

# Broken access control

## hidden html

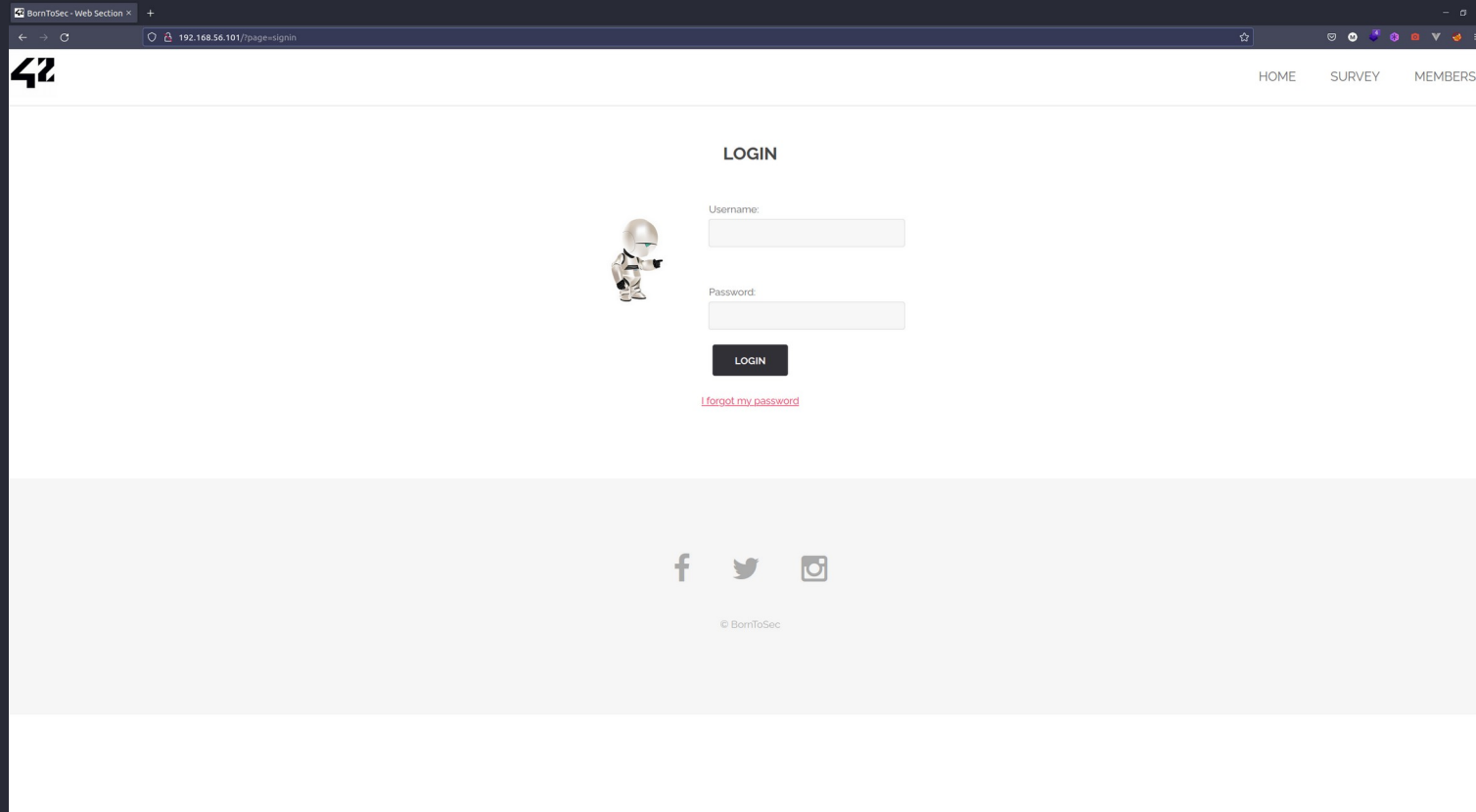
Moving up from the fifth position, 94% of applications were tested for some form of broken access control with the average incidence rate of 3.81%, and has the most occurrences in the contributed dataset with over 318k. Notable Common Weakness Enumerations (CWEs) included are CWE-200: Exposure of Sensitive Information to an Unauthorized Actor, CWE-201: Insertion of Sensitive Information Into Sent Data, and CWE-352: Cross-Site Request Forgery.

Access control enforces policy such that users cannot act outside of their intended permissions. Failures typically lead to unauthorized information disclosure, modification, or destruction of all data or performing a business function outside the user's limits.

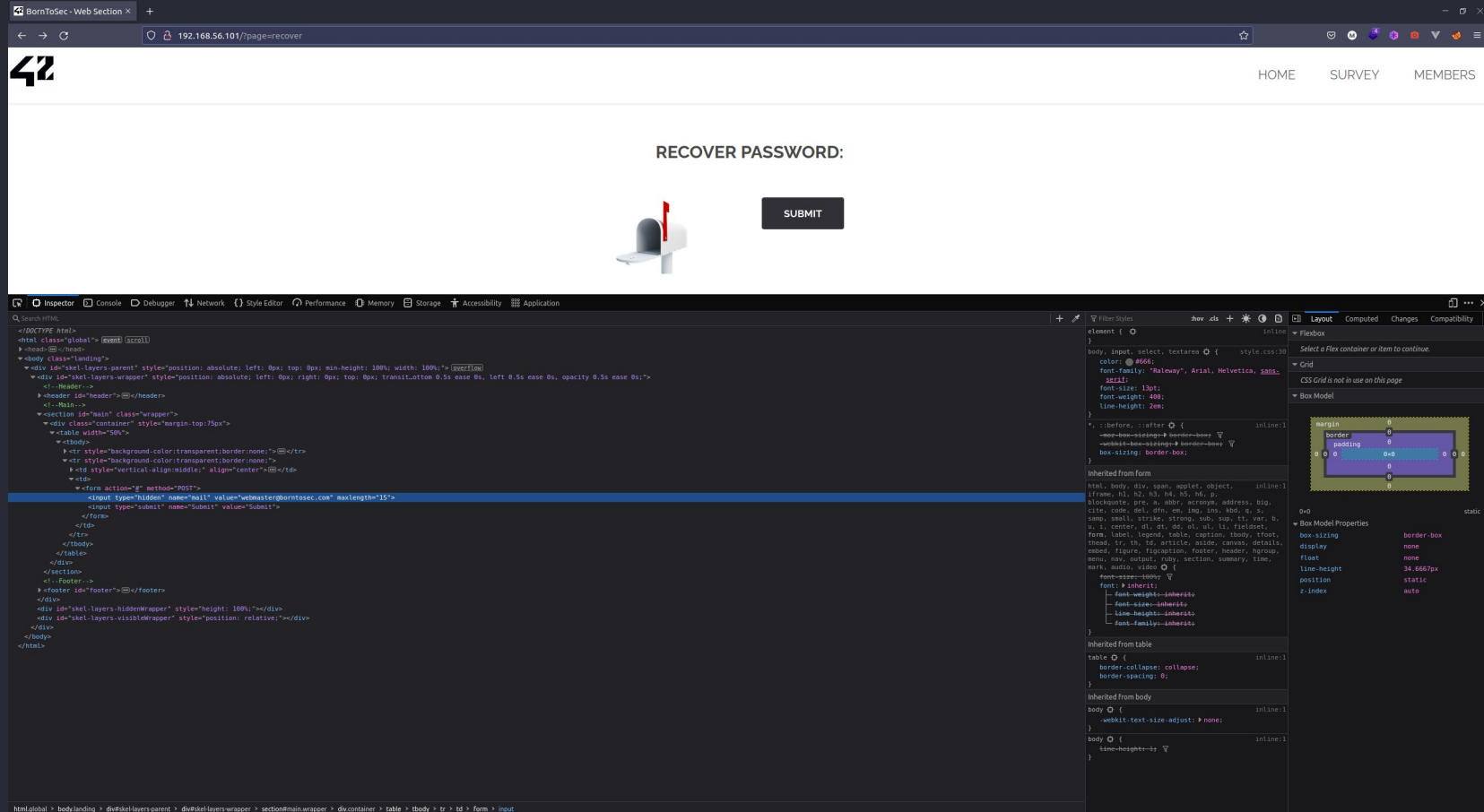
In this context we talk about an hidden html tag

# Walk through

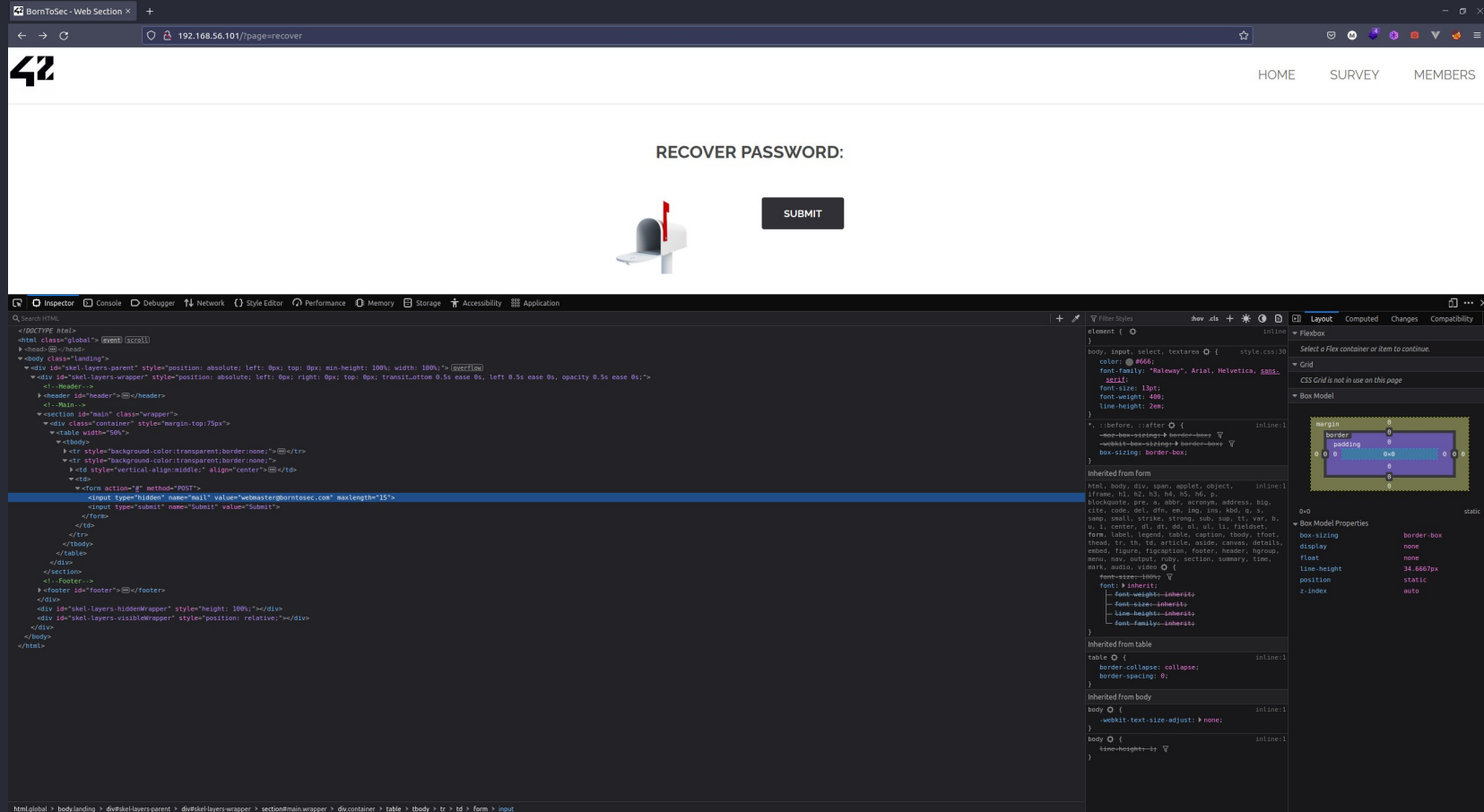
Step 1 : Click on the 'I forgot my password' link on the login page



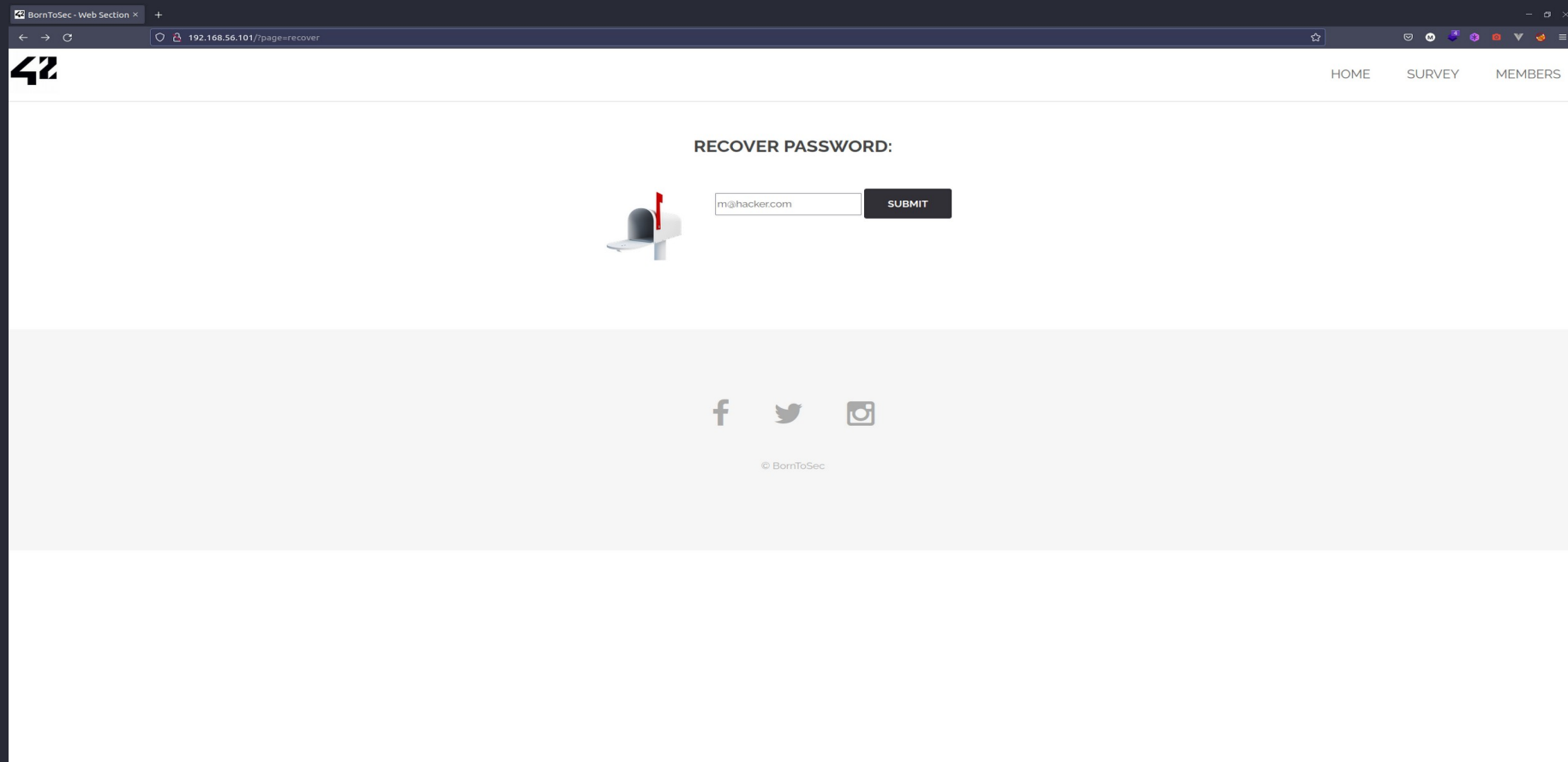
Step 2 : Open the code inspector in the devtools we saw an html tag with a type hidden try to delete the hidden property



Step 3 : we find an input tag with the webmaster email, change by your email



Step 4 : click on the submit button with the new mail



## Step 5 : Get the flag !


BornToSec - Web Section x

192.168.56.101/?page=recover#


42

HOME SURVEY MEMBERS

THE FLAG IS : 1D4855F7337C0C14B6F44946872C4EB33853F40B2D54393FBE94F49F1E19BBB0



RECOVER PASSWORD:



SUBMIT

f t i

© BornToSec

# How to fix

- Delete the hidden html tag from the codebase and send the mail to the webmaster in backend
- Log the lost password requests in an admin page