Análise de vulnerabilidade em portais de Governo Eletrônico

José Victor Pereira Costa[1], **Rodrigo Sanches Miani**[1]

[1]Faculdade de Computação (FACOM)
Universidade Federal do Uberlândia (UFU)
Uberlândia – MG – Brasil

josevictorpatos@ufu.br, miani@ufu.br

Nível: Trabalho de Conclusão de Curso

Resumo. *Este trabalho tem como objetivo identificar as eventuais vulnerabilidades de segurança em portais de governos eletrônicos, buscando compreender a relação entre a estrutura econômico-tecnológica e a segurança de sistemas. As análises a serem desenvolvidas levarão em conta o uso de ferramentas, Web Scanners, que irão auxiliar na obtenção de resultados mais efetivos. O desenvolvimento do projeto é feito observando cenário tecnológico nacional bem como suas estruturas de segurança.*

Palavras-Chave. *Segurança da Informação, Governo Eletrônico, Vulnerabilidades de Segurança*

1. Introdução e objetivos

A necessidade de sistemas mais seguros tem se tornado um desafio a instituições privadas e públicas em todo mundo. Enquanto a evolução tecnológica transforma as formas de comunicação e comércio novas vulnerabilidades têm surgido como limitantes desse desenvolvimento, como citado no trabalho de [Nakamura and de Geus 2007].

O objetivo dessa pesquisa é identificar as eventuais vulnerabilidades de portais de governos eletrônicos, buscando compreender a relação entre a estrutura econômico-tecnológica e a segurança de sistemas. De acordo com [Wikipédia 2016], Governos Eletrônicos tem por função a entrega de produtos do Estado tanto aos cidadãos como à indústria e no uso de ferramentas eletrônicas e tecnologias da informação para aproximar governo e cidadãos. Essa aproximação tem por objetivo superar obstáculos existentes entre a comunicação das duas esferas. Dentre as diferentes ferramentas utilizadas podem ser citadas: portais de internet com fóruns, exposição de bancos de dados, aplicativos para telefonia móvel e telefones de serviço. Os governos eletrônicos tem finalidade de automatizar processos já existentes no papel e em escritórios.

Através dos resultados obtidos espera-se identificar as vulnerabilidades que apresentem riscos para esses portais web e para sua estrutura de funcionamento podendo, dessa forma, alertar e prevenir eventuais problemas para segurança. Por definição, de acordo com [OWASP 2016], uma vulnerabilidade é um buraco ou uma fraqueza na aplicação, que pode ser uma falha de projeto ou um *bug* de implementação, que permite que um invasor cause danos aos *stakeholders* de uma aplicação. Dentre vulnerabilidades mais recorrentes, temos Injeção de Código, Quebra de Autenticação e XSS (*Cross-Site Scripting*), ocupando respectivamente as três posições do ranking estabelecido por [Owasp et al. 2013]. Como forma de identificar essas vulnerabilidades foram desenvolvidos softwares que automatizam todo o processo de testes. Essas mesmas ferramentas têm sido utilizadas durante todo o desenvolvimento deste trabalho, sendo classificadas por [OWASP 2017].

2. Métodos

O método utilizado na execução do projeto é centrado em quatro etapas essenciais:

1. Seleção das ferramentas – Escolha dentre os diversos softwares de detecção de vulnerabilidades;
2. Seleção dos portais web baseados no critério de avaliação;
3. Varredura do sítios web;
4. Análise dos resultados obtidos.

Esse método de análise foi elaborado com base nas abordagens utilizadas por [Doupé et al. 2010], [Rocha et al. 2011] e [Monteverde and Campiolo 2014] A seleção das ferramentas e o desenvolvimento da pesquisa tem seu apoio em uma bibliografia na qual experimentos semelhantes foram executados. Todas as ferramentas selecionadas são gratuitas, ou possuem versões gratuitas. No total foram selecionadas quatro ferramentas: Uniscan, Vega, Skipfish e W3af. Escolhidas com base no trabalho de [Rocha et al. 2011] e [Holm et al. 2011]. As ferramentas foram testadas em dois ambientes de teste(Mutilllidae e WackoPicko) e um site(sendo omitido por questões de segurança).

3. Resultados Esperados

O resultado esperado por esse trabalho é uma projeção da segurança sítios web em determinadas regiões dos país, oferecendo um ampla analise da segurança em ambientes governamentais. O relatório elaborado ao final deste trabalho servirá como um medidor do investimento em segurança da informação e também como uma estimativa das principais falhas de segurança contidas nesses sistemas. Assim como no trabalho proposto por [Doupé et al. 2010], espera-se obter um quadro com as vulnerabilidades mais recorrentes nesses sítios web, tal como a Figura 1. Espera-se também uma estimativa por cidade e região, a exemplo da matéria presente no blog PSafe escrita por [Leonardo Lorenzoni 2016], que originou os dados presentes na Figura 2. Ao final do trabalho será teremos estáticas ainda mais especificas, obtendo um quadro mais próximo do real no que se refere a situação de cada região.

Name	Detection	INITIAL Reachability	CONFIG Reachability	MANUAL Reachability
XSS Reflected	1	0	0	0
XSS Stored	2	0	0	0
SessionID	4	0	0	0
SQL Injection Reflected	1	0	0	0
Commandline Injection	4	0	0	0
File Inclusion	3	0	0	0
File Exposure	3	0	0	0
XSS Reflected behind JavaScript	1	3	3	0
Parameter Manipulation	8	0	0	0
Weak password	3	0	0	0
SQL Injection Stored Login	7	7	3	3
Directory Traversal Login	8	8	6	4
XSS Stored Login	2	8	7	6
Forceful Browsing Login	8	7	6	3
Logic Flaws - Coupon	9	9	8	6
XSS Reflected behind flash	1	9	7	1

Figura 1. Tabela ilustra a quantidade de vulnerabilidades detectadas por cada configuração. Extraído do trabalho de [Doupé et al. 2010].

Estado	Ameaças
São Paulo	1.204.337
Rio de Janeiro	490.202
Minas Gerais	378.280
Bahia	306.729
Pernambuco	243.462
Paraná	214.924
Rio Grande do Sul	180.544
Piauí	163.084
Pará	130.985
Goiás	118.793

Figura 2. Tabela ilustra a quantidade de ameças em cada estado. Extraído do trabalho de [Leonardo Lorenzoni 2016].

Referências

Doupé, A., Cova, M., and Vigna, G. (2010). Why johnny can't pentest: An analysis of black-box web vulnerability scanners. In *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, pages 111–131. Springer.

Holm, H., Sommestad, T., Almroth, J., and Persson, M. (2011). A quantitative evaluation of vulnerability scanning. *Information Management & Computer Security*, 19(4):231–247.

Leonardo Lorenzoni (2016). Brasil registra mais de 4 milhões de ataques cibernéticos em maio - Blog da PSafe — Especialista em Tecnologia Android.

Monteverde, W. A. and Campiolo, R. (2014). Estudo e Análise de Vulnerabilidades Web. pages 415–423.

Nakamura, E. T. and de Geus, P. L. (2007). *Segurança de redes em ambientes cooperativos*. Novatec Editora.

OWASP (2016). Category:Vulnerability - OWASP.

OWASP (2017). Category:Vulnerability Scanning Tools - OWASP.

Owasp, P., Serr, C., Machry, M., Revoredo, C. M., Vieira, L., Ramalho, S., Ol, J., Quint, D., Risonho, M., Assump, P., Lopes, M., Dias, C., Esta, R. G., and Top, O. (2013). OWASP Top 10 - 2013: Os dez riscos de segurança mais críticos em aplicações web. *OWASP Top 10*, page 23.

Rocha, D., Kreutz, D., and Turchetti, R. (2011). Uma ferramenta livre e extensível para detecção de vulnerabilidades em sistemas Web. *10th International Symposium on Autonomous Decentralized Systems (ISADS)*, (July):747–752.

Stallings, W. (2006). *Cryptography and network security: principles and practices*. Pearson Education India.

Wikipédia (2016). Governo eletrônico — wikipédia, a enciclopédia livre. [Online; accessed 28-setembro-2016].