TUTELIS AEGIS

Website Vulnerabilty and Security Assessment

Client: **Example Company**
Date: 13 September 2025

Security Assessment

This report provides a comprehensive assessment of your website's security posture. Automated and manual scans (including vulnerability detection, configuration checks, and exploit analysis) have been performed to identify critical, high, medium, and low risk issues. Security findings are prioritised by severity, with critical vulnerabilities requiring immediate attention to maintain site functionality and protect user data.

GDPR & Compliance

The GDPR section reviews your website's compliance with privacy and data protection regulations. While some issues may overlap with security, GDPR findings focus on legal requirements, privacy notices, cookie management, and user rights. Addressing GDPR risks is essential for regulatory compliance, but security vulnerabilities are prioritised for their direct impact on site safety and operation.

Disclaimer: *This report is provided as a professional assessment to help clients understand and improve their website's security and regulatory posture. It is not a legal document and does not constitute legal advice.*

Table of Contents

Executive Summary

Security Summary

Overall Risk	Risk Ratings
Critical Note: Highest CVSS score (4.0 / 10) is from Vuln Detector, but overall risk is set by the most severe finding (Critical). 0.0/10 being excellent, 10/10 being critical	Critical: 1 High: 0 Medium: 3 Low: 2 Info: 0

CRITICAL SECURITY ALERT

1 CRITICAL VULNERABILITY DISCOVERED

Search Replace DB script found: https://example.com/searchreplacedb2.php CRITICAL

Database manipulation script exposed: https://example.com/searchreplacedb2.php. This allows attackers to modify database contents directly.

Source: WordPress Security

→ See WPScan Results section

⚡ IMMEDIATE ACTION REQUIRED

1. **Review each critical finding** in the detailed sections of this report
2. **Prioritise remediation** of these critical vulnerabilities immediately
3. **Consider taking affected systems offline** if they pose immediate risk
4. **Contact your development team or security consultant** for immediate assistance
5. **Schedule follow-up security assessment** after remediation is complete

GDPR / Cyber Essentials Summary

GDPR Status	Critical: No Privacy Policy Found

GDPR Summary	No privacy, legal, or GDPR compliance page was found on the website. This is a critical GDPR non-compliance issue. Immediate action is required.
Boilerplate Pages	0
Cyber Essentials Score	1.0/10 (Website Controls Compliant)
GDPR Score	10 / 10 ('0' = excellent compliance, '10' = serious compliance failings)

How We Calculate Security and GDPR Scores

CVSS (Common Vulnerability Scoring System) is an industry-standard method for rating the severity of security vulnerabilities. Each finding in this report is assigned a CVSS score from 0 (no risk) to 10 (critical risk), based on its potential impact and exploitability.
Note: For both CVSS and GDPR scores, a lower score is better. A score of 0 means excellent (no risk or full compliance), while a score of 10 means critical risk or major compliance gaps.

- **Security Score:** Calculated using the CVSS scores of all findings detected by automated tools (such as ZAP and Nuclei). Higher CVSS scores indicate more severe vulnerabilities.
- **GDPR Score:** Determined by evaluating your site’s compliance with key GDPR requirements, including data protection, privacy notices, cookie management, and user rights. Each GDPR finding is assessed for its impact on legal compliance and user privacy. The overall GDPR score reflects the proportion of requirements met, with deductions for missing or incomplete privacy features, lack of transparency, or non-compliance with user rights and data handling obligations.

Why this matters: CVSS scoring provides a transparent, objective way to prioritise remediation efforts. By understanding your overall security and GDPR scores, you can focus on the most critical issues first and demonstrate compliance to stakeholders.

WordPress Scan Summary

- **Search Replace DB script found: https://example.com/searchreplacedb2.php** (Severity: Critical)
- **WordPress readme found: https://example.com/readme.html** (Severity: Low)
- **This site has 'Must Use Plugins': https://example.com/wp-content/mu-plugins/** (Severity: Medium)
- **The external WP-Cron seems to be enabled: https://example.com/wp-cron.php** (Severity: Low)

Scope and Methodology

This assessment evaluates the security posture and compliance of the target website using a combination of automated and manual techniques. The following tools and methods were employed:

Web Application Security Testing

- **OWASP ZAP:** Automated vulnerability scanning and active web application testing for OWASP Top 10 vulnerabilities.
- **Nuclei:** Fast, template-based vulnerability scanning for known CVEs, misconfigurations, and security issues.
- **WPScan:** WordPress-specific vulnerability scanning for themes, plugins, and core vulnerabilities (when WordPress is detected).
- **Custom Vulnerability Detection:** Proprietary scripts for malware detection, advanced plugin analysis, and CMS security checks.

Infrastructure & Network Assessment

- **Amass:** Comprehensive subdomain enumeration and attack surface discovery using passive and active techniques.
- **Subfinder:** Fast subdomain discovery using multiple data sources and APIs.
- **DNSx:** DNS toolkit for subdomain resolution, validation, and DNS security analysis.
- **httpx:** HTTP toolkit for probing live hosts, technology detection, and web service discovery.

Reconnaissance & Asset Discovery

- **Puppeteer:** Automated browser-based reconnaissance, URL discovery, and screenshot capture.
- **Technology Detection:** Identification of web technologies, frameworks, and server configurations.
- **Attack Surface Mapping:** Comprehensive enumeration of accessible endpoints and services.

Compliance & Governance Assessment

- **GDPR Compliance Analysis:** Automated review of privacy policies, cookie usage, and data protection controls.
- **Cyber Essentials Framework:** Assessment against UK government security standards for small businesses.
- **Risk Scoring:** CVSS-style 0-10 scoring system for clear risk communication and prioritization.

Assessment Scope: All findings are based on the state of the website and accessible infrastructure at the time of testing. This assessment focuses on web application security with infrastructure reconnaissance.

For questions, clarifications, or enhanced security assessments, please contact the assessment team.

ZAP Vulnerability Summary

Understanding ZAP Security Ratings

ZAP findings show two important pieces of information: **Risk Level** and **Confidence Level**. For example, "Medium (High)" means a moderate security risk with high confidence it's a real issue.

ZAP Finding	Interpretation	Priority
High (High)	Critical vulnerability, definitely real	URGENT
Medium (High)	Moderate risk, very confident it exists	HIGH
Medium (Medium)	Moderate risk, probably real	MEDIUM
Low (High)	Minor issue, but definitely present	LOW
Info (High)	Informational finding, confirmed accurate	INFO

Tip: *Focus first on findings with "High" confidence levels, as these are most likely to be real security issues requiring attention.*

[redacted]

ZAP scan completed fo [redacted] *zap_scan (13 findings)*

Medium (High)

Title: Content Security Policy (CSP) Header Not Set
Description:

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

CVSS Score: 6.1
Affected URLs:

- https://example.com (GET)

Solution:

Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

References:

https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy

https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html

https://www.w3.org/TR/CSP/

https://w3c.github.io/webappsec-csp/

https://web.dev/articles/csp

https://caniuse.com/#feat=contentsecuritypolicy

https://content-security-policy.com/

Medium (Medium)

Title: Missing Anti-clickjacking Header
Description:

The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.

CVSS Score: 4.3
Affected URLs:

- https://example.com (GET)

Solution:

Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app.

If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.

References:

https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

Medium (High)

Title: Sub Resource Integrity Attribute Missing
Description:

The integrity attribute is missing on a script or link tag served by an external server. The integrity tag prevents an attacker who have gained access to this server from injecting a malicious content.

Affected URLs:

- https://example.com (GET)
- https://example.com (GET)
- https://example.com (GET)
- https://example.com (GET)
- https://example.com (GET)
- https://example.com (GET)
- https://example.com (GET)
- https://example.com (GET)
- https://example.com (GET)
- https://example.com (GET)
- https://example.com (GET)

Solution:

Provide a valid integrity attribute to the tag.

References:

https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity

Low (Medium)

Title: Cross-Domain JavaScript Source File Inclusion
Description:

The page includes one or more script files from a third-party domain.

Affected URLs:

- https://example.com (GET)
- https://example.com (GET)
- https://example.com (GET)
- https://example.com (GET)
- https://example.com (GET)
- https://example.com (GET)
- https://example.com (GET)
- https://example.com (GET)
- https://example.com (GET)
- https://example.com (GET)
- https://example.com (GET)

Solution:

Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.

Low (Medium)

Title: Insufficient Site Isolation Against Spectre Vulnerability
Description:

Cross-Origin-Resource-Policy header is an opt-in header designed to counter side-channels attacks like Spectre. Resource should be specifically set as shareable amongst different origins.

CVSS Score: 3.7
Affected URLs:

- https://example.com (GET)
- https://example.com (GET)
- https://example.com (GET)

Solution:

Ensure that the application/web server sets the Cross-Origin-Resource-Policy header appropriately, and that it sets the Cross-Origin-Resource-Policy header to 'same-origin' for all web pages.

'same-site' is considered as less secured and should be avoided.

If resources must be shared, set the header to 'cross-origin'.

If possible, ensure that the end user uses a standards-compliant and modern web browser that supports the Cross-Origin-Resource-Policy header (https://caniuse.com/mdn-http_headers_cross-origin-resource-policy).

References:

https://developer.mozilla.org/en-US/docs/Web/HTTP/Cross-Origin_Resource_Policy

Low (Medium)

Title: Permissions Policy Header Not Set
Description:

Permissions Policy Header is an added layer of security that helps to restrict from unauthorized access or usage of browser/client features by web resources. This policy ensures the user privacy by limiting or specifying the features of the browsers can be used by the web resources. Permissions Policy provides a set of standard HTTP headers that allow website owners to limit which features of browsers can be used by the page such as camera, microphone, location, full screen etc.

Affected URLs:

- https://example.com (GET)

Solution:

Ensure that your web server, application server, load balancer, etc. is configured to set the Permissions-Policy header.

References:

https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Permissions-Policy

https://developer.chrome.com/blog/feature-policy/

https://scotthelme.co.uk/a-new-security-header-feature-policy/

https://w3c.github.io/webappsec-feature-policy/

https://www.smashingmagazine.com/2018/12/feature-policy/

Low (High)

Title: Server Leaks Version Information via "Server" HTTP Response Header Field
Description:

The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.

CVSS Score: 2.6
Affected URLs:

- https://example.com (GET)
- https://example.com/robots.txt (GET)
- https://example.com/sitemap.xml (GET)

Solution:

Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

References:

https://httpd.apache.org/docs/current/mod/core.html#servertokens

https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)

https://www.troyhunt.com/shhh-dont-let-your-response-headers/

Low (High)

Title: Strict-Transport-Security Header Not Set
Description:

HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

CVSS Score: 3.1
Affected URLs:

- https://example.com (GET)
- https://example.com/robots.txt (GET)
- https://example.com/sitemap.xml (GET)

Solution:

Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

References:

https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html

https://owasp.org/www-community/Security_Headers

https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security

https://caniuse.com/stricttransportsecurity

https://datatracker.ietf.org/doc/html/rfc6797

Low (Medium)

Title: X-Content-Type-Options Header Missing
Description:

The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

Affected URLs:

- https://example.com (GET)

Solution:

Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.

If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.

References:

https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)

https://owasp.org/www-community/Security_Headers

Informational (Low)

Title: Information Disclosure - Suspicious Comments
Description:

The response appears to contain suspicious comments which may help an attacker.

CVSS Score: 2.0
Affected URLs:

- https://example.com (GET)
- https://example.com (GET)

Solution:

Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.

Informational (Medium)

Title: Modern Web Application
Description:

The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

Affected URLs:

- https://example.com (GET)

Solution:

This is an informational alert and so no changes are required.

Informational (Low)

Title: Re-examine Cache-control Directives
Description:

The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

CVSS Score: 1.0
Affected URLs:

- https://example.com (GET)

Solution:

For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".

References:

https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching

https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control

https://grayduck.mn/2021/09/13/cache-control-recommendations/

Informational (Medium)

Title: Storable and Cacheable Content
Description:

The response contents are storable by caching components such as proxy servers, and may be retrieved directly from the cache, rather than from the origin server by the caching servers, in response to similar requests from other users. If the response data is sensitive, personal or user-specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where "shared" caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.

CVSS Score: 1.5
Affected URLs:

- https://example.com (GET)
- https://example.com (GET)
- https://example.com/robots.txt (GET)
- https://example.com/sitemap.xml (GET)

Solution:

Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user:

Cache-Control: no-cache, no-store, must-revalidate, private

Pragma: no-cache

Expires: 0

This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.

References:

https://datatracker.ietf.org/doc/html/rfc7234

https://datatracker.ietf.org/doc/html/rfc7231

https://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html

Nuclei Scan Summary

Nuclei scan was performed, but no findings were detected.

Custom Vulnerability Detector Summary

Title:	Premium plugin detected: elementor-pro
Description:	Premium plugin "elementor-pro" detected. License verification recommended.
Severity:	**Medium**
Source:	Vuln Detector

Title:	Premium plugin detected: wpml-
Description:	Premium plugin "wpml-" detected. License verification recommended.
Severity:	**Medium**
Source:	Vuln Detector

WordPress Vulnerability Scan Results

WordPress Security Findings

- **Search Replace DB script found: https://example.com/searchreplacedb2.php**
  Database manipulation script exposed: https://example.com/searchreplacedb2.php. This allows attackers to modify database contents directly.
  Severity: Critical
- **WordPress readme found: https://example.com/readme.html**
  WordPress readme file exposed: https://example.com/readme.html. Reveals WordPress version information.
  Severity: Low
- **This site has 'Must Use Plugins': https://example.com/wp-content/mu-plugins/**
  Must-Use plugins directory accessible: https://example.com/wp-content/mu-plugins/. May reveal plugin information.
  Severity: Medium
- **The external WP-Cron seems to be enabled: https://example.com/wp-cron.php**
  External WP-Cron enabled: https://example.com/wp-cron.php. Could be used for DoS attacks.
  Severity: Low

GDPR & Cyber Essentials Summary

GDPR Compliance Overview

No privacy, legal, or GDPR compliance page was found on the website. This is a critical GDPR non-compliance issue. Immediate action is required.

GDPR Score: 10/10

Flagged Pages & Missing Sections

No flagged pages detected.

Cyber Essentials Assessment

⚠ Assessment Scope

This assessment covers website-level security controls only. Infrastructure controls such as firewalls, network security, and endpoint malware protection are outside the scope of this web application security assessment.

Website Controls Assessed:

- Web Application Configuration (secure settings, information disclosure)
- Application Access Control (authentication, session management)
- Component Management (web application patches, versions)
- Security Governance (GDPR compliance as indicator of security maturity)

Infrastructure Controls (Not Assessed):

- Network firewalls and gateway security
- Server-level malware protection
- Operating system security configuration
- Network access controls

Cyber Essentials Score: 1.0/10

('0' = excellent compliance, '10' = serious compliance failings)

Status: Website Controls Compliant

Risk Level: Low

UK Legal Requirements

For UK-based organizations: While Cyber Essentials is not yet legally mandatory for all businesses, it is increasingly becoming a requirement for:

- Government contracts (mandatory for contracts involving personal data and ICT)
- Insurance coverage (many cyber insurance policies require or offer discounts for certification)
- Supply chain requirements (larger organizations requiring suppliers to be certified)
- Professional services (demonstrating due diligence to clients)

For international organisations: Cyber Essentials provides an excellent framework for demonstrating security maturity and is recognised globally as a baseline security standard.

Areas for Improvement

- Overall Website Security: High-risk vulnerabilities present

Assessment Details

Your website demonstrates good security practices for the controls assessed. For full Cyber Essentials certification, you would also need to implement infrastructure controls (firewalls, endpoint protection) which are outside the scope of this assessment.

Website-Level Security Controls Assessed

1. **Web Application Configuration:** Ensuring web applications are configured securely and don't expose sensitive information
2. **Application Access Control:** Evaluating authentication mechanisms and session management controls
3. **Component Management:** Checking for outdated web application components and frameworks
4. **Security Governance:** GDPR compliance as an indicator of overall security policy maturity

***Note:** Full Cyber Essentials certification requires assessment of infrastructure controls (firewalls, endpoint protection, network security) which are outside the scope of this website security assessment.*

Next Steps

Address identified security issues before pursuing formal certification:

- Remediate the vulnerabilities identified in this assessment
- Implement proper security controls for the five key areas
- Consider engaging a security consultant for guidance
- Re-assess security posture after implementing improvements

Puppeteer Scan Results

What is Puppeteer?

Puppeteer is a powerful browser automation tool that allows us to programmatically control a web browser (Google Chrome/Chromium). It is used to simulate real user interactions, crawl websites, and collect data such as URLs, screenshots, and page content.

How Did We Use Puppeteer?

In this assessment, Puppeteer was used to automatically browse the target website, discover all accessible URLs, and capture screenshots of key pages. The collected URLs were then used as input for further security scans (e.g., ZAP, Nuclei) and GDPR compliance checks. This ensures that all parts of the site, including those not directly linked from the homepage, are tested for vulnerabilities and compliance issues.

What Did Puppeteer Find?

- Discovered and listed all accessible URLs on the site.
- Captured screenshots of main pages for documentation and review.
- Identified hidden or unlinked pages that may not be found by traditional scanners.
- Provided a comprehensive map of the site structure for use in subsequent scans.

The findings from Puppeteer were used to enhance the coverage and accuracy of the security and GDPR assessment.

No vulnerable JavaScript libraries were detected during the scan.

DNS Security Assessment (DNSx)

DNS Resolution Summary: 15 hosts successfully resolved from 15 discovered subdomains

Resolution Success Rate: 100.0% *- Good resolution rate*

Resolved Hosts

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

www.example.com

[redacted]

[redacted]

[redacted]

www.test.example.com

173.[redacted]

example.com

www.intranet.example.com

www.intra.example.com

Email Security Analysis

Mail Security Issues: 7/10

(0 = No Issues Found, 10 = Critical Issues Detected)

Mail Servers (MX Records)

- 20 alt1.aspmx.l.google.com.
- 20 alt2.aspmx.l.google.com.
- 10 aspmx.l.google.com.
- 30 aspmx3.googlemail.com.
- 30 aspmx2.googlemail.com.

✅ SPF Record Found

```
v=spf1 include:_spf.google.com ~all
```

✕ DMARC Record Missing

No DMARC record found - advanced email authentication not configured

Mail Security Findings

Secure Mail Provider: Using reputable mail provider: 20 alt1.aspmx.l.google.com.

SPF Soft Fail: SPF policy uses soft fail (~all) - consider upgrading to hard fail (-all)

Infrastructure Analysis

DNS Security Recommendations

DMARC Configuration MEDIUM

Recommendation: Implement DMARC policy for email authentication

Benefit: Advanced protection against email-based attacks

Recommendations

Security Hardening

Based on the findings, consider the following:

- **Search Replace DB script found: https://example.com/searchreplacedb2.php:** Database manipulation script exposed: https://example.com/searchreplacedb2.php. This allows attackers to modify database contents directly.
- **This site has 'Must Use Plugins': https://example.com/wp-content/mu-plugins/:** Must-Use plugins directory accessible: https://example.com/wp-content/mu-plugins/. May reveal plugin information.
- **Premium plugin detected: elementor-pro:** Premium plugin "elementor-pro" detected. License verification recommended.
- **Premium plugin detected: wpml-:** Premium plugin "wpml-" detected. License verification recommended.

Glossary

- **CVSS (Common Vulnerability Scoring System):** An industry-standard method for rating the severity of security vulnerabilities, scored from 0 (no risk) to 10 (critical risk).
- **Cyber Essentials:** A UK government-backed scheme that helps organizations protect themselves against common cyber threats.
- **Data Controller:** The person or organization that determines how and why personal data is processed.
- **GDPR (General Data Protection Regulation):** A European law that governs how personal data must be handled and protected.
- **ICO (Information Commissioner’s Office):** The UK’s independent authority set up to uphold information rights and data privacy.
- **Nuclei:** An automated security scanning tool used to detect vulnerabilities and misconfigurations in web applications and infrastructure.
- **OWASP ZAP (Zed Attack Proxy):** An open-source web application security scanner used to find vulnerabilities in websites.
- **Privacy Policy:** A statement that explains how an organization collects, uses, and protects personal data.
- **Risk Rating:** A classification (Critical, High, Medium, Low, Info) that indicates the severity of a security issue or vulnerability.
- **Severity:** The level of impact a vulnerability or issue may have on the security or privacy of a system.
- **Vulnerability:** A weakness in a system that could be exploited to compromise its security or data.
- **WPScan:** An open-source WordPress security scanner developed by Automattic. WPScan is used to identify vulnerabilities, misconfigurations, and outdated plugins or themes in WordPress websites.

Appendix

Website Screenshot

No screenshot available.

Methodology Details

This comprehensive security assessment employed multiple industry-standard tools and methodologies to identify vulnerabilities, misconfigurations, and compliance gaps across web applications, infrastructure, and privacy implementations.

Scanning Tools & Techniques

- **OWASP ZAP (Zed Attack Proxy)** - Comprehensive web application security testing including automated crawling, passive/active vulnerability detection, and authentication testing
- **Nuclei** - High-speed vulnerability scanner using community-maintained templates for CVE detection, misconfigurations, and security checks
- **WPScan** - WordPress-specific security scanner for plugin/theme vulnerabilities, user enumeration, and configuration issues
- **Nmap** - Network discovery and port scanning to identify open services and potential attack vectors
- **Amass** - Advanced subdomain enumeration using multiple data sources and techniques
- **DNSx** - DNS toolkit for resolution, validation, and security analysis
- **httpx** - Fast HTTP probe for service detection and response analysis
- **Subfinder** - Passive subdomain discovery tool

Assessment Scope

- Web application vulnerability assessment
- Infrastructure security evaluation
- WordPress-specific security analysis (where applicable)
- GDPR compliance review
- Network security assessment
- SSL/TLS configuration analysis
- Subdomain enumeration and analysis

Limitations

- Assessment reflects the security posture at the time of testing
- Limited to publicly accessible components and interfaces
- No source code review or internal network assessment performed
- Cloudflare-protected sites may have limited scan coverage

References & Links

- CVSS (Common Vulnerability Scoring System)
- GDPR (General Data Protection Regulation)
- Cyber Essentials
- OWASP ZAP
- Nuclei
- WPScan (WordPress Security Scanner)
- Nmap (Network Mapper)
- Amass (Subdomain Enumeration)

- DNSx (DNS Toolkit)
- httpx (HTTP Toolkit)
- Subfinder

Change Log

- Version 1.0 - Initial assessment and report generation.

Contact Information

Website: https://www.tutelis.eu / https://www.tutelis.co.uk
Email: audit@tutelis.eu