ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 8, Issue 4, April 2021

Security Issues of Website Protection for Financial Services

[1] Manikanta V
[1] SRP in CIIL, Mysore, Karnataka, India and Research Scholar in Bharathiar University, Coimbatore, Tamilnadu

Abstract: A financial service is to provide customers for significant tasks. The financial transactions are required for mechanism to support customer activities. The financial involvement of transactions in online for any types services. The services are involved the privacy of data, customer identification and financial growth depends with security. The financial procedure involves add, delete, update of reports, customer information with many credentials. The financial activity depends on the website and website is required for security from hackers, password, etc. From this phenomenon, How to secure websites in financial activities is explored.

1. INTRODUCTION

The security involves the several features of authentication, data encryption, authorization, transport level security, permissions, privacy of data, etc. Many questions are raised under the hacking of website based on why, what, etc. Today, many open source technologies are exists to create any content management systems using WordPress, Joomla, etc. From this technologies, easily create website with little cost and virtual enviornment. The website we create using open source technology is not feasible to security with domain data loss from hackers. Majority of websites are hacked in the Server and loose, steal data in various aspects of the financial issues. The website hackers hacked the server and convert the server into for their purposes of emails, alerts, messages, etc. The reason behind of hacking website is different purpose depending upon their requirement. The Websites get hacked from mainly features of the Automation(Key), Attack of opportunity, Targeted attack, Hacking motivations and Drivers, Economic Gains, System Resources, Hacktivism, Pure Boredom, etc. Websites are get hacked due to the following reasons.

1) Access Control

The access control is focused on authentication, authorization, hosting panel and servers of user privileges, network, etc. for accessing the system. Access control mechanism for log in to hosting panel, server (FTP, SFTP, SSH), log in WordPress or Joomla, log in of computer, login to social media forums, etc. Hackers are uses brute-force method of attacks naturally to guessing username and password, generation password tools, automatic password generator, password hacking from email, etc.

2) Software Vulnerabilities and Security configuration

Software vulnerability is a defect or weakness occurs in the software or in the OS. Attackers perform unauthorized method to steal or broken websites. The vulnerability and security configuration are involved website or application code based on SQL injection to inject malicious SQL statements, Web development frameworks selection, CMS and their plugins, Operating System Command Injection, Buffer overflow, Uncontrolled String Format, Overflow of integer, Outdated components, etc.

3) Shared hosting

Hosted website is used hundreds of many other websites then hacker is used hack the website using any one of the website. The Hosted website and other websites are completely damages. The shared hosting involved causing from Shared directory like WordPress files, plugins, content, etc. Slow load time is another shared service to hack and hackers easily use storing illegal files, folders, sending spam to break the files, mail activities, etc. Distributed Denial of Service attack makes website to slow using many of malicious bots and to send traffic of website. The more traffic website response to site becomes unresponsive message for server problem. Shared IP address is IP address maps to all the websites hosted with same address of server. If any one of the website is affected to spam or illegal activity then all the IP address are blacklisted of malicious website. In untrusted Neighbours, usually web hosting provides space to other sites also. The neighbor hosting server is easily hacking to steal data from their users and hackers use spam and destroy the data easily.

ISSN (Online) 2394-6849

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 8, Issue 4, April 2021

4) Third-Party Services

The third-party tools is good but security is essential while to protect from hackers. Website is added third party tools for some specific function and the program is executed. Later, third party tool weakness of security is vulnerability for our websites.

Protect Website methods

1) Keep software up to date

The website of software are working properly with their functions and activities is needed while security point of time. The security applies to the operating system of software and website running the application for avoiding the attackers. If any software damages or not security updated then hackers easily do their job.

2) SQL injection

Hackers are usually access the web form field or parameter are linking with URL to interact with database and manipulate the database. So, from this avoid SQL statement write parameter within the Query.

Ex: select * from tables where column='" + parameter + "';"

Hackers their change URL location while adding additional queries like

"select * from tables where column=" OR '4'='4';"

Then Hackers is easily changed their queries while 4 is equal to 4.

From this, PHP Data Objects (PDO) query is easily handles the problem of injection queries.

$stmt = $pdo→prepare('select * from tables where column = :value');

$stmt->execute(array('value' => $parameter));

3) Multiple Sessions

Create session filter for avoiding multiple session for security to maintain their resources and restricting the user session at server side modules.

4) Cross site scripting attacks

XSS runs in the browsers to inject malicious JavaScript pages and steal or change their content information from attacker. The hacker is to write their scripts any of the field without validation and then easily hack their data, cookie and all the values to change their pages. From this Content security Policy method of writing JavaScript and CSS is useful to protect from XSS attacks.

Ex: the old style of JavaScript page

```
<script>function clickAction() {
alert('You clicked the button!');}
</script>
<button onclick='clickAction();'>
Want to click the button?
</button>
```

Modernized javascript method of Content Security policy style is

```
<script src='example.js'></script>
<button id='examplebutton'>Want to click the button?</button>
// example.js
function clickAction() {
alert('You clicked the button!');
}
document.addEventListener('DOMContentLoaded',
function () {
document.getElementById('examplebutton')
.addEventListener('click', clickAction);
});
```

5) Beware of Error logs

Error logs provide information of error messages and avoid the error to minimize. In order to protect the secrets of logs file from hackers.

6) Password Policy

Encryption algorithm are required to adopt SHA, MD5 encrypted method for password mechanism. Salted Hashing Password is one of the BCrypt Password encoder to generate same password to different encryption value.

7) Validate on both sides

Validations of fields are required for client side and server side scripts. Server side validation protects the data against the malicious users. Client side validation is use for browsers level compatibility is required.

8) Avoid file uploads

Using file upload option hackers usually attacks infrastructure of overwriting existing files, malicious content, service disruption, etc. For this reason, Allow only specific file types, file types verification, remove unwanted files, scan for malware, uploading user authentication, file size limit, set upload location to outside of the web root, etc.

9) Use HTTPS

Replace the website of keyword http: to https: in all pages for avoiding to steal information and SSL certificate is essential to move http: to https: for more secure.

10) Website security tools

Many Website security technologies is available like SUCURI, Qualys, Quttera, Intruder, UpGuard, SiteGuarding, Observatory, Web Cookies Scanner, Detectify, Probely, Pentest-tools, ImmuniWeb, netsparker, etc.

ISSN (Online) 2394-6849

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 8, Issue 4, April 2021

11) Authorization

The authorization of website involves the activities of the web page security and privileges. The access rights are essential part of the security to executes their functions and not allow to any other types.

12) Permission

Setting file permissions are essentially for avoiding the security problem to create a new user except root and add it to the www-data group, set the ownership of webroot directory to the www-data user and www-data group, directories are set to 755, config files are set to 644 or 604 and files are set 644 permission.

13) Alerts and notification

While login through website, alerts are required to log in time, logout time, not allow multiple session to users to send notification in each and every transactions. Alerts are used the user to save their data if any malicious problem. Alerts are required to send notifications to email and mobile no through one time password. Each and every activity belongs to the verification of security code, mobile OTP and email OTP. The notifications are required to adopt the functionality of any transactions, execute the website activities, etc.

Results

Through registration and login with security to adopt mobile OTP, email OTP, security code, security questions and apply through all the methods it will be security website and avoiding the hack of websites. The website scan through the SSL Lab, the Fig 1 shows that A+ Security and Fig 2 shows that F Security. So, website security tools are used to verify the website. The security F indicates that hackers steal the information easy and A+ security protects the website.

Figure 1

ISSN (Online) 2394-6849

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 8, Issue 4, April 2021

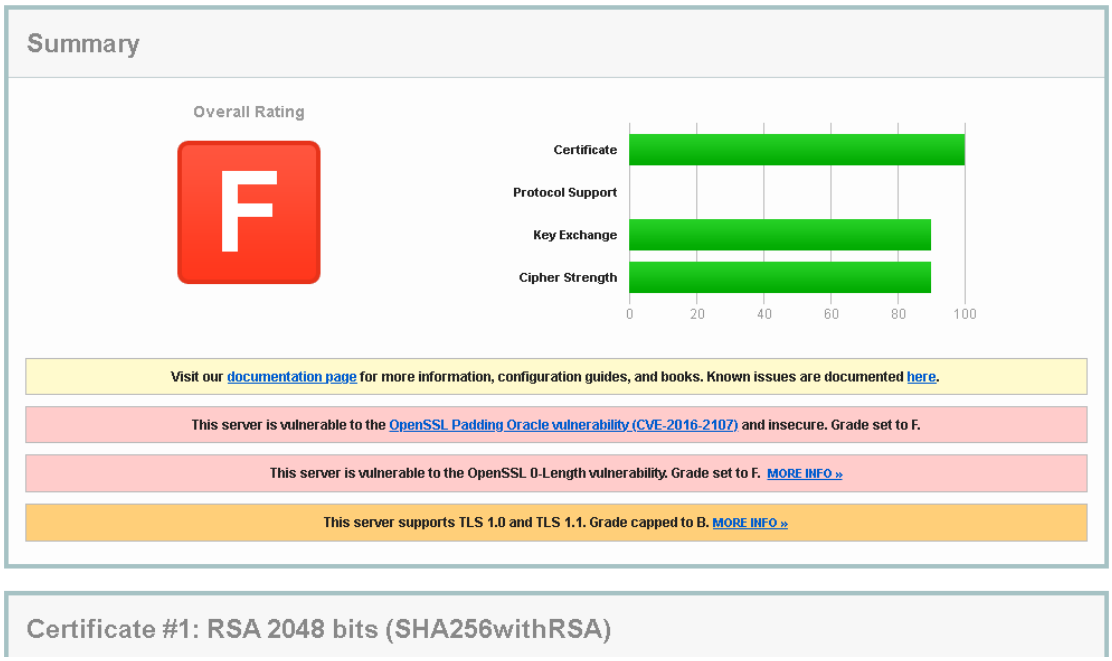

Figure 2

Conclusion

The security mechanisms involve varies activities of the website. The website security protects all the activities financial, managerial and all the intellectual properties to provide sustainable environment. Many security tools are available to maintain their Organizations of profit and loss. The cyber crime are establishes the weakness of organization and lose their dependency throughout the world market. So, security developments are required in various factor of networking and server also. The dedicated server of restore, backup and other functionalities are essential.

REFERENCES

[1] Brain Messenieechner and Jason Coleman, Building Web Apps with WordPress
[2] James Mallison, Mastering PHP 7.
[3] Krishna Shasankar, Zend Framework 2.0 by Example.
[4] Nathan George. WordPress FOR BEGINNERS: A Visual Guide to Building Your WordPress Site. 2018 Edition.
[5] Arun K Pujari, Data Mining Techniques, University press. 2001.
[6] Jaiwei Han, Michelinne Kamber. Data Mining : Concepts and Techniques.
[7] C S R Prabhu. Data Warehousing Concepts, Techniques and Applications 2nd Edition. Prentice Hall of India, 2002.