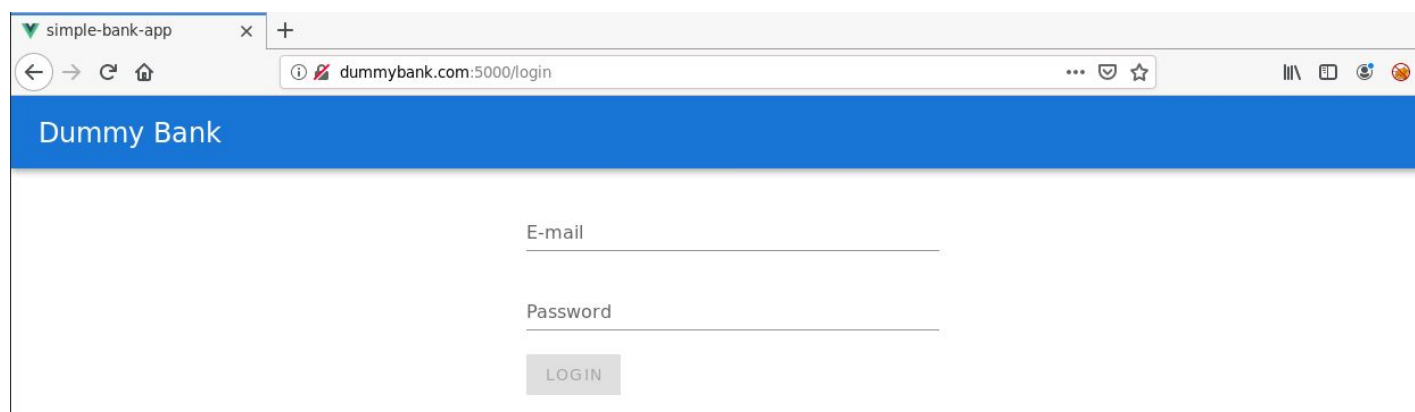


Name	Improper Input Validation II
URL	https://attackdefense.com/challengedetails?cid=1968
Type	REST: API Security

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

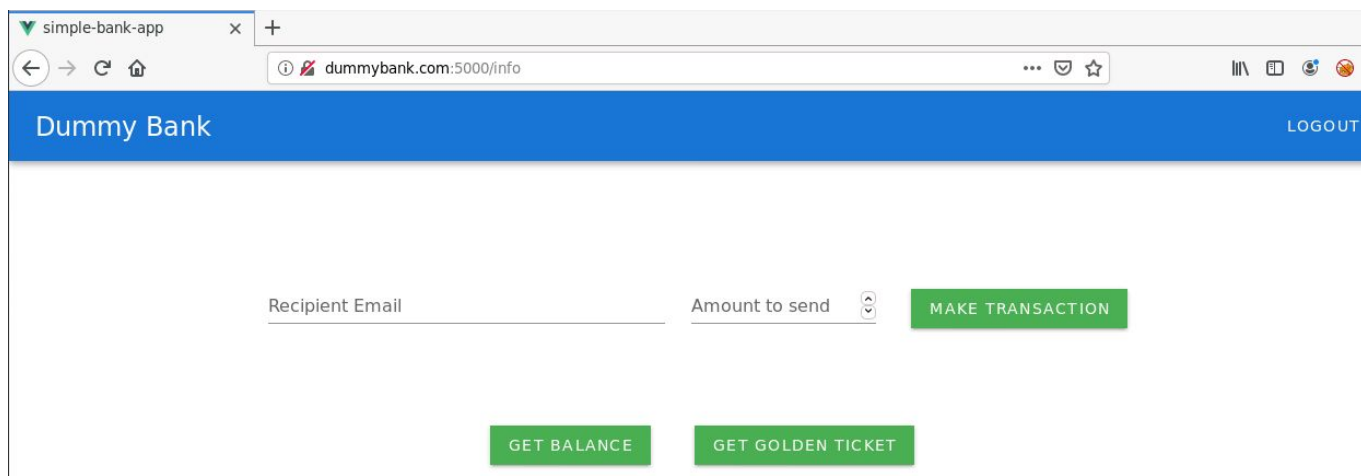
When the lab is launched, the Banking WebApp is opened in Firefox.



Step 1: Login into the Banking WebApp using the provided credentials.

Email: jake@dummybank.com

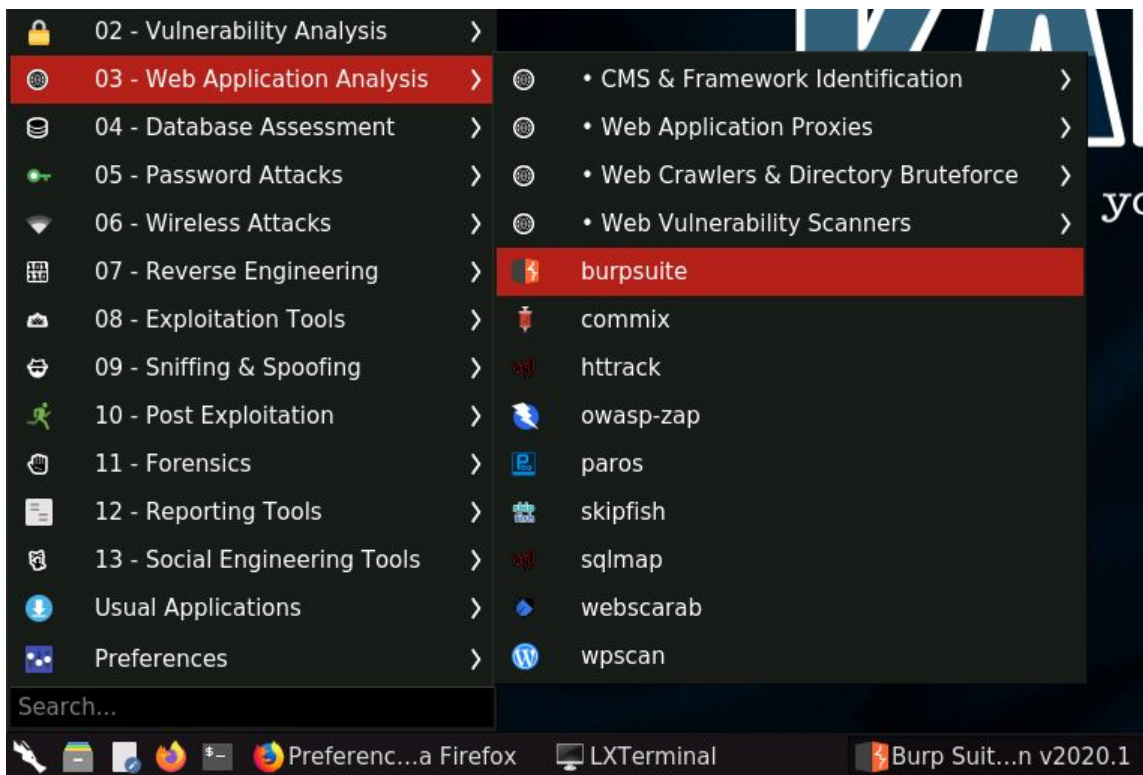
Password: s1mpl3p@s5w0rd



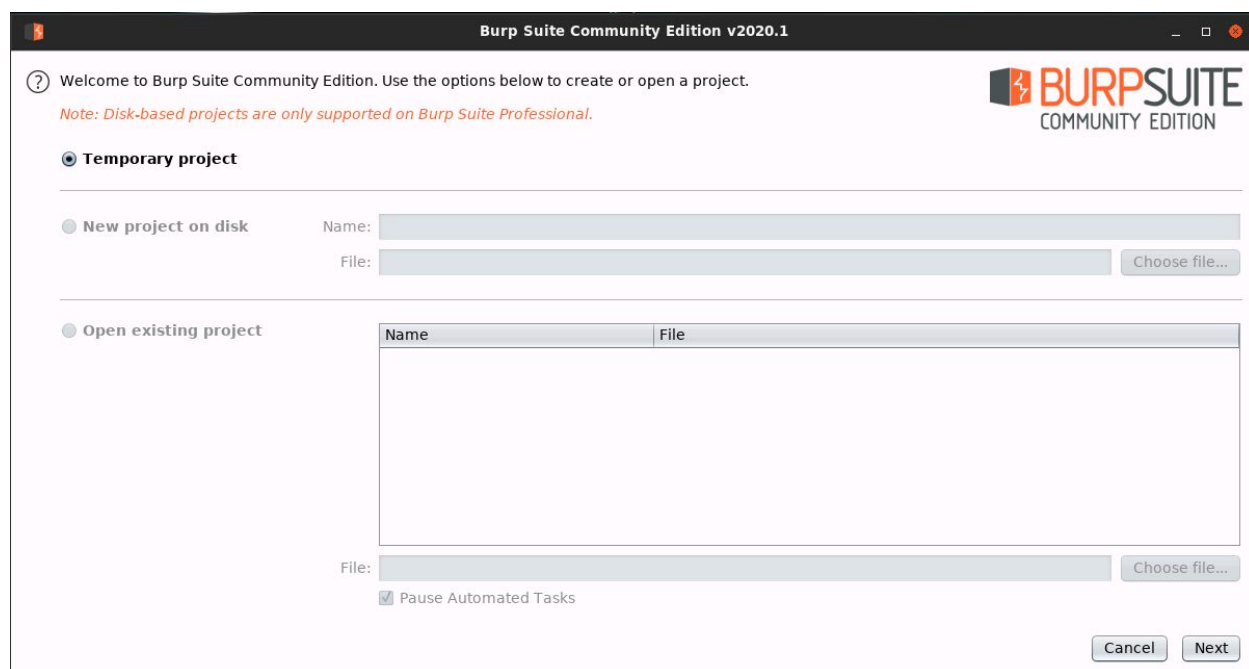
Step 2: Configuring the browser to use BurpSuite proxy and making BurpSuite intercept all the requests made to the API.

Launch BurpSuite.

Select Web Application Analysis > burpsuite

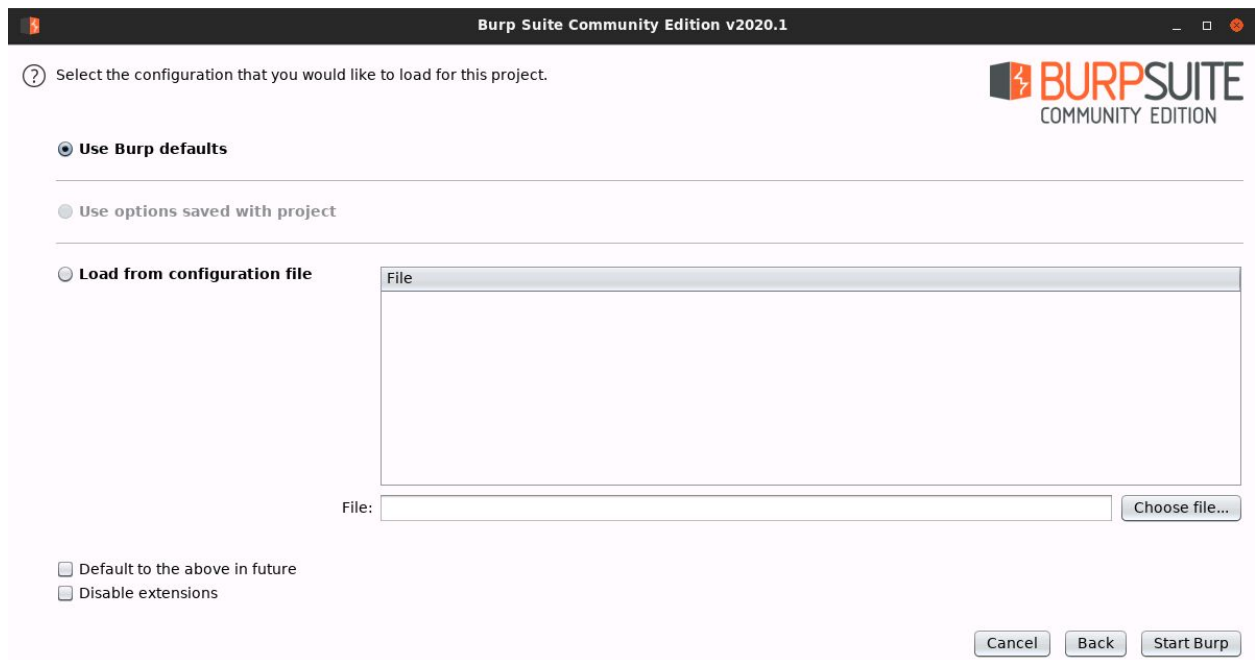


The following window will appear:

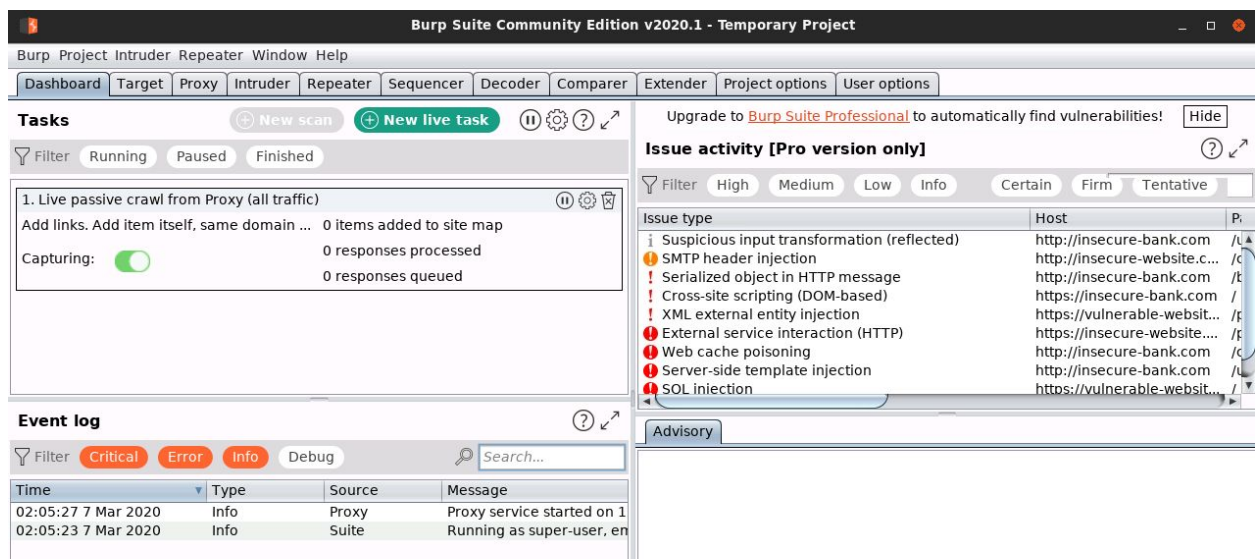


Click Next.

Finally, click Start Burp in the following window:

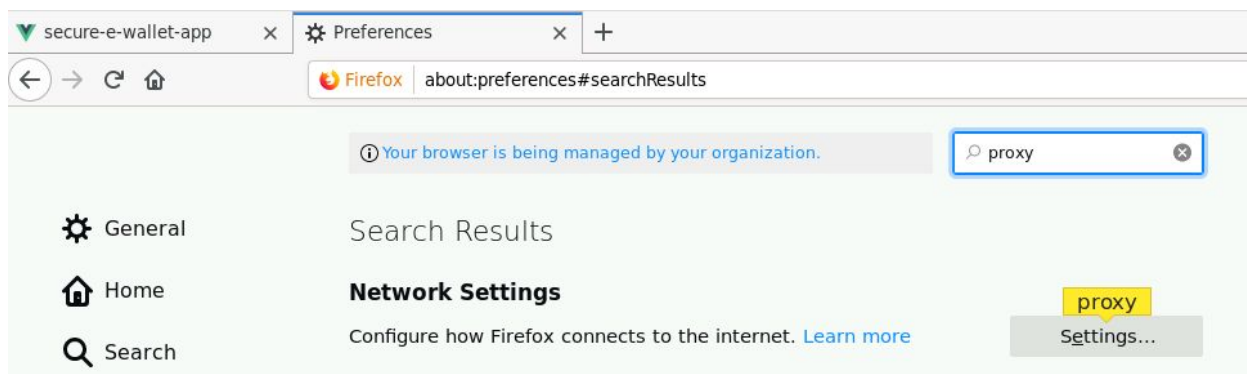


The following window will appear after BurpSuite has started:

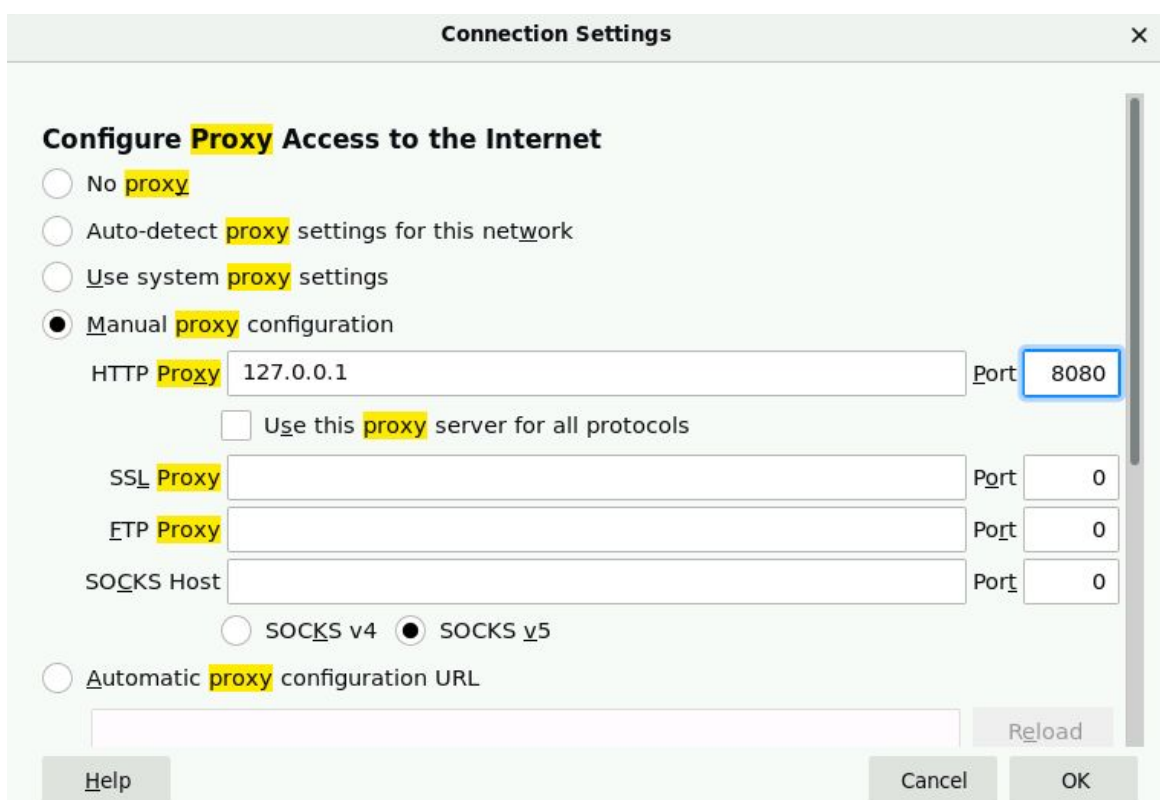


Configure the browser to use the Burp proxy listener as its HTTP Proxy server.

Open the browser preference settings and search for network proxy settings.

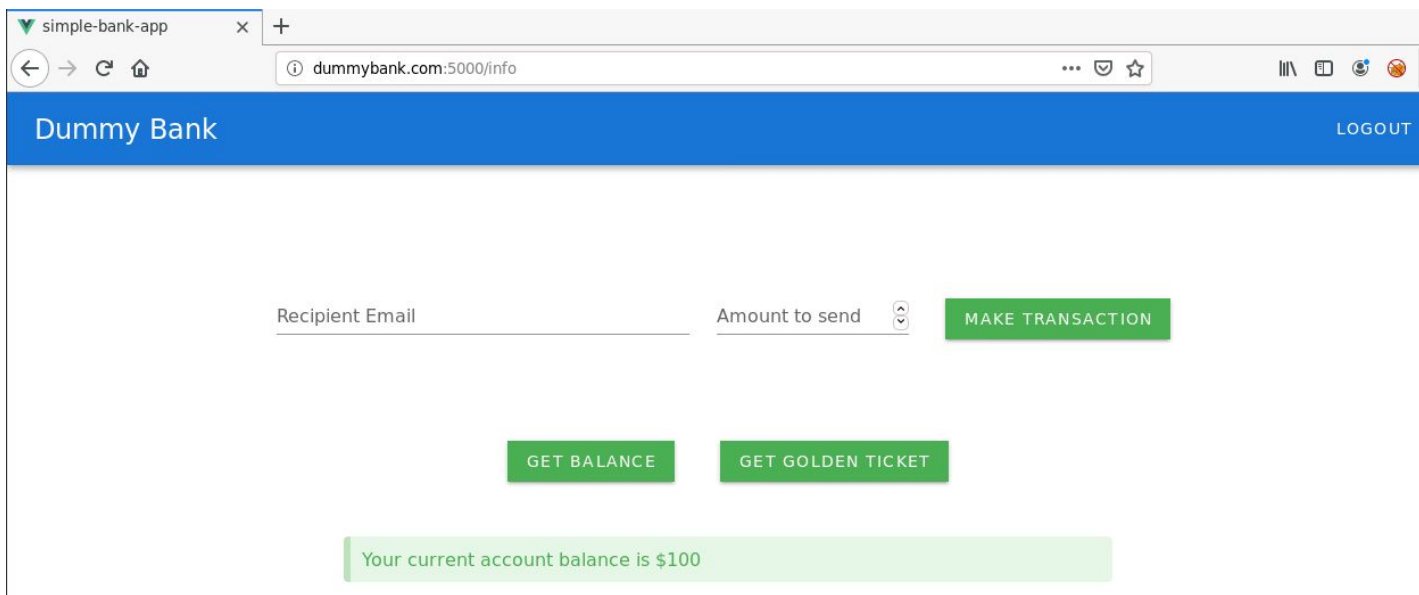


Select Manual Proxy Configuration and set the HTTP Proxy address to localhost and the port to 8080.



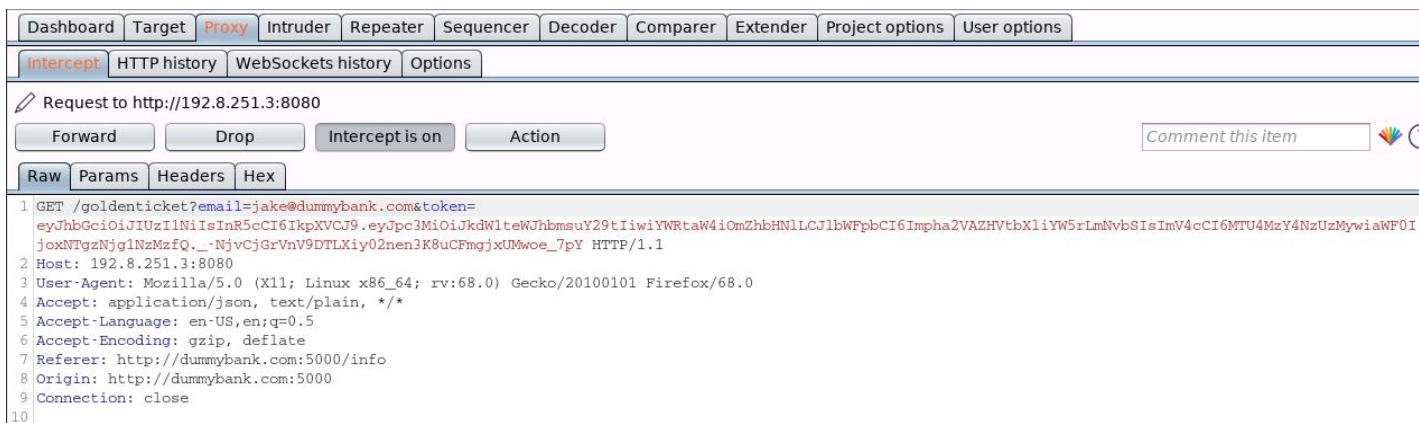
Click OK.

Everything required to intercept the requests has been set up.



The current account balance is \$100.

Retrieving the Golden Ticket:



Forward the above request and check the response on the web page.

simple-bank-app x +

dummybank.com:5000/info

Dummy Bank LOGOUT

Recipient Email Amount to send MAKE TRANSACTION

GET BALANCE GET GOLDEN TICKET

Your current account balance is \$100

Balance must be > \$5000 to get the Golden Ticket!

The Golden Ticket couldn't be retrieved due to insufficient bank balance.

Transferring funds to Bob's account:

simple-bank-app x +

dummybank.com:5000/info

Dummy Bank LOGOUT

Recipient Email Amount to send MAKE TRANSACTION


bob@dummybank.com 1

GET BALANCE GET GOLDEN TICKET

Your current account balance is \$100

Balance must be > \$5000 to get the Golden Ticket!

Make this request to transfer \$1 to Bob's account.



The web page shows that the transaction was successful.

Checking the balance again:

So, now the account balance is \$99.

As it is mentioned in the challenge description that the backend server does not validate the transferred amount, a negative amount could be transferred which in turn would actually increase the balance of Jake's (current logged in) account.

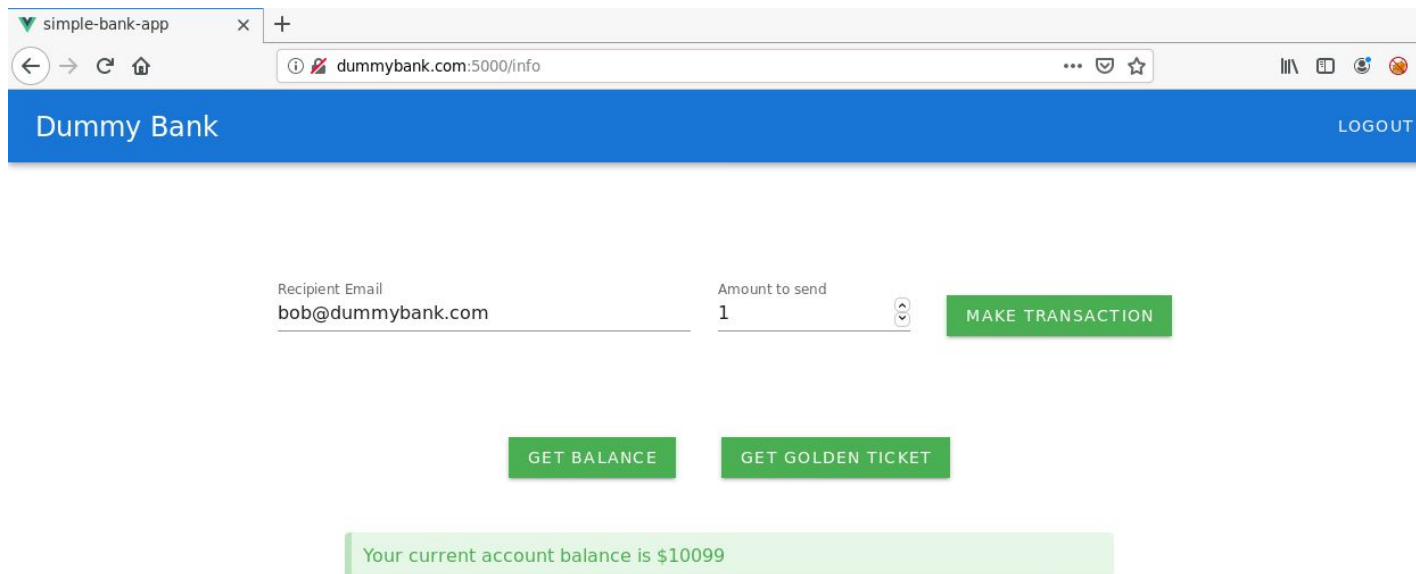
Step 4: Leveraging the issue to transfer funds from Bob's account.

Set the transfer amount to a negative value to transfer the money from Bob's account.

Send the request in Repeater after modifying the amount to be transferred (balance parameter in the POST request payload).

The transaction was successful.

Check the updated balance.



simple-bank-app x +

dummybank.com:5000/info

Dummy Bank LOGOUT

Recipient Email
bob@dummybank.com

Amount to send
1

MAKE TRANSACTION

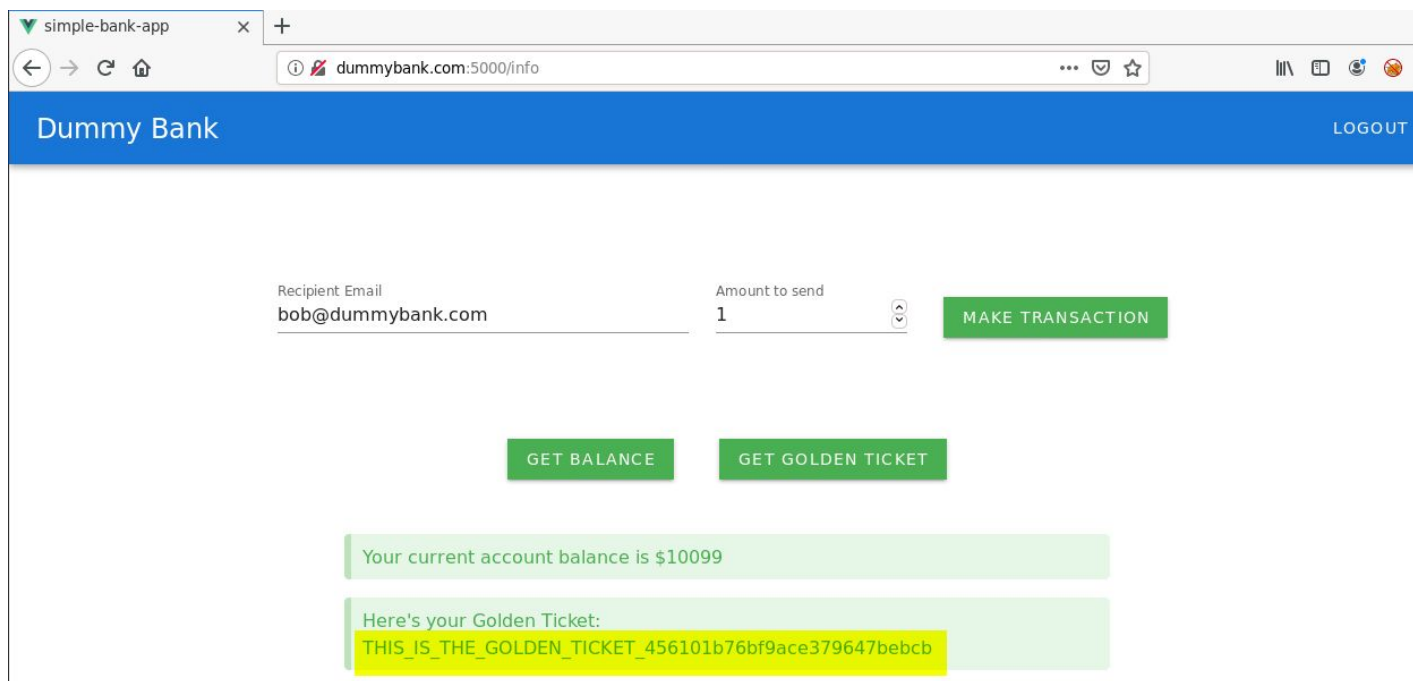
GET BALANCE GET GOLDEN TICKET

Your current account balance is \$10099

So, the server didn't check if the amount transferred was positive and that transaction resulted in the funds being transferred from Bob's account to the current account.

The updated balance exceeds \$5000. So now the Golden Ticket could be retrieved.

Step 5: Retrieving the Golden Ticket.



Golden Ticket: THIS_IS_THE_GOLDEN_TICKET_456101b76bf9ace379647bebcbb

References:

1. JWT debugger (<https://jwt.io/#debugger-io>)