ANTHONY WEEMS

+1 512 565 6059 • amlweems@gmail.com

Last updated on July 28, 2020

EDUCATION

University of Texas at Austin September 2012 - December 2015
Bachelor of Science in Electrical and Computer Engineering

EXPERIENCE

Staff Security Engineer at Praetorian - Austin, TX January 2016 - Present

- Led complex product security assessments across cloud platforms, web applications, mobile applications, desktop applications, embedded systems, and vehicles
  - Developed risk-based approach focused on high impact vulnerabilities and custom attack paths, while still maintaining coverage guided by OWASP ASVS [1]
  - Contributed to over two hundred customer security assessments in tenure at the company
- Advised engineers on application security projects across the company to ensure consistent quality
- Lectured part-time for the *Ethical Hacking* class at the University of Texas at Austin [2]
- Led teams in development of internal tools and projects across the company
- Led architecture and development of internal web application security labs
- Created several internal web security challenges for training purposes
- Created a series of technical onsite interview challenges
- Created a public Internet of Things security challenge [3]

Senior Security Engineer at Praetorian - Austin, TX August 2014 - December 2015

- Performed web, mobile, and embedded security assessments
- Formed a vulnerability research team with a colleague, focused on fuzzing techniques and symbolic execution
- Created and developed a reporting system to produce clear, consistent, and actionable client deliverables
- Created public pwnable and machine learning security challenges [4] [5]

Intern at Praetorian - Austin, TX Summer 2013 and Summer 2014

- Shadowed and performed web / mobile application security assessments
- Contributed to the development of a public mobile application security product [6]
- Co-created a public online password cracking service [7]
- Co-created a set of public cryptography challenges [8]

DISTINCTIONS

2nd place in PortSwigger's Web Security Academy [9] as of July 28, 2020
Certified Kubernetes Administrator (CKA) [10] April 2020
Offensive Security Web Expert (OSWE) [11] July 2019

[1] https://github.com/owasp/asvs
[2] https://cs.utexas.edu/courses/378-ethical-hacking
[3] https://praetorian.com/challenges/iot-security-tech-challenge
[4] https://praetorian.com/challenges/pwnable
[5] https://praetorian.com/challenges/machine-learning
[6] https://neptune.praetorian.com
[7] https://mars.praetorian.com
[8] https://praetorian.com/challenges/crypto
[9] https://portswigger.net/web-security/hall-of-fame
[10] https://go.lf.lc/cka
[11] https://go.lf.lc/oswe

GIAC Web Application Penetration Tester (GWAPT) [12] October 2016
Stanford University Cryptography I September 2014

PUBLIC VULNERABILITIES

CVE-2015-5238: Stack Overflow in libtre5, also found by P0 [13]
CVE-2016-4991: Command Injection in nodepdf PDF rendering library [14]
CVE-2016-7063: Privilege escalation to root in Pritunl VPN client [15]
CVE-2016-7064: Man-in-the-middle compromise of Pritunl VPN client [16]
CVE-2018-2813: MySQL privilege esc via missing file access checks [17]
CVE-2019-1003040: Jenkins Groovy sandbox escape via type coercion [18]
CVE-2019-1003041: Jenkins Groovy sandbox escape via type coercion [19]

NOTABLE SIDE-PROJECTS

(All of the following can be found at github.com/amlweems)

- **gringotts**: proof of concept for CVE-2020-0601 (Windows ECC CA issue)
- **local-gce-metadata**: local implementation of the GCE metadata service
- **abci**: array-based command injection guide
- **stun**: TLS proxy with automated certificate provisioning based on SNI
- **atmin**: automatic test-base minification library (e.g. minimize http requests)
- **cert-welder**: a tool to show certificate chains from a collection of certificates
- **viewstateless**: encrypted viewstate generator
- **dnlog**: simple dns logging tool in the style of Burp Collaborator
- **cryptopals** (private): solutions to sets 1 through 7 of cryptopals
- **sandbox-escapes** (private): research into Java sandbox escapes
- **hexpand**: proof of concept hash length extension attack
- **maildump**: implementation of RFC 5321 for use as a catch-all email server

[12] https://go.lf.lc/gwapt
[13] https://lf.lc/CVE-2015-5238.txt
[14] https://lf.lc/CVE-2016-4991.txt
[15] https://lf.lc/CVE-2016-7063.txt
[16] https://lf.lc/CVE-2016-7064.txt
[17] https://lf.lc/CVE-2018-2813.txt
[18] https://lf.lc/CVE-2019-1003040.txt
[19] https://lf.lc/CVE-2019-1003040.txt