# A Survey on Web Application Vulnerabilities

##### **Matthi Naveen\*, Dr.Pragnyaban Mishra\*\*,**

\* Department Of CSE, KLUniversity, India

\*\* Department of CSE, Associate Professor*, KLUniversity, India.*

***Abstract*-** The world is exceedingly dependent on the Internet and Web applications is using very extensively by every organization and human for information sharing, business purpose like online sales, money transfer etc and services Exchange. Nowadays, web security is greatest challenge in the corporate world because web application will be main way for their daily business and if web application is effected then daily business and reputation will loosed. As almost all organizations has using the web application service to share or store sensitive information about their clients. So Web applications are inclined to security attacks and new security vulnerabilities has grown in last two decades in web application. so web applications become a well known and important target for security attacks by attackers. So it is very vital to secure a web application from attacks. A major security issues in web application will basically occur due to improper input validation at client side which will take advantage by attacker to inject payloads. This paper reviews about the vulnerability assessment and pretesting steps and types, area of web application security Vulnerabilities like sqlinjection,cross site scripting, file inclusion and broken authentication

***Index Terms***- Cross site scripting(XSS),cross site request forgery, file incusion,penetrating testing, steps in VAPT, Sqlinjection ,vulnerability assessment, VAPT Types, Types of XSS,Types of Sqlinjection.

1. Introduction

World Wide Web has advanced from a framework that delivers static pages to a stage that supports distributed and dynamic applications and web application has become the most important source for delivering information and service to the world. Web application advancements give a promising system of coordinating numerous useful segments over the web and therefore empower people and associations to cooperate each other utilizing application program interface along enormous topographical separations. Billions of people everywhere throughout the world use web application advancements to exchange data, perform money related exchanges, and have fun and communicate and to socialize themselves

Web application grew tremendously in the last few decades and it has brought great benefits to the people, however, these benefits are associated with some challenges like security which will be very important. Security in web application refers to the threat which occurs due to flaws in software design, coding, testing and implementation. Web application services are more prone to cyber attacks due to their public access. And web applications are increasingly used to deliver security critical services so they become a valuable target for security attacks. Most web applications will use database that helps to manage data easily and this data will also contain sensitive information, if web application is hacked, a large amount of information would be infringed, resulting in severe economic damages, ethical and legal implications.

The Web platform is a dynamic architecture that involves various components and technologies such as HTTP protocol, web server and application development technologies on the server side, web browser and client-side technologies. For developers with insufficient security vulnerabilities knowledge or awareness results in a high rate of web applications sent on the Web is uncovered to security vulnerabilities. According to a report by the Internet Application Security Consortium, around 49% of the internet applications being looked into contain vulnerabilities of tall hazard level and more than 13% of the websites can be compromised totally naturally .A later report uncovers that over 80% of the websites on the Web have had at least one high level Vulnerability. Vulnerability refers to a weakness in system’s security requirement, design, coding or operation that could accidently occur or intentionally violated and result in security failure. In last few years, number of reported web application security vulnerabilities has increased. Some commonly found web application vulnerabilities include SQL injection, cross site scripting, command line injection, cross site request forgery and malicious file upload and execution.

this paper is presented as follow.

1. Introduction to web application
2. **overview of VAPT**

## A. **Steps in VAPT**

1. Pre-Engagement Interactions or Scoping
2. Reconnaissance
3. Threat Modeling & Vulnerability Identification
4. Exploitation
5. Post-Exploitation
6. Reporting
7. Resolution & Re-Testing

## **B. types of VAPT**

1. Black box pen testing
2. White box pen testing
3. Grey box pen testing
4. **web application vulnerabilities**

The different high level vulnerabilities are disused below:

## **Sqlinjection**

Types of SQL injection

1. In-band SQL Injection

* Error Based SQL Injection
* Union Based SQL Injection

1. Inferential (Blind) SQL Injection

* Boolean based SQL Injection
* time based SQL Injection

1. Out-of-band SQL Injection

## **Cross site scripting**

1. Reflected Cross Site Scripting
2. Stored Cross Site Scripting
3. DOM Based Cross Site Scripting

**The Impact of Cross-Site Scripting (XSS) is**

* Session Hijacking
* Stealing credentials
* Targeting Sensitive Data
  + Key logger:
  + Port scan:
* Web site defacement:

## **File inclusion**

1. Local file inclusion (LFI)
2. Remote file inclusion(RFI)

## **Cross site request forgery**

## **Broken authentication**

1. **CONCLUSION**

**Acknowledgment**

I wish to express my sincere gratitude to the administration of Andhra Pradesh Technology Service Ltd, Department of Information Technology Govt. of Andhra Pradesh and Security Audit Team of APTS Ltd, KL University for providing the excellent environment and resource. In particular I wish to express my sincere appreciation to Mr. SANTHI MOHANA KRUSHNA, who has the substance of a genius: he convincingly guided and encouraged me to be professional and do the right thing even when the road got tough.

**References**

1. Ayeni, Bakare K., et al. “Detecting Cross-Site Scripting in Web Applications Using Fuzzy Inference System.” Journal of Computer Networks and Communications, vol. 2018, Jan. 2018, pp. 1–10., doi:10.1155/2018/8159548.
2. “Cross Site Scripting (XSS).” OWASP, owasp.org/www-community/attacks/xss/.
3. Glossary - Web Application Security Consortium, www.webappsec.org/projects/glossary/.
4. Kaur, Parminder, and Navdeep Kaur. “Input Validation Vulnerabilities in Web Applications.” Journal of Software Engineering, vol. 8, no. 3, Jan. 2014, pp. 116–126., doi:10.3923/jse.2014.116.126.
5. Muscat, Ian. “What Is Local File Inclusion (LFI)?” Acunetix, 11 Mar. 2019, www.acunetix.com/blog/articles/local-file-inclusion-lfi/.
6. “SQL Injection.” Wikipedia, Wikimedia Foundation, 14 Jan. 2020, en.wikipedia.org/wiki/SQL\_injection.
7. “Types of XSS.” OWASP, owasp.org/www-community/Types\_of\_Cross-Site\_Scripting.
8. “Types of XSS (Cross-Site Scripting).” Acunetix, www.acunetix.com/websitesecurity/xss/.
9. “Web Application Vulnerabilities: Statistics for 2019.” Web Application Vulnerabilities: Statistics for 2019, Positive Technologies, 13 Sept. 2019, www.ptsecurity.com/ww-en/analytics/web-application-vulnerabilities-statistics-2019/.
10. “What Is SQL Injection (SQLi) and How to Prevent It.” Acunetix, www.acunetix.com/websitesecurity/sql-injection/.
11. “What Is SQL Injection: SQLI Attack Example & Prevention Methods: Imperva.” Learning Center, Imperva, www.imperva.com/learn/application-security/sql-injection-sqli/.