1300 - Wiping out CSRF

Thursday at 13:00 in 101 Track 2
45 minutes | Art of Defense, Demo
Joe Rozner*Senior Software Security Engineer, Prevoty*

CSRF remains an elusive problem due to legacy code, legacy frameworks, and developers not understanding the problem or how to protect against it. Wiping out CSRF introduces primitives and strategies for building solutions to CSRF that can be bolted on to any http application where http requests and responses can be intercepted, inspected, and modified. Modern frameworks have done a great job at providing solutions to the CSRF problem that automatically integrate into the application and solve most of the conditions. However, many existing apps and new apps that don't take advantage of these frameworks or use them incorrectly are still plagued with this problem. Wiping out CSRF will provide an in depth overview of the various reasons that CSRF occurs and provide payload examples to target those specific issues and variations. We'll see live demos of these attacks and the protections against them. Next we'll look at how to compose these primitives into a complete solution capable of solving most cases of CSRF explaining the limits and how to layer them to address potential short comings. Finally we'll finish by looking at Same Site Cookies, a new extension to cookies that could be the final nail in the coffin, and see how to use the prior solution as a graceful degradation for user agents that don't support it yet.
Joe Rozner
Joe (@jrozner) is a software engineer at Prevoty where he has built semantic analysis tools, language runtimes, generalized solutions to common vulnerability classes, and designed novel integration technology leveraging runtime memory patching. He has a passion for reverse engineering, exploitation, teaching, and sharing research with others. He is the undisputed champion of the Brawndo and Booze competition from DEF CON s past with his Irish Car Mutilator winning in both the drink and dip categories.

@jrozner

#defcon25/by_track/101-Track2/Thursday #defcon25/By_Day/_thursday