Regular expressions Denial of Service -ReDoS

Michael Hidalgo

OWASP Costa Rica

michael.hidalgo@owasp.org

OWASP

The Open Web Application Security Project

About Me

OWASP
The Open Web Application Security Project

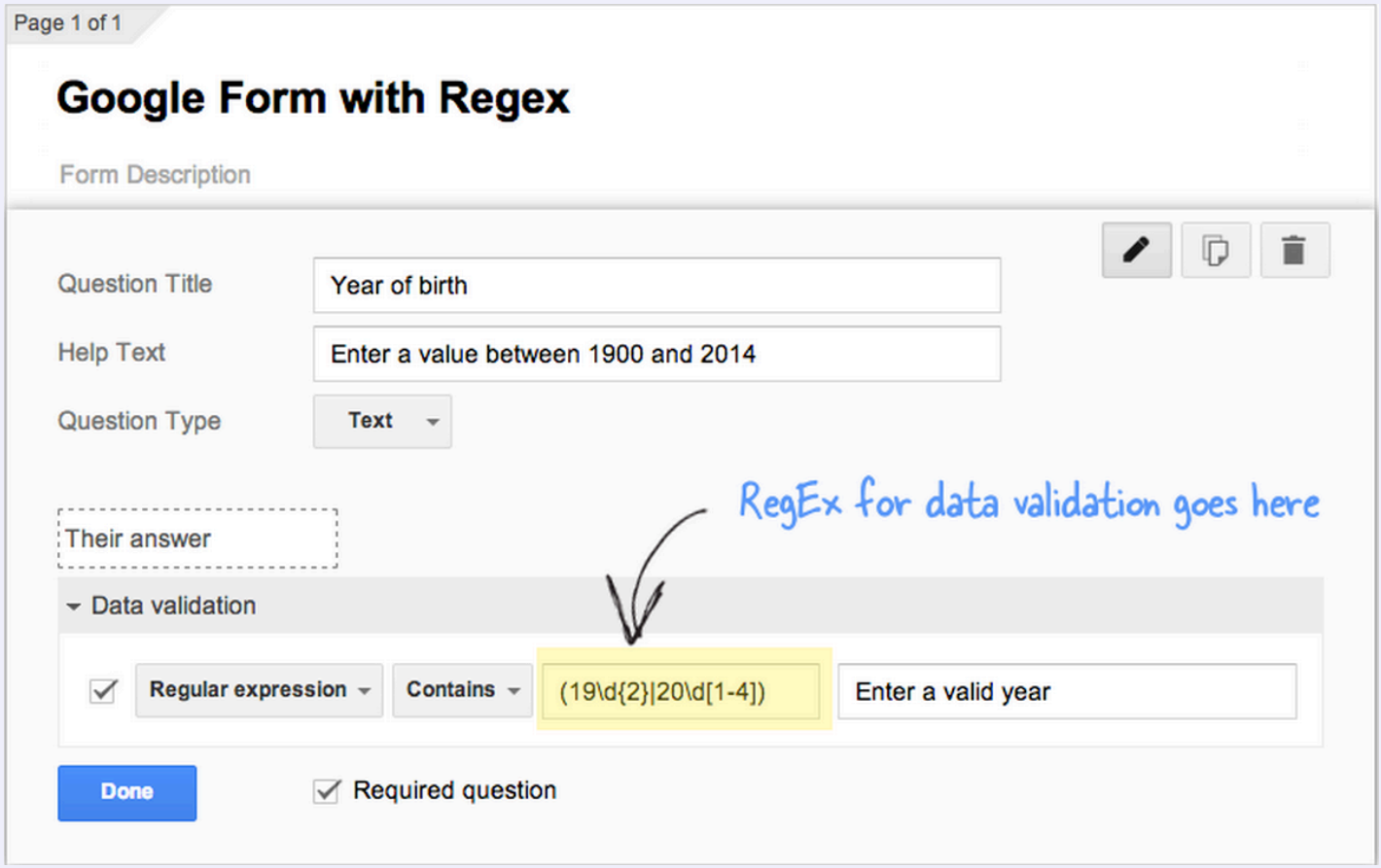
- Líder del capítulo de OWASP Costa Rica.
- Software engineer Security Innovation.
- Experiencia en el área financiera.
- Investigador seguridad de aplicaciones.
- Participo en proyectos de OWASP (Plataforma O2, SafeNuGet).

Agenda

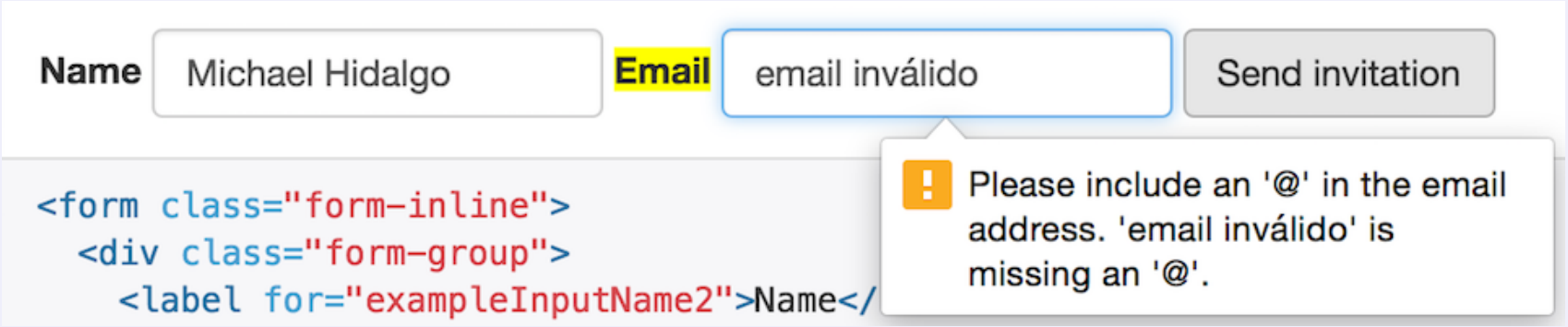
OWASP
The Open Web Application Security Project

- Breve introducción a las expresiones regulares.
- Ejemplo de expresiones regulares usadas frecuentemente
- Autómata determinístico no Finito (NFA)
- Problemas de denegación de servicio
- Demo
- Conclusiones, recomendaciones oportunidades de mejora.

- Expresiones regulares son muy usadas



- Expresiones regulares facilitan validación de campos de entrada.



Algunos usos comunes de las expresiones regulares

- Validar formatos como número de teléfono, correos electrónico, direcciones Web, etc.
- Servir como filtro de datos.
- Encontrar cierto texto dentro de un archivo.

OWASP
The Open Web Application Security Project

Pero ¿qué es una expresión regular?

- Cadena que contiene una combinación de caracteres normales y caracteres especiales o meta secuencias.
- Caracteres normales tienen su propio significado.
- Meta caracteres o meta secuencias son caracteres o secuencias que tienen significado (cantidades, ubicaciones etc.).

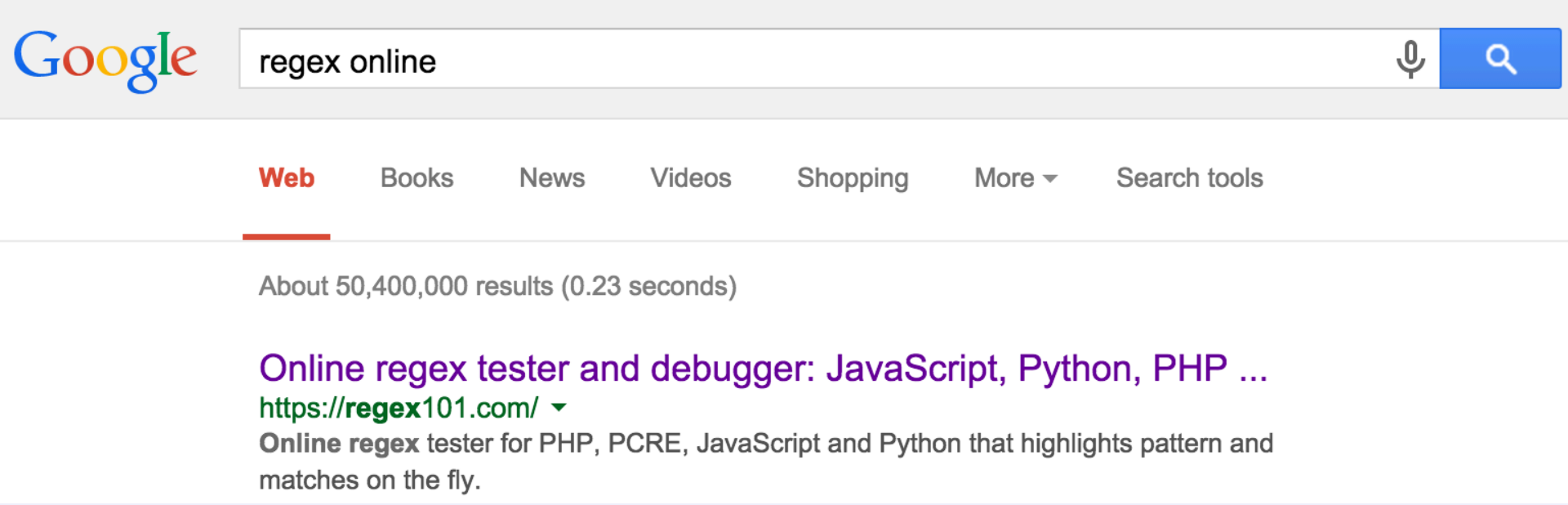
Elementos de una expresión regular

- Coincidencia de Patrones (Pattern matching) : Encontrar una sección de texto que es descrita por la expresión regular (matching).
- Motor de expresiones regulares: Código o programa encargado de buscar ese texto

OWASP
The Open Web Application Security Project

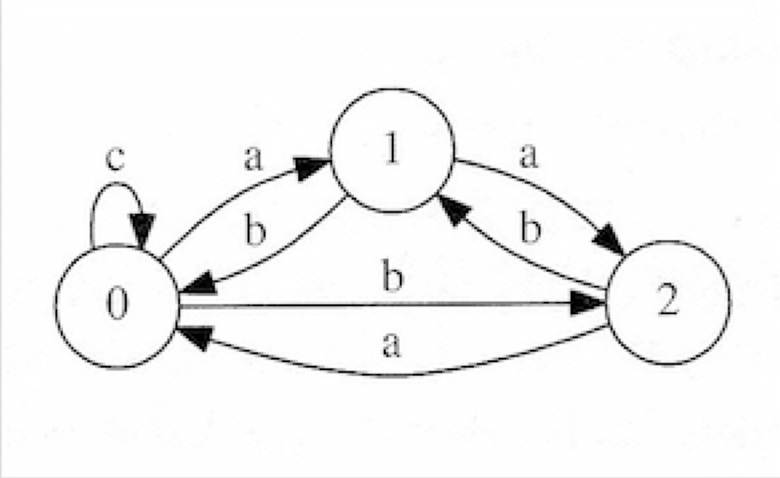
- Expresiones regulares usadas frecuentemente
- Contraseñas : **/^[a-z0-9_-]{6,18}$/**
- Correo electrónico : **/^([a-z0-9_\.-]+)@([\da-z\.-]+)\.([a-z\.]{2,6})$/**
- Solo dígitos: **^[0-9]*$**
- Solo letras: **/[a-zA-Z]+/**

- Existen muchos lugares donde aprender y probar expresiones regulares.



Autómata finito no determinístico (NFA)

- Autómata: simple computadora, con estados y la transición de un estado a otro de acuerdo a una secuencia de entradas.



Autómata finito no determinístico (NFA)

- Retroceso (Backtracking)
- El motor encuentra fácilmente una coincidencia positiva (positive matching), no obstante confirmar una coincidencia negativa (negative matching) toma más tiempo.

OWASP
The Open Web Application Security Project

Denegación de Servicio a través de Expresiones regulares (ReDoS)

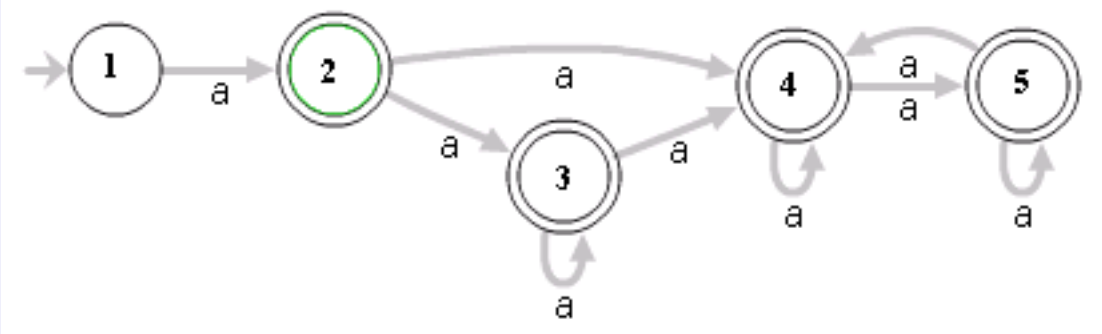
- Implementaciones de expresiones regulares pueden alcanzar situaciones extremas.
- Ralentización crece exponencialmente relacionado al tamaño del dato de entrada.
- Atacante puede ocasionar que el sistema se enfrente a estas situaciones extremas y se comporte de forma lenta por un periodo de tiempo prolongado.

El algoritmo problemático de naïve

- Algoritmo de expresiones regulares que implementa un NFA.
- Máquina de estado finito.
- Por cada par de estados y símbolos de entrada puede haber múltiples estado.
- La mayoría de los motores de expresiones regulares usan el algoritmo de naïve.

Ilustrando el problema

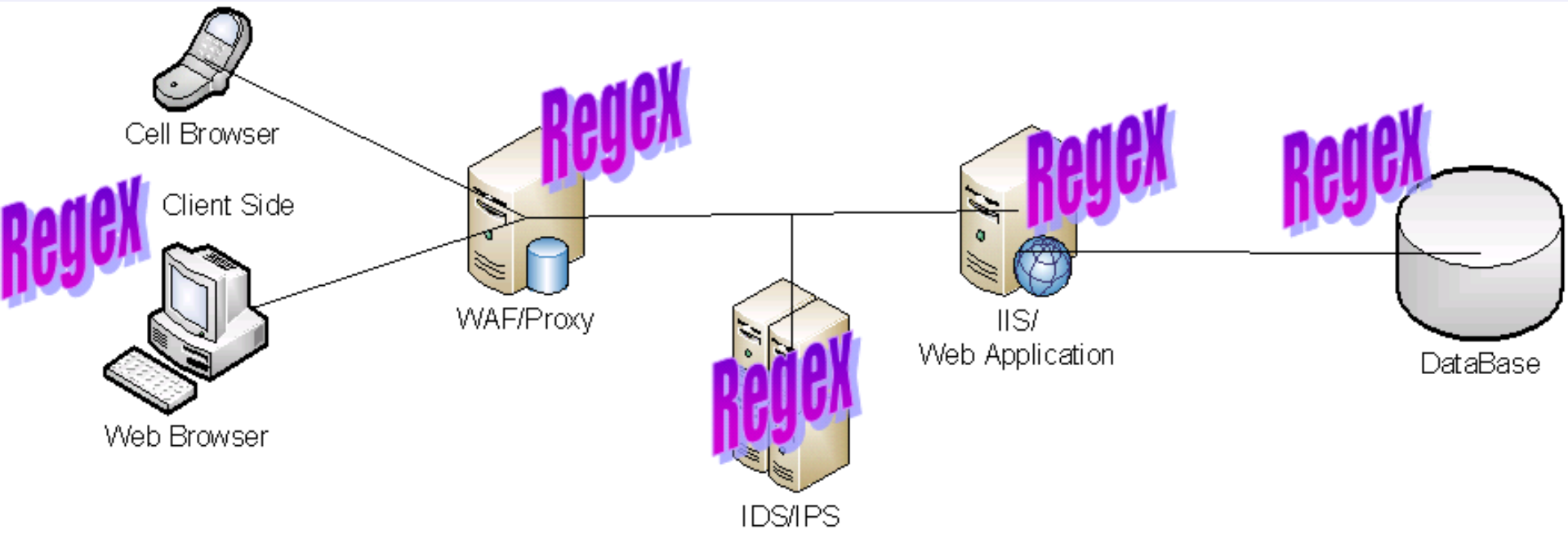
Dada la expresión regular: ***^(a+)+$***



Dada una entrada como **aaaaX** existen 16 posibles rutas (2^4).

No obstante dada la entrada aaaaaaaaaaaaaaaaX, hay 65,536 posibles rutas (2^16).

- La Web se basa en expresiones regulares




Demo

OWASP
The Open Web Application Security Project

Algunos patrones de expresiones regulares problemáticas

- Agrupamiento con repetición
- (a+)+
- ([a-zA-Z]+)*
- (a|aa)+
- (a|a?)+
- (.*a){x} | for x > 10

OWASP
The Open Web Application Security Project

Conclusiones, recomendaciones, oportunidades de mejora

- Es muy fácil escribir código inseguro.
- Siempre se debe probar las expresiones regulares a través de pruebas unitarias.
- No utilizar expresiones regulares que implementan complejos agrupamientos.
- Siempre se debe validar la longitud del dato de entrada antes de evaluar dicho dato con la expresión regular.

Muchas Gracias!

OWASP
The Open Web Application Security Project

- Referencias

1. Hollos, F. Hollos R : Finite Automata and Regular Expressions Problems and Solutions
2. Stubblebine, T. Regular Expressions Pocket Reference.
3. Regular Expressions Denial of the Service Attacks and Defenses https://msdn.microsoft.com/en-us/magazine/ff646973.aspx
4. OWASP https://www.owasp.org/index.php/Regular_expression_Denial_of_Service_-_ReDoS
5. http://www.cs.bham.ac.uk/~hxt/research/reg-exp-sec.pdf