AJAX - DOM Injection

Wednesday, October 18, 2017 9:49 PM

How to perform DOM injection attacks

- Some applications, especially the ones that use AJAX, manipulate and update the DOM directly using JavaScript, DHTML and eval() method
- An attacker may take advantage of that by intercepting the reply and try to inject some javascript commands to exploit the application

- AJAX requires XML communication between the browser and the web application
  - When you view the source of the HTML page, you will notice the usage of XMLHttpRequest

Solution

Inspect element on the button and edit the HTML to activate it

- You can also use WebScarab to intercept the request/response and edit the JavaScript (document.form.SUBMIT.disabled = false;) to enable the button