TASK 2 (Report)

The website **http://zero.webappsecurity.com/** has some vulnerabilities in it. I have found three vulnerabilities in it to be specific. These three are as follows:

1. The anti-clickjacking X-Frame-Options header is not present.
2. The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS.
3. The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type.

These vulnerabilities can be harmful for the website and the users both as this can be used by attackers to any kind of attack. As this can give the attacker the access of database as well as protected information. Which attacker can use to blackmail someone or can sell this information in any hand for money. The user privacy will be breached and will lead to a not secure website.

Steps used:

1. Operating System used was Linux.
2. Software used was Nikto.
3. So after starting nikto we used the command : nikto -host <http://zero.webappsecurity.com/>
4. -host command in nikto is used to perform automatic scanning on target website.
5. Then it automatically displays all the vulnerabilities found.

