Kalle Jalkanen AB8822 TTV21S2
time used: 2 hours

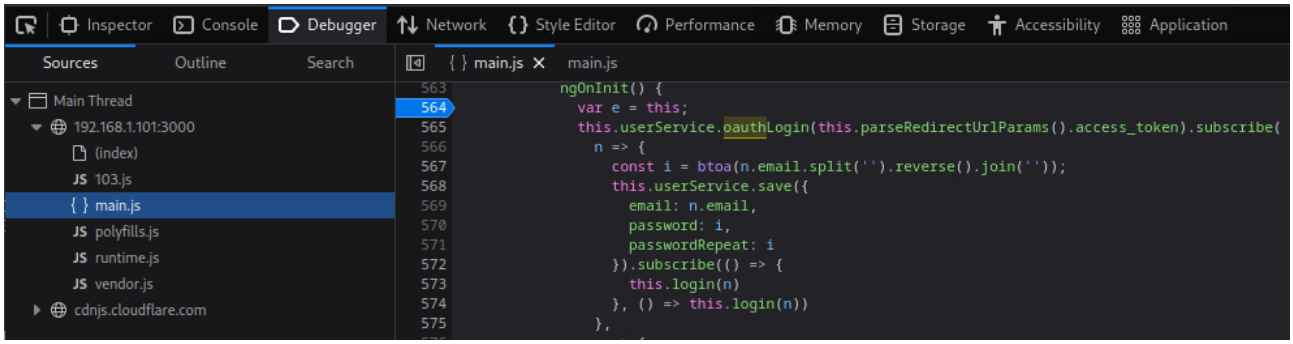
# Juice Shop - Login Björn

## Description

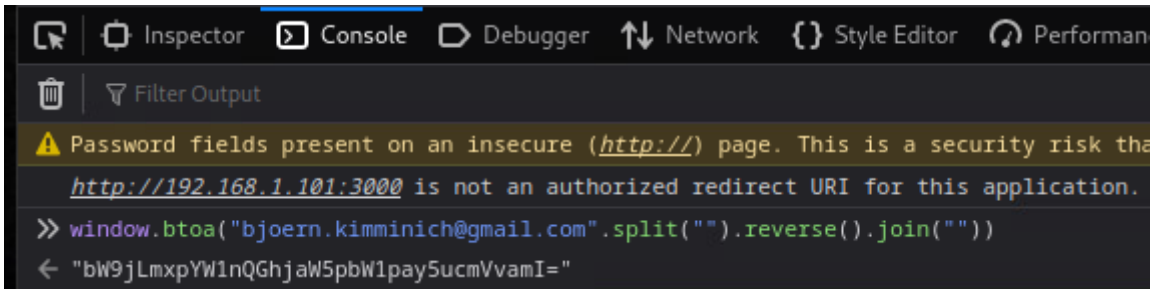
Attacker can get user passwords because of poor OAuth.

## Steps to produce

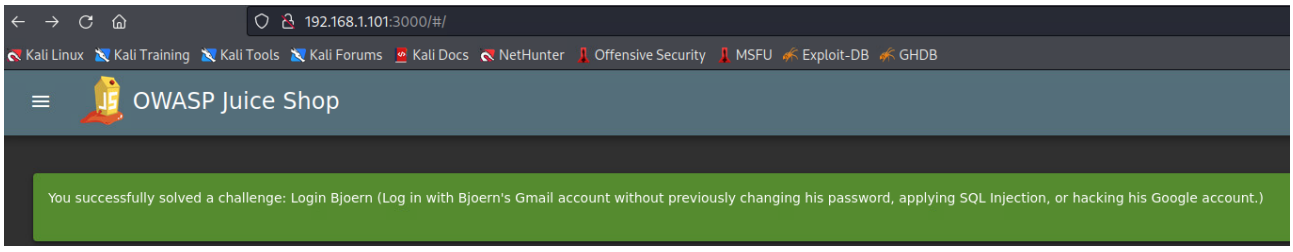
Press F12 to open dev tools and go to debugger tab. There select main.js and search ‘oauth’. Password uses variable ‘i’ witch reverses email address and encodes it to base64.




Then go to console tab and make that email encrypt variable.
‘window.btoa("bjoern.kimminich@gmail.com".split("").reverse().join(""))’




Now go to login page and use Bjoern’s email and that encoded password we just created.
‘bW9jLmxpYW1nQGhjaW5pbW1pay5ucmVvamI=’




## Impact estimation

Medium severity. With this attacker can get sensitive information like customers addresses. It has low severity first but affects peoples trust to the company and by that it may have bigger impact.

### Mitigation

Passwords should be stored securely using strong encryption mechanisms, such as bcrypt or Argon2. They should never be manipulated in ways that can be easily reversed.

## Main target - Missing Authentication for Critical Function

### Description

Deleting products does not need authentication, so anyone can delete them.

### Steps to produce

Open command line and use curl command. End of the URL put the product number you want to delete. ‘curl ‘http://wasdat.fi/product/10’ -X DELETE’


### Impact estimation

Low severity. This will only do damage for a short period of time until the vulnerability is patched and the products are added back to the online store.

### Mitigation

Implement authentication and authorization mechanisms to ensure that only authorized users can delete products.