Automation Techniques to Increase Accuracy of Website Vulnerability: A Review

Srishti Dikshit
M.Tech. Student,
CSE Department,
R.B.S. Engg. Tech. Campus,
Agra, U.P., India

Brajesh Kumar Singh
Professor,
CSE Department,
R.B.S. Engg. Tech. Campus,
Agra, U.P., India

ABSTRACT

There are many types of tools for finding the vulnerability of the website online through internet. This review paper, "Automation Techniques to Increase Accuracy of Website vulnerability", focused on the accuracy, review and the results of the web application scanners (Appscan by IBM, Accunetix [2], Retina web bt eEye, Hailstorm by Cenzic, Webinspect by HP). Thi study consists of 'Point & Shoot' (PaS) as well as 'Trained' scans which were performed for every scanner. The 'trained' scans, each tool was made to be aware of all the pages of the websites that was supposed to test, mitigating the limitations of the scanners are in the results. Testing the effectiveness of these five web vulnerability scanners in following areas:

a) Number of vulnerability using Point & Shoot (PaS).

b) Number of vulnerability finding after the tool was trained.

c) Report of vulnerability based on accuracy.

Keywords

Automation Techniques

1. INTRODUCTION

Sometimes, the large number of weaknesses missed by the tools even if they are fully trained (59%) it is focused on the security primarily & the accuracy to a vulnerability of the web application.

Retina Web found many of the vulnerability as the average competitor having 78% of accuracy, Hailstrom having the rating of 87% but after wide-ranging training, by an expert. The second

Point & Shoot rating had Appscan is 64% & rest of them having below 63% [1].

When any scanner was reviewed, most of the vendors provided host websites that are vulnerable in different ways. The website vulnerability scanners have seen many types of vulnerabilities during their research & testing the scanners. They had definitely added some newly discovered techniques to test different kind of vulnerabilities with their scanner. By these test of web applications the thousands of hours of research & real world scans & are a good representation of the types of vulnerabilities that exist in today's world. To know that hoe well the scanners actually do these tests to audit web applications. We decided to run each scanner against the test sites & comparing the results. Assumption is that each developer would do the best against their own websites & the question is that which developer of the scanner would get the 1st position according to analysis [4]. The purpose of doing it this way is that it will be freely available for anyone to review. Each scanner was run in 'Point & Shoot' & then again after being 'Trained' to know all the links. The sites of the test are small, being most in the 10-15 link range, with one or two in the 75-100 range.

2. METHODOLOGY

To cover many bases possible was decided to run each scanner in two ways:

1. Point & Shoot (PoS): Includes the default scanning options & provides credentials to the scanners.

2. Trained: This includes configurations, macros, scripts or other training determined to be required to get best results.

No. of scanners was increased are as follows:

a) Acunetix (V6.5-20091130) from Acunetix

b) Appscan (V7.8.0.2.891) from IBM.

c) Hailstorm (V6.0 build 4510) from Cenzic.

d) Retina web (V5.0.019) from eEye.

e) Webinspect (V8.0.753.0) from HP.

The types of attacks it can perform & the types of vulnerabilities that were counted which could be useful against custom applications. These are as follows:

- Authentication
- Brute force
- Cross site scripting
- Command Injection
- XPath Injection
- Remote file Include (PHP Code Injection)
- Application Error

3. RESULT AND DISCUSSION

The result includes the testing of the scanners which were analyzed & the details are in the report explained further. There are a number of ways to look at the data. Instead of focusing on the code coverage, it focuses on comparing the results of the scanners with 'Point & Shoot' to 'Trained'.

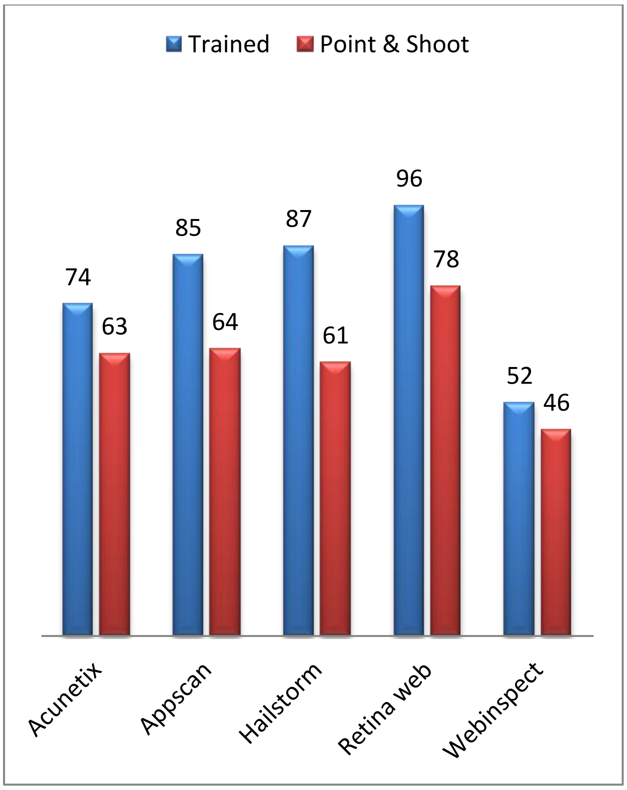

Figure 1: Comparison of vulnerabilities at Point & shoot and after trained

Figure 1, shows a report based on the comparison of the scanners with 'Point & shoot' and 'Trained'. As we could see that before getting trained only the Retina web tool is having the more accuracy towards the vulnerabilities of the websites. These scanners are tested based on before trained i.e. Point & Shoot and after trained. Acunetix is having 63% of the accurate vulnerability while after get trained it became 74% of accuracy. Appscan was having 64% of the accuracy of the vulnerabilities of the websites and after got trained it increased to the 85%. The Hailstorm had 61% of the accuracy to scanned the vulnerabilities of the websites after got trained it was having 87% of the accuracy. Retina web is the type of a tool which is having the more accuracy before and after got trained it was having 78% of the accuracy before trained and after got trained it got the accuracy of the 96%. The last but definitely not the least tool was Webinspect, it was having 46% of the accuracy and after got trained it only increased 52% of the accuracy of the vulnerabilities of web applications. The findings from this graph are based on the accuracy of the different tools.

4. CONCLUSION

The conclusion of this study is to find a good scanner which could be accurate & will be able to traverse the websites thoroughly & will find the true vulnerabilities on the basis of before and after being trained the tool.

Only one tool that is Retina web which has the best accuracy after got trained it was having 96% of accuracy rate of the website vulnerability, otherwise all the other tools are not that much accurate and having some limitations. The rest of the tools can provide good & accurate results after getting some efforts towards them.

5. ACKNOWLEDGEMENT

My thanks to the experts who have contributed towards development of the paper.

6. REFERENCES

[1] Larry Suto, Application Security Consultant, "Analyzing the Accuracy and Time Costs of Web Application Security Scanners", Beyond Trust Software, Inc. (pp.2-19), 2010.

[2] Acunetix - Website security - keep in check with Acunetix. (n.d.). Retrieved from https://www.acunetix.com

[3] Jasmine, M. S., Devi, K., & George, G. (2017). Detecting XSS based Web Application Vulnerabilities. International Journal of Computer Technology & Applications, 8(2), 291-297.

[4] OWASP [Open Web Application Security Project]. (2015, October 6). Path Traversal. Retrieved from https://www.owasp.org/index.php/Path_Traversal.

[5] Saeed, F. A. (2014). Using WASSEC to evaluate commercial Web Application Security Scanners. International Journal of Soft Computing and Engineering, 4(1), 177-181.

[6] Levin, D. (2017, March 14). How Should We Address the Cyber security Threats Facing K12 Schools? Retrieved from https://www.edtechstrategies.com/blog/how-should-weaddress-cybersecurity-threats-facing-k-12-schools/.

[7] Jeeva, S., Raveena, K., Sangeetha, K., & Vinothini, P. (2016). Web Vulnerability Scanner using Software Fault Injection Techniques. International Journal of Advanced Research Trends in Engineering and Technology, 3(2), 637-649. Retrieved from https://www.researchgate.net/publication/303756552_WEB_VULNERABILITY_SCANNER_USING_SOFTWARE_FAULT_INJECTION_TECHNIQUES.