Testing and Analyzing the Accuracy of Websites by Automated Scanner

Srishti Dikshit, Brajesh Kumar Sing

Abstract: ***According to the research on "scanning the vulnerabilities in websites using automation technique"the tool was only scanned those website which have the vulnerabilities in it, we reviewed the tool one more time and scanned more websites for monitoring the accuracy of the scanner and changed some parameters for diverse results [1]. Whenever it comes to the online security, this phrase "precaution is better than a cure" suits the situation in today's life. People have some laziness or they may be naive for this because they do not know that they could be hacked anytime that's why they need to be secure every time even on social media. Instead of the social media account there are many websites which could also be hacked easily. So, this tool/scanner is being updated and getting more accurate day by day so once we will know about the problems (flaws) of the websites then we could easily make them (websites) secure.***

Index Terms: automated tool, scanner's accuracy, secured websites, website flaws.

I. INTRODUCTION

When term online security comes in our mind, we relate it to the security of our social media accounts & their personal memory spaces or drives but the common people don't have any idea about the hacking of the websites too. For the security of the Indian websites we reviewed the tool again and scanned some more websites from both the sides on the basis of security parameter, error parameter, attacks parameter, vulnerability parameter & information parameter (accessing the information of the tool).Here, the following table shows the parameters to understand it more clearly. The table 1 shows the parameters in a sequence on which these websites has been tested. In the security parameter the firewalls has been tested that how many websites are having a secure connection and network.

Table 1: Parameters Identification

Sl. No.	Names of the parameters
1	Security parameter
2	Error parameter
3	Attacks parameter
4	Vulnerability parameter
5	Information parameter

The error parameter tells us about how many websites are having an error and how many of them do not have any of them. The attack parameter is for knowing about the possible attacks could be done in future on a website. Vulnerability parameter refers to the openness of a website that how many websites have the vulnerabilities and a weak security. Information parameter only the information about the operating system, server and the languages of the website could be seen as a result. After testing the websites on the basis of these parameters, we compared both the sides (Indian websites and other country's websites), it was useful for me to find out about the particular problem in the security of the websites nowadays.

II. MATERIALS AND METHODS

The tool shown in the research on "***scanning the vulnerabilities in websites using automation technique"*** is being used to scan some more websites and found the accuracy of the tool. [1]

Pros: The tool could be different form the others because we do not have to enter our query/url again and again for testing multiple modules at a time, we could scan all the full module by selecting the full scan module in the tool. The accuracy of the tool is being improved. At the beginning the accuracy of the "SriScanner" was 72% and after the tool got trained, it has now 86% of accuracy in finding the vulnerabilities.The tool is getting more updates on regular basis and also increasing the parameters.

Cons: When it comes to the network connection the tool starts using misbehave, it always needs a good internet connection. "RetinaWeb" was the most accurate scanner, finding many of the vulnerabilities as the average competitor even without training was able to discover 92% of the vulnerabilities, compared to the SriScanner competition which was only able to find 72%. Once it is trained it increased to 94%, compared to the SriScanner competition which is only able to find 86%. [4]

III. RESULT AND DISCUSSION

Sofirst of all the first parameter is the security parameter, we have tested the websites and got the results are shown in the following graph. As shown in figure 1, only 30 websites out of 50 are protected with firewalls and 20 of them are not protected, it means that those 20 websites could be hacked easily.

Revised Manuscript Received on July 05, 2019.

Srishti Dikshit, Department of C.S.E., R.B.S. Engineering Technical Campus, Bichpuri, Agra, INDIA.

Dr. Brajesh Kumar Singh, Department of C.S.E., R.B.S. Engineering Technical Campus, Bichpuri, Agra, INDIA.

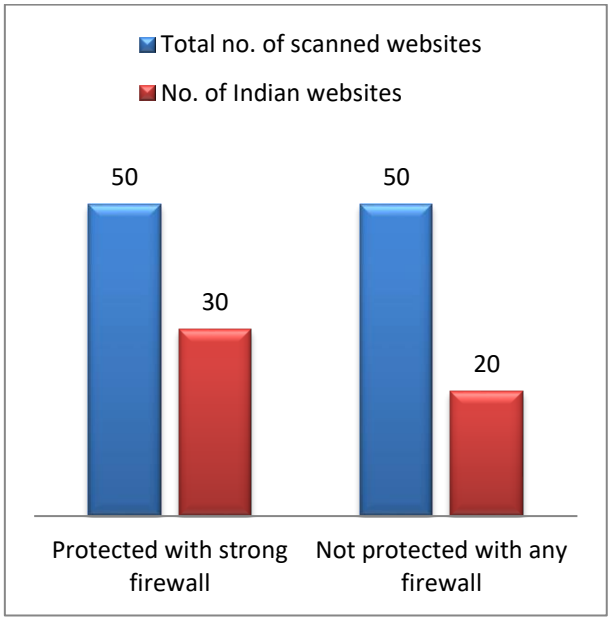

Fig 1: Security parameter in Indian websites

Now let's have a look on other country's websites.

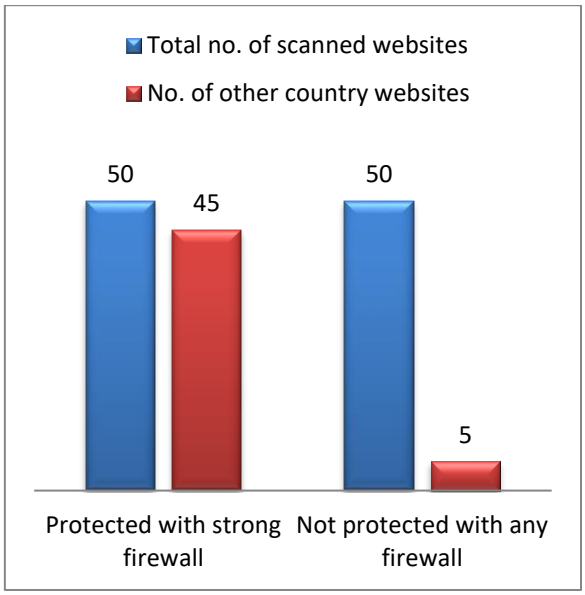

Fig 2: Security parameter in other country

As we can see in the figure 2, the difference in the quantity of having firewalls in other countries in comparison of Indian websites is more than India. The 45 websites of those countries are protected with firewalls and only 5 of them are not. Second parameter is the error parameter, the websites we have tested on the basis of this parameter the results are as follows:

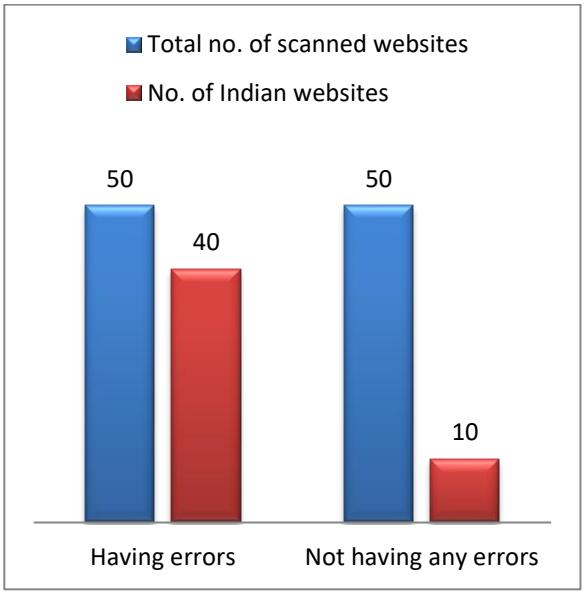

Fig 3: Error parameter in Indian websites

Figure 3 illustrates the result of the websites of India. There are 40 websites out of 50 are having the error, and rest of them are free from errors this could be any kind of error like backend files having some issues and websites do not have any transparency, they could be hacked easily by knowing all this they could made a proper solution for these websites. Similarly, on the basis of error parameter the websites of other countries have also been scanned to find out how secure they are. The results are as follows:

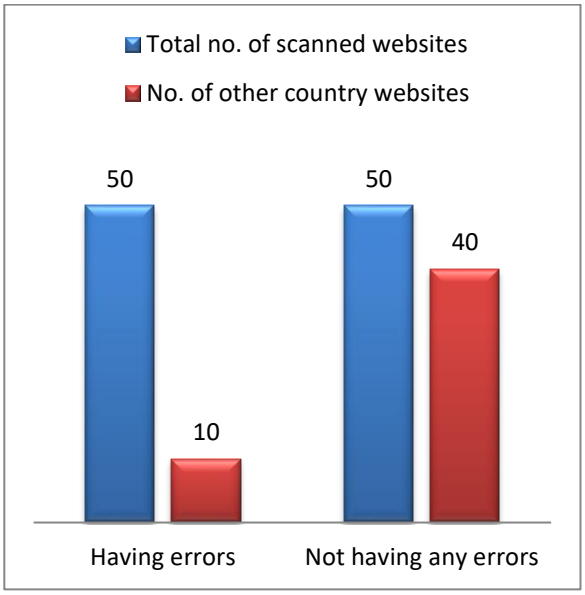

Fig 4: Error parameter in other country websites

The figure 4 shows the graph of those websites of other countries having errors in the 10 websites out of 50 they may have some problem with their backend file or may have some issues with the transparency of website and 40 of them does not have any type of error. Now, on the third parameter we have tested the websites was attack parameter, in this the websites have some possibilities of having these type of attacks in it like sql injection, bruteforce attack,

bash commands injection, html injections, XSS in headers etc. so some of these attacks were found in the websites of India and other countries also the graph related to this parameter is shown in the following figure:

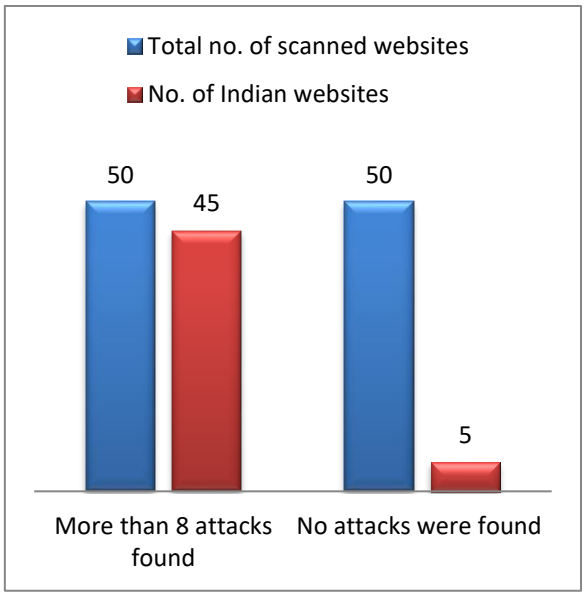

Fig 5: Attack parameter in Indian websites

Figure 5 tells us about the websites having attacks in them. We have made the criteria of 8 attacks and tested the websites. On the basis of the following criteria 45 websites out of 50 are having the possibilities of getting more than 8 attacks in their where only 5 of them are safe. Concerning attack parameter we have also tested the websites of the other countries and found the results about possibilities of getting more than 8 attacks. The result is shown in following figure:

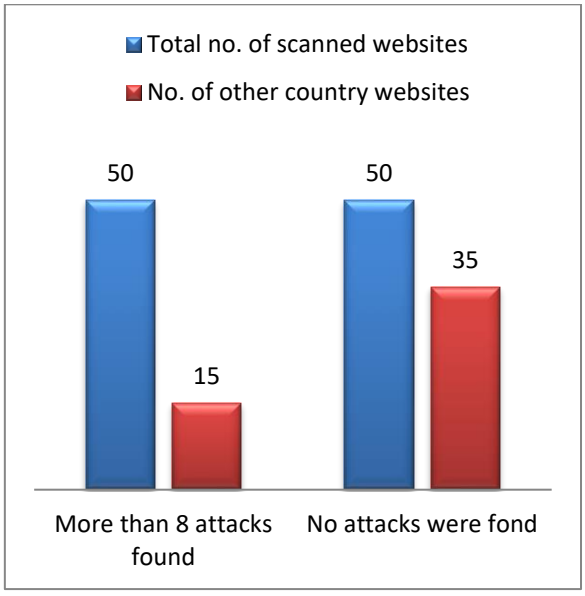

Fig 6: Attack parameter in other country

As shown in figure 6 the attacks parameter of websites of other country is more secure. Only 15 websites are having possibilities of getting attacks in their websites while 35 of them are secure and does not having any type of openness of getting attacks in them. Then we have tested more websites on the basis of vulnerability parameter to find the openness of the websites of India that how much secure it is on the basis of minor flaws like having some problem in the coding part and do not have the proper knowledge of developing a secure coding. The results are as follows:

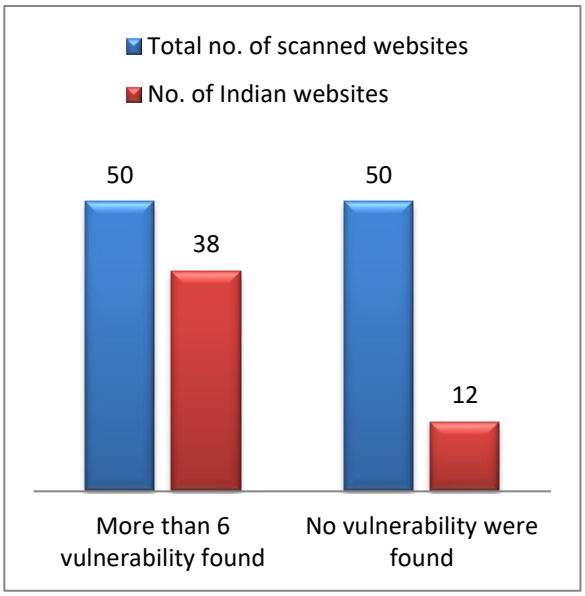

Fig 7: Vulnerability parameter in Indian websites

The figure 7 illustrates the results of the vulnerable websites of India. As we can see in the figure there are 38 websites having more than 6 vulnerabilities like the developer may not have the proper knowledge of the secure coding, and only 12 websites out of 50 not having any type of vulnerability. Similarly, we tested the websites of the other countries with vulnerability parameter we got the following results: In figure 8 we could see that only 8 websites are having the vulnerability and rest of them (42) are secured and having no vulnerability.

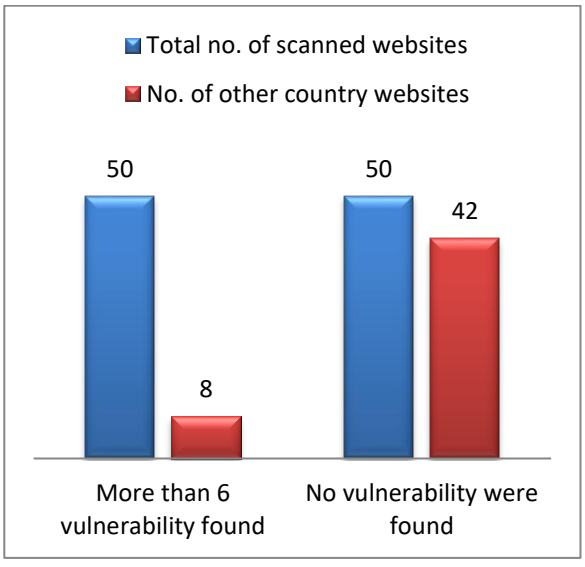

Fig 8: Vulnerability parameter in other country websites

Then we have tested the websites with the information parameter. The advantage of this parameter is that how many of the websites are having fake information and having some kind of weak and the hacked server, and

having problem with their operating system. The results of the Indian websites regarding information parameter are as follows:

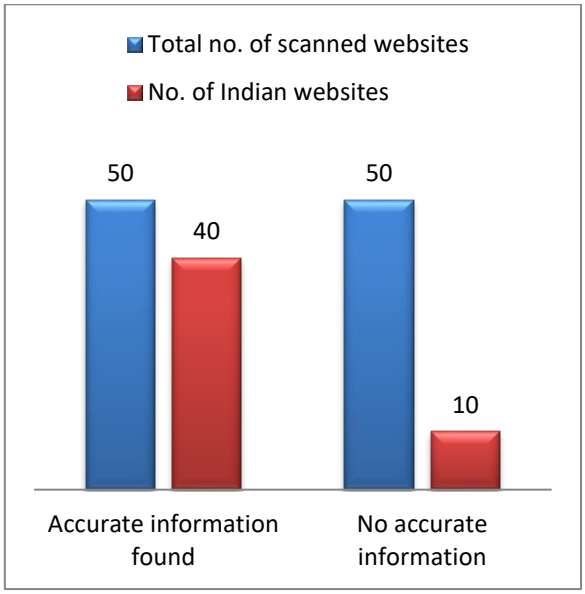

Fig 9: Information parameter of Indian websites

As we can see in the figure 9, the no. of 40 websites having the fake/unreal information and only 10 of them are true according to the scanner. Then we have scanned the other country's websites regarding the information parameter, the results are as follows:

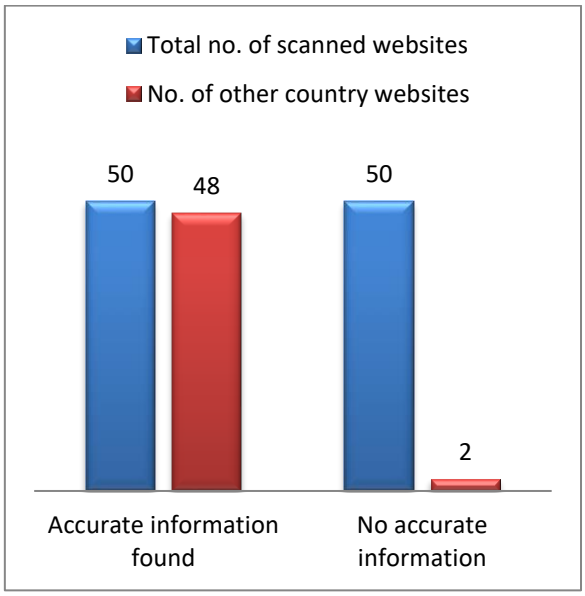

Fig 10: Information parameter of other country websites

As shown in figure 10 according to the scanner there are 48 websites of the other countries having the accurate information and only 2 of them does not having accurate information.

Now, on comparing all the graphs of all the parameters form both the sides (Indian and other country) the results are as follows:

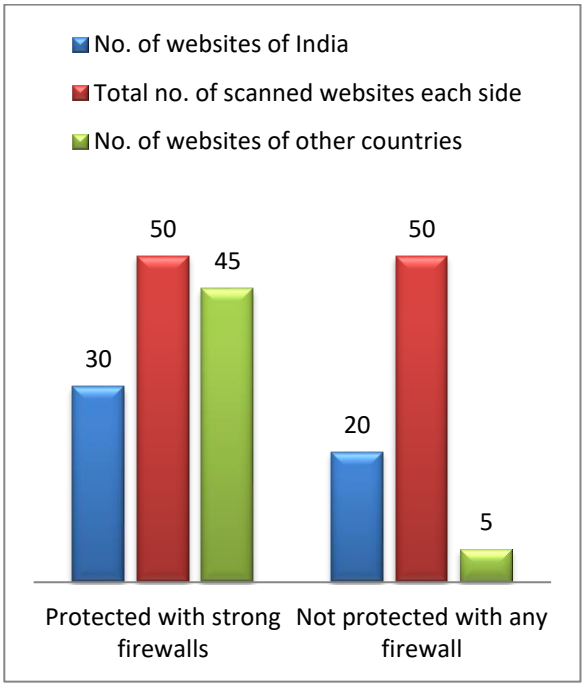

Fig 11: Comparison: Security Parameter

As shown in figure 11, the websites of other countries are more secure on the basis of the security parameter according to the scanner.

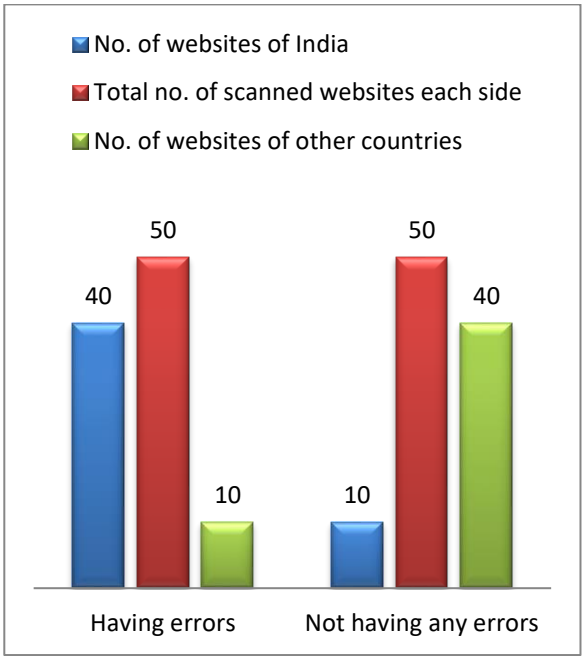

Fig 12: Comparison: Error Parameter

Figure 12 shows a graph of the comparison of websites of the Indian and other countries it illustrates that Indian websites are having more errors in their websites while the websites ofother country have less no. of websites having error

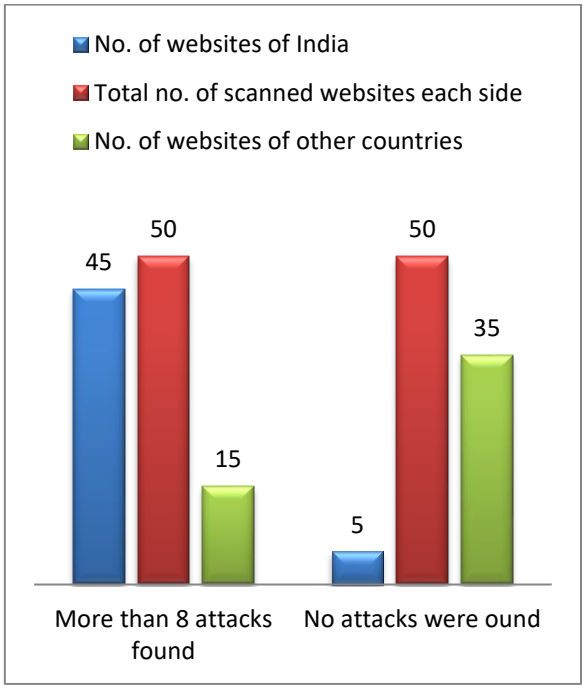

Fig 13: Comparison: Attacks Parameter

According to the tool, figure 13 shows the comparison, on comparing the websites of India and the other country on the basis of attacks parameter also Indian website are having more possibilities of getting various types of attacks. On the other hand the no. of other country's websites is more secure.

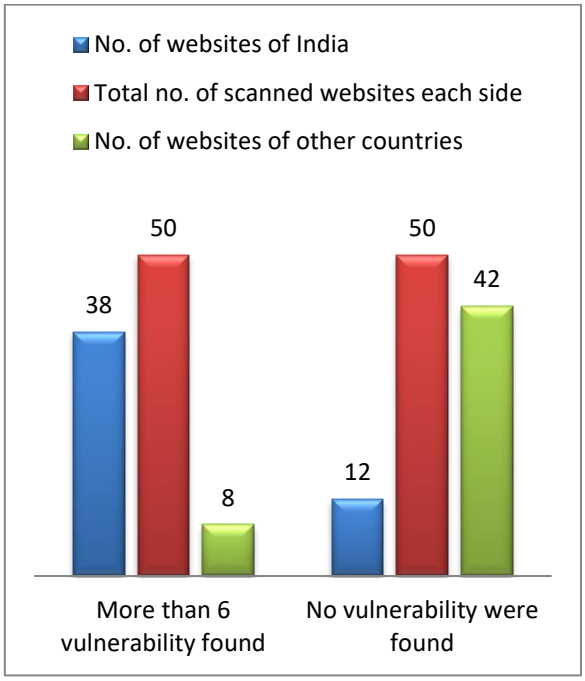

Fig 14: Comparison: Vulnerability Parameter

Figure 14 illustrates the comparison of the websites on basis of having vulnerability, according to the tool the no. of Indian websites are having vulnerability is more than the websites of the other country which have less openness in their websites

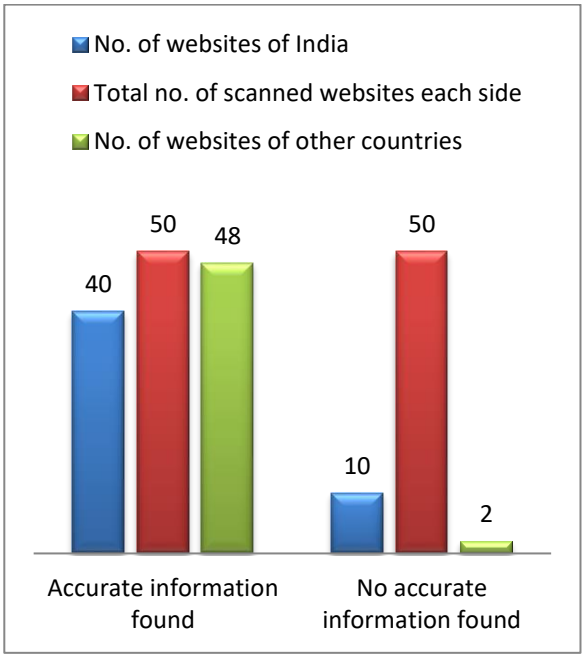

Fig 15: Comparison: Information Parameter

The figure 15 displays on the basis of the information parameter, according to the tool the Indian websites are having more fake/unreal information regarding server and the operating system in comparison of the websites of the other countries.

IV. CONCLUSION

Only purpose of this research is for awareness of the citizens of India to take the website security more seriously. According to the research, the websites of other countries are more secure than the websites of India. We have tested the websites on 5 different types of parameters. We have tested 50 websites from each side testing with the security parameter the security of the Indian websites is 60% while other countries have 90% of security in their websites. The results of error parameter Indian websites having80% of error websites and other countries have only 20% of error in it. The percentage of attack parameter is 90% of Indian websites are having the possibilities of getting attacks while other countries having only 30% chances. On the basis of vulnerability we found that 76% websites of India are vulnerable and other countries have16% of vulnerability. On the basis of information parameter, we found that 20% of Indian websites are having fake information and other countrieshaving 4% of the websites are with fake information.

REFERENCES

1. Srishti Dikshit & Brajesh Kumar Singh, (June 2019)"Scanning the vulnerabilities in websites using automation tool", Journal of Emerging Technologies and Innovative Research, volume 6, Issue 6, (pp. 201-209).
2. Abdulqader, F. B., Thiyab, R. M., & Ali, A. M. (2017). The impact of SQL injection attacks on the security of databases. In Proceedings of the 6th International Conference on Computing and Informatics (pp. 323-331).
3. OWASP [Open Web Application Security Project]. (2015, October 6).
4. Larry Suto, Application Security Consultant, (February

2010) "Analyzing the Accuracy and Time Costs of Web Application Security Scanners" 2013. BeyondTrust Software, Inc.(pp. 2-19), (WHITE PAPER).

5. Vala, R. and Jasek, R., Proposal of Improving Web Application Security in Context of Latest Hacking Trends", Recent Advances in Computer Science,(pp. 107-111), 2011.
6. Ceponis, J., Ceponiene, L., Venckauskas, A. and Mockus, D., "Evaluation of Open Source Server-Side XSS Protection Solutions", SpringerVerlag Berlin Heidelberg, (pp. 346-356), 2013.
7. AbdallaWasefMarashdih, Security Vulnerability of Cross-Site Scripting: Detection and Removing Approach in PHP Web Application, M.S. Thesis, UniversitiSains Malaysia (Malaysia), 2016.
8. Google github, SafeHtml. Available: https://google.github.io/closure-library/api/goog.html.SafeHtml.html.

AUTHORS PROFILE

Dr. Brajesh Kumar Singh was born in District Agra (U.P.) in 1978.He completed his doctorate degree in Computer Science and Engineering from Motilal Nehru National Institute of Technology, Allahabad (U.P.) in year 2014. He joined as a Lecturer/Asstt. Prof. at R.B.S. Engineering Technical Campus, Bichpuri, Agra in Year 2001. In year 2007, he was appointed as Reader/ Assoc. Prof. in same organization. In December 2017, he took over charge as Head of The department in Computer Science and Engineering. In Oct 2018, he got promoted on the post of Professor.

Srishti Dikshit, student of Master of technology. Currently in final year at R.B.S. Engineering Technical Campus, Bichpuri, Agra. She joined the campus in the summer of 2017 and will graduate in 2019 with a Master of Technology in Computer Science & Engineering. She has a passion for computer due to this reason she opted for Computer Science. She has passed her High school from KendriyaVidyalaya No.2, Jhansi in 2011 & Diploma from B.R.E.I., Bichpuri, Agra in 2014. Then she had done Under Graduation from R.B.S. Engineering Technical Campus, Bichpuri, Agra.