I. J. Computer Network and Information Security, 2013, 3, 56-62
Published Online March 2013 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2013.03.07

Vulnerabilities in Academic E-governance Portals

Subhash Chander
Govt. P.G. College,Sec-14, Karnal (Haryana), India
subhashjaglan@gmail.com

Ashwani Kush
University College, Kurukshatra University , Kurukshetra (Haryana), India
akush20@gmail.com

Abstract — Internet has become one of the most versatile sources of information and on the other way it has become source of various security threats. Various existing vulnerabilities in the web portals are compromised easily by hackers sitting at their places. There are so many vulnerabilities available in various websites in case of government sectors may be because of financial constraints or other. E-government is a new fast growing area in developing as well as in developed countries. New e-governance applications are emerging and being implemented and utilized by the common man. Providing government information and services on the web has resulted in mushrooming of websites with very little attention is paid to security issues of these websites. This paper discusses certain security issues & vulnerabilities in websites of educational institutes. The organizations taken into consideration are educational institutes of Haryana.

Index Terms — E-governance, security, ICT, E-government, website, vulnerability

I. INTRODUCTION

E-government is an evolving area and most research in this field has been done in formulating challenges and barriers, implementation plan, evaluation/assessment and success factors of e-government while studies on knowledge management in e-government, readiness for e-government, e-Gov. process and security/privacy issues could get only limited attention [1].Quality in education sector is very important for development in any country. Education sector is the basic building block for so many other sectors which are necessary for becoming a developed nation. In India not much attention is given to this sector and it is also considered as non productive sector for various stakeholders including bureaucrats and politicians. Education sector may not be giving direct benefits but indirectly this sector is the beneficial for the democratic society. Keeping in view such benefits Right to Education Act has implemented in India so that poor man can also send their children to schools and get free education. Also certain welfare schemes for the students have been implemented by various state governments in India. For enhancing certain ICT skills among college students various state governments have started giving them Computers and other ICT related gadgets so that students may take keen interest in the technology and, may take full benefits of this technology in the future. Invention of the most economical tablets like Ubislate in India has confirmed this thinking. India is having a billion plus population and varied demography has excellent window of opportunity in this new economy. Our educational system needs to be substantially upgraded to impart globally competitive training if we have to make use of this opportunity. There is an urgent need to attract best of the students to teaching careers with reasonable opportunities, nurturing and a better option [2]. In case of Governance, corruption is in all walks of life in India. India was ranked at 85th place out of 179 countries in transparency international Corruption Perception Index. This index also stated that corruption in Indian politics and bureaucracy has taken toll on the overall development of the country. Latest survey by political and economic risk consultancy on the bureaucracy in Asia shows that respondents are impressed with the quality and efficiency of civil service in Singapore and they are least impressed with Indian bureaucracy [3]. Also present movements by civil society confirm this fact. Citizens concern about inadequate and inefficient services at unbearable costs is transforming into anger and frustration. Now the time has come to frame super counters [4] available online and eliminate the endless maze citizens have to negotiate in going from door to door, floor to floor to get services.. Also time for services has to be cut from months and weeks to days and hours. ICT in education and e-governance applications will surely help in diminishing these problems. Secured websites will certainly help in transferring the basic information and services without any direct involvement of the bureaucratic procedures. At education level websites need to be developed and admissions forms may also be filled online. Out of these at the time of admission only selected candidates may get roll numbers and that information may be utilized by

college authorities for various purposes. Purposes may be sending university registration return and making bus pass etc. All such information is to be sent to various authorities in the digital format. Various Universities require registration return of the new students in the computer readable format. Also transport authorities have started to make bus passes through an online system. Hence the database created at the time of admissions may be utilized for this purpose by universities and transport departments for their respective purposes. But once database is involved on a website chance of breach of security of the website is increased. Database involving websites mostly suffer from the SQL injection attacks. In this attack certain queries are sent to legitimate users to take fruitful information from the database of the website of portal. Various issues related with website and web portal are broken links, accessibility, obsolete contents, nonavailability of sitemap, search function etc. But here stress is given on security of these websites and portals which are of great matter of concern these days in India. Due to certain Information Technology (IT) related flaws in the system various offensive morphed images and videos have been uploaded on social networking sites to disturb peace and harmony in the country. In this regard certain social networking sites have refused to cooperate and India had to share information with US because most of the social networking sites web servers and head offices are there in US. It has also been found that Proxy servers and Virtual Private Network (VPN) service that hides the identity of the users operating from various countries has been used for uploading such hate & low level content. Such instances force one to think about the security issues of the websites. Hackers after having control over the website may deface and change the content as he likes. Hence security of web portals is major burning issue now days. The information available in student database may be needed by various entities directly or indirectly. The organizations directly in need of student database are shown in fig.1 below. Indirectly students' database may be required by various placement & counseling agencies to visit the campus and welfare department to select students for various welfare schemes like scholarship.

Section 2 gives description about the websites chosen, section 3 gives description about various tools for scanning of vulnerability in various websites, section 4 gives experimental results and section 5 gives conclusion of the paper.

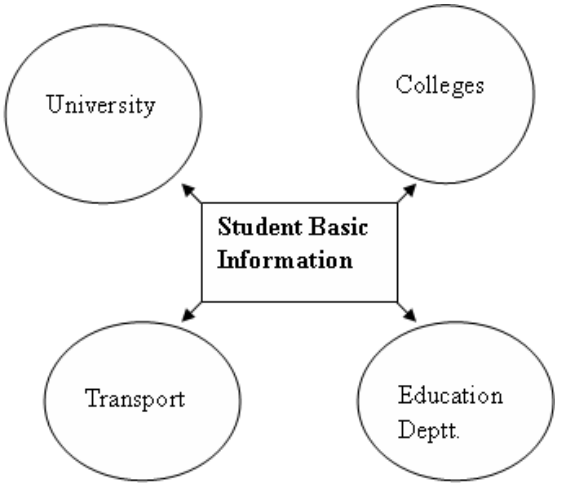

Figure.1. Direct need of student database

1.1 Information gathering for Vulnerability analysis

The number of vulnerable targets within the network (communication protocols, operating systems, servers, databases, etc.) has increased a lot. Hackers want to know more and more system internal details. After identifying the services and infrastructure of the target system hackers can proceed to the next step of exploiting the services. Services can be exploited by identifying known and unknown vulnerability in the target systems. Hackers can also exploit errors in the system configuration or other components of the system [5]. Less expensive devices if used in any transaction system will be more vulnerable as compared to costly devices because of lack of certain features. Whereas costly devices may have highly typical security features that may be easy for the intruders to turn off useful features and device may start giving wrong results. A sophisticated intruder may modify the device so that it maliciously manipulates management activities, deliberately providing inaccurate or misleading information to network administrators [6]. Hackers' first check connected devices and trace route of the target before going further to attack on particular site or portal. A number of tools are available in market to get information about devices that are connected to the network. These tools are based on two approaches for gathering information. If this information is available to management or service queries it may prove invaluable in network vulnerability analysis. Firewalls, security gateways (VPNs), web proxies and other application servers often acquire and store information about network neighbors [6]. A patch enhances the security of the software, to mitigate eventual threats. But this strategy is also not successful to control threats and vulnerabilities. Figure 2 shows that more intrusions take place after a patch have been released, than before [7]. This shows that patches are not installed even when vulnerability clearly exists. Most of users are unaware of the situation, and also do not apply the patch even if it available.

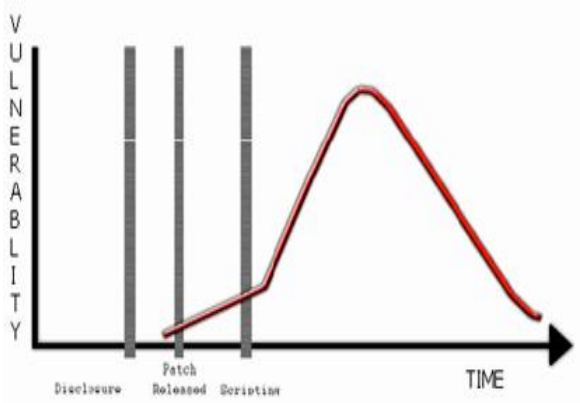

Figure.2. Intrusion after & before patch release; Source [1]

II CHOICE OF PORTALS

In this age of digitization education sector has also changed a lot. The new technology and gadgets available help us not only enrich and enhance our existing education system but also offer new opportunities and modes which can take the process of learning beyond institutions and allow people to learn on their own time and own terms [8]. This new technological environment has forced us to think how to tap this technological potential. Choice of the portals for vulnerability scanning is an important issue. Delivery of services through Internet and websites has increased lot in the last decade. A new kind of administration namely Virtual administration is taking place in the society. A large number of government websites have been set up in India over the last few years to deliver a wide variety of information and services to its citizens. The concepts of quality and security for a website need to be quantified in some way to avoid subjective interpretations [9]. Delivery of services through Internet and websites has increased lot in the last decade. Websites are collection of WebPages and portals are collection of websites. Portals cover a wider range of functions, and they can be designed to cater for specific demands of their users. Major aim of portals is to provide information about services. It provides the complete details about performing a particular function. For citizen service related matters it has all details about physical location of the office if user wants to visit, he may download forms [10] available online and most importantly the portal may have varied types of services for the convenience of the citizens. Moreover such portals provide variety of services at a single place and users need not to visit many offices to complete a particular job. That is why many of the times such portals are named as one stop portals. Portals of educational Institutes must have sufficient information and download facility so that fewer people prefer to visit physically these offices. Some of the information may be like courses offered, number of seats course wise, institution affiliated to, details of faculty member subject wise so that neither parents nor students feel cheated after getting their admissions in educational institutes. As compared to banking and e-government portals educational websites have less important information. The information contained in educational portals may have students and teachers databases, infrastructure, courses and such type of other details. This type of whole information is not as fruitful as it can be any banking or e-government website. For a hacker banking and e-government information is more fruitful as compared to educational websites information. But for a common man information is just information and it has great value for the organization and the user itself. Hence for the sake of information to the stakeholders four educational institutes' websites have been taken. The results obtained will certainly help in the improving the websites from security point of view. Security of networks is one of the important problems of modern information technology. The importance of security of networks is confirmed by permanently increasing significance of information itself, growing size and interconnectivity of networks, number of users and by potentially devastating consequences of successful attacks on integrity, confidentiality and availability of network recourses. Unauthorized access to facilities and network resources, especially in global networks (such as Internet) participating in real-time control operations, may be really disastrous [5]. The following websites have been tested for vulnerability through Acuentix Web Vulnerability Software (WVS). Haryana state was formed on 1 November 1966, on the recommendation of the Parliamentary Committee. The state is divided into four divisions for administrative purpose - Ambala , Rohtak, Gurgaon and Hisar Division. There are 21 districts, 47 sub-divisions, 67 tehsils, 45 sub-tehsils and 116 blocks in Haryana. Haryana is the state in India that surrounds the national capital from three sides and its own capital as Union territory Chandigarh. Its area is 44212Km^2 and population is 25,353,081 as per 2011 census. Literacy rate in Haryana is 76.64 and sex ratio is 877. Haryana Government has its own state-wide area network by which all government offices of all districts and blocks across the state are connected with each other thus making it the first SWAN of the country [11]. As per latest report of University Grants Commission (UGC), Haryana has scored high on setting up of educational institutes and enrolment of students as compared to its neighboring states like Punjab, Himachal Pradesh, Uttrakhand, Chhatisgarh, Jharkhand and Jammu Kashmir. State boasts of having 22 Universities and 902 colleges [12]. All these institutions are providing higher education in various streams in Haryana. All these colleges taken in consideration are degree colleges offering various undergraduate and post graduate courses.

(1) S D College, Ambala Cantt (SDC)
(2) DAV P.G College, Karnal (DAVC)
(3) Guru Nanak Khalsa College, Karnal (GNKC)
(4) University College, Kurukshetra (UCK)

Snapshots of various chosen sites are shown in figures 3 to 7.

Figure 3: Hoe Page of SDC; Source [13]

SDC was established in 1916 at Lahore (now in Pakistan) by Mahamana Pt. Madan Mohan Malviya Ji,Pt. Rishi Ram Ji and Maharaja of Darbanga . It was re-established at Ambala Cantt in 1948 by untiring efforts of Tyagmurti Goswami Ganesh Dutt Ji, Dewan Ragunath Sahai Ji and Pt. Rishi Ram Ji. With over 2800 students on its rolls, the college today is a premier, multi-faculty, co-educational institute of higher education in Northern India. College has good infrastructure and has been awarded the Status of 'College with Potential for Excellence' by University Grants Commission, New Dehli. IT has also been accredited with A grade by NAAC [13].

Figure 4: Home page of DAVC; Source [14]

DAVC was established in 1974 to cater the needs of underprivileged sections of society like rural, semi urban & urban areas. Now it has grown into a premier Institution of quality education, having good infrastructure. In the beginning there were nearly 272 students and only two faculties, Arts and commerce. But now the college has 1900 students on its rolls with multi-disciplinary faculties [14].

Figure 5: Home page of GNKC; Source [15]

GNKC was established in 1969 to commemorate the birth quine-centenary of Guru Nanak Dev Ji,, a great philosopher and social reformer. It was intended to be a great centre of ideal education in the true spirit of our ancient cultural heritage. Since its inception the institute has been deeply committed to the propagation of nationalism, patriotism and secularism. Besides traditional courses, the college has been running successfully various Job - oriented courses like B.Com with Computer Application and several post graduate courses. It has good infrastructure and accredited as B+ grade by NAAC [15].

Figure 6: Home page of UCK; Source [16]

UCK is a co-educational institute offering courses upto undergraduate & postgraduate levels. It enjoys the singular distinction of being a college maintained by Kurukshetra University, Kurukshetra, which is well-reputed at the national level in general and in North India in particular. College has good infrastructure including library with a vast collection of books and journals with internet facility to the users. It maintains its unstinted records of being a holy place for the acquisition of

knowledge for those who pursue perfection and excellence. It has lush green lawns and is situated in campus of Kurukshetra University that is accredited as 'A' grade by NAAC [16].

III. TOOLS FOR VULNERABILITY SCANNING

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 [11]. Although the two terms namely Vulnerability assessment and penetration testing are normally used in the same situation yet there is a lot of difference between the two terms. There are various tools available for the vulnerability scanning of websites and portals. Out of these one is namely Acuentix WVS and used for the purpose. It (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 [17]. Acunetix WVS scans any website or web application that is accessible via a web browser. Acunetix Web Vulnerability Scanner is used for website security scanning that checks for SQL injection, Cross site scripting and other vulnerabilities. This scanner checks password strength on authentication pages and automatically audits shopping carts, forms, dynamic content and other web applications. Websites taken in consideration are educational institute websites. SQL Injection is hacking mechanism used by hackers to steal data from organizations. With the help of SQL injection the data from the backend database may be stolen easily and websites may be compromised. In Such attacks, when legitimate user enters username and password to enter secure area, SQL query is generated from these details and submitted to the database for verification and on verification user is granted appropriate access.

IV. EXPERIMENTAL RESULTS

Acuentix web Vulnerability Scanner was used for checking the vulnerabilities on the above mentioned websites. After completion of the scan a detailed report is provided and this report pinpoints existing vulnerabilities in these websites. Various vulnerabilities reports are shown in figures 7 to 10.

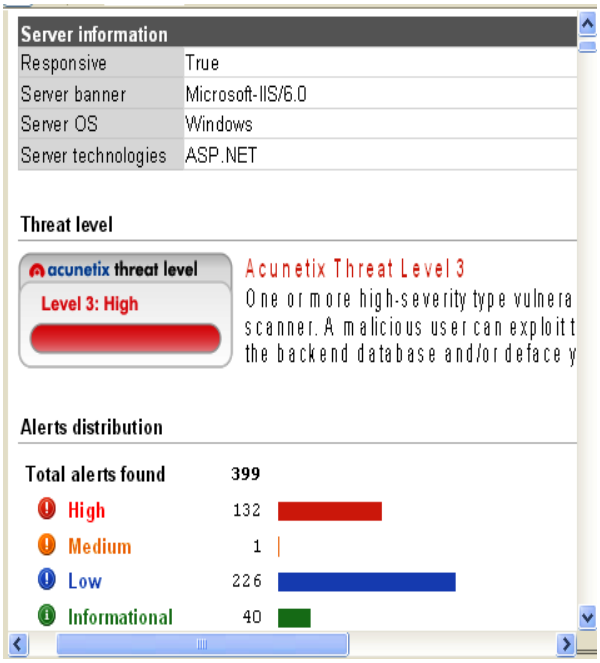

Figure 7: Vulnerability Report of SDC

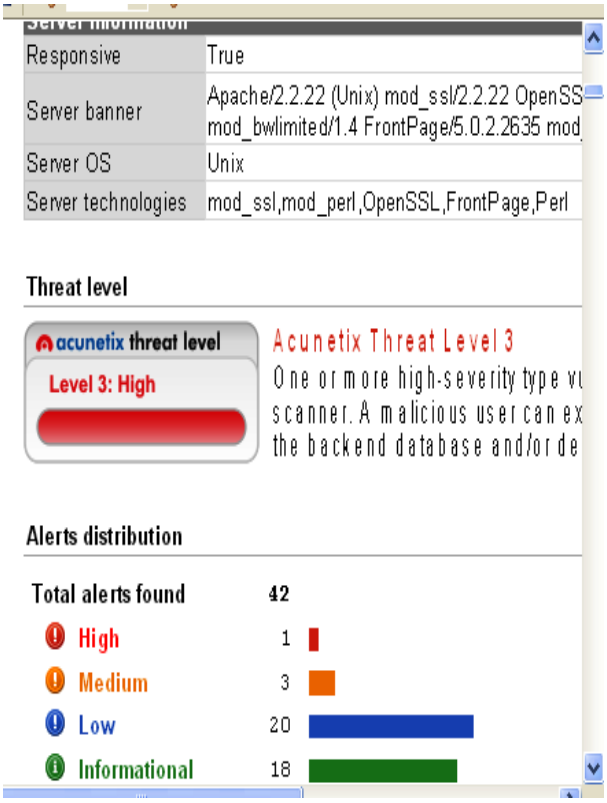

Figure 8: Vulnerability Report of DAVC

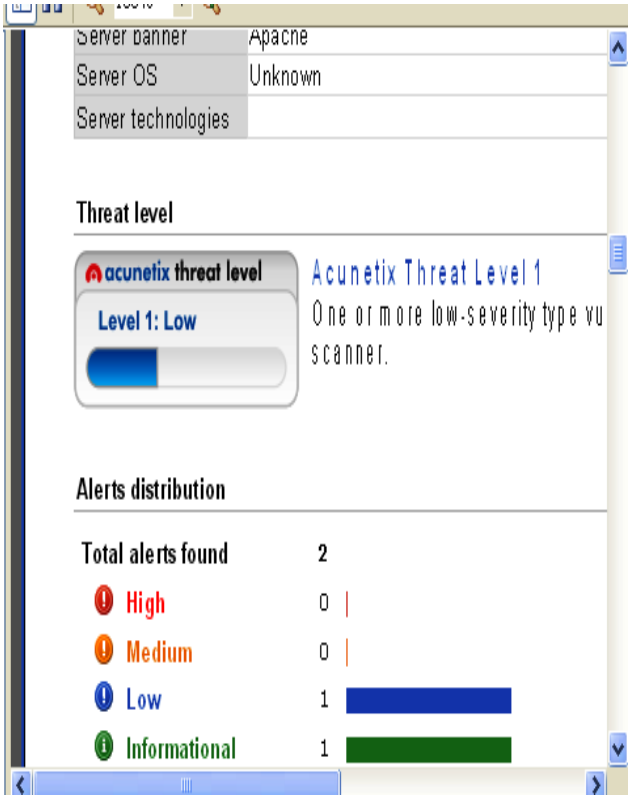

Figure 9: Vulnerability Report of GNKC

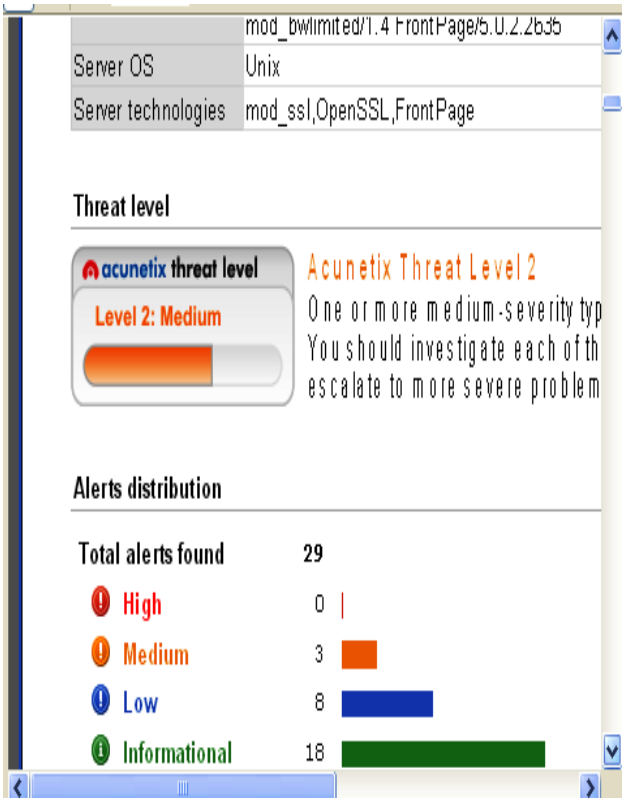

Figure 10: Home page of UCK

The above results were generated on 19th and 20th of August 2012 on Pentium IV machine, 256 MB RAM and Windows XP as Operating system. Results related with scan time may differ from machine to machine depending on its configuration. Table 1 shows the threat alerts distribution of all these portals.

Table 1: Threat alert levels

Organization Name	High	Medium	Low	Informational	Total Alerts
SDC	132	1	226	40	399
DAVC	1	3	20	18	42
GNKC	0	0	1	1	2
UCK	0	3	8	18	29

This table shows that SDC is most vulnerable website out of all the considered websites. In this High level threats are more that shows that it is highly vulnerable and hackers may exploit the available vulnerabilities. Out of all 132 high level threats on this portal 131 are under the category of SQL injection and single threat is DNS zone transfer. SQL injection is a vulnerability that allows an attacker to change backend SQL statements by manipulating the user input. SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters [4]. This is one of the most common application layer attacks currently being used on the Internet. The remote DNS server allows zone transfers. Alone, DNS records are not sensitive, but if a malicious entity obtains a copy of the entire DNS zone for a domain, that may have a complete listing of all hosts in that domain. That makes the job of a computer hacker much easier and it affects server and sensitive information may be disclosed with the help of such threats. Thirty email addresses were found on the portal. But email addresses are the informational type of threats but email addresses present on the website may invite spam. DAVC is again having one high level alert that is related with DNS zone transfer and three medium level alerts are based on the mod_ssl. Majority of the threats are of low level and informational type on this portal and portal is also more vulnerable than GNKC and UCK. GNKC is the most secured web portal and is having only two threats. UCK is having the total 29 threats including three of medium level. All here medium level threats are based on the mod_ ssl. Such mod_ssl related threats may invite the Denial Of Service (DOS) attack, may allow the attacker to execute the arbitrary code on the affected computer and may allow an attacker to gain root access.

V. CONCLUSION

As lot of money is invested to design, develop, host and manage websites by various government and private organizations.. Various threat levels are also shown. Among these, level 1 shows low threat level, level 2 shows medium threat level whereas level 3 shows high threat level. High threat level means website can be easily compromised by hackers and stakeholders must

necessary steps to mitigate the risks involved in breach of security of the website. The detailed summary of complete scanning is given in Table 2.

Table 2: Summary of scanning results

Attributes	SDC	DAVC	GNKC	UCK
Scan Time (in Minutes)	78	55	129	26
Threat Level 1(low),2(medium), 3(high)	3	3	1	2
Total Threats(high, med, low and informational)	399	42	2	29
Report Size (number of pages)	179	29	5	22

Looking at the report it is clear that majority of the security alerts are available in SDC and DAVC websites. These websites are also having high level of threats. Whereas GNKC is having very less threats but information available on this site is also very less as compared to other sites and time taken in scanning this website is much more than other sites. Overall this site seems to be much secure as compared to other sites. Hence stakeholders of the websites must also remove these existing vulnerabilities so that these may not be utilized by the hackers for penetration into these websites and deface these websites.

REFERENCES

[1] Mishra Alok, Mishra Deepti ," E-Government – Exploring the Different Dimensions Of Challenges, Implementation, and Success Factors", The DATA BASE for Advances in Information Systems, Pp 23-37, Volume 42, Number 4, November 2011, ACM publication

[2] Ramamurthy V S," Faculty Deficit in Higher education", Pp 32-33, Volume 7 issue 7, digital Learning, Asia's First Monthly Magazine on ICT in Education, July(2011), ISSN 0973-4139

[3] Budki Sandeep," Indian Bureaucarcy rated worst in Asia", Pp 10-13, Volume 5 Issue 7, e-gov, Asia's First Monthly Magazine on E-Government, July (2009), ISSN 0973-161x.

[4] Kapur Jagdish C," Process reforms and e-governance" , Pp 14-20, chapter 2, Enablers of Change: Selected e-governance Initiatives in India, IUP publication (2010), ISBN : 978-810314-2702-6

[5] Kotenko Igor," Active Vulnerability Assessment of Computer Networks by Simulation of Complex Remote Attacks", Proceedings of the 2003 International Conference on Computer Networks and Mobile Computing (ICCNMC), IEEE computer Society , 2003

[6] Henning Ronda R.,"Vulnerability Assessment in Wireless Networks", Harris Corporation

[7] Boldt Martin, Carlsson Bengt and Martinsson Roy ," Software Vulnerability Assessment :Version Extraction and Verification" International Conference on Software Engineering Advances(ICSEA), IEEE computer society, 2007.

[8] Chopra Nidhi, Lal Manohar," Research methodology for Educational Data mining in India",Pp325-328, proceedings of the 6th National Conference ; INDIACom-2012, Computing for nation development, BVICAM, New Delhi, February, 2012

[9] Sarnot S.L., Nandwani U.K. and Sondhi R.P., "Website Quality – A Prerequisite to Addressing Citizen Expectations in e-governance ", ICEGOV2008, Pp 469-470, ACM Publication, Cairo, Egypt (2008)

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

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

[12] Sharma Dinesh," Haryana Scores high on student enrolement, colleges and Unoversities", Pp 4 ,Vol. 132 No. 231, Haryana edition , The Tribune national daily, August 22, 2012

[13] Available at www. sdcollegeambala.org

[14] Available at www.davcollegekarnal.com

[15] Available at www.gnkckarnal.com

[16] Available at www.uckkr.org

[17] Available at www.acunetix.com

Subhash Chander: has been working as Assistant Professor in Govt. P.G. College, Karnal Haryana (India). He is a member of Computer Society of India (CSI) and Internet Society (ISOC). He has been a resource person for the Edusat Programme of Haryana Govt. for college students since its inception. He has published more than thirty papers in various Journals and National and International Conferences. The author's major fields of study include ICT, e-governance and security. Author can be contacted at subhashjaglan@gmail.com

Dr. Kush: has been working as Associate Professor in Computer Science Department of University College, Kurukshetra University, Kurukshetra, Haryana (India). He is member of CSI, IEEE, IAENG, IJCSA. He has published more than 110 papers in various Journals and Conferences in India and abroad. His major fields of study include Mobile Adhoc Network (MANet), Security, e-governance. Author can be contacted at akush20@gmail.com