Project Synopsis

on

Securing Website from Cross Site Scripting

Submitted as a part of course curriculum for

Bachelor of Technology

in

Computer Science

Submitted by
Amish Mishra
1900290120013

Under the Supervision of
Dr. Sapna Juneja
Professor

KIET Group of Institutions, Ghaziabad
Department of Computer Science
Dr. A.P.J. Abdul Kalam Technical University

2021-2022

DECLARATION

We hereby declare that this submission is our work and that, to the best of our knowledge and belief, it contains no material previously published or written by another person nor material which to a substantial extent has been accepted for the award of any other degree or diploma of the university or other institute of higher learning, except where due acknowledgement has been made in the text.

Signature of Students
Name: Amish Mishra
Roll No.: 1900290120013
Date: April 04, 2021

CERTIFICATE

This is to certify that Project Report entitled **"Securing Website from Cross Site Scripting "** which is submitted by **Amish Mishra** in partial fulfilment of the requirement for the award of degree B. Tech. in Department of Computer Science of Dr A.P.J. Abdul Kalam Technical University, Lucknow is a record of the candidates own work carried out by them under my supervision. The matter embodied in this report is original and has not been submitted for the award of any other degree.

Date:

Supervisor Signature
Dr. Sapna Juneja
(Professor)

ACKNOWLEDGEMENT

It gives us a great sense of pleasure to present the synopsis of the B.Tech Mini Project undertaken during B.Tech. Third Year. We owe a special debt of gratitude to Dr. Sapna Juneja , Professor, Department of Computer Science, KIET Group of Institutions, Delhi-NCR, Ghaziabad, for her constant support and guidance throughout the course of our work. Her sincerity, thoroughness and perseverance have been a constant source of inspiration for us. It is only her cognizant efforts that our endeavours have seen the light of the day.
We also take the opportunity to acknowledge the contribution of Dr. P. K Singh, Head of the Department of Computer Science, KIET Group of Institutions, Delhi- NCR, Ghaziabad, for his full support and assistance during the development of the project. We also do not like to miss the opportunity to acknowledge the contribution of all the faculty members of the department for their kind assistance and cooperation during the development of our project.
Last but not the least, we acknowledge our friends for their contribution to the completion of the project.

Signature:
Date : April 04,2021
Name : Amish Mishra
Roll No: 1900290120013

ABSTRACT

Website is a collection of related web pages address with certain IP address in an Internet Protocol-based network. Website contains information to be shared and exchanged with others. With the help of Web Browsers anyone can access any website and connect with anyone in the world . These Websites are accessed and transported using HTTP(Hyper Text Transfer Protocol) which can use encryption As HTTPs as a security mechanism .

In this paper we are studying about Cross Site Scripting(XSS) Attacks . These attacks are currently the most popular security problem in modern web applications . These attacks inject malicious JavaScript into your pages, which then runs in the browsers of your users, and can change page content, or steal information to send back to the attacker.

This paper provides some best existing tools/methods and some new methods to client-side to prevent from these attacks . Some existing solutions degrade the performance of the client-system resulting in a poor web surfing experience . This paper provide some better and efficient methods step by step to protect XSS without degrading the user's web browsing experience .

KEYWORDS : Cyber Security , XSS , JavaScript Injection

TABLE OF CONTENTS

CHAPTER 1: INTRODUCTION

1.1 INTRODUCTION

Cross-Site Scripting (**XSS**) is a type of vulnerability that affects web applications. It allows an attacker to send malicious code to a website. That same code is then sent to other users to be executed on their browsers. When successful, an XSS attack can provide the attacker with sensitive information from other users' browsers. For instance, the attacker can retrieve user cookies and session tokens, which they can then use to perform session hijacking. Cross-site scripting vulnerabilities normally allow an attacker to masquerade as a victim user, to carry out any actions that the user is able to perform, and to access any of the user's data. If the victim user has privileged access within the application, then the attacker might be able to gain full control over all of the application's functionality and data.

The aim of this project is to make and provides some useful methods and techniques by which anyone can use these methods to prevent their websites from Cross Site Scripting .

1.2 PROBLEM STATEMENT

In this Project , The aim is to create a website which can automatically detect, identify and block Cross Site Scripting with the help of a dummy website which is designed by us . On this website we will inject some XSS code and then test the functionality .

1.3 OBJECTIVE

- Developing a Website
- Researching & Developing some methods/techniques to prevent website from XSS
- Making this Website XSS proof.

CHAPTER 2 : LITERATURE REVIEW

2.1 Cyber Security for Website of Technology Policy Laboratory

Jarot S. Suroso(2019)

Website is a collection of related web pages address with certain IP address in an Internet Protocol-based network. Website contains information to be shared and exchanged with others. Using an application called browser, users can browse any kind of website and connect with other users in network. Web pages are accessed and transported with Hypertext Transfer Protocol (HTTP), which can use encryption (HTTP Secure) as a security mechanism. The website created and utilized by all researcher. The most stressed part in this research is to understand the way how the attack works and also how is the prevention method. In addition, it then should be combined it all and make it simple to be implemented in website and it must be completed by the short time provided. It will be better to use hosting with unlimited privilege. Furthermore, the defense code implemented here is just the well-known , attacks protection. As there are still so many threats, this code needs a lot of improvements. Since the security is a never-ending job, so maintenance needs every time. It will be very helpful for the new web developer to implement this security functionality in their website. Website of Technology Policy Laboratory (TPL), proved to be able to support the government' s technology policy-making and to address social needs for globalization and the coming era of knowledge economy.

2.2 XSS Attack : Detection and Prevention Techniques(2016)

Monika Rohilla
Rakesh Kumar
Girdhar Gopal

Web applications provide access to online services. Web application' s security is the most critical part of web development. The attacker can exploits the vulnerabilities of web applications by injecting the malicious code in application which results in theft of cookies and other credential information. Cross site scripting (XSS) attack is one of the web application vulnerabilities. This paper discusses about various techniques to detect and prevent XSS attacks like sanitization, input validation, web proxy, Browser Enforced Embedded Policy (BEEP), Saner, deDcaota, NOXES etc. The details of these techniques with their shortcomings have been conducted so that one can use these techniques and tools as applicable to avoid the XSS attacks on Web applications.

2.3 Prevention Of Cross-Site Scripting Attacks (XSS) On Web Applications In The Client Side

SHALINI
USHA

Cross Site Scripting (XSS) Attacks are currently the most popular security problems in modern web applications. These Attacks make use of vulnerabilities in the code of web-applications, resulting in serious consequences, such as theft of cookies, passwords and other personal credentials. Cross-Site scripting (XSS) Attacks occur when accessing information in intermediate trusted sites. Client side solution acts as a web proxy to mitigate Cross Site Scripting Attacks which manually generated rules to mitigate Cross Site Scripting attempts. Client side solution

effectively protects against information leakage from the user's environment. Cross Site Scripting (XSS) Attacks are easy to execute, but difficult to detect and prevent. This paper provides client-side solution to mitigate cross-site scripting Attacks. The existing client-side solutions degrade the performance of client's system resulting in a poor web surfing experience. In this project provides a client side solution that uses a step by step approach to protect cross site scripting, without degrading much the user's web browsing experience.

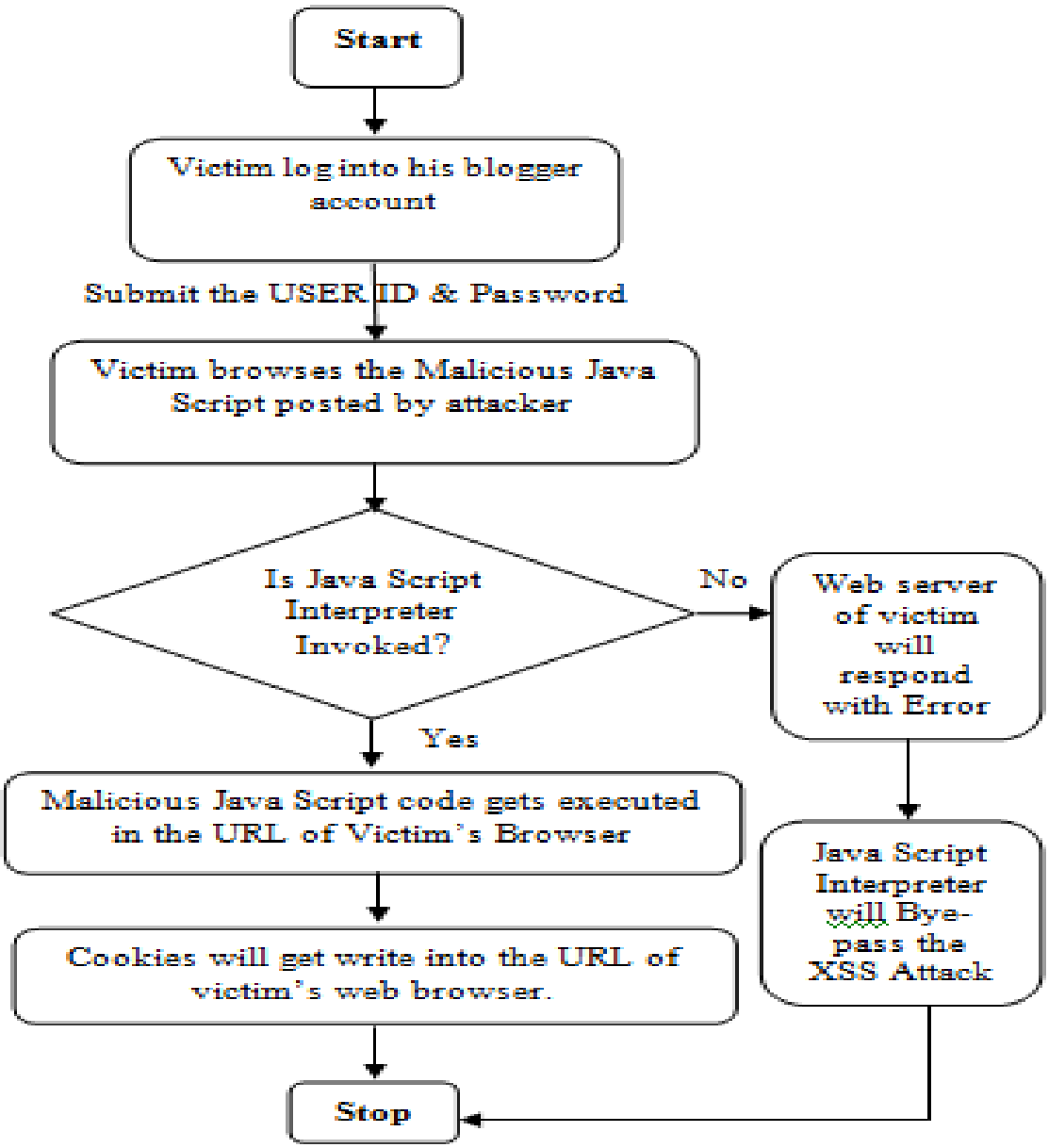
2.4 Robust Prevention of Cross-site Scripting Attacks for Existing Browsers

Mike Ter Louw
V.N. Venkatakrishnan

Due to the prevalence of XSS attacks and current trends in web applications, there exists a strong need for preventing these attacks. We address this need by presenting the design and implementation of BLUEPRINT: an XSS defense that satisfies all three objectives mentioned above. We observe that existing web browsers cannot be entrusted to make script identification decisions in untrusted HTML due to their unreliable parsing behavior. Therefore, in BLUEPRINT, we enable a web application to effectively take control of parsing decisions. By systematically reasoning about the flow of untrusted HTML in a browser, we develop an approach that provides facilities for a web application to automatically create a structural representation — a "blueprint" — of untrusted web content that is free of XSS attacks.

CHAPTER 3: PROPOSED METHODOLOGY

Flow Chart and Algorithm for Exploitation of XSS Attack on Victim's Website

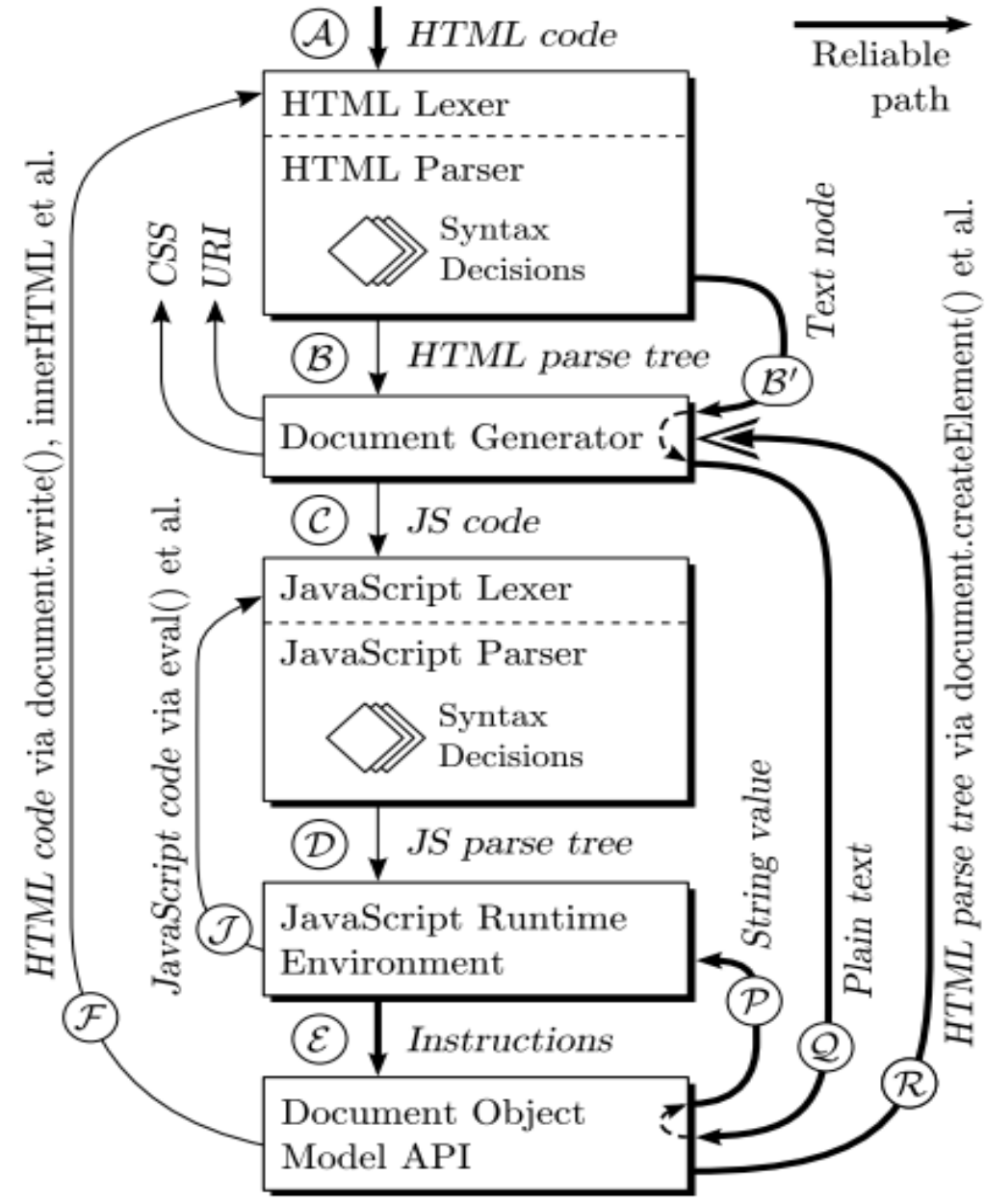


CHAPTER 4: TECHNOLOGY USED

FRONTEND – HTML , CSS , JAVASCRIPT

BACKEND - Core Java

CHAPTER 5: DIAGRAMS



CHAPTER 6 : CONCLUSION

The proposed solution is found to be very effective by the experimental results. The solution is platform independent so we block suspected attacks by preventing the injected script from being passed to the JavaScript engine rather than performing risky transformations on the HTML. Cross-site scripting attacks are among the most common classes of web security vulnerabilities. Every browser should include a client-side XSS to help mitigate unpatched XSS vulnerabilities. Cross-site scripting is a Web-based attack technique used to gain information from a victim machine or leverage other vulnerabilities for additional attacks. These practices employ policy, people, and technology countermeasures to protect against XSS and other Web attacks. In general, the system successfully prohibits and removes a variety of XSS attacks, maximizing the protection of web applications.

REFERENCES

- Prevention Of Cross-Site Scripting Attacks (XSS) On Web Applications In The Client Side
  - July 2011
  - International Journal of Computer Science Issues 8(4)
  - License
  - CC BY-NC-ND 4.0
- Robust Prevention of Cross-site Scripting Attacks for Existing Browsers
- XSS Attack : Detection and Prevention Techniques(2016)
  - **Monika Rohilla**
  - **Rakesh Kumar**
  - **Girdhar Gopal**
- Cyber Security for Website of Technology
  - Policy Laboratory
  - Jarot S. Suroso(2019)