Vol. 03, No. 4,(2019),219–228, **ISSN:2581-3242**

IJMLNCE
JOURNAL

International Journal of Machine Learning and Networked Collaborative Engineering

Journal Homepage: http://www.mlnce.net/home/index.html

DOI : https://doi.org/10.30991/IJMLNCE.2019v03i04.004

Scanning the Database with The XSS Detection Using the Fitness Algorithm

Bhavna Dwivedi

M. Tech CyberSecurity

Jain University Bangalore

bhavnadwivedi96@gmail.com

Abstract

In this paper, we provide anoverview of the tool used in XSS detection. This tool helps us to detect the XSS attacker. XSS is the malware which helps the attacker to attack in any web-application and stolen the client data from the server, which the client or customer is storage when even the fill form in that web application. We analyze a new and efficient algorithm that helps us to secure the database for the server-side. The Genetic Fitness Algorithm is used to secure the database for the server-side, there are many algorithms like multi-path, crossover which is used to detect the XSS attacker but this algorithm is not accurate and satisfied the database security.We will analyze the genetic fitness algorithm and have many properties to achieve security for the database. It is complicated for which it is difficult for any attackers to break the security and steal the data from the server site.

Keywords

XSS, pmd tool, Veracode tools, Genetic fitness, crossover

1. Introduction

In the web application, there are three most common type of attacker

SQL injection

XSS

CSRF.

This review paper is based on XSS attacker, XSS attacker sent the malicious link in the web application, and with the help of that malicious link, all the personal data of the victim's come to the attacker web site.

This XSS attacker can steal the data from the abuse of the browser, and also stealing the data from cookie's data (which can be used to supplant the client's session) and many other actions [4-6].

XSS is based like DOM, reflected based detection from which we are using fuzzy login similarly like Namely, reflected, stored. myreview project is related to the XSS detection based on stored based .my review paper is based on XSS storage persistent [7-10].

2. Background

There are many hybrid algorithms like a gray box, browser-based, enhanced algorithm work in the storage persistence in Stored (Persistent) XSS Attacks.

2.1 Main Purpose

Cross-site scripting attack or XSS attacksis the topmost vulnerabilities which existing in web application when the client enterstheirdata. The main purpose of this paper is to protect the client data from the XSS attacker with the help of the hybrid code analysis, when the XSS attacker sent the malicious to the web application to encrypt the data on that time hybrid code scanner that web application and detected the attacker and vulnerabilities and secure the database.

The attacker uses the XSS attacker to stolen the data from the storage of the server site to protect that we are using the genetic fitness algorithm.to detect the Cross-site scripting attack or XSS attacks, XSS is the topmost vulnerabilities existing in the Web applications The XSS attack when the victim is enter the personal data.

This is the prime reason why XSS attacks are a live problem even though many detection approaches have been proposed over the years.

This Genetic Fitness hybrid scanner is used to detect the XSS attacker and protect the client data from the XSS attacker with the help of the genetic fitness analysis, when the XSS attacker sent the malicious to the web application to encrypt the data on that time hybrid code scanner that web application and detected the attacker and vulnerabilities.

3. Literature Review

B.B Gupta [1] in the paper We have proposed a novel defensive model in this paper which can examine for the similarity between JavaScript string code embedded in the web page with the explicitly available attack vector payload. Moreover, it also verified the user to access the services provided by the web application. The observed results revealed that our model is able to recognize the XSS vulnerabilities on the Hum hub with tolerable performance surplus. To detect XSS attacks, it analyses the extracted string value by performing string analysis with the help of XSS attack vector repository. If string value is validated then, web page is XSS free.

Prof Piyush A Sonewar [2] in the paper Based on the testing done and results obtained that web server take more time to except the request of user .and find the data from theSQL, this is the approach to give that to consume the time.

Boshen Chen [3] in the paper the method which they used to detected the malware attack and also identify the attacker specially in CSS style, the malware which they hide in the webpage and accurately detect drive -by-download as malicious had a few redirections in the form of iframe tags. Malicious pages classified as benign had exploit codes in the contents of rst accessed URL. In this situation, the proposed method cannot classify web pages correctly because it uses only the information of redirections.

Denny Alvarez.E [4] in the paper Colombian reality as we could survey in march of 2015 is far from the ideal,According to the 2015 paper its serva that there is 80% attacker is analysis website atacker present is based on the vulnerabilities Now a days normal techniques is used to hack the website and take the information ,for this we use the security.

Hyunsang Choi [5] in the paper, IN this paper they are using black box which detect the XSS in both the way static and dynamic also in this paper we can login to give a proper input in URLs does not need to crawl or fuzz URLs. Phantoms, a headless browser to execute a JavaScript and detect XSS vulnerabilities

4. Methodology

To analyze the hybrid scanner with the genetic fitness algorithm.

This helps us to protect the database for the server site also in this hybrid scanner work along with static and dynamic.

StaticAnalysisis used to find out the vulnerabilities and respond before the sources code implemented

Dynamic it is used for accurate for detecting the vulnerabilities and generating lower false positive rate.

In hybrid it is used both static and dynamic also it detects the less false positive rate and also detect the vulnerabilities

4.1 Fitness Algorithm

Using the hybrid scanner with the genetic fitness algorithm. The fitness function is used to calculate the path and find out the shortest path, fitness algorithm is used to solving the measure problem evaluates the vulnerable paths that a test case needs the presence of XSS vulnerabilities It is used to protect the Database for the Server web application.

Hybrid Genetic Algorithm (Fitness) is more accurate and efficient than another Algorithm like Metaheuristic, Multi-path, Enhanced.

5. Findings

If an input traverses all the branches of a vulnerable path, it means it has covered 100% of the branches and is assigned the value 1. If it traverses 70%, it is assigned the value 0.7 and so on. Hence, our fitness function is:

F(x) = ((Cpaths% + Diff) ∗XSSp%)/100</

F(x): the fitness for an individual chromosome.

- Cpath%: the percentage of branches covered.
- Diff: the difference between the traversed and the

targeted paths.

- XSSp%: the percentage of the XSS patterns file that the GA uses to cover a test path.

5.1. Algorithm

```
publicintgetFitness(Individual individual) {
 intfitness = 0;
 for(inti = 0;i<individual.getDefaultGeneLength()
   && i <solution.length; i++)
{
  if(individual.getSingleGene(i) == solution[i])
{
        fitness++;
       }
    }
    returnfitness;
}
```

5.2. Flow Chart Propose Methodology

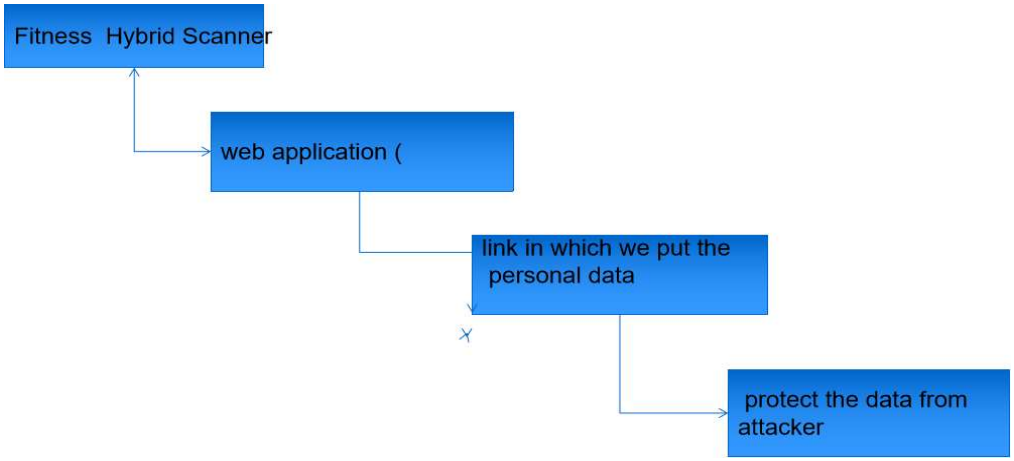


Figure 1. Flow Chart for Propose Methodology

A fitness hybrid scanner figure 1 is used to protect the data from the XSS attacker, when we use the fitness hybrid algorithm in the scanner, then whenever the client uses the web application then the scanner links with the personal site and it protects the server data. from the XSS attacker.

5.3.Block Diagram

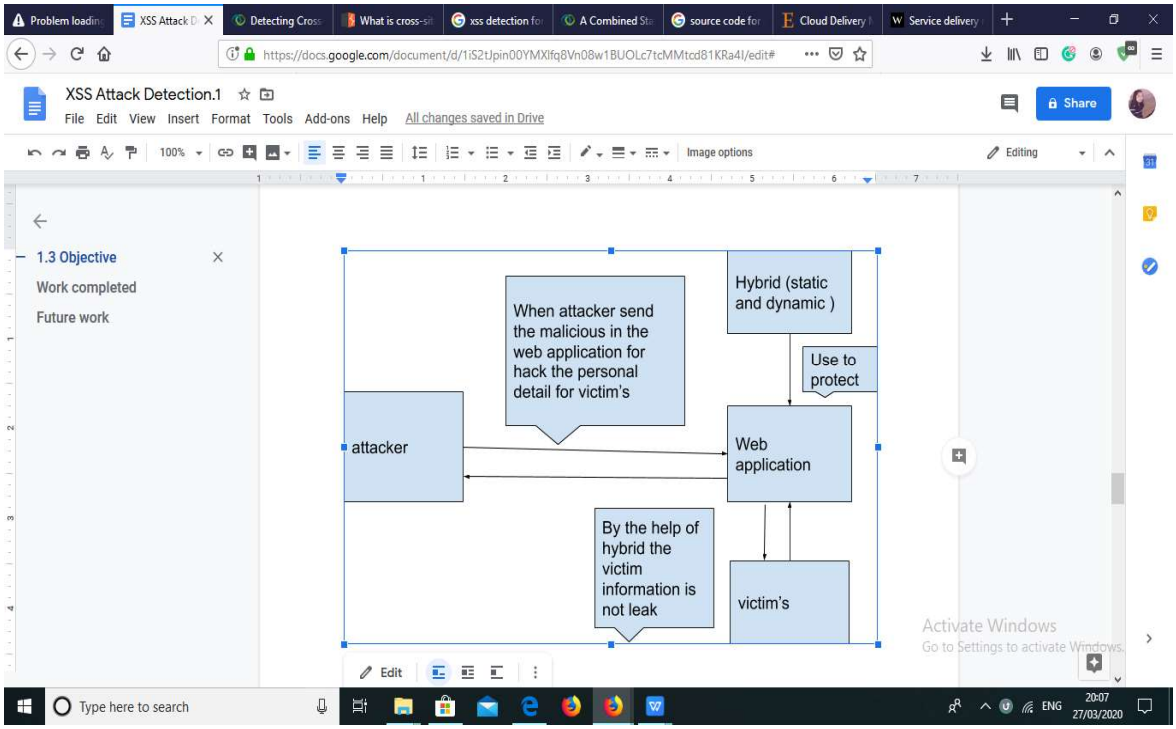


Figure 2. The Xss Attacker Attacks the Web Application for Stealing the Victim's Data from The Server Site

In this system Figure 2, it shows that whenever the xss attacker attacks the web application for stealing the victim's data from the server site, the fitness hybrid scanner protects the data from the attacker.

5.4. Hybrid Scanner

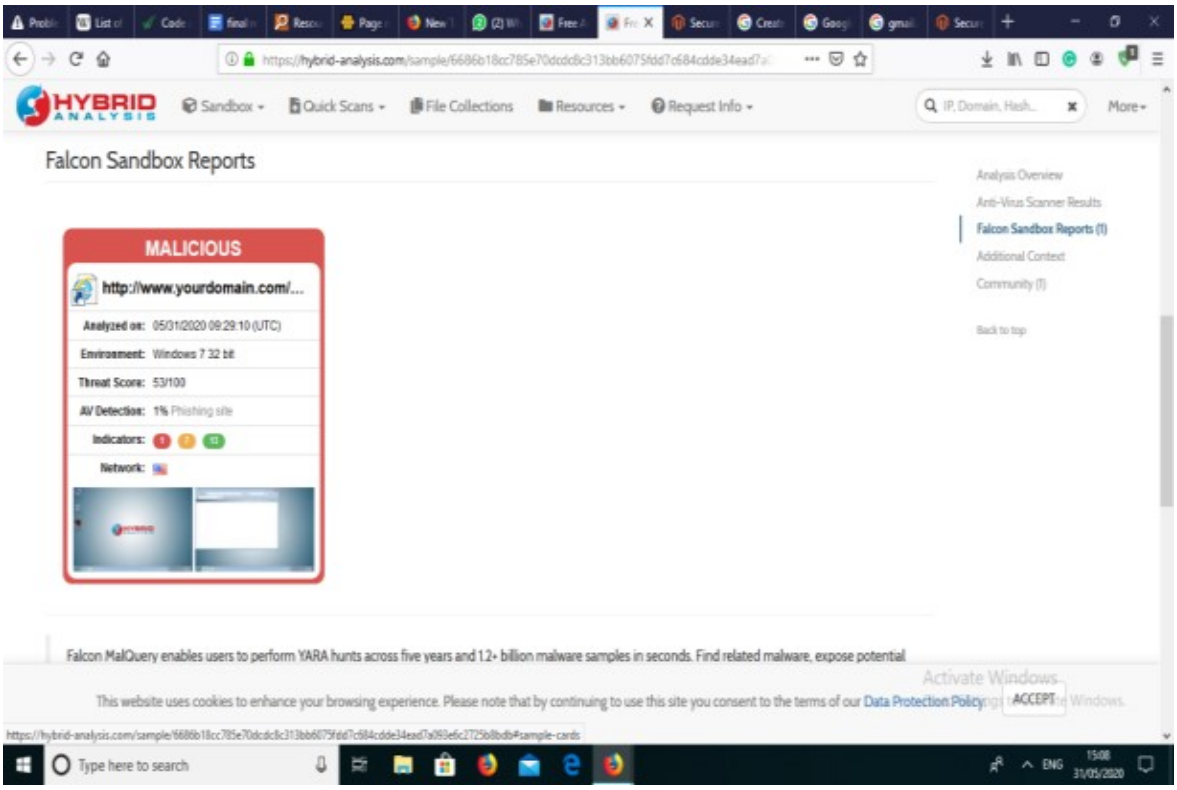
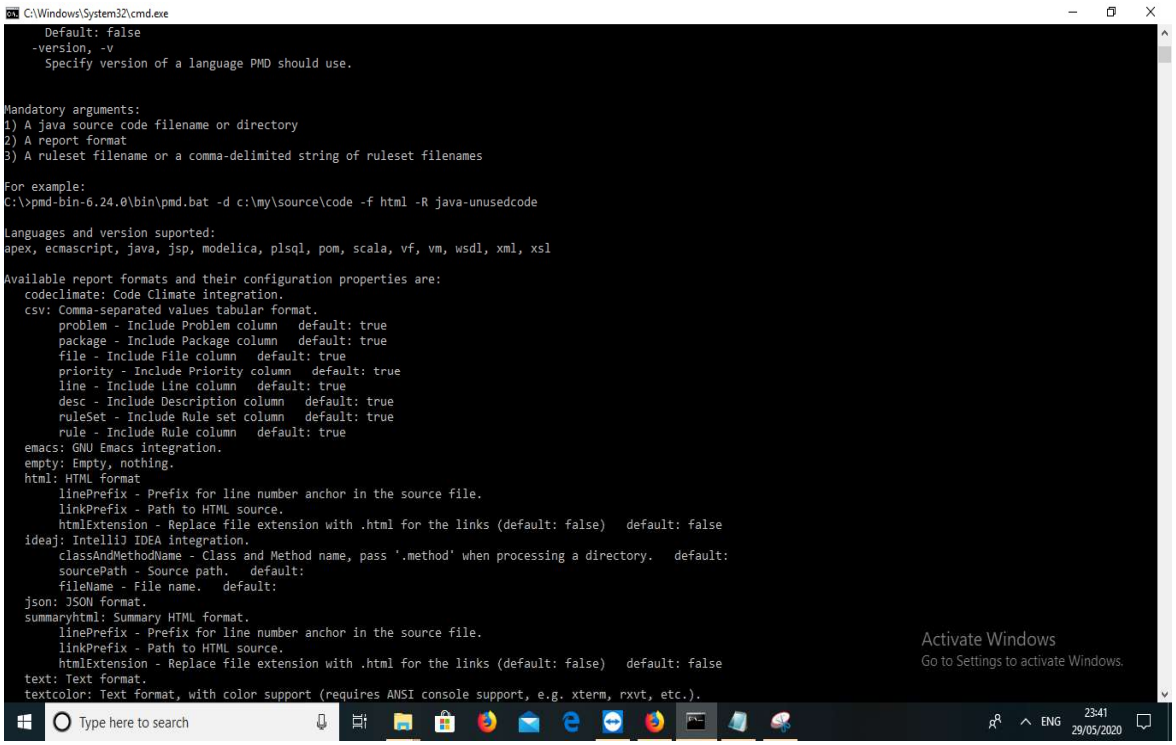


Figure 3. Hybrid scanner using multiple scanner fitness hybrid scanners tools protect the data from the XSS attacker

In this figure 3, reason to use the hybrid scanner, because the hybrid scanner is justify everything related to that URL or website like throat score, environment, av detection, etc also in the hybrid scanner using multiple scannerfitness hybrid scanners tools protect the data from the XSS attacker in this tool static and dynamic analysis .in static analysis is used to review of sources code prior to the program

5.5. Static Code Analysis

Using the static code analysis by the PMD tool helps us to find out bugs, vulnerabilities.



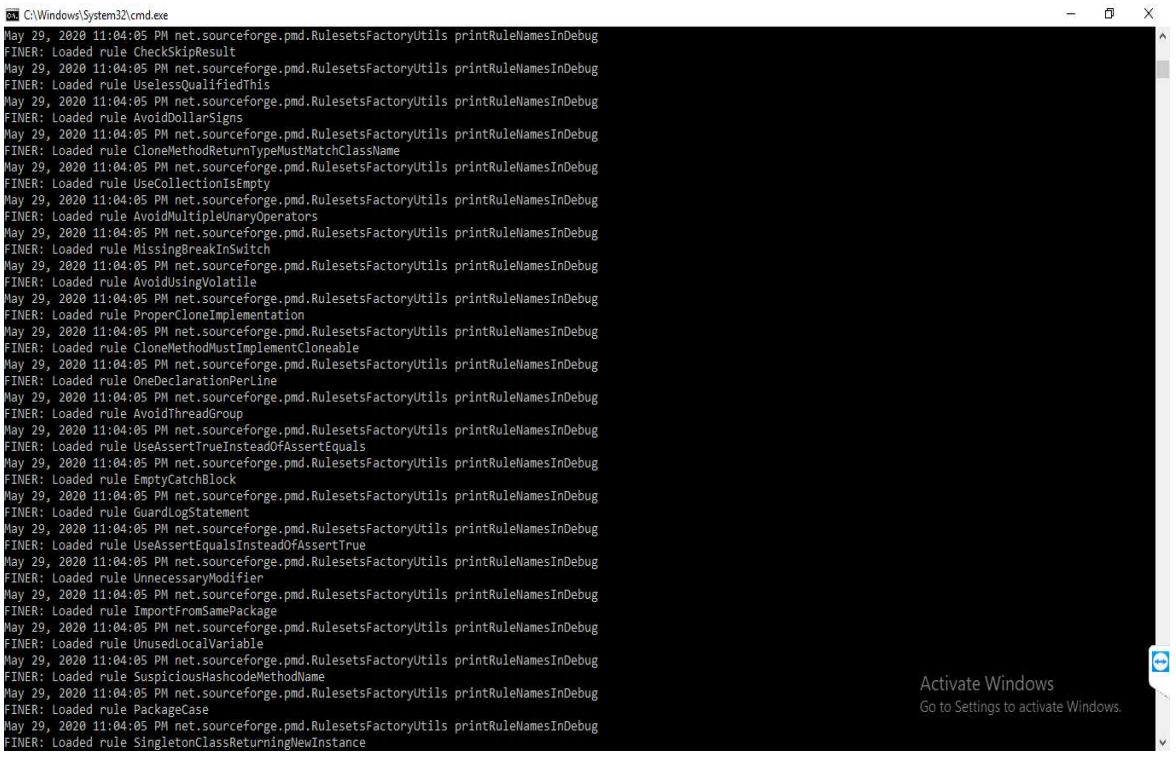


Figure 4. Static Code Analysis

It is a static code analysis that I run in a PMD tool. It is shown in figure 4 which I use the HTML command run the fitness algorithm.

5.6. Dynamic code analysis

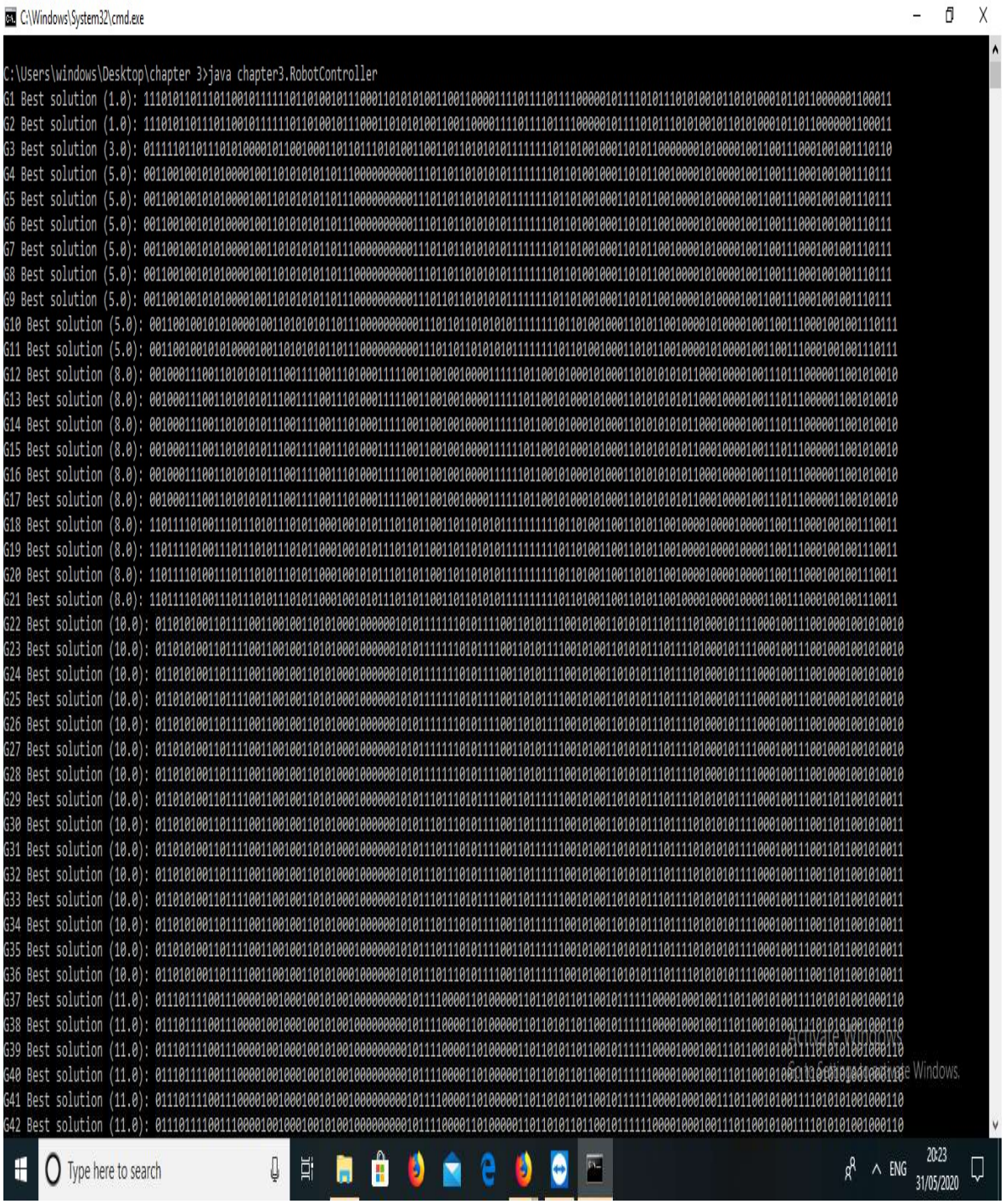


Figure 5. Dynamic code analysis

It is a dynamic code analysis which I run in J rat tool it is shown in figure 5, which I use the command to run the fitness algorithm

5.7. Static and Dynamic by Veracode With Plugin Recipes

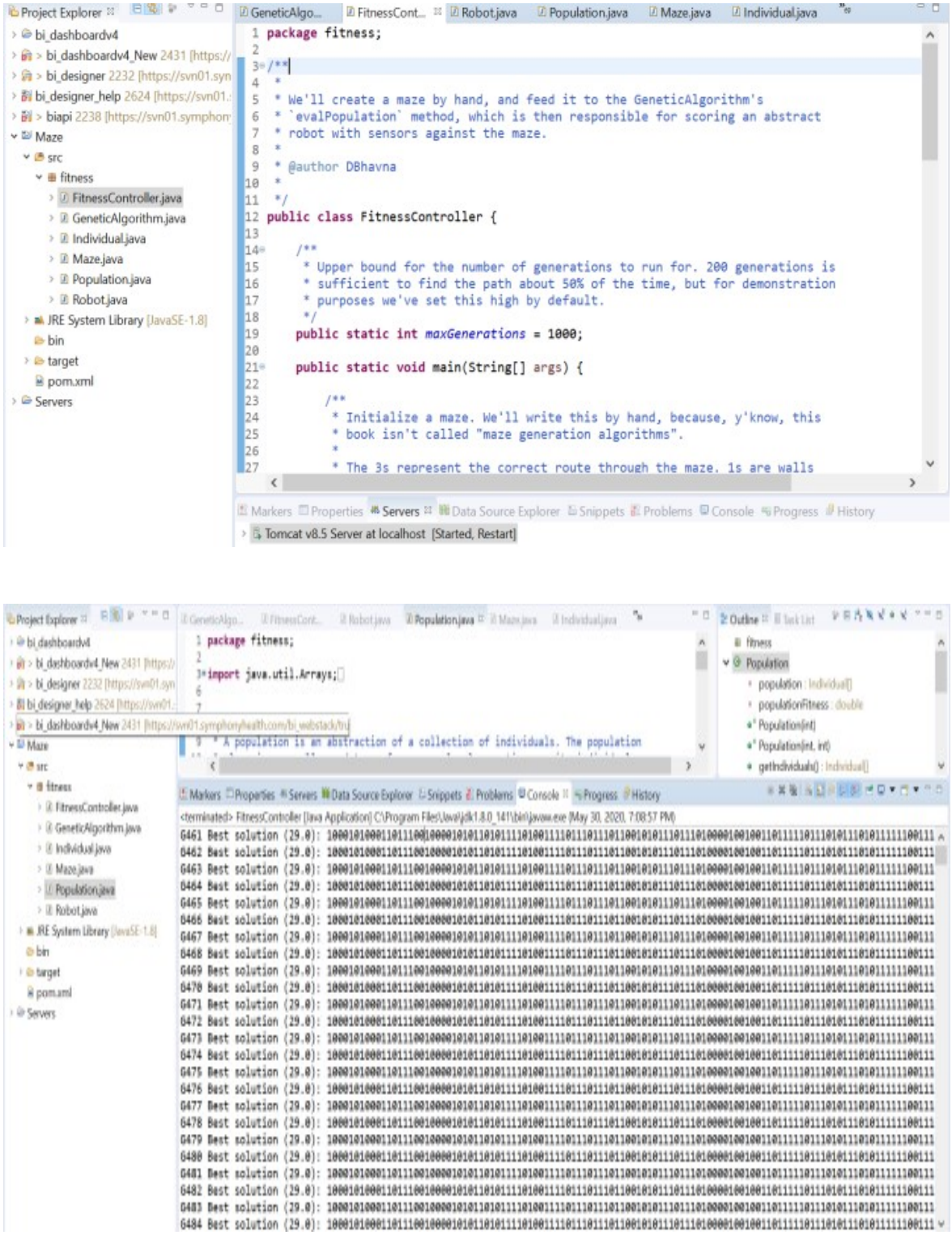


Figure 6. Static and Dynamic by VeracodeWith Plugin Recipes

Results of the eclipse of hybrid form are used to run the code to analyze the fitness algorithm in this.util.java library is used in arrays. It is shown that in eclipse tool code is running without and bugs and vulnerability

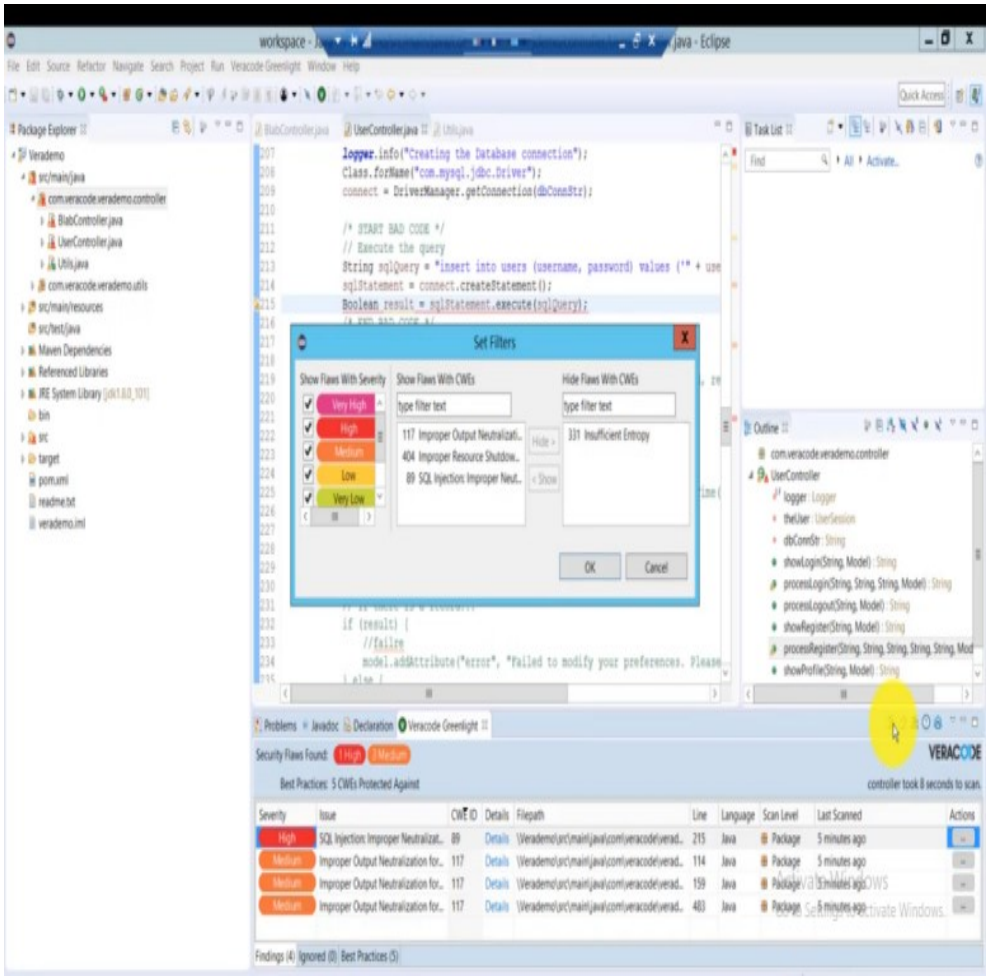


Figure 7. Output of the fitness algorithm

In this output, it is showing that the fitness algorithm shown in Figure 7.

- Show the accurate result and its performances are on the high rate
- It is using full to protect the data from the server site
- It is difficult for an attacker to break the fitness algorithm and access the data
- Also, in this, there is less false positive

6. Conclusion

With the goal of enhancing the accuracy and the rapidity of the process of security evaluation in a web application, the aim of my review project is to use hybrid code analysis with the genetic fitness algorithm to detect the XSS attacker and protect the personal data which is stored in the server. Fitness hybrid scanner is used to detect the XSS attacker and protect the server data from the XSS attacker with the help of the hybrid code analysis when the XSS attacker sent the malicious to the web application to encrypt the data on that time hybrid code scanner that web application and detected the attacker and vulnerabilities. Limitation of this paper is that the genetic fitness algorithm is a very complex calculation in which it is difficult to apply the algorithm.

7. Future Scope

In the future scope, this algorithm helps to protect the data for the XSS attack or any other attacker and also help to secure the server site in which clients data is stored a genetic fitness algorithm is complicated in which it is difficult to implement if the calculation of the algorithm is short or if we can apply some other method then it is easy to implement.

References

[1]. Chaudhary, P., Gupta, B. B., & Yamaguchi, S. (2016, October). XSS detection with automatic view isolation on an online social network. *In 2016 IEEE 5th Global Conference on Consumer Electronics* (pp. 1-5). IEEE

[2]. Piyush A Stoneware, P.A. and Thosar, S.D., 2016, August.

[3]. Chen, Boshen, and Yijie Shi. "Malicious Hidden Redirect Attack Web Page Detection Based on CSS.

[4]. Features." *2018 IEEE 4th International Conference on Computer and Communications (ICCC). IEEE*, 2018.

[5]. Ashish Mishra et al, 'Secure Cloud Storage Architecture for Digital Medical Record in Cloud Environment using Blockchain',*Elsevier SSRNInternational Conference on Intelligent Communication and computation Research,*Available at http://dx.doi.org/10.2139/ssrn.3565922, April 1, 2020.

[6]. Ashish Mishra et al, 'An Enhanced DDoS TCP Flood Attack Defence System in a Cloud Computing', *Elsevier SSRNInternational Conference on Intelligent Communication and computation Research*, Available at http://dx.doi.org/10.2139/ssrn.3565916, April 1, 2020

[7]. Ashish Mishra et al, 'A Review on DDOS Attack, TCP Flood Attack in Cloud Environment', *Elsevier SSRNInternational Conference on Intelligent Communication and computation Research,* Available at https://ssrn.com/abstract=3565043,March 31, 2020

[8]. J Mishra. Fractional hyper-chaotic model with no equilibrium, Chaos, *Solitons & Fractals* 116, 2018,43-53.

[9]. J Mishra. *Analysis of the Fitzhugh Nagumo model with a new numerical scheme Discrete & Continuous Dynamical Systems*-S, (2018), 781.

[10]. J Mishra. Modified Chua chaotic attractor with differential operators with non-singular kernelsChaos, *Solitons & Fractals* 125, (2019) 64-72.

Author's Biography

BhavnaDwivedi is currently pursuing Post Graduate in Jain University, Bangalore in Cyber Security also I am completed my engineering in Information Technology fromGyan Ganga institution of technology and sciences, Jabalpur.In that my project is based in Agro-stream.

How to Cite

Dwivedi, Bhavna (2019). Scanning the Database with The XSS Detection Using the Fitness Algorithm. *International Journal of Machine Learning and Networked Collaborative Engineering*, 3(04) pp219 -228.

doi : https://doi.org/10.30991/IJMLNCE.2019v03i04.004