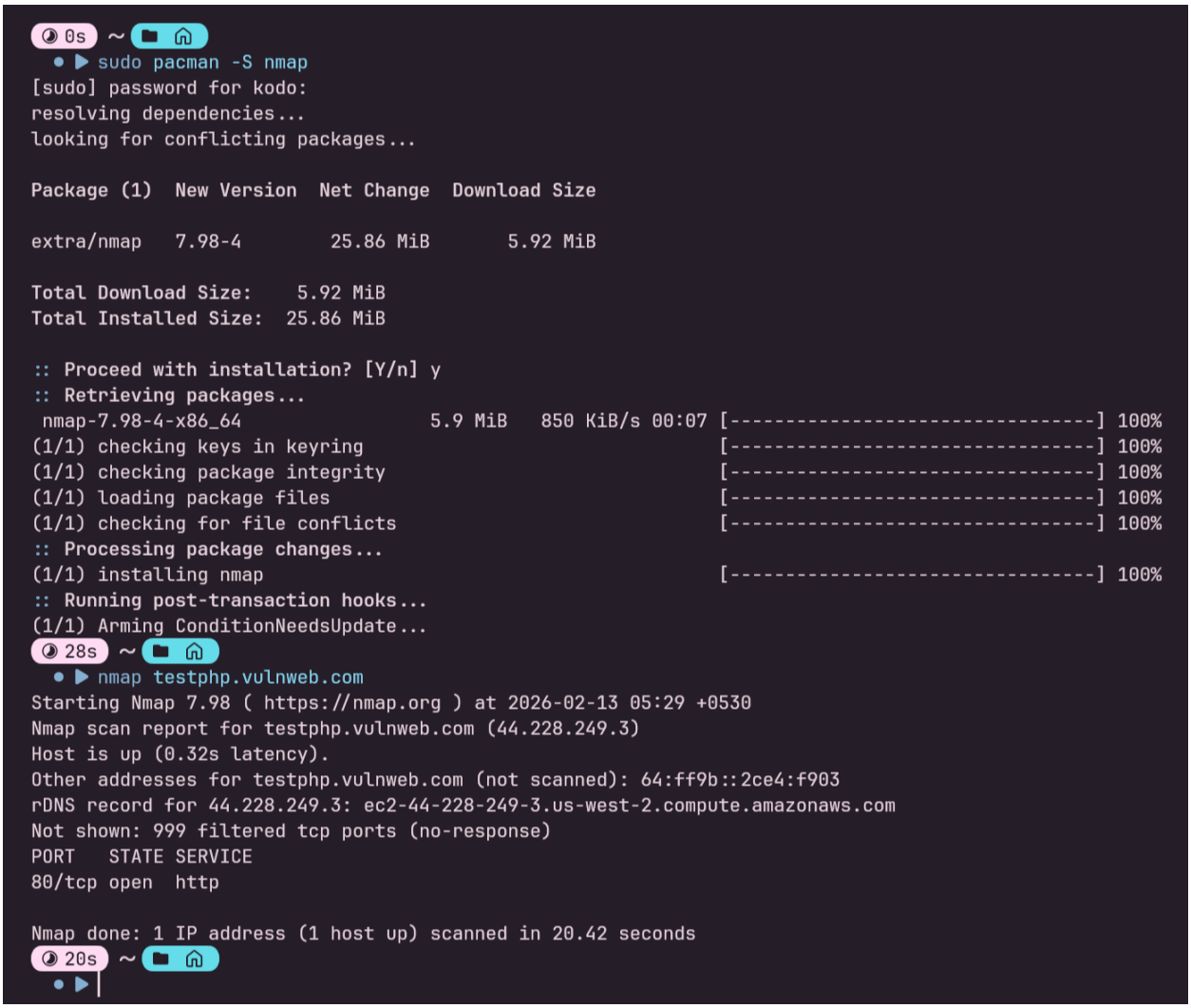
Evidence Screenshorts



acunetix acuart

TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

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

search art
go

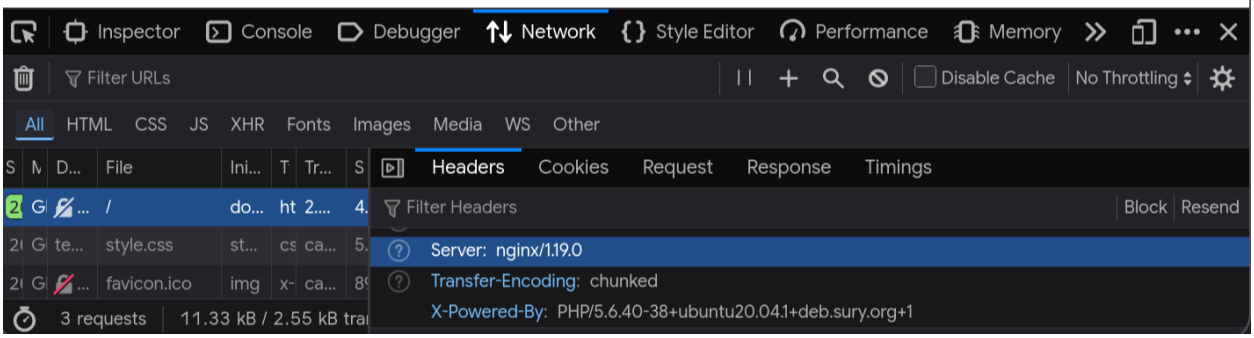
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo

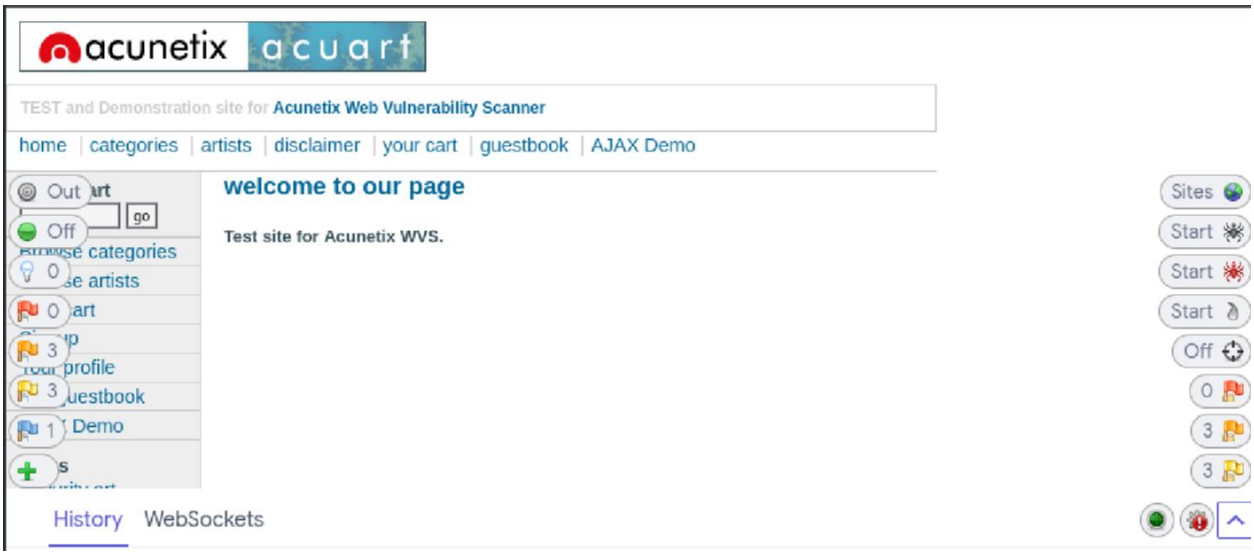
Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer

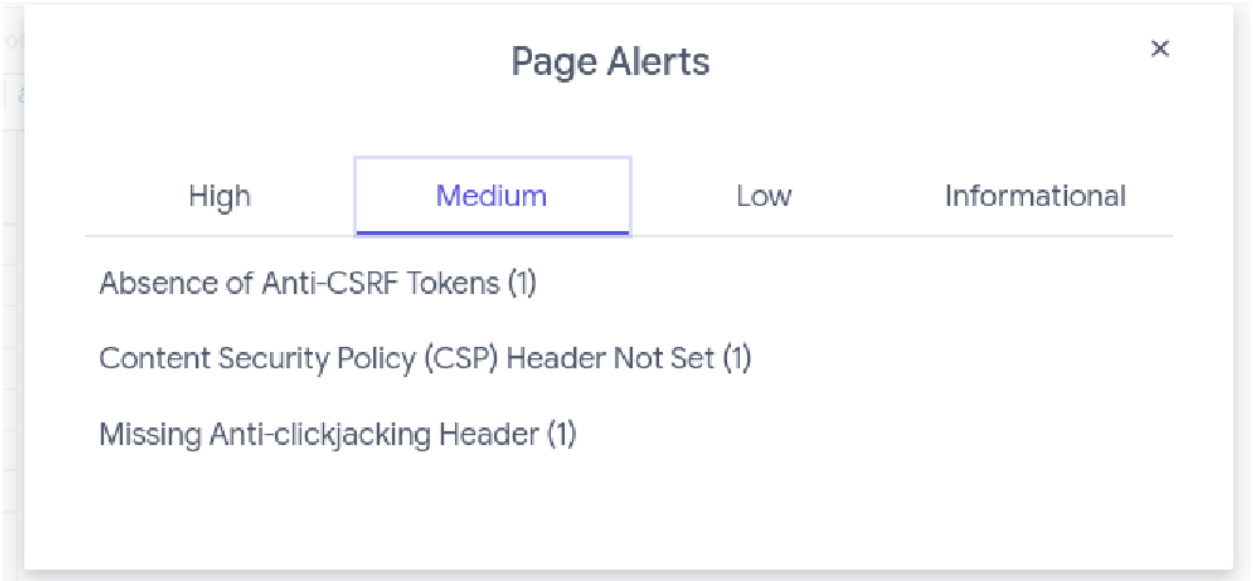
welcome to our page

Test site for Acunetix WVS.

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.




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.
Sites
Start
Start
Start
Off
History
WebSockets


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

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

High | Medium | Low | Informational

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