

involves exploiting unvalidated redirects and the use of an outdated list of allowed addresses in a web application's redirection mechanism. The task is to manipulate the URL to redirect to an unapproved or unintended cryptocurrency address by leveraging the weaknesses in the allowlist.

Tools Used

- **Web Browser**
- **Developer Tools**

Methodology

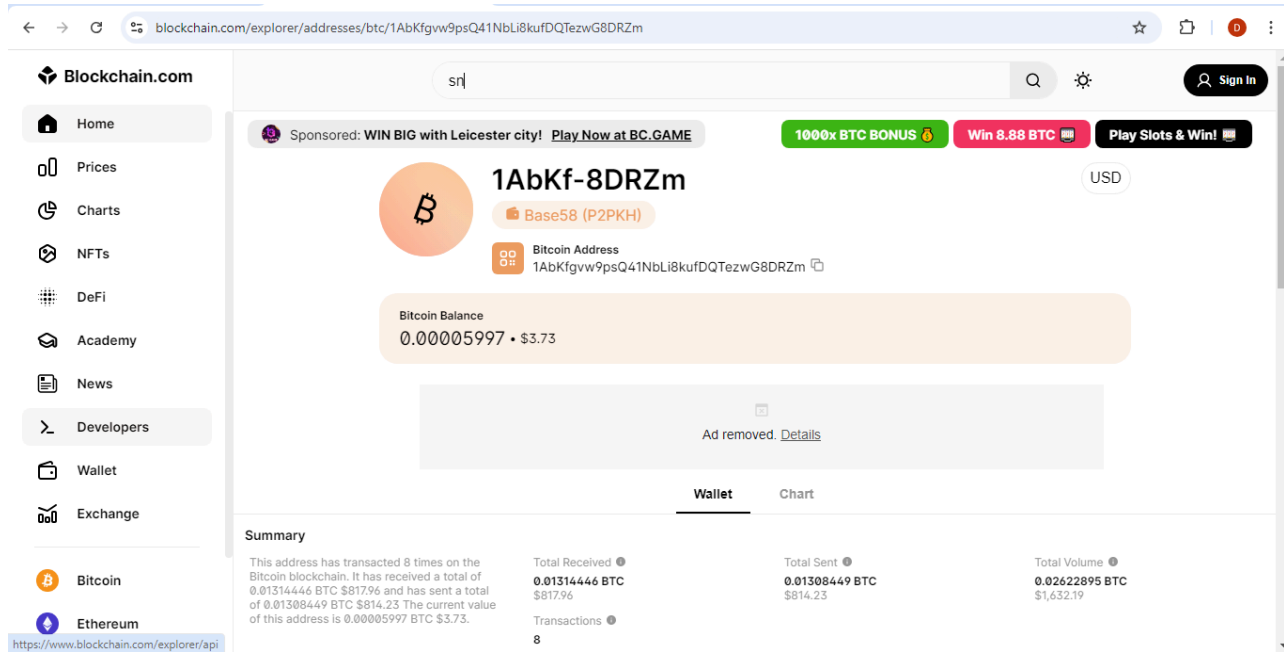
Initial Analysis

Upon interacting with the challenge, it's observed that the web application provides QR codes for cryptocurrency transactions. The JavaScript code managing these QR codes, found within the `main.js` file, reveals that specific cryptocurrency addresses are hard-coded, and there is a redirect function that points to these addresses based on the user's selection.

```
showBitcoinQrCode() {  
  
    this.dialog.open({  
  
        data: {  
  
            data: "bitcoin:1AbKfgvw9psQ41NbLi8kufDQTezwG8DRZm",  
  
            url:  
"./redirect?to=https://blockchain.info/address/1AbKfgvw9psQ41NbLi8kufDQTezwG8DRZm",  
  
            address: "1AbKfgvw9psQ41NbLi8kufDQTezwG8DRZm",  
  
            title: "TITLE_BITCOIN_ADDRESS"  
  
        }  
  
    })  
  
}
```

1. URL Manipulation:

- Modified the `redirect` URL parameter to point to a new address that was on the allowlist.
- Accessed the modified URL: <http://192.168.1.108:3000/redirect?to=https://www.blockchain.com/explorer/addresses/btc/1AbKfgvw9psQ41NbLi8kufDQTezwG8DRZm>



Blockchain.com

Search:

Sponsored: WIN BIG with Leicester city! [Play Now at BC.GAME](#) 1000x BTC BONUS Win 8.88 BTC Play Slots & Win!

1AbKf-8DRZm USD

Base58 (P2PKH)

Bitcoin Address
1AbKfgvw9psQ41NbLi8kufDQTezwG8DRZm

Bitcoin Balance
0.00005997 • \$3.73

Ad removed [Details](#)

Wallet Chart

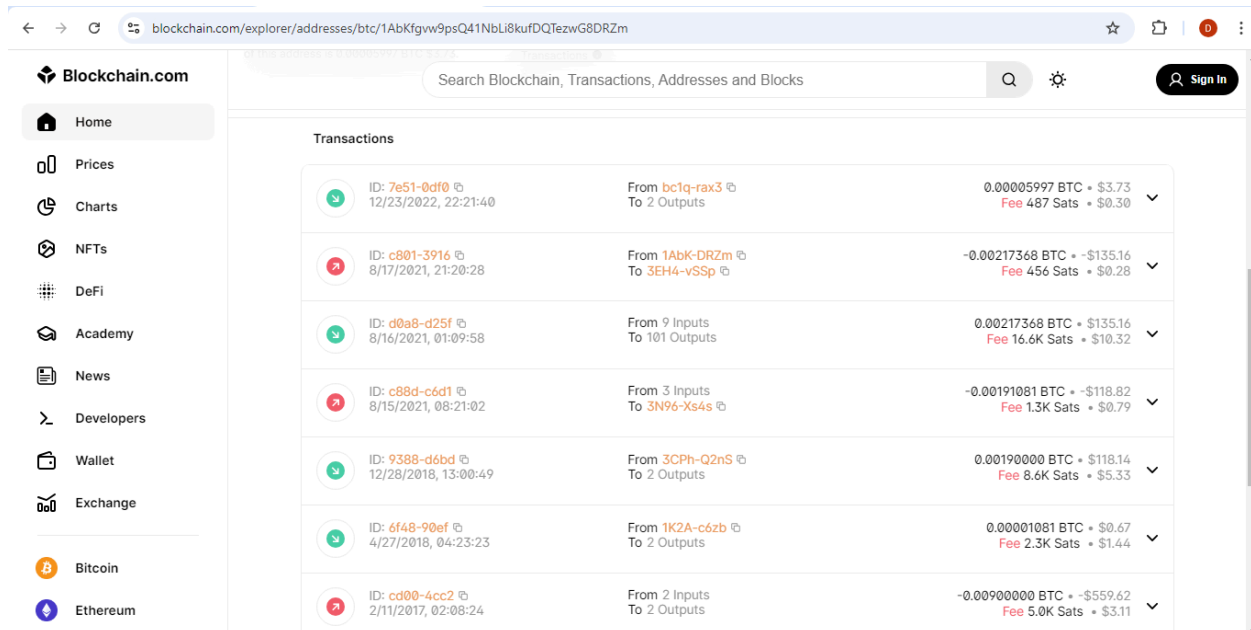
Summary

This address has transacted 8 times on the Bitcoin blockchain. It has received a total of 0.01314446 BTC \$817.96 and has sent a total of 0.01308449 BTC \$814.23. The current value of this address is 0.00005997 BTC \$3.73.

Total Received	Total Sent	Total Volume
0.01314446 BTC \$817.96	0.01308449 BTC \$814.23	0.02622895 BTC \$1,632.19

Transactions: 8

<https://www.blockchain.com/explorer/api>



Blockchain.com

Search Blockchain, Transactions, Addresses and Blocks

Transactions

ID	From	To	Amount	Fee
7e51-0df0	bc1q-rax3	To 2 Outputs	0.00005997 BTC • \$3.73	Fee 487 Sats • \$0.30
c801-3916	1AbK-DRZm	To 3EH4-vSSp	-0.00217368 BTC • -\$135.16	Fee 456 Sats • \$0.28
d0a8-d25f	9 Inputs	To 101 Outputs	0.00217368 BTC • \$135.16	Fee 16.6K Sats • \$10.32
c88d-c6d1	3 Inputs	To 3N96-Xs4s	-0.00191081 BTC • -\$118.82	Fee 1.3K Sats • \$0.79
9388-d6bd	3CPH-Q2nS	To 2 Outputs	0.00190000 BTC • \$118.14	Fee 8.6K Sats • \$5.33
6f48-90ef	1K2A-c6zb	To 2 Outputs	0.00001081 BTC • \$0.67	Fee 2.3K Sats • \$1.44
cd00-4cc2	2 Inputs	To 2 Outputs	-0.00900000 BTC • -\$559.62	Fee 5.0K Sats • \$3.11

Second : Allowlist Bypass

Tools Used

- Browser:
- Code Editor

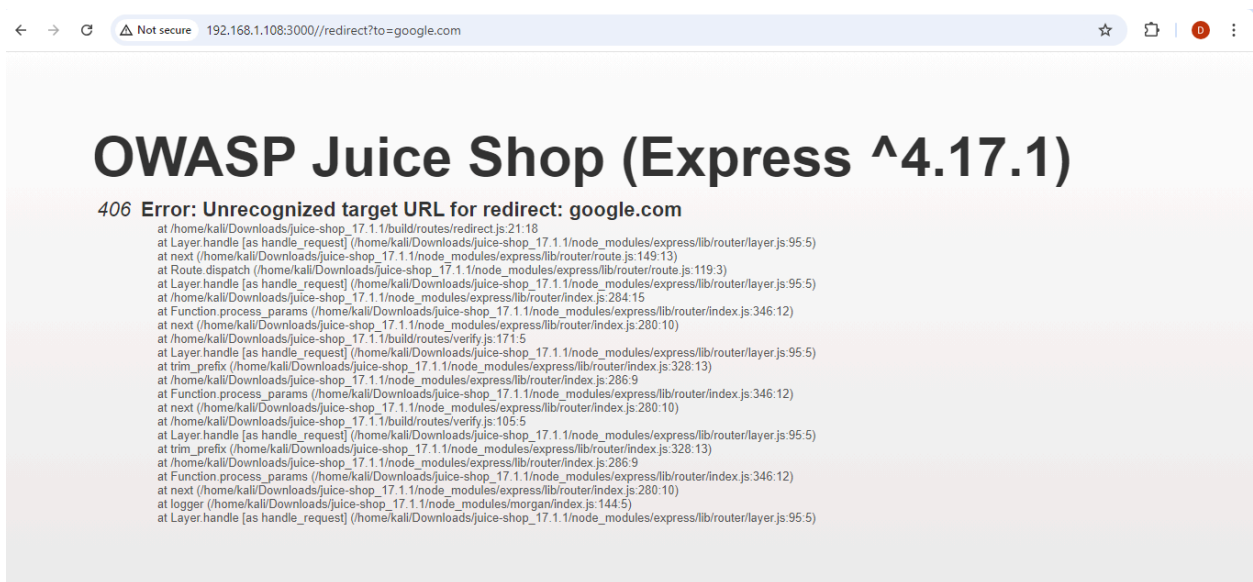
Methodology and Solution

- started by reviewing the `main.js` for how redirects are managed and handled within the application. To do this, I searched for "**redirect**". This revealed the basic form of the redirection URL as `192.168.1.108:3000/redirect?to=https://blockchain.info/address/1AbKfgvw9psQ41NbLi8kufDQTezwG8DRZm`

```
noop() {}
showBitcoinQrCode() {
  this.dialog.open(1e, {
    data: {
      data: "bitcoin:1AbKfgvw9psQ41NbLi8kufDQTezwG8DRZm",
      url: "../redirect?to=https://blockchain.info/address/1AbKfgvw9psQ41NbLi8kufDQTezwG8DRZm",
      address: "1AbKfgvw9psQ41NbLi8kufDQTezwG8DRZm",
      title: "TITLE_BITCOIN_ADDRESS"
    }
  })
}
showDashQrCode() {
  this.dialog.open(1e, {
    data: {
      data: "dash:Xr5S6RzuwX6hg5EGpkybbv5RanJoZN17kw",
      url: "../redirect?to=https://explorer.dash.org/address/Xr5S6RzuwX6hg5EGpkybbv5RanJoZN17kw",
      address: "Xr5S6RzuwX6hg5EGpkybbv5RanJoZN17kw",
      title: "TITLE_DASH_ADDRESS"
    }
  })
}
showEtherQrCode() {
  this.dialog.open(1e, {
    data: {
      data: "0x0f933ab9fCAA782D0279C300D73750e1311EAE6",
      url: "../redirect?to=https://etherscan.io/address/0x0f933ab9fCAA782D0279C300D73750e1311EAE6",
      address: "0x0f933ab9fCAA782D0279C300D73750e1311EAE6",
      title: "TITLE_ETHER_ADDRESS"
    }
  })
}
```

Testing with Non-Allowlisted URL:

- Used a common external URL (`google.com`) to test the redirect functionality. This attempt was blocked, confirming the presence of an allowlist mechanism



- The error pointed to the location of the allowlist check in the source code (/juice-shop/build/routes/redirect.js), providing a potential file path for further investigation.

Successful Allowlist Bypass:

url:

<http://192.168.1.108:3000/redirect?to=https://google.com/redirect?to=https://blockchain.info/address/1AbKfgvw9psQ41NbLi8kufDQTezwG8DRZm>

