Methods to Detect Web Application Attacks

There are several methods you can use to examine the effects of application attacks within your organization. This paper will explore the numerous methods that can examine the effects of application attacks within your organization. This paper will also discuss the different type of software you can use to determine the effects of application attacks. While doing our research we found some of the best software tools to use to examine application attacks such as OWASP Pantera, archani, and Vega. The software tools we researched would allow you to detect web application threats, find SQL injections, cross-site scripting, and automatic scanner among a host of other things. It is important to use these software tools because web application threats and vulnerabilities are happening often. Our results will show how the software detected the vulnerabilities on web applications.

Introduction

The web has been grasped by a huge number of organizations as an economical channel to convey and trade data with prospects and exchanges with clients. The web gives an approach to advertisers to become acquainted with the general population visiting their destinations and begin speaking with them. Web sites allow the capture, processing, storage and transmission of sensitive customer data such as personal details, credit card numbers, and social security information for immediate and recurrent use which is done through web applications. Web applications are computer programs enabling site guests to submit and recover information from a database over the Internet utilizing their favored internet browser. OWASP Pantera is a open source software tool to detect web applications attacks.

Another tool that we used in our research is an penetration tester for web applications call Archani. Archani like OWASP is an open source software that is integrated into the web browser but can also be used and interacted with on the command line. With these software we are able to learn and teach a lot about the protection of web application. DiscussionA main tool that we used in our application/ practice section of our research for this project is a software by the name of OWASP Pantera. Patera is an updated and improved version of SpikeProxy, With pantera, we as users are able to manually test different methods to get the best penetration results. One of the main reasons that we chose to use pantera over other software is not just the fact that is available for not just the Linux operating system but also the windows operating systems which is the operating system we are currently working with. The primary goal of Pantera is to combine automated capabilities with complete manual testing to get the best penetration testing results. Pantera has features such as powerful analysis engine, my SQL support, supports SSL, NTLM, HTTP, multi-platform meaning it can be ran on Windows or Linux, and it is 100 percent python which makes it easy to install and use. Pantera monitors and intercepts web traffic to conduct penetration test. In my opinion, one of the best things about Pantera is that it can run on multiple platforms, has several features that other programs don’t have, and it is easy to install and use.

Archani is a more than popular penetration testing software that is aimed at helping administrators evaluate the security of modern web applications. What is so great about archani is not only the fact that it is free to use and also open source meaning that people can patch

whatever bugs that might exist by themselves or send it to the community to fix meaning that no company is in charge if the software but rather the public. What is great about the software is that a user is not limited to one operating system in order to use the software because the software is available on multiple operating systems ranging from Microsoft windows, Mac OS X and Linux operating systems. With archani, it is built to be integrated into a browser interface or environment which allows it to support very complicated web languages and web applications such as AJAX, DOM manipulation, HTML5 and JavaScript. With archani, we as users can interact with the interface either with the use of the command line or with the use of the web interface. With our installation of archani, we were able to perform a couple tests such as a cross site scripting scan on a website and with archani we are able to schedule scans at any given frequency such as every five minutes as we did.

Conclusion

In conclusion, there are various ways to examine application effects on your organization, we went through various ways in our research paper with applications such as archina and OWASP Pantera which work tremendously by not only being able to be work with HTML but also various other web languages such as Javascript which allow them to work much better. These programs also not only have a have a command line interface but many of the programs such as archina have a web interface to make it easier to use. These programs alongside this research paper was aimed to educate readers on way to examine application effects and we feel as though we have accomplished that goal.