AJAX - Insecure Client Storage

Friday, October 20, 2017 7:48 AM

- It's always good practice to validate all input on the server side
- Leaving the mechanism for validation on the client side leaves it vulnerable to reverse engineering
  - Remember: anything on the client side should not be considered a secret

Solution

- Need a plugin that is capable of debugging JavaScript (firebug was one such plugin: no longer supported)
- Open clientSideValidation.js in the debugger
- Toggle a breakpoint on the line: decrypted = decrypt(coupons[i]);
- Enter a character in the coupon code field of the website
  - The JavaScript gets executed but stops at a breakpoint
  - The right side of the debugger shows the parameters and their values
- Use the step over symbol or F10
- Now you can read the clear text of decrypted to obtain the decrypted coupon code

For the next part you can inspect the HTML element and remove the readonly attributes.
Then, you can buy as many items as you want and change the price to 0 in the text box under total.