AJAX - Dangerous Use of Eval

Friday, October 20, 2017 8:36 PM

- It is always good practice to validate all input on the server side.
- XSS can occur when unvalidated user input is reflected directly into an HTTP response

Here, unvalidated user input is used in conjunction with a JavaScript eval() call

- In a reflected XSS attack, an attacker can craft a URL with the attack script and it on another website, email it, or otherwise trick a victim into clicking on it

Solution

If you inspect element on the digit access code input field and Purchase button, you will noticed that it takes input from the user and places it directly in a JavaScript eval() function.
For this reason, the attack does not require the <script> tags.

- Because of this implementation, we are able to enter 123');alert(document.cookie);('
  - Directly into the form field to carry out our attack
- Here, we executed alert(document.cookie);('
  - But really we could've inserted any malicious JavaScript code we wanted to here
  - We could call malicious JS code from other websites even