1000 - There's no place like 127.0.0.1 - Achieving reliable DNS rebinding in modern browsers

Thursday at 10:00 in 101 Track
45 minutes | Demo, Tool, Exploit
Luke Young*Senior Information Security Engineer, LinkedIn*

Most people lock their doors at night, however if you walk into someone's home you likely won't find every piece of furniture bolted to the floor as well. We trust that if someone is inside our home they are supposed to be there. Unfortunately many developers treat local networks just the same, assuming all internal HTTP traffic is trusted, however this is not always the case. They incorrectly assume that their services will be protected by the same-origin policy in browsers, rather than implementing proper authentication mechanisms. By abusing this implicit trust we can gain access to confidential data and internal services which are not intended to be publicly accessible.

I will demonstrate that this is a poor security control and can be trivially bypassed via an older technique, DNS rebinding. The talk will cover how DNS rebinding works, the mitigations imposed by modern browsers and networks, and how each mitigation can be bypassed. I will discuss the notorious unreliability of DNS rebinding attacks that causes many developers to ignore the issue and how to overcome this unreliability.

Finally, I will examine a variety of popular services and tools to understand how they are affected by DNS rebinding. I will be releasing a tool that allows researchers to automate DNS rebinding attacks, the associated mitigation bypasses and generate drop-dead simple proof-of-concept exploits. I will demonstrate this tool by developing exploits for each vulnerable service, ending the talk by exploiting a vulnerable service to obtain remote-code execution, live.

Luke Young

Luke Young is a security researcher originally from the frozen plains of Minnesota who recently migrated to the much warmer state of California. He presented at DEF CON 23 on the topic of exploiting bitflips in memory, DEF CON 24 on the subject of large DDoS attacks and has investigated a variety of well-known products and network protocols resulting in numerous CVE assignments. He spends his free-time maintaining his position as one of the top researchers on various bug bounty platforms and is currently working as a Senior Information Security Engineer at LinkedIn.

@TheBoredEng

"https://bored.engineer

#defcon25/by_track/101/thursday
#defcon25/By_Day/_thursday