

```
msfadmin@metasploitable:~$ sudo adduser samay1
Adding user 'samay1' ...
Adding new group 'samay1' (1004) ...
Adding new user 'samay1' (1004) with group 'samay1' ...
Creating home directory '/home/samay1' ...
Copying files from '/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for samay1
Enter the new value, or press ENTER for the default
    Full Name []: adduser: '/usr/bin/chfn samay1' exited from signal 2. Exit
ing.
msfadmin@metasploitable:~$ su samay1
Password:
samay1@metasploitable:/home/msfadmin$ whoiam
bash: whoiam: command not found
samay1@metasploitable:/home/msfadmin$ su samay1
Password:
samay1@metasploitable:/home/msfadmin$ whoiam
bash: whoiam: command not found
samay1@metasploitable:/home/msfadmin$ _
```



Snapshot created 01-Jan-26 2:27:52 AM

Name: Snapshot 1

Description:

[illegible]

Take Snapshot...

Keep

Clone...

Delete

☐ Show AutoProtect snapshots

Go To

AutoProtect...

Close

Help

1 snapshot(s) selected

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law.

To access official Ubuntu documentation, please visit:

<http://help.ubuntu.com/>

No mail.

```
msfadmin@metasploitable:~$ ls
```

vulnerable

```
msfadmin@metasploitable:~$ cd vulnerable
```

```
msfadmin@metasploitable:~/vulnerable$ ls
```

mysql-ssl samba tikiwiki twiki20030201

```
msfadmin@metasploitable:~/vulnerable$ cd
```

```
msfadmin@metasploitable:~$ cd /var/www/mutillidae
```

```
msfadmin@metasploitable:/var/www/mutillidae$ ls
```

add-to-your-blog.php	notes.php
arbitrary-file-inclusion.php	opendb.inc
authorization-required.php	owasp-esapi-php
browser-info.php	page-not-found.php
capture-data.php	password-generator.php
captured-data.php	passwords
captured-data.txt	pen-test-tool-lookup.php
change-log.htm	php-errors.php
classes	phpinfo.php
closedb.inc	phpMyAdmin.php

```
msfadmin@metasploitable:~$ cd /var/www/mutillidae
```

```
msfadmin@metasploitable:/var/www/mutillidae$ ls
```

```
add-to-your-blog.php          notes.php
arbitrary-file-inclusion.php    opendb.inc
authorization-required.php     owasp-esapi-php
browser-info.php              page-not-found.php
capture-data.php              password-generator.php
captured-data.php             passwords
```

```
GNU nano 2.0.7
```

```
File: config.inc
```

```
<?php
```

```
    /* NOTE: On Samurai, the $dbpass password is "samurai" rather than blank
```

```
    $dbhost = 'localhost';
```

```
    $dbuser = 'root';
```

```
    $dbpass = '';
```

```
    $dbname = 'owasp10';
```

```
?>
```

```
msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin# service mysql status
The program 'service' can be found in the following packages:
 * debian-helper-scripts
 * sysvconfig
Try: apt-get install <selected package>
bash: service: command not found
root@metasploitable:/home/msfadmin# /etc/init.d/mysql start
 * Starting MySQL database server mysqld [ OK ]
root@metasploitable:/home/msfadmin# /etc/init.d/mysql status
 * /usr/bin/mysqldadmin Ver 8.41 Distrib 5.0.51a, for debian-linux-gnu on i486
Copyright (C) 2000-2006 MySQL AB
This software comes with ABSOLUTELY NO WARRANTY. This is free software,
and you are welcome to modify and redistribute it under the GPL license

Server version      5.0.51a-3ubuntu5
Protocol version    10
Connection          Localhost via UNIX socket
UNIX socket         /var/run/mysqld/mysqld.sock
Uptime:             49 min 0 sec

Threads: 1  Questions: 444  Slow queries: 0  Opens: 420  Flush tables: 1  Open t
ables: 64  Queries per second avg: 0.151
root@metasploitable:/home/msfadmin#
```




Mutillidae: Born to be Hacked

Version: 2.1.19

Security Level: 0 (Hosed)

Hints: Disabled (0 - I try harder)

Not

Logged In

[Home](#)

[Login/Register](#)

[Toggle
Hints](#)

[Toggle
Security](#)

[Reset
DB](#)

[View
Log](#)

[View Captured
Data](#)

[Core Controls](#)

[OWASP Top 10](#)

[Others](#)

[Documentation](#)

[Resources](#)



Site

hacked...err...quality-
tested with Samurai
WTF, Backtrack,
Firefox, Burp-Suite,
Netcat, and [these
Mozilla Add-ons](#)



[@webpwnized](#)



Mutillidae: Deliberately Vulnerable PHP Scripts Of OWASP Top 10

Latest Version / Installation

- [Latest Version](#)
- [Installation Instructions](#)
- [Usage Instructions](#)
- [Get rid of those pesky PHP errors](#)
- [Change Log](#)
- [Notes](#)

Samurai WTF and Backtrack contains all the tools needed or
you may build your own collection



Samurai Web Testing Framework

BUILT ON
eclipse

