International Journal for Innovative
Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

IJIEMR Transactions, online available on 29th Jan 2021. Link :http://www.ijiemr.org/downloads.php?vol=Volume-10&issue=ISSUE-01

DOI: 10.48047/IJIEMR/V10/I01/68

Title Automatic Detection of Web Vulnerabilities and Prevention of Attacks
Volume 10, Issue 01, Pages: 337-343.

Paper Authors

Dr.Mohammad Imran

Automatic Detection of Web Vulnerabilities and Prevention of Attacks

Dr.Mohammad Imran

Associate Professor, Department of CSE, Neil Gogte Institute of Technology(NGIT),Kachavanisingaram(V),Peerzadiguda,Uppal,Hyderabad

imran.quba@gmail.com

Abstract: Web security plays important role in protective interests of real users related to completely different internet applications that area unit deployed in internet server running either in native space Network (LAN) or Wireless native space Network (WLAN). There are units several attacks doable to violate internet security. They embrace address interpretation, impersonation and session hijacking to say few. These attacks create important injury to legitimate users and cause money different risks. The prevailing solutions to stop such attacks area unit terribly helpful. However, a framework that's protractible and caters to the safety services needed by internet server is vital to possess property and continuous effort to possess countermeasures to the famous attacks and additionally unknown attacks that will be devised by adversaries in future. Towards this finish, during this paper, we tend to projected a framework called Attack Detection and bar Framework (ADPF) with mechanisms and underlying algorithms to discover and forestall numerous sorts of attacks that threaten internet security. This paper has centered on 3 attacks although the framework is protractible to support bar of different attacks. They're called address interpretation, session hijacking and impersonation. We tend to engineer an image framework that's deployed in internet server to demonstrate proof of the conception.

Keywords – Web security, automatic vulnerability detection, URL interpretation attack, impersonation attack, session hijacking attack.

Introduction

Web applications deployed in web server running in LAN or WLAN may be exposed to vulnerabilities. There might be developers who are not aware of different kinds of attacks leading to violating web security. Therefore the security of web applications deployed in wireless environments especially depends on the expertise of application developers. This is an important drawback as it is not possible to expect the software engineers to have such level of acumen in making security algorithms. The existing literature found that there are many attacks that need attention. Three attacks are in the scope of this paper. They are URL interpretation, impersonation and session hijacking. Solutions to URL interpretation attacks [1], [2], session hijacking attacks and impersonation attacks. In the literature it is found that there are many useful contributions towards prevention of attacks like URL interpretation, session hijacking and impersonation. However, a comprehensive framework to cater to the needs of present and future attacks is highly desired. Therefore in this paper we proposed a framework that is deployable in web server and monitors web applications to prevent various kinds of attacks. The framework is known as Attack Detection and Prevention Framework (ADPF). Our contributions in this paper are as follows.

1. We proposed a framework known as Attack Detection and Prevention Framework (ADPF) which has mechanisms to detect and prevent attacks made on web security. The scope of this paper is three attacks known as URL interpretation, session hijacking and impersonation.
2. Mechanisms are defined and algorithms are proposed to make the framework effective against the aforementioned attacks.
3. A prototype application is implemented and deployed in web server to protect other deployed web applications from these attacks. The framework is evaluated and found to have good utility in ensuring web security.

The remainder of the paper is structured as follows. Section 2 provides review of literature. Section 3 provides preliminaries to understand the attacks considered in this paper. Section 4 presents the proposed framework in detail. Section 5 presents experimental results. Section 6 concludes the paper and provides directions for future work.

2. RELATED WORK

This section provides review of literature on different kinds of attacks made on web server in LAN or WLAN. Mainly it throws light into three kinds of attacks namely URL interpretation attack, session hijacking attack and impersonation attack. URL interpretation is a kind of phishing attack as explored in [1] and [2]. Various researchers in [3], [4], [5], and [6] focuses on different kinds of interpretations of URLs in order to provide security to web applications. Attack recognition with malware analysis is made in [7] while security and privacy to web applications is explored[9].

Session hijacking and its prevention measures are explored. A methodology for detection of SQL injection attacks is made in while the focuses on the cross site scripting attacks and prevention measures. The concept of data hijacking and its prevention is studied in while the attacking scenarios on SCADA systems are the main focus in and. Attacks on network layers and their countermeasures are investigated. Identity based attacks with cryptography is studied in Wi-Fi impersonation attacks, impersonation detection in sensor networks, detection of impersonation attacks using weighted feature selection methods and mechanism to prevent voice impersonation attacks are other important contributions towards preventing impersonation attacks. Authentication schemes are explored as general security mechanisms. In the literature it is found that there are many useful contributions towards prevention of attacks like URL interpretation, session hijacking and impersonation. However, a comprehensive framework that is extensible and caters to the needs of present and future defence against web security vulnerabilities is found to be desired. Therefore, the objective of this paper is to propose and implement an extensible framework for attack detection and prevention to ensure web security.

3. PRELIMINARIES

This section provides description of the three attacks considered in this paper. They are known as URL interpretation, session hijacking and impersonation. These attacks are analyzed and counter measures are provided in this paper in the context of web security for the application deployed in local (LAN) or Wireless LAN (WLAN) or remote web server (WAN). As wireless networks are used widely in different domains like education, information technology, entertainment and other commercial applications, there is importance to secure them. In this context, there is week security in case of wireless networks. Thus web security is under threat. The following sub sections provide information on the aforementioned attacks.

3.1 URL Interpretation Attack

It is the attack in which attackers alter the URL to achieve their objectives of deceiving web server and gain access to certain web applications for monetary and other gains. Every URL has protocol information, port number and certain parameters. When the parameters are altered, it can cause potential risk to the web security. By interpreting URLs differently, the adversaries try to achieve their goals.

3.2 Session Hijacking Attack

Session is the duration in which the web server is capable of remembering user identity and conversation. The web server is able to identify a user after authentication using the session ID. Therefore web server creates unique session id for each user who has been authenticated and sends session id to client. This session id is to be used by client with further communications so as to help the server to identify the client. When the attackers are able to steal the session ID, they are able to hijack sessions of legitimate users and perform their intended operations. This causes potential risk to genuine users.

3.3 Impersonation Attack

It is an attack made by adversaries to perform activities on behalf of other users. It is also known as IP spoofing attack. Such attacks exploit vulnerabilities of authentication protocols and gain access to legitimate data of users. Special IP packets are created by hackers to inject IP addresses that are not genuine and gain entry to the application running in web server.

4. PROPOSED FRAMEWORK

We proposed and implemented a framework named Attack Detection and Prevention Framework (ADPF) for web security. The framework resides in web server and communicates with web components like Servlets and JSP pages in order to detect security vulnerabilities and prevent them. There are many attacks that breach web security. In this paper we focused on three important vulnerability attacks known as session hijacking, impersonation and URL interpretation. The framework is in the middle tier in the three tier architecture. Browser is the presentation tier. Web server forms web tier while database server forms data tier. The attacks are possible with the web tier. Therefore the proposed framework runs in the web tier. The framework is extensible as it can be improved further to handle other vulnerabilities in future. The overview of the proposed framework for web security is shown in Figure 1.

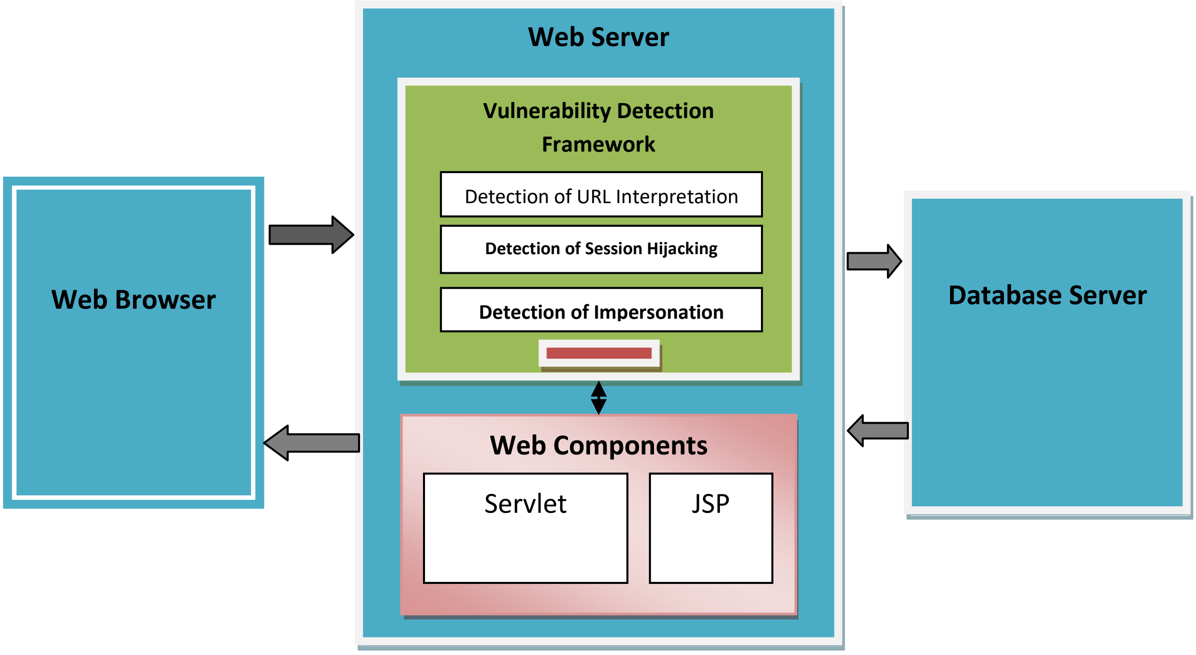
Web Server
Vulnerability Detection Framework
Detection of URL Interpretation
Detection of Session Hijacking
Detection of Impersonation
Web Components
Servlet
JSP
Web Browser
Database Server

Figure 1: Proposed Attack Detection and Prevention Framework (ADPF) for web security

Every request provided by web browser goes to web server. Attackers may follow this approach or may invoke web server directly to launch attacks. When attacks are launched in either way, there needs to be protection against vulnerabilities so as to protect web applications. Web applications are deployed in the form of .WAR archives into web server. The applications run in web container. Web container is responsible to create web components, manage life cycle of web components and create other objects like request, response, session, servlet config and servlet context. Out of all the objects, session is an important object that holds identity and conversation of a single user. It does mean that session object is created for each and every user. It may be subjected to session hijacking attack that has potential financial and other risks as adversaries can simply use the session to perform their intended activities as if done by a legitimate user. There is possibility of launching impersonation attack and URL interpretation attack. The framework proposed and implemented at server side deals with these attacks and prevents them. Towards this end, the framework has interaction with web container either directly or indirectly besides web components like Servlets and JSP pages that are server side Java technologies. The requests made by web browser are actually processed by Servlets and JSP pages. In turn these web components interact with database server in order to have the dynamism and interaction and provide dynamic responses to end users. Legitimate requests are processed as per the general approach followed in a three tier application. However, when there are suspected attacks, the proposed framework comes into picture and takes care of web security by detecting and preventing attacks aforementioned.

4.1 Prevention of URL Interpretation

Obfuscated URLs are used by adversaries to achieve their goal. In this paper we perform six kinds of tests against URL interpretation attacks to detect and prevent such attacks. The tests include DNS test, IP address test, URL encode test, shorted URL test, whitelist and blacklist test and URL pattern matching test. The DNS test finds any kind of phishing attack or the hidden intentions of attacker. The IP address test checks whether the IP address is in blacklist to generate security alert. The URL encode test actually finds whether the attacker encoded the URL. Shorten URL detection helps in understanding the intention of attacker to make phishing attack. Whitelist and blacklist test as the name suggests finds whether the URL is in blacklist and provides timely alert. The URL pattern matching test on the other hand detects similarity between anchor and hyper texts to know malicious intentions of attacker if any.

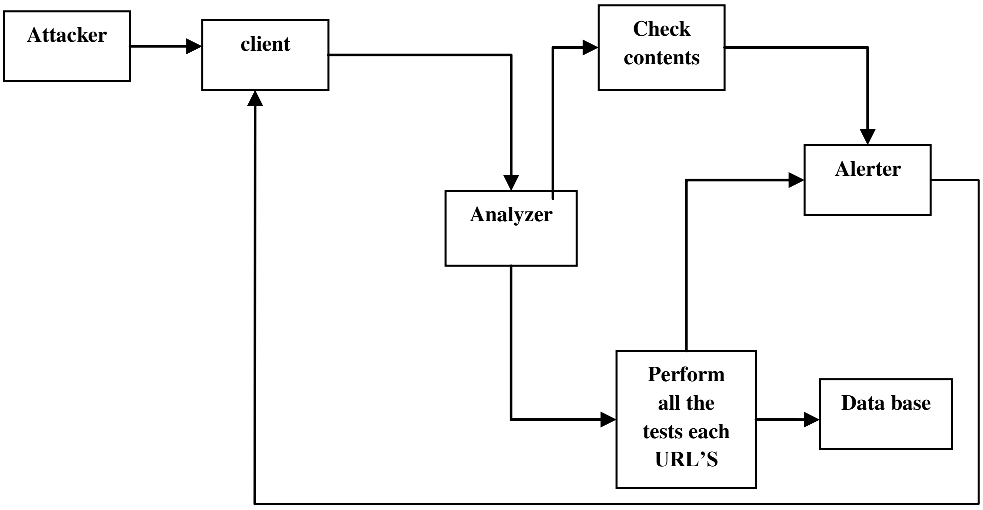

Figure 2: Detection of URL interpretation attack

As presented in Figure 2, the proposed framework has this URL interpretation mechanism. Analyzer is the module that checks any issues with URL submitted by the attackers or genuine users. Then if it suspects any vulnerability, it detects and prevents attack by providing timely alerts. If analyzer does not suspect URL, the URL is subjected to the six kinds of tests aforementioned and alerts are raised if there are suspected URLs.

4.1.1 Obfuscated URL Detection (OUD) Algorithm

This algorithm takes URLs that come to web server in any means either direct or indirect and then detects any URL interpretation attacks and prevent them. Therefore, it takes URL as input and generates alerts appropriately as output and prevents such attacks.

Algorithm: Obfuscated URL Detection
Inputs: URLs, whitelist W, blacklist B
Output: Alerts to prevent attack

```
Initialize URL vector
URL = URLs
For each url in URL
  If hypertext != anchor text Then
    Alert user
  End If
  If IP address not in W Then
    Alert user
    Add IP address to B
  Else
    Safe URL
    Add IP address to W
End If
If url is found encoded Then
  Decode URL
  Inform user
End If
If url is found shortened Then
  Alert user
End If
If patters in hypertext and anchor text are not matching Then
  Alert user
End If
```

Algorithm 1: Obfuscated URL Detection

The proposed algorithm is simple and effective as it performs all kinds of tests to know whether there is URL interpretation attack in all the URLs that reach web server either through browser or directly from thick clients.

4.2 Prevention of Session Hijacking Attack

It is one of the “man in the middle” attacks well known to the world as it causes potential risk to genuine users. The legitimate user who has logged in already to a web server and has credentials proved to perform various operations loses control to an attacker. Then the attacker performs illegal activities as if doing from legitimate session. We proposed an attack prevention mechanism as illustrated in Figure 3.

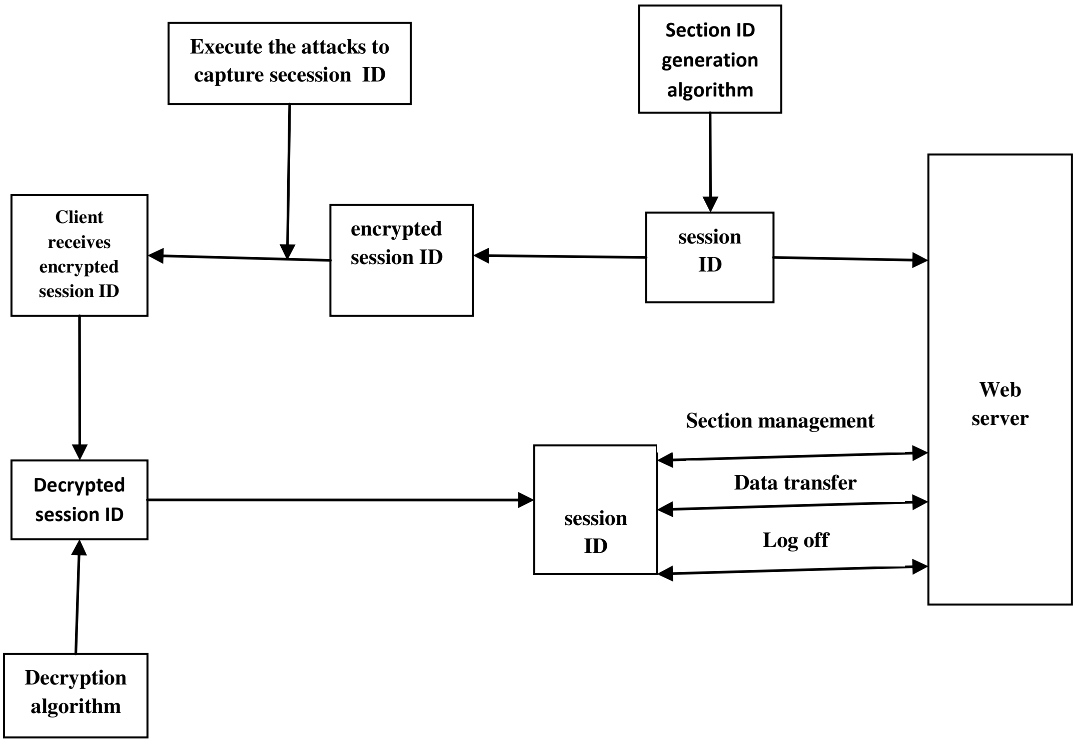

Figure 3: Mechanism to detect session hijacking attack

Before understanding the mechanism, it is important to know how sessions are created and maintained by web servers. When any user logs in, then the authenticated user will have his/her own session. It does mean that the web server creates a session object that keeps track of user's identity and conversation until he logs out. This session when hijacked, the legitimate user loses control on it while the attacker gains control over it to do his intended operations. Generally it is potential risk to genuine users in case of financial web applications pertaining to banking and other domains. As soon as session is created, the web server needs to send session ID to browser. In this process, attackers steal session ID and hijack the session. In order to prevent this kind of attack, we proposed the mechanism with encrypted session ID sent to client where decryption is made with a secret key that has been shared to client. As the session ID is encrypted, the hijackers cannot use it to have session hijacking attacks.

5. EXPERIMENTAL RESULTS

Experiments are made with the proposed framework. The results of the proposed methodology are cross validated with standard measures such as precision and recall. These are statistical measures that reflect the accuracy of the proposed algorithm in the detection of attacks. The results of experiments are presented in terms of precision and recall against different attacks explored.

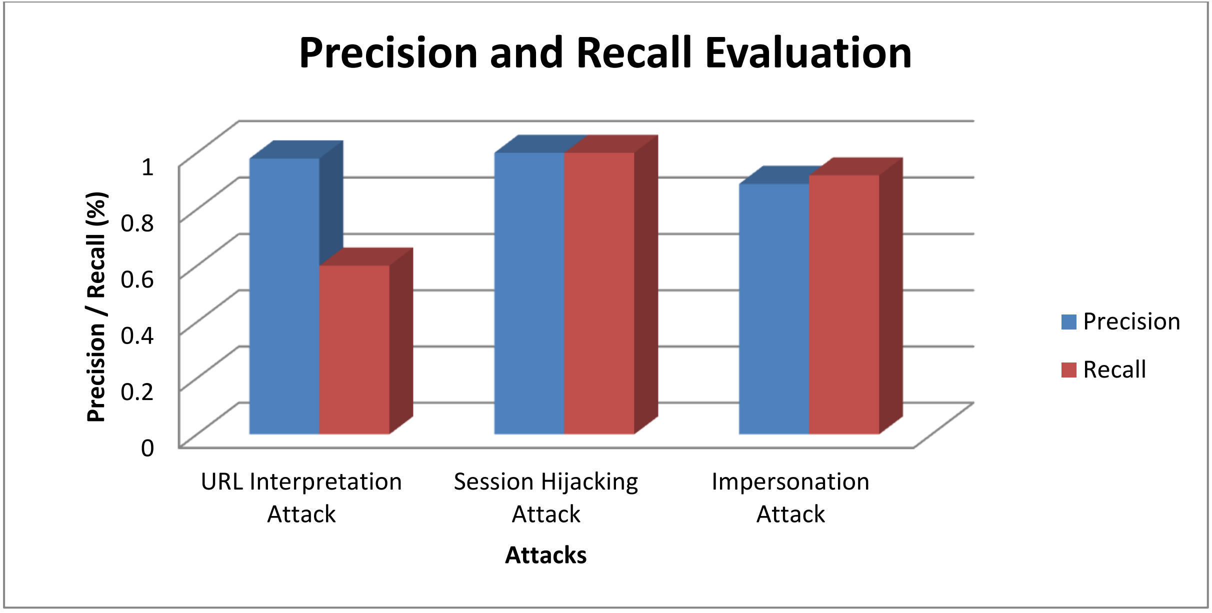

Figure 5: Results of evaluation of the ADPF

As presented in Figure 5, it is evident that the proposed framework is capable of detecting and preventing the three kinds of attacks known as URL interpretation, session hijacking and impersonation. The results revealed that the three mechanisms employed by the framework to detect and prevent attacks and ensure web security.

6. CONCLUSION

In this paper we studied security vulnerabilities that result in attacks leading to web security problems. Various attacks are found in the literature including counter measures. The individual solutions to various kinds of attacks may help in preventing particular attacks. However, a framework that resides in web server for detection and prevention of all possible attacks is highly desired. Moreover that framework should be extensible to be futuristic. In this paper we proposed an extensible framework known as Attack Detection and Prevention Framework (ADPF) for web security. It can detect all kinds of attacks and prevent them. However, three attacks are considered in the scope of this paper. They are known as URL interpretation, session hijacking and impersonation. The framework has detection mechanism for these attacks with underlying algorithms. We built a prototype framework and deployed in web server which works to protect all web applications from aforementioned attacks.

References

[1] Ria Sankhyan, Ankit Shetty, Lubdha Dhanopia, Chetan Kaspale, Prof. Gayatri Dantal. (2018). PDS - Phishing Detection Systems. International Research Journal of Engineering and Technology. 5 (4), p1-3.

[2] Jema David Ndibwile, Youki Kadobayashi, and Doudou Fall. (2017). Phishing Attack Detection by Deceptive Login Simulation through an Android Mobile App. Asia Joint Conference on Information Securit, p2-11.

[3] Mostafa A. Elgendy,Ahmed Shawish,Mahmoud I. Moussa. (2014). An Enhanced Version of the MCACC to Augment the Computing Capabilities of Mobile Devices Using Cloud Computing. International Journal of Advanced Computer Science and Applications, Special Issue on Extended Papers from Science and Information Conference 2014, p13-153.

[4] Sweety R. Lodha,S. Dhande. (2014). International Journal of Advance Research in Computer Science and Management Studies. ISSN. 2 (3), p1-6.

[5] Swaswati Goswami, Nazrul Hoque, Dhruba K. Bhattacharyya, Jugal Kalita. (2017). An Unsupervised Method for Detection of XSS Attack. International Journal of Network Security,. 19 (5), p1-15.

[6] Leslie F. Sikos. (2017). Utilizing Multimedia Ontologies in Video Scene Interpretation via Information Fusion and Automated Reasoning. Proceedings of the Federated Conference on Computer Science and Information Systems 11, p1-8.

[7] Sarah Zennou, Saumya K. Debray, Thomas Dullien, and Arun Lakhotia. (2017). Malware Analysis: From Large-Scale Data Triage to Targeted Attack Recognition . IEEE, p1-10.

[8] Tyrone Grandison,Larry Koved. (2015). Security and Privacy on the Web. IEEE, p1-4.

[9] Sajjad Arshad,Seyed Ali Mirheidari,Tobias Lauinger,Bruno Crispo,Engin Kirda,William Robertson. (2015). Large-Scale Analysis of Style Injection by Relative Path Overwrite. IEEE, p1-10.