Abstract

The global presence of ASP.NET websites is increasing with each passing day. With increase in the number of ASP.NET websites, issues pertaining to website’s security vulnerabilities, performance and bandwidth have come up to the surface. The security vulnerabilities in a website enable access to critical data and resources of the website. The most two common security holes in the ASP.NET Websites are SQL Injection and Cross Site Scripting. The performance and bandwidth issues in a website present usability obstacles for its intended users. ASP.NET websites mostly contains server side data bound controls and most of the developers use their default properties leading to performance issues and bandwidth issues. The global distribution of the ASP.NET websites further aggravates the problem of the impact of these issues. This paper aims to discuss issues related to the ASP.NET website’s security, performance and bandwidth.

References

An Approach to Security, Performance and Bandwidth Issues in ASP.NET Websites

- Common-threats-in-web-applica

Index Terms

Computer Science Software Engineering

Keywords

ASP.NET Websites Vulnerability Threats Security Script; JavaScript; HTML SQL Injection

Cross Site Scripting XSS