International Journal of Enterprise Computing and Business Systems
ISSN (Online) : 2230-8849
Volume 6 Issue 1 January - June 2016
International Manuscript ID : 22308849012016-299

OWASP TOP 10 VULNERABILITY ANALYSES IN GOVERNMENT WEBSITES

Deven Pandya [1], *Dr. N. J. Patel* [2]

[1]*Research Scholar, Department of Computer Application, Ganpat University Kherva, Gujarat, India*

[2]*HOD, Department of Computer Application, U.V.Patel Engineering College, Ganpat University Kherva, Gujarat, India*

ABSTRACT

Government websites are useful constituents for information dissemination and citizen centric services. Various vulnerabilities exist in Government websites. In this paper, vulnerabilities found in Government website are categorized and analysed as per Open Web Application Security Project (OWASP) Top 10 to understand impact of these vulnerabilities on web security of Government websites. In this study we have analysed security pertaining to 99 Government websites. Out of 99 websites we have found vulnerabilities in 97 websites. To achieve the results we have cross tabulated vulnerabilities found in these websites with their security risk level. As a result we have found that vulnerability A5-security misconfiguration is the main contributor of web security risk in Government websites. Apart from this it is clearly evident that majority of the vulnerabilities found in Government websites belongs to low risk group but still few high impacting vulnerabilities exists and needs to be take care of without delay. Thus the paper contributed towards the understanding of web security risk in Government websites

Keywords

Government, Governance, Information Security, OWSAP,Risk

INTRODUCTION

The Open Web Application Security Project (OWASP) is a Non Profit Charitable Organization with the mission to make software security visible to Individual and Organisation to help them taking informed decision about their software security risk. [1] OWASP TOP 10 is a security project sponsored by OWASP. This project publishes a list of what it considers the current top 10 web application security risks worldwide. The list explains vulnerability with a relevant example and the way to avoid it. The most recent version of the top 10 list was published in June 2013. OWASP prioritized the top 10 according to their prevalence and their relative exploitability, detectability, and impact. [2] Table 1 depicts list of OWASP TOP 10 Vulnerability.

Table 1: OWASP TOP 10 Vulnerability

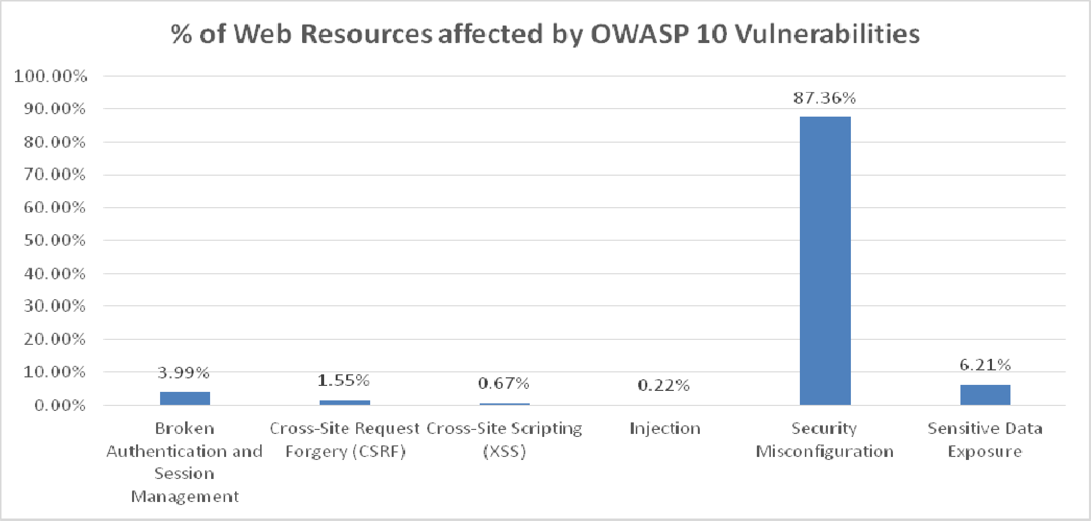
A1	Injection
A2	Broken Authentication and Session Management
A3	Cross-Site Scripting (XSS)
A4	Insecure Direct Object References
A5	Security Misconfiguration
A6	Sensitive Data Exposure
A7	Missing Function Level Access Control
A8	Cross-Site Request Forgery (CSRF)
A9	Using Components with Known Vulnerabilities
A10	Unvalidated Redirects and Forwards

Government websites are the main source of Information for the citizens and they are the key component in E-Governance projects since with increase in E-governance initiatives Government provides various citizen centric services through these websites. E-Governance is the application of Information and Communication Technology (ICT) for providing government services, exchange of information communication transactions, integration of various stand-alone systems and services between Government-to-Citizens (G2C), Government-to-Business (G2B), and Government-to-Government (G2G) as well as back office procedures and communications within the entire government framework. [3] In case website is collecting citizen's data, it must ensure confidentiality, Integrity and privacy of the data. Maintaining privacy and confidentiality of an individual's personal data that he/she provides to obtain Government services is a major impediment in implementing e-Governance. [4].Apart from this, acts of cyber terrorism, defacement of Government websites are increasing day by day. In India, the State of Gujarat is leading in E Governance initiatives. The State ranks in TOP 5 States in E-transactions as per Electronic Transaction Aggregation & Analysis Layer (E-Taal) March 2016 report. Etaal is a web portal for sharing e-Transactions statistics of National and State level e-Governance Projects. [5] . In India, it is mandatory to conduct security audit from the enlisted agencies for each Government websites/web application. The security audit should be done before hosting and after addition of a new module. Apart from this, each Department must have a security policy to address various security issues related to a website/web application. [6] Government of Gujarat has also made a security audit mandatory 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. [7] We have collected security reports related to 99 websites in the State of Gujarat, India. In the next section of the paper we have analysed the OWASP TOP 10 Vulnerability found in Government Websites.

VULNERABILITY ANALYSIS

We have reviewed security report of 99 Government websites. Out of 99 websites, we have found vulnerabilities in 97 websites. From the OWASP TOP 10 vulnerabilities mentioned in Table1, we have observed six vulnerabilities viz. A1, A2, A3, A5, A8 and A6 in Government websites. The % of web resources affected by these vulnerabilities is depicted in Chart 1. The web resource includes files, directories web pages that reside on webserver and together work as functioning website.

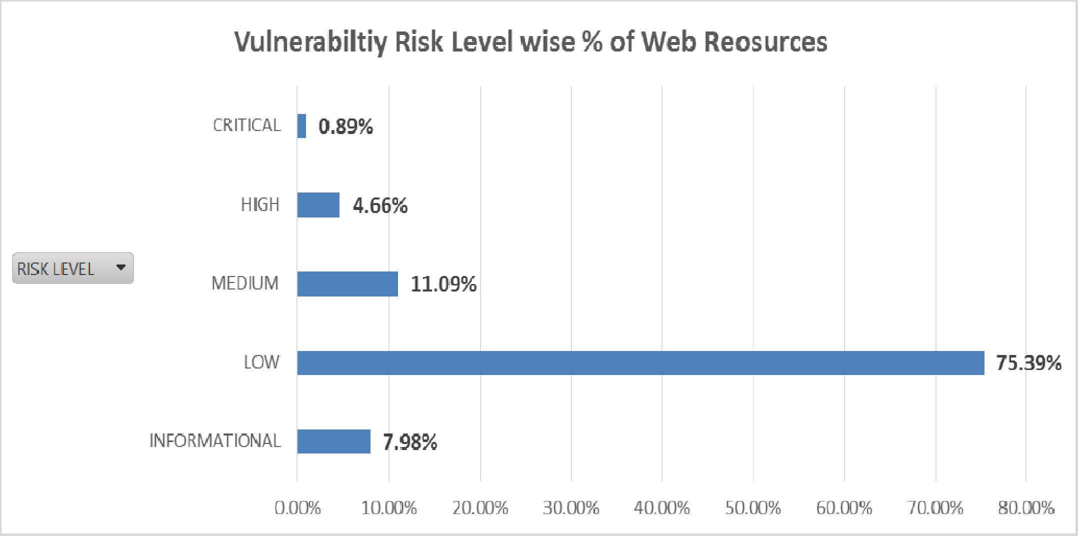
Chart1: % of Web Resources affected by OWASP 10 Vulnerabilities



As shown in above Chart 1, vulnerability A5 is the major contributor to the web security risk in Government website with 87.36% vulnerability found in web resources. The remaining vulnerabilities remain less than 7%.

We have also analysed vulnerabilities according to the risk level. In security risk level wise analysis, we have observed vulnerability in 451 web resources according to the risk level viz. low, high, medium, informational and critical. The graph given below depicts vulnerability risk level wise % of web resources.

Chart 2: Vulnerability Risk Level Wise % of Web Resources



As seen from the chart2 vulnerabilities having low risk level is the most prevalent among the Government websites. Medium risk level 11.09%, Informational risk level 7.98% and High risk level 4.66% vulnerabilities found in very few web resources in websites. Critical Risk level vulnerabilities found in negligible web resources but still looking at their critical impact, the websites having web resources with critical vulnerability needs immediate attention by concern authorities.

In the next section, we have analysed OWASP TOP 10 vulnerabilities by cross tabulating it with risk level. Table 2 depicts cross tabulation of risk level with OWASP Top 10 vulnerabilities found in Government websites.

Table 2: OWASP Top 10 Vulnerabilities vs. Risk Level

OWASP TOP 10 Vulnerability	CRITICAL	HIGH	MEDIUM	LOW	INFORMATIONAL	Grand Total
A2-Broken Authentication and Session Management	25.00%	57.14%	8.00%	0.29%	0.00%	3.99%
A8-Cross-Site Request Forgery (CSRF)	0.00%	0.00%	0.00%	2.06%	0.00%	1.55%
A3-Cross-Site Scripting (XSS)	25.00%	9.52%	0.00%	0.00%	0.00%	0.67%
A1-Injection	25.00%	0.00%	0.00%	0.00%	0.00%	0.22%
A5-Security Misconfiguration	25.00%	4.76%	90.00%	91.76%	97.22%	87.36%
A6-Sensitive Data Exposure	0.00%	28.57%	2.00%	5.88%	2.78%	6.21%
Grand Total	**100.00%**	**100.00%**	**100.00%**	**100.00%**	**100.00%**	**100.00%**

From the above table, we can easily deduce that A2, A3, A1 and A5 are equally contributing to the critical risk to the Government websites. A2 is contributing 57.14% in high risk followed by A6 with 28.57%. A5 is the single largest contributor of informational, low and medium type risk with more than 90% prevalence in each risk category. From the above, it is clear that comparative low risk levels (Medium, Informational and low) are generated due to security misconfiguration. High risk level is generated due to A2 and to some extent A6. Excluding high level in all risk level A5 is the major or equal contributor of web security risk in Government websites. From the above it is clear that Government authorities should deal with security misconfiguration to make their website more secure. Vulnerability in web resource mainly affects confidentiality, availability and integrity of information resource. Regular website security auditing is required to restrain the constantly emerging threats and keep Government websites secure and safe. [8]

CONCLUSION

From the above it is clearly understood that Government websites required web security due to its vital role in information dissemination and citizen centric services. It is equally important to save Government websites from rogue nations, hacker groups, cyber terrorist etc. who want to deface Government websites, steal confidential data and challenge Government in cyber space. From the above paper, we can easily conclude that there are vulnerabilities in Government websites among them A5-Secuirty Misconfiguration is the single largest contributor of web security risk in Government websites. In our study, A5 found to be affecting 87.36% web resource in various Government websites. Majority of the vulnerabilities belongs to the lower risk group viz. medium, low, informational with 11.09%, 75.39%, 7.98% respectively. High risk vulnerabilities are very few with 4.66% and mainly contributed by A2- broken authentication and session management and A6- sensitive data exposure with prevalence in 57.14% and 28.57 % web resource respectively. Critical risk vulnerabilities found in a very negligible web resources with 0.89 % and it is contributed by A1, A2, A3 and A5 equally with 25% but authorities must deal with these vulnerabilities urgently to prevent any risk to the Government websites.

REFERENCES

[1] "OWASP Home Page," [Online]. Available: https://www.owasp.org/index.php/Main_Page.

[2] "IBM Developerwork Library," [Online]. Available: http://www.ibm.com/developerworks/library/se-owasptop10/.

[3] "Wikipedia," [Online]. Available: https://en.wikipedia.org/wiki/E-governance.

[4] 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.

[5] "E-TAAL HOME," [Online]. Available: http://etaal.gov.in/etaal/auth/Login.aspx.

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

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

[8] D. Pandya Deven, "An E-Governance web security audit," *International Journal of Computer Engineering and Applications,* vol. IX, no. VI, June 2015.