Title: Critical Web Vulnerabilities

Tool: Nikto

Host: http://192.168.68.105/dvwa/login.php

Finding (from Nikto)	**What it really means**	**CVE / Reference**	**CVSS v3.1 (official if available)**	**Quick fix**
/?-s and ...login.php ?-s → *"PHP allows retrieval of source via -s"*	Classic **PHP-CGI argument injection / RCE** bucket. Nikto's -s hints the 2012 PHP-CGI bug.	**CVE-2012-1823**	**9.8 (Critical)**	Disable PHP-CGI, block ? args to CGI, or upgrade PHP (any modern PHP is fixed). (NVD, Red Hat Customer Portal)
Server: Apache/2.2.8 (very old)	**EOL httpd 2.2** → exposed to many unpatched vulns; not a single CVE to score. Treat as **policy/high risk**.	Apache notes on **2.2 EOL**	N/A (multiple CVEs)	Upgrade to a supported **Apache 2.4.x** immediately. (Apache HTTP Server, endoflife.date)
HTTP TRACE enabled	**Cross-Site Tracing (XST)** risk; often used to echo headers/cookies via JS. Misconfig, not one CVE.	OWASP XST / WSTG	Use custom CVSS if required (often **Low–Medium**): e.g., AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N ≈ **3.1 (Low)**	Disable TRACE/TRACK (e.g., TraceEnable off in Apache). (OWASP)

Lots of /*.tgz, *.tar, *.war, *.pem, *.jks, *.egg	Likely **backup/key dumps exposed** → **Info disclosure** (can be severe if secrets).	CWE-530 reference in Nikto	If files contain secrets: AV:N/AC:L/PR:N/UI:N/S:U/**C:H**/I:N/A:N ≈ **7.5 (High)**	Remove from web root; rotate keys; restrict direct download. (Confirm by actually fetching one benign file.)
SIPS v0.2.2 ... user account info (including password) retrievable	Auth bypass/info disclosure in **SIPS 0.2.2**. Old but real. Might not have a CVE; has Exploit-DB ref.	EDB-22381	If credentials exposed unauthenticated: AV:N/AC:L/PR:N/UI:N/S:U/**C:H**/I:N/A:N ≈ **7.5 (High)**	Remove/patch SIPS; block the path; rotate exposed passwords. (Exploit Database, Vulners)
/?=PHPE... (OSVDB-12184)	**PHP version/info disclosure** via magic query tokens.	OSVDB-12184 discussion	Usually **Low**: AV:N/AC:L/PR:N/UI:N/S:U/**C:L**/I:N/A:N ≈ **3.3**	Disable expose_php, update PHP, block these routes. (Server Fault, seclists.org, dev.nmap.narkive.com)
Missing headers: **X-Frame-Options**, **X-Content-Type-Options**, cookies without **HttpOnly**	Security-hardening gaps; not CVEs, but exploitable in chains (clickjacking, MIME-sniff, scriptable cookies).	MDN/OWASP	Treat as **Low** each, but fix as hygiene.	Add X-Frame-Options/Content-Security-Policy frame-ancestors, X-Content-Type-Options: nosniff, set HttpOnly; Secure; SameSite on cookies. (MDN Web Docs, OWASP)