Vulnerability Assessment Report: testphp.vulnweb.com

SECURITY SCORE: 0/100

OVERALL RISK LEVEL: CRITICAL

1. Network Scan Results (Nmap)

Port	Service	Version	State
80	http	1.19.0	open

2. Web Vulnerability Results (Nikto)

```
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP: 44.228.249.3
+ Target Hostname: testphp.vulnweb.com
+ Target Port: 80
+ Start Time: 2026-02-22 13:50:04 (GMT0)
---------------------------------------------------------------------------
+ Server: nginx/1.19.0
+ Retrieved x-powered-by header: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
+ The anti-clickjacking X-Frame-Options header is not present.
+ Server leaks inodes via ETags, header found with file /clientaccesspolicy.xml, fields:
0x5049b03d 0x133
+ /clientaccesspolicy.xml contains a full wildcard entry. See
http://msdn.microsoft.com/en-us/library/cc197955(v=vs.95).aspx
+ lines
+ /crossdomain.xml contains a full wildcard entry. See
http://jeremiahgrossman.blogspot.com/2008/05/crossdomainxml-invites-cross-site.html
+ /crossdomain.xml contains 0 line which should be manually viewed for improper domains
or wildcards.
+ 26 items checked: 4 error(s) and 7 item(s) reported on remote host
+ End Time: 2026-02-22 13:50:40 (GMT0) (36 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

[nikto stderr]
+ ERROR: Host maximum execution time of 180 seconds reached
```

3. Crawled Website Endpoints

- http://testphp.vulnweb.com/categories.php
- http://testphp.vulnweb.com/AJAX/index.php
- [FORM] http://testphp.vulnweb.com/search.php?test=query
- http://testphp.vulnweb.com/privacy.php
- http://testphp.vulnweb.com/hpp/
- http://testphp.vulnweb.com/Mod_Rewrite_Shop/
- http://testphp.vulnweb.com/userinfo.php
- http://testphp.vulnweb.com/index.php

- http://testphp.vulnweb.com/guestbook.php
- http://testphp.vulnweb.com/artists.php
- http://testphp.vulnweb.com/cart.php
- http://testphp.vulnweb.com/login.php
- http://testphp.vulnweb.com/disclaimer.php

4. Vulnerability Intelligence (CVE Mapping)

Modern Vulnerabilities in php 5.6.40
- {'cve_id': 'CVE-2019-6977', 'description': 'gdImageColorMatch in gd_color_match.c in the GD Graphics Library (aka LibGD) 2.2.5, as used in the imagecolormatch function in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1, has a heap-based buffer overflow. This can be exploited by an attacker who is able to trigger imagecolormatch calls with crafted image data.', 'score': 8.8, 'severity': 'HIGH'}
- {'cve_id': 'CVE-2019-9020', 'description': 'An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. Invalid input to the function xmlrpc_decode() can lead to an invalid memory access (heap out of bounds read or read after free). This is related to xml_elem_parse_buf in ext/xmlrpc/libxmlrpc/xml_element.c.', 'score': 9.8, 'severity': 'CRITICAL'}
- {'cve_id': 'CVE-2019-9021', 'description': 'An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. A heap-based buffer over-read in PHAR reading functions in the PHAR extension may allow an attacker to read allocated or unallocated memory past the actual data when trying to parse the file name, a different vulnerability than CVE-2018-20783. This is related to phar_detect_phar_fname_ext in ext/phar/phar.c.', 'score': 9.8, 'severity': 'CRITICAL'}
- {'cve_id': 'CVE-2019-9023', 'description': 'An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. A number of heap-based buffer over-read instances are present in mbstring regular expression functions when supplied with invalid multibyte data. These occur in ext/mbstring/oniguruma/regcomp.c, ext/mbstring/oniguruma/regexec.c, ext/mbstring/oniguruma/regparse.c, ext/mbstring/oniguruma/enc/unicode.c, and ext/mbstring/oniguruma/src/utf32_be.c when a multibyte regular expression pattern contains invalid multibyte sequences.', 'score': 9.8, 'severity': 'CRITICAL'}
- {'cve_id': 'CVE-2019-9024', 'description': 'An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. xmlrpc_decode() can allow a hostile XMLRPC server to cause PHP to read memory outside of allocated areas in base64_decode_xmlrpc in ext/xmlrpc/libxmlrpc/base64.c.', 'score': 7.5, 'severity': 'HIGH'}
Legacy Vulnerability Intelligence

5. Attack Possibilities & Mitigation