

# [UNIX] Multiple Vulnerabilities MetaDot Portal Server

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-01/0061.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 01/19/04

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 19 Jan 2004 12:55:12 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

-----

Multiple Vulnerabilities MetaDot Portal Server

---

## SUMMARY

" <<http://www.metadot.com/>> Metadot is a popular open source portal software (GPL) recognized for its revolutionary ease-of-use. It provides content management like file, page and link management, collaboration features like discussion forums and polls and personalization like My Yahoo. It is powered by Perl & mySQL. Users range from home users to government, banks, universities and even NASA".

Several vulnerabilities exist in the MetaDot Portal Server. A malicious user can inject arbitrary SQL commands, reveal valuable information about the server and perform Cross Site Scripting attacks.

## DETAILS

Vulnerable Systems:

\* MetaDot Portal version 5.6.5.4b5 and prior

Immune systems:

\* MetaDot Portal version 5.6.5.6 and newer

## Securiteam: [UNIX] Multiple Vulnerabilities MetaDot Portal Server

### SQL Injection:

It may be possible for an attacker to influence SQL queries by passing unexpected data to certain variables including the "id" and "key" variable. Even if an attacker is not successful with influencing an SQL query he can cause an error message to execute script into an unsuspecting users browser thus causing a Cross Site Scripting attack. Also, the SQL error messages reveal a great deal of data about the server. Below is an example error message. The URI used to create this error was:  
index.pl?isa=Session&op=auto\_login&new\_user=&key=[Problem]

--[ Begin Error Message

]

sqlSelect: SQL statement:SELECT userid, lastonline, sessioninfo FROM sessions WHERE sessionid="[Problem]'

Error: You have an error in your SQL syntax near '[Problem]' ' at line 1 at /home/sharem/metadot/metadot/index.pl

DBAccess::DBIObj::sqlSelect('DBAccess::MySQL=HASH(0x85de6a8)', 'userid, lastonline, sessioninfo', 'sessions', 'sessionid='\'[Problem]\'') called at /home/sharem/metadot/metadot/DBAccess.pm line 129

DBAccess::sqlSelect('DBAccess', 'userid, lastonline, sessioninfo', 'sessions', 'sessionid='\'[Problem]\'') called at /home/sharem/metadot/metadot/Session.pm line 508

Session::\_initialize('Session=HASH(0xb1be85c)', '\'[Problem]') called at /home/sharem/metadot/metadot/Session.pm line 161

Session::restore('Session', '\'[Problem]') called at /home/sharem/metadot/metadot/Metadot/SessionHandler/CookieSessionHandler.pm line 97

Metadot::SessionHandler::CookieSessionHandler::restore\_session('Metadot::SessionHandler::CookieSessionHandler='\'[Problem]')called at /home/sharem/metadot/metadot/Metadot/Authenticator.pm line 63

Metadot::Authenticator::authenticate('Metadot::Authenticator::UserPassAuthenticator=HASH(0x9d34338)') called at /home/sharem/metadot/metadot/Portal.pm line 3863 Portal::\_web\_init('Portal=HASH(0xb4c271c)') called at /home/sharem/metadot/metadot/Metadot/Implementations/Portal/Default.pm line 52

Metadot::Implementations::Portal::Default::initialize('Metadot::Implementations::Portal::Default', 'Portal=HASH(0xb4c271c)') called at /home/sharem/metadot/metadot/Portal.pm line 2830

Portal::\_initialize('Portal=HASH(0xb4c271c)') called at /home/sharem/metadot/metadot/Portal.pm line 160

Portal::new('Portal', 1) called at /home/sharem/metadot/metadot/index.pl line 43

Apache::ROOT::metadot::index\_2epl::handler('Apache=SCALAR(0xb42

1470)') called at /usr/local/lib/perl5/site\_perl/5.6.1/i686-linux/Apache/Registry.pm line 149 eval {...} called at /usr/local/lib/perl5/site\_perl/5.6.1/i686-linux/Apache/Registry.pm line 149

Apache::Registry::handler('Apache=SCALAR(0xb421470)') called at /dev/null line 0 eval {...} called at /dev/null line 0

Below are some examples URI's that will allow an attacker to influence queries, gather info or XSS.

/index.pl?id=[Evil\_Query]

/index.pl?iid=[Evil\_Query]

/index.pl?isa=Session&op=auto\_login&new\_user=&key=[Evil\_Query]

## Securiteam: [UNIX] Multiple Vulnerabilities MetaDot Portal Server

### Information Disclosure and Path Disclosure:

There is a great deal of information given up by interrupting the SQL query, but can also be caused in other ways than the previously mentioned. Lets look at /index.pl?iid=[ValidID]&isa=Discussion&op=Where [ValidID] is should be a valid id number such as 1000 or whatever it may be.

--[ Begin Error Message

]-----

### Software error:

```
must provide operation name at /home/sharem/metadot/metadot/Auditable.pm
line 196 Auditable::is_allowed_to_do('Discussion=HASH(0xae19218)', ",
'Metadot::User::FlexUser=HASH(0xb414f70)', 1) called at
/home/sharem/metadot/metadot/index.pl line 232
Apache::ROOT::metadot::index_2epl::handler ('Apache=SCALAR(0xacf893c)')
called at
/usr/local/lib/perl5/site_perl/5.6.1/i686-linux/Apache/Registry.pm line
149 eval {...} called at
/usr/local/lib/perl5/site_perl/5.6.1/i686-linux/Apache/Registry.pm line
149 Apache::Registry::handler('Apache=SCALAR(0xacf893c)') called at
/dev/null line 0eval {...} called at /dev/null line 0
```

-----

As you can see that will give you the server path, perl version and several other interesting bits of information. Path can also be disclosed by a bogus value in the "isa" variable. /index.pl?isa=blah

### Cross Site Scripting:

There are a number of potential cross site scripting issues in MetaDot. Below are some examples:

```
/index.pl?isa=XSS<iframe%20src=http://www.gulftech.org>
/userchannel.pl?id=435&isa=NewsChannel&redirect=1&op="><
iframe%20src=http://www.gulftech.org>
/index.pl?iid=""><iframe%20src=http://www.gulftech.org>
```

### Solution:

The MetaDot team have addressed this issue and an update was released on Thursday the 8th of January. Users of the MetaDot portal system are encouraged to upgrade immediately.

The latest version can be downloaded from:

<<http://www.metadot.com/metadot/index.pl?iid=2632&isa=Category>>  
<http://www.metadot.com/metadot/index.pl?iid=2632&isa=Category>

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:security@gulftech.org>> JeiAr

=====

Securiteam: [UNIX] Multiple Vulnerabilities MetaDot Portal Server

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====  
=====

**DISCLAIMER:**

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.