International Journal of Computer Applications Technology and Research
Volume 5–Issue 10, 619-626, 2016, ISSN:-2319–8656

Government Web Application Security: Issues and Challenges - A Case of India

Dr.V.Ranga Rao
Senior System Analyst
Soil and Land Use Survey of India
Department of Agriculture, Cooperation and Farmers Welfare
Ministry of Agriculture and Farmers Welfare ,
Government of India, India

Abstract: The public services offered by the government are trustworthy, for that reason the government needs to understand various threats, vulnerabilities, and trends in order to protect the citizen database and offered services. This paper studied various acts, rules, policies, guidelines and standards adopted by the government departments for development of design, development & deployment of web-based applications and cited various problems related to coding, manpower and funding issues as a case of India. This study shows, the majority of government departments is developing and audited web applications before hosting on the public domain. But, for this most departments have to depend on the private organizations. This drawback arises in the government departments because of lack of certified or educated staff. Thus the government departments ought to train their staff along with administrators in information security from time to time. This will ensure making improvements to the internal protection and reduce the dependency on private organization tremendously.

Keywords: E-Government, OWASP, Security, SQL Injection , Vulnerabilities , Web application

1. INTRODUCTION

The government allows citizens to get access to their information and services for citizen satisfaction. Many nations are using web-based services for improving government efficiency and transparency. The government departments at the National and State level is collecting, storing and sharing the citizen's information among their stakeholders. For this reason, the government is to increase a privacy protection and protection of the citizens' data. The e-government, privacy defined as the "credible government protection of the citizens' personal data" [1].The citizens, departments of the government and employees are afraid to utilize government services if these services are not secure. The citizens have different needs and demands for services, as a result, it is no longer sustainable for governments to use one preferred way of service provision over the other. It is now ever more need that governments exploit all possible delivery channels to reach out to as many persons as possible, irrespective of how illiterate or remote [2].

The government web applications are more significant because of the vast information related to the citizens. Web applications interact with database systems, which may store sensitive information related to such as Income Tax, financial, etc., the compromise of web-based applications would outcomes in breaching ability, for that reason, it leads to severe financial losses, ethical and legal penalties. As web applications are more and more used for important citizen services, they are a target for security attacks. These applications have more significance due to the vast amount of sensitive intelligence and confidential information of citizens. Although web applications can offer convenience and efficiency, there are also a number of the latest security threats, which would possibly pose big dangers to an organization. The e-citizens except that the e-government services are safe and secure, and the privacy of the e-citizens included. Thus the government organizations not only to an understanding of current trends in protection threats, but also be ready to find inherent vulnerabilities within current programs. Despite trusted security and privacy measures forms a crucial success reason for e-government that has not been yet addressed as only 20% of national portals have security features [2].

The aim of this paper examines various web application vulnerabilities and how they can address. This paper examines the procedure adopted by the government departments for design, development & deployment of secured web-based applications. As an Indian scenario discussed on various issues such as coding, staffing requirements, and funding issues. This study shows that government departments in India should follow proper guidelines for secured web application design, development, and deployment. However, the majority of government departments are developing web applications and conducting security audit through private organizations. Therefore the government departments should train their employees, including administrators in the web application security area from time to time. This will make sure not only improving internal security but also to cut the dependency on the private organization tremendously.

The paper organized as follows: Section 2 presents a literature review of vulnerabilities in the web applications, security standards and benchmark in governments. Section 3 provides an overview of the OWASP vulnerabilities. Section 4 studied adopted procedure for Indian government web application, development, and deployment and analyzed web defacement statistics during the year 2015.Section 5 presents issues and

challenges related to coding, staff, requirements and funding in the government organizations. Section 6 presents the results and conclusions are given in Section 7.

2. LITERATURE REVIEW

A website is a single point of contact to the citizens for information, at anyplace and anytime. On demand, they download the necessary forms and they can post their grievances to the government according to their convenience. In some nations, government was providing web-based services since 1990.The website is one type of two-way communication between citizens and government to share information and download forms. The e-citizen except that the services provided by the government are safe and secure, that the privacy of the e-citizen protected. The citizens will hesitant to utilize the online administrations offered by the legislature, because of their poor attitude, the absence of certainty, security and protection concerns [3]. The citizens of Nations namely Japan, India, and Latin America have adopted mobile services as their primary interface to the website and are demanding more and more mobile access to government services [4]. The aim of the government websites is centralizing various services to a single portal where citizens can use services, regardless of which department provides that service [2]. About 25 nations have developed separate mobile government web pages. The citizens, use the Internet to download forms for various services [5]. The citizens use e-government services if these services are secure and privacy (James, 2000). Despite the growth in the development of e-government services, the government departments are facing problems with vulnerabilities and threats [7].In this literature, the vulnerabilities related to web applications reviewed for this study .A summary of attacks in three decades from the year 1980 to 2000 given in Table 1.

Table 1: Evolution of points of attacks in three decades (Source :[10])

Vulnerability	Points of Attacks	Decade
Sensitive data left in plain view	Physical access	1980
Weak Passwords	Network Access	1990
SQL injection attacks	E-mail, Application, Wireless	2000

Moen et al., (2007) reported that, around the world , 82% of web application attacks based on the cross-site scripting and Structured Query Language (SQL) injection, 81.6% websites of the governments from 212 different countries were vulnerable to Cross Site Scripting (XSS) and Structured Query Language (SQL) injection. The Continent–wise , percentage of vulnerabilities in e-government web applications. The number of countries enclosed in parenthesis is given in Table 2.

Table 2: Percentage of vulnerabilities in E-Government for each continent and the number of countries enclosed in parenthesis. Note that some countries for more than one content., Ex: Russia belongs to both Europe and Asia (Source : [21]).

Continent	Only XSS	Only SQL	XSS and SQL	XSS or SQL	None
Africa (61)	14.75 (9)	0.00 (0)	34.43 (21)	49.18 (30)	50.82 (31)
Asia (55)	9.09 (5)	0.00 (0)	76.36 (42)	85.45 (47)	14.55 (8)
Europe (53)	7.55 (4)	0.00 (0)	83.02 (44)	90.57 (48)	9.43 (5)
North America (34)	20.59 (7)	2.94 (1)	52.94 (18)	76.47 (26)	23.53 (8)
Oceania (25)	24.00 (6)	0.00 (0)	28.00 (7)	52.00 (13)	48.00 (12)
South America (17)	17.65 (3)	0.00 (0)	52.94 (9)	70.59 (12)	29.41 (5)

The explosive rise in web application vulnerabilities between the year 1998 and 2008 (IBM, 2009) is given in Figure 1.

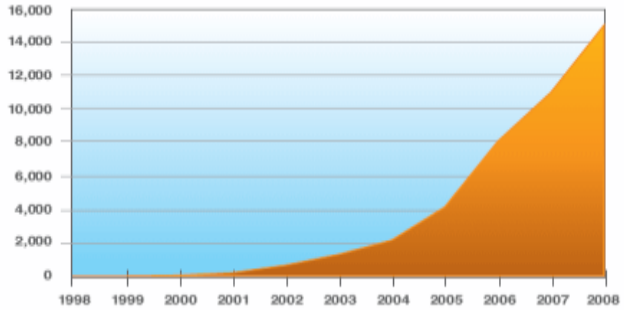

Figure 1: Cumulative count of Web application vulnerabilities (Source : [8])

About 80% of the internet sites as a minimum one severe vulnerability on the net [9] A survey identified that , more than 450 data breach investigations in 19 nations and found that an develop of 50% in the year 2012 as compared to the year 2011 [10]. A research shows that 86 percentage of websites have been noted that minimum one severe vulnerability attack day by day, on average, 61 percent resolved and only 18 percent of websites were vulnerable for fewer than 30 days, resolving these vulnerabilities took 193 days from the primary notification [11]. The analysis shows that ninety-eight% of applications have, at least one application security hazard, while average application registered 22.4 risks. A survey indicates that more than eighty% of the governments in the world are prone to normal net-application attacks of cross website Scripting and SQL injection. The Checkpoint (2013) finds that the government is the highest percentage (seventy %) in the data loss as compared to the other sectors, specifically, finance (sixty-one%) and Industries (fifty%). The web applications are staying vulnerable in the year 2014 as compared to the year 2013.The percent of websites with critical vulnerabilities increased by 6%s to 68% ([22]. A study by Veracode (2015) observed only that 27% of identified vulnerabilities get remedied in government departments, which is least amongst all industry sectors. In addition, in the government internet applications fail the top 10 Web Application Security Project [14]) when first assessed for risks. Many departments of the government use older programming languages that identified to produce extra vulnerability. Only sixty-one% perform a third party security audit before deploying their web based

applications. Moreover, spending money for web security audit increases in the year 2009 and it will increase in future by thirty-six%. Moreover, very few organizations have a special head of the account in their budget for the IT security [13]. This gives a motivation to this paper to provide an overview of the web application and top 10 OWASP vulnerabilities to the government departments to understand and to take precautionary measures pertaining to the design, development, and deployment of web applications.

2.1 Some government web application security standards

The standards in government departments are a high priority activity, which will help ensure sharing of information and seamless interoperability of data across various government departments. Many Governments are providing stands, checklist and guidelines for the security coding of web applications, some examples are given in Table 3.

Table 3: Web Application Security Standards in Some Governments

Country	Standards
1. Government of South Australia	Web Application Security Standard version 1.2, date 2014, available at http://digital.sa.gov.au/sites/default/files/content_files/policy/Web-Application-Security-Standards.pdf visited on 15.2.2016.
2. Government of British Columbia	Security standard for application and web development and deployment, Document Version 1.3,Published: April 2015, available at http://www2.gov.bc.ca/assets/gov/government/services-for-government-and-broader-public-sector/information-technology-services/standards-files/security_standard_application_web_development_deployment.pdf, visited on 15.Feb 2nd 2016.
3. Government of the Hong Kong Region	Web application security (2008) ,available at http://www.infosec.gov.hk/english/technical/files/web_app.pdf, visited on 15.02.2016
4. Government of India	Standards for e-governance applications ,available at https://egovstandards.gov.in. Indian Computer Emergency Readiness Team (CERT-In) available at www.cert-in.org.in , is a nodal agency that deals with cyber security threats and providing guidelines to the departments.
5. United States of America	In , USA, Computer Emergency Readiness Team (US-CERT) provides, technical publications, available at https://www.us-cert.gov/security-publications

3. WEB APPLICATION OVERVIEW

A study suggests that SQL Injection and cross-web site scripting are the most usual and most critical assaults (Tsai et al , 2009). These pages often contain scripting code to be executed dynamically within a web browser. Over the Internet, Web applications are accessed via a web browser [16]. A web application consists of a back-end (Database on a server) and front-end (Web pages at Client side), the users can interact web pages through a web browser such as Google Chrome. A web page may be static or dynamic. In a case of static web pages, there is no provision for filling and accepting information from the client through forms and store information in the database, but whereas in a dynamic website the user can fill online forms in order to store the information in the database. Many government departments have deployed web applications for citizen services, financial management, online tax filing etc. The web application overview and development life cycle are given in Figure 2 and 3.

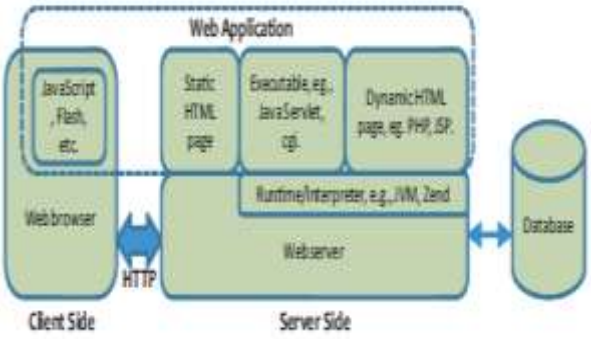

Figure 2: Web Application Overview (Source [22])

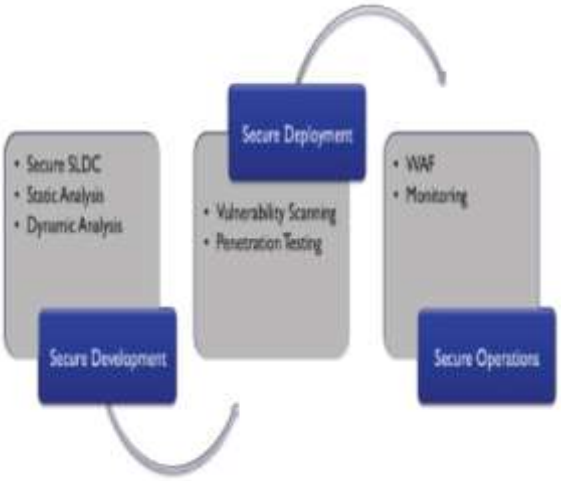

Figure 3: Web Application Development Cycle, (Source : [24])

3.1 WEB APPLICATION VULNERABILITIES

Web application attacks due to poor coding and testing before deployment of web applications on the production server or web server. It may steal information from the database like important citizen information, Income Tax , financial and etc. SQL injection vulnerabilities are very serious than XSS, because SQL injection can destroy the organization's database, so services may not available. In government, web applications SQL Injection and Cross-site Scripting are major attacks. A study found that Cross-site Scripting affects seventy-five% of government applications (seventy-five %) as compared to industry sectors. Moreover, forty% of government web applications of the government departments had SQL Injection issues as compared to thirty% for software related twenty-nine% for Finance (Veracode , 2015).A web application security is a central business issue and the biggest threat to government applications and database. Lack of awareness of any Web application security breaches can cause huge damages to the business. The Open Web Application Security Project(OWASP) has identified the ten most critical web application security threats [14]. The OWASP Top 10 referred to industry standards such as PCI-DSS, which sets forth security standards for payment card processing systems, for the purposes of this paper, a list of the Top 10 vulnerabilities given in Table 4. The OWASP Top 10 2013 web application vulnerabilities given in Table 4 for more information, readers can get more information from the website of OWASP [14].

Table 4 :OWASP Top 10 Web Application vulnerabilities

Type	Description
Injection	Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
Broken Authentication and Session Management	Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities.
Cross-Site Scripting (XSS)	XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.
Insecure Direct Object References	A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control, check or other protection, attackers can manipulate these references to access unauthorized data.
Security Misconfiguration	Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. Secure settings should be defined, implemented, and maintained, as defaults are often insecure. Additionally, software should be kept up to date.
Sensitive Data Exposure	Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data deserve extra protection such as encryption at rest or in transit, as well as special precautions when exchanged with the browser.
Missing Function Level Access Control	Most web applications verify function level access rights before making that functionality visible in the UI. However, applications need to perform the same access control checks on the server when each function is accessed. If requests are not verified, attackers will be able to forge requests in order to access functionality without proper authorization.
Cross-Site Request Forgery (CSRF)	A CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to

	force the victim's browser to generate requests the vulnerable application thinks are legitimate requests from the victim
Using Components with Known Vulnerabilities	Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications using components with known vulnerabilities may undermine application defenses and enable a range of possible attacks and impacts.
Un validated Redirects and Forwards	Web applications frequently redirect and forward users to other pages and websites, and use un trusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages

4 A CASE STUDY

Many government departments are increasingly using websites as a tool to share with the citizens. The World Wide Web (WWW) is widely used communication for implementation of e-governance services. Many numbers of websites belonging to different government departments have been available on the website to make sure maximum reach of government data and services to the citizens at various local, state and central government departments. As of today, there are over 5000 departments websites in India. The government developed Government website guidelines in an International Standards including ISO 23026, W3C's Web Content Information Technology Act, Accessibility Guidelines, Disability Act of India [18] , more information is available at http://web.guidelines.gov.in.The reason for security issues arises in the web applications , due to issues in design and development [18]). Thus, the Indian government developed website guidelines as a checklist, more information is available at the link http://web.guidelines.gov.in/compliance.php [18]. To prevent cyber threats the national cyber security policy 2013, introduced, during the Twelfth Five Year Plan, The salient features of national cyber security are available at http://www.pib.nic.in/newsite/erelease.aspx?relid=96971, visited on 09.10.2015 to read for more information.

4.1 Government website hosting procedure:

The Computer Emergency Response Team (CERT-In) have empanelled a number of agencies conduct the security audit of applications. Each web application must undergo a security audit from empanelled agencies and clear the same, prior to hosting their website or applications. The empanelled vendors for information security audit are available at the website of CERT-in namely www.cert-in.org.in. In order to host any website, whether it is static or dynamic it is necessary to check the vulnerabilities by the security auditor and obtain a security clearance certificate. Based on the security clearance certificate, the website or application will be hosted on the production server, so that these applications are safe and secure. This procedure will be adopted as and when a new application needs to upload to the web server and it is mandatory for all the departments.

4.2 Procedure adapted to remove vulnerabilities in the web applications :Since

the government departments do not have certified , trained or skilled manpower related to Information Security , the CERT-in is assisting the government departments by empanelled some private organizations , who is having the skilled and certified manpower in this area and putting their list on the cert-in.org.in website . The government departments needed to select one organization from the list of empanelled vendors, the selected vendor will find vulnerabilities in the web applications. In this way, the government departments in India are identifying the vendor to find and remove vulnerabilities in the applications.

4.3 Government applications standards : In

India, standards for e-governance applications are available, for more information can get from the link https://egovstandards.gov.in.The e-governance standards to offer a platform for sharing of ideas, knowledge, and draft documents among the members of various committees involved in standards formulation process. The Information Technology Act, 2000 provides a legal framework to address the issues connected with cyber attacks [23].

4.4 Computer Emergency Response Team (CERT-In) :The CERT-In, a technical and a cyber

security department under the Ministry of Communications and Information Technology, the government of India, is a nodal agency to analyze and respond to cyber attacks and intrusions into country's information and technology networks. The CERT-In has initiated a probe into complaints of I-T department, banks and other financial bodies who have reported a spurt in cyber attacks and fake e-mails which were affecting their operations. [19]. The vulnerability can report to CER-IN by e-mail at info@cert-in.org.in, through a prescribed form, which is available at http://www.cert-in.org.in/PDF/Vul_Report.pdf.The CERT-In reported that

308, 371 and 78 government websites during the years 2011, 2012 and 2013 respectively [20].The CERT-in is attending into complaints those who reported cyber attacks and fake e-mails which were affecting their operations. The defacement statistics during the year 2015 are given in Figure 4 , it shows 18403 defacements found in the .in domain followed by 4665 in .com, 2326 in .org 657 in others and 203 defacements in the .net domain. There is more defacement in the .in domain as compared to other domains. The status of defacements is given, domain–wise and month-wise at Figure 4 and 5 respectively.

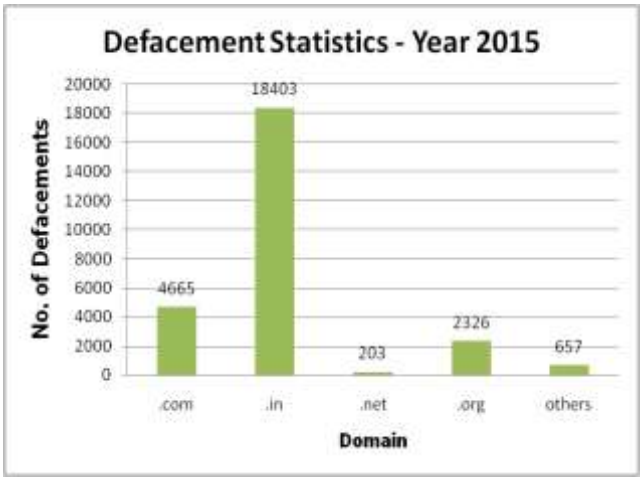

Figure 4. The Defacement statistics in the year 2015 (Source, CERT-in, 2015)

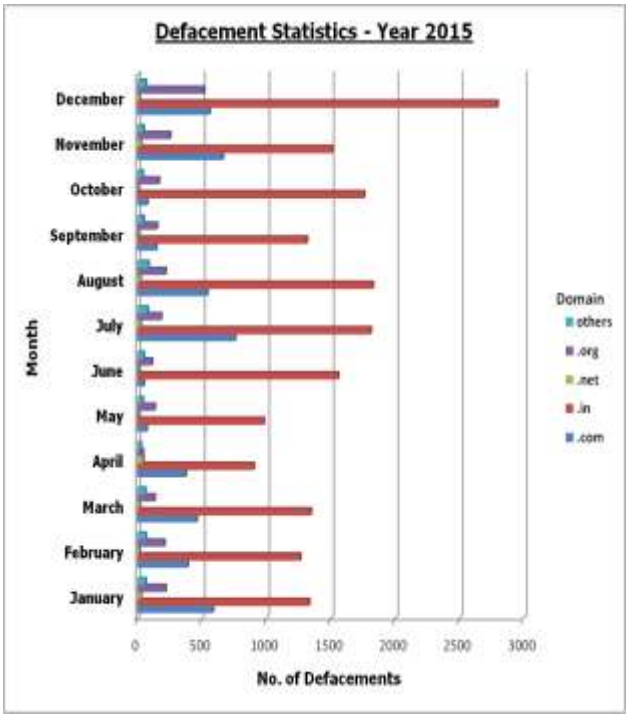

Figure 5: The defacement statistics from January to December ‘2015 (Source, CERT-in, 2015).

4.4.1 ANALYSIS OF DEFACEMENTS

It was observed the Figure 4, it shows that that number of defacements are more in the case of the .in domain and followed by the other domains namely .com, .org, and others. The least number of defacements found in .net as compared to other domains., from the Figure 5, It was observed that the number of defacements is more in .in domain in the month of December and followed by .com in the month of July 2015.

5 ISSUES AND CHALLENGES

Web applications, especially dynamic applications are more complex as compared to traditional applications. In particular, it is very challenging to the government as they do have neither certified nor trained staff in developing and testing the web application security area, even though it is essential. The challenge to the government is how to implement technology to strengthen confidence in privacy measures by creating mutual transparency between public administration and citizens pertaining to India This section discussed on various issues and challenges related to web application security. Some of the issues are:

5.1 Coding issues: The majority of web applications relates to coding issues. Many developers do not know how to develop secure applications and even they do not about various types of vulnerabilities mentioned in Table 4 and how to tackle with them. Moreover, due to lack of knowledge and/or urgency in the deployment of applications, the developers are not taking care of secured applications. As a result, without following security aspects they develop applications and finally these applications will be under the scanner. Therefore while developing web applications, the developers should take care of various vulnerabilities and threats, which may affect citizens’ data.

5.2 Manpower issues: Most of the government departments, employees do not have the technical manpower related to the information security audit such as Certified Web Application Security Professional (CWASP) ,Certified Information Systems Security Professional (CISSP),Certified Information Systems Auditor (CISA), Certified Ethical Hacker(CEH) and etc. According to the ISC² (2014), reports only 92274 members hold the CISSP certification worldwide, in 153 countries, in India, they are 1,562 (Source: https://www.isc2.org/cissp/default.aspx). Due to lack of certified manpower in the government, it has to depend on the third party or private organization. They check the application and provide a certificate as per the government norms stating that it is clear from a security point of view and then the application can be hosted. As and when changes in the application in the dynamic content, they have to conduct security audit again. It is very difficult for the government organization to conduct security audit by the private vendor as and when required. Therefore the government department should provide training to their employees, including administrative staff from time to time so that the security audit

can be done for their website without depending on the private organization. So the employees those who involved in the development must understand how web servers and browsers communicate and interact, and the protocols used in Internet communications, the more likely they are to build applications that are not vulnerable to attacks. If government employees are well trained in deployment of secured web based applications , then dependency on the private organizations will reduce tremendously, accordingly, the government can save their budget.

5.3 Funding issues: According to Gartner(2015) , Information Technology (IT) spending by various industries across the world is forecast to total $2.69 trillion in the year 2015, a 3.5 percent decrease from the year 2014.The worldwide IT budget spending Forecast by the Governments (Millions of U.S $) is given Table 5.

Table 5. : IT budget spending forecast by the Government Worldwide (Millions of U.S. Dollars) (Source [26]).

Year-2014		Year-2015	
Spending	Growth (%)	Spending	Growth (%
447,114	-1.2	424,660	-5.0

In order to provide secure services online to the citizens and employees, necessary funds should be allocated to the IT related projects to support for design, development, deployment and maintenance of secured web-based applications.

6 RECOMMENDATIONS

The government should give training to the government officials from time to time on design, development, and deployment of secured web applications. The training provided to the employees for various certifications such as CISA, and CISSP, which are useful to the employees and departments. At the graduate level, particularly in Information Technology area, the Web application security subject introduced as a compulsory subject with real-time applications. The government departments should check 1)

What type of web applications in the public domain and for what purposes? 2) What will be the damage to our applications, if attacks happen? Why our website targeted? , Who will rectify, in case of any issue and how much time required to rectifying and restoring applications on the web server? Whether updating security tools from time to time? Do we have a team of security experts to work on a 24x7 basis to resolve security issues? Do we have the necessary budget for Information Security? If the government departments can answer these questions, then they can offer security services to the citizens of the public domain on 24x7basis in secured way.

7 CONCLUSIONS

Many government departments are providing their services online and collecting information from the citizens. Citizens expect the government services are safe and secure. Therefore the web applications have more significance due to the vast amount of sensitive intelligence and confidential information about citizens. This paper discusses importance of training by the government employees, including administrators to develop and deploy secure applications to improve the overall security of the Web. This paper examines the acts, rules, guidelines, and standards adopted by the government departments for design, development & deployment of a secure web application as a case of the Indian government. This study shows that, the majority of government departments is developing and audited web applications before hosting on the public domain. But, for this most departments have to depend on the private organization (s). This problem arises in the government departments, due to of lack of certified or educated staff. Thus the government departments ought to train their staff along with administrators in information security from time to time. This will ensure making improvements to internal protection and reduce the dependency on private organization tremendously.

8 REFERENCES

[1] Lebech (2003), A. Privacy and e-government. Enterprise challenges for the Danish government. Tech. rep., IBM Privacy Technology Summit.
[2] UN,. (2012). United Nations E-Government Survey 2012, available at http://unpan1.un.org/intradoc/groups/public/documents/un/unpan048065.pdf, visited on 12.7.2015.
[3] Backus, M., (2001) "E-governance in Developing Countries", International Institute of Communication & Development (IICD), Research Brief No. 1, March, 2001, available at http://www.ftpiicd.org/files/research/reports/report3.pdf.
[4] W3C (2009) .,Improving Access to Government through Better Use of the Web,W3C Interest Group Note 12 May 2009, available at http://www.w3.org/TR/egov-improving/.
[5] Jan van Dijk, Willem Pieterson1, Alexander van Deuren1, and Wolfgang Ebbers2 (2007), E-Services for Citizens: The Dutch Usage Case, Available at http://alexandervandeursen.nl/Joomla/Articles/Journal/2007%20-%20eservices.pdf.
[6] James. G. (2000). Empowering bureaucrats MC technology marketing intelligence 20(12), 62-68 .
[7] Thibodeau, P. (2000).. E-government spending to soar through 2005, computer world, 34(17).12.
[8] IBM (2009). Cumulative count of Web application vulnerabilities, published by IBM x-force in January 2009, available at http://www.redbooks.ibm.com/redpapers/pdfs/redp4530.pdf, visited on 02.05.2015.
[9] WhiteHat Security (2010).WhiteHat website security statistic report 2010
[10] Trustwave (2013). Available at , http://www2.trustwave.com/rs/trustwave/images/2013-Global-Security-Report.pdf, visited on 12.3.2016.
[11] WhiteHat Security (2013) . WhiteHat Security Website Security Statistics Report.

[12] Checkpoint (2013): Check Point 2013 Security Report, available at http://sc1.checkpoint.com/documents/security-report/files/assets/common/downloads/publication.pdf, visited on 02.03.2015.
[13] OWASP(2009). OWASP Security Spending Benchmarks Project Report March 2009,
[14] OWASP(2016) OWASP TOP 10 vulnerabilities available at https://www.owasp.org/index.php/Top_10_2013-Top_10, visited on 10.1.2016
[15] Tsai, D.R A. Y. Chang, P. C. Liu and H.-C. Chen (2009), "Optimum Tuning of Defense Settings for Common on the Web Applications," 43rd Annual 2009 International Carnahan Conference on Security Technology, Zurich, 5-8 October 2009, pp. 89-94.
[16] Rittinghouse JW, Ransome JF (2009). Security in the Cloud. In: Cloud Computing. Implementation, Management, and Security, CRC Press. 21 Subashini S, Kavitha V (2011) A survey on Security issues in service delivery models of Cloud Computing. J Netw Comput Appl 34(1):1-11.
[17] Veracode (2015).VERACODE State of Software Security Report, Volume 6: Focus on Industry Verticals, https://www.veracode.com/sites/default/files/Resources/Reports/state-software-security-report-june-2015-report.pdf.
[18] GGW (2009). Guidelines for Government websites available: http://darpg.gov.in/sites/default/files/Guidelines_for_Government_websites.pdf
[19] Economic times (2010). Available at http://articles.economictimes.indiatimes.com/2010-03-15/news/27601159_1_cyber-attacks-certphishing-attacks, visited on 10.2.2015.
[20] Rocci Luppicini (2014). Evolving Issues Surrounding Techniques and Society in the Digital Age, Page 181, ISBN: 978-1466661226,IGI Global book series. Moen Vebjørn , André N. Klingsheim, Kent Inge Fagerland Simonsen, and Kjell Jørgen Hole (2007). "Vulnerabilities in e-governments". International Journal of Electronic Security and Digital Forensics, vol. 1, issue 1, pages 89-100. Available at http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.80.6454&rep=rep1&type=pdf,, visited on 06.03.2015.
[21] PT (2014).Positive Technologies, Web application vulnerability statistics 2014, available at https://www.ptsecurity.com/upload/ptcom/WEB_APP_VULNERABILITY_2014.A4.ENG.242465.14.OCT.2015.pdf , visited on 15.12.2015.
[22] Xiaowei Li and Yuan Xue (2011). A Survey on Web Application Security, Available at http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.434.7174&rep=rep1&type=pdf, visited on 01.02.2016.
[23] Indian Express (2013). (78 government websites under hacking attacks till June PTI: New Delhi, Wed Aug 07 2013, 18:16 hrs, http://www.indianexpress.com/news/78-government-websites-under-hacking-attacks-till-june/1152440/).
[24] Securosis (2009). Building a Web Application Security Program, Available at https://securosis.com/assets/library/reports/WebAppSec_Programv1.pdf, visited as on 10.4.2016.
[25] CERT-In (2015).Computer Emergency Response Team of India, Available at www.cert-in.org.in, visited on 02.01.2016.
[26] Gartner(2015).Gartner Says Worldwide IT Spending Across Vertical Industries to Decline 3.5 Percent in 2015, Available at http://www.gartner.com/newsroom/id/3135718 , visited on 01.02.2016

Velamala Ranga Rao obtained his Ph.D. in Statistics (1994) from Andhra University, Visakhapatnam,India and M.Tech in Information Technology (2011) from Karnataka State Open University, Mysore, India. Currently, he is working as a Senior System Analyst at Soil and Land Use Survey of India, Department of Agriculture, Cooperation and Farmers Welfare, Ministry of Agriculture and Farmers Welfare , Government of India, Delhi. His research papers have appeared in International Journals, Book reviews, and International Conference Proceedings. He is having more than 24 years of experience in the field of Information Technology in the government Sector. His primary research interests focus on applications of ICT and manpower planning in the government sector.