Pentest Ninja : XSS And SQLi Takeover Tool

KunalRelan
ManavRachnaInternationalUniversity
Faridabad(Haryana) India
+91 9560670202
Pentesterkunal@live.com

VidushiSinghal
ManavRachna International University,
Faridabad(Haryana)India
+919873507980
Vidushi.fca@mriu.edu.edu

ABSTRACT

This Research Paper is a tour of my Penetration Testing automation tool Pentest Ninja which is a firefox extension which has come up with a new way of exploiting Cross Site Scripting and SQL Injection vulnerability and in this paper , I explain about the working and in depth of my tool , and explaining the way it works, though the tool itself it really easy to understand and an easy to use utility for Penetration Testers and Developers for testing their Web Applications on a browser just with a simple utility Pentest Ninja.

General Terms

Algorithms

Keywords

Penetration Testing, Cross Site Scripting, SQL Injection , Automated testing , Pentest Ninja

1.INTRODUCTION

Web Applications an important part of our daily lives these days have been a critical part in the existence of Humans since the development of web as most our our work and daily things depend on web today right from emails to our social communication to even grocery shopping , web is playing a crucial part in the way we live these days and since the existence of web has existed vulnerabilities in the web applications and web Programming Languages and Cross Site Scripting & SQL Injection have been the most critical vulnerability existing on web.SQL Injection and Cross Site Scripting has been dominating OWASP TOP 10 Vulnerabilities , SQL Injection and Cross Site Scripting being not so easy to detect and requiring more of Manual Penetration Test have been one the main parts when it comes to Testing a web Application for Security Checks , which is my motivation to develop this tool Pentest Ninja : A SQL Injection and Cross Site Scripting Takeover Tool as an extension for the so famous Firefox Browser.

2.Background

\CopyrightYear{2016} \setcopyright{acmlicensed}

\conferenceinfo{ICTCS '16,}{March 04 - 05, 2016, Udaipur,

India} \isbn{978-1-4503-3962-9/16/03}\acmPrice{\$15.00}

\doi{http://dx.doi.org/10.1145/2905055.2905243}

available as free and Open Source Tool available for everyone to download,modify and run according to their needs.Pentest Ninja has been built keeping in mind the problem Penetration Testers feel while Testing a Web Application.It is available to download on your Firefox Browser at https://addons.mozilla.org/en-us/firefox/addon/sql-injection-and-cross-site-s/. Pentest Ninja is written in Javascript in Mozilla Firefox's Add On SDK , and can hook the currently loaded Web Page by injection Javascript from the addon , Firefox is an open platform for developing extensions and is very flexible and provides an amazing addon development kit for people to develop these add ons , and for choosing firefox as a platform also had a reason as myself being the security and development lead of Mozilla Community in Delhi/NCR i.e. Mozpacers.

3.Pentest Ninja

The whole tool and idea revolves around solving the problems of Penetration Testers while testing Web Applications , So starting from Cross Site Scripting which is one of the top OWASP web vulnerability still existing on a lot of web applications as developers are still not aware about the vulnerabilities existing on web applications , and for testing these applications there are tons of application trying their best test these applications which uses the black box approach of finding them , though most of them are really good at it but still there is no fool proof way of finding them as to find all the existing vulnerabilities manual and automated testing is a combined approach of finding them , but for this testers need to test the web application on the browser and automate it on a different tool however Pentest Ninja is a mix of both of them , it enables them to automate the test while doing the manual test as well , as it runs as an extension running in the browser.So this tool offers a platform for testers to run their test on web application

in a hybrid manner that is manual and automated as well , at the time of writing this paper , it only provides testing for Cross Site Scripting and SQL Injection though HTTP Parameter Pollution is also ready but other features would be added as it grows .

Here is a screenshot of the extension available at Firefox Add On Store ,Pentest Ninja uses some fine regular expressions to detect vulnerabilities whenever the website is loaded and Pentest Ninja is running in the sidebar and analyse the user entry point on the current web page.

3.1.Cross Site Scripting Hunting

Cross Site Scripting (XSS) is one of the most existing and one of the severe vulnerability on web , Cross Site Scripting has been a big vulnerability since the existence of the web and , there are

three types of cross site scripting vulnerability Reflected , Stored

and DOM based XSS . out the the three Reflected and Stored are the easier one to find and DOM Based being a little tricky to find, Reflected and Stored are comparatively easy to find and as I already said there are tons of automated tools available on the web for free and paid as well. Pentest Ninja when hooked in a web application goes deep inside in the loaded page and looks for injection point aka text fields and other ways an application takes data from user and then with its list of 200+ Cross Site Scripting Payloads to test against those applications.vulnerable and as the tool grows Machine Learning can be implemented to make it more robust and powerful while finding these vulnerabilities. Pentest Ninja also spoofs the User Agent of the browser and injects a Javascript Payload as some websites uses User Agent of User and even reflect it to them.Cross Site Scripting is a serious Vulnerability and finding it deserves a platform like Pentest Ninja and I am trying to make it better and powerful so that Developers and testers can rely on this tool and test their web application for this severe vulnerability.

3.2.Testing for SQL Injection

SQL Injection is one of the most severe existing vulnerabilities the cyber world has ever seen which can really give sleepless nights to the developers and can be a terror for a web application , a SQL Injection vulnerability is a vulnerability in Web Applications which deals with invalidated data communication from user to the database , SQL Injection is a severe vulnerability as it gives direct access to the database and the attacker can do anything with the database and access to the database directly means access to the whole server the application is running on , thus a small SQL Injection can prove to be a devastating thing for a web application and patching & finding which should be taken very seriously , Pentest Ninja as of now only deals with finding UNION Based SQL Injection in MySQL Based Web applications mostly running in PHP , and semi automates attacking the web application with SQL Injection and acts as a helping hand for the attackers manually penetrating websites and exploiting SQL Injection , Pentest Ninja takes some user data from the attacker while it is attacking the web application and the attacker is just watching and analysing the way it is trying to exploit the vulnerability.

3.3.Conclusion

Pentest Ninja started as a side project on which I could only work on weekends and as the scope and users of the tool are growing and it is getting serious which is the reason I am writing this paper on this beautiful tool , And as it is still under development and a lot of features will be added to it in near future , we can expect it to be capable of doing a complete black box and white box Penetration test on a web application while on the go , the hobby project is now getting serious attention to the penetration testers and thus I am looking forward to integrate some more amazing features to provide developers and Penetration Testers a complete platform on the top a web Browser to test their web applications.Cyber world is getting big day by day but still lacks basic security and thus is vulnerable and everyday we see thousands of websites getting attacked and this is the reason we should come up with more tools and try to test and patch these applications as soon as we can, Pentest Ninja is a tool which can be used for both use i.e. attack and defence and totally depends on the mindset of the person using it , and a good and ethical use of this tool is what I expect from people.

4.REFERENCES

1. Owasp SQL Injection https://www.owasp.org/index.php/SQL_Injection
2. Acunetix Guide on SQLi https://www.acunetix.com/websitesecurity/sql-injection/
3. SQLMap Project https://github.com/sqlmapproject/sqlmap
4. Owasp XSS https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)
5. MDN Add On Development https://addons.mozilla.org/en- US/developers/
6. Deep dive into XSS and SQLi http://www.troyhunt.com/2013/07/everything-you-wanted-to-know-about-sql.html
7. Havij Tool for SQL Injection http://onhax.net/havij-adv-sql- injection-tool
8. Zed Attack Proxy https://blog.codecentric.de/en/2013/10/automated-security-testing-web-applications-using-owasp-zed-attack-proxy/
9. Core Security Web Application Penetration Testing http://www.coresecurity.com/web-application-penetration-testing