Domain and Website Analysis Report

Report ID: [DWA-YYYY-MM-DD-XXX]
Classification: [Confidential/Internal/Public]
Distribution: [Authorized Personnel Only]
Date: [Report Generation Date]
Analyst: [Your Name/Team]
Version: [1.0]

Executive Summary

[Provide a concise overview of the domain and website analysis findings, highlighting critical discoveries, security posture, and overall assessment. This should be digestible for executive leadership in 2-3 paragraphs.]

Key Findings:

- [Critical finding 1]
- [Critical finding 2]
- [Critical finding 3]

Overall Risk Assessment: [Critical/High/Medium/Low]
Recommended Priority: [Immediate/High/Medium/Low]

---

1. Analysis Scope and Objectives

1.1 Target Domain Information

- **Primary Domain:** [example.com]
- **Alternative Domains:** [example.org, example.net]
- **Target Organization:** [Company/Entity Name]
- **Industry/Sector:** [Technology, Finance, Healthcare, etc.]
- **Suspected Geographic Location:** [Country/Region]

1.2 Analysis Objectives

- [ ] Domain registration and ownership analysis
- [ ] Website technology stack identification
- [ ] Content and structure analysis
- [ ] Security posture assessment

- [ ] Subdomain enumeration and analysis
- [ ] Historical analysis and changes
- [ ] Third-party integrations and dependencies
- [ ] SEO and marketing intelligence
- [ ] Threat intelligence correlation
- [ ] Other: [Specify additional objectives]

1.3 Analysis Timeline

- **Analysis Start:** [YYYY-MM-DD HH:MM UTC]
- **Analysis End:** [YYYY-MM-DD HH:MM UTC]
- **Total Duration:** [X hours/days]
- **Last Website Update Observed:** [YYYY-MM-DD]

---

2. Methodology and Tools

2.1 Information Sources

- [ ] WHOIS databases (IANA, regional registries)
- [ ] DNS enumeration and analysis
- [ ] Web crawling and content analysis
- [ ] Certificate transparency logs
- [ ] Search engine caching (Google, Bing, Wayback Machine)
- [ ] Social media and public repositories
- [ ] Threat intelligence feeds
- [ ] Website analysis tools and scanners
- [ ] Third-party security services
- [ ] Other: [Specify additional sources]

2.2 Tools and Techniques Used

Domain Analysis Tools:
- [whois] - Domain registration information
- [dig/nslookup] - DNS record analysis
- [dnsrecon] - DNS enumeration

Website Analysis Tools:
- [Wappalyzer] - Technology stack identification
- [Burp Suite] - Web application analysis
- [Nikto] - Web server scanner
- [Gobuster] - Directory/file enumeration

OSINT Tools:

- [theHarvester] - Email and subdomain enumeration
- [Shodan] - Internet-connected device search
- [Censys] - Certificate and service analysis

Verification Tools:
- [curl/wget] - Manual verification
- [Browser Developer Tools] - Client-side analysis

2.3 Analysis Limitations

- [Passive reconnaissance only - no active scanning]
- [Rate limiting encountered on certain services]
- [Time constraints affecting depth of analysis]
- [Geographic restrictions on certain tools/services]
- [Legal and ethical boundaries observed]

---

3. Domain Registration Analysis

3.1 WHOIS Information

Domain: [example.com]

Attribute	Current Value	Previous Value (if changed)	Source	Last Updated
Registrar	[Registrar Name]	[Previous if applicable]	WHOIS	[Date]
Registration Date	[YYYY-MM-DD]	N/A	WHOIS	[Original]
Expiration Date	[YYYY-MM-DD]	[Previous if extended]	WHOIS	[Date]
Last Updated	[YYYY-MM-DD]	[Previous update]	WHOIS	[Date]
Registrant	[Organization/Name]	[Previous if changed]	WHOIS	[Date]
Admin Contact	[Contact Info]	[Previous if changed]	WHOIS	[Date]
Tech Contact	[Contact Info]	[Previous if changed]	WHOIS	[Date]
Status	[clientTransferProhibited]	[Previous status]	WHOIS	[Date]

3.2 Registration Analysis

- **Domain Age:** [X years, Y months]
- **Registration Pattern:** [Bulk registration/Individual/Corporate]
- **Registrar Reputation:** [Reputable/Suspicious/Unknown]
- **Privacy Protection:** [Enabled/Disabled]
- **Historical Changes:** [Number of ownership changes, frequency]

3.3 Related Domains

Domain	Relationship	Registration Date	Registrar	Status
[example.org]	[Same registrant]	[Date]	[Registrar]	[Active/Inactive]
[example-shop.com]	[Similar name]	[Date]	[Registrar]	[Active/Inactive]
[examp1e.com]	[Typosquatting]	[Date]	[Registrar]	[Suspicious]

---

4. DNS Infrastructure Analysis

4.1 DNS Records Overview

Primary Name Servers: [ns1.example.com, ns2.example.com]
DNS Provider: [Cloudflare, Route53, etc.]

Record Type	Value	TTL	Notes
A	XXX.XXX.XXX.XXX	300	[Primary IP]
AAAA	[IPv6 if present]	300	[IPv6 support]
CNAME	www -> example.com	300	[Canonical name]
MX	mail.example.com (10)	3600	[Mail server priority]
TXT	[SPF/DKIM/DMARC records]	3600	[Email authentication]
NS	[ns1.example.com, ns2.example.com]	86400	[Name servers]

4.2 Subdomain Enumeration

Total Subdomains Discovered: [Number]
Methods Used: [Certificate transparency, brute force, search engines]

Subdomain	IP Address	Status	Purpose	Technology	Risk Level
www.example.com	XXX.XXX.XXX.XXX	Active	Main website	[Apache/Nginx]	Low
mail.example.com	XXX.XXX.XXX.XXX	Active	Email server	[Postfix]	Medium
admin.example.com	XXX.XXX.XXX.XXX	Active	Admin panel	[Unknown]	High
dev.example.com	XXX.XXX.XXX.XXX	Active	Development	[Node.js]	High
test.example.com	XXX.XXX.XXX.XXX	Inactive	Testing	[Unknown]	Medium
old.example.com	XXX.XXX.XXX.XXX	Active	Legacy site	[PHP]	High

4.3 DNS Security Analysis

- **DNSSEC:** [Enabled/Disabled]
- **DNS over HTTPS (DoH):** [Supported/Not Supported]

- **DNS over TLS (DoT):** [Supported/Not Supported]
- **DNS Resolver Security:** [Analysis of recursive resolvers]

---

5. Website Structure and Content Analysis

5.1 Website Overview

- **Primary URL:** [https://example.com]
- **Website Type:** [Corporate, E-commerce, Blog, Portal, etc.]
- **Primary Language:** [English, Spanish, etc.]
- **Additional Languages:** [List if multilingual]
- **Last Major Update:** [Estimated based on content analysis]

5.2 Site Architecture

```
Website Structure:
├── / (Homepage)
├── /about
├── /products
│   ├── /products/category1
│   └── /products/category2
├── /services
├── /contact
├── /blog
│   ├── /blog/2024
│   └── /blog/archives
├── /login
├── /admin (Protected)
└── /api
    ├── /api/v1
    └── /api/v2
```

5.3 Content Analysis

Page/Section	Purpose	Last Modified	Security Level	Notes
Homepage	[Main landing]	[Date]	Public	[CMS: WordPress]
Login Portal	[User authentication]	[Date]	Protected	[Multi-factor auth: No]
Admin Panel	[Administration]	[Date]	Restricted	[Default credentials possible]
API Endpoints	[Data access]	[Date]	Mixed	[Some endpoints unprotected]
File Uploads	[User content]	[Date]	Protected	[File type restrictions unclear]

5.4 Robots.txt and Sitemap Analysis

Robots.txt Findings:

```
User-agent: *
Disallow: /admin/
Disallow: /private/
Disallow: /backup/
Allow: /public/
Sitemap: https://example.com/sitemap.xml
```

Notable Disallowed Paths:

- `/admin/` - Administrative interface
- `/private/` - Private content area
- `/backup/` - Backup files (potential data exposure)
- `/api/internal/` - Internal API endpoints

Sitemap Analysis:

- **URLs Indexed:** [Number]
- **Last Updated:** [Date]
- **Hidden Sections:** [Sections not in sitemap but accessible]

---

6. Technology Stack Analysis

6.1 Web Server and Infrastructure

Component	Technology	Version	End-of-Life Status	Security Notes
Web Server	[Apache/Nginx/IIS]	[2.4.41]	[Supported/EOL]	[Known vulnerabilities]
Operating System	[Linux/Windows]	[Ubuntu 20.04]	[Supported]	[Last security update]
Load Balancer	[Cloudflare/AWS ALB]	[N/A]	[N/A]	[DDoS protection active]
CDN	[Cloudflare/AWS CloudFront]	[N/A]	[N/A]	[Global distribution]

6.2 Application Stack

Technology	Version	Purpose	Security Assessment
CMS	[WordPress]	[5.8.1]	[Outdated - security patches available]
Programming Language	[PHP]	[7.4]	[Approaching EOL]
Database	[MySQL]	[8.0]	[Current version]
Framework	[Laravel]	[8.0]	[One version behind]

Technology	Version	Purpose	Security Assessment
JavaScript Framework	[React]	[17.0.2]	[Current]

6.3 Third-Party Integrations

Service	Purpose	Data Exposure Risk	Privacy Implications
Google Analytics	[Web analytics]	[High - user tracking]	[PII collection possible]
Facebook Pixel	[Marketing tracking]	[High - behavioral data]	[Cross-site tracking]
Stripe	[Payment processing]	[Medium - transaction data]	[PCI compliance required]
Mailchimp	[Email marketing]	[Medium - subscriber data]	[Email addresses exposed]
Zendesk	[Customer support]	[High - support tickets]	[Customer data exposed]

6.4 Client-Side Analysis

JavaScript Libraries:

- [jQuery 3.5.1] - [DOM manipulation]
- [Bootstrap 4.6] - [CSS framework]
- [Moment.js] - [Date handling - deprecated]

Browser Compatibility:

- [Chrome]: Fully supported
- [Firefox]: Fully supported
- [Safari]: Partial support (minor CSS issues)
- [IE11]: Not supported

---

7. Security Posture Assessment

7.1 SSL/TLS Configuration

Attribute	Value	Security Level	Recommendation
Certificate Authority	[Let's Encrypt]	[Trusted]	[Consider EV certificate]
Certificate Type	[Domain Validated]	[Basic]	[Upgrade to Organization Validated]
Expiration Date	[YYYY-MM-DD]	[30 days remaining]	[Enable auto-renewal]
Key Length	[2048 bits]	[Adequate]	[Consider 4096 bits]
TLS Versions	[1.2, 1.3]	[Good]	[Disable TLS 1.2 if possible]
Perfect Forward Secrecy	[Enabled]	[Good]	[No action needed]
HSTS	[Enabled]	[Good]	[Extend max-age]

7.2 Security Headers Analysis

Header	Status	Value	Security Impact
X-Frame-Options	✅ Present	DENY	[Clickjacking protection]
X-Content-Type-Options	✅ Present	nosniff	[MIME type sniffing prevention]
X-XSS-Protection	❌ Missing	N/A	[XSS protection recommended]
Content-Security-Policy	⚠️ Partial	[Limited policy]	[Strengthen policy]
Strict-Transport-Security	✅ Present	max-age=31536000	[HTTPS enforcement]
Referrer-Policy	❌ Missing	N/A	[Information leakage prevention]

7.3 Common Vulnerabilities Assessment

Vulnerability Type	Status	Risk Level	Evidence	Recommendation
SQL Injection	[Not Detected]	[Low]	[Parameterized queries used]	[Continue monitoring]
XSS	[Potential]	[Medium]	[User input not fully sanitized]	[Implement CSP]
CSRF	[Protection Present]	[Low]	[CSRF tokens implemented]	[Verify implementation]
Directory Traversal	[Not Detected]	[Low]	[Input validation present]	[Regular testing]
Information Disclosure	[Present]	[Medium]	[Server headers reveal versions]	[Hide version information]

7.4 Authentication and Access Control

- **Login Mechanism:** [Username/password, OAuth, SAML]
- **Multi-Factor Authentication:** [Enabled/Disabled/Optional]
- **Session Management:** [Secure cookies, timeout configured]
- **Password Policy:** [Length requirements, complexity rules]
- **Account Lockout:** [Enabled after X failed attempts]
- **Privilege Escalation Risks:** [Analysis of user roles and permissions]

---

8. Historical Analysis and Changes

8.1 Wayback Machine Analysis

First Archive: [YYYY-MM-DD]

Latest Archive: [YYYY-MM-DD]

Total Snapshots: [Number]

Date	Major Changes	Technology Changes	Security Relevance
[YYYY-MM-DD]	[Site redesign]	[PHP 5 to PHP 7]	[Security improvements]
[YYYY-MM-DD]	[Added login portal]	[Implemented HTTPS]	[Encryption added]
[YYYY-MM-DD]	[New admin section]	[Updated CMS]	[Potential new attack surface]

8.2 Content Evolution

- **Design Changes:** [Major redesigns, layout modifications]
- **Feature Additions:** [New functionality, services added]
- **Content Modifications:** [Policy changes, terms updates]
- **Contact Information Changes:** [Address, phone, email modifications]

8.3 Technology Migration History

- **[2020]:** Migrated from HTTP to HTTPS
- **[2021]:** Updated from PHP 5.6 to PHP 7.4
- **[2022]:** Implemented Cloudflare CDN
- **[2023]:** Added React.js frontend components
- **[2024]:** Upgraded WordPress to latest version

---

9. Search Engine and Social Media Presence

9.1 Search Engine Optimization (SEO)

Metric	Value	Industry Benchmark	Assessment
Page Speed Score	[85/100]	[90+]	[Needs optimization]
Mobile Friendliness	[Yes]	[Required]	[Compliant]
SSL Certificate	[Valid]	[Required]	[Compliant]
Meta Descriptions	[80% pages]	[100%]	[Improvement needed]
Structured Data	[Partial]	[Recommended]	[Expand implementation]

9.2 Search Engine Visibility

Google Search Results:

- Total indexed pages: [Approximately X pages]
- Branded searches: [High/Medium/Low visibility]
- Competitor comparison: [Better/Similar/Worse than competitors]

Notable Search Results:

- [Result 1]: [Context and relevance]
- [Result 2]: [Context and relevance]
- [Result 3]: [Context and relevance]

9.3 Social Media Integration

Platform	Integration Type	Data Sharing	Privacy Impact
Facebook	[Like Button, Pixel]	[User interactions]	[Cross-site tracking]
Twitter	[Tweet embedding]	[Minimal]	[Low impact]
LinkedIn	[Company page link]	[None]	[No impact]
Instagram	[Feed integration]	[User engagement]	[Moderate tracking]

---

10. API and Data Exposure Analysis

10.1 API Discovery

Identified APIs:

Endpoint	Method	Authentication	Purpose	Data Exposure Risk
/api/v1/users	GET	[Required]	[User data]	[High - PII exposure]
/api/v1/products	GET	[None]	[Product catalog]	[Low - public data]
/api/v2/orders	POST	[API Key]	[Order processing]	[High - financial data]
/api/internal/logs	GET	[None]	[System logs]	[Critical - internal data]

10.2 Data Leakage Assessment

Potential Data Exposure Points:

- [Exposed configuration files]
- [Unprotected API endpoints]
- [Verbose error messages]
- [Backup files accessible]
- [Source code in client-side]

10.3 File and Directory Enumeration

Sensitive Files/Directories Found:

Path	File Type	Content	Risk Level	Recommendation
/backup/	[Directory]	[Database dumps]	[Critical]	[Remove/protect immediately]
/.git/	[Directory]	[Source code]	[High]	[Remove from production]
/config.php	[Configuration]	[Database credentials]	[Critical]	[Protect/relocate]
/robots.txt	[Text file]	[Site structure]	[Low]	[Review disclosed paths]

---

11. Threat Intelligence Correlation

11.1 Known Threat Indicators

IOCs Associated with Domain:

- [IP addresses with poor reputation]
- [Domain mentioned in threat feeds]
- [Similar domains used in attacks]
- [Certificate fingerprints in threat data]

11.2 Vulnerability Database Correlation

CVE ID	Affected Component	CVSS Score	Exploitation Likelihood	Mitigation Status
[CVE-2024-XXXX]	[WordPress plugin]	[8.5]	[High]	[Patch available]
[CVE-2023-YYYY]	[Apache version]	[7.2]	[Medium]	[Not patched]

11.3 Dark Web and Breach Database Analysis

Compromised Credentials Found:

- Email addresses: [X found in breach databases]
- Passwords: [X hashed passwords discovered]
- Personal information: [Names, addresses, phone numbers]
- Financial data: [Credit card numbers, banking info]

Breach Timeline:

- [Date]: [Breach name/source] - [Data types compromised]
- [Date]: [Breach name/source] - [Data types compromised]

---

12. Business and Operational Intelligence

12.1 Business Information

- **Business Model:** [E-commerce, SaaS, Services, etc.]
- **Target Market:** [B2B, B2C, Geographic focus]
- **Revenue Streams:** [Product sales, subscriptions, advertising]
- **Key Partnerships:** [Identified through integrations and links]

12.2 Competitive Analysis

Competitor	Domain	Technology Overlap	Market Position
[Competitor 1]	[domain.com]	[WordPress, similar stack]	[Market leader]
[Competitor 2]	[domain.net]	[Different tech stack]	[Emerging player]

12.3 Contact and Location Intelligence

Physical Locations:

- Headquarters: [Address from WHOIS/website]
- Office locations: [Additional addresses found]
- Data centers: [Hosting locations identified]

Key Personnel:

- [Name] - [Position] - [Contact information] - [LinkedIn profile]
- [Name] - [Position] - [Contact information] - [Social media presence]

---

13. Risk Assessment and Scoring

13.1 Risk Matrix

Risk Category	Likelihood	Impact	Risk Score	Priority
Data Exposure	High	Critical	9.0	P1
Authentication Bypass	Medium	High	6.0	P2
Information Disclosure	High	Medium	6.0	P2
Malware Infection	Low	High	4.0	P3
DDoS Attack	Medium	Medium	4.0	P3

13.2 Overall Security Score

Security Rating: [X/10]

Scoring Breakdown:

- SSL/TLS Configuration: [8/10]

- Security Headers: [6/10]
- Software Updates: [5/10]
- Access Controls: [7/10]
- Data Protection: [4/10]

13.3 Business Risk Assessment

- **Reputation Risk:** [High/Medium/Low]
- **Operational Risk:** [High/Medium/Low]
- **Financial Risk:** [High/Medium/Low]
- **Legal/Compliance Risk:** [High/Medium/Low]

---

14. Recommendations and Remediation

14.1 Critical Actions (Immediate - 0-7 days)

1. **[Priority 1]:** Secure exposed backup directory
   - **Risk:** Critical data exposure
   - **Action:** Remove or implement authentication
   - **Effort:** 1 hour
2. **[Priority 2]:** Update outdated software components
   - **Risk:** Known vulnerability exploitation
   - **Action:** Update WordPress and plugins
   - **Effort:** 4 hours

14.2 High Priority Actions (Short-term - 1-4 weeks)

1. **Implement comprehensive Content Security Policy**
   - Prevent XSS attacks
   - Reduce third-party integration risks
2. **Enable multi-factor authentication**
   - Strengthen authentication mechanisms
   - Reduce credential-based attacks
3. **Conduct thorough security header review**
   - Implement missing security headers
   - Strengthen existing policies

14.3 Medium Priority Actions (Medium-term - 1-6 months)

1. **API security assessment and hardening**
2. **Regular vulnerability scanning implementation**
3. **Employee security awareness training**
4. **Incident response plan development**

14.4 Long-term Strategic Initiatives (6+ months)

1. **Zero-trust architecture implementation**
2. **Regular penetration testing program**
3. **Security monitoring and SIEM deployment**
4. **Business continuity and disaster recovery planning**

---

15. Monitoring and Follow-up

15.1 Recommended Monitoring

- **Domain expiration monitoring**
- **SSL certificate expiration alerts**
- **Subdomain enumeration (monthly)**
- **Technology stack vulnerability monitoring**
- **Dark web monitoring for credential exposure**

15.2 Follow-up Actions

- [ ] Schedule follow-up assessment in [X months]
- [ ] Implement continuous monitoring tools
- [ ] Establish security metrics and KPIs
- [ ] Regular reporting schedule to stakeholders

---

16. Appendices

Appendix A: Raw Technical Data

[Include raw tool outputs, command results, and detailed technical findings]

Appendix B: Screenshots and Visual Evidence

[Include relevant screenshots of findings, configuration issues, or security concerns]

Appendix C: Command History

```bash
# Domain enumeration commands
whois example.com
dig example.com ANY
nslookup example.com

# Subdomain discovery
subfinder -d example.com
amass enum -d example.com

# Website analysis
nikto -h https://example.com
dirb https://example.com

# SSL/TLS analysis
testssl.sh example.com
```

Appendix D: Additional Resources

- Certificate Transparency Logs: [URLs and findings]
- Threat Intelligence Sources: [Feeds and databases consulted]
- Third-party Security Reports: [External assessments referenced]

Appendix E: Glossary

- **API:** Application Programming Interface
- **CDN:** Content Delivery Network
- **CSP:** Content Security Policy
- **CVSS:** Common Vulnerability Scoring System
- **DNS:** Domain Name System
- **OSINT:** Open Source Intelligence
- **TLS:** Transport Layer Security

Document Control

Version	Date	Author	Changes
1.0	[YYYY-MM-DD]	[Analyst Name]	Initial analysis report
1.1	[YYYY-MM-DD]	[Analyst Name]	Updated findings and recommendations

Document Classification: [Confidential/Internal Use]
Distribution List:

- [Name] - [Role] - [Department]
- [Name] - [Role] - [Department]

Next Review Date: [YYYY-MM-DD]
Retention Period: [As per organizational policy]

This report contains sensitive security information and should be handled according to organizational data classification policies. Distribution should be limited to authorized personnel with a legitimate need to know. Any questions regarding this analysis should be directed to the cybersecurity team.