Copy-paste Vulnerabilities

August 26, 2016

Vanessa Henderson

Who Am I?

- Vanessa Henderson
- AUT University Graduate
- Security Researcher at SourceClear
- Pokemon Trainer

Overview

- What is a copy-paste vulnerability (CPV)?
- Finding CPVs
- Case Study
- Recommendations
- Questions

Copy-Paste Vulnerabilities

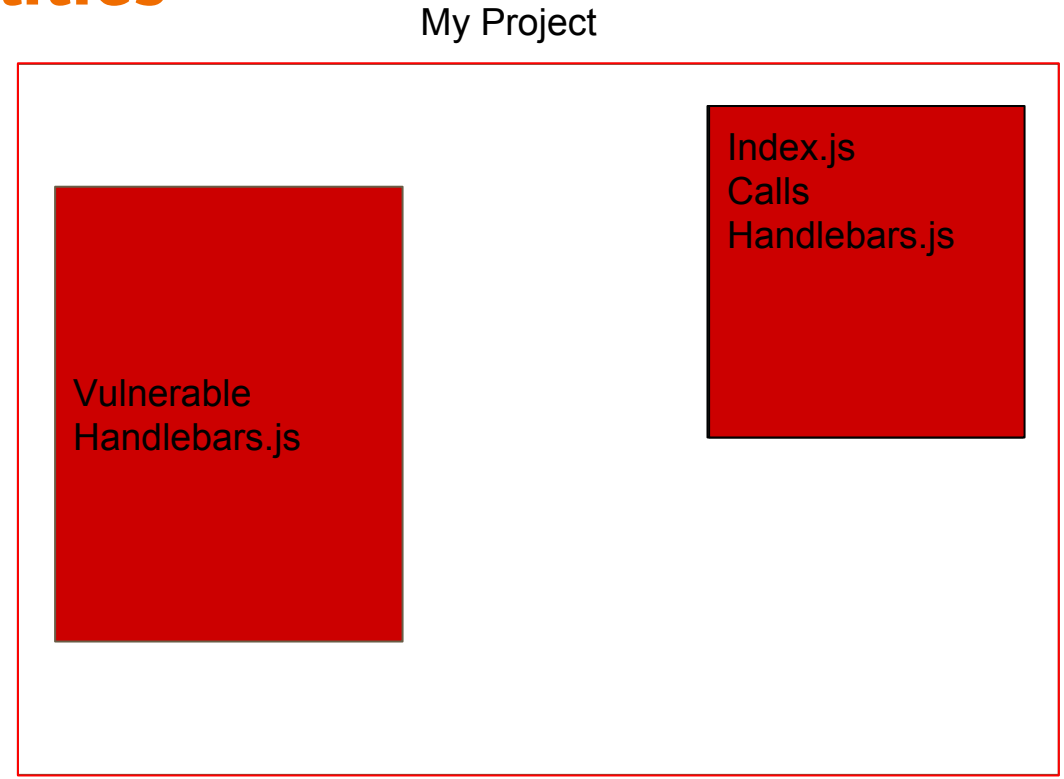
What are they?

- Vulnerable dependency or code slice is taken and copied into another project.

3 different ways of creating a CPV in your project

Copy-Paste Vulnerabilities

- Full Dependency



Copy-Paste Vulnerabilities

- Code Snippets

Random.java

```
public int generateRandom(){
   return Math.Random();
}

public void anotherMethod(){
   …
}
```

ID.java

```
public int createRandomID(){
   String number = “”;
   for( int i = 0; i <=8; i++){
         Number += generateRandom();
    }
   return number;
}

public int generateRandom(){
   return Math.Random();
}
```

Copy-Paste Vulnerabilities

- Code Snippets

/^[0-9a-f]{24}$/i → /\A[0-9a-f]{24}\z/i

- Uses new line instead of end of String
- Vulnerable to XSS

Copy-Paste Vulnerabilities

- Porting between languages

mustache.js

```
const escape = {
  '&': '&amp;',
  '<': '&lt;',
  '>': '&gt;',
  '"': '&quot;',
  "'": '&#x27;',
  '`': '&#x60;'
};
 const badChars = /[&<>"'`]/g,
        possible  = /[&<>"'`]/;
```

Escapers.java

```
/** Escapes HTML entities. */
   public static final Mustache.Escaper HTML = simple(new
String[][] {
      { "&",  "&amp;" },
      { "'",  "&#39;" },
      { "\"", "&quot;" },
      { "<",  "&lt;" },
      { ">",  "&gt;" }
   });
```

Difficulties with identification

- Minification
- Concatenation into one file
- Code structure varies between languages

Copy-Paste Vulnerabilities

- Porting between languages

mustache.js

```
const escape = {
  '&': '&amp;',
  '<': '&lt;',
  '>': '&gt;',
  '"': '&quot;',
  "'": '&#x27;',
  '`': '&#x60;'
};
 const badChars = /[&<>"'`]/g,
        possible  = /[&<>"'`]/;
```

Escapers.java

```
/** Escapes HTML entities. */
   public static final Mustache.Escaper HTML = simple(new
String[][] {
      { "&",  "&amp;" },
      { "'",  "&#39;" },
      { "\"", "&quot;" },
      { "<",  "&lt;" },
      { ">",  "&gt;" }
   });
```

Identification

- String matching
- Hash matching files

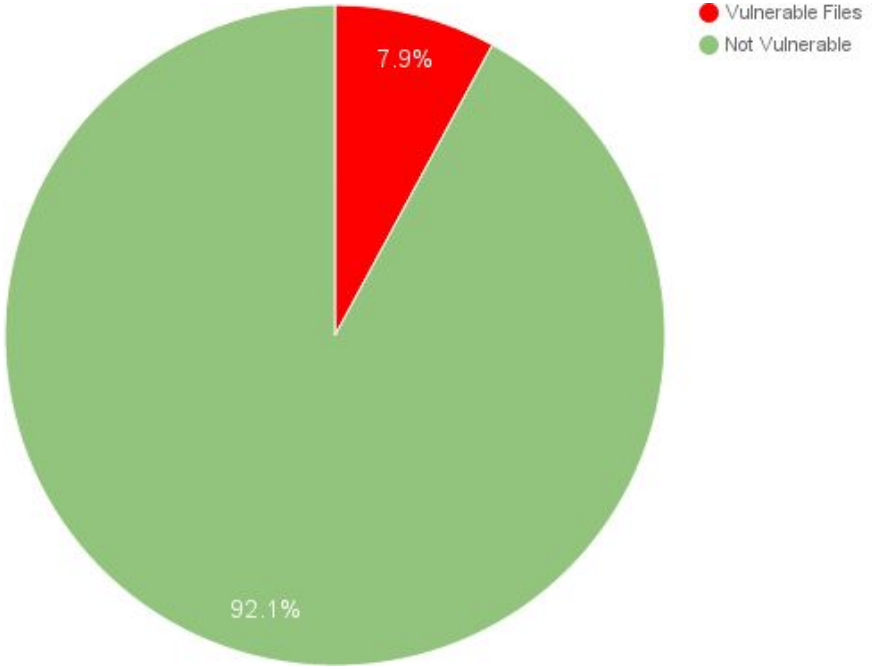
```java
/**
 * Clone and hash the js files in the respository
 * @param remoteURL
 * @param localPath
 * @return A set containing all hashes of the javascript files
 */
public HashMap<String,String> cloneAndHashRepository(String remoteURL, File localPath){
    HashMap<String,String> hashes = new HashMap<>();
    repoStrings = new HashMap<>();

    Git result = null;
    try {
        result = Git.cloneRepository()
                .setURI(remoteURL)
                .setDirectory(localPath)
                .call();
```

Case Study

- 15 vulnerable JavaScript files
  - 5 Cross-site Scripting (XSS) vulnerabilities
  - 10 Regular Expression Denial of Service (ReDoS) vulnerabilities
- 1 vulnerable C library
  - Out of Memory Denial of Service (DoS)
- 8000 Top GitHub Repositories
  - PHP, JAVA, JavaScript, HTML, Python, Ruby, C, C++

Case Study

- Vulnerable files found in over 600 popular projects

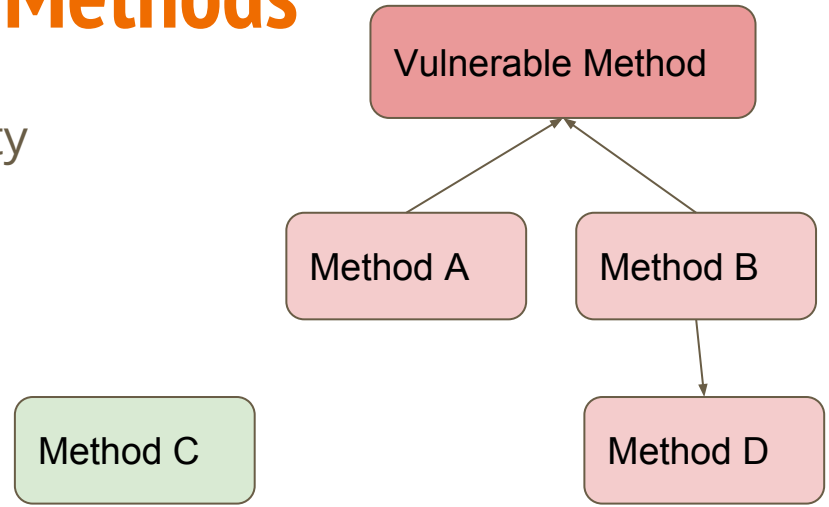


Case Study - Vulnerable Methods

- Not exploitable unless they use the affect code.

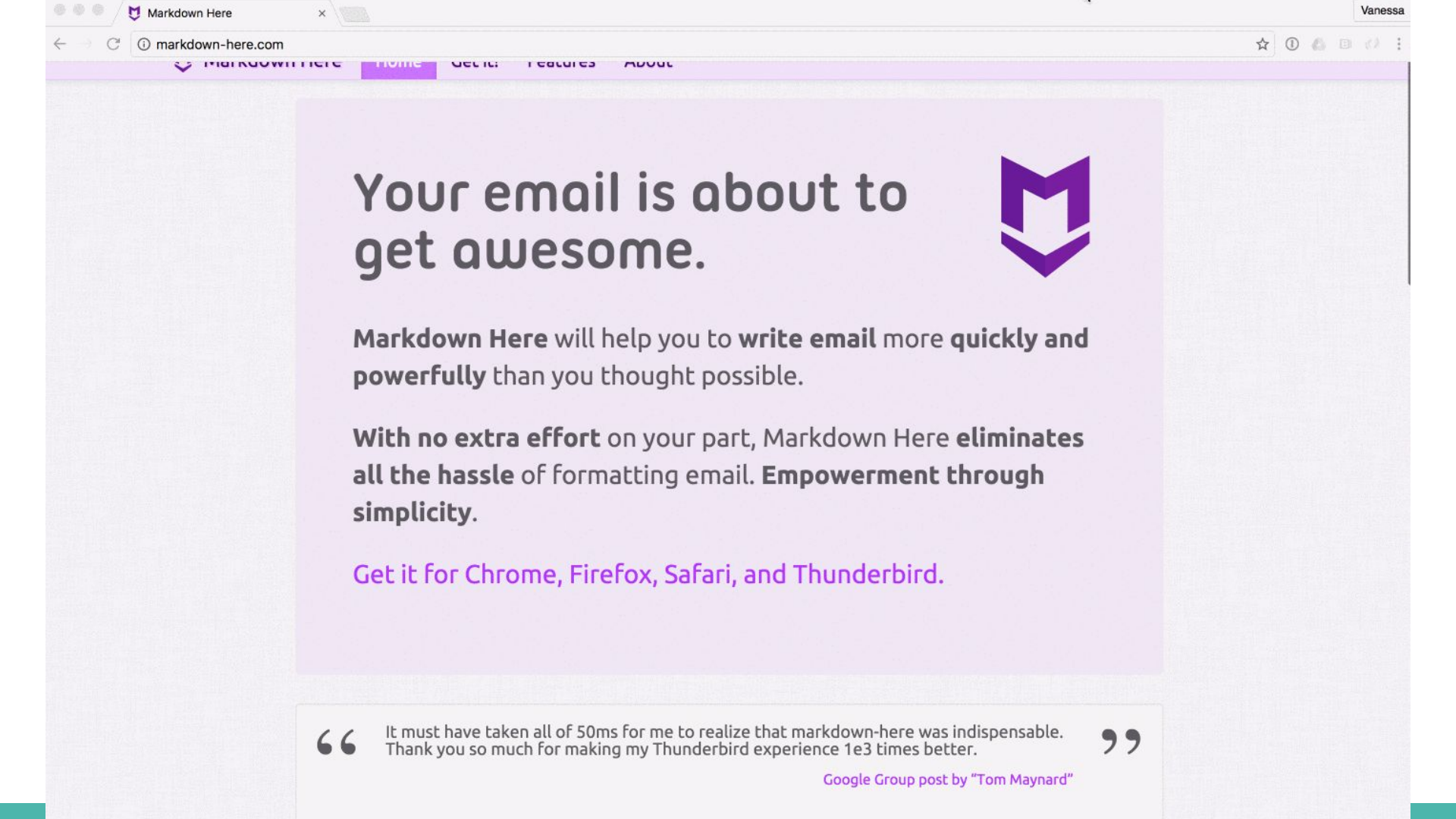
Case Study - Vulnerable Methods

1. Identify root cause of vulnerability
2. Find call chains to root method
3. Evaluate project using call chains



Case Study - Disclosures

- Total of 42 Disclosures
- adam-p/markdown-here demo
  - Vulnerable to a regular expression denial of service vulnerability


Markdown Here
Vanessa
markdown-here.com
Home
Get it!
Features
About
Your email is about to get awesome.
Markdown Here will help you to write email more quickly and powerfully than you thought possible.
With no extra effort on your part, Markdown Here eliminates all the hassle of formatting email. Empowerment through simplicity.
Get it for Chrome, Firefox, Safari, and Thunderbird.
It must have taken all of 50ms for me to realize that markdown-here was indispensable. Thank you so much for making my Thunderbird experience 1e3 times better.
Google Group post by "Tom Maynard"

Case Study - Disclosures

- Yui
- Handlebars-runtime
- Ember-precompile
- Nginb
- Markdown-here
- Templatify
- Assembly
- Malcolm
- Handlebars-serializer
- Backbone.Marionette.Handlebars
- Reid-selleck
- Ember-handlebars
- elFinder
- Uikit
- webogram

- No-CMS
- Grunt-ember-handlebars
- Grunt-static-handlebars
- Mimosa-emblem
- ss-handlebars
- Requirejs-template-plugins
- Webxhbs
- Selleck
- Assembly
- Nginb
- Awt-grunt-ember-handlebars
- Handlebars-commonjs
- Mimosa-ember-compiler-1.8
- Ember-templates
- component-builder-hbs

Recommendation for Prevention Techniques

- Don’t hard copy dependencies
- Use a package manager

```
blog master ❯ npm install
npm WARN deprecated minimatch@0.2.14: Please update to minimatch 3.0.2 or higher to avoid a RegExp DoS issue
npm WARN deprecated minimatch@0.3.0: Please update to minimatch 3.0.2 or higher to avoid a RegExp DoS issue
```

Further Study Opportunities

- Cross language identification
- Transitive copy-paste vulnerability search

Questions?

Contact information:

Twitter: @TheFruityKiwi