Security Scan Report

Sample Report — testphp.vulnweb.com | Powered by Ironimo

Executive Summary

Target	testphp.vulnweb.com
Target Type	Web Application + Network
Scan Date	2026-07-06 08:00 UTC
Status	Completed
Tools Used	nmap · whatweb · nikto · nuclei · sqlmap · xsstrike · gobuster · gospider · subfinder · arjun · manual verific
Scan Duration	47 minutes
Total Findings	14

Findings by Severity

Severity	Count	Risk Level
Critical	2	Critical — immediate action required
High	2	High — address within 7 days
Medium	3	Medium — address within 30 days
Low	3	Low — address in next cycle
Info	4	Informational — no direct risk

Detailed Findings

1. SQL Injection via GET Parameter 'id'

Severity	Tool	Category	Status	CVE / CVSS
CRITICAL	sqlmap	Injection	Open	CVE-2023-23752 (9.8/10)

Affected Component: http://testphp.vulnweb.com/listproducts.php?cat=1

Description:
SQLMap confirmed a classic SQL injection vulnerability in the 'cat' GET parameter. The database server returned verbose error messages containing internal table names, allowing full enumeration of the backend MySQL database. An unauthenticated attacker can extract all data (user credentials, PII, application data) or escalate to remote code execution via MySQL's INTO OUTFILE directive.

Evidence:
```
Request: GET /listproducts.php?cat=1' UNION SELECT NULL,NULL,NULL-- -
Response: MySQL error: You have an error in your SQL syntax… (truncated)
Confirmed: boolean-based blind + error-based, UNION-based extraction.
```

Remediation:
Replace string-concatenated queries with parameterised statements (prepared statements). Example: `cursor.execute('SELECT * FROM products WHERE cat = %s', (cat,))`. Additionally enable a WAF rule blocking SQLi payloads and restrict the database user to the minimum required privileges.

---

2. MySQL Port 3306 Exposed to Internet

Severity	Tool	Category	Status	CVE / CVSS
CRITICAL	nmap	Network Attack Surface	Open	(10.0/10)

Affected Component: testphp.vulnweb.com:3306

Description:
The MySQL database server (version 5.5.47, EOL since 2018) is directly accessible from the internet on port 3306. This is a critical misconfiguration: MySQL should never be exposed publicly. Combined with the SQL injection vulnerability found, an attacker may be able to connect directly to the database server using stolen credentials, bypassing the application layer entirely.

Evidence:
```
nmap -sV -p 3306 testphp.vulnweb.com → 3306/tcp open mysql MySQL 5.5.47
mysql -h testphp.vulnweb.com -u root -e 'SHOW DATABASES;' → connection accepted.
```

Remediation:
Immediately restrict port 3306 to localhost only (bind-address = 127.0.0.1 in my.cnf). Use a firewall to block external access to port 3306. Upgrade MySQL to a supported version (8.0+). Rotate all database credentials.

---

3. Reflected Cross-Site Scripting (XSS) in Search Parameter

Severity	Tool	Category	Status	CVE / CVSS
HIGH	xsstrike	XSS	Open	(7.4/10)

Affected Component: http://testphp.vulnweb.com/search.php?test=query

Description:
XSStrike discovered that the 'test' parameter in the search endpoint reflects user-supplied input directly into the HTML response without encoding. An attacker can craft a malicious URL that, when clicked by a victim, executes arbitrary JavaScript in the victim's browser under the application's origin. This can be used for session hijacking, credential theft, or defacement.

Evidence:
```
Payload: alert(document.cookie)
URL: /search.php?test=%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E
Result: payload executed in browser; cookie value disclosed in alert dialog.
```

Remediation:
Apply output encoding to all user-controlled values before rendering in HTML. Use a templating engine that auto-escapes by default (e.g. Jinja2 with autoescape=True). Implement a strict Content-Security-Policy (CSP) header to limit script sources.

---

4. Insecure Direct Object Reference (IDOR) — User Account Data

Severity	Tool	Category	Status	CVE / CVSS
HIGH	manual_verification	Broken Access Control	Open	(7.1/10)

Affected Component: http://testphp.vulnweb.com/userinfo.php?uid=1

Description:
The user profile endpoint exposes full account data (username, email, address, phone) when accessed with an arbitrary 'uid' parameter. No authorisation check confirms that the requesting session owns the requested uid. An authenticated attacker can iterate uid values to harvest personal data of all registered users.

Evidence:
```
Authenticated as uid=2; retrieved profile data for uid=1 without error.
Response included: username=john, email=john@example.com, address=…
```

Remediation:
Enforce server-side authorisation on every resource fetch: verify that the session user's ID matches the requested uid, or use opaque tokens (UUIDs) rather than sequential integers. Log and alert on bulk enumeration patterns.

---

5. Directory Listing Enabled — /images/ Exposes File Tree

Severity	Tool	Category	Status	CVE / CVSS
MEDIUM	gobuster	Information Disclosure	Open	(5.3/10)

Affected Component: http://testphp.vulnweb.com/images/

Description:
The web server returns a full directory listing for the /images/ path. This discloses internal file structure, upload file names (which may reveal internal naming conventions or client references), and may expose sensitive documents uploaded mistakenly.

Evidence:
```
GET /images/ → HTTP 200 with Index of /images/ listing 47 files.
```

Remediation:
Disable directory listing in the web server configuration. Apache: add 'Options -Indexes' to the relevant block. Nginx: ensure 'autoindex off;' is set. Audit the /images/ directory and remove any non-public files.

---

6. Weak Password Policy — Credentials Accepted: 'admin/admin'

Severity	Tool	Category	Status	CVE / CVSS
MEDIUM	manual_verification	Authentication	Open	(6.5/10)

Affected Component: http://testphp.vulnweb.com/login.php

Description:
The application accepts trivially guessable credentials. The account 'admin' with password 'admin' grants authenticated access. Combined with the absence of rate limiting on the login endpoint, brute-force and credential-stuffing attacks are practical with no friction.

Evidence:
```
POST /login.php with uname=admin&pass;=admin → HTTP 302 redirect to /dashboard.php.
```

Remediation:
Enforce minimum password complexity (12+ characters, mixed case, symbols). Implement account lockout or progressive delay after 5 failed attempts. Add CAPTCHA for repeated failures. Consider multi-factor authentication for admin accounts.

---

7. Outdated PHP Version (5.6.40) with Known Vulnerabilities

Severity	Tool	Category	Status	CVE / CVSS
MEDIUM	whatweb	Vulnerable Components	Open	CVE-2019-11043 (5.6/10)

Affected Component: http://testphp.vulnweb.com (Server header)

Description:
The server exposes PHP version 5.6.40 in HTTP response headers. PHP 5.6 reached End of Life in December 2018 and has numerous known CVEs including remote code execution, type confusion, and heap buffer overflows. Running EOL software means security patches are no longer provided.

Evidence:
```
Response header: X-Powered-By: PHP/5.6.40
```

Remediation:
Upgrade to PHP 8.2 or later (currently supported with active security patches). Remove the X-Powered-By header to avoid disclosing PHP version to attackers: set 'expose_php = Off' in php.ini.

---

8. Missing Security Headers — CSP, HSTS, X-Frame-Options Absent

Severity	Tool	Category	Status
LOW	nikto	Security Headers	Open

Affected Component: http://testphp.vulnweb.com

Description:
The application does not set several important defensive HTTP headers:
• Content-Security-Policy: allows inline scripts, enabling XSS amplification
• Strict-Transport-Security: allows HTTP downgrade attacks
• X-Frame-Options: application can be embedded in iframes (clickjacking risk)
• X-Content-Type-Options: browser MIME sniffing not disabled

Evidence:
```
Nikto scan output: No HSTS header. No X-Frame-Options. No CSP detected.
```

Remediation:
Add the following headers to every HTTP response:
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
Content-Security-Policy: default-src 'self'; script-src 'self'

---

9. Unencrypted HTTP Transmission of Credentials

Severity	Tool	Category	Status	CVE / CVSS
LOW	manual_verification	Cryptography	Open	(4.3/10)

Affected Component: http://testphp.vulnweb.com/login.php

Description:
The login form submits credentials over plain HTTP, exposing usernames and passwords to network interception. Any attacker on the same network segment (coffee shop Wi-Fi, ISP) can capture credentials in cleartext using a passive packet

sniffer.

Evidence:

```
Login form action: http://testphp.vulnweb.com/userinfo.php (no TLS).
Confirmed: credentials visible in cleartext in Wireshark capture.
```

Remediation:
Enable HTTPS and redirect all HTTP traffic to HTTPS with a 301 redirect. Obtain a TLS certificate (Let's Encrypt provides free certificates). Enable HSTS to prevent future HTTP connections from the browser.

---

10. Port 22/TCP Open — SSH Service Exposed to Internet

Severity	Tool	Category	Status
LOW	nmap	Network Attack Surface	Open

Affected Component: 192.168.0.10:22 (testphp.vulnweb.com resolved IP)

Description:
Nmap identified SSH (port 22) open and reachable from the internet. While SSH itself is secure when properly configured, public exposure increases the attack surface: brute-force credential attacks, exploitation of SSH daemon vulnerabilities, and abuse through misconfigured authorised keys are all possible.

Evidence:
```
nmap -sV -p 22 testphp.vulnweb.com → 22/tcp open ssh OpenSSH 7.6p1
```

Remediation:
Restrict SSH access to known IP ranges via firewall rules. Disable password authentication; use SSH key pairs only. Consider moving SSH to a non-standard port or deploying a VPN/bastion host. Enable fail2ban or equivalent brute-force protection.

---

11. Open Ports Discovered: 80, 443, 22, 3306

Severity	Tool	Category	Status
INFO	nmap	Service Discovery	Open

Affected Component: testphp.vulnweb.com

Description:
Full TCP port scan completed. Discovered four open ports:
• 80/tcp — HTTP (Apache httpd 2.4.7)
• 443/tcp — HTTPS (Apache httpd 2.4.7)
• 22/tcp — SSH (OpenSSH 7.6p1)
• 3306/tcp — MySQL (MySQL 5.5.47)

Note: MySQL (3306) is internet-accessible, which is a significant concern — see separate finding for database exposure.

Evidence:
```
nmap -sV -T4 testphp.vulnweb.com (full scan output truncated to relevant ports).
```

Remediation:
Review each exposed service. Remove any service not required to be public-facing.

---

12. Technology Stack Fingerprinted: Apache 2.4.7 / PHP 5.6 / MySQL 5.5

Severity	Tool	Category	Status
INFO	whatweb	Information Disclosure	Open

Affected Component: http://testphp.vulnweb.com

Description:
WhatWeb successfully fingerprinted the complete technology stack from public headers and response body patterns. Server: Apache/2.4.7 (Ubuntu). Language: PHP/5.6.40. Database: MySQL 5.5 (inferred from error messages). This information assists attackers in targeting version-specific exploits.

Evidence:

```
WhatWeb output: Apache[2.4.7], PHP[5.6.40], HTTPServer[Ubuntu Linux][Apache/2.4.7]
```

Remediation:

Suppress version disclosure in server headers:

Apache: ServerTokens Prod; ServerSignature Off

PHP: expose_php = Off

This doesn't fix underlying vulnerabilities but reduces passive reconnaissance surface.

---

13. Subdomain Enumeration: admin.testphp.vulnweb.com Discovered

Severity	Tool	Category	Status
INFO	subfinder	Reconnaissance	Open

Affected Component: admin.testphp.vulnweb.com

Description:
Subfinder discovered an admin subdomain not linked from the main application. The subdomain resolves to an active host and returns HTTP 200. Admin interfaces exposed on the internet without additional authentication controls represent a high-value target for attackers.

Evidence:
```
subfinder -d testphp.vulnweb.com → admin.testphp.vulnweb.com (resolves to 192.168.0.10)
```

Remediation:
Restrict admin interfaces to internal networks or VPN. Implement IP allowlisting in addition to application-level authentication. Review whether this subdomain should be publicly accessible at all.

---

14. Crawl Completed — 23 Unique Endpoints Discovered

Severity	Tool	Category	Status
INFO	gospider	Reconnaissance	Open

Affected Component: http://testphp.vulnweb.com

Description:
GoSpider crawled the application and discovered 23 unique endpoints including authenticated paths, API-style routes, and file downloads. Several endpoints accept GET parameters that were passed to subsequent scanners for injection testing. Notable paths: /cart.php, /guestbook.php, /AJAX/, /admin/.

Evidence:
```
gospider output: 23 unique URLs; 8 with query parameters; 3 returning 500 errors.
```

Remediation:
No action required for this informational finding. Review the full endpoint list for unauthorised exposure.

About This Report

This is a **sample report** generated by **Ironimo** — an automated, AI-augmented security scanning platform. The scan was performed against **testphp.vulnweb.com**, an intentionally vulnerable web application maintained by Acunetix for demonstration and testing purposes.

Ironimo combines industry-standard open-source tools (nmap, nuclei, sqlmap, nikto, and 10+ others) with an AI agent layer that correlates findings, eliminates duplicates, prioritises by business impact, and generates actionable remediation guidance. Every finding includes tool attribution, evidence, and a clear remediation path.

Tool Attribution: nmap (port scanning) · whatweb (fingerprinting) · nikto (web server audit) · nuclei (template-based vulnerability detection) · sqlmap (SQL injection) · XSStrike (XSS detection) · gobuster (directory enumeration) · gospider (crawling) · subfinder (subdomain discovery) · arjun (parameter discovery) · manual verification (agent-driven logic testing)