Comparative Analysis Of WCAG 2.0 And WCAG 2.1 Based On The Accessibility Evaluation Of Pakistan's Educational And Government Websites

Muhammad Asif, Dr. Muhammad Sohail Khan, Faisal Abrar

Abstract: Website vulnerabilities are a major cause of security breaches in critical websites i.e. Government & Educational websites. Web Content Accessibility Guidelines (WCAG) provides a way to assess the level of vulnerability of a website in terms of various accessibility issues left un-noticed by website designers and developers. WCAG 2.1 is the latest version of accessibility guidelines for website vulnerability assessment which was preceded by WCAG 2.0. This paper provides a comparative analysis of WCAG 2.0 and WCAG 2.1 based on vulnerability assessment of Pakistan's educational and government websites. The study also investigates how effective WCAG 2.1 is with respect to WCAG 2.0. A total of 118 Pakistani Educational and Government websites have been examined for vulnerabilities based on both versions of the guidelines. Data gathered from both assessments was then utilized for comparative analysis and also visualizes via graphs to clearly understand the effectiveness of WCAG 2.1. The overall results show that WCAG 2.1 is more critical in identifying various types of vulnerabilities in websites.

Index Terms: WCAG 2.0, WCAG 2.1, XXS, CSRF, LFI, CNNVD, HTML, SQL, Vulnerabilities, EDU, GOV, web content, accessibility guidelines.

1 INTRODUCTION

IN today's modern world, being an era of advanced technology, almost everyone and everything is performed or executed in automated and computerized way. Technology covers almost every field; thus, educational and government websites are sources for providing access to people without any confinement or limit [2]. Government and educational institutes' websites bear special place as these are the sources of very important information in this fast-paced world. These websites not only provide instant and better services to the users but also provide a constant connection between the governing bodies and the people concerned. The dissemination of critical information, no matter if at smaller scale or larger scale necessitates safety and security. Security is taken into consideration as a big challenge in the design and development of any type of software, especially websites. It is due to the fact that websites are sets of related webpages which might be placed under the same area of domain, offering a communication interface between the server and the clients. The data/information resides at the servers in the form of HTML pages and upon clients' request, it is shared via the standard protocol that is referred to as HTTP protocol. The unlimited number of clients and remote access to the websites make them vulnerable to attacks from different aspects. Accessibility based vulnerabilities are one of such aspects which are often paid less attention by the designers and developers. According to National Information Security Vulnerability Library (CNNVD), there have been a total of 1,505 new vulnerabilities in June 2018, including 18 overpowered vulnerabilities and 97 excessive-risk vulnerabilities. According to the vulnerability variation graph, the range of vulnerabilities detection has steadily improved [6] day by day. Meanwhile, in web content management systems the ultimate effect of disclosure is executed through some encrypted form, the system should be up to date extensions brought out from a reliable source. if a system missing these fundamental security steps it will provide a way for security threats vulnerabilities probably SQL injection, Cross-side scripting (XSS), and some other sort of vulnerabilities interventions, due to these vulnerabilities an organization may squander their important data [9]. The Act legislated in the European Parliament refers to all of their member states, including Hungary. Directive made by Parliament, websites and mobile applications should be accessible at the end of 2021 including all government sector organizations, failing any of the public sector results in the country being scolded. For this purpose, a comprehensive study must be taken out by the Hungarian government on priority basis of all of their websites and mobile applications. In early 2010, few studies [15] [16] [22] were conducted in this regard on Hungarian websites, results have shown that all of these studies are outmoded and explicitly not concentrating government organizations. However new technologies are providing the possibility of contingency, the latest information, and the enhancement of some other resources have increased [8]. E-government propagate web-based information to support the public and also renders services to citizens [10], is frequently growing more prevalent. Current inquiries have shown e-government affords facilities to citizens and accessibility traits for the entire population of the country [7].

The rest of this paper is organized as follows:
Section 2 provides a review of the relevant literature. Section 3 describes the methodology used in the study. Section 4 presents the results of the study and makes suggestions to improve the presented issues. Finally, section 5 presents the conclusions.

2 RELATED WORK

This research is related on the discussion of comparative analysis of vulnerabilities captured in WCAG 2.0 and WCAG

- *Muhammad Asif is currently pursuing master's degree program in computer software engineering in UET Peshawar, Pakistan, PH-03127959697. E-mail: muhammadasif1142@gmail.com*
- *Dr. Muhammad Sohail Khan having PHD degree program in computer software engineering in UET Mardan, Pakistan, E-mail: sohail.khan@uetmardan.edu.pk*
- *Faisal Abrar Computer Science Department UET Mardan*

2.1. However, a large portion of the today's research on web security pays attention on vulnerabilities and discovery tools of vulnerabilities. Most recent researchers began to pay a code audit test for a little web application with 30 subjects [3]. The records from Gartner indicate that 75% of the attacks on the network are centered at websites and web application [11]. According to 2017 China website security state of affairs, analysis file was launched with the aid of 360 Threat Intelligence Center, from January to October 2017. The 360 Website security detection platforms were scanned and examined 1.047 million websites, of which 691,000 were found susceptible, accounting for 66%, and a complete of 16.741 million holes had been scanned. There are 345,000 excessive-risk web sites, which are 2.5 times higher than in 2016 [4]. Because of an absence of control over downloading data facility, an authorized user can take advantage of the shortcomings. Other unapproved records can be gotten too, which can prompt the divulgence of the organization secret data. Various research studies have been directed on various web vulnerabilities. For example, SQL infusion, XSS, CSRF, buffer overflow, broken authentication, local file inclusion (LFI), etc. The Government of Bangladesh has established an administrative policy, essential for all educational institutions to set up sites. The goal is to have an application for task management and provide performance too, so that simple and opportune access to institution is guaranteed [18]. To go along with this prerequisite, 30,000 educational organizations had enrolled for domain and had propelled their sites by July 2015[12]. Tragically, the nature of those sites and web applications did not follow secure structure and coding design. This rendered them vulnerable in numerous angles [19] [21]. Information or record sharing through download facility, for simple dissemination, is most widely recognized component in the educational sites. An overview led on web uses in which the researchers made sense of that 60% of assets in the web were not in safe situation because of presence of the application level vulnerabilities [17]. Another overview has been performed on different kinds of SQLi and XSS vulnerabilities in web application, where the researcher of the article proposed a few countermeasures to safeguard those attacks [20]. Survey on the most overarching vulnerabilities on web applications were misused utilizing diverse hacking instruments and preventive rules were additionally given through an answer of those attacks [1]. An assessment performed to distinguish the presence of different web vulnerabilities. The overview performed on 110 sites and uncovered the reason for application layer vulnerabilities [13]. Three primary variables were additionally recognized for the above explanation that incorporates absence of experience, absence of information in web security programming and ignoring utilizing of encryption techniques [5]. comprehend the presence of security weakness in their product. To get secure programming, a committed program testing individual is required. Such a professionally sound person would physically test the sites and in quest of vulnerabilities. Shockingly, the manual programming test may be a major agony [14]. Consistently, numbers of vulnerabilities are tending to be developing. A real challenge exists for Software program engineers as they do not Therefore, in an effort to tackle the issue, we need a mechanized vulnerability scanner device for testing the product repeatedly. Web applications are vital piece of our life these days. Simultaneously, the attack utilizing web application vulnerabilities and the harm brought about by them are expanding. Therefore, it is out of question that a web application could be considered hundred percent secure. Besides, manual checking of all web application vulnerabilities infeasible. These are tedious, blunder inclined and expensive. In this manner, a decent computerized instrument to recognize web application vulnerabilities is required.

3 THE RESEARCH METHOD

A series of steps is carried out during analysis of WCAG 2.0 and WCAG 2.1. The strategy is based on the following steps:

- Identification of Pakistan educational and government websites.
- Identification of information related to user's accessibility in websites.
- Using Automation WCAG 2.1 tool that will help to captures accessibility issues and to collect data.
- Comparison of data collected by WCAG 2.0 and WCAG 2.1
- Based on the WCAG 2.1 search tool, accessibility tasks completion in a required time period.
- Evaluate the effectiveness of the website.

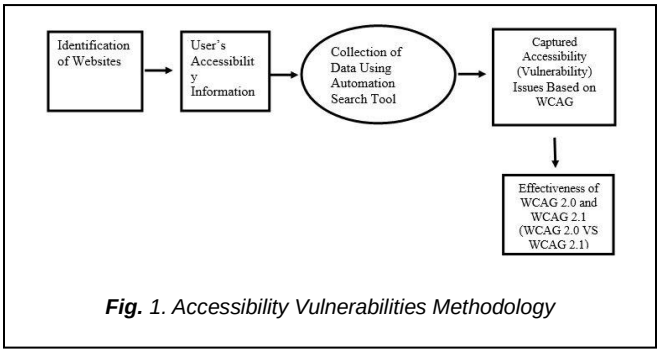

***Fig.** 1. Accessibility Vulnerabilities Methodology*

In Fig. 1. research methodology is discussed, we conducted our studies on the basis of above steps in which first we identified 118 GOV and EDU sites after identification we categorize the vulnerabilities as High (H), Medium (M) and Low (L) encountered by automation search tool, captured vulnerabilities are listed in various tables mentioned in this paper, finally we compare the web guidelines i-e WCAG 2.0 and WCAG 2.1 and concluded that WCAG 2.1 is more efficient and convenient for capturing vulnerabilities.

4 DISCUSSION ON EFFECTIVENESS OF WCAG 2.1

This study investigates if WCAG 2.1 is more effective than WCAG 2.0 in uncovering the vulnerabilities associated with websites. Appended below is a table named Table 1.1 pertaining to sample websites, wherein figures have been shown that sums up the data acquired through the study.

TABLE 1
CAPTURED VULNERABILITIES BY WCAG 2.0

WCAG 2.0	Educational websites			Govt websites		
	High	Medium	Low	high	Medium	Low
Min vulnerabilities per website	1	1	1	1	1	1
Average per website	5.8631	11.717	25.141	18	26.722	28.566
Max vulnerabilities	56	201	291	138	276	295

TABLE 2
HIGHEST VULNERABILITIES DETECTED BY WCAG 2.0 AND WCAG 2.1

	No of high vulnerabilities	High Vulnerabilities Identified by 2.1	No of high vulnerabilities	Medium Vulnerabilities Identified by 2.0	No of medium vulnerabilities	Medium Vulnerabilities Identified by 2.1	No of medium vulnerabilities
Unsafe or Unrecognized Character Set in Response Body	77	Cleartext Password Over HTTP	634	Directory Listing Detected	777	Local Filesystem Path Found	824
Possible social security No. Detected	83	Sql Injection	133	Form password with autocomplete enabled	15	PHP Error Detected	235
Http authentication over encryption HTTP	36	Shell Injection	132	Email addresses found	32	Possible source close disclosure	32
Insecure Cross Origin Resource Access Control	32	MySQL Error Detected	82	Certificate signed using SHA-1	17	URL Injection	48
SQL Server Error detected	7	Base Shell Shock Injection	68	Client Cipher suite Preference	141	HTTP Trace Support Detected	60
MySQL Error Detected	10	Differential Detected	70	Java Debug Output Detected	55	Possible HTTP Put File Upload	14
Blind Text Injection Differential	22	Page Fingerprint Differential Detected	59	Possible XML injection	122	Forward Secrecy Not Prioritized	1

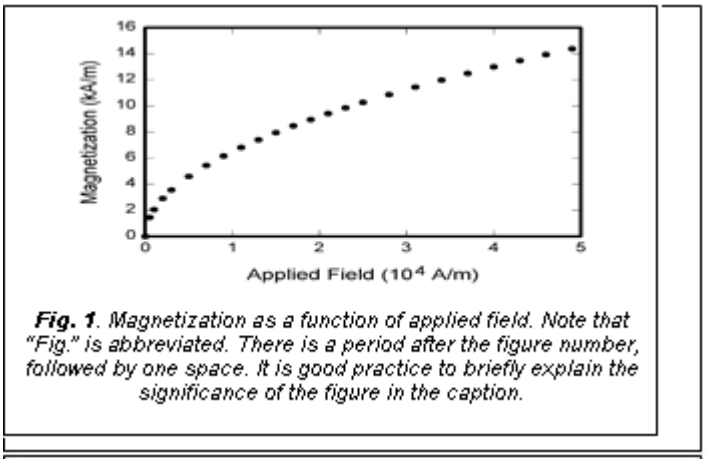

Fig. 1. *Magnetization as a function of applied field. Note that "Fig." is abbreviated. There is a period after the figure number, followed by one space. It is good practice to briefly explain the significance of the figure in the caption.*

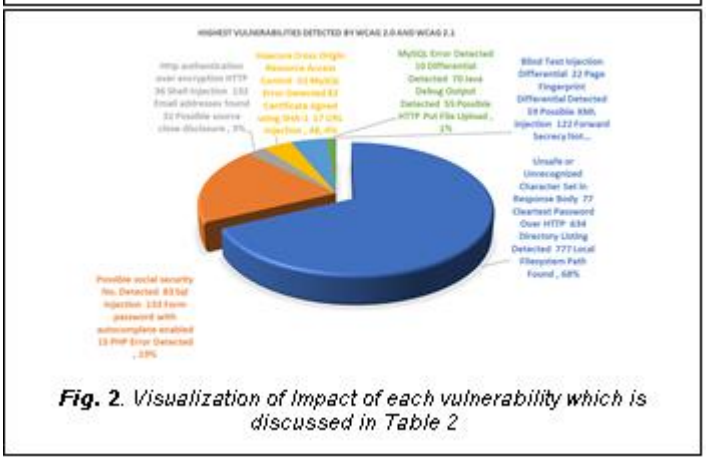

Fig. 2. *Visualization of Impact of each vulnerability which is discussed in Table 2*

In Table 2 a list of high vulnerabilities and low vulnerabilities are shown along with number of occurrences of each high and medium vulnerabilities in WCAG 2.0 and WCAG 2.1. In Figure 2 clearly demonstrated the impact of each vulnerability discussed in Table 2. Also, in Figure 2 it is clearly mentioned that up to which percent a vulnerability captured. Figure 2 display a total of 100% vulnerability in which HTTP Authentication, Shell Injection, Email Addresses found, Possible source close disclosure vulnerabilities are 3%, Insecure cross origin resource access control, MySQL Error Detected, Certificate Signed using SHA-1, URL Injection is 4%, MySQL error detected, Differential Detected, Java Debug Output Detected, Possible HTTP Put File Upload is 1%, Blind Text Injection, Differential Detected, Possible XML Injection, Forward Secrecy Not Prioritized is 5%, Unsafe Character Set in Response Body, ClearText Password Over HTTP, Directory listing Detected, Local Filesystem Path Found is 68% and Possible social security no detected, SQL Injection is, Form Password with autocomplete enabled, PHP Error Detected is 19%.

Table 3 pertaining data of Minimum, average and maximum occurrence of high, medium, and low vulnerabilities per websites as mentioned in above Table 1.3 in EDU and GOV Sites Minimum occurrence of High Vulnerability is 1, EDU AVG {(H:10.28235, M:14.36.145, L:30.16), GOV AVG(H:18.77215, M:18.82759, L:38.63636), EDU MAX(H:83, M:343, L:338), GOV MAX(H:507, M:276, L:295)}

TABLE 3
CAPTURED VULNERABILITIES BY WCAG 2.1

WCAG 2.1	Educational websites			Govt websites		
	High	Medium	Low	high	Medium	Low
Min vulnerabilities per website	1	1	1	1	1	1
Average per website	10.282	14.361	30.16	18.772	18.827	38.636
Max vulnerabilitie	83	343	338	507	276	295

TABLE 4
COMPARATIVE ANALYSIS OF IDENTIFIED SCANNED VULNERABILITIES

Websites	Total Pages Scanned by 2.0	Total Pages Scanned by 2.1	Number of High Vulnerabilities identified by 2.0	Number of High Vulnerabilities identified by 2.1	Number of Medium Vulnerabilities identified by 2.0	Number of Medium Vulnerabilities identified by 2.1
Educational Websites	70095	79430	557	874	1078	1192
Government Websites	56323	66026	1440	1483	1443	1092

Table 4 demonstrated the comparative analysis of identified scanned vulnerabilities of EDU, GOV sites based on WCAG 2.O and WCAG 2.1 web guidelines. A total of 70095 pages of educational websites were scanned by WCAG 2.0 whereas 79430 pages scanned by WCAG 2.1 also the GOV sites scanned performance of WCAG 2.1 is better than WCAG 2.0 as WCAG 2.0 has 56323 and WCAG 2.1 has scanned 6606 web pages. Furthermore, number of High vulnerabilities and medium vulnerabilities encounters of WCAG 2.1 is quite impressive than WCAG 2.0 mentioned in Table 4.

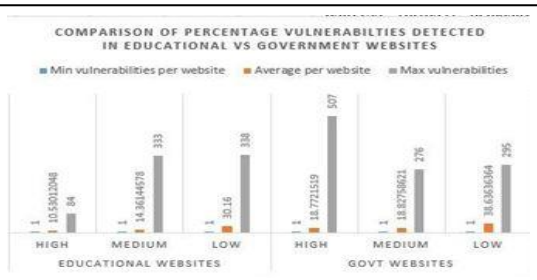

Fig. 3*. Comparative Analysis of WCAG 2.1*

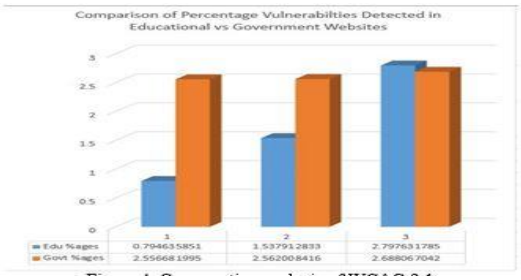

Fig. 4*. Comparative Analysis of WCAG 2.1*

Figure 3 illustrated percentage vulnerabilities in a quantitative format captured by WCAG 2.1, however these percentage vulnerabilities are clearly demonstrated in Figure 4 concluded that Edu websites are better than Gov because they keep up to date with the technology change. Developers are responsible for the vulnerabilities in websites because they have to keep in mind the web content accessibility guidelines while developing after that the site will be secure from the accessibility issue if they follow the proper WCAG guidelines.

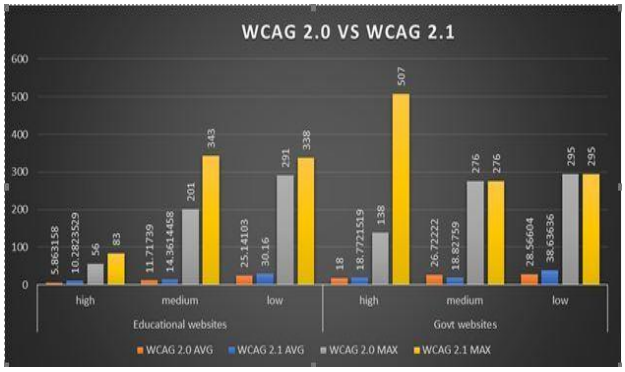

Fig. 5*. Comparative Analysis of WCAG 2.0 VS WCAG 2.1*

4.1 Educational Websites

Figure 5 illustrates number of captured vulnerabilities of WCAG 2.0 EDU {H (5.863158avg, 56max), M (11.71739avg, 201max), L (25.14103avg, 291max)}. Details with regard to number of captured vulnerabilities of WCAG 2.1 is quite impressive as compared to 2.0 i.e EDU{H(10.2823529avg,83max), M(14.3614458avg, 343max), L(30.16avg, 338max)} were encountered. From the factual position as illustrated above, it is concluded that 2.1 is more effective and can cope more vulnerabilities as compared to 2.0.

4.2 Government Websites

From figure 5, we have reached towards a conclusion that by applying WCAG 2.0 and WCAG 2.1 on government websites, a high range of vulnerabilities could be captured more effectively through WCAG 2.1. Details are WCAG 2.0 GOV {H (18avg, 138max), M (26.72222avg, 276max), L (28.56604avg, 295max)} and WCAG 2.1 GOV {H (18.7721519avg, 507max), M (18.82759avg, 276max), L(38.63636avg, 295max)}.
From the above facts and figures, an updated version WCAG 2.1 has captured more vulnerability as compared to 2.0.

5 CONCLUSIONS

In this paper, we have studied emerging web vulnerability, discovered through the usage of WCAG 2.0 and WCAG 2.1 and their comparative analysis. It includes different vulnerabilities of educational and government organizations. The data shows that various security researchers have been contributing significantly towards the security of tens of thousands of organizations on the Internet. We conducted quantitative analyses for different aspects of web vulnerability discovery. Based on our findings, we suggest that those organizations, who intend to develop a web site, should take care of vulnerabilities in accordance with the laid down criteria provided in WCAG rules.

REFERENCES

[1] A.Torkaman Atashzar et al., "A survey on web application vulnerabilities and countermeasures,"6th International Conf. on Computer Sciences and Convergence Information Technology (ICCIT),Seogwipo, 2011, pp. 647-652.Acunetix Ltd, Web Vulnerability Scanner, 2007, http://www.acunetix.com/vulnerability- scanner/

[2] Akgul, Y., 2016. Web Site Accessibility, Quality and Vulnerability Assessment: a Survey of Government Web Sites in the Turkish Republic. "Journal of Information Systems Engineering & Management, 1(4), p.50".

[3] A. Edmundson et al., "An empirical study on the e_ectiveness of security code review". In Engineering Secure Software and Systems, 2013.

[4] B. Rexha et al., "Impact of secure programming on web application vulnerabilities," 2015 IEEE International Conference on Computer Graphics, Vision, and Information Security (CGVIS), Bhubaneswar, 2015, pp. 61-66.

[5] Banks reluctant to use 'white hat' hackers to spot security aws. NPR, 2014.

[6] Bug bounty highlights and updates. Facebook, 2014.

[7] Benavides, A.D., Nukpezah, J, Keyes, L.M AND Soujaa, I., 2020. Adoption of Multilingual State Emergency Management Websites: Responsiveness to the Risk Communication Needs of a Multilingual Society. International Journal of Public Administration, pp. 1-11.

[8] Bennett, L. V., & Manoharan, A. P. (2017). The use of social media policies by US municipalities. International Journal of Public Administration, 40(4),317–328. doi:10.1080/01900692.2015.1113182

[9] Csontos, B. and Heckl, I., 2020. Accessibility, usability, and security evaluation of Hungarian government websites. Universal Access in the Information Society, pp.1-18.

[10] D'agostino, M. J., Schwester, R., Carrizales, T., & Melitski, J. (2011). A study of e-government and e-governance: An empirical examination of municipal websites. Public Administration Quarterly, 35(1). 3-25. doi:10.1111/puar.2004.64.issue-1

[11] "Evaluation of Web Vulnerability Scanners"The 8th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications24-26September2015, Warsaw, Poland.

[12] El et al., 2017, July. Benchmarking vulnerability scanners: An experiment on SCADA devices and scientific instruments. In 2017 IEEE International Conference on Intelligence and Security Informatics (ISI) (pp. 83-88). IEEE.

[13] G.Deepa and P. S.Thilagam, "Securing web applications from injection and logic vulnerabilities: Approaches and challenges, " 2016 Information and Software Technology, 74, 160-180".

[14] Hassan et al., 2016. An Investigation of Educational Web Applications in Bangladesh: A Case Study on Local File Disclosure Vulnerability. In 4th International Conf. on "Engineering & Technology, Computer, Basic & Applied Sciences" (ECBA-2016), Sydney.

[15] Lanyi, C.S., Czank, N., Sik, A.: Testing the accessibility of web- sites. Int. J. Knowl. Web Intell. 2(1), 87 (2011).

[16] Merkovity, N.: Hungarian party websites and parliamentary elec- tions. Cent. Eur. J. Commun. 4(7), 209–225 (2011)

[17] OWASP 2013 Top 10. www.owasp.org/index.php/Top_10_2013-Top_10.

[18] P. V. Ami et al, "Top Five Dangerous Security Risks over Web Application" 2013 International Journal of Emerging Trends & Technology in Computer Science, 2(1), 41-43.

[19] Parimala et al., "Efficient Web Vulnerability Detection Tool for Sleeping Giant-Cross Site Request Forgery." In Journal of Physics: Conference Series, vol. 1000, no. 1, p. 012125. IOP Publishing, 2018.

[20] R. Johari and P. Sharma, "A Survey on Web Application Vulnerabilities (SQLIA, XSS) Exploitation and Security Engine for SQL Injection," 2012 International Conference on Communication Systems and Network Technologies, 2012, Rajkot, pp. 453-458. H.

[21] Suteva, Natasa, Dragan Anastasov, and Aleksandra Mileva. "One unwanted feature of many Web Vulnerability Scanners." (2015): 279-283. Updates on vulnerability handling process. www.wooyun.org/notice.php?action=view&id=28,2013.

[22] Szeróvay, K.: Usability of e-Government websites, evaluation of the Hungarian e-Government portal. In: COFOLA 2011, pp. 1596–1635 (2011)