VIT | Vidyalankar Institute of Technology

"Finding Faults and Protecting Web Application Using Open Source Tools"

by Dr. Dilip Motwani, Associate Professor, Vidyalankar Institute of Technology
online lecture held on 18th September 2020, 5.30 PM

Today everyone uses various Web Applications for different purposes like Banking, E-Commerce, E-mails etc. But during the use of all such web applications, security of personal information is at stake. Attackers tend to find bugs as well as errors in the web application to attack the websites and web applications are many a times at risk. Dr. Motwani discussed various facts about web application designs, protection criteria and tool kits used for the purpose.

Event Insights

Working of Web Applications

In web applications the first layer is of the Browser from where the user can fire the query, then comes the open network i.e., the Internet through which we send the http request from where it traverses to the web servers, scripting engines, database servers etc. Since, the user has access only till web server, the attacker is prone to attack the application.

Flow of Data in the Computer Networks

Suppose the user uses the shopping cart on a Website which is a two-way communication where user will request the query and then after processing get desired output on the same channel. The attacker performs various attacks like man-in-the-middle attack, ARP poisoning, DNS spoofing, etc. that will cause loss of confidentiality and integrity of user's transaction.

Attacks on Web Applications

Now by using the open source tool one can attack various servers and access the secret information from it. Hackers are intelligent enough to find the vulnerabilities and launch an attack on the Web Application. Highest number of cyber-attacks that take place are on web application level which involve;

- SQL Injection
- Cross Side Scripting attack (XSS attack)
- Social Engineering Attack
- Directory Traversal
- Local File Inclusion

Tools explained

SQL MAP

It is an open source penetrating testing tool which is free to use and capable of supporting various types of SQL injection techniques like Boolean based blind, Error-based, Out-of-band, etc.

OWASP Zap

One can use an open source tool called OWASP which is made using ZAP that exposes;

- Missing anti-CSRF tokens and security headers.
- XSS injection.
- SQL injection.
- Application error disclosure.

Key features of OWASP ZAP are automatic scanning, easy to use, multi-platform, uses traditional and powerful AJAX spiders.

The session was insightful and informative as it made the students aware about how to protect the Web Applications which tends to get attacked by the hackers very often these days.

Report compiled and edited by Prof. Amit K. Nerurkar, Prof. Mohini Chaudhari and CSI-VIT Team