ScienceDirect

Computer Networks

Volume 166, 15 January 2020, 106960

Cross-site scripting (XSS) attacks and mitigation: A survey

Germán E. Rodríguez [1 a b], Jenny G. Torres [1 a], Pamela Flores [1 a], Diego E. Benavides [1 a b]

Show more

https://doi.org/10.1016/j.comnet.2019.106960

Get rights and content

Abstract

The results of the Cisco 2018 Annual Security Report show that all analyzed web applications have at least one vulnerability. It also shows that web attacks are becoming more frequent, specific and sophisticated. According to this report, 40% of all attack attempts lead to a method known as Cross-Site Scripting (XSS), which was the most widely used technique. According to the OWASP Top 10 - 2017 security risk, this type of attack is ranked No. 7, and it is noted that XSS is present in approximately two thirds of all web applications.

This attack occurs when a malicious user uses a web application to execute or send malicious code on another user's computer. Also, Cross Site Scripting is a type of cyber attack by which vulnerabilities are searched in a web application to introduce a harmful script. This implies that user information can be affected by stealing cookies, phishing, or attacking a company's entire network.

In this context, we have analyzed a total of 67 documents to collect information of the tools and methods that the scientific community has used to detect and mitigate these type of attack. It has been hypothesized that the trend in the proposal of traditional methods to mitigate XSS attacks is greater than the proposals that use some artificial intelligence technique. Our results show that the trend is increasing in the proposals that analyze the content of web pages (13.20%), as well as those that serve as a toolkit for web browsers (16.98%). Also, we have found that there is a low tendency in the use of artificial intelligence techniques to detect or mitigate this attack, using Web Classifiers (9.43%).

Introduction

The application layer has support a large number of attacks, with a large-scale increase, it is a

security threat that has become very common. Techniques such as malicious codes that are vulnerable are used with the aim of penetrating and paralyzing a website. It has also been used from low-level attacks to high-level attacks that expose web application infrastructure [1]. This represents the greatest security concern for different applications, especially those that are implemented in high availability operations or priority services, such as medical care, banking, e-commerce, etc. [2]. According to the annual global security report 2018 [3], where billions of security events were analyzed, all tested applications show at least one vulnerability. The average is 11 failures per application. This report shows that web attacks are becoming more specific, frequent and sophisticated. Many events of rape show signs of prior planning by cyber criminals who investigate their victims more thoroughly.

Cross-Site Scripting (XSS) is a known web attack. It occurs when malicious web code is sent or executed, usually in script form, from the browser on the victim's computer, using their web applications. With this execution you could filter the personal information, or, steal the user [4] cookies to hijacking the identity in a fraudulent session, so it offers the attackers the possibility of stealing sensitive data or even being able to take control of certain devices. XSS is presents 40% attack attempts, SQL injection (SQLi) 24%, an attack called cross-section a 7%, the inclusion of local files (LFI) a 4% and in the last position is the denial of services distributed (DDoS) with 3%. This year, there has been a record number of vulnerabilities in web applications that include XSS, but also categories such as insecure deserialization [5]. According to data from Imperva [6] the XSS attacks represent the highest number of web application vulnerabilities in 2017. In fact, their number has doubled compared to 2016. And according to Imperva's predictions, they will follow being the most frequent offensives in 2018.

Currently, implementing server-side solutions to protect web applications is no longer profitable, according to Shanmugam and Ponnavaikko [7], because developers do not always have code assurance experience. Therefore, the providers of browsers such as Firefox, Chrome or IExplorer have tried to develop filters to act on the client side and thus defend against these attacks. Some papers such as [8] propose the incorporation of adequate prevention measures during the software development cycle, thus avoiding potential damages.We have also found proposals where dynamic, static statistical analysis or a combination of these two models have been applied. However, according to Shar and Tan [9] dynamic analysis approaches incur overhead, on the other hand, existing approaches to static analysis lack precision in the identification of XSS vulnerabilities.

In this context, we have set as a goal to find the methods and tools that have been used or proposed to detect and mitigate this type of attack. We have searched the different scientific databases and have oriented our research to the search for tools that have been proposed or used. From this search we have filtered the works that have used some artificial intelligence method. Our contribution shows as a result the current trend in the use of traditional methods vs methods that use artificial intelligence. The novelty of our research is related to the search for tools and methods to detect and mitigate a type of attack that is very little known by users. When proposing a classification of these tools, a guide will be established for researchers who are studying these types of attacks. In this way, the scientific contribution will show what is the trend in the use of tools or new proposals for this type of attacks.

The rest of the document has been structured as follows. Section2 summarizes a background on

Cross-Site Scripting attacks. Section3 details the theft of cookies through XSS attacks and the most common type of cookies. Section4 analyzes all the methods and tools found in the literature. Section5 presents a discussion of the information found. Finally, Section6 discusses the conclusions of the proposal and future work.

Section snippets

Background of cross-site scripting attacks

Web applications are insecure by default. The main reason, their developers do not establish secure development protocols, this contributes to the theft of personal and crucial information from users [10]. This lack of good practices is considered a vulnerability. If the website is not developed correctly, a hacker takes advantage of this flaw to execute some malicious code on the systems, in addition, it could scale through the network of the entire organization. Nowadays, the most popular …

Cookie theft through XSS attacks

These attacks are popular for stealing cookies from a browser's database. Thus, an attacker executes an arbitrary script and personal information is extracted from the victim's computer. The execution of the attack is to use some weakness or vulnerability. …

Analysis of methods and tools

This section has been structured in three subsections, the first details the methodology used to select the documents, the second explains the methodology used to analyze the documents, and the third explains the technical characteristics of each selected document. …

Analysis of results

In Fig.12 a mental map that is summarized in the Table9 has been proposed. Here, the classification of methods or tools that use traditional technology to mitigate XSS attacks has been structured.

In the same way, in Fig.13 a mental map detailing the methods and tools that are based on artificial intelligence to stop or detect XSS attacks has been proposed. Table10 summarizes the information found.

As seen in Table10, the following methods have been proposed that use artificial intelligence …

Conclusions

A total of 67scientific documents have been analyzed, in order to find out the tendency of using tools or methods to detect/combat Cross-Site Scripting (XSS) attacks. Through the selection of common parameters, each of the documents has been evaluated. The results of this research show 2 high

trends: the use of tools for web browsers (16.98%) and the analysis of the content of web pages (13.20%). For the use of artificial intelligence methods to detect / mitigate XSS attacks there is a low …

Future work

The study systematizes the tools and methods found to mitigate a little known type of attack called Cross-Site Scripting (XSS). The issues and open challenges are detailed below, as well as the possible solutions and lines of research that are derived from this study. …

Declaration of Competing Interest

None. …

German Rodriguez is an Engineer in Electronics and Computing, graduated from the Escuela Superior Politecnica de Chimborazo, has a Master's Degree in communications networks from the Pontificia Universidad Católica del Ecuador, currently pursuing his research phase in the Doctoral Program in Informatics of the Politécnica Nacional in Quito city. He is a full-time professor at the Universidad de las Fuerzas Armadas-ESPE in Santo Domingo de los Tsáchilas, and is also the Research Coordinator of …

…

…

Recommended articles

References (100)

T.S. Mehta *et al.*
Model to prevent websites from XSS vulnerabilities
IJCSIT) Int. J. Comput. Sci. Inf. Technol. (2015)

F. Duchene *et al.*
XSS vulnerability detection using model inference assisted evolutionary fuzzing
2012 IEEE Fifth International Conference on Software Testing, Verification and Validation(2012)

D.A. Suju *et al.*
An automaton based approach for forestalling cross site scripting attacks in web application
2015 Seventh International Conference on Advanced Computing (ICoAC)(2015)

D. Das *et al.*
Detection of cross-site scripting attack under multiple scenarios
Comput. J. (2015)

IT-Digital, El 100% de las aplicaciones web contienen vulnerabilidades, 2018,...

H. Takahashi *et al.*
Preventing abuse of cookies stolen by XSS
2013 Eighth Asia Joint Conference on Information Security(2013)

Imperva, The state of web application vulnerabilities in 2017, 2018,...

PandaSecurity, Equifax no fue un caso aislado: el peligro de las web apps, 2018,...

J. Shanmugam *et al.*
XSS application worms: New internet infestation and optimized protective measures
Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD 2007) (2007)

J. Bozic *et al.*
Purity: a planning-based security testing tool
2015 IEEE International Conference on Software Quality, Reliability and Security - Companion (2015)


View more references

Cited by (151)

Detection of cross-site scripting (XSS) attacks using machine learning techniques: a review ↗
2023, Artificial Intelligence Review

A Survey on Industrial Internet of Things Security: Requirements, Attacks, AI-Based Solutions, and Edge Computing Opportunities ↗
2023, Sensors

A hybrid deep learning-based intrusion detection system for IoT networks ↗
2023, Mathematical Biosciences and Engineering

Internet of Things: Security and Solutions Survey ↗
2022, Sensors

A systematic review on security of E-commerce systems ↗
2021, International Journal of Applied Science and Engineering

Systematic Mapping Study on Security Approaches in Secure Software Engineering ↗
2021, IEEE Access

View all citing articles on Scopus ↗

German Rodriguez is an Engineer in Electronics and Computing, graduated from the Escuela Superior Politecnica de Chimborazo, has a Master's Degree in communications networks from the Pontificia Universidad Católica del Ecuador, currently pursuing his research phase in the Doctoral Program in Informatics of the Politécnica Nacional in Quito city. He is a full-time professor at the Universidad de las Fuerzas Armadas-ESPE in Santo Domingo de los Tsáchilas, and is also the Research Coordinator of the Department of Computer Science, as well as Innovation Entrepreneurship Coordinator. He has worked for more than 6 years in the Public sector and has experience in the areas of Electronics, Networks and Communications. His current research area is computer security, specifically cookie mining as a proposal to mitigate XSS attacks and propose a framework to teach computer security.

1 All the authors contributed equally to this research.

View full text