

Evidence Screenshots

```
⌚ 0s ~ 
• ➔ sudo pacman -S nmap
[sudo] password for kodo:
resolving dependencies...
looking for conflicting packages...

Package (1) New Version Net Change Download Size

extra/nmap 7.98-4 25.86 MiB 5.92 MiB

Total Download Size: 5.92 MiB
Total Installed Size: 25.86 MiB

:: Proceed with installation? [Y/n] y
:: Retrieving packages...
nmap-7.98-4-x86_64 5.9 MiB 850 KiB/s 00:07 [-----] 100%
(1/1) checking keys in keyring [-----] 100%
(1/1) checking package integrity [-----] 100%
(1/1) loading package files [-----] 100%
(1/1) checking for file conflicts [-----] 100%
:: Processing package changes...
(1/1) installing nmap [-----] 100%
:: Running post-transaction hooks...
(1/1) Arming ConditionNeedsUpdate...
⌚ 28s ~ 
• ➔ nmap testphp.vulnweb.com
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-13 05:29 +0530
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.32s latency).
Other addresses for testphp.vulnweb.com (not scanned): 64:ff9b::2ce4:f903
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 20.42 seconds
⌚ 20s ~ 
• ➔ |
```

acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art go

welcome to our page

Test site for Acunetix WVS.

Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo

Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer

About Us | Privacy Policy | Contact Us | Shop | HTTP Parameter Pollution | ©2019 Acunetix Ltd

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

Inspector Console Debugger Network Style Editor Performance Memory ... X

Filter URLs

All HTML CSS JS XHR Fonts Images Media WS Other

S M D... File Ini... T Tr... S Headers Cookies Request Response Timings

2 G / do... ht 2... 4. Filter Headers

2 G te... style.css st... cs ca... 5. Server: nginx/1.19.0

2 G fav... favicon.ico img x- ca... 86 Transfer-Encoding: chunked

X-Powered-By: PHP/5.6.40-38+ubuntu20.041+deb.sury.org+1

3 requests | 11.33 kB / 2.55 kB tra

acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

welcome to our page

Test site for Acunetix WVS.

Out art
Off categories
categories
0 se artists
0 art
3 ip
your profile
3 questbook
1 Demo
s
submit

History WebSockets

Sites Start Start Start Off 0 3 3

0 Page Alerts

High Medium Low Informational

Absence of Anti-CSRF Tokens (1)

Content Security Policy (CSP) Header Not Set (1)

Missing Anti-clickjacking Header (1)

Page Alerts

x

High

Medium

Low

Informational

Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (1)

Server Leaks Version Information via "Server" HTTP Response Header Field (1)

X-Content-Type-Options Header Missing (1)

Page Alerts

x

High

Medium

Low

Informational

Charset Mismatch (Header Versus Meta Content-Type Charset) (1)