ISSN XXXX XXXX © 2018 IJESC

Research Article Volume 8 Issue No.3

Bug Detection Tool for Websites

Sanjay Kadam[1], Samrudhi Shinde[2], Nirmala Patekar[3], Sayali Rain[4]
Professor[1], BE Student [2, 3, 4]
Department of Information Technology
Bharti Vidyapeeth College of Engineering, India

Abstract:
Web bug is a websites error or an object file that is placed on the web page or in the email so to monitor the behavior of the system user or to fetch the confidential information of the user. There already exist various bug detection tools in order to improve websites security. These tools have different functions according to the various parameters of websites. But they are not that efficient for providing the result and security to a website. Along with that much time and efforts get invested and no guarantee of accurate results. So, we require new tools which will make us available with accurate results by gathering information in less time which is the first main step performed in any bug detection process for single or multiple sites simultaneously. As there are thousands of different websites with various Web services having their different versions running on the websites they can be called as one of the component of the websites along with domains, subdomain, IP, ports, etc. This tool will ease the job of bug researchers.

Keywords: bug detection, click jacking, vulnerabilities, accurate, and bug researchers, ports, scanning.

I. INTRODUCTION

In the world of computer, error can be referenced as a bug in a software or program as a form of object files on the website or in emails that can be used to monitor the behavior of a user or cause threat to the theft of confidential data. A web bug can be just as another object of the GIF file unlike cookies that can be accepted or declined through the browser. The user can usually find an error, if you take a look at the version of the source to find a label that is loaded from several different web servers than the rest of the pages. A web bug can gather information about the different components of the Web site or the information on the computer system which includes your IP address, cookie, URL parameters, etc. Web bugs leads to various threats including sub domain DNS zone transfer, capture, click jacking, SQL injection, XSS, URI request-SSL vulnerability, etc. that are difficult to solve the major vulnerabilities. This error detection tool will have the ability to detect vulnerabilities that it is not yet possible for existing systems. The current system lacks as they are designed to run only a single function for a particular component of the website also fails to maintain the basic data that leads to recurrent or manually work websites and even test results available are inaccurate or incomplete. This error detection tool is simply beneficial for researchers since it not only collects all information of the web page and keep the database but also provides accurate results in less time. Several sites can be detected simultaneously at a time without putting a huge burden on the processor. In short, it will be useful for researchers for faster bug detection and will provide more accurate results to improve the web security of the websites.

II. ATTACKS IN WEBSITES

Some of the attacks or vulnerabilities that are difficult to solve are listed below:

A. ***Click jacking***: this is also known as UI attack, a browser security issue which is malicious technique that tricks the web user to click on something different from what the user perceives they are clicking on , leads that potentially leads to revealing of confidential information or taking over control of the computer system of the user.

B. ***CRLF injection***: CRLF stands for Carrier Return Line Field of special characters which is used to terminate a line in http.If the attacker is able to inject some malicious code in the CRLF-sequence in the http stream, they can gain control over the http response.

C. ***Subdomain Takeover***: It is a high level severity threat that can cause the takeover or control of the domain by the malicious user by boiling down the registration of the domain.

D. ***DNS Zone Transfer***: It is a type of DNS transaction which uses Transmission Control Protocol for transport and takes the form of client-server transaction. The client requests for zone transfer from the server which can be a slave or secondary server also known as primary server and then a part of database is replicated.

E. ***Host Header injection***: In most cases, developers use http host header value to generate links, import links, and generate password reset links with its value which is a bad idea because the host header can be controlled by the malevolent user by exploiting it using web-cache poisoning and by abusing alternative channels like password reset emails.

F. ***SPF vulnerability***: Not having SPF (Sender Policy Framework) record for a domain may help an attacker to send spoofed email, which will look like, originated from the vulnerable domain. Not only that, this will also result to land emails in SPAM box when SPF missing.

G. ***SSL vulnerability***: Various SSL vulnerabilities are detected.

II. LITERATURE REVIEW

Prof. SSA Subhash Pingale, Prof. SSA R.A. Taklikar, Ankita

Godse) (IJCSIT) International Journal of computing and Information Science, vol. 7 (2), 2016, 875-877) In this work, a step slow to manage software bugs that are known as triaging bugs, will want to assign the correct developer to fix a bug again. Refers to the technique of data reduction that transforms digital information derived experimentally in numeric or alphabetic form corrected, organized and simplified. The proposed work addresses the issue of data for classification of error reduction, that is, how to reduce data errors to save the work of developers and improve quality to facilitate the process of bug triage. Data for the classification of error reduction aims to build a system in small scale and high quality of data error by eliminating error reporting and words, which are redundant or not knowledgeable. The work has two data reduction goals such as the reduction of the scale of the data and improved accuracy. In the following sections, the authors present a bug that is assigned to a document and a developer related is mapped to the label of the document. Then, bug triage becomes a problem of classification of text and automatically sorting; a human triager assigns new bugs through the incorporation of knowledge. This report presents a recommendation for a developer profile, where you create a profile for each his own development-oriented earlier work. This profile is assigned to an array of domain assignment indicating the experience of each developer in your area. Additionally, the authors describe a supervised classification seeds that trained to combine unlabeled reports tagged that improves the accuracy of classification errors marked and unmarked. To adjust the classification of the error, submit weighted list (WRL) recommendations to increase the effectiveness of unlabeled bug reports. (M. Suresh, Amarnath m., g. Baranikumar, m. Elia) (International Journal of engineering and technology (IRJET) search volume: theme 03:02, Feb-2016) Error is a major challenge for any organization software. A repository of data to support a phase fault on the types of activities, for example, the failure prediction, troubleshooting and reopened error analysis. Large projects transmitting insect repository also called bug tracking systems that support the collection of information and assist developers to handle errors. This section explains the different techniques used for the separation of the insect. Techniques included are pruning Top-K, and feature selection algorithm instance selection, algorithms of Apollo, Naïve Bayes Classifier, method of Markov chains. This book offers an approach to effective problem solving with truncate data that deals with data reduction in repository error and improves data quality and reduces the time and cost of misclassification. High pruning that applies to improve results by reducing the quality of the data, getting the wise solution domain error. The authors state the comments about the technique of combining your selection by selecting the instance of bug triage effective that faces the problem of data reduction for the classification of error using text classification techniques. The book also focuses on the classification of automatic text classification semi errors like error efficient classification using text mining under.

III. SYSTEM ARCHITECTURE

Given below is the architecture of bug detection tool which will help the bug researchers in performing the operation of detecting bugs. The architecture describes the process flow of the working of tool to reach the desired result. The architecture consists of five components. The working begins initially by interacting with the KALI terminal to execute the established script which is written in python. After initializing the terminal the bug researcher enters the location of the folder containing the script along with the name of website he is willing to scan. Gathering information is the main step in any bug detection process which takes abundant time. But this time consumption problem gets solved by using this tool. First in the scanning process information gathering will be carried out. Information gathering involves subdomain enumeration, port scanning, service enumeration, and banner grabbing.

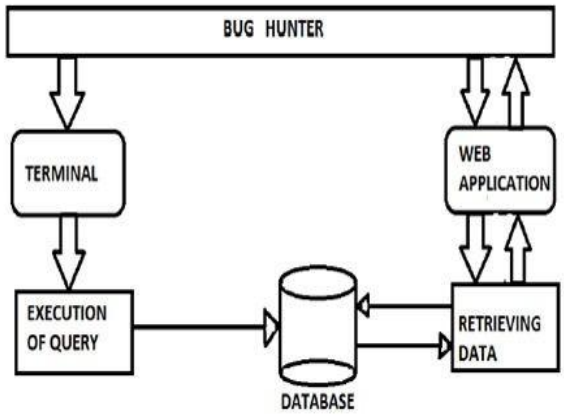

Figure.1. (Bug Detection tool architecture)

- Service enumeration: This process involves gathering the information related to the web services that are running on the ports of the websites with their versions.
- Subdomain enumeration: This is the process of finding the valid (resolvable) subdomains for one or more domains.
- Port scanning: This process involves gathering the information related to ports like open ports.
- Banner grabbing: It is used to acquire the whole information about the computer system and the services. Lastly the tool performs the function of detecting the vulnerabilities present in the website which includes click jacking, URI-XSS, CRLF injection, subdomain takeover, DNS Zone transfer SPF vulnerability, host header injection, SSL vulnerability. The bug researchers can retrieve data whenever required by interacting with the web application. They just need to mention the website name they are willing to retrieve data about in the search box or they can mention the vulnerability which will list the result of those website names that contain it. The bug researcher can also request for listing the sub- domains of the websites.

IV. PROPOSED SYSTEM

The bug detection tool is different from all the existing systems as it not only reduce the work and time but also Performs the scanning of multiple websites simultaneously and provides accurate results. The proposed system has the following features:

1. This is the Best Recon (Information Gathering) tool for bug hunting.
2. It will automate the process of Information gathering by

collecting all the required Target information.
3. It will automate the process of finding the common bugs so bug hunter can spend more time on finding logical bugs.
4. It can automatically detect Bugs like Subdomain Takeover, CRLF Injection which traditional vulnerability scanners cannot detect.
5. This tool is made to do the Mass Recon of 1000s of sites and store all the information gathered Into Database.
6. Bug Hunter can use this information to find bugs manually and more efficiently.
7. This feature will help a lot when there is new zero-day bug and bug hunter wants to find websites with specific vulnerable configuration.
8. This tool will help bug researchers to find vulnerabilities faster than before.
9. This will result in lesser number of Duplicate bugs on Platforms like Hacker one and Bug crowd.
10. Bug hunter will not miss any Information about target because of automation.
11. In manual information gathering there are high chances of missing Gems, while this script will help to find hidden gems.

V. RESULTS

The output after implementation of the script is displayed as given below.

Figure.2. (a)

The above fig 2(a) shows the execution of the script along with the site name which is coinbase.com for scanning the vulnerabilities. The website coinbase.com is vulnerable to click jacking and the port on which it is running is open is displayed.

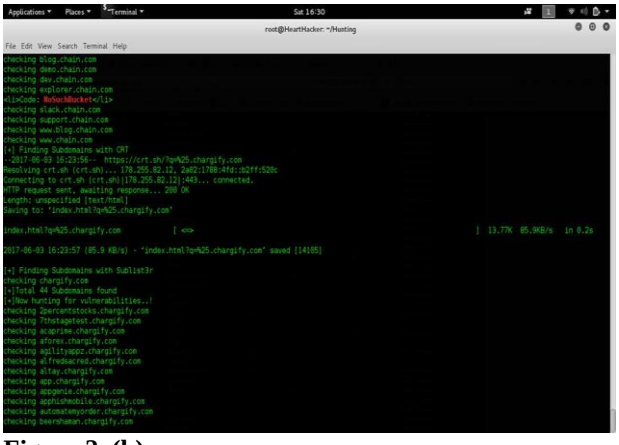

Figure.2. (b)

The above fig 2(b) is the continuation of the above fig 2(a) that further has listed the subdomains of the site coinbase.com and checking for their subdomain vulnerability.

VI. CONCLUSION

Bug detection greatly depends on information gathering. To get accurate full information makes solving bugs more efficient. It takes a lot of time to gather information for bug researchers. So, this bug detection tool whose function is gathering information and detecting vulnerabilities provides advantage for bug researchers to find and test the bugs by reducing their efforts and time and at a time multiple websites information can be gathered. It helps to maintain the database of thus when the researchers want to test any of the website they can make request for related information for bug detection.

VII. REFERENCES

[1]. J. Xuan, H. Jiang, Z. Ren, J. Yan, and Z. Luo, "Towards Effective Bug Triage with Software Data Reduction Techniques," IEEE Transactions on Knowledge & Data Engineering, Vol. 27, No. 1, JAN 2015.

[2]. J. Anvik, L. Hiew, and G. C. Murphy, "Who should fix this bug?" in Proc. 28th Int. Conf. Softw. Eng., May 2006, pp. 361–370.

[3]. Ashwini Jadhava, Komal Jadhava, "A Survey on Software Data Reduction Techniques for Effective Bug Triaging", "International Journal of Computer Science and Information Technologies, Vol. 6 (5), 2015, 4611-4612".

[4]. JifengXuan, He Jiang, "Automatic Bug Triage using Semi-Supervised Text Classification", "Chinese Academy of Sciences, Beijing, 100190 China.

[5]. AMD'sQuad-CoreBarcelonaBug revealed.http://www.infor mation week .com/blog/main/archives/2007/12/amds_qu adcore _b.html.