MIS|TI™ PRESENTS

InfoSecWorld

Conference & Expo 2018

ATTACK DRIVEN DEVELOPMENT

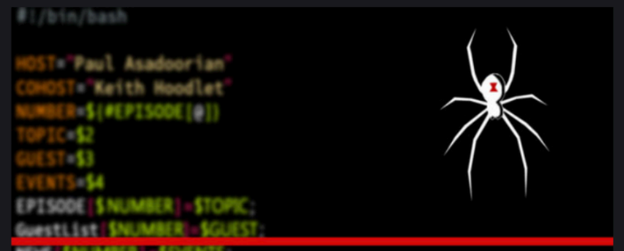
Keith Hoodlet

Trust & Security Engineer, Bugcrowd

@andMYhacks

```
001     function biography( author ) {
002         author.experience = {
003             "title" : "Trust & Security Engineer",
004             "company" : "Bugcrowd",
005             "misc" : "Host, Application Security Weekly",
006             "history" : "InfoSec Hobbyist (1996-2014)",
007             "other_experiences" : {
008                 "Rapid7" : "Customer Success Engineer",
009                 "Veracode" : "Intern, Code Security Engineering"
010             }
011         }
012
013         author.beginnings = {
014             "game" : "Diablo",
015             "platform" : "Battle.net",
016             "protocol" : "Telnet",
017             "language" : "Visual Basic"
018         }
019     };
```

bugcrowd



```
013         author.beginnings = {
014             "game" : "Diablo",
015             "platform" : "Battle.net",
016             "protocol" : "Telnet",
017             "language" : "Visual Basic"
018         }
019     };
020
021
022     function why_add( focus, learning ) {
023         focus.change = {
024             "from" : "Software Development",
025             "to" : "Web Application Security"
026         }
027
```

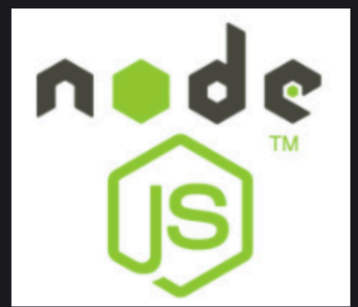
```
023         focus.change = {
024             "from" : "Software Development",
025             "to" : "Web Application Security"
026         }
027
028         learning.involves = {
029             "dedication" : "a sense of purpose",
030             "practicing" : {
031                 "tools" : "Burp / ZAP / Docker",
032                 "languages" : "HTLM / CSS / JS",
033                 "frameworks" : "Angular / React / Node"
034             },
035             "repetition" : "reinforcing acquired knowledge"
036         }
037     };
038
039     // And you don't want to get Rusty
```







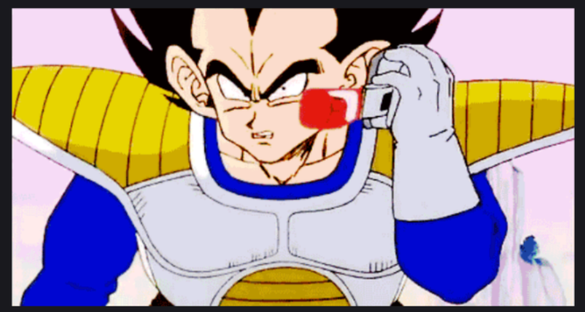


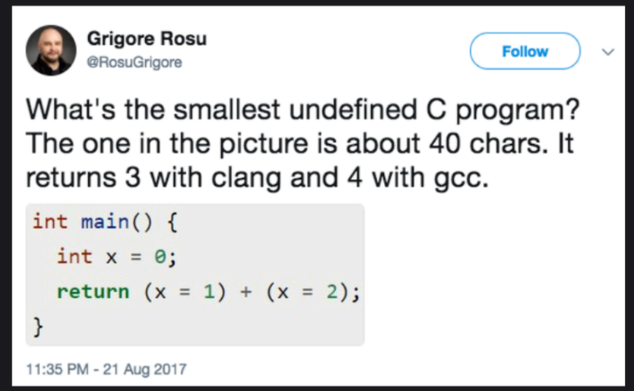

InfoSecWorld
Conference & Expo 2018

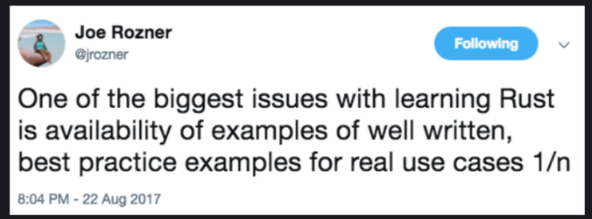
```
037     };
038
039     // And you don't want to get Rusty
040
041
042     function differences( method ) {
043         if (method == "TDD") {
044             method.focus = "testable development";
045             method.goals = "acceptable behavior (happy path)";
046             method.outcomes = "productive developers";
047             method.indifferent_toward = "security";
048         } else if (method == "Misuse & Abuse Cases") {
049             method.developed = "circa 2004 by Cigital & NCSU";
050             method.intended_use = "Waterfall Development";
051             method.outcomes = "secure design";
052             method.lacks = "integrated security testing";
053         } else if (method == "Attack Driven Development") {
054             method.intended_use = "Agile Development";
055             method.focus = "learning security features";
056             method.goals = "secure development & continuous testing";
057             method.outcomes = "Cont. testing 'Misuse & Abuse' cases";
```

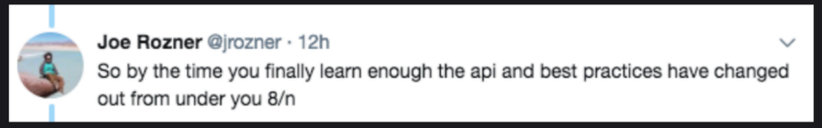
```
061
062     function when_to_use_add( attack_driven, dev_stack ) {
063         if (dev_stack.involves == "Web Applications") {
064             dev_stack.foundation = "Fairly stable (HTML / CSS / JS)";
065             dev_stack.complexity = "Conceptually simple";
066             dev_stack.prototyping = "Relatively easy";
067             dev_stack.information = "Widely available (and free!)";
068             attack_driven.effectiveness = "It's over 9000!?";
069         } else if (dev_stack.involves == "Greenfield Project") {
070             dev_stack.foundation = "Determined by dev resources";
071             dev_stack.complexity = "Conceptually simple (at first)";
072             dev_stack.prototyping = "Generally drives decisions";
073             dev_stack.information = "Helps determine the stack";
074             attack_driven.effectiveness = "Informative";
075         } else if (dev_stack.experience == "Novice") {
076             dev_stack.knowledge = "Compiling...";
077             dev_stack.prototyping = "Valuable for gaining knowledge";
078             dev_stack.information = "Needs to be accessible";
079             attack_driven.effectiveness = "Fast & Iterative";
080         }
081     };
```



```
085     function when_to_avoid_add( app, attack_driven, dev_stack ) {
086         if (dev_stack.includes == "Undefined Behavior") {
087             app.foundation = "tenuous at best";
088             app.complexity = "requires deep knowledge";
089             app.prototyping = "relatively difficult";
090             app.information = "generally conflicting";
091             attack_driven.effectiveness = null;
092         } else if (dev_stack.lacks == "Practical Examples") {
093             dev_stack.foundation = "under construction";
094             dev_stack.complexity = "divide by zero";
095             dev_stack.prototyping = "assembling Ikea w/o instructions";
096             dev_stack.information = "likely enigmatic";
097             attack_driven.effectiveness = "tread carefully";
098         } else if (dev_stack.status == "Incomplete") {
099             dev_stack.knowledge = "continuously out-of-date";
100             dev_stack.prototyping = "breaks with new versions";
101             dev_stack.information = "chaotic neutral";
102             attack_driven.effectiveness = "short-lived";
103         }
104     };
105
```







```
function building_your_lab( app ) {
    if (app.location == "localhost") {
        app.tools = {
            "native" : "NodeJS",
            "virtual" : {
                "contained" : "Docker",
                "staging" : "Vagrant",
                "full-featured" : "VMware / VirtualBox"
            },
            "environment" : {
                "editor" : "VS Code",
                "IDE" : "WebStorm",
                "browser" : "Firefox",
                "addons" : "Several"
            },
            "attack" : {
                "free" : "OWASP ZAP",
                "free" : "Postman",
                "paid" : "Burp Suite Pro"
            }
        };
```

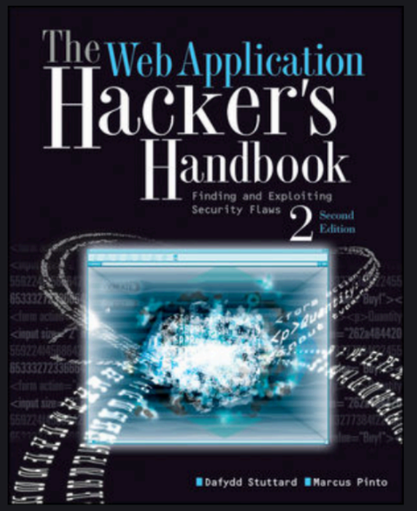
InfoSecWorld
Conference & Expo 2018

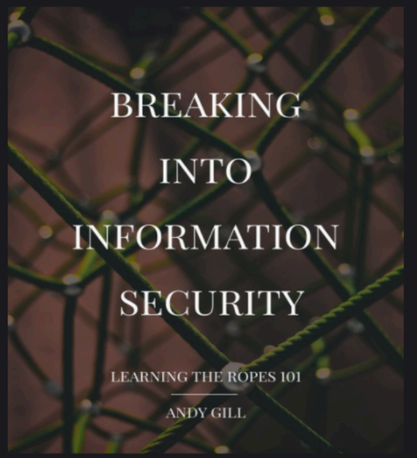
```
136         } else if (app.location == "The Cloud") {
137             app.tools = {
138                 "Linux" : "AWS",
139                 "Microsoft" : "Azure",
140                 "other" : "Heroku"
141             };
142
143             app.considerations = {
144                 "cost" : "minor",
145                 "legality" : "questionable",
146                 "interference" : "built-in protections by the provider",
147                 "recommendation" : "don't (at least, not at first)"
148             };
149         }
150     }
```

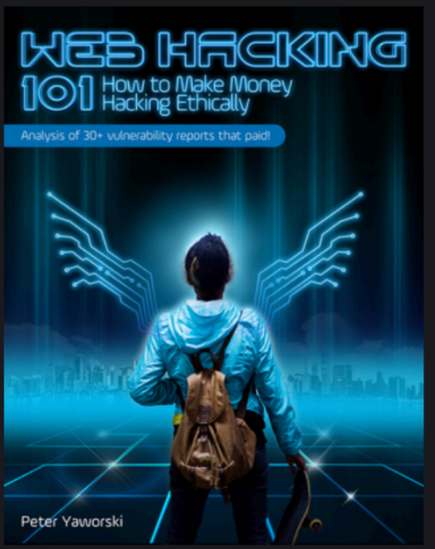
```
150     }
151
152
153     function who_benefits( description, reasons ) {
154         if (description == "Security Engineer") {
155             reasons.include = {
156                 "responsibilities" : "scope creep",
157                 "dependencies" : "Agile Development",
158                 "value" : "career growth opportunities"
159             };
160         } else if (description == "Developer") {
161             // developers developers developers...
162             reasons.include = {
163                 "responsibilities" : "feature development & deployment",
164                 "dependencies" : "security is now your problem, too",
165                 "value" : "more features, less fixes"
166             };
```

```
166             };
167         } else if (description == "Student") {
168             reasons.include = {
169                 "responsibilities" : "learn",
170                 "dependencies" : "time",
171                 "value" : "hiring potential increases"
172             };
173         }
174     };
```

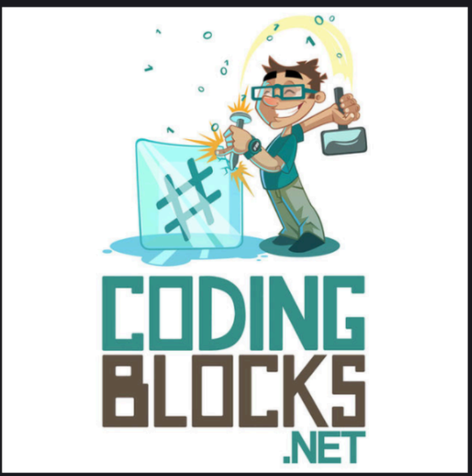
```
176
177     function getting_started( resources ) {
178         resources.books = {
179             "Web Application Hacker's Handbook" : {
180                 "Author" : "Dafydd Stuttard",
181                 "Co-Author" : "Marcus Pinto"
182             },
183             "Web Hacking 101" : {
184                 "Author" : "Peter Yaworski"
185             },
186             "Breaking into Information Security" : {
187                 "Author" : "Andy Gill"
188             }
189         };
190
191
```







```
193         resources.podcasts = {
194             "Source Code podcast" : {
195                 "Host" : "Chris Sanders",
196             },
197             "Exploring Information Security" : {
198                 "Host" : "Timothy DeBlock"
199             },
200             "Coding Blocks" : {
201                 "Host" : "Joe Zack",
202                 "Co-Host" : "Michael Outlaw",
203                 "Co-Host" : "Allen Underwood"
204             },
205             "Software Engineering Radio" : {
206                 "Host(s)" : "SE-Radio Team"
207             }
208         };
```



```
209
210         resources.websites = {
211             "development" : {
212                 "documentation" : "https://devdocs.io",
213                 "docker" : "https://docs.docker.com",
214                 "node" : "https://nodejs.org"
215             },
216             "attack" : {
217                 "PortSwigger" : "https://portswigger.net",
218                 "Tim Tomes" : "http://www.lanmaster53.com",
219                 "Attack Driven (coming soon!)" : "https://attackdriven.io"
220             }
221         };
222     }
```

```
223
224
225     function final_thoughts( ) {
226         let thanks = {
227             "partner" : "Sarah Hoodlet",
228             "inspiration" : "Katie Ledoux",
229             "sensei" : "Jason Haddix"
231         };
232         let further_research = {
233             "Build it, Break it, Fix it" : "https://builditbreakit.org/",
234             "Underhanded C Contest" : "http://www.underhanded-c.org/",
235             "Getting Past the Positive" : {
236                 "link" : "https://www.cigital.com/papers/download/bsi2-misuse.pdf",
237                 "more" : "http://bit.ly/2G8gbop"
238             },
239             "Secure SDLC " : {
234                 "OWASP Cheat Sheet" : "http://bit.ly/1GrLqEp",
240                 "7 Phases of SDLC" : "https://www.microsoft.com/en-us/sdl/"
241             }
242         };
243     };
```

MIS|TI™ PRESENTS

InfoSec World

Conference & Expo 2018

THANK YOU

PLEASE FILL OUT YOUR EVALUATIONS!

Keith Hoodlet

Trust & Security Engineer, Bugcrowd

@andMYhacks