1. Алгоритмический стейбл USDS

Код: https://gist.github.com/mixbytes-audit/7acd83757f40ac486a40c812fd2ca4a0

Смарт-контракт реализует ERC-20 токен USDS, который можно обменивать на ETH и обратно по текущему курсу USD/ETH, определяемому оракулом Band Protocol.

Разработчики инвестировали собственные средства, чтобы выпустить 100 000 000 USDS, предоставив соответствующее количество ETH. Однако, через некоторое время обнаружилось, что количество ETH на смарт-контракте постоянно падает и близко к нулю. Разработчики подозревают тут злонамеренную активность и попросили Вас расследовать этот инцидент, и, если проект действительно уязвим, предложить решение.

2. Блокчейн-лотерея

Группа программистов из СНГ открыла самое честное в мире онлайн-казино на основе блокчейн-технологий. Самая популярная игра - орел/решка. Вот код соответствующего смарт-контракта: https://gist.github.com/mixbytes-audit/b01de38db5189fe816f3f0396f0bf918

Было задумано, что вероятность каждого исхода - 50%, выигрыш составляет x2 от ставки за вычетом комиссии 2%. По теории вероятностей, такой смарт-контракт должен работать в плюс. Однако, создателям постоянно приходится добавлять средства на смарт-контракт, они подозревают, что пользователи почему-то выигрывают чаще, чем должны. Попробуйте найти причину и предложить решение.

3. Обменник USDC на USDT

DeFi корпорация loss.finance разработала обменник, который позволяет производить обмены между равноценными ERC20 стейблами один к одному. Это гораздо удобнее, чем держать огромную ликвидность на uniswap-клонах. Вот код смарт-контракта обменника: https://gist.github.com/mixbytes-audit/ee8c42ed9ed6fbb4590ed513e1415cee

Предполагается, что каждый обмен повышает стоимость ERC-20 токена обменника за счет того, что комиссия с каждого обмена добавляется в пул ликвидности. Однако, цена токена постоянно падает, хотя это и не было предусмотрено логикой работы контракта. Найдите проблему в коде и дайте рекомендации по исправлению.

4. Ловушка для хакера

Вася - начинающий blackhat, и он нашел явную проблему reentrancy в этом вот смарт-контракте:
https://etherscan.io/address/0x14db723a05620d3bbe4303f9e566eb2c782e70f0#code

На балансе лежит аж 15 эфирок. Наконец-то он сможет съехать от мамы и купить себе собственную квартиру! Правда, сначала ему потребуется занять у кого-то денег на покупку 1 ETH.

Объясните, почему квартиру Вася не купит (не в этот раз), да и свои 1 ETH потеряет.

5. Взлома пароля в блокчейне

Стартапер Федя - новичок в теме блокчейна, но решил нести его в массы. Первое, что ему показалось слишком сложным - это приватные ключи, которые практически невозможно запомнить. И вот он создал кошелек, где можно хранить средства, защитив их простым паролем. При этом всё хранилось в блокчейне. А чтобы никто не взломал пароль перебором, он ввел штраф за неправильно введенный пароль.

Однако, когда его кошельком стали активно пользоваться, кто-то взял и вывел средства очень многих клиентов. Как это было сделано?

Вот код смарт-контракта:
https://gist.github.com/mixbytes-audit/180e3e4ed1d1e9221a3e3d685cee6c7d