

# Benjamin Wolf

## EDUCATION

---

<b>M.Sc. in CyberSecurity</b>	2017
<i>Liberty University, Lynchburg, VA</i>	<i>GPA: 3.85</i>
<b>B.Sc. in Management Information Systems</b>	2011
<i>Penn State University, Harrisburg, PA</i>	<i>GPA: 3.5</i>

## CERTIFICATIONS

---

<b>Google Professional Cloud Security Engineer (PCSE)</b>	2024
<b>SANS GIAC Web Application Penetration Tester (GWAPT)</b> [Score: 98%]	2023
<b>SANS GIAC Security Essentials (GSEC)</b> [Score: 96%]	2022

## EXPERIENCE

---

### UPS InfoSec Vulnerability Management, Remote

*SR. PENTEST ANALYST*

*August 2022 – Present, Full-time*

- Participated in comprehensive web application and network penetration testing, identifying and remediating significant security vulnerabilities.
- Developed and implemented automated tools for penetration testing, significantly enhancing the efficiency and accuracy of the testing process.
- Processed bug bounty submissions, collaborating closely with application development teams to understand and address reported vulnerabilities efficiently.
- Acted as a Subject Matter Expert (SME) on offensive security capabilities, providing guidance to junior and senior pentest analysts.
- Contributed to the development and refinement of the CrowdStrike technical and management tabletop exercises, improving organizational preparedness for security incidents.

*PENTEST ANALYST*

*January 2022 – August 2022, Full-time*

- Assisted application teams in identifying, understanding, and remediating vulnerabilities, promoting a security-focused development environment.
- Onboarded applications into the Invicti web application security testing tool, evaluating scan results and providing actionable remediation insights.
- Performed manual vulnerability assessments on applications not suitable for automated scanning, ensuring thorough security evaluations.
- Promoted security awareness and best practices among development teams, enhancing the overall security culture within the organization.
- Ensured compliance with policies and standards outlined in the UPS Standard Practice Manual (SPM).

### UPS Corporate IE EUD, Remote

*SENIOR WEB APPLICATION DEVELOPER*

*February 2019 – January 2021, Full-time*

- Made significant contributions to the P2101 – Peak Helper Track Improvements Charter; developed the internet-facing HelperTrack REST API and led the security testing and mitigation efforts, resulting in a clean Netsparker scan.
- Established a schema-based access control security model for MS SQL Server databases to better enforce the principles of least privilege, segregation of duties, and need-to-know.
- Identified vulnerabilities in iGate and other web applications and implemented preventive and mitigating measures.
- Contributed to updating code assessment line items to include secure coding practices.
- Implemented Azure-based authentication in the iGate Web System.

## TECHNICAL SKILLS

---

**Operating Systems:** Kali Linux, Microsoft Windows, Windows Server/IIS, Unix/Linux, Android, iOS

**Applications:** Burp Suite Pro, Postman, Insomnia, OWASP Zap, Invicti, Nmap, Virtual Box, NetCat, SSLScan, K8s, Wireshark, Metasploit, and various other security testing and development tools

**Languages:** Python, JavaScript, PowerShell, HTML, CSS, SQL, LaTeX

PERSONAL ACHIEVEMENTS

---

<b>Erie Marathon</b> <i>[Time: 2:51]</i>	<i>2022</i>
<b>Boston Marathon</b> <i>[Time: 2:55]</i>	<i>2023</i>
<b>Boston Marathon</b> <i>[Time: 2:58]</i>	<i>2024</i>