A Study on Web Application Security Vulnerabilities

**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

Keywords: 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.

**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.

1. **Introduction to web application**

The Web Application Security Consortium (WASC) defines a web application as “a software application, executed by a web server, which responds to dynamic (or) static web page requests over HTTP.”[web constrium citation ]A web application consists of a series of scripts, style sheets, html pages, images etc. that reside on a web server and communicate with dynamic content repositories or other sources. Using the Internet infrastructure, web applications enable service providers and consumers to exchange and manipulate information. For a good introduction to web application from the penetration tester’s perspective the information can be gathered from . Web application develpment technologies include PHP, Active Server Pages (ASP), Perl, Common Gateway Interface (CGI), Java Server Pages (JSP), JavaScript, VBScript, Hyper Text Markup Language (HTML), and with large categories of web application technologies include different   communication protocols, formats, server-side and client-side scripting languages, browser plug-ins, and web server API.

A web application has a distributed n-tiered architecture. Typically, there is a client (web browser), a web server, an application server (or several application servers), and a backend (database). Figure 1 represents communication flow of web application request and responce. and There may be a firewall ,proxy servers,WAF’s in between web client and web server for additional security.



Figure 1. Web Application Environment

1. **Overview Of VAPT**
   1. **vapt steps**
   2. **vapt types**
2. **Vulnerabilities in Web application**

Vulnerability is a weakness in application which can be design flaw or implementation bug that allows an attacker to cause harm to stakeholders of an application.Formally, vulnerability is defined as “The existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable event compromising the security of the computer system, network, application, or protocol involved” ([Enisa, 2014](https://scialert.net/fulltextmobile/?doi=jse.2014.116.126#66656_an)) [pramideer chaur citation].

In many of web application the Vulnerabilities will arises due to poor design padigarimage, configuration mismanagement, complexity of software, accepting unsanitized input from user, weak password management and features misuse. The impact of vulnerabilities depends on the impact of the vulnerability for example if a attacker obtains the confidential details of an user, he can misuse this information (like account number, account balance, loan amount, etc.) and can also alter the data to cause harm to the concerned user then the impact will be very high. Vulnerability assessment for web applications be done periodically for identifying, classifying, remediating and mitigating vulnerabilities. the testing guidelines for webapplication will be given by the organization like OWASP, OSSTMM,ISSAF,Microsoft etc and will classify the vulnerability based on their risk rating,exploitability,detectability,prevalence and impact. The owasp standard are the commonly used standard an classicafication of web application vulnerability based on owasp standards is given in below table and owasp will also release the testing guidelines with checklist

|  |
| --- |
| OWASP TOP 10 |
| A1:2017-injection |
| A2:2017-Broken Authentication |
| A3:2017-Sensitive Data Exposure |
| A4:2017-Xml External Entities(XXE) |
| A5:2017-Broken Access control |
| A6:2017-Security misconfiguration |
| A7:2017-Cross-site Scripting |
| A8:2017-Insecure Deserialization |
| A9:2017-Using components with known Vulnerabilities |
| A10:2017-Insufficient logging and Monitoring |

**Table1.** OWASP (2017) Top Ten application security Risks

In 2018, around 70 types of weaknesses in web applications are found. As always, Cross-Site Scripting (XSS) vulnerabilities are present in many web applications{citation Ayeni, Bakare}. Four out of five web applications contained configuration errors such as default settings, standard passwords, error reporting, full path disclosure, and other information leaks that might have value for potential intruders [9].More applications are vulnerable to information exposure. Access to configuration and debug information, source code, session identifiers, and other sensitive information is possible in 79 percent of web applications. This is concerning when compared to past years such as 2016 (60%) and 2017 (70%).



The percentage of application based on vulnerabilities severity (high, medium, low).in the span of 4 years is shown in below image and the major of web applications is affected with high level of vulnerabilities only

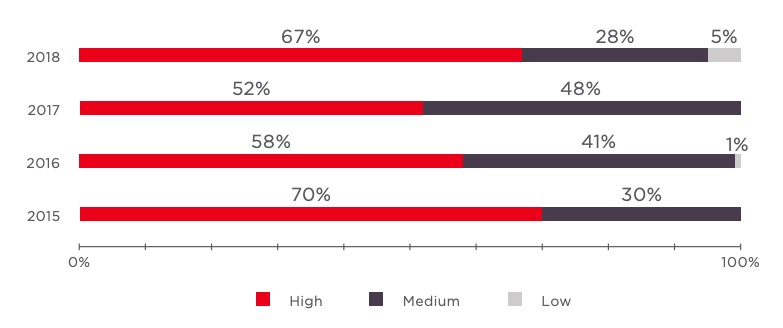


Figure 2. Percentage of Web Application Affected yearly

as there are many automated tools like accunetix,burpsuite suite scanner,netsparter ettc are available in market but he it will leave some

1. **Sql injection and its type**

**jk**

1. **Xss and its types**

**uuu**

1. **file inclusion**

**Hfg djk**

1. **Conclusion**

**Sk fjgvd,jmf**

1. **References**