Denial of Service's Natural Evolution

FAP DDoS

Reverend H. Helix
revy@fapddos.com

Overview

- What Is JavaScript
  - Origin
  - ECMAScript
- How we knew JavaScript
- Breaking Out - Where is JS used now?
- What is a DDoS attack?
- Anatomy of a DDoS Attack
- FAP - About & Demos

What Is JavaScript

JavaScript (JS) is an interpreted computer programming language.

It was originally implemented as part of web browsers so that client-side scripts may interact with the user.

-- Wikipedia

Origin...

Made by Netscape

Released as part of Netscape Navigator 2.0

Developed as part of Mocha, under the name of lightscript.

In 1997 it was submitted to ECMA and became....

ECMAScript - Standardization

ECMAScript is the scripting language standardized by Ecma International in the ECMA-262 specification and ISO/IEC 16262. The language is widely used for client-side scripting on the web, in the form of several well-known dialects such as JavaScript, JScript and ActionScript.

How We Knew JavaScript

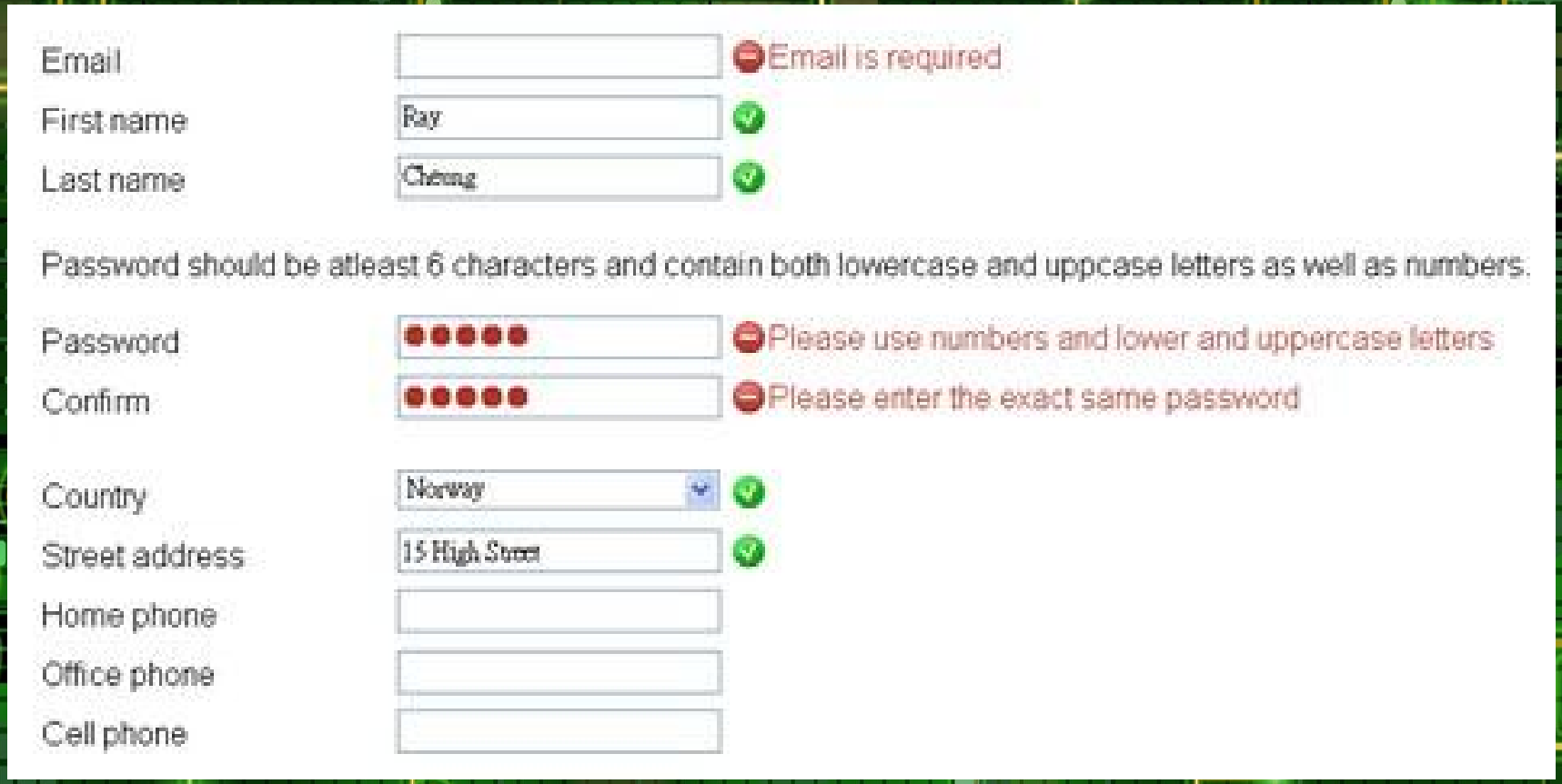
When I think of my first introduction to JavaScript, I can't help but remember the silly web browser garbage.

Silly things I've seen (light):

- Mouse Cursor Trails
- Password Protection (kinda sorta, not really...)
- Alert box greetings.
- Form interaction (validate, populate, etc)

JavaScript was meant for so much more than that crap..

Web Browser - Forms



AJAX

Asynchronous methods are awesome, even more awesome when used with JSON! AJAX made Web 2.0, and it was first implemented by Microsoft.

AJAX is a group of interrelated web development techniques used on the client-side to create asynchronous web applications. With Ajax, web applications can send data to, and retrieve data from, a server asynchronously (in the background) without interfering with the display and behavior of the existing page. Data can be retrieved using the XMLHttpRequest object.

-- Wikipedia

Breaking Out

JavaScript is no longer a web browser only language!

- Widgets
- Desktop Applications
- Spreadsheets
- PDFs / Documents in general
- Database Language
- In the end, a JavaScript engine can be easily integrated into any application!

  [C/C++, and languages that can interact, ie: Perl]

JSON - JS Object Notation

JSON is a subset of the object literal notation of JavaScript. Since JSON is a subset of JavaScript, it can be used in the language with no muss or fuss.

-- JSON.org

* Supported by almost every programming language that is in use today.

What Is A DDoS Attack

A distributed denial of service attack (DDoS) occurs when multiple systems flood the bandwidth or resources of a targeted system, network, adjacent network facility. Usually the targets are one or more web servers.

This is the result of multiple compromised systems (for example a botnet) flooding the targeted system(s) with traffic.

When a server is overloaded with connections, new connections can no longer be accepted.

-- Wikipedia Definition [mostly]

Anatomy of a DDoS

All denial of service attacks have a goal to achieve, very few large scale attacks are "for fun".

The main reasons are:

- Extortion
- Removing Competition
- Political / Activism

DDoS Anatomy

Every DDoS attack is structured.
Typically composed of the following:

- Contention
- Campaign
- Command & Control
- Implementation

Contention

A contention is your reason for attacking.
Somehow your target is the reason for strife in your world.

Let us re-visit the main reasons:

- Extortion
  - They haz money you want!
- Removing Competition
  - They haz money you should have!
- Political / Activism
  - They haz your Playstation!

Campaign

A campaign or mission is the current battle in the war.

At this point you are going to identify the targets that need to be "altered".

Command & Control

Command and control, or C2, in a military organization is the exercise of authority and direction by a properly designated commanding officer over assigned and attached forces in the accomplishment of the mission. The term may also refer to command and control systems within a military system.

-- Wikipedia

Implementation

At this layer the C2 will tell the troops how to attack the target(s).

In the DDoS world, you will define the types of attacks, and depending on the properties of a participating bot's environment could determine the attack vector.

You can't tell a ground tank to fly to a location on its own.

Coming Together

So how does this come together?

What was the point of all of this gibberish about a programming language?

Why do we care?

Why Is JavaScript Dangerous?

So what is the big deal?

What makes JavaScript so different from any other language?

Why Is JavaScript Dangerous?

JavaScript can run almost anywhere!

JavaScript can run on almost every device, many that most people carry on themselves today. (cell phone, tablet, PC, watches*)

JavaScript can run almost anywhere, on any device and any platform and within many applications.

JavaScript is fast enough with the right engine.

Why Is JavaScript Dangerous?

JavaScript does not have to be signed in order to be executed!

JavaScript Signing Exists

* JavaScript supposedly can be signed, but who does that? I haven't noticed it anywhere!

* Useless, made for Netscape Navigator 4 and hasn't been expanded for present day threats:

http://www.mozilla.org/projects/security/components/signed-scripts.html

Even if this was used, it would not impact much, if anything that is covered in this presentation.

Language Focus

Even though this presentation is about JavaScript, the problems here are still universal.

JavaScript is just too easy to pick on today. Lots of XSS to be had.

Policies need to be updated and ENFORCED.

JavaScript Is Ripe

So we now know JavaScript is pretty much everywhere, and it will continue to creep into more applications and be in every device.

Tools are already showing up in the wild:
LOWC - Low Orbit Web Cannon

LOWC is simple, this tool and other tools are bound to get more complex.

Securing JavaScript: Almost..

Implement Strict Mode: This will add a layer of encapsulation.

*Not fully supported and some odd behaviour from many browsers.

https://developer.mozilla.org/en-US/docs/JavaScript/Reference/Functions_and_function_scope/Strict_mode#.22Securing.22_JavaScript

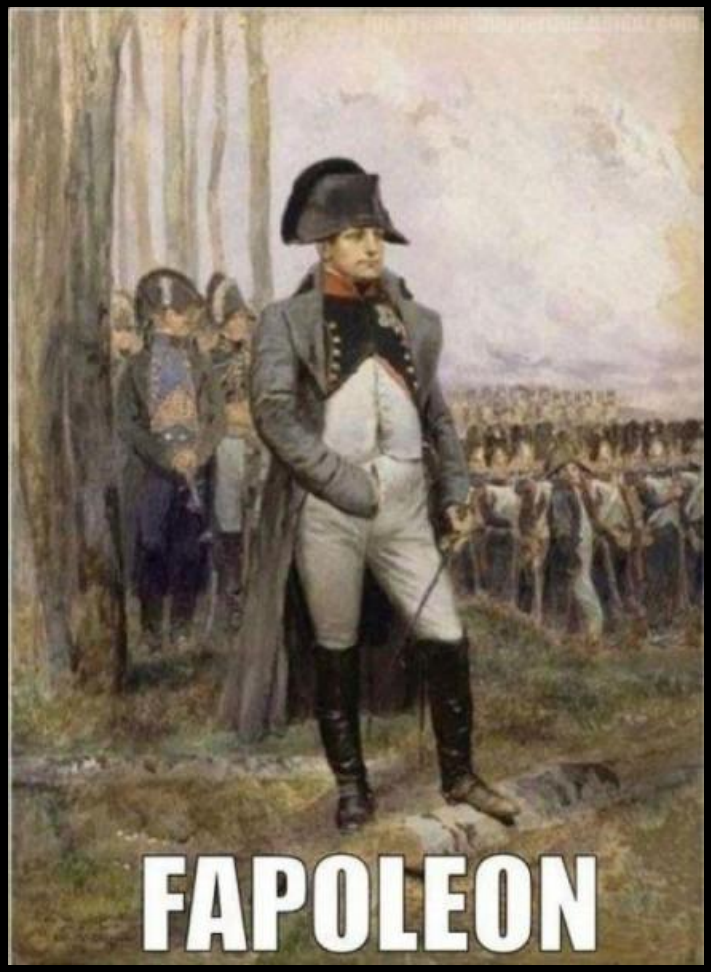
This will help secure the script, but it is only a start.

MOAR FUN

These methods have already been applied in the "wild".

Browser Exploitation Framework
http://beefproject.com/

FAP - For All Platforms



FAP - For All Platforms

FAP is a proof of concept, not a full scale war kit.

This demonstration is contained in a sandbox environment. No websites outside of this sandbox will be harmed.

If your or someone uses FAP to attack anyone outside of a sandbox environment, that is your own ass! I will not be responsible for anyones stupidity!

THIS TOOL IS FOR EDUCATIONAL PURPOSES ONLY!

C2 Features

Define Campaigns
Define Targets
Define Attack Types
Attack Management
Flexible and Dynamic control of your botnet

Injection - Deployment

This is for you to determine / figure out.

In short, find a way to inject your code.

Demo - Post Flood

DEMO - Attack Script

Post Flood

Get Flood

Details of A Get Flood

Information Gathering

Download

www.fapddos.com

Prior Art

Securing JavaScript - Douglas Crockford

http://vimeo.com/54087885

jgrahamc

http://www.slideshare.net/jgrahamc/javascript-security-2064979

Thank You

Questions?