PENETRATION TEST REPORT - PAPERWORKS ONLINE LTD.

Report ID: PENTEST-2024-001
Classification: CONFIDENTIAL
Date: October 21, 2024
Prepared For: PaperWorks Online Ltd., 123 Stationery Ave, Dublin, Ireland
Prepared By: SecureSphere Security Consultants
Test Period: October 15-18, 2024
Report Version: 1.0

EXECUTIVE SUMMARY

1.1 Overview

A comprehensive penetration test was conducted against PaperWorks Online Ltd.'s external infrastructure and web application from October 15-18, 2024. The assessment followed a black-box methodology with limited prior knowledge, simulating a real-world attacker targeting a small e-commerce retailer.

1.2 Key Findings

- Overall Risk Rating: MEDIUM
- Total Vulnerabilities: 14 (Critical: 1, High: 2, Medium: 5, Low: 6)
- Security Posture Assessment: The organization demonstrates basic security hygiene but lacks defense-in-depth controls. The payment processing architecture effectively limits PCI DSS scope.

1.3 Critical Finding

One critical vulnerability was identified: Improper Access Control on Admin Portal (CVE-2024-PW-001) allowing unauthorized access to administrative functions without MFA verification.

1.4 Recommendations Priority

1. Immediate (0-7 days): Patch critical access control vulnerability
2. Short-term (8-30 days): Implement WAF, enhance authentication controls
3. Medium-term (31-90 days): Comprehensive security hardening
4. Long-term (91-180 days): Advanced monitoring and security program maturity

---

2.0 SCOPE AND METHODOLOGY

2.1 In-Scope Assets

Target	Type	IP/URL	Notes
Primary Website	Web Application	https://www.paperworksonline.ie	WordPress/WooCommerce
Admin Portal	Web Application	https://admin.paperworksonline.ie	Custom administration panel
API Endpoints	REST API	https://api.paperworksonline.ie/v1/*	Order management API
Mail Server	Infrastructure	mail.paperworksonline.ie	Office 365 tenant
Network Range	Infrastructure	203.0.113.0/24	Public-facing IP range

2.2 Out-of-Scope Assets

- Payment gateway (Stripe) - Third-party, PCI DSS Level 1 certified
- Employee workstations
- Internal corporate network
- Third-party SaaS services (except where interfaces exist)

2.3 Testing Methodology

- OWASP Testing Guide v4.2 for web application testing
- PTES Technical Guidelines for infrastructure testing
- Automated Scanning: Nessus Professional, Burp Suite Professional
- Manual Testing: Exploitation, business logic testing, authentication bypass attempts
- Social Engineering: Limited phishing simulation (authorized)

2.4 Rules of Engagement

- Testing conducted during business hours (09:00-17:00 GMT)
- No denial of service attacks
- No customer data exfiltration
- Immediate reporting of critical findings
- Safe exploitation with rollback procedures

3.0 DETAILED FINDINGS

3.1 Critical Severity Findings

FINDING CVE-2024-PW-001: Broken Access Control in Admin Portal

- CVSS Score: 9.1 (Critical)
- Affected Component: Admin Portal (/admin/*)
- Discovery Date: October 16, 2024
- Exploitation Complexity: Low

Description:

The admin portal's session management mechanism contains a flaw allowing authenticated but unauthorized users to access administrative functions beyond their assigned role. Specifically, sales staff accounts can bypass role-based checks and access functions reserved for system administrators.

Technical Details:

text

```
Vulnerable Endpoint: GET /admin/system-config
Normal Request (Sales Role):
  GET /admin/system-config HTTP/1.1
  Cookie: session=eyJ1c2VyX2lkIjoxMjMsInJvbGUiOiJzYWxlcyJ9
  Response: 403 Forbidden

Exploit Request:
  GET /admin/system-config HTTP/1.1
  Cookie: session=eyJ1c2VyX2lkIjoxMjMsInJvbGUiOiJhZG1pbiJ9
  Response: 200 OK (Administrative panel loaded)
```

The application validates the session cookie for authentication but fails to verify the role parameter against the server-side session store.

Impact:

- Unauthorized access to customer PII database
- Ability to modify product pricing and inventory
- Potential for privilege escalation to full administrative control
- GDPR violation risk through unauthorized data access

Proof of Concept:

[Evidence screenshot REDACTED] - Shows sales user accessing admin functions

Recommendation:

1. Implement server-side session validation for all privileged endpoints
2. Apply proper role-based access control checks
3. Implement mandatory re-authentication for sensitive operations
4. Add audit logging for all admin function access

3.2 High Severity Findings

FINDING CVE-2024-PW-002: SQL Injection in Product Search

- CVSS Score: 8.5 (High)
- Affected Component: Product search functionality
- Discovery Date: October 15, 2024

Description:

The product search feature is vulnerable to time-based blind SQL injection through the category parameter.

Technical Details:

text

```
Vulnerable Parameter: category
Exploit: /products?category=1' AND (SELECT * FROM (SELECT(SLEEP(5)))a)--
Result: 5-second delay indicates successful injection
```

The application concatenates user input directly into SQL queries without parameterization.

Impact:

- Extraction of customer database (PII)
- Database compromise leading to full system control
- Potential ransomware deployment vector

Recommendation:

1. Implement prepared statements with parameterized queries
2. Deploy WAF with SQL injection rules
3. Conduct code review of all database interactions

FINDING CVE-2024-PW-003: Weak Password Policy Enforcement

- CVSS Score: 7.4 (High)
- Affected Component: User authentication system
- Discovery Date: October 17, 2024

Description:

While the password policy requires 12-character passwords, the enforcement occurs only client-side. Server-side validation is incomplete, allowing weak passwords through API calls.

Technical Details:

text

```
POST /api/v1/user/create HTTP/1.1
{"username":"test","password":"123456"}  # Accepted by server

POST /web/register HTTP/1.1
{"username":"test","password":"123456"}  # Rejected by client-side JS
```

Impact:

- Increased risk of credential stuffing attacks
- Easier brute-force attacks against admin accounts
- Compromise of administrative functions

Recommendation:

1. Implement consistent server-side password validation
2. Enforce password complexity requirements
3. Implement account lockout after 5 failed attempts

3.3 Medium Severity Findings

ID	Vulnerability	CVSS	Component	Status
CVE-2024-PW-004	Cross-Site Scripting (Reflected)	6.1	Customer review form	Open
CVE-2024-PW-005	Sensitive Data Exposure in Logs	5.5	Application logs	Open
CVE-2024-PW-006	Missing Security Headers	5.3	All web pages	Open
CVE-2024-PW-007	Insecure Direct Object Reference	5.0	Order API	Open
CVE-2024-PW-008	Directory Listing Enabled	4.3	Static assets	Open

3.4 Low Severity Findings

ID	Vulnerability	CVSS	Component	Status
CVE-2024-PW-009	Verbose Error Messages	3.8	API endpoints	Open
CVE-2024-PW-010	Missing Cookie Security Flags	3.7	Session cookies	Open
CVE-2024-PW-011	Outdated Software Components	3.5	WordPress plugins	Open
CVE-2024-PW-012	Information Disclosure via HEAD	2.8	Web server	Open

CVE-2024-PW-013	Predictable Resource Location	2.5	Admin interfaces	Open
CVE-2024-PW-014	Missing X-Frame-Options	2.2	All pages	Open

4.0 EXPLOITATION CHAIN ANALYSIS

4.1 Potential Attack Scenarios

Scenario 1: Customer Data Exfiltration

text
Step 1: Attacker identifies XSS in review form (CVE-2024-PW-004)
Step 2: Creates malicious review stealing admin session cookies
Step 3: Uses stolen session to exploit broken access control (CVE-2024-PW-001)
Step 4: Accesses admin panel, exports customer database via SQL injection (CVE-2024-PW-002)
Step 5: Exfiltrates 5,200 customer records containing PII

Impact: GDPR breach, potential €4.36M fine (2% of global turnover estimate)

Scenario 2: Payment System Compromise

text
Step 1: Attacker brute-forces weak admin password (CVE-2024-PW-003)
Step 2: Accesses admin portal, modifies payment processing JavaScript
Step 3: Injects card-skimming script into checkout page
Step 4: Harvests payment card data despite PSP integration

Impact: PCI DSS violation, card brand fines, loss of merchant account

4.2 Business Impact Assessment

Impact Area	Severity	Likelihood	Overall Risk
Regulatory Compliance (GDPR)	High	Medium	High
Financial Loss	Medium	High	Medium

Reputational Damage	High	Medium	High
Operational Disruption	Medium	Low	Medium
Legal Liability	High	Medium	High

5.0 POSITIVE FINDINGS

5.1 Security Strengths Identified

1. Payment Processing Architecture: Proper use of hosted payment pages eliminates PCI DSS scope for cardholder data
2. TLS Configuration: Strong cipher suites and proper certificate management
3. Network Segmentation: Clear separation between web, application, and database tiers
4. Regular Backups: Automated daily backups with off-site storage
5. Basic Security Policies: Documentation exists for key security areas

5.2 Effective Controls

- MFA implemented for administrative access
- Rate limiting on login endpoints
- Security headers partially implemented
- Regular software updates (with some exceptions)

6.0 RISK ASSESSMENT MATRIX

6.1 Vulnerability Distribution

text

```
Critical:   1  (7%)
High:       2  (14%)
Medium:     5  (36%)
Low:        6  (43%)
Total:      14 (100%)
```

6.2 Risk Heat Map

The following heat map visualizes the identified risks based on their assessed Impact and Likelihood.

Impact / Likelihood	High	Medium	Low
High		GDPR Breach	
Medium	Payment Fraud	SQLi	XSS
Low			Info Disclosure

7.0 RECOMMENDATIONS

7.1 Immediate Actions (0-7 Days)

Priority 1: Patch Critical Vulnerabilities

1. Fix Broken Access Control (CVE-2024-PW-001)
   - Implement server-side authorization checks
   - Add session validation middleware
   - Deploy emergency patch by October 25, 2024
2. Mitigate SQL Injection (CVE-2024-PW-002)
   - Deploy virtual patch via WAF
   - Schedule code remediation for next development sprint

Priority 2: Emergency Controls

1. Enable Web Application Firewall (WAF) with rule sets for:
   - SQL injection prevention
   - XSS protection
   - Access control enforcement
2. Implement temporary monitoring:
   - Alert on admin portal access attempts
   - Monitor for SQL injection patterns
   - Enhanced logging of authentication events

7.2 Short-term Remediation (8-30 Days)

Technical Controls

1. Authentication & Authorization
   - Implement consistent server-side password validation
   - Enforce MFA for all administrative functions
   - Implement session management best practices
2. Input Validation & Output Encoding
   - Deploy parameterized queries for all database interactions
   - Implement context-aware output encoding

   - Add content security policy headers
3. Security Configuration
   - Harden web server configuration
   - Remove directory listings
   - Implement security headers (HSTS, CSP, X-Frame-Options)

Process Improvements

1. Patch Management
   - Establish 30-day patch cycle for critical vulnerabilities
   - Implement vulnerability scanning schedule
   - Create emergency change process
2. Access Control Review
   - Conduct quarterly user access reviews
   - Implement privilege escalation approval process
   - Regular review of administrative accounts

7.3 Medium-term Improvements (31-90 Days)

1. Security Development Lifecycle
   - Implement secure coding standards
   - Add security testing to CI/CD pipeline
   - Conduct developer security training
2. Monitoring & Detection
   - Implement SIEM solution
   - Create incident response playbooks
   - Establish 24/7 monitoring capability
3. Third-party Risk Management
   - Assess all vendor security postures
   - Review data processing agreements
   - Implement vendor security requirements

7.4 Long-term Strategic (91-180 Days)

1. Security Program Maturity
   - Implement ISO 27001 framework
   - Conduct regular security awareness training
   - Establish security metrics and reporting
2. Advanced Controls
   - Implement runtime application self-protection (RASP)
   - Deploy deception technology
   - Conduct red team exercises
3. Compliance Automation
   - Automate PCI DSS compliance reporting
   - Implement GDPR data mapping tool
   - Regular compliance assessments

8.0 TESTING LIMITATIONS

8.1 Scope Limitations

- Internal network testing was excluded
- Social engineering was limited to phishing simulation
- Mobile application testing was not performed (no mobile app)
- Physical security assessment was out of scope

8.2 Methodology Limitations

- Limited time for manual exploitation (4 days)
- Black-box approach limited insider knowledge advantage
- No zero-day vulnerability research conducted

8.3 Environmental Factors

- Testing conducted during business hours only
- Limited impact testing to avoid service disruption
- No destructive testing performed

9.0 CONCLUSION

PaperWorks Online Ltd.'s security posture shows the typical characteristics of a small e-commerce business: adequate foundational controls but lacking defense-in-depth. The critical finding of broken access control represents an immediate and severe risk requiring urgent remediation.

The organization's decision to use a hosted payment gateway successfully limits PCI DSS scope and demonstrates sound risk-based decision making. However, the web application contains multiple vulnerabilities that could lead to data breach, financial loss, and regulatory penalties.

Overall Security Rating: 5.8/10 (Needs Improvement)

Next Steps Recommended:

1. Immediate patching of critical vulnerabilities
2. Implementation of WAF as temporary protection
3. Comprehensive code review and remediation
4. Enhanced security monitoring and incident response capabilities

10.0 APPENDICES

Appendix A: Tools Used

- Burp Suite Professional v2024.1
- Nessus Professional v10.5
- Nmap v7.94
- SQLMap v1.7
- Custom Python scripts for exploitation
- OWASP ZAP v2.13

Appendix B: References

- OWASP Top 10 2021
- PCI DSS v4.0 Requirements
- GDPR Article 32 Security Requirements
- ISO/IEC 27001:2022 Controls

Appendix C: Glossary

- CVSS: Common Vulnerability Scoring System
- PII: Personally Identifiable Information
- WAF: Web Application Firewall
- MFA: Multi-Factor Authentication
- SQLi: SQL Injection
- XSS: Cross-Site Scripting

11.0 CONTACT INFORMATION

SecureSphere Security Consultants
CyberSecurity House,
Grand Canal Dock,
Dublin 2, Ireland
Email: reports@securesphere.ie
Phone: +353 1 234 5678
Emergency Contact: +353 87 123 4567
PaperWorks Online Ltd. Contacts
Primary: Michael Scott (CEO)
Technical: Pam Beasley (IT Administrator)
Compliance: Designated Data Protection Officer

SIGNATURES

Test Lead:

Dr. Alan Turing
Senior Security Consultant
SecureSphere Security Consultants
Client Acknowledgment:

Michael Scott
CEO
PaperWorks Online Ltd.
Date: October 21, 2024

DOCUMENT CONTROL
Distribution: PaperWorks Ltd. Management, IT Administrator
Retention: 7 years minimum
Review Cycle: Annual penetration test recommended
Next Test Scheduled: April 2025 (Q2)