International Journal of Computer Applications Technology and Research
Volume 3– Issue 12, 809 - 811, 2014, ISSN:- 2319–8656

CMS Website Security Threat Protection Oriented Analyzer System

Pritesh Taral
Department of Computer Engineering
Sinhagad Academy of Engineering,
Kondhwa (University of Pune)
Pune, Maharashtra, India

Balasaheb Gite
Department of Computer Engineering
Sinhagad Academy of Engineering
Kondhwa (University of Pune)
Pune, Maharashtra, India

Abstract - Website security is a critical issue that needs to be considered in the web, in order to run your online business healthy and smoothly. It is very difficult situation when security of website is compromised when a brute force or other kind of attacker attacks on your web creation. It not only consume all your resources but create heavy log dumps on the server which causes your website stop working.

Recent studies have suggested some backup and recovery modules that should be installed into your website which can take timely backups of your website to 3rd party servers which are not under the scope of attacker. The Study also suggested different type of recovery methods such as incremental backups, decremental backups, differential backups and remote backup.

Moreover these studies also suggested that Rsync is used to reduce the transferred data efficiently. The experimental results show that the remote backup and recovery system can work fast and it can meet the requirements of website protection. The automatic backup and recovery system for Web site not only plays an important role in the web defence system but also is the last line for disaster recovery.

This paper suggests different kind of approaches that can be incorporated in the WordPress CMS to make it healthy, secure and prepared web attacks. The paper suggests various possibilities of the attacks that can be made on CMS and some of the possible solutions as well as preventive mechanisms.
Some of the proposed security measures –

1. Secret login screen
2. Blocking bad boats
3. Changing db. prefixes
4. Protecting configuration files
5. 2 factor security
6. Flight mode in Web Servers
7. Protecting htaccess file itself
8. Detecting vulnerabilities
9. Unauthorized access made to the system checker

However, this is to be done by balancing the trade-off between website security and backup recovery modules of a website, as measures taken to secure web page should not affect the user's experience and recovery modules.

Keywords –WodrPress,Rsync.Web Security

1. INTRODUCTION

As WWW is becoming more and more complex lot of challenges has related to security of the webpage are arising. Website security is the most important part of the post development phase of the web creation. Web publisher needs to make check-ups of the websites and audit of the website to avoid the unexpected surprises. Website should be ready to withstand any attack made on it. Moreover, the website should not affect the user's experience and revenue by compromising the security of website.

It becomes a difficult situation when security of a website is compromised when any brute force attacker attacks on your creation. Attacker tries different permutations of password and username and it also consumes all your resources and create heavy log dumps on the server which causes your website stop working.

Sometimes attacker might get access to your website by injecting the code into website through open areas of the webpages such as comment box or any text field which is processed at the server side through php or any server side scripting language.

During holidays you don't have access to the administrator panel then you can put your website admin

panel into sleep mode so that no one can attack your login page.

Some of the proposed security measures are as follows–

1. Security for user accounts
2. Security for login module
3. Security while registering user
4. Security related to database module
5. htaccess and configuration file backup and restore
6. Functionality to blacklist and whitelist
7. Firewall protection and prevention of brute force login attack
8. whois lookup and security checker
9. Security for comment spam
10. Disabling access to source code and selection of text on UI

Backup can be taken using different approaches such as incremental backup, selective backup, complete backup and user can also recover from the hacking attack by using the restore mechanism which will restore system to previous working state. Backup can be complete database backup.

This paper basically deals with mechanisms mentioned above to secure website from bad boats and hackers and make your server healthy by removing possible security threats. The Paper also pesents different backup and restore mechanisms.

2. RELATED WORK

There has been extensive efforts made to understand web security by considering network traffic, encryption techniques etc. But very few efforts have been taken to understand the security needs of CMS and the techniques to deal with them.

Some of the important work related with this study is as follows:

A web site protection oriented remote backup and recovery method :

He Qian, Guo Yafeng, Wang Yong, in his thesis describes that how we can take incremental abd decremental backups of the website which will be used to recover site during disaster. [1].

Website Regional Rapid Security Detection Method:

Yong Fang ; Liang Liu, suggested that distributed design, website regional rapid security detection method can conduct security detection for the whole region by adding detection module dynamically as needed and record results of detection. [2]

Research and solution of existing security problems in current internet website system :

Guiyang ; Xiaoyao Xie analyses the network system faced by common threats and attack methods and means for the typical, sum-up a website security system by the need to address the problem, solve these problems formulate the corresponding protection measures.

4. SECURITY MEASURES

Security for user account

Sometimes CMS might have user account with default user name ‘admin’ which is easier for attacker to predict and attack or query to your CMS. It is considered as bad security practice as it makes the task of attacker 50% easier because attacker already knows one of your credentials required to login. Besides this a Password strength tool can be used to allow you to create very strong passwords.

Security for login module

It is to protect the CMS against brute force login attacks with the login lockdown feature so that users with certain IP range can be locked out of the system for a predetermined amount of time based on the configuration setting. It also force logout of all users after a configured period of time

1. **Security while registering user**
   Enable manual approve feature for registered accounts can minimize spam and bogus registrations. Captcha can also help us to prove valid user.

2. **Security related to database module**
   Table prefixes can be modified to other prefixes to make security level higher for the attacker. Attacker cannot predict the table prefix much easily

3. **htaccess and configuration file backup and restore**
   Configurations files which are useful for running website should be protected from attacks. It is main file which provides security to other CMS modules.

4. **Functionality to blacklist and whitelist**
   It is used to blacklist and whitelist IP addresses of the web surfers. It is recommended to identify the search engine boat and spam boats

4. ANALYZE AND SUGGEST TOOL

Analyze and suggest tool is used to scan the CMS website for checking out possible threat inside the system. It then analyze the website and generate the security

reports and suggest out some possible solutions and also provides option to incorporate them into the current CMS system

Figure 1: General Architecture of the System

5. CONCLUSION

CMS security is quite different from the traditional notions of website security. CMS has a predefined structure and it is used by millions of peoples to create websites. This fact makes the attacker's task easy, as he already knows the predefined structure of CMS. Our concept would modify the traditional CMS structure into a new customized CMS so that the structure of the system would not remain as a default. Thus it becomes difficult for an attacker to predict the DB and configuration structure of the CMS which would eventually boost the security level in CMS up.

.

6. REFERENCES

[1] He Qian, Guo Yafeng, Wang Yong, Qiang Baohua1 "A web site protection oriented remote backup and recovery method" INSPEC Accession Number : 14022497 2014 IEEE

[2] Yong Fang ; Liang Liu, "Website Regional Rapid Security Detection Method" 978-1-4799-0587-4 20 13 IEEE

[3] Gaoqi Wei, "Research and solution of existing security problems in current internet website system", 978-1-4244-2584-6 20 08 IEEE

[4] Wenping Liu ; Xiaoying Wang ; Li Jin, "Design and implementation of a website security monitoring system from users' perspective", 978-0-7695-4817-3/12 2012 IEEE

Pritesh A.Taral received the B.E. degree in Computer Engineering from S.A.O.E Pune, INDIA in 2011 and perusing M.E. degree in Computer Engineering from S.A.O.E , Pune

Prof. Balasaheb B.Gite is working as Head of the department of Computer engineering at SAOE Pune India. He received the B.E. degree in Computer Engineering from P.R.E.C Loni INDIA and M.E. degree from W.C.E, Pune.