Mini Project Report on

Vulnerability Testing & Analysis using Serverless Computing

Submitted by

Name of Student	Class	Roll No.
1. Aayush Joshi	TE4	50
2. Rutuja Kumbhar	TE4	53
3. Akshat Mehta	TE4	57
4. Harshith Shetty	TE4	67

Under the guidance of

Mr. Umesh Patil

DEPARTMENT OF COMPUTER ENGINEERING

SHAH AND ANCHOR KUTCHHI ENGINEERING

COLLEGE CHEMBUR, MUMBAI - 400088.

2021-2022

www.shahandanchor.com **Mahavir Education Trust's** **Tel: 022 25580854**

SHAH & ANCHOR KUTCHHI ENGINEERING COLLEGE

Mahavir Education Trust Chowk, W.T. Patil Marg, Chembur, Mumbai 400 088

Affiliated to University of Mumbai, Approved by D.T.E. & A.I.C.T.E.
ISO
Awarded accreditation for Computer & Information Technology Engineering by NBA
(for 3 years w.e.f. 1st July, 2019)

Certificate

This is to certify that the report of the mini project entitled

Vulnerability Testing & Analysis using Serverless Computing

is a bonafide work of

Name of Student	Class	Roll No.
1. Aayush Joshi	TE4	50
2. Rutuja Kumbhar	TE4	53
3. Akshat Mehta	TE4	57
4. Harshith Shetty	TE4	67

submitted to the

UNIVERSITY OF MUMBAI

during semester V

in

COMPUTER ENGINEERING DEPARTMENT

Approval for Mini Project Report for T. E. Semester V

This mini project report entitled “Vulnerability Testing & Analysis using Serverless Computing” by Aayush Joshi, Rutuja Kumbhar, Akshat Mehta and Harshith Shetty is approved for the partial fulfilment of the requirement for the completion of Semester V .

Name and Sign of Internal Examiner ______

Name and Sign of External Examiner ______ _

Date:

Place:

Declaration

We declare that this written submission represents our ideas in our own words and where others' ideas or words have been included, we have adequately cited and referenced the original sources. We also declare that we have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in our submission. We understand that any violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

Name of Student	Class	Roll No.
1. Aayush Joshi	TE4	50
2. Rutuja Kumbhar	TE4	53
3. Akshat Mehta	TE4	57
4. Harshith Shetty	TE4	67

Date:

Attendance Certificate

To,
The Principal
Shah and Anchor Kutchhi Engineering College,
Chembur, Mumbai-88

Date:

Subject: Confirmation of Attendance

Respected Sir,

This is to certify that Second year (SE) students Aayush Joshi, Rutuja Kumbhar, Akshat Mehta, Harshith Shetty have duly attended the sessions on the day allotted to them during the period from 18/07/2021 to 25/10/2021 for performing the Project titled Vulnerability Testing & Analysis using Serverless Computing.
They were punctual and regular in their attendance. Following is the detailed record of the student’s attendance.

Attendance Record:

Date	Student1	Student2	Student3	Student4
	Present/Absent	Present/Absent	Present/Absent	Present/Absent
4/8/2021	Present	Present	Present	Present
11/8/2021	Present	Present	Present	Present
18/8/2021	Present	Present	Present	Present
25/8/2021	-	-	-	-
1/9/2021	-	-	-	-
8/9/2021	-	-	-	-
15/9/2021	-	-	-	-
22/9/2021	-	-	-	-
29/9/2021	-	-	-	-

Signature and Name of the Guide

Abstract

The purpose of the project is to carry out vulnerability tests and detect if the Server or the Website is secure or not. During this project we are going to introduce "Vulnerability Testing & Analysis using Serverless Computing". In the modern scenario web security is one of the key aspects for any developer or organisation to sustain, for this whenever an organization needs to check on their websites for knowing how secure they are they need to consult a security expert for performing vulnerability tests, which is a costlier approach. Our project helps such organizations to perform these vulnerability tests and check if they are really secure or not at an extremely low cost. Our project focuses on a Serverless approach which will use Cloud Operations for testing purposes. Its function is to accept the URL of the website from the user and perform various security inspections and provide a security report based on the tests done. This report will showcase how secure their website is. The serverless vulnerability analyser we are going to create is known as VASCOT. The name VASCOT is a combination of initials which describes VULNERABILITY ANALYSIS using SERVERLESS CLOUD OPERATION TEST. This title itself describes that the product will mainly focus on vulnerability analysis using a serverless platform.

Table of Contents

List Of Figures

List Of Tables

Chapter 1
Introduction

Our project focuses on the Serverless Framework which will provide a new way to define basic integration tests for functions with HTTP endpoints. Its goal is to enable you to test your serverless applications without having to manually write a lot of code to do so. Tests are defined in a new file, serverless. This framework can also be used for performing penetration testing using the serverless cloud.

It allows the organization to carry out vulnerability tests using serverless cloud functions. without using any on-premise resource. In the background when a user enters the URL of the website or the IP address of the server and clicks on submit button then an API request is made to AWS lambda using Aws API gateway which will trigger the AWS lambda. Then AWS lambda carries out the test by collecting the parameters (the URL of the website or the IP address of the server) and performing the Vulnerability test on the user’s server.

The main perspective of the system is to create a system that can replace the unwanted financial flow of the organization in a cost-efficient way. When an organization needs to check on their websites for knowing how secure they are they need to consult a security expert for performing vulnerability tests, which is a costlier approach. Our product helps such organizations to perform such vulnerability tests and check if they are secure or not at an extremely low cost and without any help from Security Expert or any platform such as Kali Linux. It will be server-less testing using cloud service.

Chapter 2
Literature Survey

Sr. No.	Author/Title/Year	Work done /Algorithm/concept /Idea presented in the paper	Remarks
1.	Ej Miguel Francisco Caliwag, Angela Caliwag, Wansu Lim Department of Aeronautics, Mechanical and Electronic Convergence Engineering Kumoh National Institute of Technology Gumi-si, Republic of Korea. AWS Data Visualization using DynamoDB and Lambda July 2021	Created a system that contains serverless Instance like AWS lambda that integrate with S3 bucket and Dynamo Db and triggers a function when data is processed.	Using Server less service helps in creating a well structure system for data processing in system using ML or NLP.
2.	Soohyun Lee, Department of Biomedical Informatics, Harvard Medical School, Boston, MA. USA. A serverless architecture for frequency-based HTTP request filtering against distributed denial-of-service (DDoS) attacks July 2021	Created an serverless architecture which use the CloudWatch to collect the data and transfer it using api gateway and trigger serverless function to trigger notification to the user.	Implementing anti-DDoS measures is challenging partly because it requires handling of a large volume of data but without using such capacity except when an attack happens (Dotson, 2019).A serverless architecture may be a good fit for this kind of problem,
3.	Sebastian Risco ´ · German Molt ´ o´ · Diana M. Naranjo · Ignacio Blanquer Serverless Workflows for Containerized Applications in the Cloud Continuum June 2021	Using Serverless Computing for workflow created SCAR FrameWork which is an open source Platform	Cloud computing continuum that features underlying elasticity in the provisioning of resources and the ability to Cloud burst into a public Cloud using a serverless approach.
4.	Wafaa Al-Kahla, Ahmed S. Shatnawi, Eyad Taqieddin Jordan University of Science & Technology A Taxonomy of Web Security Vulnerabilities June 2021	Classification of vulnerability detection tools, moving and defining vulnerabilities and their prevalence, their ultimate impacts on the business entity, and their detection tools at different web application architectural levels.	Web application vulnerability results from misconfiguration, flaws in the design, implementation, operation, or management at the different levels of a web application
5.	Thitima Srivatanakul, Tyshaun Moore York College, City University of New York, New York, USA Promoting Security Mindset through Hands-on Exercises for Computer Science Undergraduate Students May 2021	Understanding the means that attackers use to exploit the system allows developers to gain a deeper understanding of how a successful attack exploits a vulnerability in the system.	The security mindset concept allows developers to gain a deeper understanding of how a vulnerability can be successfully exploited.
6.	Yeni Kusumaningrum, Wella, Information System Department, Universitas Multimedia Nusantara, Tangerang, Indonesia Adoption of COBIT5 Framework in Risk Management for Startup Company April 2021	For small or medium scale businesses, there are no or very few research works are done. Risk management is important for a company to lessen its impact on profit/losses. It can increase negative risks to the goals of a company, where the company's dependence on IT will further increase the impact of risk on the company.	Poor management of IT will result in critical business processes. Risks that arise need to be regulated to minimize losses if any risk occurs.

Sr. No.	Author/Title/Year	Work done /Algorithm/concept /Idea presented in the paper	Remarks
7.	Muhamad Agreindra Helmiawan, Esa Firmansyah, Irfan Fadil, Yanvan Sofivan, Fathoni Mahardika, Agun Guntara (STMIK Sumedang, Sumedang, Indonesia) Analysis of Web Security Using Open Web Application Security Project 2020	The use of OWASP 10 has guidelines for checking website security standards and website-based information systems so that theft and dissemination of data by irresponsible parties can be avoided so that the sustainability of the website and website-based information systems can continue to be used in the long term.	OWASP 10 can be used for checking out the top 10 vulnerabilities in a website. OWASP plays a great role in the security domain of websites. OWASP can be used to mark the threat level of the vulnerability found in a website.
8.	Wang Ze Wuhan Business University, Wuhan, China Design and Implementation of Core Modules of WEB Application Vulnerability Detection Model 2019	A vulnerability detection system based upon crawlers and feature detection are being proposed. The paper discusses the related technologies of the web and their potential dangers, and mainly analyses the injection and XSS vulnerabilities.	The system is helpful for a foundation of understanding the implementation and designing of a system for detecting vulnerabilities.
9.	Balume Mburano & Weisheng Si (School of Computing, Engineering and Mathematics, Western Sydney University, Australia) Evaluation of Web Vulnerability Scanners Based on OWASP Benchmark 2019	It includes the process of reviewing a web vulnerability scanner based on the OWASP standard. This standard plays a vital role in benchmarking any web vulnerability scanner.	The OWASP standard helps to understand a particular scanner its comparisons and its ranking in the industry. .
10.	K Nirmal (NIT, Trichy, India) B. Janet (NIT, Trichy, India) R. Kumar (Wipro Technologies, India) Web Application Vulnerabilities - The Hacker's Treasure 2018	Explained how different vulnerabilities in web applications can be exploited by hackers in order to affect not only the business but also the end-users whose information will be subjected to risk.	Web Application vulnerabilities are not restricted or specific to a particular domain or industry. This threat spans across every industry. It is a common misconception that web vulnerabilities are a threat only to banking and other financial domains.

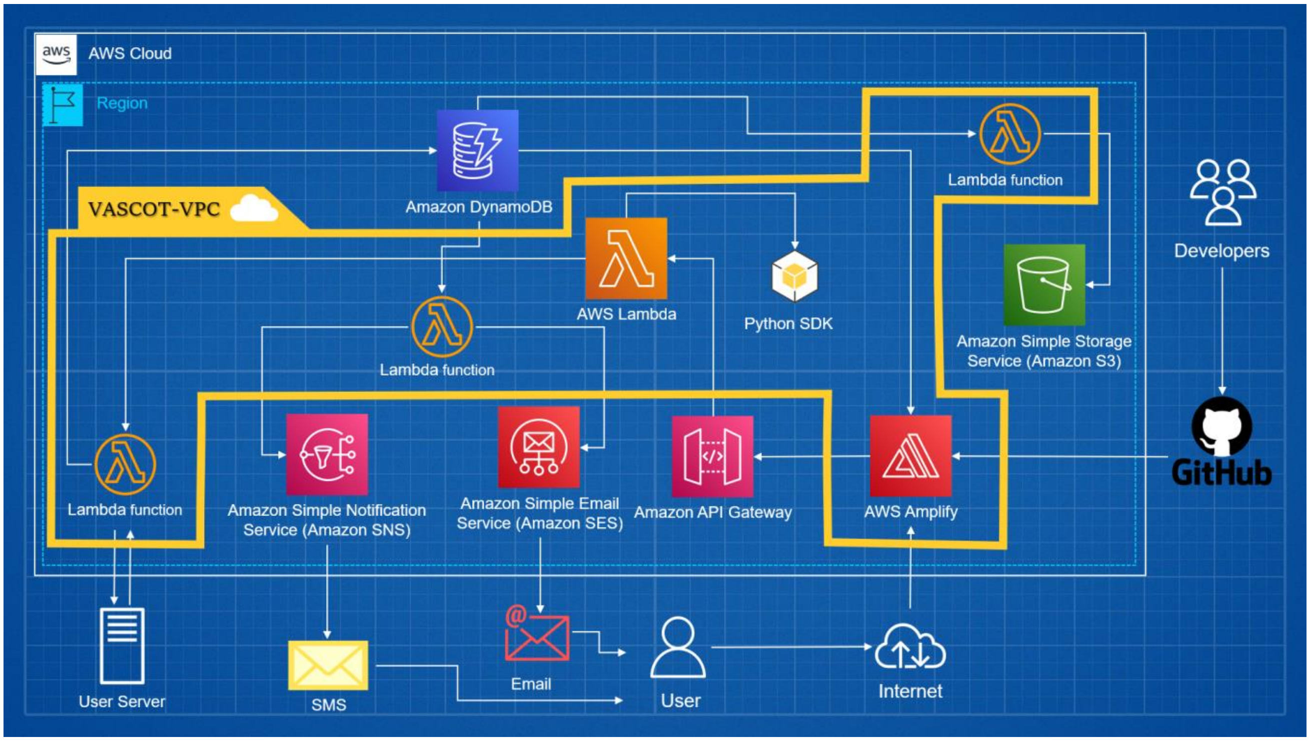
Table 2.1

Chapter 3
Problem Statement

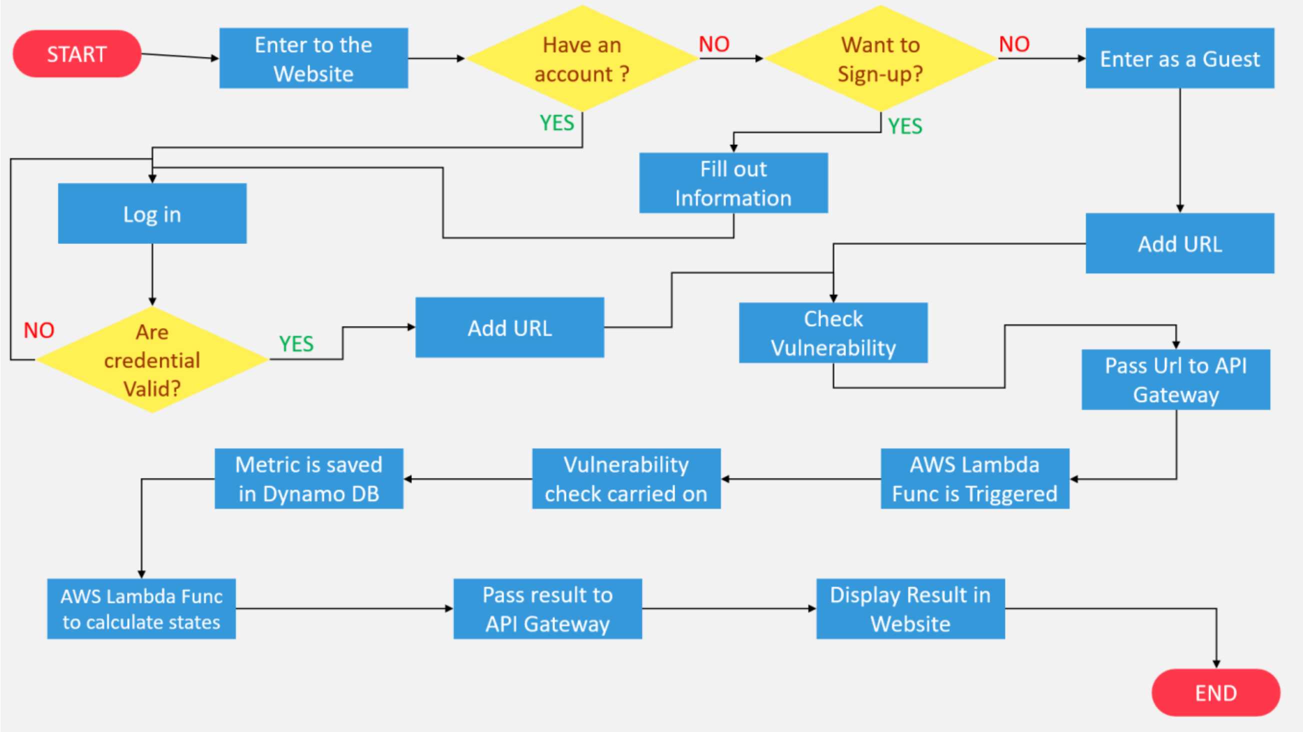
In the IT sector, the security of the platform is one of the crucial aspects to sustain and progress in the field. It said that a server or website is secure if and only if it sustains against the vulnerabilities that basically means if it passes the standard Vulnerability & Penetration tests. For an organization to carry out the Vulnerability test they avail a security engineer who can carry out the vulnerability test using Linux systems. This leads to an increase in the expense of the organization as the Remuneration of the Security Engineer and the Linux system maintenance cost using server less cloud operations. We are building a Web Application Framework that reduces the cost of the Organization and also helps in carrying out such vulnerability tests and detect if the Server or the Website is secure or not.

Chapter 4
Project Design

4.1 System Block Diagram



4.2 Flowchart



Chapter 5
Implementation Details

5.1 Module & Implementation

5.1.1 Working

The website shows login options where we can register as new user, login in existing account or proceed as guest user. Once selected the login option, user must select protocol suitable for his website and must type URL of website/IP address of his server. After giving the details, it will generate a report analysing which vulnerabilities found and whether website is secure or not. Detailed solutions of simulation questions are provided along with the graphs.

The above block diagram gives the clear view of the workflow of VASCOT. If there is any problem in provided details by user or if the given URL does not exist, then the user interface will show necessary message. In case of any issue, user can communicate with VASCOT team through given contact details.

5.1.2 Implementation

For the software part of the system, python IDE and web programming IDE is used. Also, for serverless hosting we used various AWS services like lambda function to carry out vulnerability test, API Gateway, amplify to host platform, DynamoDB for database maintenance and other serves like S3, SES, SNS. For hardware purpose we used device for development, virtual test server.

5.1.3 Layout

5.1.3.1 Home Page

Web page showing the homepage of the website with the title and menu bars at the top of the page is given.

5.1.3.2 Login Page

Web page containing login options is shown. Here, it will provide options to login, register or proceed as guest user.

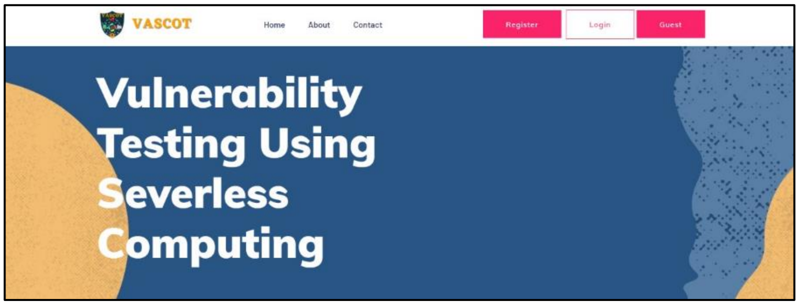
5.1.3.3 Request for checking vulnerabilities

Web page where user has to select protocol of his website and enter website URL is shown.

5.1.3.4 Report Generation

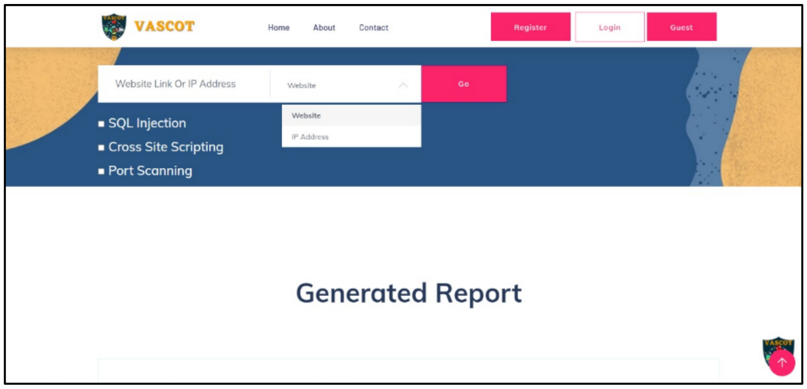
The Web Page which will show vulnerability report is shown in fig. 5. It will give the list of vulnerabilities which are provided by website showing which vulnerabilities are detected or not followed by how much website is secure.

5.2 Snapshots



Vulnerability Testing Using Severless Computing

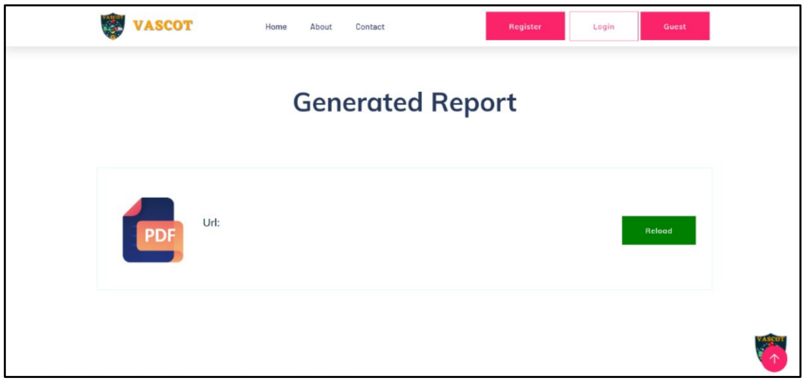
Home Page
Fig 5.2.1



- SQL Injection
- Cross Site Scripting
- Port Scanning

Generated Report

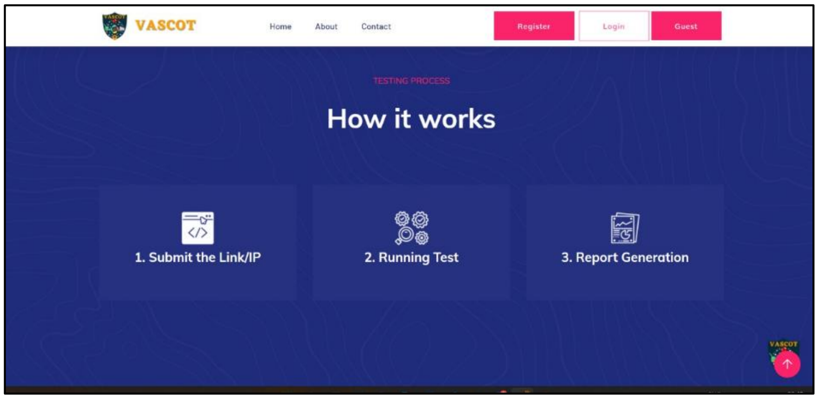
Vulnerability Tester
Fig 5.2.2



Generated Report

Url:

Report Generator
Fig 5.2.3



TESTING PROCESS

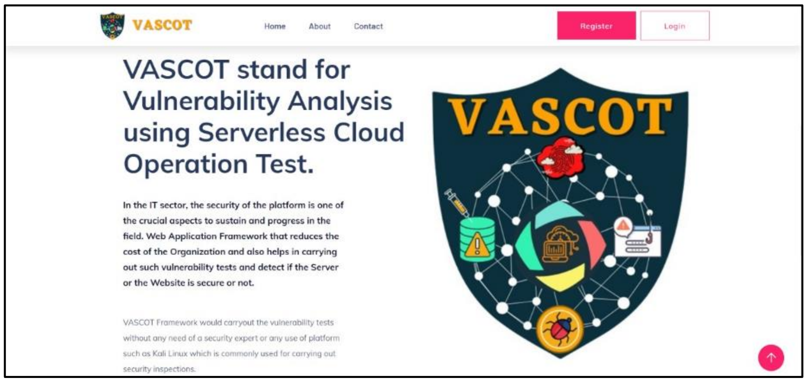
How it works

1. Submit the Link/IP

2. Running Test

3. Report Generation

Working Methodology
Fig 5.2.4

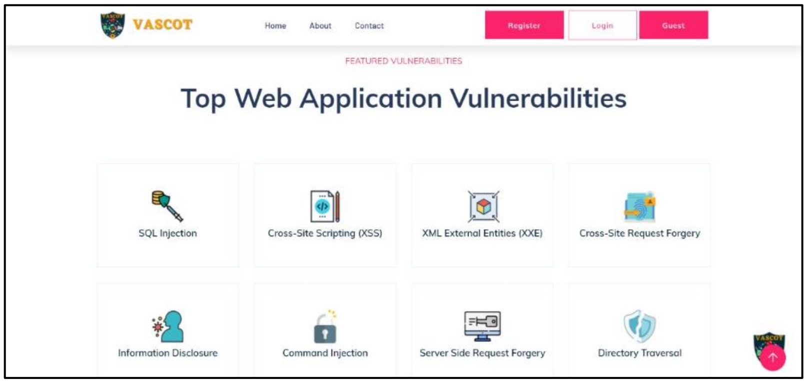


VASCOT stand for Vulnerability Analysis using Serverless Cloud Operation Test.

In the IT sector, the security of the platform is one of the crucial aspects to sustain and progress in the field. Web Application Framework that reduces the cost of the Organization and also helps in carrying out such vulnerability tests and detect if the Server or the Website is secure or not.

VASCOT Framework would carryout the vulnerability tests without any need of a security expert or any use of platform such as Kali Linux which is commonly used for carrying out security inspections.

About us
Fig 5.2.5



FEATURED VULNERABILITIES

Top Web Application Vulnerabilities

SQL Injection

Cross-Site Scripting (XSS)

XML External Entities (XXE)

Cross-Site Request Forgery

Information Disclosure

Command Injection

Server Side Request Forgery

Directory Traversal

Vulnerability Documentation
Fig 5.2.6

Chapter 6
Result & Analysis

Serverless Framework provides a new way to define basic integration tests for functions with HTTP endpoints. Its goal is to enable users to test your serverless applications without having to manually perform a lot of steps to do so. Tests are defined in a new file, serverless. Our project is made user friendly for maximum accessibility for even a user without knowledge of the cyber security domain. Our project will iterate through all the steps of the vulnerability assessment. This project focuses more on the IT start-ups which are unable to keep a cybersecurity division.

Chapter 7
Conclusion, Future Scope, References & Acknowledgement

7.1 Conclusion

So, we tried to build an efficient webpage framework which will do vulnerability detection. In which, we have provided user friendly GUI. We have also included the chatbot to guide user how to proceed for vulnerability check and given basic information about what vulnerabilities. Also, we are doing this as serverless using cloud support. Since it is serverless it will not need Linux system or any security engineer to check security aspects for the website.

7.2 Future Scope

In the future by adding more vulnerabilities test to make our website more efficient and give more accuracy about results. Also, different features and documentation can be added to make website more user friendly. Also, in future we will be enhancing user profile part for those users who have accounts on VASCOT.

7.3 References

1. Nick Galov (2021, Jan 16) "39 Jaw-Dropping DDoS Statistics to Keep in Mind for 2021" retrieved from https://hostingtribunal.com/blog/ddos-statistics/#gref
2. M. T. Islam, M. Ahmad, and A. S. Bappy, "Real-Time Family Member Recognition Using Raspberry Pi for Visually Impaired People," 2020 IEEE Region 10 Symposium (TENSYMP), 2020.
3. Charlie Osborne (2020, Feb 18) "16 DDoS attacks take place every 60 seconds, rates reach 622 Gbps" retrieved from https://www.zdnet.com/article/16-ddos-attacks-take-place-every-60-seconds-rates-reach-622-gbps/
4. Agache, A., Brooker, M., Iordache, A., Liguori, A., Neugebauer, R., Piwonka, P., Popa, D.M.: Firecracker: lightweight virtualization for serverless applications. In: 17th USENIX Symposium on Networked Systems Design and Implementation (NSDI 20), pp. 419–434. USENIX Association, Santa Clara, CA. https://www.usenix.org/conference/nsdi20/presentation/agache (2020)
5. M. Mehra, V. Sahai, P. Chowdhury, and E. Dsouza, "Home Security System using IOT and AWS Cloud Services," 2019 International Conference on Advances in Computing, Communication and Control (ICAC3), 2019.
6. de Alfonso, C., Caballer, M., Calatrava, A., Molto, G., ´ Blanquer, I.: Multi-elastic Datacenters: auto-scaled virtual clusters on energy-aware physical infrastructures. Journal of Grid Computing 17(1), 191–204 (2019). https://doi.org/10.1007/s10723-018-9449-z
7. M. D. Dzulfiqar, D. Khairani and L. K. Wardhani, The Development of University Website using User Centered Design Method with ISO 9126 Standard, 2019.
8. M. A. Helmiawan, Y. H. Akbar and Y. Y. Sofian, "Evaluasi dan Uji Kualitas Website dengan Metode Webqual (Studi Kasus: STMIK Sumedang)", *Jt. (Journal Inf. Techno!.*, vol. 1, no. 1, pp. 1-4, 2019.
9. M. M. Hassan, S. S. Nipa, M. Akter, R. Haque, F. N. Deepa, M. Rahman, M. A. Siddiqui, M. H. Sharif et al., "Broken authentication and session management vulnerability: A case study of web application", *International Journal of Simulation Systems Science & Technology*, vol. 19, no. 2, pp. 6-1, 2018.
10. F. Ajismanto, "Analisis Domain Proses COBIT Framework 5 Pada SistemInfor masi Worksheet (StudiKasus: Perguruan Tinggi STMIK, PoliteknikPalcomtech)," CogITo Smart Journal, vol. 3, no. 2,p. 2017, 2018.
11. L. N. Amali, M. R. Katili, S. Suhada dan L. Hadjaratie, "EVALUASI Tingkat Kapabilitas Proses Tata KelolaTiBerdasarkanKerangkaKerjaCobit 5 Dalam Domain Evaluate, Direct And Monitor (EDM),"Seminar Nasional SistemInformasi, vol. 3, pp. 1089-1096, 2018.
12. V. M. Nadar, M. Chatterjee and L. Jacob, "A defensive approach for csrf and broken authentication and session management attack", *Ambient Communications and Computer Systems*, pp. 577-588, 2018.
13. *Establishing an LDAP Session*, 2018, [online] Available: https://msdn.microsoft.com/en-us/library/aa366102(v=vs.85).aspx.
14. R. Weiss, F. Turbak, J. Mache and M. E. Locasto, "Cybersecurity education and assessment in EDURange", *IEEE Annals of the History of Computing*, vol. 15, no. 03, pp. 90-95, 2017.

15. G Deepa, P S Thilagam, A Khan F et al., "Black-box detection of XQuery injection and parameter tampering vulnerabilities in web applications", *International Journal of Information Security*, pp. 1-16, 2017.
16. L. McDaniel, E. Talvi and B. Hay, "Capture the Flag as Cyber Security Introduction", *2016 49th Hawaii International Conference on System Sciences (HICSS)*, pp. 5479-5486, 2016.
17. A Z M Saleh, N A Rozali, G Buja A et al., "A Method for Web Application Vulnerabilities Detection by Using Boyer-Moore String Matching Algorithm", *Procedia Computer Science*, vol. 72, pp. 112-121, 2015.
18. *SQL injection*, 2018, [online] Available: https://portswigger.net/kb/issues/00100200_sql-injection.
19. "Web Security Statistics Reprot 2015", *Whitehat Security Site*, [online] Available: https://info.whitehatsec.com/rs/whitehatsecurity/images/2015-Stats-Report.pdf.
20. Lwin Khin Shar, L.C. Briand, Hee Beng and Kuan Tan, "Web Application Vulnerability Prediction Using Hybrid Program Analysis and Machine Learning", *Dependable and Secure Computing IEEE Transactions*, vol. 12, no. 6, pp. 688-707, 2015.

7.4 Acknowledgement

We would like to express our special thanks and gratitude to all those who provided us the possibility to complete this report. A special gratitude we give to our third-year project guide Mr. Umesh Patil, whose contribution in stimulating suggestions and encouragement, helped us to coordinate our project especially in writing this report.

We also have to appreciate the guidance given by another supervisor as well as the panels especially in our project presentation that has improved our presentation skills thanks to their comment and advice.

Date

10/11/2021

Name of student	Class	Roll No.	Signature
Aayush Joshi	TE4	50	Ajoshi
Rutuja Kumbhar	TE4	53	RKumbhar
Akshat Mehta	TE4	57	AKSHAT
Harshith Shetty	TE4	67	H Shetty