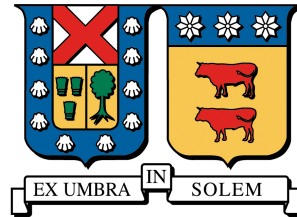


UNIVERSIDAD TÉCNICA FEDERICO SANTA MARÍA
DEPARTAMENTO DE INFORMÁTICA
VALPARAÍSO, CHILE



Estado del Arte: Web browsers bajo ataques y sus mecanismos de Seguridad.

Paulina Andrea Silva Ghio

Memoria para optar al título de: Ingeniera Civil Informática

Profesor Guía: Raúl Monges
Profesor Correferente: Javier Cañas

24 de marzo de 2015

Resumen

El uso del Internet en la vida cotidiana ya es parte de la mayoría del mundo. Para cada necesidad de información el usuario puede buscar en Internet aquello que lo aqueja, desde comprar tickets para una película, realizar reuniones por videoconferencia y muchas otras tareas que en el pasado no eran necesarias, pero que hoy en día su uso es imperante; como las redes sociales. La Web 2.0 ha sido gran colaboradora de éste éxito en la vida de las personas, entregando las herramientas para que los contenidos que los usuarios necesiten estén disponibles de diversas formas y en tiempo real.

Junto con éste desarrollo en la forma de interactuar con la Internet, parte de la responsabilidad de que existan la tienen los desarrolladores que crean Software de acuerdo a los requerimientos de sus clientes. Dentro de las necesidades de los clientes, algunos equipos de Desarrollo de Software tienen casi siempre en cuenta ciertos requerimientos no funcionales que permiten conservar ciertos atributos en el Sistema a crear, como: Confidencialidad, Integridad, No Repudio y Disponibilidad. Sin embargo, muchas veces por los costos y poco tiempo que poseen, los atributos mencionados no son salvaguardados. En consecuencia el producto final, podría llegar a tener serias consecuencias tanto en el Cliente como en los Usuarios que podrían llegar a usar el Sistema.

El Objetivo de esta Memoria es generar un cuerpo organizado de información sobre la Seguridad en el Web Browser, de manera que el conocimiento adquirido por medio del estudio se pueda compactar en un documento con formato fácil de entender para Profesionales y Estudiantes de Informática. Para lo anterior, es necesario comprender los conceptos relacionados al navegador web, sus componentes, ataques que puede estar sometido, mecanismos de defensa y otros. Una vez organizado el estudio, se construirán una Arquitectura de Referencia del Web Browser y Patrones de Mal uso para ciertos ataques, que condensarán el conocimiento obtenido de la seguridad en el Web Browser. Los artefactos mencionados permitirán sistematizar el conocimiento de cómo se ejecutan los ataques y mecanismos de mitigación que existen actualmente, en un formato fácil de entender.

Abstract

Índice

| | |
|--|---|
| Índice | 3 |
| 1. Motivación: ¿Por que estudiar el Browser? | 5 |
| 2. Contribuciones | 5 |
| 3. Estructura del Documento | 5 |
| 4. Definiciones | 6 |
| 4.1. Vulnerabilidades, Debilidades, Amenazas y Ataques | 6 |
| 4.2. Browser: HTML, DOM, CSS, Javascript y Otros | 6 |
| 4.2.1. HyperText Markup Language, HTML | 6 |
| 4.2.2. Extensible Markup Language, XML | 6 |
| 4.2.3. Document Object Model, DOM | 6 |
| 4.2.4. Cascading Style Sheets, CSS | 6 |
| 4.2.5. Javascript | 6 |
| 4.2.6. Asynchronous JavaScript And XML, Ajax | 6 |
| 4.2.7. Adobe Flash | 6 |
| 4.2.8. Render Engine | 6 |
| 4.2.9. User and X Browsing | 6 |
| 5. Riesgos al Navegar y Ataques en el Browser | 6 |
| 6. Mecanismos de Seguridad en el Browser | 6 |
| 6.1. Same Origin Policy, SOP | 6 |
| 6.2. Cross-Origin Resource Sharing, CORS | 6 |
| 6.3. CSP | 6 |
| 6.4. Sandboxing | 6 |
| 6.5. HTTP Headers | 6 |
| 6.6. Encoding | 6 |
| 6.7. Sanitization | 6 |
| 6.8. Otros | 6 |
| 7. Componentes del Browser | 7 |
| 7.1. Render Engine | 7 |
| 8. Ethical Hacking en el Browser | 7 |
| 8.1. Ataques de Ingeniería Social | 7 |
| 8.2. WebGoat | 7 |
| 8.3. BeeF y Metasploit | 7 |
| 9. Arquitectura de Referencia del Browser | 8 |
| 9.1. Definición | 8 |
| 9.2. Construcción | 8 |
| 10. Formulación de Patrones de Ataque | 8 |
| 10.1. Ataque 1: | 8 |
| 10.2. Ataque 2: | 8 |
| 10.3. Ataque 3: | 8 |
| 11. Discusión de Patrones de Mal uso existentes | 8 |

| | | |
|-----|--------------------------|---|
| 12. | Conclusiones | 9 |
| 13. | Trabajo Futuro | 9 |
| | Bibliografía | 9 |
| A. | Anexos | 9 |

1. Motivación: ¿Por que estudiar el Browser?
2. Contribuciones
3. Estructura del Documento

4. Definiciones

4.1. Vulnerabilidades, Debilidades, Amenazas y Ataques

4.2. Browser: HTML, DOM, CSS, Javascript y Otros

4.2.1. HyperText Markup Language, HTML

4.2.2. Extensible Markup Language, XML

4.2.3. Document Object Model, DOM

4.2.4. Cascading Style Sheets, CSS

4.2.5. Javascript

4.2.6. Asynchronous JavaScript And XML, Ajax

4.2.7. Adobe Flash

4.2.8. Render Engine

4.2.9. User and X Browsing

5. Riesgos al Navegar y Ataques en el Browser

6. Mecanismos de Seguridad en el Browser

6.1. Same Origin Policy, SOP

6.2. Cross-Origin Resource Sharing, CORS

6.3. CSP

6.4. Sandboxing

6.5. HTTP Headers

6.6. Encoding

6.7. Sanitization

6.8. Otros

7. Componentes del Browser

7.1. Render Engine

8. Ethical Hacking en el Browser

8.1. Ataques de Ingeniería Social

8.2. WebGoat

8.3. BeeF y Metasploit

9. Arquitectura de Referencia del Browser

9.1. Definición

9.2. Construcción

10. Formulación de Patrones de Ataque

10.1. Ataque 1:

10.2. Ataque 2:

10.3. Ataque 3:

11. Discusión de Patrones de Mal uso existentes

12. Conclusiones

13. Trabajo Futuro

Bibliografía

- [1] E. Fernandez-Buglioni. *Security patterns in practice: designing secure architectures using software patterns*. John Wiley & Sons, 2013.

A. Anexos