1700 - Introducing HUNT: Data Driven Web Hacking & Manual Testing

Saturday at 17:00 in Track 3
45 minutes | Demo, Tool
Jason Haddix*Head of Trust and Security @ Bugcrowd*

What if you could super-charge your web hacking? Not through pure automation (since it can miss so much) but through powerful alerts created from real threat intelligence? What if you had a Burp plugin that did this for you? What if that plugin not only told you where to look for vulns but also gave you curated resources for additional exploitation and methodology? What if you could organize your web hacking methodology inside of your tools? Well, now you do! HUNT is a new Burp Suite extension that aims to arm web hackers with parameter level suggestions on where to look for certain classes of vulnerabilities (SQLi, CMDi, LFI/RFI, and more!). This data is parsed from hundreds of real-world assessments, providing the user with the means to effectively root out critical issues. Not only will HUNT help you assess large targets more thoroughly but it also aims to organize common web hacking methodologies right inside of Burp suite. As an open source project, we will go over the data driven design of HUNT and it's core functionality.
Jason Haddix
Jason is the Head of Trust and Security at Bugcrowd. Jason trains and works with internal security engineers to triage and validate hardcore vulnerabilities in mobile, web, and IoT applications/devices. He also works with Bugcrowd to improve the security industries relations with the researchers. Jason's interests and areas of expertise include mobile penetration testing, black box web application auditing, network/infrastructure security assessments, and static analysis. Jason lives in Santa Barbara with his wife and three children. Before joining Bugcrowd Jason was the Director of Penetration Testing for HP Fortify and also held the #1 rank on the Bugcrowd leaderboard for 2014.

@jhaddix

Contributor Acknowledgement:
The Speaker would like to acknowledge the following for their contribution to the presentation.

JP Villanueva is a Trust & Security Engineer at Bugcrowd. Before Bugcrowd, JP spent 2 years as an Application Security Engineer and another 2 years as a Solutions Architect at WhiteHat Security helping customers become more secure. JP has also presented at OWASP and

Interop DarkReading events. In his free time, JP enjoys playing classic video games and hacking on bug bounty programs.

Fatih is an Application Security Engineer at Bugcrowd and Bug Hunter located in Istanbul/Turkey. Before Bugcrowd, he was a security consultant at InnoveraBT and performed penetration testing for clients including government, banks, trade, and finance companies. His expertise includes network, web applications, mobile security assessments, and auditing. He also holds OSCP, OSCE, GWAPT certifications.

Ryan Black is the Director of Technical Operations at Bugcrowd where he heads strategy and operations for the Application Security Engineering team. This group reviews and validates tens of thousands of vulnerability reports to bug bounty programs.

Prior to joining Bugcrowd, Ryan developed and led the static analysis and code review team for HP Fortify on Demand, later expanding to DevOps tooling and integrations for the enterprise. He has also held various InfoSec and technology positions at companies such as Aflac and Apple in the last decade. In addition to professional experience, he holds several industry certifications and participates in a variety of open source software projects and initiatives. On personal time he enjoys coding, gaming, various crafts, and nature activities with his wife, two kids, and three dogs.

Vishal Shah is an Application Security Engineer specializing in web and mobile security at Bugcrowd. Prior to Bugcrowd, Vishal spent time as a Security Consultant with Cigital hacking and building automation for hackers. In his free time, Vishal enjoys working out, CTFs, and playing video games.

#defcon25/by_track/track3/saturday #defcon25/By_Day/_saturday