International Journal of Advanced Research in IT and Engineering

ISSN: 2278-6244

VULNERABILITIES IN WEB PAGES AND WEB SITES

Subhash Chander*

Ashwani Kush**

Abstract: *The number of online resources is increasing day by day in the public and private sectors in all departments. Even small shopkeepers, vendors are trying to get themselves online because of various advantages. One can find each and every shopping Mall and even office (Government or Private) is either online or is in the process of becoming online. But while doing so certain security precautions/flaws exist in all such sites and that may be dangerous for their growth in the competitive market as well in the government sectors. Certain security related metrics are mandatory and are minimum for the smooth working of such websites and web portals. Also many e-governance sites at national, state and district level exist in India. Acuentix Vulnerability measurement tool has been used to check certain security flaws in two websites related with educational department. Two websites taken into account are gckarnal.org and uckkr.org.*

Keywords: *Web Page, website analysis, vulnerability, scanning, e-governance.*

*Department of Computer Sc. Govt. P.G. College, Sec-14, Karnal (Haryana)

**Department of Computer Science, University College, Kurukshetra University, Kurukshetra

1. INTRODUCTION

Web applications have been highly popular since 2000 as they allow users to have an interactive experience on the Internet. Various Topologies of Networking has provided great convenience to the Government and private organizations. According to the latest figures published in the Global Information Technology Report 2009-2010 only 4.4% of the Indian population has access to the internet. At the same time, the southern Indian state of Andhra Pradesh has invested some $5.5m in their Smart GOV initiative. This is intended to put all local government services online. The two main objectives are again to cut 'red tape' and reduce costs for the taxpayers [13]. With the help of Internet one can view static web pages, rather create personal accounts, add content, query databases and complete transactions. In this way web applications frequently collect, store and use sensitive personal data to deliver services to citizens. Customers are getting lot of benefits from these applications and ideas of e-government, e-commerce and e-learning have emerged. But there is always a risk of loss of private information stored in web applications that can be easily compromised through non ethical ways. To protect their critical IT assets, most organizations use various technical protective and detective solutions. Properly placing infrastructure security solutions can increase the effectiveness of an overall enterprise security profile, but technical point solutions alone won't provide a comprehensive security strategy. For an organisation to identify susceptibility to attacks before their IT systems are exploited, it must also perform regularly scheduled vulnerability assessment and remediation [14]. E-government is one of the most important aspects of the Internet. E-Government reflects the real vision for modernizing public administration and making it more effective and efficient. In this sense, it implies a holistic view on the whole administration and government system, i.e. processes, communication and information resources, cultural and social issues, organizational strategies, technical solutions, security issues etc. [1]. Organization networks often are victims of their own success. The networks that deliver ubiquitous computing to every desktop and client also bring the vulnerabilities of impatient users to their clients [2]. Those impatient users may connect themselves to the wired network without permission, resulting in a breach of perimeter defenses that leaves the wired users wide open to compromise. In the age of ICT, citizens also have become so

much aware about their rights to get information from the government offices. Also many state governments have started giving services to its citizens in time bound manner. State governments in Punjab, Haryana, Himachal Pradesh and

Rajasthan have started giving their services within the framework of Right to service act. Development of secure e-government systems requires a comprehensive model for security that businesses will have to be ready to meet the increased demand of effective and secure online services. Providing such secure online services in e-Government requires consideration at different levels and for the distinct domains of e-Government. To achieve this various technical aspects need to be taken care of. Many concepts and tools have been developed to provide secure transactions, to protect against hacker attacks. Successfully implementing e-government requires a level of trust on the part of all transaction can by implemented during the life cycle of the project [3]. Vulnerability means one can penetrate into websites or portals in an unauthorized way. There are certain Rogue access points through which hackers can penetrate into the portal and may do they like. The problems that may be faced in this situation of breach of security include anonymous access by authorized network users; denial of service attacks (intentional or unintentional); unintended release or compromise of sensitive information. Hacker also takes care of the fact that network performance is not degraded to avoid attention of system administrators. A web application security scanner is a program that communicates with a web application to identify potential security vulnerabilities in the web application and architectural weaknesses. Unlike source code scanners, web application scanners don't have access to the source code and therefore detect vulnerabilities by actually performing attacks. According to the Privacy Rights Clearinghouse, more than 18 million customer records have been compromised in 2012 due to insufficient security controls on corporate data and web application [8]. In a copyrighted report published in March 2012 by security vendor Cenzic, the most common vulnerability in recently tested applications are cross site scripting (37%) and SQL Injection (16%). One of the weaknesses is that such tools can not cover 100 % of the source code of the application [8]. There is need of developing secure code and its proper testing for various vulnerabilities claimed or unclaimed. But merely developing secure code without attesting to its assurance capabilities is akin to operating an automobile without checking to ensure that the brakes work as expected. With such an

outlook, a crash becomes not just possible but inevitable [7]. Also logical & technical flaws can not be found with such tools. Section 2 gives details major attacks Cross site scripting and SQL injection, section 3 gives detail about Vulnerability assessment and penetration testing, section 4 gives details about Working of Acunetix Web Vulnerability Scanner (WVS), section 5 gives certain results of two educational sites and their Vulnerability scan reports and section 6 gives conclusion of the paper.

2. CROSS SITE SCRIPTING AND SQL INJECTION VULNERABILITIES

By having access control, hackers are able to penetrate and are able to deface or edit the web pages. The base of web portal is web page. By combining various web pages a website is created and by combining various websites a portal, to be utilized by many people, is created. Ultimately if one can check vulnerability of web page then ultimately vulnerabilities of websites and web portals can be checked. The

hierarchical base of web portal is shown here in fig 1.

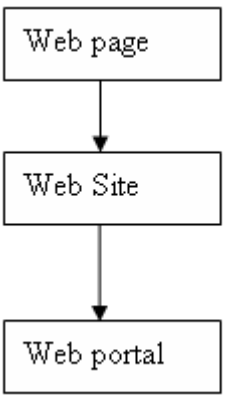

Fig. 1 Hierarchical base of a web portal

Every web page has certain security related flaws or weaknesses as SQL Injection, Privilege escalation, authentication, authorization, data loss, access control, error handling/ information leakage, command execution, session management, client side attacks, information disclosure, denial of services, audit logs, etc. For checking the vulnerability of websites and various attacks thereon, there are various soft wares available in the market. Cross–site scripting (XSS) vulnerabilities have been reported and exploited since the 1990s. The most affected sites due to XSS vulnerabilities are social networking sites. Cross-site scripting (XSS) is a type of security vulnerability that is found in web applications, such as web browsers through breaches of browser security that enables attackers to inject client-

side script into web pages viewed by other users. A cross-site scripting vulnerability may be used by hackers to bypass access controls. Cross–site scripting is also one of the special cases of code injection. Cross-site scripting uses well known vulnerabilities that are available in web-based applications, servers, or plug-in systems they depend upon. While injecting malicious scripts into web pages, an attacker can gain elevated access-privileges to sensitive page content, session cookies, and a variety of other information maintained by the browser on behalf of the user. Exploiting one of these known vulnerabilities, certain malicious content is mixed into the original content being delivered from the compromised site. This whole activity operates under the permissions granted to that system from the user side. Major classifications of the types of XSS are non-persistent and persistent. Non-persistent XSS vulnerability is the most common type of vulnerability being exploited. Google could allow malicious sites to attack its users who visit them while logged in. The persistent XSS vulnerability is a more devastating variant of a cross-site scripting flaw. It occurs when the data provided by the attacker is saved by the server, and then permanently displayed on normal pages returned to other users in the course of regular browsing, without proper HTML escaping. Here hacker's script is rendered automatically to third party websites rather than individual targets. SQL injection is a technique for targeting databases through a website. It is done by including small parts of SQL statements in a web form. SQL injection utilizes code injection technique to exploit vulnerability in a website's software. It happens when user input is incorrectly filtered for various special characters embedded in SQL statements. SQL commands are injected from the web form into the database and change the database content or dump the database information like credit card or passwords to the attacker. SQL injection is known for attacks on websites but it can also be used to attack any type of SQL database [11]. Such type of attacks can be used by the hackers to acquire and edit the information stored in Government databases. It is very critical to think about the loss if information regarding the owners of land is displayed to anti social elements in the society. Getting information about the bank accounts of a bank can be risky job for banks and its customers. Hence majority of the attacks on databases and e-governance are of the type SQL injection.

3. VULNERABILITY ASSESSMENT AND PENETRATION TESTING

Our vulnerability is increasing daily as our use of and dependence on electronics continues to grow. The current vulnerability of our critical infrastructures can both invite and reward attack if not corrected [12] Vulnerability scanner is a computer program that is used to assess computers, computer systems, networks or applications for weaknesses. There are a number of types of vulnerability scanners available today, depending on particular targets. While functionality varies between different types of vulnerability scanners, they share a common, core purpose of enumerating the vulnerabilities present in one or more targets [5]. These two terms namely Vulnerability assessment and penetration testing are normally used in the same situation. Although there are certain phases that seem to similar in both the tools yet there is a lot of difference between the two terms.

(1) Vulnerability Analysis is used to identify the vulnerabilities (weak points) on a network, whereas a Penetration Testing is used to access systems in an unauthorized way.

(2) Vulnerability Analysis deals with potential risks, whereas Penetration Testing is actual proof of concept. Vulnerability Analysis is a process of identifying and quantifying the security Vulnerabilities in a system. Vulnerability Analysis doesn't provide validation of Security Vulnerabilities. Validation can be only done by Penetration testing [4].

(3) A Vulnerability Analysis provides list of the flaws that exist on the system while a Penetration Testing provide an impact analysis of the flaws on the underlying network, operating system, database etc.

(4) Through vulnerability analysis one can know about the logical flaws whereas penetration testing is used to exploit those flaws identified through vulnerability assessment. As example through vulnerability analysis one can know the status of open ports or non availability of antivirus on a particular machine and then with the help of that Penetrating testing what resources of the machine can be accessed and used, manipulate by the hackers.

(5) Vulnerability Analysis is a passive process whereas penetrating testing is an active process where ethical hackers simulate an attack and test network and system tolerance power.

(6) A Vulnerability Analysis explains about Vulnerabilities present and used to improve security posture whereas penetration testing can be used to break-in vulnerable systems and gives only a snapshot of the effectiveness of your security programs.

4. WORKING OF ACUNETIX WEB VULNERABILITY SCANNER (WVS)

Acunetix Web Vulnerability Scanner (WVS) is an automated web application security testing tool that audits your web applications by checking for vulnerabilities like SQL Injections, Cross site scripting and other exploitable hacking vulnerabilities [10]. Acunetix WVS scans any website or web application that is accessible via a web browser. It also offers a strong and unique solution for analyzing off-the-shelf and custom web applications including those relying on client scripts such as JavaScript, AJAX and Web 2.0 web applications. It is suitable for any small, medium sized and large organizations with intranets, extranets, and websites aimed at exchanging and/or delivering information with/to customers, vendors, employees and other stakeholders. Acunetix WVS works in the following manner:

1. The Crawler analyzes the entire website by following all the links on the site and in the robots.txt file and sitemap.xml (if available). WVS will then map out the website structure and display detailed information about every file. It also analyses hidden application files, such as web.config.
2. After the crawling process, It launches a series of vulnerability attacks on each page found, in essence emulating a hacker. Also, WVS analyses each page for places where it can input data, and subsequently attempts all the different input combinations. This is the Automated Scan Stage.
3. During the scan process, a port scan is also launched against the web server hosting the website. If open ports are found, Acunetix WVS will perform a range of network security checks against the network service running on that port.
4. As vulnerabilities are found, Acunetix WVS reports these in the ‘Alerts’ node. Each alert contains information about the vulnerability such as POST variable name, affected item, http response of the server
5. If open ports are found, they will be reported in the ‘Knowledge Base’ node. The list of open ports contains information such as the banner returned from the port and if a security test failed.
6. After a scan has been completed, it can be saved to file for later analysis and for

comparison to previous scans. Using the Acunetix reporter a professional report can be created summarizing the scan [10].

5. FINDINGS AND RESUTS

Acunetix WVS has been applied to two educational institute websites namely gckarnal.com and uckkr.org. Results of the scanner are shown here in fig. 2 and fig. 3. Two websites have been checked for the existing vulnerabilities.

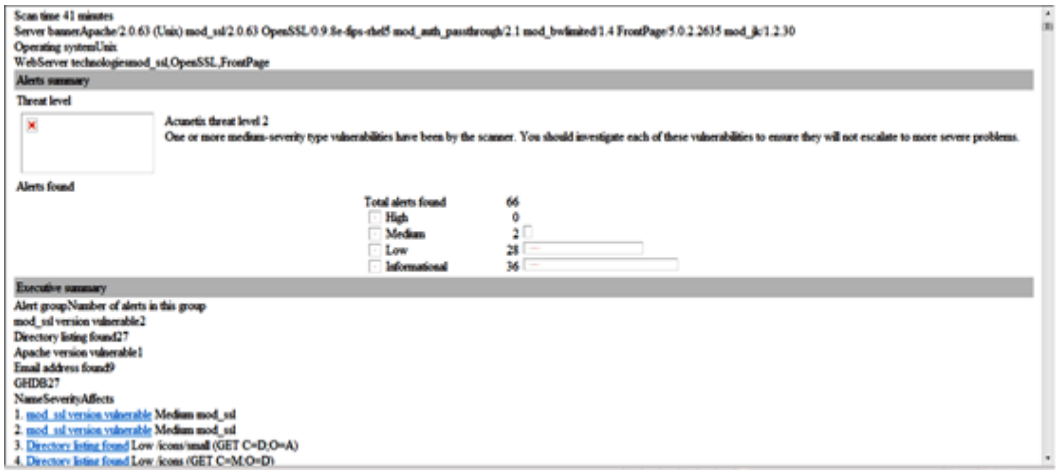

Figure 2 summary of gckarnal.com

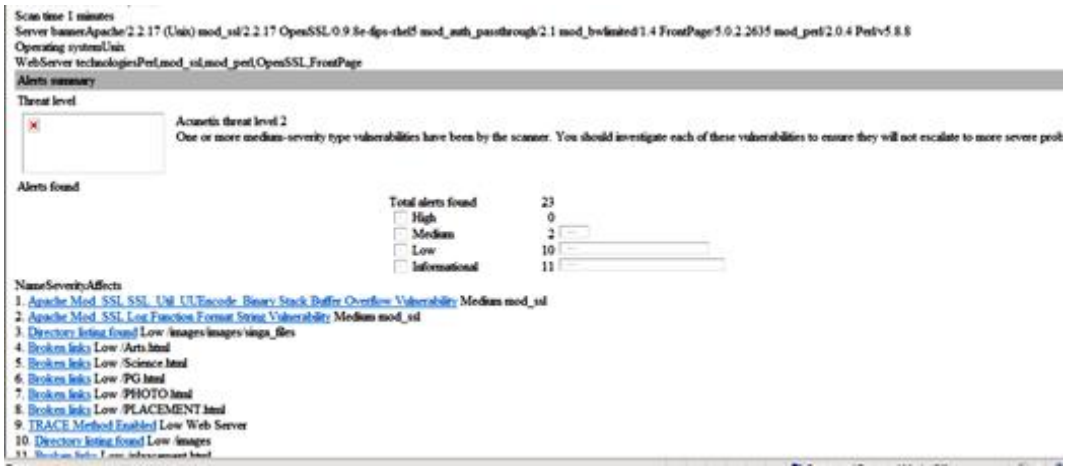

Figure 3. Summary of uckkr.org

Both the results show that gckarnal.com has more security alerts as compared to uckkr.org. Majority of the alerts are informational or low category. Number of medium and high alerts is same for both the sites. Details of various alerts shown in results are here as under. Mod_ssl alerts are the medium level alerts found in the both the results. Mod_ssl is an optional module for the Apache HTTP Server. This Mod_ssl alert would most likely result in a denial of service attack if triggered, but could theoretically allow for execution of arbitrary

code. It is also clear that these alerts may be false positive. It is one of the limitations of the Vulnerability scanners that it requires human intervention for analyzing the data after scanning process. Scanners can only report vulnerabilities as per plug-ins installed in the scan database. They cannot determine whether the response is a false negative or a false positive. Hence after medium alerts, there is one message like it can be a false positive. Regarding vulnerability scanning, "false negative" is the failure to recognize an existence of a flaw in the system or the network under assessment, whereas "false positive" is the incorrect determination of the presence of vulnerability. The former might be due to missing plug-ins in a scanner database while the latter requires human judgment to confirm [6]. It is possible to provide HTTP and HTTPS with a single server machine, because HTTP and HTTPS use different server ports. The number of low level alerts is 28 and 10 for gckarnal.com and uckkr.org respectively. Low level alerts include directory listing and broken links mainly. In gckarnal.com majority of the alerts in low level category are directory listings, whereas in case of uckkr.org majority of the alerts in low level category are broken links. A link that does not work any more is called a broken link or dead link. A link may become broken for several reasons. The simplest and most common reason is that the website concerned doesn't exist anymore. Many times one gets a message like error 404-page not found, that is because of dead link and means that web server responded, but the specific page could not be found. There may be several other reasons of the broken link .A link might also be broken because of some content filters or firewalls and on the part of the authoring side. On an Apache HTTP Server, directory listing refers to a directory on the server that does not have a default index file. The file is usually called index.html, index.htm, index.php, etc. Hence make it sure that directory does not contain sensitive information or you may want to restrict directory listings from the web server configuration. In informational alerts category majority of the alerts are based on the e-mail address found and related with icons and pictures. Other informational alerts are related with Google hacking database (GHDB) or icons and Jpg files available on these sites. While implementing e-governance projects, there is a gap between those making concepts and those who have to implement them. Action has to be taken to improve the conditions for successfully implementing e- Government projects [9].

6. CONCLUSION

Acunetix Web Vulnerability Scanner is used for website security scanning that checks for SQL injection, Cross site scripting and other vulnerabilities. It checks password strength on authentication pages and automatically audits shopping carts, forms, dynamic content and other web applications. Both the websites taken in consideration are educational institute websites. After completion of the scan a detailed report is

provided and reports those pinpoints where vulnerabilities exist. By looking at the report it is clear that majority of the security alerts are informational type and are not counted in high level of alerts. Overall uckkr.org is having fewer alerts and is more secure as compared to gckarnal.com. Also there is a lot of difference in the scan time of both the portals. Interestingly website having more vulnerability takes more time for vulnerability scanning. Hence e-governance portals must also be tested against such vulnerabilities before rolling out, otherwise sensitive information related with the citizen's database including private information may be compromised and utilized wrongly by the hackers.

REFERENCES

[1] Wimmer Maria and Bredow Bianca Von," E-Government: Aspects of Security on Different Layers", 12th IEEE International workshop on Database and Expert Systems Applications "On the Way to Electronic Government, Pp 350-355, Munich, Germany, 2001

[2] Henning Ronda R., "Vulnerability Assessment in Wireless Networks," pp.358, Symposium on Applications and the Internet Workshops (SAINT Workshops), 2003

[3] Al-Ahmad,W. and Al-Kaabi, R. ,"An Extended Security Framework for e-Government", Pp 294-295 ,Intelligence and security informatics (ISI), IEEE International Conference 17-20, June, Taipei, Taiwan, E-ISBN: 978-1-4244-2415-3, Print ISBN: 978-1-4244-2414-6 (2008)

[4] "Penetration testing Vs Vulnerability Assessment", available at www.primeinfoserv.com/pdf/consulting/VAvsPT-Prime.pdf

[5] Available at www.en.wikipedia.org

[6] "An Overview of Vulnerability Scanners", February (2008), Available at www.infosec.gov.hk/english/technical/files/vulnerability.pdf

[7] Paul Mano ," Assuring software security through testing , White ,Black and somewhere in between" , A whitepaper available on www.isc2.org

[8] Available at www.rtbot.net/Web_application_security_scanner

[9] Lenk Klaus and Traunmüller Roland," Electronic Government: Where Are We Heading?", EGOV, LNCS 2456, pp. 1–9, Springer-Verlag Berlin Heidelberg ,2002.

[10] User manual of Acunetix Web Vulnerability Scanner V8, v.1 (2012) and available at www.acunetix.com

[11] Mathur Peeyush et al. ," Sql-injection security evolution analysis in asp.net", International Journal Of Engineering Science & Advanced Technology (IJESAT), Volume-2, Issue-3,Pp 657 – 663, ISSN: 2250–3676 (2012)

[12] Caelli W.J. et al.," Policy and Law: Denial of Service Threat", An Investigation into the Detection and Mitigation of Denial of Service (DoS) Attacks: Critical Information Infrastructure Protection, Pp 41-114, Chapter 3, © Springer India Pvt. Ltd. 2011

[13] Johnson Christopher W. and Raue Stefan ," On the Safety Implications of E-Governance: Assessing the Hazards of Enterprise Information Architectures in Safety-Critical Applications", SAFECOMP 2010, LNCS 6351, pp. 402–417, Springer-Verlag Berlin Heidelberg 2010

[14] Liu Simon, Holt Larry, and Cheng Bruce ,"A Practical Vulnerability Assessment Program", Vulnerability Assessment, Pp 36-42, IT PRO , Published by the IEEE Computer Society, 2007