Research Challenges and Issues in Web Security

By

Rajendra Maurya (CCNA, CEH, CISSP)

IT Security Consultant at Scorpio Net Security Services

www.hackingmadeeasy.com, www.rajendramaurya.in, www.voaservices.com

ABSTRACT

There are millions of websites in the world now but it has been observed since very long time that Web Security has been one of most important areas of research whether be it either analysis or detection and later developing to mitigation plans. Web security threats are very much present now days and they have undergone much sophistication comparing to their initial phase. Now they are becoming more & more evolved each day. The evolution of threat on websites might be in terms of new ways of attack or bringing in resistance to using simulated Operating Systems or VM ware environments. Also, there has been considerable shift in the target of attacks in recent years. Earlier, clients were ignored while choosing targets. But, in recent years client user has become the main target for attacks as the adversary believe that the end user is the weakest link in the security chain. This paper is presented here to study the issues related to web security in cyber world.

INTRODUCTION

The advent of the internet and subsequently World Wide Web (www) in the mid 1990s has resulted in even greater demand for managing data, information and knowledge effectively and efficiently. There is now so much of data on the web that managing it with conventional tools is becoming almost impossible. New tools and techniques are needed to effectively manage this data. Therefore, to provide the interoperability as well as warehousing between the multiple data sources and systems, and to extract information from the databases and warehouses on the websites, various types of tools are being developed.

After successful inception of the websites, online stores are very common now days and Web applications are one of the most prevalent platforms for information and services delivery over Internet in present time as they are increasingly used for many critical services. Web applications have become quite popular in present times. Due to growing popularity of websites and web application, these are now soft targets to cyber criminals. Although a large body

of techniques has been developed to fortify web applications and mitigate the attacks toward web applications, there is little effort devoted to drawing connections among these techniques and building a big picture of web application security research.

Web Services are not only associated with advantages. There are many more issues that need to be addressed by standard bodies and technology vendors in order for Web Services to become a viable solution for building global service oriented architectures. Security is one such very important issue in this regard. Many of today's web service implementations are not publicly exposed because of the lack of security that the SOAP version 1.1 specifications left.

REVIEW OF LITERATURE

Websites are integral part of our lives now days and they are very much vulnerable to cyber attack by hackers. We all know there are lots of work has been done on this subject. So we went through following literature to carry our study on this topic: -

- Technical report of Threats, Challenges and Emerging Standards in Web Services Security
- Book Hacking Made Easy 2nd Edition by Rajendra Maurya
- Periodic journal : Website Security Statistics Report
- Journal : A Survey on Web Application Security
- Article on Security Issues for the Semantic Web
- Journal on Guidelines on securiing public websites

NEED / IMPORTANCE OF THE STUDY

"No language can prevent insecure code, although there are language features which could aid or hinder a security-conscious developer."

All the websites and web applications on running on www are vulnerable to cyber attacks. We need to understand the risk and security aspect involved in it then we need to find the appropriate remedial actions to neutralize all the attacks launched by hacker or cyber criminals on our websites/ web applications.

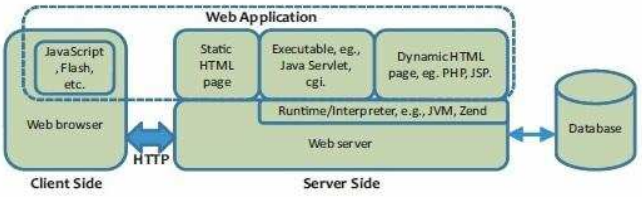

Figure: Overview of web application

There are mainly five types of attacks in the website and web applications. Here are those: -

i. Remote code execution
ii. SQL injection
iii. Format string vulnerabilities

iv. Cross Site Scripting (XSS)
v. Username enumeration

Generally poor programming approach leads to these types of attack attacks, so we need to address and study these attacks on our web application also suggest counter measures to avoid these attacks.

STATEMENT OF THE PROBLEM

Web Services are essentially an integration of technique with a potential of being used for both EAI (internal) and B2B (public) integration solutions. When used for EAI, security issues are sometimes less of a concern since the applications to be integrated are contained and protected inside the corporate network. However, depending on the application, threats may just as well exist internally to the organization as externally, so this situation should not be taken for granted.

Nevertheless, a really threatening situation appears when a Web Service that exposes an organization's internal systems is deployed publicly.

Following are the problem areas in the web security: -

- **Unauthorized Access :** This is a very broadly defined problem in web security, which may and it may encompass some of the other threats defined below, such as bypassing of firewalls and web application security and possibly also network eavesdropping.
- **Parameter manipulation or malicious input:** Malicious input means that the criminal sends non-expected data as input to the service in order for it to crash and possibly exploit the error state that the service is put in.
- **Disclosure of configuration data and message replay:** Message replay is a type of attack in which the attacker captures a legitimate message and later replays that message in order to gain unauthorized access to resources.
- **Network eavesdropping:** Interception of messages sent between the intended parties is always a threat when public infrastructures are used. Traditionally VPN or SSL have been used to protect data in transit.
- **Denial of Service attack :** Denial of services means stopping some services to execute and being utilized in the web applications
- **Reconnaissance:** Every expert hacker studies his target carefully before launching an attack. This is called reconnaissance. The attractive feature of Web Services that allows a customer to search for an interesting service to use equally means an attractive feature for a

hacker to use in order to gain intelligence about the potential victim

- **Bypassing of firewalls** One of Web Services greatest benefits is also one of the biggest threats. Since Web Services often are implemented using port 80, most firewalls will happily pass the data through without any inspection of the traffic being made.
- **Unintended software interactions – The complexity of Web Services** mean that it will take a while before a sufficiently large body of knowledge exists that can be used for defining industry best practices with regards to security. This is similar to the problem mentioned below.
- **Immaturity of the platform also points out the fact that** security is somewhat empirical in its nature. Certain vulnerabilities will not be discovered until the technology is actually attacked and tested in a real world setting. Using standards and technologies before they are fully developed and tested therefore involves a certain risk.
- **"Business process level vulnerabilities"** to the fact that the increased movement of organizations into the world of Web Services will lead to new vulnerabilities at the business process level, in enterprise software like SAP and PeopleSoft. The problem then is that not many people understand the security behind these systems. Most security experts tend to focus on the lower end of the stack.

OBJECTIVES

This research paper surveys the area of web application security, with the aim of systematizing the existing techniques into a big picture that promotes future research. We first present the unique aspects in the web application development which bring inherent challenges for building secure web applications. Then we identify three essential security properties that a web application should preserve: input validity, state integrity and logic correctness, and describe the corresponding vulnerabilities that violate these properties along with the attack vectors that exploit these vulnerabilities. We organize the existing research works on securing web applications into three categories based on their design philosophy: security by construction, security by verification and security by protection. Finally, we summarize the lessons learnt and discuss future research opportunities in this area.

HYPOTHESIS

The challenge of security based on the end user of a Web Service. One problematic aspect of Web Services is that the Web Service does not have "visibility" of the end user since the user interacts with the service through e.g. a web site. In order to be able to make authorization

decisions based on end user data, e.g. a username and password, the data needs to be included in the SOAP message sent to the service.

The challenge of maintaining security while routing between multiple Web Services is there. When the path of a SOAP message involves intermediaries, the problem is that encryption techniques that work on lower layers of the stack, like SSL, encrypt the entire communication session without any possibility to selectively choose a specific part of the message. When the message arrives to an intermediate, the intermediate needs to decrypt the data in order to extract information about where to forward the message etc. At that moment, when the data has been decrypted, it is vulnerable to unauthorized access. Another problem with a technique like SSL is that it does only provide security for data in transit. When the data is at rest, e.g. stored on a server, it is again vulnerable, i.e. SSL does not provide *persistent security*. The most likely point of attack will be when the data is in decrypted form since it follows the principle of least resistance.

A Web Service does not have to make use of HTTP for transport. Other protocols, like SMTP, could be used. If this is the case, techniques other than e.g. SSL will have to be used in order to protect the data being sent. When HTTP is used, web server security is often considered the weak link and a likely point of attack. As is evident from the above discussion, Web Services introduces many new attack vectors and threats that need to be taken into account when a Web Service is deployed. It is not sufficient to only consider technical aspects of network security, but also aspects of administrative security and physical security. If, for example, a dishonest employee gets physical access to the server hosting the Web Service at the provider's site, it may not matter how much resources have been spent on securing the data on its way to the provider. The next section will present emerging standards that will deal with the problems presented here from a technical viewpoint.

RESEARCH METHODOLOGY

Our research methodology was very simple but accurate for this paper. We contacted several cyber security professionals and experts in various organizations who are looking after web development along with cyber security. There are some companies which carry our website scanning. We contacted them also but they were hesitant respond our request, only few has cooperated with our query. Then we also gone through journals and articles based which were on the breach on web security. After lots of efforts, we could finally collect data for our research work. In the subsequent Para we will see the results of our study

RESULTS AND DISCUSSION

As simple as these questions sound, the answers have proven elusive. Most responses by the so

called experts are based purely on personal anecdote and devoid of any statistically compelling evidence, such as the data presented in this report. Many of these experts will cite various "best practices," such as software security training for developers, security testing during QA, static code analysis, centralized controls, Web Application Firewalls, penetration-testing, and more;

However, the term "best-practices" implies the activity is valuable in every organization at all times.

Following are the result for our research and survey;-

- 85 % of all websites are vulnerable to hacking.
- On average 60 % or the vulnerabilities were resolved but to do so it required an average of 3 months from notification
- 55% of companies said they provide some amount of computer-based software security training to their web developers. These organizations experienced 42% lesser vulnerabilities and resolved them 60 % faster.
- 55% of companies said their software projects contain an application library that centralizes and enforces security controls. These organizations experienced 65% more vulnerabilities, resolved them 23% slower.
- 40% of companies said they perform some amount of Static Code Analysis on their websites underlying applications. These organizations experienced 20% more vulnerabilities resolved those 27% slower.
- 60% of companies said they have a WAF (Web Application Firewall) in some state of deployment.
- 25% of companies said that their website experienced a data or system breach as a result of an application layer vulnerability. These organizations experienced 55% fewer vulnerabilities, resolved them 20% faster.

FINDINGS

The net result: websites are no less hackable today than they were yesterday. Understanding this subtle distinction is the key. Organizations must demand that software be designed in a way that makes it resilient against attack and does not require additional security products to protect it. The question that organizations should be asking themselves is: how do we integrate security throughout the website development. From the results we could find out that there are still many organizations who don't have sufficient web security measures. Whereas companies which are involved in the online commerce are opting best security measures to counter any kind of attack on their websites.

RECOMMENDATIONS / SUGGESTIONS

All the websites need to be 100 % secured in order to keep the hackers away. Let's get serious about building secure Web applications. Here are the recommendations and suggestions to keep our websites and web applications safe and secured: -

- Know which vulnerabilities will compromise you and focus on those seriously.
- Understand security controls in your languages. If you're working in a particular language, even if you're a manager, you should know the security controls for that platform.
- Never write your own security controls. "If you're a manager or stakeholder, tell your developers: 'Don't write your own security controls, because you will fail.
- Create a security community emissary. Although the information security community might seem like a bit of an insider's club and businesses would do well to ensure that at least one of their developers or managers is tasked to play Web application security champion
- User inputs are not your friend. "This will sound like it's for developers, but everyone needs to understand that user inputs are not your friend.
- Finally to be secure, you've got to be consistent so apply security controls consistently.
- Web Developers are required to be trained regularly on recent developments.

Development and testing teams are required to deliver working, robust applications under strict deadlines. In these conditions, in order to implement application security into the SDLC the suggested application security solution should be accurate, deliver clear results and be easy to use. Vulnerability testing as part of the SDLC should be part of a larger vulnerability management program. A good vulnerability testing solution not only helps you successfully identify the vulnerabilities which actually pose a threat to the application, it also shows you appropriate remediation and provides you with the means to prioritize remediation. Best of all, it should point you to the code section where these vulnerabilities exist, make remediation recommendations and even allow you to play simulations of exploits against these security flaws. It should also integrate in existing development processes.

CONCLUSIONS

Getting a grip on web security is the next important thing for Web Services if they are to be deployed in a global context and much work is being done in this field at the moment. There exist many different specifications aimed at

addressing various security problems related to Web Services. Everyone should keep in mind though, as mentioned earlier, that security is inherently empirical to its nature in that certain vulnerabilities will not be discovered until a particular technology is widely used in real world situations and subject to massive attacks. Web Services, and in particular the proposed standards for securing them, are still very immature which constitutes a big risk. Also, at this stage, most security tools available for Web Services offered by companies like Microsoft, BEA, Sun etc are only for software programmers and not administrators. This leads to several problems related to hand coded, non-reusable security solutions. Web Services security should be everyone's task, not a programming one. However, depending on the characteristics of the service, old and proved techniques like SSL can be used to provide a sufficient degree of protection. Still, most services that are up and running today seem to be deployed internally on closed and carefully monitored corporate networks and this will surely hamper the vision of Web Services as the ubiquitous technique for program to program communication

SCOPE FOR FURTHER RESEARCH

There are over 1 billion live websites all over the world. And this number is growing day by there is new things coming in this digital world, new web applications are developed also new technology comes up every day. So in this changing web world security parameters are also changing every day. We need more security professional and we need more and more research work on the developing new web security attacks launched on the websites. So when it comes to web security, whatever we do, it's never enough, it's a continuous process. We expect there should be more and more seminar and research work conducted by public and private organizations in order to prevent any kind of attack on our websites.

REFERENCES

- http://hackingmadeeasy.com/
- http://link.springer.com/chapter/10.1007%2F978-3-642-25541-0_51
- http://www.di.unipi.it/~ghelli/didattica/bdldoc/A97329_03/core.902/a90146/fundamen.htm
- https://www.whitehatsec.com/assets/WPstatsReport_052013.pdf
- http://www.symantec.com/connect/articles/five-common-web-application-vulnerabilities
- http://www.beyondsecurity.com/web-security-and-web-scanning.html
- https://www.whitehatsec.com/assets/WPstatsReport_052013.pdf
- http://www.quotium.com/content/uploads/2014/01/Seeker-Application_Security_in_the_SDLC.pdf
- http://www.beyondsecurity.com/web-security-and-web-scanning.html

- http://www.darkreading.com/risk-management/6-ways-to-strengthen-web-app-security/d/d-id/1106197?
- http://www.quotium.com/content/uploads/2014/01/Seeker-Application_Security_in_ the_SDLC.pdf
- http://www.w3.org/TR/wsc-usecases/
- http://csrc.nist.gov/publications/nistpubs/800-44-ver2/SP800-44v2.pdf