PRACTICAL-3

AIM:

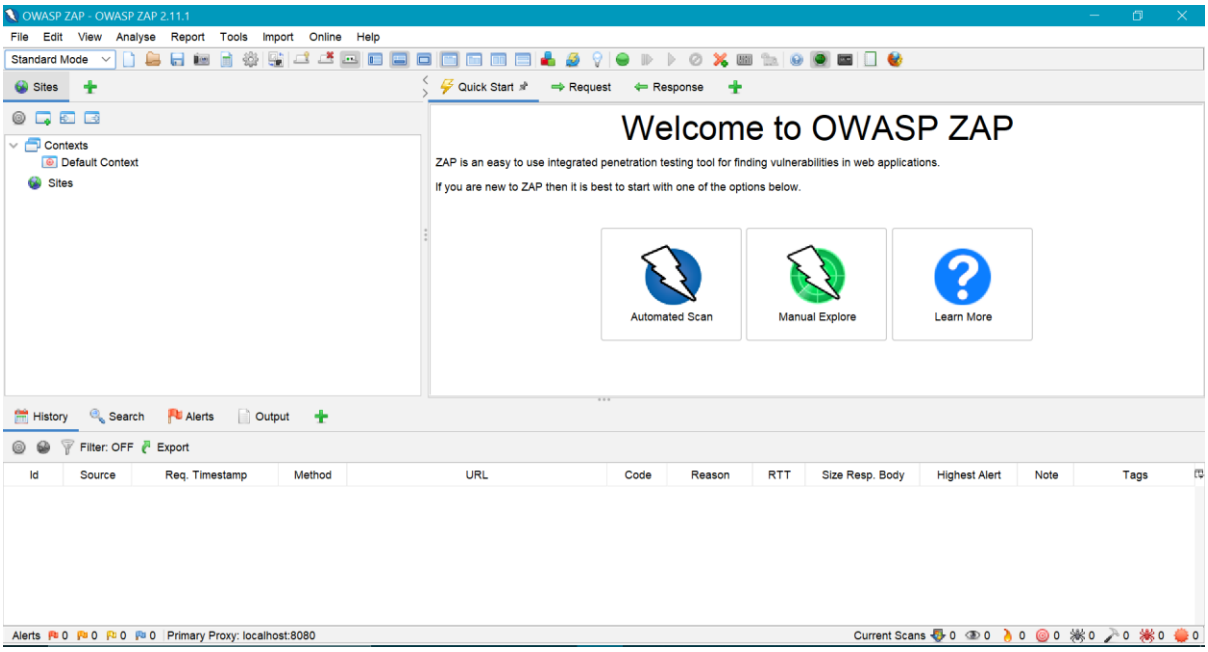
Implementation to identify web vulnerabilities, using OWASP project

THEORY:

- OWASP stands for “Open Web Application Security Project”.
- It is an open, online community that creates methodologies, tools, technologies and guidance on how to deliver secure web applications.
- OWASP ZAP (ZAP) is one of the world’s most popular free security tools and is actively maintained by hundreds of international volunteers. It can help to find security vulnerabilities in web applications. It’s also a great tool for experienced pen testers and beginners.
- ZAP is what is known as a “man-in-the-middle proxy.” It stands between the browser and the web application. While you navigate through all the features of the website, it captures all actions. Then it attacks the website with known techniques to find security vulnerabilities.
- It is one of the most active Open Web Application Security Project (OWASP) projects and has been given Flagship status.
- When used as a proxy server it allows the user to manipulate all of the traffic that passes through it, including traffic using https.
- It can also run in a daemon mode which is then controlled via a REST API.
- ZAP was added to the ThoughtWorks Technology Radar in May 2015 in the Trial ring.
- ZAP was originally forked from Paros, another pentesting proxy. Simon Bennetts, the project lead, stated in 2014 that only 20% of ZAP's source code was still from Paros.

IMPLEMENTATION:

- Starting ZAP
- Once setup you can start ZAP by clicking the ZAP icon on your Windows desktop or from the start menu.



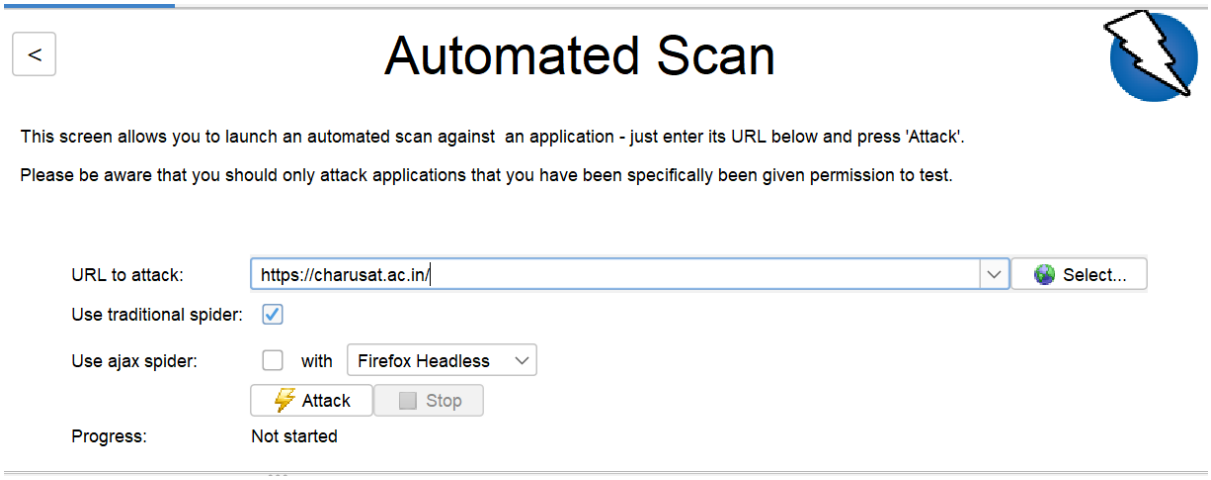
Glimpses of ZAP Console

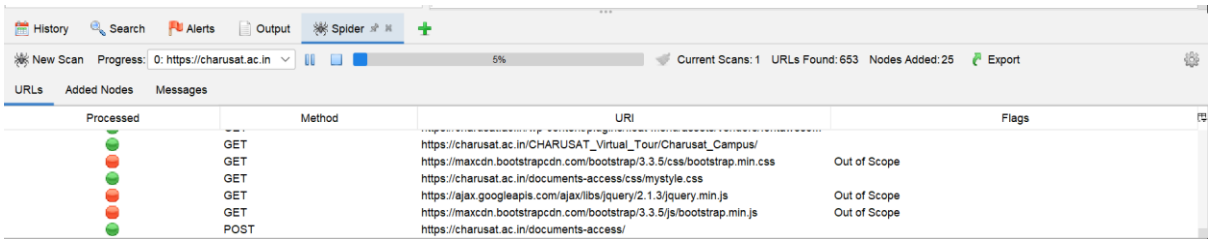
- Spidering the web application
- Spidering a web application means crawling all the links and getting the structure of the application. ZAP provides two spiders for crawling web applications;
- The traditional ZAP spider discovers links by examining the HTML in responses from the web application. This spider is fast, but it is not always effective when exploring an AJAX web application.
- This is more likely to be effective for AJAX applications. This spider explores the web application by invoking browsers which then follow the links that have been generated. The AJAX spider is slower than the traditional spider.

Automated scan

- This option allows you to launch an automated scan against an application just by entering the URL. If you are new to ZAP, it is best to start with Automated Scan mode.
- To run a Quick Start Automated Scan:

1. Start Zap and click the large 'Automated Scan' button in the 'Quick Start' tab.
2. Enter the full URL of the web application you want to attack in the 'URL to attack' text box.
3. Click the 'Attack' button.

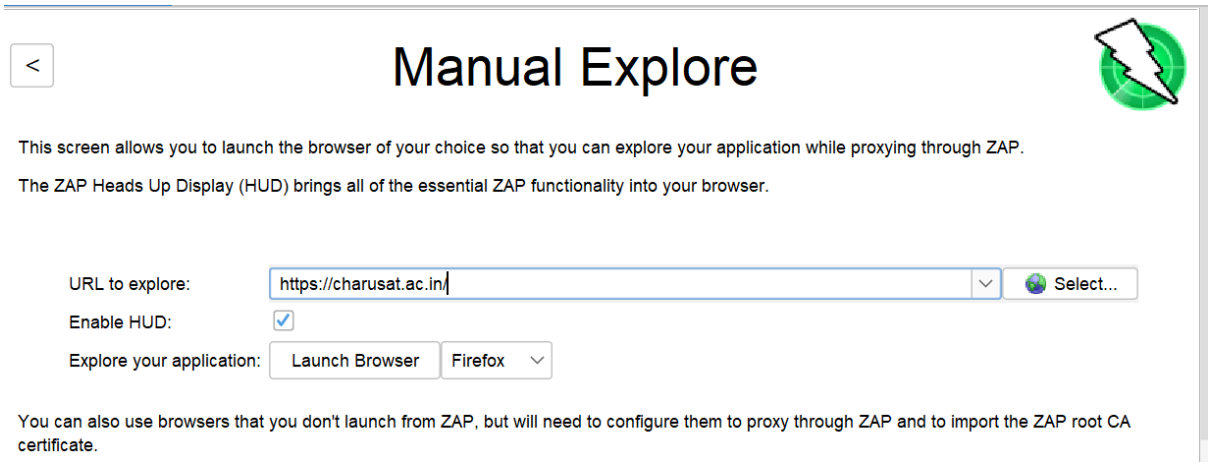




Crawling started

- Once you click the 'Attack' button, ZAP will start crawling the web application with its spider and passively scan each page it finds. Then ZAP will use the active scanner to attack all of the discovered pages, functionality and parameters.

- Exploring the web application manually
- Spiders are a great way to explore the basic site, but they should be combined with manual exploration to be more effective. This functionality is very useful when your web application needs a login or contains things like registration forms, etc.
- You can launch browsers that are pre-configured to proxy through ZAP via the Quick Start tab. Browsers launched in this way will also ignore any certificate validation warnings that would otherwise be reported.



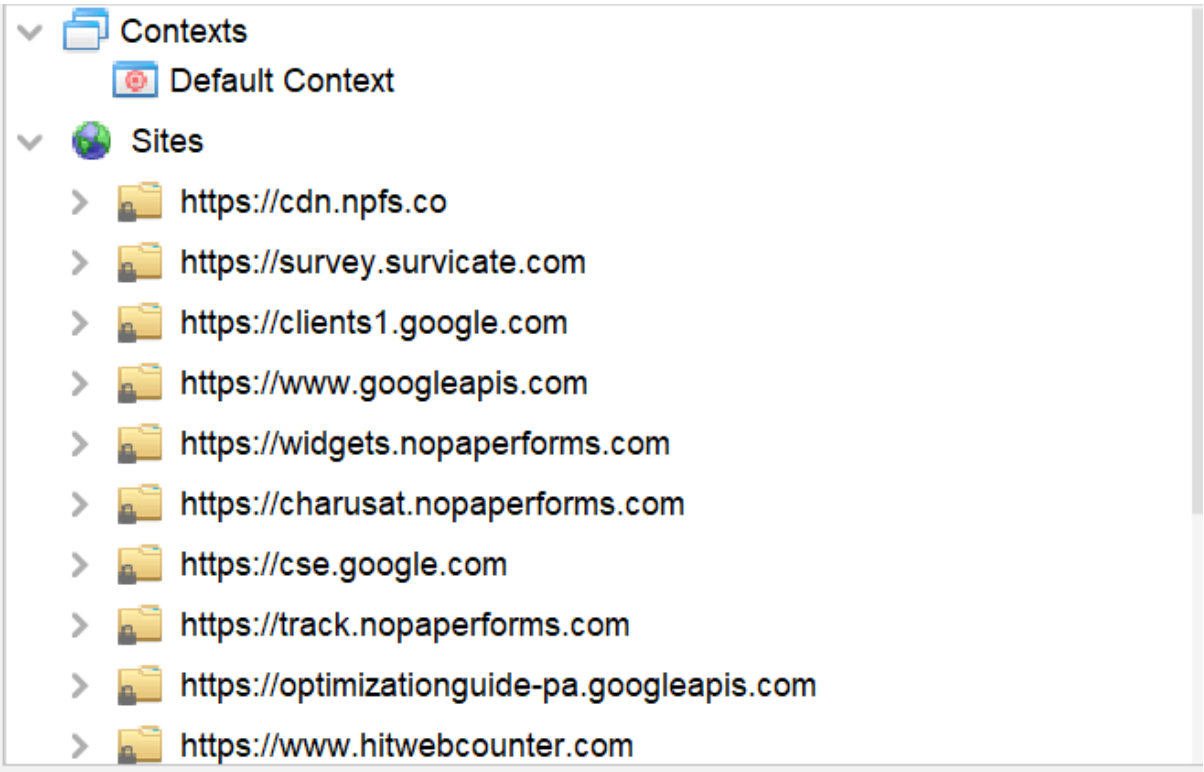
- To Manually Explore the web application:
- Start ZAP and click on the large ‘Manual Explore’ button in the Quick Start tab.
- Enter the full URL of the web application to be explored in the ‘URL to explore’ text box.
- Select the browser you would like to use and click the ‘Launch Browser’ button.
- This will launch the selected browser with a new profile. Now explore all of the targeted web applications through this browser.
- ZAP passively scans all the requests and responses made during your exploration for vulnerabilities, continues to build the site tree, and records alerts for potential vulnerabilities found during the exploration.

What is passive scanning?

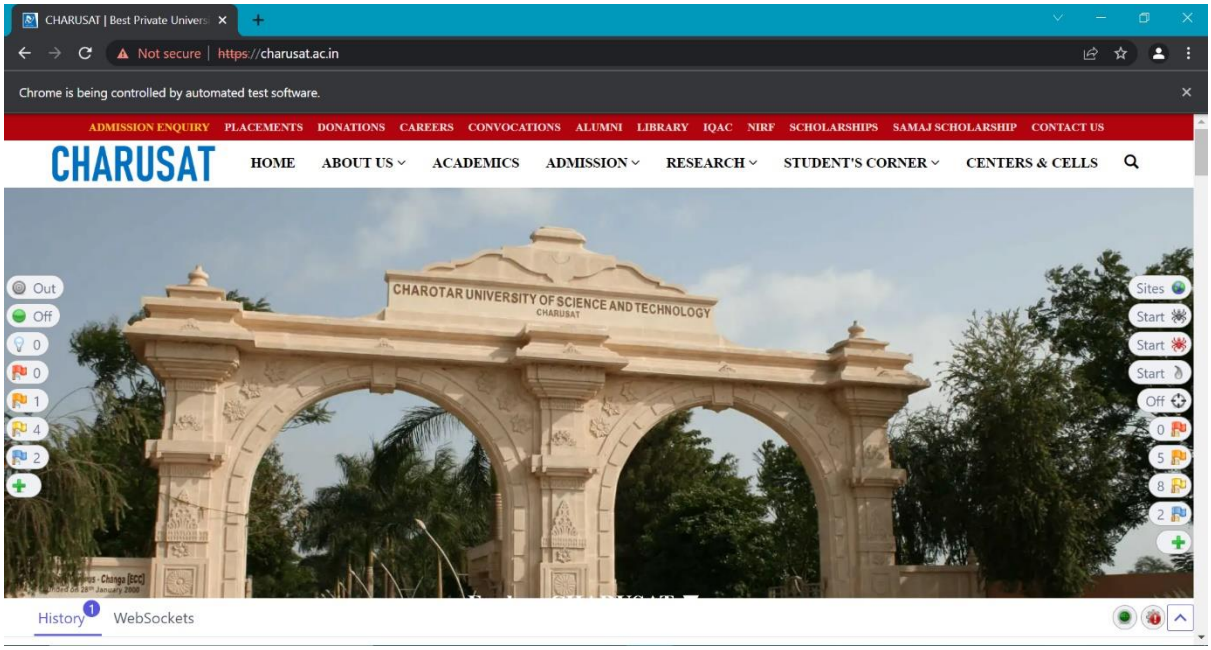
- Passive scans only scan the web application responses without altering them.
- It does not attack or insert malicious scripts to the web application, so this is a safe scan; you can use it if you are new to security testing.
- Passive scanning is good at finding some vulnerabilities and as a way to get a feel for the basic security of a web application.

What is active scanning?

- Active scan attacks the web application using known techniques to find vulnerabilities. This is a real attack that attempts to modify data and insert malicious scripts in the web application.



Sites updated



Manual scanning initiated

- We will not proceed as we are not allowed to scan the website.

CONCLUSION:

- In this practical, we learnt about how ZAP spiders the web application under test and scan for any known vulnerabilities.