UNIVERSIDADE FEDERAL DE PERNAMBUCO

Graduação em Ciência da Computação

Centro de Informática

2012.2

Análise do Aumento da Superfície de Ataque na Web Decorrente da Exploração de Recursos do HTML 5

Proposta de Trabalho de Graduação

Discente: Marcelo Frota Pinto Pessoa – mfpp@cin.ufpe.br

Orientador: Ruy José Guerra Barretto de Queiroz – ruy@cin.ufpe.br

Recife, Janeiro de 2013

Sumário

1. Motivação

Não é novidade para ninguém o fato de que a *internet*, mais precisamente a *web*, está presente nas mais diversas áreas, e que grande parte das tarefas executadas hoje, de alguma forma, a utiliza. A *web* está tão presente na vida das pessoas que até mesmo seus relacionamentos sociais estão dentro da rede, ou no mínimo, são influenciados por ela. Dada tamanha importância, as chamadas aplicações *web* vem se tornando, cada vez mais, um alvo dos *hackers*. Os ataques sobre aplicações *web* tem registrado um aumento significativo nos últimos anos, com um destaque especial para as mais populares, como o Facebook, o Twitter, e o MySpace, por exemplo [1]. Segundo estudos realizados pela Imperva [2], uma aplicação *web* comum é alvo de ataques, em média, 120 dias por ano (33% do tempo), enquanto que as mais visadas, encontram-se sob ataque cerca de 292 dias por ano (cerca de 80% do tempo).

Outro dado bastante preocupante é que a maioria das aplicações *web* desenvolvidas hoje possuem falhas de segurança, sejam elas no *front* ou no *back-end*. De acordo com a WhiteHat [3], o número de pontos susceptíveis a vulnerabilidades de **alta severidade** por aplicação é de 79 a cada ano. Este número, apesar de estar em queda, não é nada animador, visto que apenas uma vulnerabilidade dessa natureza pode ser o suficiente para que um eventual atacante consiga assumir o controle da aplicação. E com a chegada do **HTML 5** (*Hypertext Markup Language* versão 5), que engloba um conjunto de novas tecnologias, essa situação tende a piorar.

A introdução de novas funcionalidades, além de tornar uma aplicação potencialmente mais poderosa, torna-a também potencialmente mais vulnerável. O motivo é que o aumento da complexidade, quando se trata de segurança, inevitavelmente insere novos potenciais vetores de ataque, causando o **aumento da superfície de ataque**. E com o **HTML 5** não será diferente, suas novas *features* ou introduzem novas vulnerabilidades ou tornam mais crítico o impacto de vulnerabilidades já conhecidas, causando assim o **aumento da superfície de ataque** na *web*, e tornando não só as aplicações, mas também os *browsers*, mais susceptíveis a ataques [4]. Dessa forma, surge a necessidade da realização de uma análise detalhada destas novas tecnologias por parte dos especialistas em segurança, de modo que seja possível estar em pé de igualdade com os *hackers*.

2. Objetivos

O objetivo principal deste trabalho é realizar uma análise da **insegurança** das tecnologias que compõem o padrão **HTML 5**, com o objetivo de identificar novos vetores de ataque, e assim comprovar o aumento da superfície de ataque na *web*. Além disso, como objetivo secundário, mas não menos importante, este trabalho tentará, sempre que possível, ilustrar formas de mitigar as vulnerabilidades encontradas. A metodologia que será empregada para a realização desta análise consistirá de quatro passos básicos, são eles:

1. Identificar os principais recursos que representam potenciais ameaças;
2. Encontrar as vulnerabilidades exploráveis nestes recursos;
3. Descrever ao menos um cenário de ataque possível para cada recurso identificado;
4. Sugerir contramedidas para mitigar os cenários de ataque descritos, se possível.

3. Cronograma

Na tabela a seguir proponho um cronograma inicial, contemplando as principais atividades necessárias ao desenvolvimento deste trabalho, que poderá sofrer futuras modificações de acordo com a necessidade.

Atividade	Dezembro	Janeiro	Fevereiro	Março	Abril
Levantamento bibliográfico e leitura	X	X	X		
Elaboração da proposta preliminar		X			
Identificação das potenciais ameaças		X	X		
Simulação de cenários de ataque			X	X	
Escrita geral da monografia				X	X
Preparação para a apresentação					X

4. Referências Bibliográficas

[1] CORREIA, Miguel Pupo; SOUSA, Paulo Jorge. **Segurança no Software**. Lisboa: FCA, 2010.

[2] **Imperva's Web Application Attack Report**. Ed. 3, 2012. Disponível em: <http://www.imperva.com/docs/HII_Web_Application_Attack_Report_Ed3.pdf >. Acesso em: 27 dez. 2012.

[3] **WhiteHat's Website Security Statistics Report**. Ed. 12, 2012. Disponível em: <https://www.whitehatsec.com/assets/WPstats_summer12_12th.pdf >. Acesso em: 03 jan. 2013.

[4] SCHMIDT, Michael. **HTML5 Web Security**. Compass Security AG, 2011. Disponível em: <http://dl.packetstormsecurity.net/papers/web/HTML5_Web_Security_v1.0.pdf >. Acesso em: 02 dez. 2012.

5. Possíveis Avaliadores

- ✓ Djamel F. H. Sadok – jamel@cin.ufpe.br
- ✓ Carlos Ferraz – cagf@cin.ufpe.br

6. Assinaturas

_____

Marcelo Frota Pinto Pessoa
Discente

_____

Ruy José Guerra Barretto de Queiroz
Orientador