IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 19, Issue 1, Ver. IV (Jan.-Feb. 2017), PP 01-03
www.iosrjournals.org

An E-Governance Web Security Survey

Deven C. Pandya[1], Dr. Narendra J. Patel[2]
[1](*Department of Computer Application, U.V. Patel Engg. College/ Ganpat University,Kherva, Gujarat India)*
[2]*((Department of Computer Application, U.V. Patel Engg. College/ Ganpat University,Kherva, Gujarat India)*

Abstract: *The purpose of the study is to explore web security status of the E-Governance websites and web applications. The central theme of the paper is to study and analyze the security vulnerabilities in the technologies utilized for E-Governance website and web application development. The study was conducted in the State of Gujarat,India. The data related to web development technologies, vulnerabilities affecting those technologies, vulnerability severity, and vulnerability type were gathered from 26 E-Governance website/Web application for detail analysis. The outcome of the study depicts the relationship between technology vis-a-vis vulnerability type and vulnerability severity.*

Keywords: *Web Security, Vulnerability, Risk, E-Governance*

I. Introduction

E-Governance is the public sector's use of information and communication technologies with the aim of improving information and service delivery, encouraging citizen participation in the decision-making process and making government more accountable, transparent and effective. [1] Information security, at times, shortened to InfoSec, refers to the processes and methodologies which are designed and implemented to protect print, electronic, or any other form of confidential, private and sensitive information or data from unauthorized access, use, misuse, leak, destruction, alteration, or disruption. [2]. Information security is important for successful E-Governance implementation. Protecting confidentiality of an individual's personal data that he/she provides to obtain government services is an important challenge in implementing e-Governance. [3] Apart from E-Government implementation, effective Information Security is essential to protect Government IT assets from Cyber terrorism, Advance Persistent Threats, hackers etc.

In India, it is compulsory for each Government web sites/web application to go through security audit from enlisted agencies before hosting and after addition of new module. In addition to this department must devise a security policy to address various security issues related to website/web application [4] Government of Gujarat has also made security audit obligatory on each instance of website update or every six month whichever is earlier for all the organizations through Computer Emergency Response Team –India enlisted security auditors. [5]

II. Web Security Survey

Vulnerability scanners are effective tools for web security survey and finding vulnerabilities in the web application or website. Total 26 Websites/Web Applications related to Government Departments were surveyed and scanned for vulnerabilities. Accunetix scanner is utilized for this purpose. Accunetix ranked no 1 according to the 2013/2014 Web Application Vulnerability Scanners Benchmark. [6] [7] The websites/Web Application was chosen randomly from Government website directory. The websites/ web applications were scanned for parameters like Vulnerability, Vulnerability severity, Vulnerability type, Asset information, and Technology used for development. Using the survey results the research article was already published to depict the vulnerability its severity, impact and solutions in our paper on E-governance web security audit. [8] The remaining results and analysis is discussed here to gain full insights of E-Governance web security in Indian context

The Vulnerability found and their type and severity level given in **Table 1** below. In each severity level group below table depicts vulnerabilities having occurrence in more than 10% websites/web applications.

III. Technology Vs Severity analysis

Web security scanner crawler identified mainly two technologies Microsoft and Apache during the scan. All web application/websites either hosted on Microsoft Server or Apache Server. The Apache technology here includes Apache Tomcat and Apache HTTP Server.

Table 1

Vulnerability	Severity Level	Vulnerability Type
Cross Site Scripting	HIGH	Validation
Proxy accepts CONNECT requests	HIGH	Configuration
ASP.NET Padding Oracle Vulnerability	HIGH	Validation
Microsoft IIS tilde directory enumeration	HIGH	Configuration
Application error message	MEDIUM	Validation
HTML form without CSRF Protection-Cross Site Request forgery	MEDIUM	Informational
User credentials are sent in clear text	MEDIUM	Informational
ASP.NET error message	MEDIUM	Validation
Session Cookie without Secure flag set	Low	Informational
OPTIONS method is enabled	Low	Validation
Broken Links	Informational	Informational
Password type input with autocomplete enabled	Informational	Informational
Typical login page	Informational	Informational
Possible internal IP address disclosure	Informational	Informational
Error page Web Server version disclosure	Informational	Configuration

The server technology pattern depicts that software development technology like Microsoft .net framework, Java, PHP has been utilized for website/web application development. Below given **Table 2** depicts relation between server Technology and Vulnerability severity.

Table 2

Technology Vs. Severity	High	Medium	Low	Informational
Apache	9.84%	27.87%	44.26%	18.03%
Microsoft-IIS	9.09%	24.24%	37.37%	29.29%

As seen from the **Table 2**, in Apache technology, incidence of low severity vulnerability is highest with 44.26% followed by medium 27.87%, informational 18.03% and high with 9.84% occurrence. In Microsoft Technology occurrence of low severity vulnerability is highest with 37.37% followed by medium 24.24%, informational 29.29% and high with 9.09% occurrence. Here we can conclude that in both the technologies occurrence of low and medium severity level vulnerabilities is higher in comparison to high or informational severity type vulnerabilities. In addition to this, we can also notice that occurrence of medium and low vulnerabilities are higher in Apache technology than Microsoft technology while occurrences of high and informational vulnerabilities are higher in Microsoft technology than Apache technology.

Table 3

Technology	Utilization
Apache	38.13%
Microsoft-IIS	61.88%

Table 3 depicts % utilization of technology for website/web application development. As per the **Table 3**, it is clear that Microsoft Technology is utilized in 61.88% sites while Apache Technology is utilized for 38.13% websites. It means the majority of websites/web applications used Microsoft Technology for Development.

IV. Technology Vs Vulnerability Type analysis

Below **Table 4** depicts the relation between Technology and Vulnerability type.

Table 4

Technology Vs. Vulnerability Type	Configuration	Informational	Validation	Grand Total
Apache	18.18%	58.18%	23.64%	100.00%
Microsoft-IIS	12.90%	50.54%	36.56%	100.00%

As seen from the **Table 4**, incidence of configuration type vulnerabilities i.e Proxy accepts CONNECT requests, Microsoft IIS tilde directory enumeration etc. and Informational type vulnerabilities i.e. Possible internal IP address disclosure, Broken Links etc. is higher in the websites using Apache Technology as compared to the websites based on Microsoft technology. The incidence of Validation type vulnerabilities i.e. Cross-Site Scripting, Application error message etc. and Informational type vulnerabilities i.e. Possible internal IP address disclosure, Broken Links etc. are higher in websites based on Microsoft Technology than websites based on Apache Technology.

V. Severity VS Vulnerability Type

Below given **Table 5** depicts the relation between Vulnerability severity and Vulnerability Type found in the E-Governance websites.

Table 5

Severity vs. Vulnerability Type	Configuration	Informational	Validation
High	58.33%	0.00%	41.67%
Medium	23.08%	30.77%	46.15%
Low	3.28%	57.38%	39.34%
Informational	11.11%	88.89%	0.00%
Grand Total	14.86%	53.38%	31.76%

It is clearly evident from the results depicted in above **Table 5** that major high severity vulnerabilities found in configuration type vulnerability group. Medium severity vulnerabilities mostly found in validation type vulnerability group. Low and informational severity vulnerabilities found mainly in informational vulnerability type group.

VI. Conclusion

Among 26 Websites/Web applications Microsoft Technology is utilized in 61.88% websites while Apache Technology is utilized for 38.13% websites. From the analysis, it is observed that in both the technologies occurrence of low and medium severity level vulnerabilities is higher in comparison to high or informational severity type vulnerabilities. Apart from this, it is also observed that occurrence of medium and low vulnerabilities are higher in Apache technology than Microsoft technology while occurrences of high and informational vulnerabilities are higher in Microsoft technology than Apache technology. In technology and vulnerability type relation, it is observed that incidence of configuration type and informational type vulnerabilities is higher in the websites using Apache Technology as compared to the websites based on Microsoft technology. The incidence of Validation type vulnerabilities are higher in websites based on Microsoft Technology than websites based on Apache Technology. In severity vs. vulnerability type relation, it is observed that major high severity vulnerabilities belong to configuration type vulnerability group while medium severity vulnerabilities mostly belong to validation type vulnerability group. Low and informational severity vulnerabilities mainly exist in informational vulnerability group.

References

[1]. UNESCO, "E-Governance," UNESCO, 2001. [Online]. Available: http://portal.unesco.org/ci/en/ev.php-URL_ID=3038&URL_DO=DO_TOPIC&URL_SECTION=201.html. [Accessed 14 July 2016].

[2]. Sans. Institute, "Information Security Resource," SANS, [Online]. Available: https://www.sans.org/information-security/. [Accessed 14 July 2016].

[3]. P. Mittal and A. Kaur, "E-Governance - A challenge for India," *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, vol. 2, no. 3, March 2013.

[4]. "Guidelines for Indian Government Websites," Department of Administrative Reforms and Public Grievances, Government of India, 2009.

[5]. "Guidelines for Registration, Hosting and periodic security audit of Government Websites," Science and Technology Department of Government of Gujarat, Gandhinagar, 2014.

[6]. S. Chen, "Security Tools Benchmarking," [Online]. Available:] http://sectooladdict.blogspot.in/2014/02/wavsep-web-application-scanner.html.

[7]. "Web Application Scanner Comparision," Acunetix, [Online]. Available: https://www.acunetix.com/blog/news/acunetix-comparison-web-application-scanners/.

[8]. "Security Innovation Appsec. Blog," Security Innovation, Inc. , [Online]. Available: http://web.securityinnovation.com/appsec-weekly/blog/bid/89728/Prevent-Information-Disclosure-in-Error-Messages.