

Broken Access Control

Frontend validation

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 input invalidated

Walk through

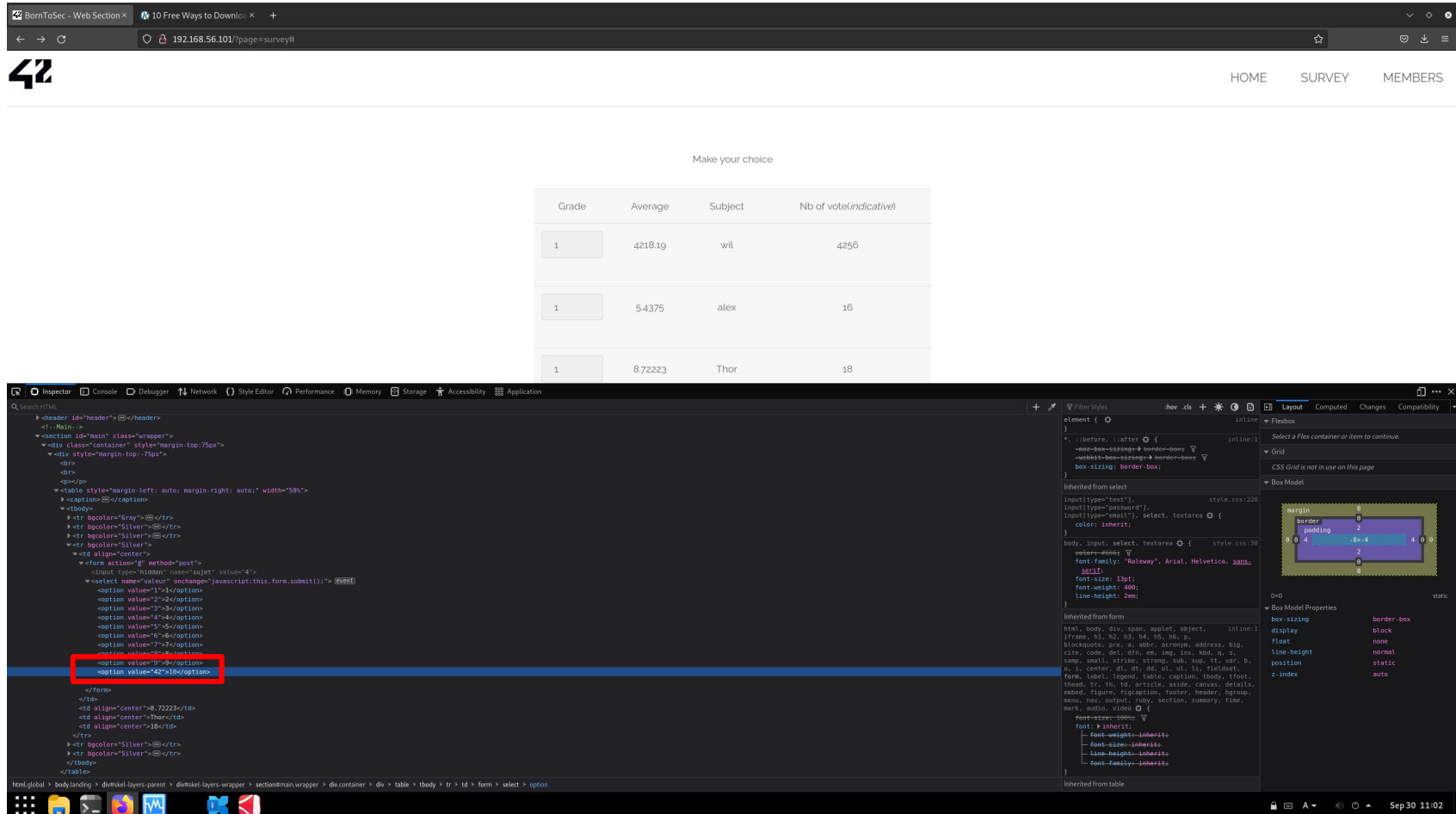
Step 1 : Inspect the code source of the survey page

The screenshot shows a web browser with the URL `192.168.56.101/?page=survey#`. The page features a navigation bar with links for `HOME`, `SURVEY`, and `MEMBERS`. Below the navigation bar, there is a section titled "Make your choice" containing a table with the following data:

Grade	Average	Subject	Nb of vote(indicative)
1	4218.19	wil	4256
1	5.4375	alex	16
1	8.72223	Thor	18

The bottom half of the image displays the browser's developer tools. The `Inspector` panel shows the HTML structure, with the `tbody` of the table selected. The `Styles` panel on the right shows the default browser styles for the `tbody` element, including `margin-top: 7px`, `border: 1px solid black`, and `border-bottom: 1px solid black`. The `Layout` panel on the right shows a visual representation of the element's box model, with dimensions of 1400x956 pixels.

Step 2 : Try to change the value of the grade inputs (option tag in the select form) to an negative note or a note > 10



Step 3 : Submit the changed notes and get the flag !


BornToSec - Web Section x10 Free Ways to Downlo... x+

← → ↻ 192.168.56.101/?page=survey# ☆ 📄 ⌵ ⌵ ⌵

42

HOME SURVEY MEMBERS


THE FLAG IS 03A944B434D5BAFF05F46C4BEDE5792551A2595574BCAFC9A6E25F67C382CCAA




Make your choice

Grade	Average	Subject	Nb of vote(indicative)
<input type="text" value="1"/>	4218.19	will	4256
<input type="text" value="1"/>	5.4375	alex	16
<input type="text" value="1"/>	8.72223	Thor	18
<input type="text" value="1"/>	9.1	Ben	666
<input type="text" value="1"/>	6.969	ol	69

Your voice is important for us !!!





How to fix

- Make a validation in backend for the grade don't accept it if $(0 > \text{grade} > 10)$