INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 5, Issue 6)
Available online at: www.ijariit.com

A study on detection of Cross Site Scripting (XSS) attacks

Vinayak Pai
vinayakpi13@gmail.com
Manipal Institute of Technology, Manipal Academy of higher education, Manipal, Karnataka

Govardhan Hegde K.
govardhan.hegde@manipal.edu
Manipal Institute of Technology, Manipal Academy of higher education, Manipal, Karnataka

ABSTRACT

The advancement in internet technology has changed the daily activities of human life. The information available here is ample and is available with a single click. In present-day, most of service-oriented companies use web applications to improve services to their clients. With the increase in web users, web attacks are also increasing due to the vulnerabilities in applications. Cross-Site Scripting (XSS) is a computer security vulnerability found in web applications. Hackers, use this vulnerability in web applications to steal identity, credit card details, etc. According to the Internet Security Threat Report 2019(ISTR 2019), there is an increase in web attacks by 56 percent in 2018.

Keywords— *Cross site Scripting, XSS*

1. INTRODUCTION

Nowadays, web applications are used by everyone and in all sectors, it is becoming a standard platform for all services. Web applications are dynamic and they must be secured as a user uses it for all types of transactions. But, due to vulnerabilities in some websites, the user information is not validated properly.

Cross-Site Scripting (XSS) is a computer security vulnerability found in web applications. This attack involves injecting malicious script code into web applications by the attacker in the client-side browser or a server within the database. The malicious code is written in JavaScript, HTML, ASP or PHP, etc. XSS vulnerabilities are easy to spot, exploit and high impact on business security. The cross-site scripting attacks were discovered in the 1990s [13]. These are common, serious problems affecting web applications. They are serious because they can affect either both the user and application or any one of them, the adversary will gain access and they can inject malicious code which may be used to collect cookies, personal information, credit card credentials, etc.

There are three types of XSS attacks. (a) Stored XSS attacks, (b) Reflected XSS attacks and (c) DOM-based XSS attacks. In these attacks, stored and reflected attacks are server-side attacks, while DOM Based is Client-side attack.

The purpose of this paper is to show the literature review of papers that were used on the topic cross-site scripting (XSS), the review includes papers from the year 2014 to 2018. The rest of the paper is structured as follows. Section 2 describes the research method; results are shown in section. Section 4 contains answers to the research questions and conclusion of the paper in section 5.

2. RESEARCH METHOD

The study is a review of the research papers related to XSS.

2.1 Research Questions

a) How much research has been done from 2015 to 2018?
b) What are the solutions or techniques used to address XSS?
c) Is the research focused on the detection or prevention of XSS Attacks?
d) Which country has contributed much in the field of XSS research?

To address (RQ1), collected twenty papers which range from 2015-2018 and did a literature review. To address (RQ2), the techniques depicted in various articles were recorded. To address (RQ3), wanted to know what solutions were given in each article. To address (RQ4), the country of the authors has been recorded.

2.2 Search Process

The online databases were used to collect the articles for study. The articles selected for the study were based on my search terms. The search terms, used were:

- Cross Site Scripting. XSS.
- Cross Site Scripting Attacks.

Table 1 gives the names of the databases and their URL which I used to collect articles.

Table 1: Online databases and URL 5

Database	URL
Scopus	https://www.scopus.com/home.uri
IEEE Explore	https://ieeeexplore.ieee.org/Xplore/home.jsp

© 2019, www.IJARIIT.com All Rights Reserved

2.3 Inclusion Criteria

The articles were selected based on

- Articles which described tools and methods.
- Articles that address the vulnerabilities and defense mechanisms of XSS.
- Articles that focused on XSS and was published between 2014 and 2018.

2.4 Data Collection

The data collected from each article are as follows:

- Name of the Paper. Year of publication.
- Name of the author(s).
- Country of the author(s).
- Summary of the solution proposed.
- Name of the Journal.
-

3. DISCUSSIONS

3.1 RQ1 How much research has been done from 2015 to 2018?

In the study, I have used only 20 papers due to constraint in time. In actual figures, the total number of publications from 2015 to 2018 in the Scopus database is 268. This contains conference papers, articles and review papers. Table 1, gives us the details of the 20 papers studied for this study. From fig 1, we can see that the trend has been increasing since 2015 except for 2017. The papers considered for the study includes fourteen articles, four conference paper, and two review papers. The study also shows that there are 468 conference papers and 155 articles in XSS in the Scopus Database. From this, we can infer that most of the new ideas are proposed in the conferences as this gives a double advantage to the researcher. First one is, they can discuss new ideas with like-minded people and the second one is that knowledge can reach a large number of people reach once and it is very important in security research. Hence, there are a smaller number of articles, but we should make a note that the journal gives a better explanation of the experiments and the results than a conference.

3.2 RQ2 What are the solutions or techniques used to address XSS?

The proposed solutions or techniques suggested by researchers are different. They can be static, dynamic, etc.

3.2.1 Static Analysis: In this analysis only the source code is checked to find any XSS worm is present or not. A technique used to check for XSS vulnerabilities during the software development cycle [1]. In [2] concept on how to detect is given and no experiments were done, another technique is classifying using machine learning algorithms [9]

3.2.2 Dynamic Analysis: In this analysis checks for XSS worm during runtime. The common approach used by a researcher here is, the first crawler is used to crawl the whole script and compare it with the white list store for any changes and if there are any changes then they are sanitized and the valid response is sent to the user. The technique is used in, Vulscan [5] automated discovery of JavaScript injections PHP web applications [6], Online Social Networking (OSNs) sites [7],[16], HTML5 web applications [8], JavaScript's code [12], contemporary platforms of web applications [14], PHP web application [15], cloud computing [17],[18].

3.2.3 Others: The remaining 3 studies did not fall in any category mentioned above. The different approaches used here are penetration testing [11],[5], content-security policy [19] and hybrid methods[20] which include both static and dynamic analysis. The remaining papers reviewed are review papers which gives the details of the papers that were published before 2014.[3],[4],[10],[13].

3.3 RQ3 Is the research focused on the detection or prevention of XSS Attacks?

The research is focused on both prevention and detection. The paper which comes under static analysis is focused only on detection, if there is any logical or any kind of script which does not come in a predefined manner, then it cannot be determined. Dynamic analysis papers are focused on both prevention and detection. At first, code is scanned and checked for analysis and the code is compared with the repository which contains proper code. Second, if there are any changes in code when compared with repository then it is sanitized and the response is sent to the user. The first part focuses on the detection and the latter one is used to prevent XSS attacks.

3.4 RQ4 Which country has contributed much in the field of XSS research?

From the study, the country of the author was collected and found that most of the research papers were from India. From the data collected from Scopus, the countries which contributed much in the field of XSS from 2015 to 2018 is given in fig 2.

4. RESULTS

In this section, summarization of the results was done.

Table 2 shows 20 papers that have been selected for the study. The table consists of labels labeled from P01 to P20 uniquely along with the author(s) name, the title of the article, year of publication and journal name.

Figure 1 shows the number of publications published in each year from 2015 to 2018 in Scopus. It also includes the trendline which helps us in knowing whether the research topic is in the interest of researchers or not.

Table 3, gives a summary of techniques used in the arti-cles and whether it is a prevention or detection strategy.
Figure 2 shows which countries have contributed much in the field of XSS

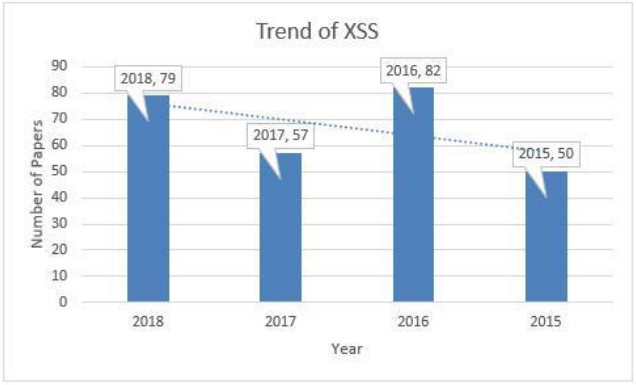

Fig. 1: Number of publications from 2015 to 2018 with trend line

5. CONCLUSION

A study of 20 papers related to XSS was conducted. From the study, we found the answers to all the four questions we had before the research. Most of the papers focused on the detection and prevention of XSS. Many ideas were proposed.

© 2019, www.IJARIIT.com All Rights Reserved

Table 2: Details of the Paper

Paper Number	Author(s)	Title	Year of Publication	Journal
P01	Ms. Daljit Kaur, Dr. Parminder Kaur	Cross-Site-Scripting Attacks and Their Prevention during Development	2017	Journal of Engineering Development and Research 5.3 (2017).
P02	Kaur, Gurvinder	Study of Cross-Site Scripting Attacks and Their Counter measures	2014	International Journal of Computer Applications Technology and Research 3.10 (2014)
P03	Deepa, G., and P. Santhi Thilagam.	Securing web applications from injection and logic vulnerabilities: Approaches and challenges.	2016	Information and Software Technology 74 (2016)
P04	Mahmoud, Shaimaa Khalifa, Marco Alfonse, Mohamed Ismail Roushdy, and Abdel-Badeeh M. Salem	A comparative analysis of Cross Site Scripting (XSS) detecting and defensive techniques.	2017	2017 Eighth International Conference on Intelligent Computing and Information Systems (ICICIS).
P05	Huang, H. C., Zhang, Z. K., Cheng, H. W., Shieh, S. W	Web application security: threats, countermeasures, and pit-falls.	2017	Computer 6 (2017): 81-85.
P06	Gupta, S., Gupta, B. B.	Automated discovery of JavaScript code injection attacks in PHP web applications.	2016	Procedia Computer Science, 78, 82-87.
P07	Gupta, Shashank, And Brij Bhooshan Gupta	XSS-secure as a service for the platforms of online social network-based multimedia web applications in cloud	2018	Multimedia Tools and Applications 77.4 (2018)
P08	Gupta, Shashank, And Brij Bhooshan Gupta.	JS-SAN: defense mechanism for HTML5-based web applications against JavaScript code injection vulnerabilities.	2016	Security and Communication Networks 9.11 (2016)
P09	Rathore, Shailendra, Pradip Kumar Sharma, and Jong Hyuk Park.	XSS Classifier: An Efficient XSS Attack Detection Approach Based on Machine Learning Classifier on SNSs	2017	Journal of Information Processing Systems 13.4 (2017).
P10	Gupta, Shashank, And Brij Bhooshan Gupta	Cross-Site Scripting (XSS) attacks and defense mechanisms: classification and state-of-the-art	2017	International Journal of System Assurance Engineering and Management 8.1 (2017)
P11	Shinde, P. S.,and Ardhapurkar, S. B	Cyber Security Analysis using Vulnerability Assessment and Penetration Testing	2016	2016,World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave).
P12	Gupta, Shashank, and B. B. Gupta	XSS-SAFE: a server-side approach to detect and mitigate cross-site scripting (XSS) attacks in JavaScript code.	2016	Arabian Journal for Science and Engineering 41.3 (2016)
P13	Hydara, I., Sultan, A. B. M., Zulzalil, H., and Admodisastro, N.	Current state of research on cross-site scripting (XSS)–A systematic literature review.	2015	Information and Software Technology, 58, 170-186
P14	Gupta, S., and Gupta, B. B.	XSS-immune: a Google chrome extension-based XSS defensive framework for contemporary platforms of web applications.	2016	Security and Communication Networks, 9(17), 3966-3986.
P15	Gupta, Shashank, And Brij Bhooshan Gupta.	PHP-sensor: a prototype method to discover workflow violation and XSS vulnerabilities in PHP web applications.	2015	Proceedings of the 12th ACM International Conference on Computing Frontiers. ACM, 2015
P16	Chaudhary, P., and B. B. Gupta	A Novel Framework To Alleviate Dissemination Of XSS Worms in Online Social Network(OSN) Using View Segregation	2017	Neural Network World 27.1(2017): 5.

© 2019, www.IJARIIT.com All Rights Reserved

P17	Gupta, Shashank, Brij Bhooshan Gupta, and Pooja Chaudhary	Hunting for DOM-Based XSS vulnerabilities in mobile cloud-based online social network.	2018	Future Generation Computer Systems 79 (2018): 319-336.
P18	Gupta, Shashank, and B. B. Gupta.	Enhanced XSS defensive framework for web applications deployed in the virtual machines of cloud computing environment.	2016	Procedia Technology 24 (2016): 1595-1602.
P19	Yusof, Imran, And Al-Sakib Khan Pathan	Mitigating cross-site scripting attacks with a content security policy.	2016	Computer 49.3 (2016): 56-63.
P20	Marashdih, Abdalla Wasef, And Zarul Fitri Zaaba	Cross Site Scripting: Detection Approaches in Web Application.	2016	International Journal of Advanced Computer Science and Applications 7 (2016).

Table 3: Summary of the Papers

Page Number	Summary	Type of Attacks
P01	In this paper, the author discusses various attacks other than XSS like DOS, hijacking, etc., but only the detection is done and not specified how to use these detection techniques during SDLC.	Static
P02	In this paper, the author discusses how XSS attacks are affecting businesses. Various types of XSS attacks are discussed. The limitations of the securities provided by the applications are also given. The proposed approach secures the applications from all the types of attacks without any extra cost and infrastructure.	Static
P03	In this paper, the author gives a detailed literature review of different types of web-based attacks. They have considered three categories in the study, a) SQL injection, b) Cross-Site Scripting, c) Logical flaws. The results of the study show that they have categorized the attacks based on the different stages in the software development cycle. The articles focus on the detection and prevention of web-based attacks.	Review
P04	In this paper, the author describes cross-site scripting(XSS), three different types of cross-site scripting attacks and the XSS attack incident that has taken place. There is a detailed literature survey of the prevention and detection methods along with the tools, dataset, strengths, and weaknesses. The future idea is to detect and prevent DOM-Based Attack, using machine learning and data mining techniques.	Review
P05	In this paper, the author describes a tool Vulscan that is used to detect web vulnerabilities.Vulscan is used to detect web vulnerabilities that generate test data using a combination of bypass techniques to reveal XSS and SQL injection vulnerabilities. Vulscan uses 4 main components: 1) web crawler;2) Scanner engine;3) scanner knowledge base;4) evasion technique knowledge base. Vulscan is better than OWASPs ZED (Zed Attack proxy).	Dynamic
P06	In this paper, the author has proposed a system whose aim is to discover injection points and malicious JavaScript injection vulnerabilities. The proposed system has 3 agents:1) HTML Crawler 2) XSS Attack Vector injector and 3) Script Locator. This discovers Persistent XSS Attack locations..	Dynamic
P07	In this paper, the author has proposed a framework called XSS secure. XSS secure is a framework for securing online social networks (OSN) on the cloud from XSS Attacks. It operates on two modes i.e. training and detection. It is tested for both OSN and Non OSN sites and it gives a low false positive false negative and low overhead	Dynamic
P08	In this paper, the author proposes the first defense mechanism that uses a clustering-based sanitization framework for detecting code injection-based vulnerabilities in HTML 5 based web applications. This is tested on 2 web applications. The result shows that the system's performance is better and computation overhead is less when compared to older proposed sanitization systems.	Dynamic
P09	In this paper, the author proposes an XSS-Classifier that is used to classify whether the attacks on Social Networking Sites(SNSs) are XSS based or non-XSS based. This uses machine learning algorithms to classify. The features used here are URL features, HTML tag features, and SNSs features. The data is collected from multiple sites like Alexa and Elgg. Ten machine learning algorithms are compared and the best one is selected.	Static
P10	In this paper, the author discusses various types of attacks in XSS and also detailed attacks that took place around the world and also about the worms that were used. From this paper, we got to know what the different loopholes may be present, and the developers can look into it before developing the software which will help in reducing the XSS attacks.	Review

© 2019, www.IJARIIT.com All Rights Reserved

P11	The Cyber Security of the organizations can be increased by using the vulnerability Assessment and Penetration testing(VAPT). This has two stages. The first one is to discover the existing vulnerabilities, the second one is to Exploit the detected set of vulnerabilities. Here, the first step is passive and the second step is active. If this test is done periodically then the security flaws can be detected and can be improved which will reduce the loss.	Penetration test-ing
P12	XSS safe is a server-side solution to detect XSS attacks. It has 2 components: 1)Feature Injection: features are generated automatically and generate tokens, which will be included in the HTTP response generated by the server. 2)Sanitizer: this checks for the variation in the generated and observed features. If any changes are detected then it is malicious code and the response will be sent to the web browser. It has a zero false negative response.	Dynamic
P13	In this paper, the author gives a detailed review of 115 papers that wer available on different sites. It covers all the papers from 2000 to 2012.	Review
P14	In this paper, the author proposes a system named XSS-Immune. It is based on JavaScript string comparison and context-aware sanitization framework. It works on the client-side. It has two stages 1)It compares the script between an HTTP request and HTTP response for discovering malicious code because the attackers use similar approaches to find vulnerabilities and exploit them. It identifies the partial script injections. 2)it finds any similarity in the variables available in the malicious code in worms and removes them. The result shows that the system's performance is better and computation overhead is less when compared to older proposed systems.	Dynamic
P15	In this paper, the author proposes a system named PHP-Sensor. This discovers the vulnerabilities in workflow violation attack and cross-site scripting attacks in PHP applications. For detecting workflow violation attack we need to make a set of axioms by monitoring the HTTP requests and HTTP responses. It compares the workflow violation attack by comparing the expected and observed workflow. XSS attacks can be found by extracting HTTP requests with the injected scripts.	Dynamic
P16	In this paper, a client server-based XSS method is used which scans the JavaScript and lessens the effect of JavaScript vectors. Generates the views by performing segmentation of the received HTTP response. views give the region of accessibility. Based on the views extracted the attack vector is recognized by comparing the blacklisted repository. The sanitization process is performed in which the extracted vectors are used as input and the safe script is sent to the client-side browser.	Dynamic
P17	In this paper, the author presents a framework that will detect DOM-based XSS Attacks in mobile cloud-based online social networking (OSNs). It works in two modes.1) Training mode: deep crawls and extracts unharmful scripts by traversing the static DOM tree.2) Detection Mode: scans the dynamic DOM tree and compares it with the whitelist script stored. If there is variation then it will send the script to the sanitization engine and then the sanitized response is sent to the user. The advantage is that there is no need to trace code dynamically as it generates a DOM tree. The result shows that the system's performance is better and computation overhead is less when compared to older proposed systems.	Dynamic
P18	In this paper, the author presents a framework for web applications deployed in the virtual machines in a cloud computing environment. This detects reflected XSS Attacks. It scans both HTTP requests and response, if there is similarity in the two, then there is XSS worm else not.	Dynamic
P19	In this paper, the author proposes a new approach named content security policy (CSP)in which the server administrator will have a whitelist of approved resources. If any entry given in the website violates this then it is blocked. This approach is better than context sanitization techniques. It helps mitigate all three XSS attacks. Results show that all XSS vector was eliminated using CSP in different resources.	Content Security Policy
P20	In this paper, the author focuses on the detection of XSS attacks. There are various approaches in detecting XSS attacks and they can be categorized into static, dynamic and hybrid. Static gives more false-positive and dynamic gives less accuracy. The hybrid approach does not give efficient results. The genetic algorithm is also used but it does not give good results for PHP as the infeasible paths are not removed from the Control Flow Graph (CFGs).	Hybrid

© 2019, www.IJARIIT.com All Rights Reserved

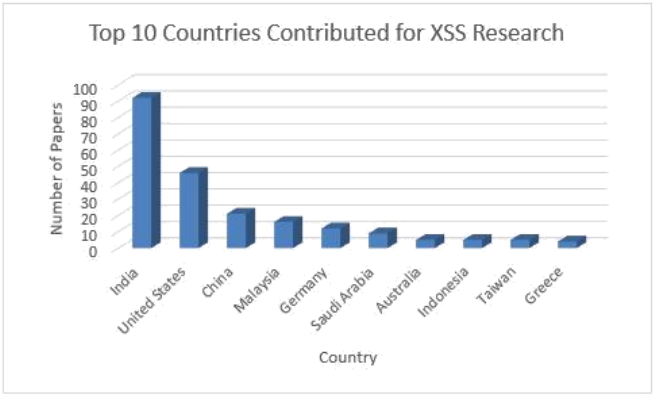

Fig. 2: Number of publications from 2015 to 2018 with trendline.

by researchers to prevent and detect XSS attacks but it is still prevalent. Now it's time for researchers to think about how to eliminate XSS attacks completely, but is not so simple. To remove XSS vulnerabilities, security checks need to be done at each stage of the development, regular penetration testing and other dynamic analysis has to be done.

5. REFERENCES

[1] Kaur, M. D., Kaur, D. P., Attack, C. S. S. Their Prevention during Development. International Journal of Engineering Development and Research, 5(3).2017

[2] G. Kaur, "Study of Cross-Site Scripting Attacks and Their Counter-measures", International Journal of Computer Applications Technology and Research, vol. 3, no. 10, pp. 604-609, 2014. Available: 10.7753/ij-catr0310.1001

[3] G. Deepa and P. Thilagam, "Securing web applications from injec-tion and logic vulnerabilities: Approaches and challenges", Informa-tion and Software Technology, vol. 74, pp. 160-180, 2016. Available: 10.1016/j.infsof.2016.02.005.

[4] S. K. Mahmoud, M. Alfonse, M. I. Roushdy, and A.-B. M. Salem, "A comparative analysis of Cross Site Scripting (XSS) detecting and de-fensive techniques," 2017 Eighth International Conference on Intelligent Computing and Information Systems (ICICIS), 2017

[5] H. Huang, Z. Zhang, H. Cheng and S. Shieh, "Web Application Security: Threats, Countermeasures, and Pitfalls", Computer, vol. 50, no. 6, pp. 81-85, 2017. Available: 10.1109/mc.2017.183.

[6] S. Gupta and B. Gupta, "Automated Discovery of JavaScript Code Injection Attacks in PHP Web Applications", Procedia Computer Science, vol. 78, pp. 82-87, 2016. Available: 10.1016/j.procs.2016.02.014.

[7] S. Gupta and B. Gupta, "XSS-secure as a service for the platforms of online social network-based multimedia web applications in cloud", Multimedia Tools and Applications, vol. 77, no. 4, pp. 4829-4861, 2016. Available: 10.1007/s11042-016-3735-1.

[8] S. Gupta and B. Gupta, "JS-SAN: defense mechanism for HTML5-based web applications against javascript code injection vulnerabilities", Security and Communication Networks, vol. 9, no. 11, pp. 1477-1495, 2016. Available: 10.1002/sec.1433

[9] S. Rathore, P. Sharma and J. Park, "XSSClassifier: An Efficient XSS Attack Detection Approach Based on Machine Learning Classifier on SNSs", Journal of Information Processing Systems, 2017. Available: 10.3745/jips.03.0079.

[10] S. Gupta and B. Gupta, "Cross-Site Scripting (XSS) attacks and defense mechanisms: classification and state-of-the-art", International Journal of System Assurance Engineering and Management, vol. 8, no. 1, pp. 512-530, 2015. Available: 10.1007/s13198-015-0376-0.

[11] Shinde, P. S., Ardhapurkar, S. B. Cyber security analysis using vulner-ability assessment and penetration testing. In 2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave) (pp. 1-5),2015,IEEE.

[12] S. Gupta and B. Gupta, "XSS-SAFE: A Server-Side Approach to Detect and Mitigate Cross-Site Scripting (XSS) Attacks in JavaScript Code", Arabian Journal for Science and Engineering, vol. 41, no. 3, pp. 897-920, 2015. Available: 10.1007/s13369-015-1891-7.

[13] I. Hydara, A. Sultan, H. Zulzalil and N. Admodisastro, "Current state of research on cross-site scripting (XSS) – A systematic literature review", Information and Software Technology, vol. 58, pp. 170-186, 2015. Available: 10.1016/j.infsof.2014.07.010.

[14] S. Gupta and B. Gupta, "XSS-immune: a Google chrome extension-based XSS defensive framework for contemporary platforms of web applications", Security and Communication Networks, vol. 9, no. 17, pp. 3966-3986, 2016. Available: 10.1002/sec.1579

[15] Gupta, S., Gupta, B. B. PHP-sensor: a prototype method to discover workflow violation and XSS vulnerabilities in PHP web applications. In Proceedings of the 12th ACM International Conference on Computing Frontiers (p. 59).2015 ACM.

[16] P. Chaudhary and B. Gupta, "A NOVEL FRAMEWORK TO ALLEVI-ATE DISSEMINATION OF XSS WORMS IN ONLINE SOCIAL NET-WORK (OSN) USING VIEW SEGREGATION", Neural Network World, vol. 27, no. 1, pp. 5-25, 2017. Available: 10.14311/nnw.2017.27.001.

[17] S. Gupta, B. Gupta and P. Chaudhary, "Hunting for DOM-Based XSS vulnerabilities in mobile cloud-based online social network", Future Generation Computer Systems, vol. 79, pp. 319-336, 2018. Available: 10.1016/j.future.2017.05.038.

[18] S. Gupta and B. Gupta, "Enhanced XSS Defensive Framework for Web Applications Deployed in the Virtual Machines of Cloud Computing Envi-ronment", Procedia Technology, vol. 24, pp. 1595-1602, 2016. Available: 10.1016/j.protcy.2016.05.152.

[19] I. Yusof and A. Pathan, "Mitigating Cross-Site Scripting Attacks with a Content Security Policy", Computer, vol. 49, no. 3, pp. 56-63, 2016. Available: 10.1109/mc.2016.76.

[20] A. Wasef and Z. Fitri, "Cross Site Scripting: Detection Ap-proaches in Web Application",
International Journal of Advanced Computer Science and Applications, vol. 7, no. 10, 2016. Avail ble: 10.14569/ijacsa.2016.071021.

© 2019, www.IJARIIT.com All Rights Reserved