An application to manage and monitor multiple agile software development tools in a secure manner

Dr.K.E.Kannammal[1], G.V.Abhinavkishore[2],

[1]Dr.K.E.Kannammal, Head of the Department, Department of CSE Sri Shakthi Institute of Engineering and Technology Coimbatore, India
[2]G.V.Abhinavkishore, Department of CSE Sri Shakthi Institute of Engineering and Technology, Coimbatore,

---

Abstract - This application contains simple forms and buttons that will run automated scripts in the backend when it is clicked. Multiple "Agile software development" tools are integrated within this dashboard to make things much easier for the DevSecOps team. Using the latest technology makes this application faster and secure. This way the access to sensitive information and the access to various outsourced services can be maintained on record. The most commonly used industrial tools and services are integrated into this dashboard to make this a generic product. We have user authentication included for security and keeping the trail of all user activities.

Key Words: DevOps, DevSecOps, AWS, SCA, SAST, MobSF, AWS, Boto3, python, automation, python3.

1. Introduction

All over the internet, there are many companies moving towards Cloud computing. All the big companies have moved to cloud-based architectures. The cloud service providers like Amazon, Google, Microsoft and etc are providing the cloud as well as a browser application to manage all the cloud services. There are many other providers who provide SaaS of some agile-based applications to make our job easier.

The services like Github, Bitbucket, Jira, Circleci, Jenkins, and many more are used by most of the companies on the internet. These services have their own management applications and those make the job very easy for a lot of developers.

For example, AWS is one of the leading cloud providers in the market and they provide a web-based console to manage their services. Their console is the heart of their cloud services and applications. All the functionalities can be performed over there and everything has become just a click away. The same way Microsoft Azure and Google GCP also have those features similar to AWS Console.

And when we see other Saas providers, they also have their own management console and all the stuff has become just a click away, but when we see all the companies who are using cloud providers and Saas, They all use the combination of different services from different providers. Each company has its own style and its own needs of services. They all use services based on their comfort and budget. Some companies may use only open source services, some may spend money so that they get more reliable support and services, etc.

This is a project for such companies who use different services in their daily deployments and daily tasks. Different services integrated within one application to make our jobs much easier and much more efficient. The dashboard integrates multiple services based on the user's needs and can be modified to work for their own purpose. Everywhere on the Internet there are numerous organizations moving towards Cloud figuring. All the enormous organizations have moved to cloud-based designs. The cloud specialist co-ops like Amazon, Google, Microsoft, and so forth are giving the cloud just as a program application to deal with all the cloud administrations. There are numerous different suppliers who give SaaS of some deft-based applications to make our work simpler.

The administrations like Github, Bitbucket, Jira, Circleci, Jenkins, and a lot more are utilized by the majority of the organizations on the web. These administrations have their own administration applications and those make the work simple for a lot of engineers.

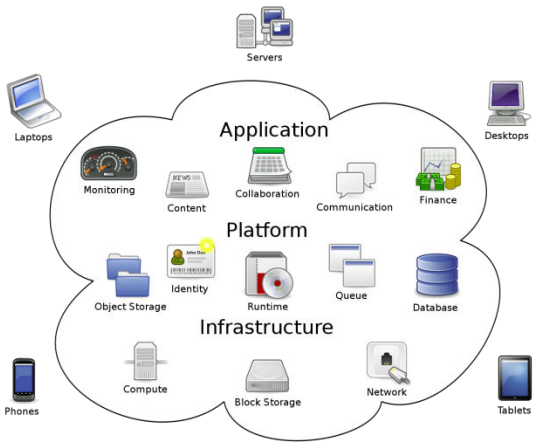
For instance, AWS is one of the main cloud suppliers on the lookout and they give electronic reassurance to deal with their administrations. Their reassurance is the core of their cloud administrations and applications. All the functionalities can be performed over yonder and everything has become recently a tick away. The same way Microsoft Azure and Google GCP likewise have those highlights like AWS Console.

2. Literature Survey

2.1 Cloud Computing

Distributed computing has experienced a fast improvement during the latest years, and it is needed to keep on developing

to an always expanding degree. Cloud organizations will be useful in business applications, which will change organizations in cloud-based organizations. This change is required especially for applications like ERP (try resource masterminding) or CRM (client relationship the executives). Banks are a huge part of the business zone that circulated figuring is centering in the accompanying relatively few years. As a result of this sort of business needs, cloud organizations ought to be tantamount with a "silver shot". There are various advantages that cloud obliges banks as customers. As an issue of first significance, cost venture reserves, using cloud-laborers instead of individual specialists, will put to the side a huge load of money. In addition, cloud gives: utilize based charging, business congruity, business deftness, green IT. Thus, nowadays conveyed figuring organizations have a couple of obstacles that stops banks from accepting the cloud, similar to security, characterization of the data, and moreover nature of organizations.

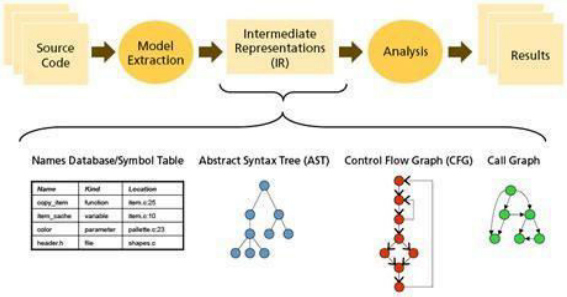


Security is probably the greatest contention utilized against the real distributed computing framework. In any case, distributed computing frameworks are regularly more secure than centralized server frameworks oversaw at the nearby level, in any event for little and medium organizations (banks). This may list the qualities of distributed computing frameworks: private cloud, information centralization, multifaceted confirmation, sharing security, economy of scale and others. Private cloud is presumably the main contention for utilizing distributed computing frameworks by associations (banks). An intriguing correlation is between the current circumstance of web banking and distributed computing. Security issues were likewise an inhibitor to reception of web banking (about mid 90's), which can be viewed as a forerunner of distributed computing. Also, as distributed computing suppliers who keep on tending to advertise concerns identifying security, economy and comfort of distributed computing will turn into a typical like web based banking and other online monetary exchanges today.

The objective to accept appropriated registering has extended rapidly in various affiliations. Conveyed processing offers various probable benefits to nearly nothing and medium endeavors like brisk association, pay-for-use, lower costs, versatility, quick provisioning, quick adaptability, ubiquitous association access, more conspicuous strength, and on-demand security controls. Despite these exceptional benefits of appropriated registration, considerations show that affiliations are postponed in accepting it on account of safety issues and challenges related with it. With everything taken into account, security is one of the huge issues which reduce the disseminated registering determination. Organizations use the Cloud in a wide scope of organization models (SaaS, PaaS, IaaS) and plan models (Private, public, crossbreed, and neighborhood). There are different security issues or concerns related with conveyed registering, yet these issues fall into two general arrangements: security issues looked by cloud providers and security issues looked by their customers (associations or affiliations who have applications or store data on the cloud. For settling these issues, the commitment goes the two distinct ways, in any case: the provider should ensure that their structure is secure and that their clients' data and applications are guaranteed while the customer should take measures to support their application and use strong passwords and affirmation measures. According to Takabi et al. (2010), cloud expert communities and customers are liable for security and assurance in disseminated processing conditions anyway their level of commitment will change for different transport models. System as a Service (IaaS) fills in as the foundation layer for the other transport models, and a shortfall of safety in this layer impacts the other movement models. In IaaS, notwithstanding the way that customers are responsible for guaranteeing working structures, applications, and substance, the security of customer data is a basic obligation with respect to cloud providers. In Platform as an assistance (PaaS), customers are responsible for getting the applications that designers create and run on the stages, while providers are at risk for managing the customers' applications and workspaces from one another.

2.2 Static Code Analysis

One of the strategies for source code confirmation is static code examination. SCA is the way toward assessing a framework or part dependent on its structure, design, substance, or documentation. From a product confirmation viewpoint, static examination tends to shortcomings in program code that may prompt weaknesses. SCA is performed without really executing programs and can be applied on the beginning phases of the programming lifecycle. Such investigation might be manual, as in code examinations or mechanized through the utilization of at least one device. Robotized static code analyzers regularly check source code yet there is a more modest arrangement of source code analyzers that check byte code and double code. They are particularly helpful when source code is not accessible. Static code analyzers are utilized to reveal hard to track down execution mistakes before run-time, since they might be much more troublesome or difficult to track down and evaluate during execution. These devices can find numerous legitimate, wellbeing and security blunders in an application without the need to execute the application.



Today there are various examinations on improving the proficiency of SCA. There are various guidelines to guarantee the nature of the static examination of the application in the improvement of military programming. Michael Howard proposes a rundown of proposals for improving SCA effectiveness

Different apparatuses ought to be utilized to counterbalance instrument predispositions and limit bogus positives and bogus negatives and limit bogus positives and bogus negatives. Investigators should focus on each notice and mistake. (for Code ought to be assessed early, best with each form, and rethought at each achievement.

Likewise, examiners should ensure that code audits cover the most well-known weaknesses and shortcomings, like whole number-crunching issues, support invaders, SQL injection, and cross-site scripting (XSS). Hotspots for such normal weaknesses and shortcomings incorporate the Common Vulnerabilities and Exposures (CVE) and Common Weaknesses Enumeration (CWE) databases, kept up by the Miter Corporation. Miter, in collaboration with the SANS Institute, additionally keeps a rundown of the "Top25 Most Dangerous Programming Errors" that can prompt genuine weaknesses. Static code examination apparatus and manual methods ought to at least address this Top 25. The better static code investigation apparatuses are costly. Alternate approaches to improving the proficiency of SCA is to utilize different apparatuses to counterbalance device predispositions and limit bogus positives and bogus negatives. Notwithstanding, this is cost restrictive.

The functional execution of the suggested steps has various issues. Diverse SCA instruments has various deformities order frameworks. It is difficult to look at results acquired from various apparatuses. Additionally, the bases of certain analyzers don't cover the most widely recognized weaknesses and shortcomings. All of which make it difficult to completely utilize all advantages of the static investigation innovation.

2.3 Vulnerability Scanners

A vulnerability scanner is an apparatus worked to improve on the pen analyzer task. They can perform programmed assaults to web applications with little or none human intercession . A decent web scanner gives comparable conduct to an internet browser. The functionalities that make a total web scanner as per WASC characterized in the WASSEC are:

1. Protocol Support - Like an internet browser, a web scanner should have the option to convey however HTTP and support its protocols, basic HTTP or HTTP over SSL/TLS. There are numerous programs and forms, a web application supplier can't ensure that the customer utilizes the most refreshed and secure programs, besides, a web scanner performs better on the off chance that it reenacts various programs and forms.

2. Authentication - Is the manner in which the client affirms he is who he says and it approaches the solicitation he makes through the program. Most web applications, exceptionally applications with various degrees of freedom, have diverse authentication strategies who will make the web scanner futile in the event that it can't support, for instance, HTTP Negotiate or Federated authentication techniques.

3. Session Management - During the sweep, a "living" session should be kept up with the application untouched. Without it, the scanner can't play out the crawling or assaults to levels where "in-session" is required.

4. Crawling - Oneof the fundamental elements of a web scanner is crawling, the capacity to find which pages exist in the web application with the goal that a full test can be made. Web scanners permit quick testing and fluffing, numerous assault modes and facilitate the pen analyzer task. In a dark or dim box pen testing where the pen analyzer has no admittance to the application source code or when he doesn't know about the programming language web scanners are thoughts. Notwithstanding that, the measure of

solicitations a web scanner can perform naturally is generously greater than manual testing. The test time decrease and inclusion are two of the main benefits a web scanner can give.

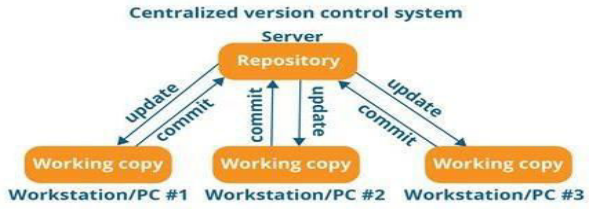
5. Parsing - Parsing is the capacity to peruse, decipher and fathom the substance present in web applications. Substances like Javascript, HTML and Flash. Web applications can have various innovations with numerous executions. Parsing is one method of distinguishing weaknesses that may exist in the code.

6. Testing - These are the assault parts of a web scanner. The more noteworthy weaknesses type inclusion, the better. This is the module liable for assaulting setup and vulnerability misuse. The more assaults and systems a web scanner knows, the better outcomes can be gotten however a low bogus positives rate is additionally a decent three pointer in a web scanner. On the off chance that the web scanner orders numerous discoveries as weaknesses yet indeed are bogus positives, it will require the pen analyzer to put a lot of time in approving the discoveries.

7. Command and control - A web scanner is additionally a mind boggling instrument with numerous highlights, a decent UI and critical convenience is needed for smooth testing. Functionalities like "delay and resume" filters, support various clients and continuous investigation. The use of the web scanner ought to be straightforward so all genuine work is in the pen test and not in the learning of use of the tools.8. Detailing - A web scanner ought to permit to make reports to see results outside the apparatus scope in configurations, for example, ".doc", ".xml" or ".pdf". The sweep pivotal data ought to be assembled and arranged in a standard report design. In the event that the scanner likewise gives data about the vulnerability or connections to references, it improves on the correspondence with its areas of expertise for critical weaknesses.

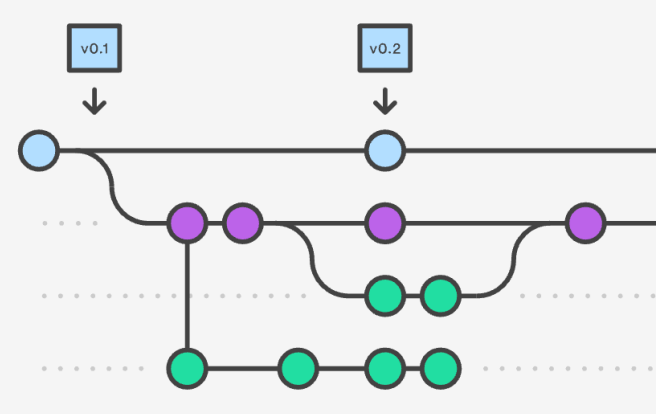
2.4 Introduction to Version Control and Git

Numerous scientists write code as a component of their research. Similarly as experiments are logged in lab notebooks, it is critical to document the code you use for analysis. However, a few key problems can arise when iteratively developing code that make it hard to document and track which code version was used to create each result. In the first place, you often need to experiment with new ideas, like adding new features to a content or increasing the speed of a sluggish step, yet you would prefer not to chance breaking the currently working code. One often-utilized arrangement is to make a duplicate of the content before making new edits. However, this can immediately become a problem because it clutters your file system with uninformative filenames, e.g., analysis.sh, analysis_02.sh, analysis_03.sh, etc. It is hard to remember the differences between the versions of the files and, more significantly, which version you used to produce specific results, especially in the event that you return to the code months later. Second, you will likely share your code with multiple lab mates or colleagues, and they may have suggestions on the best way to improve it. In the event that you email the code to multiple people, you should physically incorporate every one of the changes each of them sends.



Luckily, programmers have effectively evolved programming to deal with these issues: form control. A rendition control framework (VCS) licenses you to follow the iterative changes you make to your code. Therefore, you can explore different avenues regarding novel thoughts yet reliably have the decision to return to a particular past form of the code you used to create explicit outcomes. Moreover, you can record messages as you save each progressive adaptation with the objective that you (or any other person) auditing the advancement history of the code can comprehend the reasoning for the given alters. It furthermore encourages joint exertion. Utilizing a VCS, your accomplices can make and save changes to the code,

and you can normally join these progressions to the essential code base. The cooperative angle is upgraded with the rise of sites that have form controlled code.



In this smart guide, we acquaint you with one VCS, Git (https://git-scm.com), and one web based facilitating website, GitHub (https://github.com), the two of which are right now notable among researchers and developers all in all. All the more fundamentally, we desire to persuade you that in spite of the fact that dominating a given VCS requires some serious energy, you would as of now have the option to accomplish extraordinary advantages by beginning utilizing a couple of straightforward orders. Moreover, not only does utilizing a

VCS take care of various normal issues when composing code, it can similarly improve the logical cycle. By following your code advancement with a VCS and facilitating it on the web, you are performing science that is more straightforward, reproducible, and open to joint exertion. There is no explanation this structure should be restricted particularly to code; a VCS is appropriate for following any plain-text documents: creations, electronic lab journals, shows, and so forth.

3. Proposed Work

An interactive web application to get inputs and display outputs.Add authorization and authentication to the application to use it securely.Store all the records into a database for future reference.Maintain logs.Manage users and their details with User management and avoid getting similar information repeatedly. Create Scripts to run background tasks and make application faster.Host it on a cloud compute service with a high performance machine to make the application handle a huge load of data.Testing the application with Load testing.Testing the application with invalid inputs and using secure coding styles.Testing the application based on workflow.

4. Methodology

Dashboard consists of 5 main functionalities and other additional features will be added in the next releases. In this dashboard we are using the python Django framework for the frontend and backend of the application. Django by default has few security features implemented so that we don't have to do those separately. All the inputs are being sanitized so that some simple web application attacks will not affect the system.

In DevSecOps the important thing is to automate anything and everything. All kinds of tools are present to automate the devops tasks. For example we can use python to automate most of the tasks that we do on a daily basis. So based on our specific daily needs i have written python automation scripts combined with some shell scripting. Using python and Django make the application not only secure but also make the application portable and easy to deploy anywhere. All the services used in our daily agile process have python support so automating all the actions that are repeated will give us more time to work on new things everyday. the work / learning graph will be increasing everyday when there are many more automations happening.

The most repeated process that most of the organization follows are static code analysis for web and mobile applications, a generic vulnerability scanner. So we have integrated those to this dashboard to make things easy.

Another important feature is all the requests made here will be generated as emails and will be sent to the respective person or team. So that all the actions are recorded in the database for the future references. There is an email script which will collect all the data of the request made and will parse it into an email that will be sent to the devsecops team with the requester in cc. This feature is for recording all the requests in the gmail.

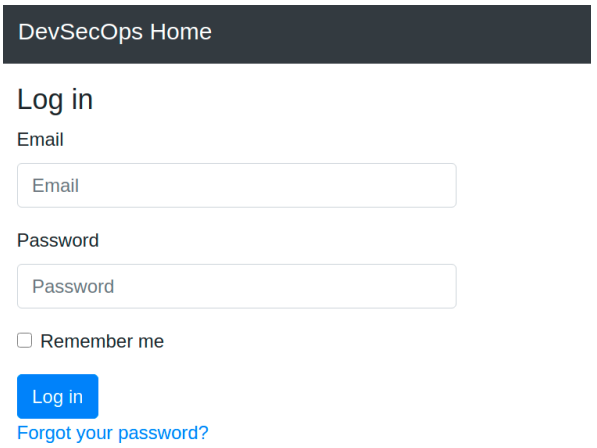
There are pages just to get output and email it to the devops team because those are critical tasks which need human attention and need approval from some higher official.

This application is going to be deployed inside AWS ec2 using ecs and load balancer. This deployment will be easy as mentioned before we are using docker service to make this into the micro service and make it easy for anyone to deploy it anywhere.

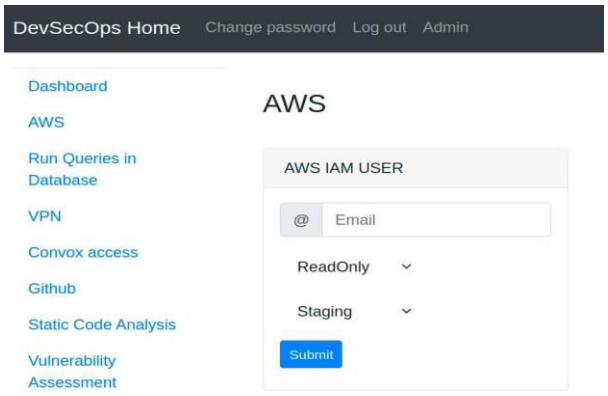
5. Web Application Hosting

The Application can be hosted on any machine with docker running in it. Docker is a Software which can be used for easy transportation and easy deployment of the software or tools without changing any configurations in the machine. This docker can be run in any operating system. We are hosting the application in a linux based machine with docker installed. That will make the application easy deployable and easy set up with mins.

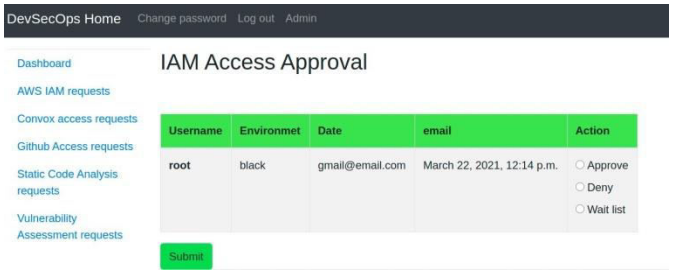
The authentication in this application will protect the secure pages / paths from the normal user . The login page will not have any create account so no one can create an account and use it without the devops permission. DevOps personnel should create accounts for the users that can be done from the admin side of the application which is only accessible to the admin user.



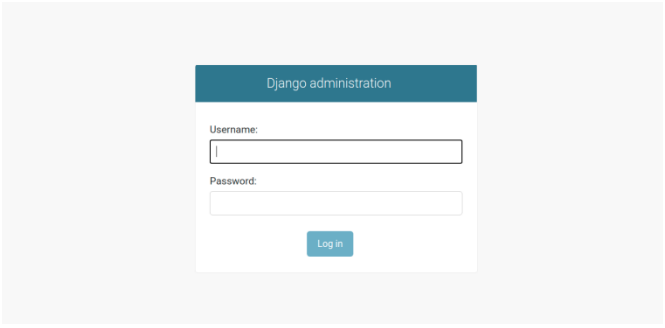
The services on the user page will create a request and that request will be sent to devops team email and will also saved in the database.



The Admin will have the request approval pages and tables in a different path. That path can be reached by pressing the admin button in the menu bar. when choosing, approving and submitting, that will run some scripts in the background that will do the work.



The super admin configuration and creating users are done in the /admin path where django has its own admin panel which we are using.



As said before all the services are made into simple microservices and hosted inside the docker containers. This will help us easily set up for the future. and the generic version can be easily set up by others easily using docker

6. Conclusion

The DevSecOps Dashboard application will help devops personnel to increase productivity as all the most needed are being integrated inside one application and all are present in one dashboard that is user friendly. Due to this we can say that their concentration on more advanced things can be increased and the low priority stuff that they repeatedly do will be automated with this application.

All the services integrated here are simple actions as this is the first version. In future versions this can be changed into a tool with all kinds of devsecops tools integrated into it.

7. Future Works

In future the dashboard can be modified to more open source and generic tools and integrated into the current application for more productivity and automation. This dashboard will be a perfect automation and security based application for DevSecOps teams all over the IT Industry.

All the new things introduced in SDLC is now in a process in DevOps. and DevSecOps will have the process of DevOps with the security checks in the right places to make it a routine for the developers to check for the security test as well as unite tests before a deployment is made. This will give us the most stable releases. and sure.

8. References

[1] *Alanda, A., Satria, D., Mooduto, H. and Kurniawan, B., 2020. Mobile Application Security Penetration Testing Based on OWASP. IOP Conference Series: Materials Science and Engineering, 846, p.012036.*

[2] *Ballmann, B (2012), "Inside Django Security. InformatikSpektrum", 35(3), pp.182-189.*

[3] *Blischak JD, Davenport ER, Wilson G (2016) A Quick Introduction to Version Control with Git and GitHub. PLoS Comput Biol 12(1): e1004668. https://doi.org/10.1371/journal.pcbi.1004668.*

[4] *Galliard, J., 1971. Two Examples for Operators' Console Communications: DDC Console; Console for Gas Chromatographs. IFAC Proceedings Volumes, 4(3), pp.211- 215.*

[5] *Ghilic-micu, B., Stoica, M. And Uscatu, C, 2014. Cloud Computing and Agile Organization Development. Informatica Economica, 18(4/2014), pp.5-13.*

[6] *Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz,Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, and Matei Zaharia (February 10, 2009): Above the Clouds: A Berkeley View of Cloud Computing.*

[7] *Lüdtke, R., 2019. Static Code Analysis for Automotive*

Real Time Applications. ATZ Electronics worldwide, 14(10), pp.40- 43.

[8] Kaur, A. and Nayyar, R., 2020. A Comparative Study of Static Code Analysis tools for Vulnerability Detection in C/C++ and JAVA Source Code. Procedia Computer Science, 171, pp.2023- 2029.

[9] Pomorova O.V. and Iwanchyshyn D.O. Making Static Code Analysis More Efficient Received 19 March 2014; Accepted 27 April 2014; Publication 2 June 2014 Journal of Cyber Security, Vol. 3 No. 1, 77–88.

[10] SQMB 2009 Workshop, SE 2009 conference, Kaiserslautern, Germany, July 2009."

[11] "A Django Based Educational Resource Sharing Website: Shreic Adamya Shyam*1, Nitin Mukesh*2 "