



The screenshot shows a web browser window with the title "Damn Vulnerable Web Application (DVWA)Source :: Damn Vulnerable Web Application (DVWA) - Chromium". The address bar displays the URL "http://localhost/DVWA/vulnerabilities/view_source.php?id=fi&security=medium". The main content area is titled "File Inclusion Source" and shows the source code for "vulnerabilities/fi/source/medium.php". The code is a PHP script that takes a file path from the 'page' GET parameter, performs basic validation by replacing 'http://' with 'https://' and removing '..\' characters, and then includes the file. A "Compare All Levels" button is visible at the bottom left.

```
<?php
// The page we wish to display
$file = $_GET[ 'page' ];

// Input validation
$file = str_replace( array( "http://", "https://" ), "", $file );
$file = str_replace( array( "..\'", "..\\\'" ), "", $file );

?>
```

Compare All Levels

```
root:x:0:0:root:/root:/usr/bin/zsh daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mail List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin _apt:x:100:65534:./nonexistent:/usr/sbin/nologin systemd-timesync:x:101:101:systemd Time Synchronization/./run/systemd:/usr/sbin/nologin systemd-networkd:x:102:103:systemd Network Management/./run/systemd:/usr/sbin/nologin systemd-resolve:x:103:104:systemd Resolver/./run/systemd:/usr/sbin/nologin mysqld:x:104:110:MySQL Server/./nonexistent:/bin/false tss:x:105:111:TPM software stack/./var/lib/tpm:/bin/false strongswan:x:106:65534:/var/lib/strongswan:/usr/sbin/nologin httpd:x:107:113:/nonexistent:/usr/sbin/nologin messagebus:x:108:114:/nonexistent:/usr/sbin/nologin redsocks:x:109:115:/var/run/redsocks:/usr/sbin/nologin rwhod:x:110:65534:/var/spool/rwho:/usr/sbin/nologin iodine:x:111:65534:/run/iodine:/usr/sbin/nologin miredo:x:112:65534:/var/run/miredo:/usr/sbin/nologin _apt:x:113:65534:/run/rpcbind:/usr/sbin/nologin arptach:x:114:102:ARP Watcher/./var/lib/arptach:/bin/sh usbmux:x:115:46:usbmux daemon/./var/lib/usbmux:/usr/sbin/nologin tcpdump:x:116:121:/usr/sbin/nologin rtkit:x:117:122:RealtimeKit/./proc:/usr/sbin/nologin sshd:x:118:65534:/run/sshd:/usr/sbin/nologin stdm:x:119:65534:/var/lib/nfs:/usr/sbin/nologin postgres:x:120:124:PostgreSQL administrator/./var/lib/postgresql:/bin/bash avahi:x:121:126:Avahi mDNS daemon/./run/avahi-daemon:/usr/sbin/nologin stunnel4:x:122:127:/var/run/stunnel4:/usr/sbin/nologin Debian-snmpp:x:123:128:/var/lib/snmpp:/bin/false ssh:x:124:129:/nonexistent:/usr/sbin/nologin nm-openvpn:x:125:130:NetworkManager OpenVPN/./var/lib/openvpn/chroot:/usr/sbin/nologin nm-openconnect:x:126:131:NetworkManager OpenConnect plugin/./var/lib/NetworkManager:/usr/sbin/nologin pulse:x:127:132:PulseAudio daemon/./var/run/pulse:/usr/sbin/nologin saned:x:128:135:/var/lib/saned:/usr/sbin/nologin inetmimic:x:129:137:/var/lib/inetmimic:/usr/sbin/nologin colorc:x:130:138:color color management daemon/./var/lib/color:/usr/sbin/nologin geoclue:x:131:139:/var/lib/geoclue:/usr/sbin/nologin lightdm:x:132:140:Light Display Manager/./var/lib/lightdm:/bin/false king-phisher:x:133:141:/var/lib/king-phisher:/usr/sbin/nologin dradis:x:134:142:/var/lib/dradis:/usr/sbin/nologin beef-xss:x:135:143:/var/lib/beef-xss:/usr/sbin/nologin kali:x:1000:1000:kali/./home/kali:/usr/bin/zsh systemd-coredump:x:999:999:systemd Core Dumper/./usr/sbin/nologin
```