

Loop Holes in Web Based Security

Kashiram Jeevan Vengurlekar

Student, Master of Computer Application

Late Bhausahab Hiray S S Trust's Institute of Computer Application, Mumbai, India

Abstract: *Loopholes in web-based security is very important topic to learn and understand during creating and running an web based application, as there are many different was to breach an application some of them are since the 1st ever site was made, such as SQL Injection, Broken Authentication & Session Management, XSS, Security Misconfiguration, CSRF and many more, where there is many different ways to manage those type of vulnerability like sanitization of data before accepting it, proper validation of data, proper handling and configuring of web-based application.*

Keywords: *SQL Injections, Cross Site Scripting (XSS), Broken Authentication & Session Management, Insecure Direct Object References, Security Misconfiguration, Cross-Site Request Forgery (CSRF)*

REFERENCES

- [1]. DPLOOP: Detection & Prevention of Loopholes in Web Application Security.
- [2]. Security Estimation Framework for Development of Secure Software and Cyber Attacks.
- [3]. Idea: Towards Architecture-Centric Security Analysis of Software
- [4]. A Survey on Web Application Security
- [5]. Security of Open Source Software
- [6]. <https://www.acunetix.com/websitesecurity/sql-injection/>
- [7]. <https://www.oreilly.com/library/view/securing-node-applications/9781491982426/ch04.html>
- [8]. <https://blog.eccouncil.org/most-common-cyber-vulnerabilities-part-5-security-misconfiguration/>