STRENGTHS

Quiet risk discovery
Found overlooked authorization and session weaknesses during careful workflow review; application owners gained clearer closure priorities.

Evidence that travels
Turned packet captures, screenshots, and reproduction steps into reports that vendors could act on without guesswork.

Steady remediation follow-through
Returned after fixes, repeated approved tests, and separated closed findings from residual exposure for honest decisions.

Calm stakeholder communication
Explained exploit paths to technical and government audiences; difficult findings became workable conversations.

Disciplined engagement planning
Built schedules, labor estimates, milestones, and acceptance criteria before testing began, giving teams a dependable path.

Secure evidence custody
Kept U.S.-based records controlled through testing, reporting, packet logging, and documented destruction attestations.

SKILLS

Penetration Testing

Black-Box Testing | REST APIs

Web Applications | OWASP Testing

Ali Myers

Penetration Tester

(802) 555-0147 ali.myers.sec@gmail.com
linkedin.com/example/alimyers Burlington, VT 05401

SUMMARY

Senior penetration tester with eight years assessing external web applications, REST APIs, and production-like public-sector systems through authenticated and unauthenticated **black-box testing**. Defines scope, traces network traffic, validates exploitability, and converts technical findings into risk-ranked reports with reproducible evidence, **criticality levels**, **corrective actions**, and **acceptance criteria**. Delivered engagements across transportation, licensing, benefits, and citizen-service platforms while maintaining U.S.-based testing and data-residency controls. Uses Burp Suite, Nmap, Metasploit, OWASP ZAP, Postman, Python, Wireshark, tcpdump, Microsoft Office, Adobe PDF, and OWASP testing practices. Applies PMBOK-aligned planning across schedules, work breakdown structures, Gantt charts, quantified deliverables, and remediation retesting. Ready to support secure state services through disciplined testing, clear reporting, and dependable stakeholder collaboration.

EXPERIENCE

Senior Penetration Tester

CivicShield Assessment Group May 2024 - Present Burlington, VT

Leads external black-box assessments for state licensing and transportation platforms, directing scope, testing, reporting, remediation validation, and secure evidence handling.

- Led external black-box assessments across **authenticated** workflows and REST APIs in **production-like environments**.
- Built PMBOK-aligned schedules, work breakdown structures, Gantt charts, milestones, and **acceptance criteria**.
- Validated authorization flaws, injection paths, session weaknesses, exposed services, and API abuse with **Burp Suite**.
- Produced risk-ranked reports with exploit narratives, **screenshots**, **reproduction steps**, criticality, and corrective actions.
- Captured packet traffic with Wireshark and tcpdump, supplying logs as controlled report addenda.
- Directed remediation retests and completed destruction attestations for collected engagement information.

Penetration Tester

HarborPoint Cyber Advisory January 2022 - April 2024 Portland, ME

Executed public-sector web application and REST endpoint assessments, translating evidence into client-ready reports while coordinating remediation validation and secure records management.

- Executed **authenticated** and **unauthenticated** assessments across benefits, permitting, and motor-vehicle service portals.
- Scoped workflows, role boundaries, API parameters, file handling, error responses, and session controls.
- Combined Burp Suite, **OWASP ZAP**, Nmap, Nikto, **Postman**, and Python utilities for exploit validation.
- Converted technical evidence into Word and **Adobe PDF** reports with prioritized corrective guidance.
- Coordinated remediation validation with developers and infrastructure contacts, separating open and closed findings.
- Maintained scope approvals, packet logs, evidence records, and destruction certification for audit review.

Security Consultant

Redwood State Security Services June 2020 - December 2021 Albany, NY

Planned and delivered penetration tests for state and municipal applications, supporting project schedules, labor estimates, stakeholder briefings, and measurable closure criteria.

Burp Suite | OWASP ZAP | Nmap | Metasploit | Vulnerability Ranking | Exploit Validation | Remediation Retesting | Packet Logging | Technical Reporting | PMBOK

LANGUAGES

English — Native

Spanish — Intermediate

MY CAREER

- Senior Penetration Tester at CivicShield Assessment Group (2.3 Years)
- Penetration Tester at HarborPoint Cyber Advisory (2.2 Years)
- Security Consultant at Redwood State Security Services (1.5 Years)
- Cybersecurity Analyst at Blue Ridge Information Assurance (1.8 Years)

- Conducted penetration tests for externally accessible applications and REST services supporting citizen transactions.
- Mapped attack surfaces with **Nmap**, **Burp Suite**, OWASP ZAP, and Postman before manual validation.
- Prepared findings linking weaknesses with operational consequences, affected endpoints, and practical corrective methods.
- Performed follow-up testing after patches, preserving before-and-after evidence for application owners.
- Supported **Microsoft Project** and Excel schedules, labor estimates, milestones, and concurrent engagement tracking.
- Presented **reproduction steps** to security, development, vendor, and project management teams.

Cybersecurity Analyst

Blue Ridge Information Assurance | July 2018 - May 2020 | Richmond, VA

Supported controlled web application and API assessments, organizing evidence, test accounts, packet captures, reports, and remediation retesting under senior review.

- Supported web application and API assessments under documented rules of engagement and testing windows.
- Enumerated public-facing assets with Nmap and validated suspected weaknesses through **Burp Suite**.
- Documented affected URLs, request evidence, response evidence, severity context, and mitigation language.
- Monitored packet captures and application logs during controlled production-like test activities.
- Assisted **authenticated** account setup, **unauthenticated** workflow coverage, evidence organization, and remediation retesting.
- Maintained assessment records in Word, Excel, and **Adobe PDF** for senior reviewers.

PROJECTS

State Transportation API Assessment | 2025

Assessed authenticated and unauthenticated REST workflows across transportation services, producing risk-ranked findings, exploit evidence, corrective actions, and retest criteria.

Public Benefits Web Security Review | 2023

Mapped external attack surfaces for benefits portals, validated access-control and session findings, and delivered client-ready reports with reproducible evidence.

Municipal Citizen Services Test | 2021

Tested public-facing citizen transaction services, coordinated patch validation, and preserved before-and-after evidence for project stakeholders.

LEADERSHIP & AWARDS

- Client Excellence Recognition for Public-Sector Security Reporting, CivicShield Assessment Group, 2025.
- Outstanding Cybersecurity Capstone Award, Virginia Commonwealth University, 2018.
- Dean's List, Virginia Commonwealth University, 2017.

EDUCATION

Bachelor's Degree in Cybersecurity

Virginia Commonwealth University | GPA: 3.7 | 2018 | Richmond, VA

Coursework: *Penetration testing, network security, ethical hacking, digital forensics*

CERTIFICATIONS

- Offensive Security Certified Professional (OSCP) 2021
- Certified Ethical Hacker (CEH) 2020
- CompTIA Security+ 2018
- PMI Project Management Basics Certificate 2022

TECHNICAL SKILLS

- **Penetration Testing:** Black-box testing, authenticated testing, unauthenticated testing
- **Web Application Testing:** External web applications, OWASP testing, browser testing
- **API Testing:** REST endpoints, Postman, API abuse testing
- **Security Tools:** Burp Suite, OWASP ZAP, Metasploit
- **Network Discovery:** Nmap, Nikto, exposed-service analysis
- **Scripting:** Python, custom scripts, automation utilities
- **Packet Analysis:** Wireshark, tcpdump, packet logging
- **Vulnerability Reporting:** Risk ranking, exploit documentation, criticality levels
- **Remediation Validation:** Retesting, before-and-after evidence, closure criteria
- **Project Management:** PMBOK, Microsoft Project, Gantt charts
- **Office Deliverables:** Microsoft Word, Microsoft Excel, Microsoft Visio
- **Document Formats:** Adobe PDF, screenshots, report addenda
- **Planning Artifacts:** Work breakdown structures, schedules, labor estimates
- **Data Governance:** U.S. data residency, secure destruction, destruction attestation
- **Engagement Controls:** Rules of engagement, testing windows, scope approvals

PROFESSIONAL AFFILIATIONS

- Volunteer Mentor, Vermont Cybersecurity Workforce Program, September 2024 - Present.
- Workshop Facilitator, Mid-Atlantic OWASP Community, January 2022 - Present.
- Student Security Lab Coordinator, Virginia Commonwealth University, 2017 - 2018.

ADDITIONAL INFORMATION

Work Status : Authorized to work in United States. No sponsorship required.

REFERENCES

AVAILABLE ON REQUEST