JUSTIN WHITE

justin.white.itsec@gmail.com | 410-330-4800 | 12013 Waterside View Drive Reston, VA 20194
US CITIZEN | Active Public Trust

Professional Summary

Web Application Security Tester with **6 years of proven experience** in identifying, exploiting, and remediating vulnerabilities across **enterprise, government, and cloud environments**. Demonstrated expertise in **web application penetration testing, vulnerability assessment, secure configuration, and exploit development**, ensuring applications and networks are hardened against real-world attack scenarios.

Skilled in using industry-standard tools such as **Burp Suite, OWASP ZAP, Nmap, Nessus, Metasploit, Nikto, Gobuster, SQLMap, Wireshark, CyberChef, and Kali Linux**, along with **Python scripting** for automation, payload generation, and reporting. Experienced in **testing web applications built on Python, PHP, JavaScript, C#, and SQL platforms**, uncovering misconfigurations, injection flaws, and access control weaknesses in alignment with **OWASP Top 10** and **NIST SP 800-53** guidelines.

Proven success in executing large-scale web vulnerability assessments (400+ systems) and achieving 95–100% remediation rates for critical findings through collaboration with DevSecOps, and development teams. Hands-on experience with **virtualization and container environments** including **VMware, VirtualBox, Proxmox VE, Docker, and Kubernetes.**Adept at creating **custom attack simulations**, integrating **vulnerability assessment data with SIEM and compliance tools**, and generating **executive-level dashboards and reports**

Strong foundation in **secure coding practices, NIST Risk Management Framework (RMF)**, and **federal web application security requirements (ICD 503, DHS standards)**. Holds deep knowledge of **network and system administration** across Windows, Linux, and macOS environments, with hands-on skills in **Active Directory, pfSense firewalls**, and **threat simulation workflows**.

Known for an automation-first approach using tools like Python, GitHub, and n8n to streamline vulnerability tracking, exploit validation, and compliance reporting—reducing manual workload by 30%, and enhancing overall penetration testing efficiency.

Skills

- **Penetration Testing & Vulnerability Assessment:**
  Web Application Penetration Testing · Vulnerability Scanning · Exploitation Techniques · Threat Modeling · Risk Assessment · Red Team/Blue Team Collaboration
- **Tools & Frameworks:**
  Burp Suite Pro · OWASP ZAP · Nmap · Nessus · Metasploit · SQLMap · Nikto · Gobuster · DirBuster · Wireshark · CyberChef · Hydra · Acunetix · Qualys
- **Web Security & OWASP Top 10:**
  SQL Injection · Cross-Site Scripting (XSS) · Path Traversal · Broken Access Control · Command Injection · IDOR · CSRF · Security Misconfiguration · Sensitive Data Exposure · SSRF
- **Operating Systems & Virtualization:**
  Kali Linux · Parrot OS · Windows Server · Ubuntu · pfSense Firewall · VMware · VirtualBox · Proxmox VE · Docker · Kubernetes
- **Programming & Automation:**
  Python (Scripting, Automation, Regex, Log Parsing) · Bash · GitHub · Workflow Automation with n8n · Report Generation & Exploit Scripting
- **Security Standards & Compliance:**
  OWASP Top 10 · NIST SP 800-53 · NIST RMF · ICD 503 · Secure SDLC · DevSecOps Practices · Federal/DHS Security Requirements
- **Networking & Infrastructure:**
  TCP/IP · DNS · VPN · IDS/IPS Configuration · Packet Analysis · Firewall & Router Hardening · Cloud Security (AWS/Azure)
- **Reporting & Communication:**
  Vulnerability Reporting · Executive Dashboards · Risk Remediation Tracking · Developer Collaboration · Compliance Audit Documentation

Experience

09/2023 - Current
United States Department of Transportation
Washington, D.C.

Cyber Security Analyst

- Conducted business-logic testing that exposed flaws enabling bypass of payment limits and authorization checks; provided PoCs and remediation recommendations to development teams.
- Supported bug-bounty style engagements with reproducible PoCs and prioritized remediation guidance.
- Performed **10,000+ automated and manual scans**, identifying **120+ critical CVEs**, and closed high-risk exposures within SLA.
- Authored **50+ detailed technical reports** and executive summaries, improving compliance posture and reducing security incidents by **25%** for the current project.
- Collaborated with IT and development teams to achieve a **95% SLA closure rate** for critical vulnerabilities.
- Performed passive reconnaissance (OSINT, Google Dorking, Shodan, Recon-ng) to gather target intelligence and inform attack paths.
- Conducted active enumeration using **Nmap, DirBuster, Gobuster**, and SSL/TLS certificate analysis to discover hidden endpoints and services.
- Executed automated vulnerability scans with **Nessus / OpenVAS** and validated critical findings through manual exploitation and verification.
- Tested authentication mechanisms, demonstrating weaknesses such as brute-force, credential-stuffing, and session-hijacking vulnerabilities.
- Exploited IDOR and insecure object references to demonstrate unauthorized data access and recommended access-control fixes.
- Tested file upload routines to identify arbitrary file execution and RCE vectors; proposed secure file-handling mitigations.
- Identified and remediated server misconfigurations, weak/default credentials, and insecure SSL/TLS implementations.

01/2022 - 08/2023
United States Department of Labor
Washington, D.C.

Penetration Tester

- Exploited **SQLi, XSS, CSRF, and SSTI vulnerabilities** to demonstrate business impact and confirm exploitability.
- Evaluated **authentication and session security** (brute force, MFA bypass, session fixation, cookie handling).
- Used Metasploit Framework with Meterpreter payloads to validate vulnerabilities and achieve controlled shell access.
- Conducted **API penetration testing**, discovering BOLA, excessive data exposure, and missing rate-limit controls.
- Tested **WAF coverage and bypass techniques** to demonstrate potential evasion paths.
- Delivered **detailed security reports** including CVE references, CVSS scoring, exploit proof-of-concepts, and remediation guidance for both technical and executive audiences.
- Discovered and validated 350+ vulnerabilities across enterprise web apps and APIs, including OWASP Top 10 and logic flaws.
- Accelerated remediation cycles by **30–40%** through effective prioritization with DevSecOps teams.
- Reduced false positives by 35–42% using cross-tool validation and custom Python/Bash
- Executed the full penetration testing lifecycle: reconnaissance, scanning, enumeration, exploitation, post-exploitation, and reporting.
- Conducted web application testing with Burp Suite, OWASP ZAP, and Kali Linux; uncovered injection flaws, broken authentication, and IDOR vulnerabilities.
- Performed network scanning and analysis using Nmap and Wireshark, identifying exposed services, misconfigured ports, and weak SSL/TLS configurations.

- Performed **passive reconnaissance (OSINT, Google Dorking, Shodan, Recon-ng)** to gather intelligence on targets.
- Conducted **active enumeration** with Nmap, Dirbuster, Gobuster, and SSL/TLS certificate analysis to uncover hidden endpoints and services

01/2020 - 12/2021
Nooks
Arlington, VA

Junior Cybersecurity Analyst

- **Executed 60% of vulnerability scans** using **Nessus, Nmap, Zenmap, and Zap**, identifying **12+ high-severity vulnerabilities** in web applications and network services.
- **Configured pfSense firewall rules and IDS/IPS policies**, reducing unauthorized access attempts by **20%** within the first quarter.
- **Performed packet capture analysis with Wireshark** and used **CyberChef** for data parsing and encryption validation, improving detection accuracy by **15%**.
- **Conducted penetration testing with Kali Linux tools** in **VirtualBox and Proxmox VE labs**, validating exploit paths and ensuring a **90% remediation success rate** with development teams.
- **Reviewed Active Directory policies** to validate least-privilege access controls, reducing potential privilege escalation risks by **10%**.
- **Developed Python scripts** for automating basic log analysis and vulnerability reporting, reducing manual workload by **20%**.
- **Maintained GitHub repositories** for security scripts and remediation guides, improving team collaboration efficiency by **15%**.
- **Assisted in Secure SDLC practices** by embedding Zap scans during application testing, preventing recurring injection vulnerabilities.
- **Prepared weekly vulnerability reports** documenting findings, false positives, and closure status for senior analysts.
- Tested **authentication mechanisms** for brute force, credential stuffing, and session hijacking flaws.
- Exploited **IDOR and insecure object references** to demonstrate unauthorized data access.
- ·Tested **file upload functionalities** for arbitrary file execution, identifying RCE exposures.
- Identified **server misconfigurations**, weak/default credentials, and insecure SSL/TLS implementations.
- Conducted **business logic testing**, exposing flaws that allowed bypassing payment limits and authorization checks.
- Supported **bug bounty style engagements**, delivering reproducible PoCs and detailed remediation guidance.

Education

Bachelor of Science in Hospitality Management
East Stroudsburg University of Pennsylvania

Certifications

- **CompTIA Security+**
- **Google Cyber Security Professional**