week - 05

1. Using the Microsoft Threat Modeling methodology, execute a threat model for a given application architecture using Microsoft threat Modeling tool.

Microsoft Threat Modeling Tool 2016 is a tool that helps in finding threats in the design phase of Software Projects.

Microsoft Threat Modeling Tool applies STRIDE threat classification scheme to the identify threats.

Steps to install & Configure the Threat Modeling Tool:

Step 1:- Download Microsoft Threat modeling tool and install

Step 2:- Open the application and click on "Create an model" Option to get started with the threat analysis.

Step 3:- Then create a threat model of any web application (Design)

Step 4:- To see the threats of an designed web application, "click on View" then "Analysis View" the threat list will open click any threats to see the "Threat Properties".

Step 5:- Now generate a report, click on "Reports" Select "Create a file Report"; Set a "Name" to it the report will be saved in .html file. Open that file and you will see the total report of threat Modeling.

Teacher's Signature:

2] Write the steps to install OWASP ZAP and automated & Manual scan.

OWASP ZAP is an open-source free tool & is used to perform penetration test.

The main goal of ZAP is to allow easy penetration testing to find the vulnerability in web application.

Download and Install OWASP ZAP In Kali:

Step 1:- Download OWASP ZAP application from ZAPproxy website.
Step 2: Open the browser and search "Download OWASP ZAP"
Step 3:- click on First link and Select the "Linux installer" and download it.
Step 4: After downloading it will downloaded as a ".sh" file to install open command prompt copy that ".sh" and Type $ Sudo bash paste that file (Sudo bash ZAP 2.0.12.0 unix.sh) click on enter and the is installed successfully.

Automate Scan:

Step 1:- open OWASP ZAP application.
Step 2: Select the "Automate Scan" and paste the Vulnerable website URL (eg: Altoromutual") and click on attack.
Step 3: Run a spider scan to traverse all paths in the website.

Teacher's Signature:

Step 4:- Once the Spider Scan is completed the Active Scan is Start.

Step 5:- Now click on "Alerts" section and Analyze the type of risk which was exposed by Automated Scan.

To Manual Scan:

Step 1:- Open OWASP ZAP.

Step 2:- Select the "Manual Scan" and Paste the Vulnerable website URL and click on "Attack".

Step 3:- Here the ZAP browser will open we can Start the Scanning manually in various type.

To Generate a Report:

Step 1:- In OWASP ZAP After completing Scans click on "Report".

Step 2:- Select the "Generate Report". you will see the report of that vulnerability of application or website.

Teacher's Signature:

EXPT. NO. | NAME | Page No.: 32 | Date: | YOUVA

M T W T F S S

3]. Analysis the vulnerbile website using OWASP ZAP and add a False Positive Generate a Report. or execute a Report.

A False Positive error, is a result that indicates a given condition exists when it does not.

Using OWASP ZAP Scan the Altoro Mutual web site and adding a false Positive.

Steps:-

Step 1:- Open the OWASP ZAP application.

Step 2:- Scan the "Altoro Mutual" web site.

Step 3:- Click on "Alerts" and daubl tap on any vulnerbile file. Click on "Confidence" and "choose" "False Positive" or click on "Save".

Step 4:- To Generate a Report of False Positive. Click on "Generate" and Select the "False Positive" in "Filter" Click on Save or "Generate".

Step 5:- To view the False Positive Report click on "Confidence -- False Positive" option you can view.

Teacher's Signature: