



1 Business Opportunities – loanbuilder.com

Key evidence: 4 High-risk vulnerabilities; 5 Medium-risk vulnerabilities; 1420 URLs without HTTPS; 7% hosts lack WAF; 3 leaked credentials; 16 unusual port assignments

1.1 Top Opportunities

1. Implement HTTPS Across All URLs

- Problem: 1420 URLs are using unencrypted HTTP, exposing data to interception.
- Impact: High risk of data breaches and man-in-the-middle attacks.
- Service: Web Application Penetration Testing
- Scope: All web applications and URLs.
- Evidence: 1420 URLs identified without HTTPS.
- ROI: Reduces risk of data breaches, enhancing user trust and compliance.

2. Deploy Web Application Firewall (WAF)

- Problem: 7% of hosts lack WAF protection, increasing vulnerability to attacks.
- Impact: Elevated risk of injection-based attacks.
- Service: WAF Enterprise Implementation
- Scope: All hosts, including `http://msoid.loanbuilder.com`.
- Evidence: 1 host identified without WAF.
- ROI: Strengthens defense against web attacks, reducing potential breach costs.

3. Secure Leaked Credentials

- Problem: Email addresses and passwords leaked on the deep web.
- Impact: High risk of unauthorized access and phishing attacks.
- Service: Data Leak Detection
- Scope: All identified accounts and credentials.
- Evidence: 3 leaked credentials from databases like AntiPublic.
- ROI: Prevents unauthorized access, safeguarding sensitive information.

4. Reconfigure Unusual Port Assignments

- Problem: 16 unusual port assignments detected, indicating potential evasion.
- Impact: Increased risk of unauthorized access and misconfigurations.
- Service: Infrastructure Security Assessment
- Scope: Hosts under `msoid.loanbuilder.com`.
- Evidence: 8 High-risk port assignments.
- ROI: Enhances network security, reducing the risk of exploitation.

5. Mitigate DoS Vulnerabilities

- Problem: High timeout rate on HTTPS services, suggesting DoS susceptibility.
- Impact: Potential service disruptions and downtime.
- Service: DDoS Protection
- Scope: Port 443 (HTTPS) services.
- Evidence: 54.68% timeout rate on HTTPS.
- ROI: Ensures service availability, maintaining business continuity.



1.2 Proposed Offer

- Scope: Comprehensive security enhancement across web applications, infrastructure, and data protection.
- Deliverables: HTTPS implementation, WAF deployment, credential security, port reconfiguration, DoS mitigation.
- Timeline (weeks): 12

1.3 30/60/90 & KPIs

- 30d: Complete HTTPS implementation on 50% of URLs.
- 60d: Deploy WAF on all hosts; secure all leaked credentials.
- 90d: Reconfigure all unusual port assignments; mitigate DoS vulnerabilities.
- KPIs: Reduction in high-risk vulnerabilities by 80%; 100% HTTPS coverage; 0 unauthorized access incidents.

1.4 Objections & Responses

- **Objection:** Cost of implementation is high. Response: The investment reduces potential breach costs and enhances compliance, offering long-term savings.
- **Objection:** Disruption to current operations. Response: Implementation will be phased to minimize impact, ensuring continuous operation.
- **Objection:** Lack of internal expertise for ongoing management. Response: We offer training and support to empower your team for effective management.
- **Objection:** Uncertainty about ROI. Response: Enhanced security posture will lead to increased customer trust and reduced incident response costs.

1.5 Immediate Next Steps

- Client: Review and approve proposed security enhancements.
- Consultancy: Prepare detailed project plan and resource allocation.
- Joint: Schedule kickoff meeting to align on objectives and timelines.