Volume 5, Issue 9, September 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Review on WebSecurity: Need of Today

Sameer Patil
Goa Multifaculty College
Dharbandora Goa, India

Abstract— As internet usage increases, websitesusage also increases , as a result web development also increases, as old saying " every coin has two sides , same manner technology also has two sides". Hacking is part of second side , many people now involve in web hacking and web defacement, this paper talk about how to provide security in that regards. As now a days Web Security needs a vital role, since todevelop a website many tools are available , so one need to security for suchwebsite. This paper mostly talks on how we provide security for the websites and which is need for today .As today many companies start their business online , so one need to provide secure solution for them.

Keywords—web security, data security, hacking, Internet , websites

I. INTRODUCTION

As the Internet usage increased, web design and web development increased drastically, so need to update with web security, and security of web is not one time event. One has to do continues provide security for the websites. It is insufficient for a code to secure only one time. Security should come throughout of SDLC.Security of web should be from all sides such as from Designing to coding. Now a days many people uses Ecommerce site for shopping so need the security in Ecommerce based websites also.Althogh the web is convenient place due to access at any time anywhere to access Service and usage ,and due to this its prime target for miscreant who attack unsuspecting web users with the aim of making an easy profit.

II. REVIEW FROM LITERATURE

Web security can be done in different ways , many a times hacker hack the website through admin panel ,with the help of sql injections, so need take care of that , solution for this is one can redirect the admin page to index page for making the admin panel secure, and if any username password field is available at front end , also make form secure by making limited value for data types.

SQL injection is a very old approach but it's still popular among attackers. This technique allows an attacker to retrieve crucial information from a Web server's database. For example :- www.xyz.com is the web url , one can open the admin panel by www.xyz.com/admin or www.xyz.com/administrator if hacker open the admin panel can attack on site through sql injection as username and password text box with submit button available . so redirect the page is the best alternative;. So best option will be provide security by placing additional text i.ewww.xyz.com/admin/?securitytext .

Secondly change the database table prefix, instead of keeping the prefix as fix , we can use random db prefix for security reasons, means if hacker knows the db prefix he can attack on the site so to avoid it change the db prefix as needed.

Third use of captcha wherever on the site user gives permission to fill the form to user or for admin panel, as without captcha many robotics action can be carried out on the site so to avoid that use captcha.CAPTCHA helps to prevent artificially intelligent automated software programs known as bots (that pose as human users) from performing malicious activities like spamming and other fraudulent activities. These Web-bots pose a major threat to web services. Web-bots try to automatically register for a large number of free accounts and then use these accounts to spam legitimate users by sending junk e-mail messages or slowing down the service by repeatedly signing on to multiple accounts simultaneously or causing other denial of services.

File permission , this is very critical as many web developer don't take this serious as 777 permission talks about full permission whereas it depends on the user usage , never give index.php as 777 permission , chances of Hacking will be increased .

IP Security is one of the best alternatives as to open the admin panel , developer need to write a code for this so that only on few IP it will work or else if any one access the web admin , email message along with details to be send to admin email id.

Session also plays vital role in web security.Most of web programming languages (e.g., PHP, JSP) offer developers a collection of functions for managing the web session. For example, in PHP, session start () can be called to initialize a web session and a pre-defined global array $ SESSION is employed to contain the session state. In either case, the client plays a vital role in maintaining the states of a web application, for security reasons its duty of developer to work properly with sessions specially while developing ecommerce site , as session plays important role and money involve over there.

Website content updating, regular interval updating of content updating is also equally important, or else hackers will target such website to hacked , many website hacked which is not updated in regular intervals. Recently few website from various state government website hacked due to not updated status. So the updating of website is equally important and plays vital role. Recently 13 Goa Government hacked and web updatation was also one of the reason.

With usage of web 2.0 increase information sharing with Social media, as a result many company promotes product services through social media , hackers try to attack this area too, so better to update this area of social networking.

Content spoofing, also referred to as *content injection* or *virtual defacement*, is an attack targeting a user made possible by an injection vulnerability in a web application. When an application does not properly handle user supplied data, an attacker can supply content to a web application, typically via a parameter value, that is reflected back to the user. This presents the user with a modified page under the context of the trusted domain.

This attack is typically used as, or in conjunction with, social engineering because the attack is exploiting a code-based vulnerability and a user's trust.

To make secure web following terminology are useful

- ✓ Firewall
- ✓ Privacy
- ✓ Integrity
- ✓ Authenticity

Firewall: web security can be done through content Regulation and Data Filtering. Blocking unwanted traffic to enter in your subnetwork .Preventing subnet user's use of unauthorised materials / sites.

Privacy:- when working on website such as ecommerce based or any banking website , need to secure data , so privacy needed to save data properly. Your personal details are equally important, so while using any banking website for net banking always use virtual keyboard. Buying and Selling of emails and demographic details are big business.

Integrity:-Maintaining the data integrity of any communication is vital, so strong password is needed in encrypted format. Even if an intruder see the transmission, it would be useless since its encrypted.

Authentication:- we need to authenticate a message to make sure it was sent by correct person.so digital signature is most effectively used in this case. Public key & Private key method can be also be used to authenticate.

Most of us use webmail for email handling and it create a problem many a times to get unwanted emails .

Code used here was:

<? php mail(reciepient@gmail.com, "hi from xyz", " hi I am xyz", "from:xyz@gmail.com");?>

Received email :-

From :-xyz@gmail.com

To:reciepient@gmail.com

Sub : hi from xyz

Hi I am xyz

So any one can send email from any one's email address its possible due to SMTP protocol.

To develop a website one should think in terms of Quality work which includes Security of website.

Mitigation :-

Do not upload personal information that you don't want to share with whole world, especially on social sites. Cause now a days many people share the details on social media which create a problem like phone number, photos.

Disallow certain dangerous nodes or attributes. For instance, nodes might be disallowed, and<object> nodes only permitted when instantiating the Flash player with known content.

Browsers: if we consider while developing a website developer need to use browser and in that case Firefox is the best browser since it provide many add-ons which helps web developer to work on quickly and provide proper checking with add-ons.

Host Provider : when one can think of security, hosting also equally important to create and make security.

SQL Injection :-Through Sql Injection one can attack the website which deals with database.SQL queries can be used to query a database, insert data into a database or modify/delete data from a database. A lot of modern websites use scripting and SQL to generate page content dynamically.

Security Requirements can be classified in Three ways:

- ➢ Confidentially
- ➢ Integrity
- ➢ Availability

Confidentially:-Only authorised user and read the data and secondly Disclose the data for relevant sources.

Integrity:-Only authorised users can modified the data

Availability: Only authorised user can access the data

In Web security Encryption of data and decryption of data can be done .Encryption: encoding and scrambling of messages to prevent their access without specific authorization.

Digital Signature also a key part in web security, Digital code attached to electronic transmitted message to uniquely identify the content and sender.

Secure Electronic Transaction: For Ecommerce based website this kind of security needed to transfer the credit or debit card information safely.

Our Solution For web security:-

- ✓ Monitorthewebsites:Its advisable to monitor the website in regular intervals , if any unknown code or file found delete it as per monitoring purpose.
- ✓ ProperBackup: always keep backup so that if any thing like hacking or defacement occur by any means we can replace the backup file , Many service provider provide that ,so we have to purchase SECURE hosting or server.
- ✓ FilePermission:-File Permission is critical, Permission 777 talks about full access of file which acess read write execute mode. If such permission given to any main file such as index.php or configuration.php then hacking might occur to avoid this always don't give full access to file.
- ✓ Data Validation at Server Side :-
- ✓ Secure Network : secure network needed with HTTPS so that its helpful for website.
- ✓ Keep Software Update if your using Third party software for web development like CMS , for cms website we need to update the version as CMS website update in regular interval so its advisable to update.
- ✓ Change your password in regular Intervals. Changing the password is good sign to update and maintain website. Its advisable to use strong password.
- ✓ Md5 data security for password field.
- ✓ File upload with proper restriction:-File upload need proper restriction.

III. CONCLUSION

Web Security is equally important aspect while developing the website , Now time has come to do make secure website from the start or when the actual web development work start that is from while creating the base idea of website . Since more than 65% of people using Internet for shopping or banking transactions to make them secure need of security in the web. So its need of today to work with Web Security .Now Security of web is most important aspect of web development as we are using web 2.0 and this age is of Digital Marketing one need to provide proper security or else it will create a problem , so Web Security is need of Today.

REFERENCES

[1] Ashwin Garg and Shekhar Singh. A Review on Web Application Security Vulnerabilities security
[2] Xiaowei Li and Yuan Xue . A Survey on Web Application Security
[3] Martin Szydlowski, Christopher Kruegel, EnginKirda, secure input for web application
[4] https://www.sophos.com/medialibrary/PDFs/technical%20papers/sophossecuringwebsites.pdf
[5] https://www.owasp.org/index.php/Content_Spoofing
[6] A Survey on Web Application Security Xiaowei Li and Yuan Xue Department of Electrical Engineering and Computer Science Vanderbilt University

