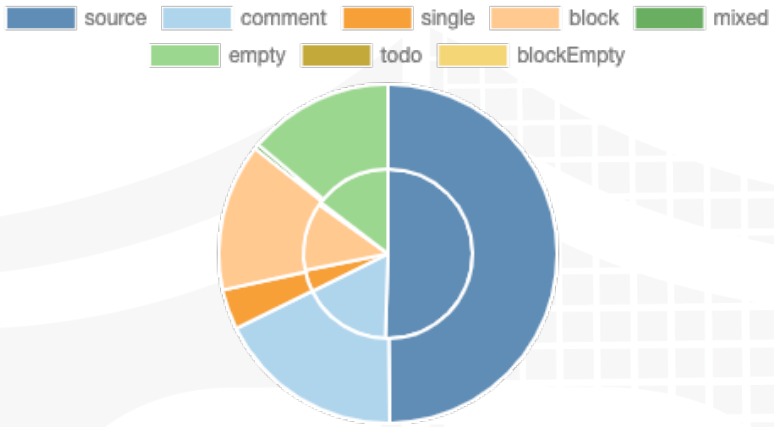
Этот аудит охватил следующие файлы, перечисленные ниже, с хешем SHA-1.

Файл с другим хешем был изменен намеренно или иным образом после проверки безопасности. Другой хеш может (но не обязательно) указывать на изменившееся состояние или потенциальную уязвимость, которые выходят за рамки этого обзора.

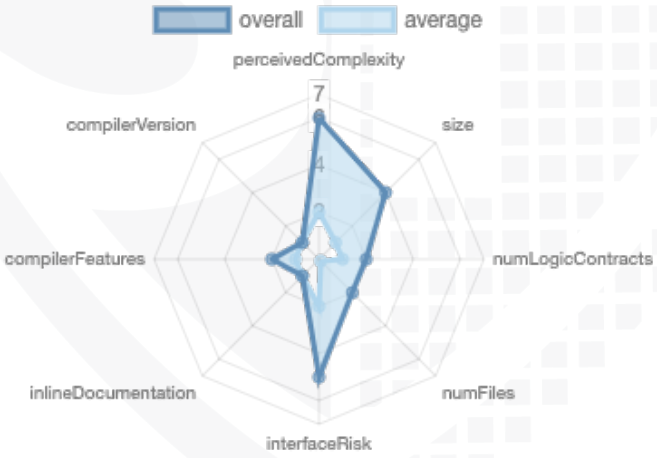
File Name	SHA-1 Hash
contracts/MasterChef.sol	99eeb28871b13fe85b2fdac37adc83fc21bfc8e7
contracts/IUniswapV2Factory.sol	a5d78edcba4e2228f92a4a0df03190c12d869184
contracts/interfaces/IBEP20.sol	324dfe448abd17cec338bd2c274034761b49b619
contracts/interfaces/IFeeStrategy.sol	a477aa89a952d09fe28eb72376f90c425dbd467f
contracts/interfaces/IDYNAReferral.sol	c5df10b3c1b7c07eb04c3c238929fc64b92de8b1
contracts/Address.sol	595164bf7303fff6779af7fa51d70d69ccd26bb0
contracts/SafeMath.sol	13fa35570fcd3209e8065231260df3a4fdbb06a5
contracts/Ownable.sol	55fa0c87da244fdcfbcbb536c50725d526f4184f
contracts/IUniswapV2Router02.sol	9b9f4c23ac1e66692519984e3d449605afa8a3bc
contracts/Pausable.sol	dd52d19e3f4a104ba818c423e5ac16007dca75e8
contracts/DYNAToken.sol	db1ed02ef3a191995509c1c539069e241fae2c3e
contracts/IUniswapV2Router01.sol	fc9a0f0007cb1ba6c3f8f3e63f0fa6280d4459d4
contracts/ReentrancyGuard.sol	c53345c941397872d8a81c4193a94df456ca6bf5
contracts/hardhat/console.sol	b1e9d9fe3a5c1ce12f551fee5038b5ef3c499292
contracts/utils/BEP20.sol	d6468b1229ec1643cfd79ee8d64797c4c206a760
contracts/utils/MinterRole.sol	974a11f04f403c19dc0881df00530b2992d9e78a
contracts/utils/Context.sol	70f8e53ab0ac56119de6d69be68014c53d90b3c5
contracts/utils/SafeBEP20.sol	e2f8a211cfaf755f7f50bebf5f7875abf1369c9a
contracts/utils/Roles.sol	a71c6b1b13d6b1dfd8b09e54da96e2487adf5ca6

Метрики

Исходные строки



Уровень риска



Возможности

Компоненты

Контракты	Библиотеки	Интерфейсы	Абстрактный
4	5	6	4

Открытые функции

В этом разделе перечислены функции, которые явно объявлены общедоступными или оплачиваемыми.

Обратите внимание, что методы получения для общедоступных переменных состояния не включены.

Общественные	К оплате
102	4

Внешний	Внутренний	Частный	Чистый	Вид
64	526	6	21 год	421

Переменные состояния

Общий	Общественные
53	35 год

Возможности

Твердость Версии наблюдаемый	Experim Ent аль Featu res	Жестяная банка Получать Фонды	Использует сборка	Имеет Разрушаемый Контракты
^ 0.8.0 > = 0,5,0 > = 0,4,0 > = 0,6,12 > = 0,6,2 > = 0,8,0 > = 0,4,22 <0,9,0 > = 0,7,0 > = 0,6,0		да	да (4 асм блоки)	

Переводы ETH	Низкий-Уровень Звонки	Делегат Вызов	Использует Хеш Функция s	ECRecov э	Новый/ Создавать/ Create2
да		да	да		

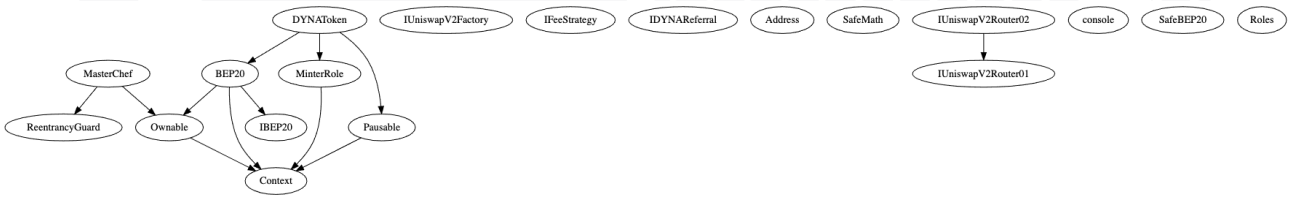
Объем работ

Команда вышеупомянутого токена предоставила нам файлы, которые необходимо протестировать (Github, Bscscan, Etherscan, файлы и т. Д.). Объем аудита - это основной контракт (обычно то же имя, что и команда с добавлением .sol).

Мы проверим следующие утверждения:

1. Правильная реализация стандартного токена Deployer
2. не может создать новые токены Deployer не может
3. записать или заблокировать средства пользователя
4. Deployer не может приостановить контракт Общая
5. проверка (Smart Contract Security)

График наследования



Проверить претензии

Правильная реализация стандарта Token

Tested Ve	расколотый

Функция	Описание	Существуют	протестированные	Проверено
TotalSupply	предоставляет информацию об общем поставка токенов	✓	✓	✓
Баланс	обеспечивает баланс счета аккаунт владельца	✓	✓	✓
Передача	выполняет переводы указанного количества токенов на указанное адрес	✓	✓	✓
Трансфер от	выполняет переводы указанного количество токенов из указанного адрес	✓		✓
Утвердить	разрешить спонсору забрать набор количество токенов из указанного учетная запись	✓		✓
Разрешение	возвращает заданное количество токенов из спонсор собственнику	✓	✓	✓

Необязательные реализации

Функция	Описание	Существуют	протестированные	Проверено
отказаться от владения	Владелец отказывается от права собственности на больше доверия	✓	✓	✓

Deployer не может чеканить новые токены

Проверено	Развертыватель не может мятить	Файл	Комментарий
✓	✘	Главный	Строка: 118

Максимальное / общее предложение: 10.184.000

```
constructor() public {
    _mint(msg.sender, PRESALE_SUPPLY);
    _mint(msg.sender, INITIAL_SUPPLY);
    _operator = msg.sender;

    _excludedFromAntiWhale[msg.sender] = true;
    _excludedFromAntiWhale[address(0)] = true;
    _excludedFromAntiWhale[address(this)] = true;
    _excludedFromAntiWhale[BURN_ADDRESS] = true;

    _excludedFromTransactionFee[msg.sender] = true;
}
```

DYNAToken.sol

```
function mint(address _to, uint256 _amount) public onlyMinter {
    if (totalSupply() < MAX_SUPPLY) {
        _mint(_to, _amount);
    }
}
```

Deployer не может сжечь или заблокировать средства пользователя

Имя	Проверено	Существовать	Проверено
Нет функции блокировки	✓	✓	✓
Нет функции прожига	✓	✓	✗

DYNAToken.so

• Функция записи может быть вызвана только владельцем (l)

```
function burn(address _from, uint256 _amount) public onlyOwner {
    _burn(_from, _amount);
}
```

```
function _burn(address account, uint256 amount) internal {
    require(account != address(0), 'BEP20: burn from the zero address');

    _balances[account] = _balances[account].sub(amount, 'BEP20: burn amount exceeds balance');
    _totalSupply = _totalSupply.sub(amount);
    emit Transfer(account, address(0), amount);
}
```

MasterChef.sol

1. add →
2. deposit →
3. emergencyWithdraw →
4. massUpdatePools →
5. renounceOwnership →
6. set →
7. setBuybackAddress →
8. setDevAddress →
9. setDynaReferral →
10. setFeeAddress →
11. setFeeStrategy →
12. setReferralCommissionRate →
13. transferOwnership →
14. updateEmissionRate →
15. updatePool →
16. withdraw →

Развертыватель не может приостановить контракт

Проверено	Развертыватель не мочь Пауза	Существовать
✓	✗	✓

DYNAToken.sol

• Оператор является создателем контракта

```
function pause() public onlyOperator {
    _pause();
}

function unpause() public onlyOperator {
    _unpause();
}
```

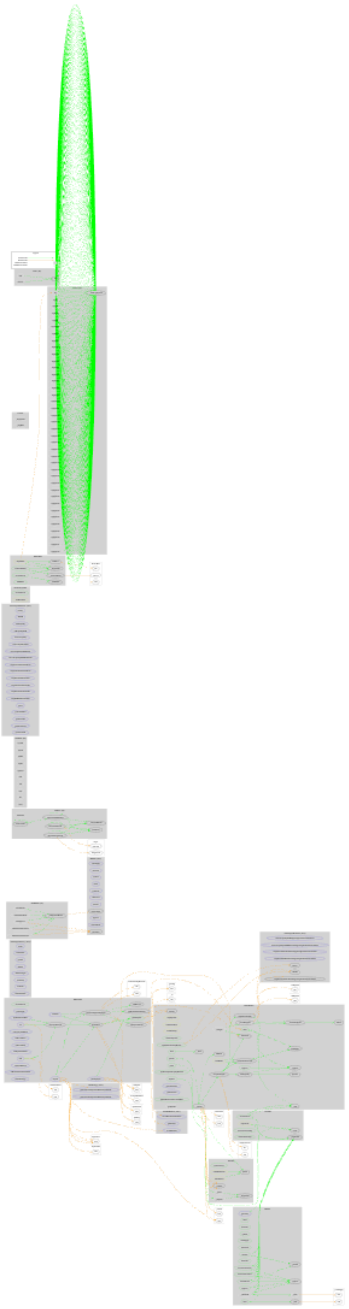
Общий осмотр (безопасность смарт-контрактов)

Tes Ted	Вер я подал

Легенда

Атрибут	Условное обозначение
Проверено / Проверено	
Частично проверено	
Непроверено / Не проверено	

CallGraph



Источники в объеме

Type	File	Logic Contracts	Interfaces	Lines	nLines	nSLOC	Comment Lines	Complex. Score	Capabilities
📝	contracts/MasterChef.sol	1	————	368	368	262	76	213	📫
🔍	contracts/IUniswapV2Factory.sol	————	1	17	6	4	————	17	————
🔍	contracts/interfaces/IBEP20.sol	————	1	98	23	17	66	21	————
🔍	contracts/interfaces/IFeeStrategy.sol	————	1	7	5	3	1	5	————
🔍	contracts/interfaces/IDYNAReferral.sol	————	1	19	8	3	10	7	————
📚	contracts/Address.sol	1	————	189	169	78	113	47	💻👥
📚	contracts/SafeMath.sol	1	————	218	218	69	134	10	🔅
💊	contracts/Ownable.sol	1	————	68	68	27	33	24	————
🔍	contracts/IUniswapV2Router02.sol	————	1	44	6	4	————	16	💰
💊	contracts/Pausable.sol	1	————	90	90	29	50	16	————
📝	contracts/DYNAToken.sol	1	————	417	400	260	77	203	💻🧱
🔍	contracts/IUniswapV2Router01.sol	————	1	95	4	3	————	48	💰
💊	contracts/ReentrancyGuard.sol	1	————	62	62	15	38	5	🔅
📚	contracts/hardhat/console.sol	1	————	1532	1532	1149	1	778	💻
📝	contracts/utils/BEP20.sol	1	————	320	308	108	169	91	————
📝	contracts/utils/MinterRole.sol	1	————	48	48	35	1	26	————
💊	contracts/utils/Context.sol	1	————	24	24	10	12	1	————
📚	contracts/utils/SafeBEP20.sol	1	————	100	78	37	32	25	————
📚	contracts/utils/Roles.sol	1	————	36	36	18	15	7	🔅
📝📚🔍💊	**Totals**	**13**	**6**	**3752**	**3453**	**2131**	**828**	**1560**	💻💰📫👥🧱🔅

Легенда

Атрибут	Описание
Линии	итоговые строки исходного блока
nLines	нормализованные строки исходного блока (например, нормализует функции, охватывающие несколько строк)
nSLOC	нормализованные строки исходного кода (только строки исходного кода; без комментариев, без пустых строк)
Строки комментариев	строки, содержащие одиночные или блочные комментарии
Оценка сложности	настраиваемая оценка сложности, полученная из операторов кода, которые, как известно, вносят сложность кода (ветви, циклы, вызовы, внешние интерфейсы, ...)

Результаты аудита

АУДИТ ПРОЙДЕН

Критические проблемы

- критических проблем не обнаружено -

Высокие проблемы

- серьезных проблем не обнаружено -

Средние проблемы

- Средних проблем не обнаружено -

Низкие проблемы

Проблема	Файл	Тип	Линия	Описание
# 1	Главный	Задана плавающая прагма	2	Текущая прагма Solidity директива - ""> = 0.8.0 "".

Информационные вопросы

- проблем с информацией не обнаружено -

Закомментированный код существует

Некоторые примеры кода закомментированы в следующих файлах, которые следует удалить:

Файл	Линия	Комментарий
MasterChef.sol	203	// dyna.mint (devAddress, dynaReward.div (10));

	220-223	// если (адрес (pool.lpToken) == адрес (dyna)) {
		// uint256 transferTax = _amount.mul (dyna.transferTaxRate ()). div (10000);
		// _amount = _amount.sub (transferTax); //}

Рекомендация

Удалите закомментированный код или исправьте их.

Комментарии аудита

31 июля 2021 г .:

DYNAToken.sol

- Владелец может чеканить токены ниже установленной переменной MAX_SUPPLY
- Владелец может приостановить действие контракта на неопределенный срок. Когда контракт приостановлен, вы не можете передавать токены
- Владелец может включить отключение подкачки и разжижение переменной.
- Владелец не отказался от права собственности

MasterChef.sol

- Владелец не отказался от права собственности
- Владелец может установить ставку реферальной комиссии равной 0, чтобы предотвратить выплату реферальной комиссии рефереру, который направил этого пользователя.

SWC атаки

Я БЫ	Заголовок	Отношения	Положение дел
ЮЗ С-136	Незашифрованный Личные данные В сети	CWE-767: доступ к критической частной переменной через открытый метод	ПРОШЕДШИЙ
ЮЗ С-135	Код без Эффекты	CWE-1164: несоответствующий код	ПРОШЕДШИЙ
ЮЗ С-134	Сообщение вызов с участием жестко запрограммированный газ количество	CWE-655: Неправильно Инициализация	ПРОШЕДШИЙ
ЮЗ С-133	Хеш-коллизии С несколькими Переменная Длина Аргументы	CWE-294: Обход аутентификации путем захвата-воспроизведения	ПРОШЕДШИЙ
ЮЗ С-132	Непредвиденный Баланс эфира	CWE-667: Неправильная блокировка	ПРОШЕДШИЙ
ЮЗ С-131	Присутствие неиспользованный переменные	CWE-1164: несоответствующий код	ПРОШЕДШИЙ
ЮЗ С-130	Справа налево- Переопределить контроль персонаж (U + 202E)	CWE-451: Пользовательский интерфейс (UI) Искажение важной информации	ПРОШЕДШИЙ
ЮЗ С-129	Типографский Ошибка	CWE-480: Использование неправильного оператора	ПРОШЕДШИЙ
ЮЗ С-128	DoS с блокировкой Лимит газа	CWE-400: неконтролируемый Потребление ресурсов	ПРОШЕДШИЙ

ЮЗС-127	Произвольный прыжок с функцией Тип Переменная	CWE-695: Использование функциональности низкого уровня	ПРОШЕДШИЙ
ЮЗС-125	Неверно Наследование порядок	CWE-696: неправильный порядок действий	ПРОШЕДШИЙ
ЮЗС-124	Написать в Произвольный Место хранения Место нахождения	CWE-123: условие записи-где-то	ПРОШЕДШИЙ
ЮЗС-123	Требование Нарушение	CWE-573: неправильное следование спецификации вызывающим абонентом	ПРОШЕДШИЙ
ЮЗС-122	Отсутствие надлежащего Подпись Проверка	CWE-345: Недостаточно Проверка данных Подлинность	ПРОШЕДШИЙ
ЮЗС-121	Отсутствует Защита против Подпись Воспроизведение атак	CWE-347: неправильная проверка криптографической подписи	ПРОШЕДШИЙ
ЮЗС-120	Слабые источники случайности fromChain Атрибуты	CWE-330: Использование недостаточно случайных значений	ПРОШЕДШИЙ
ЮЗС-119	Затенение Переменные состояния	CWE-710: Несоблюдение стандартов кодирования	ПРОШЕДШИЙ
ЮЗС-118	Неверно Конструктор Имя	CWE-665: Неправильно Инициализация	ПРОШЕДШИЙ
ЮЗС-117	Подпись Пластичность	CWE-347: неправильная проверка криптографической подписи	ПРОШЕДШИЙ

ЮЗС-116	Отметка времени Зависимость	CWE-829: включение Функциональность из недоверенной сферы управления	ПРОШЕДШИЙ
ЮЗС-115	Авторизация через tx.origin	CWE-477: Использование устаревшей функции	ПРОШЕДШИЙ
ЮЗС-114	Сделка порядок Зависимость	CWE-362: одновременно Выполнение с использованием общего доступа Ресурс с неподходящим Синхронизация ('Race Состояние')	ПРОШЕДШИЙ
ЮЗС-113	DoS с ошибкой Вызов	CWE-703: неправильная проверка или обработка исключительных условий	ПРОШЕДШИЙ
ЮЗС-112	Делегатозвонить Ненадежный Callee	CWE-829: включение Функциональность из недоверенной сферы управления	ПРОШЕДШИЙ
ЮЗС-111	Использование Устарело Твердость Функции	CWE-477: Использование устаревшей функции	ПРОШЕДШИЙ
ЮЗС-110	Заявить о нарушении	CWE-670: Всегда некорректная реализация потока управления	ПРОШЕДШИЙ
ЮЗС-109	Неинициализированный Указатель хранилища	CWE-824: Доступ Неинициализированный указатель	ПРОШЕДШИЙ
ЮЗС-108	Переменная состояния Дефолт Видимость	CWE-710: Несоблюдение стандартов кодирования	ПРОШЕДШИЙ
ЮЗС-107	Реентерабельность	CWE-841: Неправильно Обеспечение соблюдения поведенческой работы	ПРОШЕДШИЙ
ЮЗС-106	Незащищенный САМОСТРОЕНИЕ Инструкция T	CWE-284: Неправильный контроль доступа	ПРОШЕДШИЙ

ЮЗС-105	Незащищенный Эфир Снятие	CWE-284: Неправильный контроль доступа	ПРОШЕДШИЙ
ЮЗС-104	Непроверенный вызов Возвращаемое значение	CWE-252: непроверенное возвращаемое значение	ПРОШЕДШИЙ
ЮЗС-103	Плавающий Прагма	CWE-664: Неправильный контроль ресурса через его Продолжительность жизни	НЕТ ПРОШЕДШИЙ
ЮЗС-102	Устаревший Компилятор Версия	CWE-937: Использование компонентов с известными уязвимостями	ПРОШЕДШИЙ
ЮЗС-101	Целое число Переполнение и Под течением	CWE-682: неправильный расчет	ПРОШЕДШИЙ
ЮЗС-100	Функция Дефолт Видимость	CWE-710: Несоблюдение стандартов кодирования	ПРОШЕДШИЙ

Blockchain Security | Smart Contract Audits | KYC

MADE IN GERMANY