Comparative Analysis Of Web Security In Open Source Content Management System

Savan K. Patel
Research Scholar, Ganpat University
Mehsana, Gujarat, INDIA
savan.patel@ganpatuniversity.ac.in

V. R. Rathod
Rajkot, Gujarat, INDIA
profvrr@gmail.com

Jigna B. Prajapati
Research Scholar, JJT University,
jigna.prajapati@ganpatuniversity.ac.in

***Abstract*— Internet has become priceless tool that enables corporate world to show their capabilities. While Web applications have gained importance on the Internet, security is the only thing to worry. Business data is very critical that floats on the cloud and that's why Web Application Security is rapidly becoming a growing concern for all enterprises. In this paper we tried to show what is Hacking and its symptoms. In web development Content Management System (CMS) is gaining so much popularity as it uses to make easy editing and publishing process for novice even if he doesn't know web programming. There are over thousand of open source CMS available in the market. When we just talk about content management concept two or three names like Joomla, Drupal and WordPress strike in mind. As these are the one of the best CMSs in the market and their community provides nice basic security still we want to compare these CMS and want to know which CMS provides best security. To do the comparison we have done two case studies. In case 1 we have developed one common page in all CMS and host it then after we have applied different web attacks like SQLi, XSS, CSRF etc. and derived their hacking results. In case 2 we used Acunetix WVS Reporter v6.0 to find out the strength of security in different CMS. Apart from this we also try to find out Broken links in all listed CMSs.**

***Keywords—Joomla; Drupal; WordPress; Open Source; CMS; Security; Comparison*.**

I. INTRODUCTION

Internet has started in early 1960. And in last 10 years number of internet users have grown rapidly as so internet. So many user friendly web development tools and programming languages invented in last decade. There are lots of web development tool and programming languages developed by the programmer in the last few years. Web marketing has become crucial in today's world and widely accepted in commercial market in last few years. As number of websites grow their security issues also grow in the same speed. Before a decade to create and maintain website was not an easy task but with the help of CMS you can make this task so easy that even novice can handle their site. The content management system is " A system that's lets you apply management principles to content".[1] Generally all CMSs fulfill common task of content like create, edit, publish. As we have mentioned before and it is widely acceptable that Joomla, Drupal and WordPress are one of the best CMSs in open source.[5] As these listed CMSs provide best security still in this paper we want to compare these CMSs using web hacking techniques and testing tools and want to derive the best secure CMS out of these three. We have used following CMS to carry out the research.

TABLE I
CMS VERISON DETAIL

NO	CMS	VERSION
1	JOOMLA	1.6.2
2	DRUPAL	6.22
3	WORDPRESS	3.2.1

II. ROLE OF SECURITY IN WEB DEVELOPMENT

In a recent study by top analyst companies and leading security software vendors said that two-thirds of Web Applications are vulnerable to attacks and 80 percent of them will experience attacks soon. Web Security is going to be the spotlight in the future, more than ever before.It is fact that a little part of everyone's network is open, which is used to exposes business logic, system complexities and subsequent vulnerabilities to Security risks and exploitation.

Below are some of the number that highlight eminent threats to Web Applications and the importance of Security Testing:

- Watchfire says 90% of the sites are vulnerable to attacks
- Gartner says 75% of the attacks are at the application layer
- Symantec says 78% of the easily exploitable vulnerabilities affected web applications[2]

III. WEBSITE HACKING

Our website files are stored on computer somewhere. The computer, called a "server" or "web server", which is not having too much difference from our home PC, except that its configuration is specialized for making files available to the World Wide Web. Your website and server have several security systems that determine what kind of access each person has. If you are the owner, you have passwords that give you read/write access to your site. You can view files (read) and you can also change them (write).

A hacker is the one who gets through these security systems and obtains write access to your server, the same kind you have. Once they obtain that, they can change, add, or delete files whenever they want. They might do only a

little damage, or a lot. The choice is up to them.[3]

A. HACKING SYMPTOMS

As there are lots of way to know your website is hacked or not but here we present some of the best symptoms of hacking.

1) Google says "This site may harm your computer"

If Google or Yahoo search engine result pages (SERPs) display a warning about your site, the most common cause is that your site was hacked.

2) Visitors report getting viruses from your web pages

If visitors report to you that they get viruses or antivirus alerts from browsing your pages, it usually means your site has been hacked. Google and Yahoo will soon start displaying malware warnings about your site. It is possible that, your pages to deliver viruses even if your site has not been hacked. This can be occurred when your pages taking some contain from third parties such as advertisers, and they got hacked or some malicious content are in their advertisement

3) Visitors report being redirected to other websites

If you or other people try to visit your website but get automatically taken to some other website instead, it's another symptom of being hacked.

4) Your traffic decreases dramatically and suddenly

Normally web users not come back to those sites from where they get warning “This site may harm your computer”. Most web surfers stay away from sites that have the warning "This site may harm your computer". Those who continue to the site and get a virus or antivirus alert will leave immediately and might not come again. Either way, you'll see a drop in traffic. Anytime when you found, your traffic drops suddenly, investigate.

5) Your files contain code you didn't put there

If you suddenly found that your page contain some links, text or objects you didn’t put, it is clear indication you have been hacked. The source code and content of your page should always stay the same as it was when you created it. If it changes, it’s an indication that someone break your site security and change it. It should not be happen.

6) Your search engine result page (SERP) listings suddenly change

When your site listed in search engine result, the page link and its’ content should be such that you know really exist. If listings show some weird-named pages or text about topics that is not related to your site's content, it's another symptom of being hacked.[4]

IV. HACKING METHODS

A. SQL INJECTION

SQL injection is a one kind of web security attacks in which the attacker adds SQL code via web form input box to gain access to the data to make changes. An SQL query is a request for some action to be performed on a database. Normally, on a Web form is for user authentication, when a user enters their username and password into the text boxes provided for them, those values are inserted into a SELECT query. If the values entered are found as expected, the user is allowed access; if they are not found, access is denied. In most cases, web forms have no mechanisms to block user input other than username and password. If these kinds of precautions are not taken, an attacker can use the input boxes to send their own request to the database, which could allow them to download the entire database or interact with it in other illegal ways.[6]

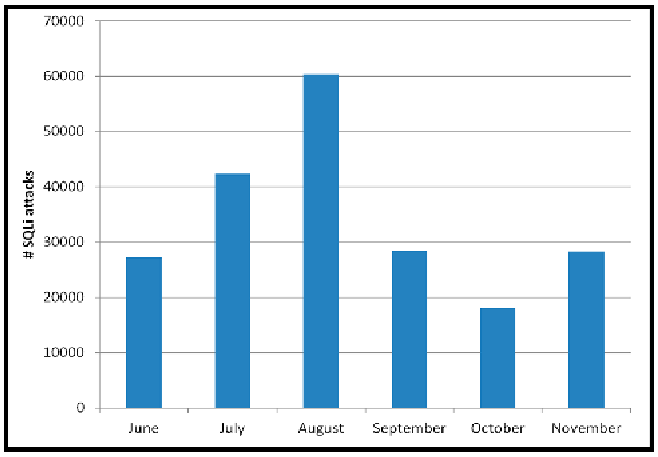

Fig. 1.The number of SQLi attacks per month in 2011[7]

The above figure sows number of SQLi attacks in 2011. From the figure data we can make a judgment about the frequency of attacks in all over the world.

B. Cross Site Scripting

Most of the websites add dynamic content to web page to make better look of the site and more enjoyable experience for the users. Dynamic content is content generated by some server process, which when delivered can behave and display differently to the user depending upon their settings and needs. Most Dynamic Web sites also accept user input which increase the risk of threat that static Web sites don't, threat like "cross-site scripting," also known as "XSS."

After an application on site is known to be vulnerable to cross-site scripting, an attacker often use VBScript, ActiveX, HTML or Flash to formulate an attack for execution a victim's system with the victim's privileges. Once an attack is activated, everything from account hijacking, changing of user settings, cookie theft and poisoning, or false advertising is possible. The XSS can be done in mostly three ways.

1. Scripting via a malicious link
2. Stealing users' cookies
3. Sending an unauthorized request[8]

The number of XSS in 2011 shown in below figure.

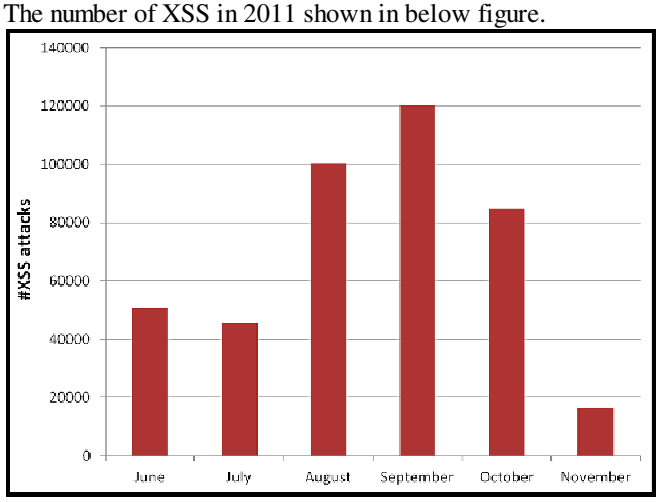

Fig. 2. The number of XSS attacks per month in 2011 [7]

C. *Remote File Inclusion*

In RFI using remote file usually called SHELL you can get admin rights of the server. A shell is graphical user interface file which is used to browsing the remote files and running your own code on the web servers. Shell inclusion allows the hacker to execute the server side commands in the same way as legitimate users and also assign access to all the server files. Remote File Inclusion (RFI) is the best ever technique to hack websites. And more than 60% websites on the internet using PHP are vulnerable to this attack. Many of the web servers are vulnerable to this type of attack because of PHP's default settings of register_globals and allow_url_fopen being enabled.[9] The number of RFI attacks in 2011 shown in below figure.

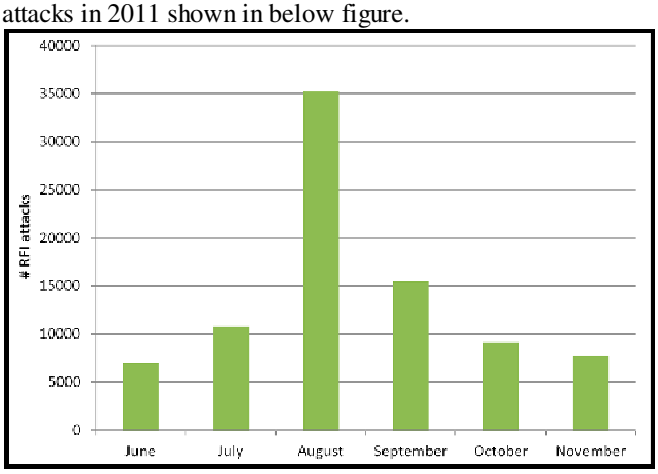

Fig. 3. The number of RFI attacks per month in 2011 [7]

D. *LFI*

Today, all the websites wants to deliver dynamic content to their users and for that they have to include file inclusion functionality. LFI vulnerabilities are formed due to improper input refinement/validation for those user specified parameters. File inclusion functions are implemented using either include (or require) directives or any of the available file handle functions (fread, file_get_contents etc). In case of file handling functions there is not much to do because every imported file is processed as string.

It is possible to execute server side code contained in the imported file when you used include directive. The next challenge is now to find a proper way to store server side code into a file that is readable from the web service running at user side. This is not an easy task and might be even impossible under some server configuration setups.[10]

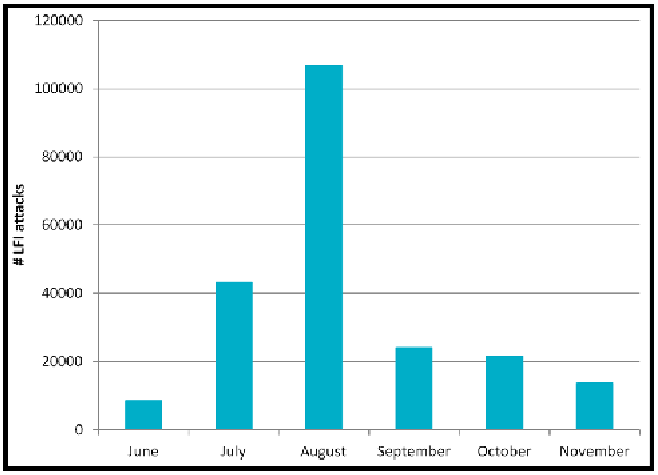

Fig. 4. The number of LFI attacks per month in 2011 [7]

The number of RFI attacks in 2011 shown in above figure.

E. *Directory Traversal*

Attackers use directory traversal attacks to try to access restricted Web server files residing outside of the Web server's root directory. The basic role of Web servers is to serve files. Files can be static, such as image and HTML files, or dynamic, such as ASP and JSP files. When the browser requests a dynamic file, the Web server first executes the file and then returns the result to the browser. Hence, dynamic files are actually files executed on the Web server. To prevent users from accessing unauthorized files on the Web server, Web servers provide two main security mechanisms: the root directory and access controls lists. The root directory limits users' access to a specific directory in the Web server's file system. All files placed in the root directory and in its sub-directories are accessible to users. To limit users' access to specific files within the root directory, administrators use access control lists. Using access control lists, administrators can determine whether a file can be viewed or executed by users, as well as other access rights.

The root directory prevents attackers from executing files such as cmd.exe on Windows platforms or accessing sensitive files such as the "passwd" password file on Unix platforms, as these files reside outside of the root directory. The Web server is responsible for enforcing the root directory restriction. By exploiting directory traversal vulnerabilities, attackers step out of the root directory and access files in other directories. As a result, attackers might view restricted files or execute powerful commands on the Web server, leading to a full compromise of the Web server. The number of Directory Traversal attacks in 2011 shown in below figure.[11]

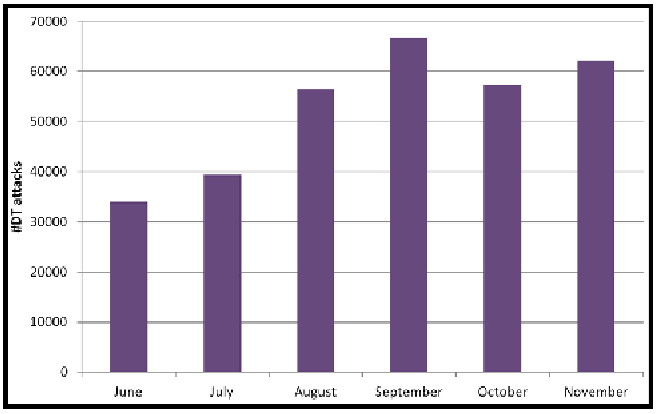

Fig. 5. The number of Directory Traversal attacks per month in 2011 [7]

F. *Brute Force Attack*

G. *Cookie Poisoning*

H. *Cross-Site Request Forgery (CSRF)*

V. SECURITY COMPARISON OF JOOMLA, DRUPAL AND WORDPRESS

A. *Case 1*

To make security comparison easy it necessary to have same condition for all the listed CMS. And for that we have created common page in all CMS with almost similar kind of content. After that we were hosted that page in three different domains one for each CMS.

1) *www.savankpatel.in (Joomla)*
2) *www.savanpatel.in (WordPress)*
3) *www.savan-patel.in (Drupal)*

below figure is an example of page that were developed to check and compare the security of listed CMS.

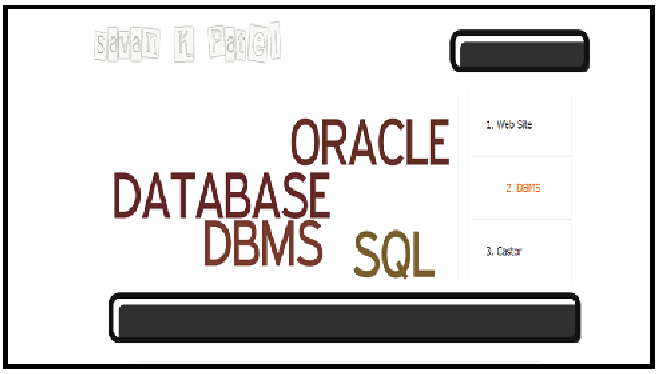

FIG. 6. Common page developed for security comparison

Result: While doing this comparison we come to know that as Joomla, Drupal and WordPress are the best CMSs, it is very hard to directly hack these CMSs by different web hacking methods. Their community provides such nice basic security that you cannot hack it straight forward in most of the case. The above listed CMSs site were hacked in the most of the cases when you use third party faulty plugins which is not certified by concern CMS.

B. *Case 2*

Now, as we were not succeed to make the comparison in the case 1, we tried to make the same thing in little different way. We have used Acunetix WVS Reporter v6.0 free tool to check security vulnerabilities in three CMS. This tool give the report of sensitive directories and files through we can get unauthorized access to exploit the site. Apart from all this it also gives report of broken links from given domains. So let's start with Joomla first.

1) *Joomla (www.savankpatel.in)*

The detail report of Joomla is as below

TABLE II
JOOMLA SECURITY REPORT

Total alerts found	18
High	0
Medium	0
Low	15
Informational	3
Possible sensitive directories	
/administrator	
/administrator/cache	
/administrator/help	
/cache	
/cgi-bin	
/logs	
/media/system	
/media/system/css	
/templates/alex-temp/css	
/templates/alex-temp/html	
/templates/system	
/templates/system/css	
/templates/system/html	
/tmp	
Possible sensitive files	
/readme.txt	
Broken links	
/a	

Above list of directories and files are open to access because its cookie is easily available so restrict access to this directory or remove it from the website will increase security strength. For an example if you take the first directory (/administrator), hacker can have following information easily which can be used to exploit the site content.

Directories:

- /administrator

Cookie:4bf74202891437c14598333521edf42=ff0af016fa45388bb62250597bdc468f
Location: http://savankpatel.in/administrator/
Content-Length: 159

- /administrator/cache

Cookie:
d4bf74202891437c14598333521edf42=ff0af016fa45388bb62250597bdc468f;60c07385b52f3b8f4c1d9523279c2477=be335630460bf7d7f8a955b0112dc08d
Location: http://savankpatel.in/administrator/cache/
Content-Length: 165

And like above two directories we can have same kind of information for all the directories.

We can get all above information for all the directories and files.

In Joomla we also get one broken link which refers to any link that should take you to a document, image or webpage, that actually results in an error. This page was linked from the website but it is inaccessible.

2) WordPress (www.savanpatel.in)

TABLE III
WORDPRESS SECURITY REPORT

Total alerts found	6
High	0
Medium Low	0
Informational	4
	2
Possible sensitive directories	
/cgi-bin	
/wp-admin	
/wp-content	
/wp-content/uploads	
Broken links	
/a	

Compare to others in WordPress only 6 alerts are found. Same like Joomla you can also have Cookie, Location and Content Length information for WordPress as well.

Directories:

- /cgi-bin

Location: http://savanpatel.in/cgi-bin/
Content-Length: 152

- /wp-admin

Location: http://savanpatel.in/wp-admin/
Content-Length: 153

- /wp-content

Location: http://savanpatel.in/wp-content/
Content-Length: 155

- /wp-content/uploads

Location: http://savanpatel.in/wp-content/uploads/
Content-Length: 163

And so on..

3) Drupal (www.savan-patel.in)

TABLE IV
DRUPAL SECURITY REPORT

Total alerts found	16
High	0
Medium	0
Low	14
Informational	2
Possible sensitive directories	
/modules/blog	
/modules/contact	
/modules/forum	
/modules/help	
/modules/php	
/modules/search	
/modules/system	
/modules/update	
/modules/upload	
/modules/user	
/scripts	
Possible sensitive files	
/install.txt	
/modules/readme.txt	
/themes/readme.txt	

- /modules/blog

Cookie: SESS4bc7e4c618cb486571212cc63bd05e46=1ad7b7c6d9c6e77b038e06b6d4145914
Location: http://savan-patel.in/modules/blog/
Content-Length: 158

- /modules/contact

Cookie: SESS4bc7e4c618cb486571212cc63bd05e46=1ad7b7c6d9c6e77b038e06b6d4145914
Location: http://savan-patel.in/modules/contact/
Content-Length: 161

- /modules/forum

Cookie: SESS4bc7e4c618cb486571212cc63bd05e46=1ad7b7c6d9c6e77b038e06b6d4145914
Location: http://savan-patel.in/modules/forum/
Content-Length: 159

- /modules/help

Cookie: SESS4bc7e4c618cb486571212cc63bd05e46=1ad7b7c6d9c6e77b038e06b6d4145914
Location: http://savan-patel.in/modules/help/
Content-Length: 158

- /modules/php

Cookie: SESS4bc7e4c618cb486571212cc63bd05e46=1ad7b7c6d9c6e77b038e06b6d4145914
Location: http://savan-patel.in/modules/php/
Content-Length: 157

- /modules/search

Cookie:
SESS4bc7e4c618cb486571212cc63bd05e46=1ad7b7c6d9c6e77b038e06b6d4145914
Location: http://savan-patel.in/modules/search/
Content-Length: 160

- /modules/system

Cookie:
SESS4bc7e4c618cb486571212cc63bd05e46=1ad7b7c6d9c6e77b038e06b6d4145914
Location: http://savan-patel.in/modules/system/
Content-Length: 160

In all three CMS, all the sensitive directories that were found are not directly linked from the website. This check looks for known sensitive directories like: backup directories, database dumps, administration pages, temporary directories. Each of those directories may help an attacker to learn more about his target.

This directory may expose sensitive information that may help malicious user to prepare more advanced attacks. So restrict access to this directory or remove it from the website.

VI. CONCLUSION

This paper is written after analyses of the performance of security in Joomla, Drupal and WordPress in the same condition. It also focuses on hacking and it's relevant information like hacking symptoms and different web hacking techniques. We tried to focus on importance of security in web development by showing number of web attacks statistics taken in 2011. To make comparison for the listed CMSs two separate experiments were carried out and tried to see that out of these CMSs which provides better web security. From the result of case 1 it is concluded that the listed CMSs provide such a nice basic security that you cannot directly hack the site using different web hacking techniques. It seems that generally these CMSs site hacked due to faulty plugins user has used which is not certified by concern CMS. By looking on the result of case 2 it can be said that we have some controversial result compared to case 1 as we got cookie information of some sensitive files and directories apart from that we also found some broken links in all three CMSs using testing tool. All above information might help hacker to prepare better attacks to hack the site. But compare to Joomla and Drupal, WordPress has very less number of sensitive files and directories so we can conclude that WordPress provides better security than other two.

ACKNOLEDGEMENT

It is my privilege to express my sincerest regards to my guide Dr. V. R. Rathod for their valuable inputs, able guidance, encouragement, and whole-hearted cooperation along with him I also thanks Mr Malay Vyas for his support.

REFERENCES

1. Web CMS report 2009 & CMS report2010, http://www.cmswatch.com/Research/Channel/CMS (accessed 6th august 2010).
2. Ananth B, "Importance of Web Application Security", sonata blogs, available at: http://www.sonatablogs.com/2010/09/02/importance-of-web-application-security/
3. 25yearsofprogramming.com," What is a website hack? Basic information to help webmasters block hackers", available at: http://25yearsofprogramming.com/blog/2008/20080311.htm
4. 25yearsofprogramming.com, "How to know if your website has been hacked ", available at : http://25yearsofprogramming.com/blog/2008/20080228.htm
5. Savan patel," Joomla, Drupal and WordPress- A statistical Comparison of Open Source CMS ", Proceedings of 3rd international conference on Trendz in Information Sciences and Computing (TISC), 2011, IEEE conference publication, pp 182-187.
6. Margaret Rouse," SQL injection", updated on January 2010, available at: http://searchsoftwarequality.techtarget.com/definition/SQL-injection
7. Imperva's Web Application Attack Report Edition #2 - January 2012, available at: http://www.imperva.com/download.asp?id=344
8. Paul Lee," Cross-site scripting", www.ibm.com, available at: http://www.ibm.com/developerworks/tivoli/library/s-csscript/
9. Suraj Bhosale, "How To Hack A Pc", March 20, 2011, available at: http://computerexperts4u.blogspot.in/2011/03/hacking-website-by-remote-file.html
10. A.Bechtsoudis, "From web app LFI to shell spawn", March 19th,2012, available at: https://bechtsoudis.com/hacking/from-web-app-lfi-to-shell-spawn/
11. www.imperva.com," Directory Traversal", available at: http://www.imperva.com/resources/glossary/directory_traversal.html