HATFIELDS AND MCCOYS
FEUDS, ANTI-PATTERNS AND OTHER CROSSED-CONNECTIONS IN THE DEV/SEC RELATIONSHIP
Chapter 1: Introduction

Welcome

Welcome to the CSA Field Manual!

In this manual, we will be covering the basics that you'll find useful during your time at the Cyber Security Agency. By no means is this a thorough education; you will need to look things up for yourself, particularly as you progress, but this guide will help you through over half of the levels and work as a reference.

We'll start you off with a quick introduction to the virtual machine, how to get setup and some basic usability tasks such as getting your keyboard mapping right. After that, we'll be taking you through a whirlwind tour of Linux, Programming, Web Attacks, Binary Attacks, Cryptography, and Forensics.
import sublime
import sublime_plugin

def plugin_loaded():
    # Ugly hack for icons in ST3
    kudos:
github.com/facelessuser/BracketHighlighter/blob/Bh2ST3/bh_core.py#L1380

    from os import makedirs
    from os import exists, join

    icon_path = join(sublime.packages_path, "Theme - Default")
    if not exists(icon_path):
        makedirs(icon_path)

class GitGutterCommand(sublime_plugin.WindowCommand):
    region_names = ['deleted_top', 'deleted_bottom',
                    'deleted_dual', 'inserted', 'changed']

    def run(self):
        self.view = self.window.active_view()
        if not self.view:
            # View is not ready yet, try again later.
            sublime.set_timeout(self.run, 1)

            return

        self.clear_all()  # self.inserted, modified, deleted = ViewCollection.diff(self.view)

        self.lines_removed(deleted)
UNLESS YOU ARE BREAKING STUFF, YOU ARE NOT MOVING FAST ENOUGH.
There's a package for that
DEPENDENCY TREES

API BACK END

```
"dependencies": {
  "bcrypt": "^1.0.3",
  "body-parser": "^1.18.2",
  "connect-mongo": "^2.0.1",
  "express": "^4.16.2",
  "express-session": "^1.15.6",
  "mongoose": "^5.0.0-rc2",
  "validator": "^9.2.0"
}
```

FRONT END

```
"dependencies": {
  "axios": "^0.17.1",
  "bootstrap": "^4.0.0-beta.2",
  "bootstrap-vue": "^1.4.1",
  "querystring": "^0.2.0",
  "vue": "^2.5.2",
  "vue-router": "^3.0.1"
}
```
DEPENDENCY TREES

API BACK END – 282 LINES

FRONT END – 69 LINES
## DEPENDENCY TREES

### API BACK END

<table>
<thead>
<tr>
<th>Description</th>
<th>LOC</th>
<th>Files Counted</th>
</tr>
</thead>
<tbody>
<tr>
<td>SLOC</td>
<td>926</td>
<td></td>
</tr>
<tr>
<td>Lines of Comments</td>
<td>41</td>
<td></td>
</tr>
<tr>
<td>Blank lines</td>
<td>107</td>
<td></td>
</tr>
<tr>
<td>Total LOC</td>
<td>967</td>
<td></td>
</tr>
</tbody>
</table>

### FRONT END

**Mine**

<table>
<thead>
<tr>
<th>Description</th>
<th>LOC</th>
<th>Files Counted</th>
</tr>
</thead>
<tbody>
<tr>
<td>SLOC</td>
<td>955</td>
<td></td>
</tr>
<tr>
<td>Lines of Comments</td>
<td>21</td>
<td></td>
</tr>
<tr>
<td>Blank lines</td>
<td>145</td>
<td></td>
</tr>
<tr>
<td>Files Counted</td>
<td>14</td>
<td></td>
</tr>
<tr>
<td>Total LOC</td>
<td>976</td>
<td></td>
</tr>
</tbody>
</table>

**Not Mine**

<table>
<thead>
<tr>
<th>Description</th>
<th>LOC</th>
<th>Files Counted</th>
</tr>
</thead>
<tbody>
<tr>
<td>SLOC</td>
<td>202240</td>
<td></td>
</tr>
<tr>
<td>Lines of Comments</td>
<td>83799</td>
<td></td>
</tr>
<tr>
<td>Blank lines</td>
<td>41829</td>
<td></td>
</tr>
<tr>
<td>Files Counted</td>
<td>2437</td>
<td></td>
</tr>
<tr>
<td>Total LOC</td>
<td>280839</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Description</th>
<th>LOC</th>
<th>Files Counted</th>
</tr>
</thead>
<tbody>
<tr>
<td>SLOC</td>
<td>1261218</td>
<td></td>
</tr>
<tr>
<td>Lines of Comments</td>
<td>385167</td>
<td></td>
</tr>
<tr>
<td>Blank lines</td>
<td>233378</td>
<td></td>
</tr>
<tr>
<td>Files Counted</td>
<td>12008</td>
<td></td>
</tr>
<tr>
<td>Total LOC</td>
<td>1646385</td>
<td></td>
</tr>
</tbody>
</table>
Express 4 came out in April 2014. **17 months** to transition.

Significant breaking changes between 3 and 4.
DEPRECATION NOTICE

I don’t want to maintain this module anymore since I just use minimist, the argument parsing engine, directly instead nowadays.

See yarg for the modern, pirate-themed successor to optimist.

Maybe if we ask nicely, they’ll just give us their riffiwboggles!

Pirate Joe, the eternal optimist

47th most depended-upon package on npm.

Last updated Feb 2014.
ROOT CAUSE

WHAT ARE YOU DOING?
DEBUGGING

GOTCHA!

REAL PROBLEM

OH SHIT
WHO ELSE...

✓ Searches for high impact bugs missed by dev teams
✓ Tests minutia of a system, including unexpected interactions and edge cases
✓ Is shunted to the far right of the lifecycle
✓ Acts as gatekeeper and bearer of bad news
✓ Is rarely invited into the planning stages
✓ Rarely represented or integrated into the dev team
✓ Often the first to get “automated” away
QUALITY ASSURANCE
WHO ELSE...

✓ Provides vague requirements
✓ Which suddenly get very specific at the last minute
✓ Need to “see” something finalized before they can provide feedback or review
✓ Rarely participates more than superficially in planning
✓ Single-mindedly pursues an agenda while often ignoring other contexts or considerations
SECURITY CREEP
Agent Directory

1. Touching "Home" will take user back to homepage.
2. Touching Search Box will bring up keyboard. As letters are entered, results are filtered live below.
3. Office Contact will be at top of page. Touching will take user to Profile page with office contact information.
4. Touching an agent's name will take user to that agent's profile page.
5. If user came from Agent Directory, button will read "Directory". Touching will take user back to the Agent Directory page.
6. If user came from Homepage, button will say "Home". Touching will take user back to homepage.
7. If agent profile, display agent picture. If office profile, display office app.
8. Touching "Call Me" will take user to GPS app with this address presented.
9. Touching "Text Me" will take user to Text app with agent-office number presented. (Functionality can be disabled by Rezort/Office.)
10. Touching any form field will bring up keyboard. All fields required.
11. Touching "Send" will send message to agent. System will file message as a Mobile Lead in Work Station.

Profile

1. Profile page with profile picture.
2. Jane Doe
3. My Slogan is Best
4. Best Realty Group
5. 12301 104 Street
6. Edmonton, AB
7. T9X 0G0
8. Call Me
9. Text Me
10. Email Me:
   
   First Name:
   Last Name:
   Phone:
   Message:

Form Builder Field Config: Text Input

1. Configure Field pane. This will appear when the user clicks on any of the field container in the Form Preview pane. Changes made should update live in the Form Preview pane.
2. Label/Text editor. Allows agent to modify the text input label. "Text Label" by default.
5. Required Field option. Allows the agent to specify if this is a required field. If unchecked, the field is optional and can be submitted when this field is blank.
6. Show Advanced Settings option. Closed by default. Clicking this will expand the Configure Field pane down and show the Advanced Configuration options.
7. Cancel. If the agent clicks this, the Configure Field pane will disappear and the field will revert to its previous state in the Form Preview.
8. Save button. If the agent clicks this, the Configure Pane will disappear and the field will save with the configurations as set.
Average Developer Experience

Stack Overflow 2016 Survey
56,000 Responses in 173 Countries

- < 1 years: 5.8%
- 1 – 2 years: 12.4%
- 2 – 5 years: 32.1%
- 6 – 10 years: 23.2%
- 11+ years: 26.5%

50.3% have 5 years or less experience
How long have you been using Node.js?

NodeSource 2017 Survey
(Unknown # Responses)

- < 1 years: 19%
- 1 – 2 years: 25%
- 3 – 4 years: 38%
- 5 – 6 years: 14%
- 6+ years: 4%

82% have 4 years or less experience. 44% have 2 years or less.
SECURITY COWORKER

Some general rules:
1. Put all uploaded files into a folder, disable running of PHP in that folder with an .htaccess rule.
2. Don't allow filenames that include 'php'.
3. Restrict files by extension.
4. Check the mime type with finfo_file
5. Rename the image on upload
6. Use move_uploaded_file()
7. Make sure an upload cannot overwrite the .htaccess file in your uploads folder
We need some new jargon, the public are starting to understand what we're talking about!
HOW TO SHIFT LEFT
ADVICE FROM SOMEONE WHO IS SHIFTING RIGHT

✓ Code is not a spectator’s sport.
  • Know at least as much about the language as a brand new junior developer.
  • Help me with the weird security quirks of my language I won’t think to look for, ie: preg_replace in php and REDOS risks in js.

✓ Know your what your team’s libraries and middleware does.
  • This is the best place to start making secure code a default.
  • Help us select and build systems to manage dependencies.
  • Ask for prototypes to pen test dependencies early.
HOW TO SHIFT LEFT
ADVICE FROM SOMEONE WHO IS SHIFTING RIGHT

✔ Learn how to write tests.
  • Add specific cases for security.

✔ Be part of early stage planning.
  • Speak my language: not just code, but business requirements, user stories, etc.
  • Put explicit security acceptance criteria into user stories and requirements.
  • “Pen test” a wireframe.

✔ Train – and learn from – your QA team.
  • Good QA people have a lot of experience pushing left, making their expectations known early, and creating good working relationships with developers.
HOW TO SHIFT LEFT
ADVICE FROM SOMEONE WHO IS SHIFTING RIGHT

✔ Help us create good, useful, uncluttered logs.
✔ Your suggestions – and timing - have broader implications than just security.
  • Security changes rarely make code simpler or easier to understand.
  • Tired, overworked developers write worse code. Backending risk is another form of scope creep.
  • Opaque UI and errors can cause major support headaches.
QUESTIONS?