Biomedical Research 2017; Special Issue: S129-S136

ISSN 0970-938X
www.biomedres.info

Analysis and selection of risk assessment frameworks for cloud based enterprise applications.

K Vijayakumar[1*], C Arun[2]

[1]Faculty of Computer Science and Engineering, St.Joseph's Institute of Technology, Sathyabama University, OMR, Chennai, India

[2]Department of Electronics and Communication Engineering, R.M.K College of Engineering and Technology, Chennai, Tamil Nadu, India

Abstract

A lot of enterprise applications are available for the end users to use in different domains including business, healthcare, industrial and manufacturing. In the advent of cloud computing, it is imperative for organizations to determine risks involved in adopting cloud-based solutions or applications to ensure enterprise interest. The problem is the risk assessment of enterprise applications from the context of business. It is essential to adapt the right risk assessment strategy to handle the security situation proactively. We analyze the different risk assessment frameworks which would help to evaluate frameworks against enterprise application such as business, medical, finance accounting applications. We have evaluated both CWRAF and CVSS as two predominant frameworks in the risk assessment process against three business applications. The results help identifies the appropriate approach and framework which should be used for risk assessment.

Keywords: Risk assessment, Security issues, Cloud security, Business context.

Accepted on January 16, 2017

Introduction

Risks always need to be looked at from a negative perspective risk assessment and identification is a sweet spot to identify the opportunity to enhance security and mitigate the security loopholes in the system. According to ISO 31000 risks are defined as the "effect of uncertainty on the objectives [1]. As Cloud adoption is increasing day by day as it holds the benefit of scalability, performance, and agility, this also means that there is critical need for cloud users to make sure that they are doing the right thing when they adopt it. It is imperative for the business users to ensure to weigh-up the risk landscape in such adoption or minimize the risks in taking up such initiatives [2].

As per large cloud adoption survey for Q4 2014 conducted by NorthBridge based GigaOMResearch with 1358 respondents, 49% have already adopted the cloud for revenue generation and product development activities and 45% want to adopt cloud in the organization. This shows the level of significance of increasing demand for cloud adoption among the business community. The adoption of SaaS applications has increased from 13% in 2011 to 72% in 2014 [3]. The readiness of an enterprise to adopt cloud depends on the a) business benefit the enterprise is going to gain b) technical feasibility of moving the legacy or existing an app to the cloud and finally c) risks involved in moving towards the cloud based apps.

Though cloud adoption helps to ramp up the service levels and performance rapidly, it might oversee the risks. As platforms such as Azure and Amazon have made pay-as-you-go based cloud administration in a more simplified way, ill-administration of these portals without understanding the impact might be an exposure to financial risks if it is not well handled. When organizations are multinational and spread out in different geographies, the availability of services via different data center in a distributed environment has to be brought into context.

Cloud Apps Security does not end with the developers taking care of all the threats during the development stage various factors such as deployment platform, access privileges, vulnerabilities in the physical environment of deployment, etc., so it is very important to address the security risk from the perspective of the business user based on his security needs. The business user needs to be cognizant of the impact of a probable security breach so that such risks can be mitigated.

In a well-connected world, the risk and exposure are multiplying as new technology tools, frameworks and concepts are being introduced every day. This paper attempts to identify the Risk frameworks for evaluating Cloud SaaS Apps in the context of the business user and help them in choosing the right risk frameworks.

Related Works

In the research paper by Johnson and Qu, they provided "A Holistic Model for Making Cloud Migration Decision" which deals with the factors on Security, Architecture and Business Economics delve into the business decision of adopting to the cloud. These models recommended some standard criteria which can be utilized for assessing the cloud service providers and quantify them. This could be a very viable model to evaluate among multiple Cloud service providers to before taking a final decision. In this risk is considered as one of the factors for the evaluation of SaaS vendors [4].

In the research done on Collaboration-Based Cloud Computing Security Management Framework by Almorsy et al. [5] they have tried to align the existing NIST-FISMA (National Institute of Standards and Technology-Federal Information Security Management Act) [6] to suit the cloud standards or platforms that primarily address the concern of the cloud providers rather than the consumers.

QUIRC, A Quantitative Impact and Risk Assessment Framework for Cloud Security revolve around 6 objectives such as Confidentiality, Integrity, Availability, Multi-Trust breach, Auditability, and Usability. This paper provides a quantitative assessment methodology of Risk based on threat modeling using Wideband Delphi methodology. Though this paper can quantify the risk for vendors and customers it also highlights that risk assessment expertise could be based on industry vertical and knowledge base [7].

Microsoft Australia has released a white paper which discusses the risk assessment framework based on ISO 31000:2009 [1]. It outlines various risk factors which need to be evaluated. This paper also categorizes the risk in terms of Compliance related risks, Strategic Risks, Operational Risks and Market & Financial risk categories during the risk identification process [2].

In the research paper titled cloud computing: A new business paradigm for biomedical information sharing a lot of different options of cloud application architecture which includes risk reduction, flexibility, and scalability. It also ascertains that right to set security and enforce its own information security policies of the application based on risks it does foresee [8].

Chou and Oetting [9] presented a research paper which would outline the risk assessment approach on cloud-based IT Systems which also attempted to showcase a risk assessment based upon the ISO/IEC 27002 and OWASP Top 10 Risks.

Security issues in the cloud environment which are posing to be a threat might have an impact on the service delivery models of the cloud offerings. These issues are evaluated in "A survey on security issues in service delivery models of cloud computing'. It also outlines the need for "Security as a Service" to encounter the security challenges [10].

In the paper "Addressing cloud Security Issues" Dimitros Zissis and Dimitros Lekkas identified User specific security requirements and identified different cloud deployment mechanisms to alleviate threats and vulnerabilities the cloud environment poses. These generic principles proposed would address aspects such as Confidentiality, Integrity, and Authenticity [11].

Need for risk assessment frameworks

Though different risk analysis methodology exists there is no specific framework exists which can be comprehensively applied or adopted. The research by Drissi et al. [12] concludes that there is lack of structured method which can be used for risk assessment for the cloud consumers to put forth their resources in order maximize cloud adoption and take advantage of the current trends in cutting edge technologies via cloud.

In the research by Saxena [13], on the utilization of Cloud Control Matrix by Cloud Security Alliance is extensively discussed in the context of risk assessment of a cloud provider. It concludes with the need for a robust framework which can take care of elementary issues in the cloud environment pertaining to security.

Risk assessment scope

There is a set of known fears for cloud computing which is essential for the business is outlined in Business News Daily [14].

- Data is handled by someone else not part of your organization
- Cyber attacks
- Insider Threats
- Government Intrusion
- Legal Liability
- Lack of Standardization
- Lack of support
- Other Risks

Existing risk assessment

The various cloud categories such as IaaS, PaaS and SaaS are to be focused on risk assessment while doing a risk assessment for cloud adoption. The factors which would affect cloud adoption are Technology, Organizational, and Environmental.

Existing cloud platforms

Most of the virtualized infrastructures are deployed on cloud platforms as IaaS (Infrastructure as a Service). They are classified into two broad categories as given below:

IaaS Platforms (Proprietary):

- Microsoft Azure
- Amazon

IaaS Platforms (Open Source):

- OpenStack
- Apache CloudStack

Virtual resources or client tools can even be deployed for handling the virtual machines to test their behavior.

Literature Review

Critical factors are to be evaluated in a typical cloud setup and analyzed the existing cloud computing risk assessment methodologies available and find the methodology which would be made easy for the end consumer to analyze and implement the framework. This paper will attempt to identify the existing risk assessment frameworks available for cloud computing and will evaluate its pros and cons by implementing some of the risk factors to cloud-based applications by simulating or deploying it in the cloud (Table 1).

Table 1. *Five important characteristics of Cloud environment are given in the work by Alliance [15].*

S.no	Characteristics	Benefits
1	On-Demand, Self-Service	Provisioning of services on Demand (Storage, Compute, etc.)
2	Resource Pooling	Sharing of resources such as Memory, Bandwidth, etc.
3	Measured Service	Metering the usage, pay-as-you-go
4	Rapid Elasticity	Scale-out, Scale-in
5	Broad Network Access	Resources and apps available over network

CWRAF

Common Weakness Risk Analysis Framework helps the organization interested in finding the weakness exists the solution they have chosen based on the CWE (Common Weakness Enumeration). A key aspect of this framework is to focus on weakness existing in the target system. CWE is used by popular security bulletins such as OWASP (Open Web Application Security Project). CWRAF uses CWSS (Common Weakness Scoring System) which is a mechanism used for scoring the severity of CWE identified in Enterprise applications. It helps the quantification of the weakness, acts as a common framework across development and business community [16].

CWRAF goes by the principle that though the software is same the application and its use would vary from user to user there by their security needs and risk assessment also will vary accordingly. CVE Initiative has correlated and documented over 47,000+ publicly known vulnerabilities in the commercial and open source software used around the globe, there have been some vulnerabilities that were very harmful to pretty much all of us, as well as many that were harmful only to specific types of businesses and business practices (Figure 1) [17].

To find the Base Finding Subscore, Attack Surface Subscore and Environmental Subscore. These are calculated as followed:

Base = [(10 * TechnicalImpact + 5*(AcquiredPrivilege + AcquiredPrivilegeLayer) + 5*FindingConfidence) * f (TechnicalImpact) * InternalControlEffectiveness] * 4.0

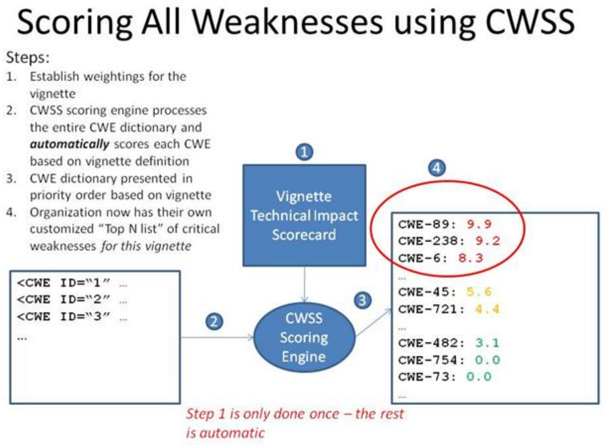
f (TechnicalImpact) = 0 if TechnicalImpact = 0; otherwise f (TechnicalImpact) = 1.

AttackSurfaceSubscore = [20*(RequiredPrivilege + RequiredPrivilegeLayer + AccessVector) + 20*DeploymentScope + 15*LevelOfInteraction + 5*AuthenticationStrength] / 100.0

EnvironmentalSubscore = [(10*BusinessImpact + 3*LikelihoodOfDiscovery + 4*LikelihoodOfExploit) + 3*Prevalence) * f(BusinessImpact) * ExternalControlEffectiveness] / 20.0

Basically the CWE scoring is done based on the following metrics [16]:

- Base Finding sub score: This capture the inherent risk of the weakness, confidence in the accuracy of the finding, and strength of controls.
- Attack Surface metric group: the barriers that an attacker must overcome in order to exploit the weakness.
- Environmental metric group: characteristics of the weakness that are specific to a particular environment or operational context.



Scoring All Weaknesses using CWSS

Steps:

1. Establish weightings for the vignette
2. CWSS scoring engine processes the entire CWE dictionary and ***automatically*** scores each CWE based on vignette definition
3. CWE dictionary presented in priority order based on vignette
4. Organization now has their own customized "Top N list" of critical weaknesses *for this vignette*

```
<CWE ID="1" ...
<CWE ID="2" ...
<CWE ID="3" ...
...
```

```
CWE-89: 9.9
CWE-238: 9.2
CWE-6: 8.3
...
CWE-45: 5.6
CWE-721: 4.4
...
CWE-482: 3.1
CWE-754: 0.0
CWE-73: 0.0
...
```

Step 1 is only done once – the rest is automatic

Figure 1. *Source CWRAF - Scoring weakness.*

CVSS

The Common Vulnerability Scoring System (CVSS) is an open framework for communicating the characteristics and severity of software vulnerabilities [18]. FIRST is a US based non-profit organization. CVSS has a risk framework version 3.0 which handles the scoring of vulnerabilities based on the Base, Temporal, and Environmental Group.

The following are the aspects upon which the CVSS risk assessment will work:

- Base score represent the most fundamental, immutable qualities of a vulnerability.

- Temporal Metrics which represent the time dependent qualities of a vulnerability.
- Environmental Metrics which represent the implementation and environment specific qualities of a vulnerability.

Base Score= round_to_1_decimal (((0.6*Impact) + (0.4*Exploitability)–1.5)*f(Impact))

Temporal Score = round_to_1_decimal (BaseScore*Exploitability*RemediationLevel*ReportConfidence)

EnvironmentalScore=round_to_1_decimal ((AdjustedTemporal +(10-AdjustedTemporal)*CollateralDamagePotential)*TargetDistribution)

Cloud risk decision framework (CRDA)

Cloud Risk Assessment Framework is based on the ISO 31000 standard. The governing principles of CRDA are based on ISO 31000 standard. The CRDA focuses on the Process component of the standard for the Cloud risk decision framework as shown in Figure 2.

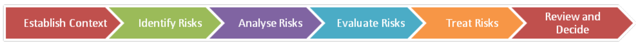


Figure 2. *Cloud risk decision framework (CRDA).*

The analysis is done based on the Risk Control Areas, Risk Likelihood, and risk impact. During the risk identification process, the risks are classified into the following risk groups such as Compliance Risks, Strategic Risks, Operational Risks, Market, and Finance Risks. Risks are measured in the range of 0-25 with the ratings such as Very High, High, Moderate, Low and Very low. Based on the risk formula of Likelihood x Impact function with a possible 1-25 rating.

COBIT 5

COBIT 5 consolidates COBIT 4.1 Control Objectives for Information and related Technology (COBIT®) is a Control framework for IT Governance [19], Val IT and Risk IT. COBIT is divided into 4 domains containing 34 high-level control objectives [20]. COBIT 5 version is said to have been built to align with ITIL Frameworks (Figure 3).

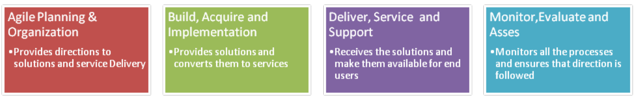

Agile Planning & Organization
•Provides directions to solutions and service Delivery
Build, Acquire and Implementation
•Provides solutions and converts them to services
Deliver, Service and Support
•Receives the solutions and make them available for end users
Monitor,Evaluate and Asses
•Monitors all the processes and ensures that direction is followed

Figure 3. *COBIT function divided into 4 domains containing 34 high-level control objectives.*

Research methodology

Our approach is based on the identification of the existing frameworks and identifying the gaps for implementation and recommends steps for bridging those gaps. The following are the steps involved in the process:

1. Identify the existing framework which would suit the cloud environment or cloud-based solutions in identifying security risks.
2. Identify tools which will help identify the security vulnerabilities or weakness existing in the 3 enterprise application under selection
3. Map the weakness and vulnerabilities against the Framework
4. Apply the risk calculation methodology using the framework
5. Compare and outline the results based on the how the risk assessment ratings are evaluated. Figure 4 outlines the high-level steps involved in the research.

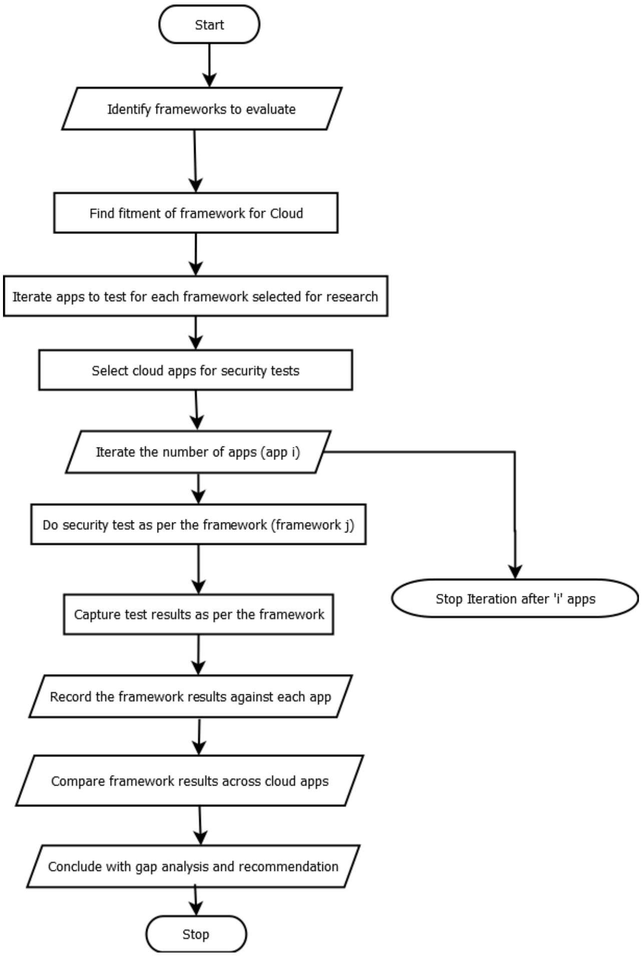

Start
Identify frameworks to evaluate
Find fitment of framework for Cloud
Iterate apps to test for each framework selected for research
Select cloud apps for security tests
Iterate the number of apps (app i)
Do security test as per the framework (framework j)
Stop Iteration after 'i' apps
Capture test results as per the framework
Record the framework results against each app
Compare framework results across cloud apps
Conclude with gap analysis and recommendation
Stop

Figure 4. *Flow chart of research methodology.*

Also, the 10 security principles defined by Information Systems Audit and Control Association (ISACA) for risk assessment frameworks offers a guideline for choosing the right risk assessment framework for the cloud app [21]. There is also a reference to the risk assessment frameworks based on the standards such as ISO/IEC 9126, COBIT 5.

Besides it is essential that the framework which is to be used must be aligned with the existing industry security aspects. It is very important for the framework to have continuous updates and stay ahead with the changing technology landscape. The standards-based framework does not directly address the threats and vulnerabilities that exist in the cloud-based applications though they provide a governance structure based on the industry standards.

In this context chosen two frameworks are chosen which are CWRAF and CVSS because these two are having standardized and codified weakness/threats which are being updated unlike standards like COBIT or ISO which depend on generic methods to identify weakness/vulnerabilities. Moreover, the frameworks such as COBIT and Cloud Risk Decision framework cannot be used independently.

Use cases

The SaaS application is considered as our scope for risk assessment because SaaS applications can cut across the Cloud platform dealing with Applications, Data, Runtime, Middleware, Operating System, Virtualization, Servers, Storage and Networking [22].

For evaluating the selected framework Content Management System (CMS), Customer Relationship Management (CRM) and Financial Management Tool are being used. The reason for choosing these is that most of the business users require these kinds of apps to effectively run their business operations. These applications are cloud-based apps which can be also self-hosted for Local behind the firewall as well. SaaS kind of applications under the scope for these use cases (Table 2).

Table 2. Apps under consideration.

S.no	Application	Rationale
1	Zurmo CRM	CRM used by business to handle customer relationship efforts
2	Wordpress	Widely used content management system deployed by corporate
3	Webzash	Finance software which is web based and needs to be more secure
4	Open LIMS	Laboratory Information Management System

Wordpress: Wordpress is a leading open source content management system used to develop websites for business purpose or managing blogs for corporate. This content Management System is based on PHP. This is one of the Open Source Content Management Systems next to Joomla, Drupal.

Zurmo CRM: Zurmo CRM is a Customer Relationship Management tool which has the capability to manage sales force with Badges and Points. This tool helps to track the Opportunities, Leads, and Contacts and help manage the sales pipeline effectively.

WebZash: WebZash is an open source PHP-based double entry accounting system. It has capabilities like Chart of Accounts, Managing the accounts, making the financial transaction, Receipts, and Payments. It has additional features like Reports, Authentication, Roles, Profit & Loss and Balance Sheet.

Open LIMS: OpenLIMS helps to conduct experiments in a Lab in a structured manner. The end user can select the appropriate template based on the complexity of the experiment and track it over the web. There can tasks which can be created and managed by the lab staff. The samples can also be collected and updated with the help of this application.

Tools used

1. OpenVAS
2. Vega
3. RIPS – Static Code Analysis tool

Implementation

As the layering of the cloud application goes through the IaaS, PaaS, and SaaS, it essential to look at ways to find the risks by doing an appropriate vulnerability analysis using the right tools. Then based on the results of these tools the quantification of risks has to be done for the appropriate prioritization of the risks and effort required to mitigate them.

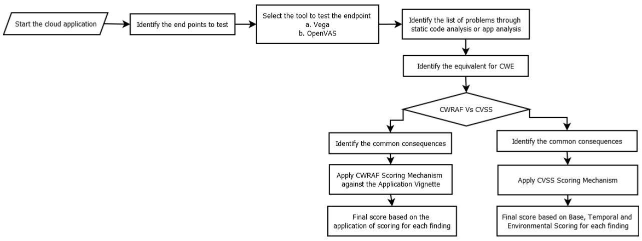
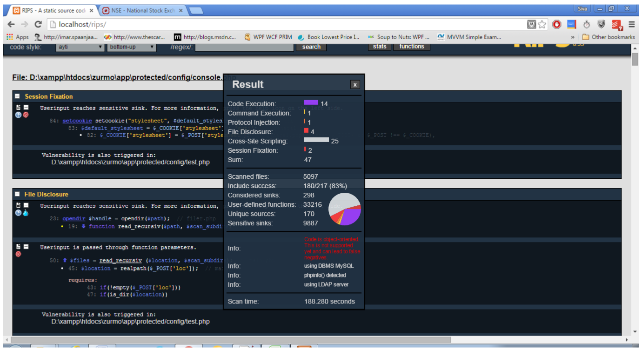

Start the cloud application
Identify the end points to test
Select the tool to test the endpoint
a. Vega
b. OpenVAS
Identify the list of problems through static code analysis or app analysis
Identify the equivalent for CWE
CWRAF Vs CVSS
Identify the common consequences
Apply CWRAF Scoring Mechanism against the Application Vignette
Final score based on the application of scoring for each finding
Identify the common consequences
Apply CVSS Scoring Mechanism
Final score based on Base, Temporal and Environmental Scoring for each finding

Figure 5. The approach opted for determining the risk score for the vulnerabilities identified with CWRAF and CVSS.

Figure 5 provides the approach opted for determining the risk score for the vulnerabilities identified with CWRAF and CVSS as per its appropriate guidelines. First, the application was deployed locally for static code analysis. The static code analysis was done using an open source tool called RIPS. RIPS is used in this case because all the 3 applications are using PHP as codebase (Figure 6).

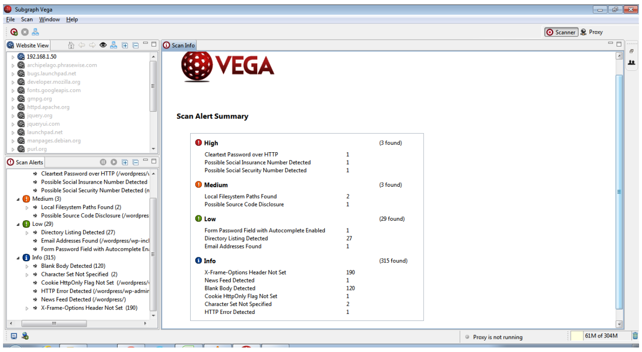


```
File: D:\xampp\htdocs\zurmo\app\protected\config\console.php

Session Fixation
    Userinput reaches sensitive sink. For more information,
      84: setcookie setcookie("stylesheet", $default_styles
        83: $default_stylesheet = $_COOKIE['stylesheet']
        • 82: $_COOKIE['stylesheet'] = $_POST['style
    Vulnerability is also triggered in:
      D:\xampp\htdocs\zurmo\app\protected\config\test.php

File Disclosure
    Userinput reaches sensitive sink. For more information,
      23: opendir $handle = opendir($path);  // filer.php
      • 19: function read_recursiv($path, $scan_subdi
    Userinput is passed through function parameters.
      50: $files = read_recursiv ($location, $scan_subdir
      • 45: $location = realpath($_POST['loc']);
        requires:
          43: if(!empty($_POST['loc']))
          47: if(is_dir($location))
    Vulnerability is also triggered in:
      D:\xampp\htdocs\zurmo\app\protected\config\test.php
```

```
Result
Code Execution:          14
Command Execution:       1
Protocol Injection:      1
File Disclosure:         4
Cross-Site Scripting:    25
Session Fixation:        2
Sum:                     47

Scanned files:           5097
Include success:         180/217 (83%)
Considered sinks:        298
User-defined functions:  33216
Unique sources:          170
Sensitive sinks:         9887

Info:                    Code is object-oriented. This is not supported yet and can lead to false negatives.
Info:                    using DBMS MySQL
Info:                    phpinfo() detected
Info:                    using LDAP server

Scan time:               188.280 seconds
```

Figure 6. Analysis of the Zurmo CRM codebase using RIPS.

The 3 apps were deployed on cloud based on a specific endpoint. Then, the endpoint is given as the input to the application OpenVAS and Vega for vulnerability or analysis. Vega is used for analysis, with the application end point as the input and configuring the same for analysis. Vega is an open source and free tool from the organization called Subgraph. It is a java based tool which can be helpful in finding XSS (cross-site scripting), SQL injection, and other vulnerabilities (Figure 7).



Cleartext Password over HTTP (/wordpress/\
Possible Social Insurance Number Detected
Possible Social Security Number Detected (n
Medium (3)
Local Filesystem Paths Found (2)
Possible Source Code Disclosure (/wordpres
Low (29)
Directory Listing Detected (27)
Email Addresses Found (/wordpress/wp-incl
Form Password Field with Autocomplete En
Info (315)
Blank Body Detected (120)
Character Set Not Specified (2)
Cookie HttpOnly Flag Not Set (/wordpress/\
HTTP Error Detected (/wordpress/wp-admir
News Feed Detected (/wordpress/)
X-Frame-Options Header Not Set (190)

Scan Alert Summary

High		(3 found)
Cleartext Password over HTTP	1	
Possible Social Insurance Number Detected	1	
Possible Social Security Number Detected	1	
Medium		(3 found)
Local Filesystem Paths Found	2	
Possible Source Code Disclosure	1	
Low		(29 found)
Form Password Field with Autocomplete Enabled	1	
Directory Listing Detected	27	
Email Addresses Found	1	
Info		(315 found)
X-Frame-Options Header Not Set	190	
News Feed Detected	1	
Blank Body Detected	120	
Cookie HttpOnly Flag Not Set	1	
Character Set Not Specified	2	
HTTP Error Detected	1	

***Figure** 7. Vega used for analysis post deployment.*

CWRAF basically approaches the assessment with 8 Technical impacts. By the way of attempting to find the risks involved, the applications under scope are prioritized them with the help of CWRAF. The scoring of the weakness identified with in the cloud applications would be determined by CWSS in conjunction with the approach defined in CWRAF. The key advantage in using the CWRAF is obtaining the list of risks with respect to the business context using the vignette. Once the CWRAF calculations are done, the Top N List specific to the business application is essential to take the necessary action.

On the other hand, CVSS calculates the Base Score, Temporal Score, and Environmental Score to give the overall understanding of the risk involved with respect to a specific vulnerability. Though the base score indicates the critical vulnerabilities the environmental score indicates the context based significance of the issue. The base score highly depends on the Impact and Exploitability factors. The formula given below is for calculating the base score:

Base Score = round_to_1_decimal(((0.6*Impact) +(0.4*Exploitability)–1.5)*f(Impact))

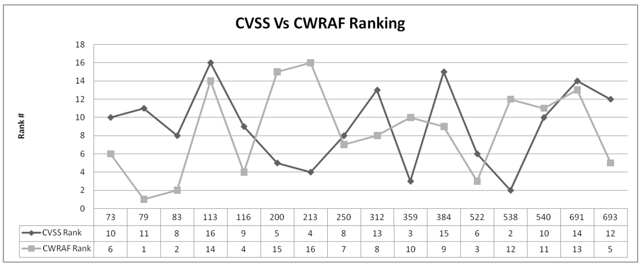
Findings and Discussion

Code analysis or vulnerability analysis is done with the help of tools like Vega and RIPS. Out of the scanning of the source code of the apps, issues are identified. Some examples of such issues found commonly found across apps are tabulated below for reference.

***Table** 3. CWE – Identified based on the Issues exhibited during the static code analysis across 3 apps.*

CWE ID	Common Consequences
CWE-384: Session Fixation	Access Control Gain privileges / assume identity
CWE-113: Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Response Splitting')	Integrity Access Control Modify application data Gain privileges / assume identity
CWE-691: Insufficient Control Flow Management	Other Alter execution logic
CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	Access Control Confidentiality Bypass protection mechanism Read application data Integrity Availability Execute unauthorized code or commands

From Table 3 it is understood that the CWE-ID related issues could further cause serious business risks if unattended. To understand the impact of these CWE, the risk scores were calculated of these applications based on Vignette for CWRAF and Environmental factors for CVSS. For instance, the CVSS based scores calculated on the Base score which primarily depends on the impact and exploitability. As per the CVSS calculation CWE-73, CWE-538, and CWE-359 seem to have a higher base score which needs attention (Figure 8).



	73	79	83	113	116	200	213	250	312	359	384	522	538	540	691	693
◆ CVSS Rank	10	11	8	16	9	5	4	8	13	3	15	6	2	10	14	12
■ CWRAF Rank	6	1	2	14	4	15	16	7	8	10	9	3	12	11	13	5

***Figure** 8. CWRAF Vs. CVSS rank comparison.*

With respect to the CWRAF calculation CWE-79, CWE-83 and CWE-522 seem to have the higher priority to be fixed. This is purely based on the assessment of the security analyst calculation on the context driven for the business need and CWRAF calculation.

Observations

According to Bozorgi et al. [23] in his paper, it's indicated that for considering the exploitability aspects more data sources are to be used. Considering the fact that CWE database may not be sufficient to understand and get protected due to the inherent nature of the hacker community and rapidly growing vulnerabilities, exploits information need to be used from sources such as Exploit-DB.

Three Commercial companies and 7 research institutes in Germany, Greece, and Norway initiated a project named CORAS for the purpose of developing a precise, unambiguous and efficient risk analysis of security critical system [24]. It is not an integrated solution to the cloud-based environment which is currently developing at a rapid pace.

The following are some of the problems which are essential for improvement of risk assessment of cloud security and to effectively manage its risk lifecycle:

1. Risk assessment has to be a continuous process which must be followed through a reference architecture aligned with existing cloud and IT ecosystem.
2. Risk occurs all around the cloud due to a connected network so well connected information exchange must be enabled through existing protocols or new means.
3. In the context of public cloud, the threat and vulnerability may be occurring which may be pre-cursor to the enterprise apps.
4. The risk assessment frameworks have to be continuously integrated seamlessly with the CWE, CVE, ExploitDB and other such databases to establish holistic capability.
5. The framework should support or have facilities to handle the Internet of things which are either part of private/public cloud within the context.
6. The interface should be expanded upon the risk management which must be used by the end users, development teams, dev ops team, and support teams to enhance the mitigation of security risks.
7. The continuous evolution of risk management across the enterprise through an integrated platform along with industry best practices is essential.
8. Dev and DevOps team involved in development and deployment must ensure the security vulnerabilities are reported back to the community which should help the community to be aware of such loopholes and its context behind it so that such threats can be managed proactively.
9. Visually represented dashboard is essential for the respective stakeholders which must be available through ubiquitous interface
10. Risk lifecycle workflow has to be automated and tracked with complete visibility across the lifecycle for safe and risk-free information systems.

Conclusion and Future Work

The existing frameworks such as CWRAF and CVSS are not comprehensive as a whole to handle the integrated SDLC life cycle. The need for integrated risk management approach is most need across the ecosystem for effective risk management in the cloud based platforms.

A possible approach for automating vulnerability check on continuous integration or new deployment can be evaluated for future. The implementation of Risk assessment framework must get integrated with Workflow and data visualization tool for effectiveness. There is the scope of enhancing the architecture to implement the integration aspects such as file types, distributed computing environment scenarios.

References

1. http://www.iso.org/iso/home/standards/iso31000.htm
2. Greg Stone. Cloud Risk Decision Framework. Microsoft, 2014.
3. Skok MJ. 2014 Future of Cloud Computing survey. NorthBridge and GigaomResearch, 2014.
4. Jhonson B. A Holistic Model for Making cloud migration decision. 10th International Symposium on Parallel and Distributed Processing with Applications, 2012.
5. Almorsy M. Collaboration-Based Cloud Computing Security Management Framework. IEEE 4th International Conference on Cloud Computing, 2011.
6. NIST. Federal Information Security Management Act (FISMA) Implementation Project, 2014.
7. Saripalli P. QUIRC: A Quantitative Impact and Risk Assessment Framework for Cloud Security. IEEE 3rd International Conference on Cloud Computing, 2010.
8. Rosenthal A. Cloud computing: A new business paradigm for biomedical information sharing. J Biomed Informat 2010.
9. Chou Y. Risk Assessment forCloud-Based IT Systems. Int J Grid High-Performance Comput (IJGHPC) 2011.
10. Subhashini S. A survey on security issues in service delivery models of cloud computing. J Network Comput Appl 2010.
11. Zissis D. Addressing cloud computing security issues. Future Generation Computer Systems 2010.
12. Drissi S. Survey: Risk assessment for cloud computing. Int J Adv Comput Sci Appl 2013; 4: 143-147.
13. Saxena S. Ensuring Cloud Security Using Cloud Control Matrix. Int J Informa Comput Technol 2013; 3: 933-938.
14. http://www.businessnewsdaily.com/5215-dangers-cloud-computing.html
15. https://cloudsecurityalliance.org/csaguide.pdf
16. cwe.mitre.org/cwraf
17. Martin RA. The Software Industry's "Clean Water Act" Alternative. IEEE.
18. https://www.first.org/cvss. Retrieved August 14, 2015, from https://www.first.org
19. https://www.isaca.org: https://www.isaca.org/Knowledge-Center/cobit/Documents/COBIT4.pdf
20. Krutz RL. Cloud Security: Comprehensive guide to secure cloud computing. Indianapolis: Wiley Publishing Inc, 2010.
21. Vohradsky D. Cloud Risk-10 Principles and a Framework. ISACA J 2012; 5: 1-11.
22. Ristov S. Cloud computing security in Business Information Systems. Int J Network Security Appl (IJNSA) 2012; 4: 75-93.
23. Bozorgi M. Beyond Heuristics: Learning to Classify vulnerabilities and predict exploits, 2010.
24. http://www.ercim.eu/publication/Ercim_News/enw49/dimitrakos.html

***Correspondence to**

K Vijayakumar

Faculty of Computer Science and Engineering

St.Joseph's Institute of Technology

Sathyabama University

India