OUR HERITAGE
ISSN: 0474-9030 Vol-68, Special Issue-27 (Feb. 2020)
5th International Conference On “Innovations in IT and Management”
Organised by: Sinhgad Technical Education Society’s
SINHGAD INSTITUTE OF MANAGEMENT AND COMPUTER APPLICATION (SIMCA),
Narhe Technical Campus, Pune, Maharashtra (India) 411041.
Held on 6th & 7th February 2020

A Study On Web Application Security Of Management Institutes In Aurangabad district

Miss. Mrunal Milind Pandit

Department of Management Science (B.A.M.U) A’bad.
mrunalpandit07@gmail.com

ABSTRACT

The rise in protection for web applications has reached a large degree, less trusting users and more vulnerable attacks. Software reviews, penetration testing, and intrusion detection systems are just a few of the methods that companies use to monitor that attacks, and by adding SSL, firewall, vulnerability scanner, periodic evaluation, anti-virus, professional web developers will not solve web application security problems.The security mechanism has therefore been developed to provide a solution to the growing problem of web application security. The research areas of this paper focused on the commonly reported security vulnerabilities in web applications. Unvalidated Feedback, Improper Error Handling, Parameter Modification and Directory Traversal have been the most popular web security features. In addition, the work provides methods for defining threats and then providing security strategies to secure the web application from those securities.Securing websites against the protection of the internet is a challenge. The result shows the security mechanisms for the protection of the web application. The analysis of web application protection, detecting vulnerable attacks and providing security for the same.

Introduction

In recent years, the popularity of the internet and web applications has drastically increased. Web applications delivered over the HTTP protocol are the primary way of providing services on the internet and these services play a significant role in our everyday life in a variety of fields such as finance, education, industry, commerce, healthcare and even critical infrastructures. In consequence, web servers and web applications have become an attractive target for attackers and an important vector for successful attacks. Many of those attacks rely on techniques aimed at the application layer (e.g.: SQL injection, Cross Site Scripting, parameter tampering, etc.) and they are not detected by detection mechanisms operating on the transport or network layers such as network firewalls or network Intrusion Detection Systems (IDSs) . In order to detect and prevent attacks targeted towards web applications, specific Web Application Firewalls (WAFs) are commonly used. Although IDS and WAF systems have been studied and employed for decades, they have great difficulty in keeping up with the amount of new attacks that are constantly appearing. The use of zero-day exploits, sophisticated Advanced Persistent Threats (APTs) and other forms of attacks are on the rise and they are able to bypass the protection layer of IDS and WAF systems that usually rely on signature or anomaly detection technique. The shortcomings of signature-based detection techniques are well known because they can't detect new unknown attacks. The research community has focused its attention to anomaly-based detection techniques aiming to detect new unknown attacks, but the effectiveness of those techniques has also been challenged. Some researchers even state that anomaly detection is flawed in its basic assumptions , as machine learning techniques being used are good to find similar events to ones previously seen, but they are not effective to find new unknown events that are not present in the training datasets.

Objectives

To identify the key security objectives in web application security.

1. To create an overview of the application by itemizing the important of web services.
2. To highlight on the characteristics of web security and application.
3. To deconstruct the application to identify the features and modules that have a security impact, and that need to be evaluated in web securities

Methodology of Web Application Security

The following are recommended administrative controls that may help in strengthening the security of web applications and protecting data handled by such applications.

1. Put in place key guidelines to provide direction on the development and maintenance of websites and/or online applications.

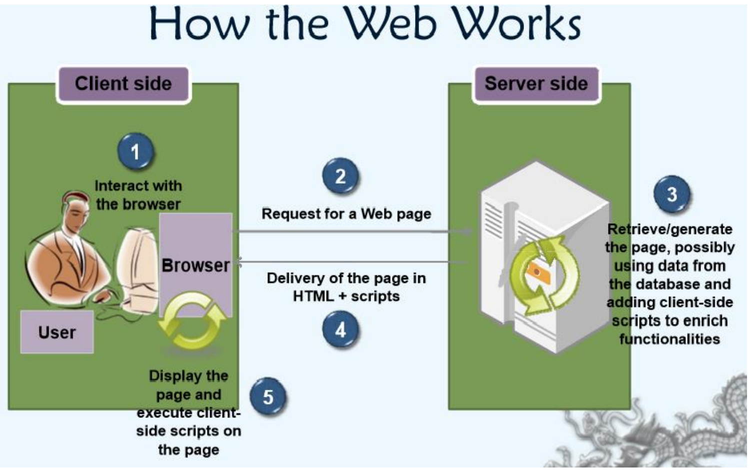
2. Put in place key guidelines on coding and development practices for web applications. Software development teams should follow a set of secure web application coding practices

3. Collect and manage sensitive information and user data in compliance with policy and regulations.

4. Prepare a security and quality assurance plan, and adopt quality assurance methods such as code review, penetration testing, user acceptance tests, and so on;

WEB APPLICTION SECURITY

IMAGE 1.


How the Web Works
Client side
Server side
1
Interact with the browser
Browser
User
2
Request for a Web page
Delivery of the page in HTML + scripts
4
3
Retrieve/generate the page, possibly using data from the database and adding client-side scripts to enrich functionalities
5
Display the page and execute client-side scripts on the page

CONCLUSION

Upon reviewing the findings of this systematic review of literature, the review supported the professionals, researchers and policy makers of web application development projects. The lack of standard security techniques to direct the creation of secure web applications indicates that more research needs to be done to decide what the correct implementation methodology is and what method is needed. Similarly, a consistent reference to the OWASP Top 10 or risk assessment in the different studies under this review suggests to both practitioners and researchers that improving safety around the development lifecycle using different tools and techniques can be effective or easier to adopt than other methods. Other approaches, such as security patterns and digital signatures, are also crucial. In addition, policy makers and practitioners need to institutionalize, in their various projects, the culture of safety considerations at an early stage and throughout the lifecycle of development, with a focus on the vulnerability of requirements.

References

[1] J.D. Meier, Alex Mackman, Michael Dunner, Srinath Vasireddy, Ray Escamilla and Anandha Murukan Microsoft Corporation http://msdn.microsoft.com/enus/library/ff648636.aspx [Retrieved: 2012-11-17]

[2] OWASP Foundation, A Guide to Building Secure Web Applications and Web Services 2.0 Black Hat Edition July 27, 2005 [Retrieved: 2012-11-22]

[3] J.D. Meier, Alex Mackman, Michael Dunner, Srinath Vasireddy, Ray Escamilla and Anandha Murukan Microsoft http://msdn.microsoft.com/enus/library/ff648651.aspx [Retrieved: 2012-11-19]