Cybersecurity Homework

Jeffrey Simpson
March 2th, 2020

Issue 1

The first issue is that the page has at least one script that is from a third-party domain (cloudfare). It is best to ensure that JavaScript source files are loaded from trusted sources and can't be controlled by the end user.

Issue 2

According to the ZAP report, the web browser XSS Protection is either not enabled or is disabled by the configuration of the 'X-XSS-Protection' HTTP response header on the web server. Simply setting the X-XSS-Protection HTTP response header to '1' will ensure that the web browser's XSS filter is enabled.

Issue 3

A private IP or an Amazon EC2 private hostname is in the HTTP response body. Information like this can be useful for further attacks on internal systems and should be removed from the HTTP response body. If the information is in a comment, a JSP/ASP/PHP comment should be used because it can't be seen by the user.

Some other tools, DAST tools, that could be used to find vulnerabilities in a web app are AppScan by IBM, Vega by Subgraph, and Ride by Adobe. There are tons of these tools at a programmer's (or anybody's) disposal and OWASP has a pretty comprehensive list of them on their website.