Detection of Software Vulnerabilities Related To Security Tactics

Anjumol T Many [1], Ushus Maria Joseph [2]
[1, 2] Dept of Computer Science and Engineering
[1, 2] Mar Baselios Christian College , Idukki, Peermade-685531

Abstract- *Software architects works to identify the security requirements, and adopt some architectural solutions to address it. These architectural solutions are based on security tactics for resisting, detecting and recovering from attacks. Less experienced ones, often struggle with implementation of security tactics. The incorrect implementation or the deterioration of security tactics during coding can result in vulnerabilities named as tactical vulnerabilities. For these issues, here introducing MVC new framework that can detect the logical errors. It is able to solve the problem with input validation and actor authentication.*

I. INTRODUCTION

Security tactics are a useful tool that can help people immediately start reasoning about secure software design [1]. A security tactic is a design concept that addresses a security problem at the architectural design level. In particular, incorrect implementation of security tactics or the deterioration of security tactics during coding and maintenance activities [2] can result in vulnerabilities in the security architecture of the system, we refer to these vulnerabilities as tactical vulnerabilities. The correct implementation of "Manage User Sessions "tactic in a web application would allow the system to keep track of users that are currently authenticated [3]. Once the user authenticates him/herself with this forged session identifier, the attacker would be able to hijack or steal his/her authenticated session. Although architects have used the "Manage User Sessions" tactic in the architecture design of the web application, the developers have failed to implement it correctly. So, we conduct a deep study about the vulnerabilities related to security tactics.

User authentication is a process that allows a device to verify the identity of someone who connects to a network resource. There are many technologies currently available to a network administrator to authenticate users[4]. The actor authentication is performed in all human with computer interactions and they can automatically logged in. The Authentication means, it authorizes client to server interactions on every networks to allow access control to network and Internet connected systems. In many systems, user authentication has typically considered as a simple user ID and password combination. Nowadays, there are, more authentication tactics are added to improve the security of interactions.

If an actor authentication is not implemented strictly, the attacker can steal the user information and act as a user by providing identical requests to the application. So here introducing MVC new framework to monitor the security issues to the application developed while or after the execution. Validation detection and access control specification are the two methods used here to solve the basic issues.

The model , view and controller (MVC) is an architectural pattern that could separate an application into three main components: the model, the view, and the controller. All of these components are able to handle specific development theme of an application. To create an extensible project, one of the most frequently used web development framework is MVC.

For security of interactions, access control specifications includes the authorization, authentication and an entity trying to gain access. Access control models depends on the user. The thing is, the client or user is the one trying to gain access to the application or the software. In many systems, an access control list is there, that contains a list of permissions and it know about to whom these permissions apply. Such kind of data can be viewed by some specific people and not by others and is controlled by access control. This permits an administrator to protect information and set some rules as to what information, who can access it and at what time it can be accessed.

The input validation is considered as one of the older method to provide security as authentication. The correct testing for of any input that is supplied by someone else. This is the concept of input validation. All applications require some type of input. User inputs could come from different sources, an end-user, another application, a malicious user, or any number of other sources. The malicious users is not going to announce that, they are going to attack our software or

application. This stands to reason that all input should be checked and validated, because you do not know exactly who or what is giving you input to process. Applications and software should check all input entered by a user or coming from anywhere, but this is not the only time that input should be checked. Maybe you are getting input from a database.
do not contain all of these features, most contain one or two.

II. CONCEPT

The programmer creating a framework to retrieve the data from the system. The framework is used to call validation and actor authentication. The problem existing here is, the system cannot know who the user is or whether the user is a authenticated person or not. To solve this issue, we created a new framework called MVC new framework. This concept is showed in figure 1.By using this new framework the system can monitor the security issues to the application developed while or after the execution. If an actor authentication is not implemented strictly, the attacker can steal the user information. The attacker can act as a user by providing similar requests to the application.

III. MVC FRAMEWORK

As touched on above, model,view and controller is called as a new framework named as MVC new framework. They can solve the problem with input validation and access control. It can identify the vulnerability type. Some MVC frameworks

A simple way to understand the concepts of framework is, A user can interacts with the view state by clicking on a link or submitting a form. The controller will handles the user input when it entered, and transfers the user information to the model state The model receives the information and can updates it's state like adds data to a database. The view will checks the state of the model and its updates. It responds accordingly or one by one. The view waits for another interaction from the user or it waits for some inputs from user.

Some details of MVC new frameworks

User Request

The software architects often adopt some security mechanisms for resisting attacks. Incorrect implementation or deterioration during software evolution leads to some security bugs. If a system that contains a lots of information, that may be used by an administrator or a user. Sometimes the user can act as an administrator like requesting to the application. They can steal their information.

Frameworks for basic issues

There are many frameworks in many platform to provide security to the system. Most commonly used framework is model, view, controller framework. But in php, there is no framework for input validation and access control specification as logical issues. So, we are introducing an MVC new framework to solve the problem with logical issues.

MVC framework

A framework for any web application security. If an attacker injects some spywares to the administrator, the spywares will take the IP address of administrator and give it to the user. By this way, the user can change the IP address of itself as same as administrator. So, the system cannot differentiate them as user and as administrator. MVC new framework can solve this issue.

IV. CONCLUSION

Software architects often adopt some security mechanisms to recovering from attacks. But still we are facing some problem with input validation and access control specification. If an actor authentication is not implemented strictly, others can steal their information. There are many frameworks to find the attacker by tracking the IP address of users. Although there exists some attackers by changing the IP address of attacker as same as administrator. So, here introducing an MVC new framework to monitor and suggesting the system. This framework could solve the problem with input validation and access control specification.

REFERENCES

[1] “Towards an Architecture-centric Approach to Security Analysis”, Qiong Feng∗, Rick Kazman†, Yuanfang Cai∗, Ran Mo∗, Lu Xiao∗∗ Drexel University †University of Hawaii & SEI/CMU Philadelphia, PA, USA Honolulu, HI, USA {qf28, yc349, rm859, lx52}@drexel.edu kazman@hawaii.edu

[2] “Detecting, Tracing, and Monitoring Architectural Tactics in Code”, Mehdi Mirakhorli∗ Member, IEEE Jane Cleland-Huang† Member, IEEE ∗Department of Software Engineering Rochester Institute of Technology, Rochester, NY mehdi@se.rit.edu †School of Computing DePaul University, Chicago, IL 60604 jhuang@cs.depaul.edu

[3] "A Principled Way to Use Frameworks in Architecture Design", Humberto Cervantes, Autonomous Metropolitan University, Mexico City Perla Velasco-Elizondo, Autonomous University of Zacatecas Rick Kazman, University of Hawaii

[4] "A First Step Towards Automated Detection of Buffer Overrun Vulnerabilities",David Wagner Jeffrey S. Foster Eric A. Brewer Alexander Aiken,∗This research was supported in part by the National Science Foundation Young Investigator Award No. CCR-9457812, NASA Contract No. NAG2-1210, and an NDSEG fellowship