International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-2, December, 2019

vSTAAS - an Integrated Pen-Testing Tool

Grusha Kaur Sahni, K. Ravindranath

Abstract*: With the increasing threat in the cyber world, securing our networks and applications are becoming costlier. An enormous quantity of cash is being spent on direct or indirect resources. Along with this, with the increasing number of tools in the market, it is leading to confusion in the IT Industry. How can we reduce the amount spent by the organization on these resources without compromising the company's security and get deep security insight on projects? For this, vSTAAS orchestrates the process of testing applications for flaws and vulnerabilities by Integrating Solutions, Increasing Accuracy, Simplify Management, and Accelerates the testing of Third-Party Software. It offers Strong, actionable intelligence with RPA, Machine Learning, and AI Automation concerning security requirements across the SDLC. The end to end automated Application & Infrastructure security solution helps users to secure their web/mobile/infra applications. It provides cost-effective solutions with necessary remediation and posts remediation revalidation measures. The Centralized portal helps customers to review the report on vulnerability risk remediation status with high-quality end to end testing across SDLC phases.

***Keywords* : Pen-Testing, SAST, DAST, Mobile, API, Network, Automation, Risk rectification**

I. INTRODUCTION

Penetration testing, also known as pen testing or moral hacking, is that the follow of testing an automatic data processing system, network, or net application to search out security vulnerabilities that Associate in Nursing wrongdoers might exploit. Penetration testing may be machine-controlled with software package applications or performed manually. The objective of penetration testing is to spot security weaknesses. Penetration checks are generally called white hat attacks as a result of a real pen test that the great guys are trying to interrupt in.

Web security testing aims to search out security vulnerabilities in net applications and their configuration. The first target is the application layer, Testing the protection of an online application usually involves causing differing types of input to electrify errors and create the system behave in unexpected ways.

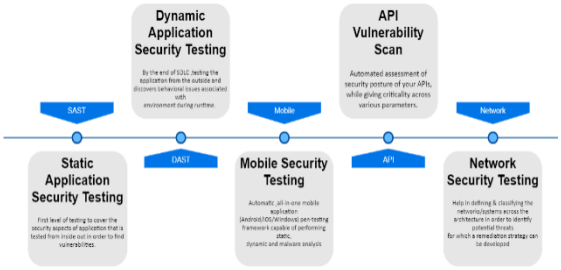


Fig 1: Sub-Divisions of Pen- Testing

These, therefore, referred to as "negative tests," examine whether the system is doing one thing it isn't designed to try and do. It's equally necessary to check that different options are enforced in a very secure manner. The goal is to confirm that the functions exposed within the net application are secure.

Static application security testing (SAST), or static analysis, could be a testing methodology that analyses ASCII text file to search out security vulnerabilities that create your organization's applications vulnerable to attack. It's additionally referred to as white box testing. SAST takes place early within the software package development life cycle (SDLC) because it doesn't need an operating application and might occur while not code being dead. It helps developers determine vulnerabilities within the initial stages of development and quickly resolve problems while not breaking builds or passing on vulnerabilities to the ultimate unleash of the appliance.

Dynamic application security testing (DAST) could be a method of testing an Associate in Nursing application or software package in an Associate in the Nursing operational state. This type of testing is useful for industry-standard compliance, and general security protections for evolving comes. DAST involves operational testing and should be referred to as "behavioral testing" this tester usually realize issues that aren't joined explicitly to a code module; however, it happens throughout use.

Mobile application security testing testing method includes:

- Interacting with the appliance and understanding; however, it stores receives and transmits information By Decrypting and encrypting components of the appliance.
- Utilizing dynamic analysis and penetration testing to judge the effectiveness of security controls (e.g., authentication and authorization controls) that are used inside the appliance.

Network security is the method of preventing unauthorized activity across a given networking infrastructure. Associate in Nursing wrongdoer solely must be right just one occasion to compromise a network.

Revised Manuscript Received on December 30, 2019.
* Correspondence Author
Grusha Kaur Sahni*, M.Tech - Cyber Security and Digital Forensics, Department of CSE, KLEF, Vaddeswaram, A.P, India. Email: grushakaursahni30@gmail.com
Dr. K Ravindranath, Associate Professor, Department of CSE, KLEF, Vaddeswaram, A.P, India.. Email: Ravindra_ist@kluniversity.in

However, the team accountable for securing Associate in Nursing organization's network has no space for error. For this reason, it's essential to require a holistic approach, instead of merely configuring a firewall. One key component of this process is threat modelling. Conducting a threat model identifies potential weaknesses that might be evaluated before conducting a network penetration check.

II. LITERATURE REVIEW

According to Bau evaluated and tested eight commercially vulnerable scanners well-known applications. When examining the results, they deduced that almost all scanners had detected SQL injection vulnerability and mirrored XSS vulnerability. Different vulnerabilities weren't detected in the least or were detected with a meager rate.

Ferreira [2] and al. careful a vulnerable net application and tested some vulnerability scanners against it. [9] The result was that the scanners couldn't observe mirrored XSS and SQL injection. However, they might observe hold on XSS and Cross-Site Request.

The open-supply net vulnerability scanners are consistent with OWASP [3] prime. Then, they compared their detection capabilities, to spot the scanners .

Sudo test three scanners of vulnerabilities [4] against three different net applications. Alyssa [5]and al. centered on the detection of hold on XSS.

As known by Fahmida[6], despite the very fact that cyber-attacks and malware are rocketing during this century of data, several corporations and organizations these days are still not proactively testing their infrastructure to identify security vulnerabilities. [4] Once connected to the net, companys [7]. As a result, each organization must shield their systems against unauthorized access severely.

Kind of like hackers, [8] whacky are individuals to require advantage of weaknesses of AN IT system to accumulate contraband edges, social attention, or respect from a selected community, a hacker cluster, for instance. On the opposite hand, [10] script-kiddies are sometimes intruders lacking in-depth information and sometimes driven by curiosity to attack straightforward targets they'll realize with obtainable tools obtained from the net.

III. ARCHITECTURE

vSTAAS Consists of 5 main modules which check vulnerability or loopholes of any application that needs to be tested for Security Issues.

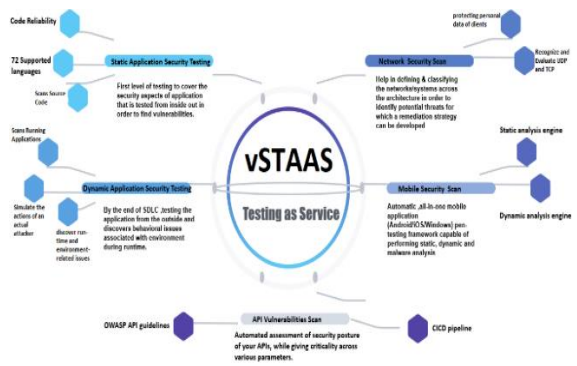


Fig 2: vSTAAS Architecture

IV. IMPLEMENTATION

The tool has been in-built such a way that it may be upgraded to feature more functionalities. Modules for penetration testing of those vulnerabilities also can be another to create it additional powerful.

The algorithms and techniques presently used may be changed or replaced with additional advanced and economic ones for higher accuracy of results.

Port scanner may be created rib to boost the speed and potency of the scan.

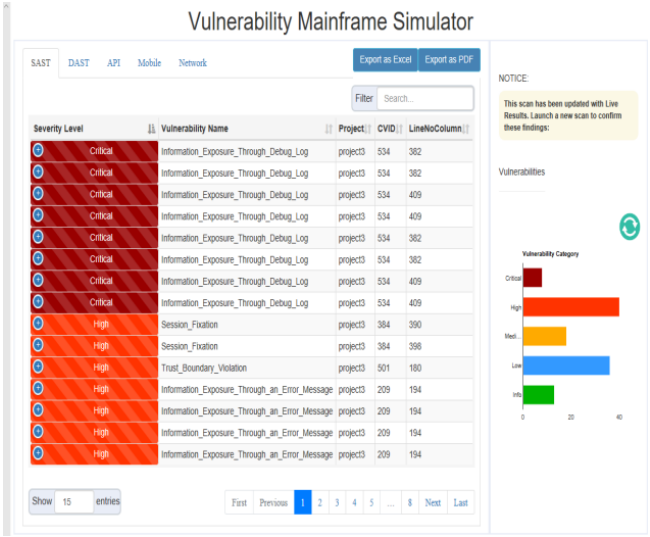
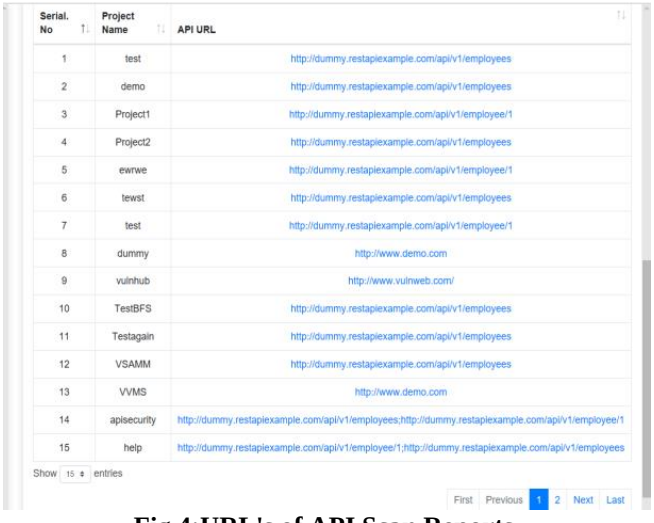


Fig 3: Vulnerability Mainframe Stimulator

By exploiting the options of Python three, an interface version of the tool also can be developed to any increase the benefit of use.



Serial. No	Project Name	API URL
1	test	http://dummy.restapiexample.com/api/v1/employees
2	demo	http://dummy.restapiexample.com/api/v1/employees
3	Project1	http://dummy.restapiexample.com/api/v1/employee/1
4	Project2	http://dummy.restapiexample.com/api/v1/employees
5	ewrwe	http://dummy.restapiexample.com/api/v1/employee/1
6	tewst	http://dummy.restapiexample.com/api/v1/employees
7	test	http://dummy.restapiexample.com/api/v1/employee/1
8	dummy	http://www.demo.com
9	vulnhub	http://www.vulnweb.com/
10	TestBFS	http://dummy.restapiexample.com/api/v1/employees
11	Testagain	http://dummy.restapiexample.com/api/v1/employees
12	VSAMM	http://dummy.restapiexample.com/api/v1/employees
13	VVMS	http://www.demo.com
14	apisecurity	http://dummy.restapiexample.com/api/v1/employees;http://dummy.restapiexample.com/api/v1/employee/1
15	help	http://dummy.restapiexample.com/api/v1/employee/1;http://dummy.restapiexample.com/api/v1/employees

Show 15 entries

First Previous 1 2 Next Last

Fig 4:URL's of API Scan Reports

Apart from a police investigation of the SQLI vulnerabilities, additional modules are another for the detection of different significant vulnerabilities like XSS. Buffer overflows OS command injections.

V. RESULTS AND DISCUSSION

The total Vulnerabilities found within the project is represented within the graph 5.

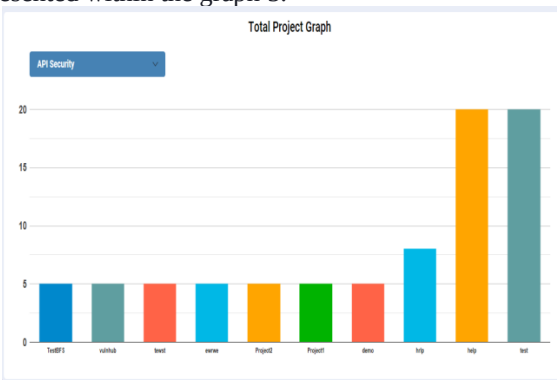


Fig 5: Total Project Graph

The Vulnerabilities of the project is displayed for every part like SAST, DAST, API, Mobile, Network in figure 6.

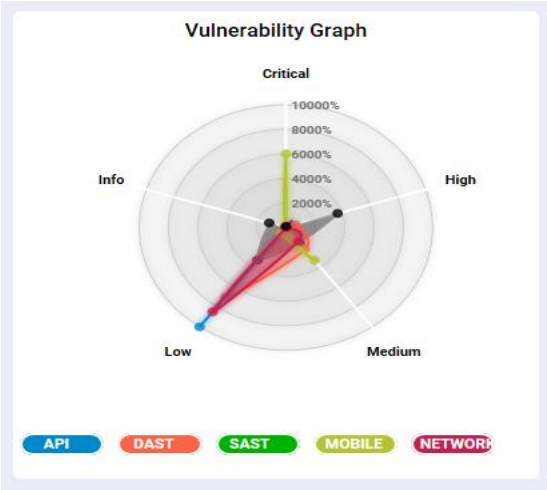


Fig 6: Vulnerability Graph

VI. CONCLUSION AND FUTURE SCOPE

vSTAAS helps you perform security engineering by increasing your team's resources, increasing risk visibility by ever-changing all of your info into Valuable information. Additionally, the current, the tool is intended for simplicity; users ought to notice no distinction between their terminal application and the one enclosed in vSTAAS. It's developed with a specialized set of functionalities that permits users to improve their work. This paper proposes the most straightforward tool for integrated pen testing which exports in CSV format from Web UI,

Future work is to search out additional vulnerabilities that are important and to create an ideal open supply tool that supported those vulnerabilities, which can be free and straightforward to use and reduces time complexness.

REFERENCES

1. J. Bau,, E. Bursztein, D. Gupta, and J. Mitchell, 2010 "State of the Art: automatic Black-Box net Vulnerability Testing," in Proc. 2010 IEEE conference on Security and Privacy, pp. 32-345.
2. A. M. Ferreira, and H. Kleppe, "Effectiveness of automatic Application Penetration Testing Tools," Master treatise., Master Education SNE/OS3, University of European country|national capital}, Netherlands.
3. Fakhreldeen A. and Eltyeb E., 2014 "Assessment of Open supply net Application Security Scanners," faculty of engineering science and data Technology, KAU, Khulais, Asian country.
4. L. Suto, 2010 "Analyzing the Accuracy and Time prices of net Application Security Scanners,"BeyondTrust, http://www.beyondtrust.com/Content/whitepapers/Analyzing-the-Accuracy-and-Time-Costs-of-Web-Application-Security-Scanners.pdf
5. Yuliana M., 2012 "Security analysis of net Application Vulnerability Scanners' Strengths and Limitations victimization Custom net Application," California State University.
6. Security Testing of net Applications: a hunt based mostly Approach for Cross-Site Scripting Vulnerabilities, Andrea Avancini, Mariano Ceccato , 2011- eleventh IEEE International operating Conference on ASCII text file Analysis and Manipulation.
7. Special section on testing and security of net systems Alessandro Marchetto. printed online: fourteen Gregorian calendar month 2008 © Springer Verlag 2008.
8. Idea: Automatic Security Testing for net Applications. Thanh-Binh Dao1 and Etsuya Shibayama2 one Dept. of Mathematical and Computing Sciences, Tokio Institute of Technology, two-12-1 O-okayama Meguro Tokio Japan 2 data Technology Center, The University of Tokio,2-11-16 Yayoi Bunkyo-ku Tokio Japan F. Massacci, S.T. Redwine Jr., and N. Zannone (Eds.): ESSoS 2009, LNCS 5429, pp. 180–184, 2009. laptop Springer-Verlag Berlin Heidelberg 2009.
9. Automatic take a look at Approach of net Application for Security (AutoInspect). Kyung Cheol Choi and Gun atomic number 67 Lee, Springer-Verlag Berlin Heidelberg 2006.
10. SUPPORTING SECURITY TESTERS IN DISCOVERING INJECTION FLAWS. Sven T¨urpe, Andreas Poller, Gregorian calendar month Trukenmuller, J¨urgen cloth and Christian Bornmann, Fraunhofer-Institute for Secure data Technology SIT, Rheinstrasse seventy five,64295 Darmstadt, Germany, 2008 IEEE,Testing: educational & Industrial Conference - observe and analysis Techniques.

AUTHORS PROFILE

Grusha Kaur Sahni is a student pursuing her M.Tech in the field of Cyber Security and Digital Forensics -Department of CSE, KLEF, Vaddeswaram, A.P, India. She is a University Innovation Fellow from the Design at Stanford, Hasso Plattner Institute at Stanford University since spring2017 cohort. She is a graduate who completed her B.Tech at Godavari Institute of engineering and technology, Rajahmundry, Andhra Pradesh, India.

Dr. K Ravindranath received a Ph.D degree from Achrya Nagarjuna University in 2016. Currently, he is Associate Professor of Computer Science & Engineering at K L University, Vaddeswaram, AP, India. Prof. Ravindranath's research interests include Cloud, Mobile Clouds and Security. His work has appeared in over 24 publications. He is a member of ACM, Senior Life member in Computer Society of India.