Не так давно нашей командой была обнаружена уязвимость типа SQL-injection в этой CMS. В публичные источники данная информация не попадала потому что анализ мы проводили по просьбе автора SmartCMS. Но сейчас уязвимость уже исправлена и поэтому можно эту информацию раскрыть. Суть уязвимости в том что при загрузке аватара никак не фильтровалось имя загружаемого файла. Из-за этого, отправив файл со специально сформированным именем, можно было получить права администратора на текущий аккаунт .

Рассмотрим уязвимый код. Он расположен в файле "mod/users/index.php" в строках 244-250:

```
$int = $db->query("UPDATE ".$pr."_users set email = '$email',
                website = '$website',
                icq = '$icq',
                land = '$land',
                avatar = '$ava',
                interes = '$interes',
                age = '$age' where uname = '$uname'");
```

Как видите имя аватара, про которое я говорил, находится в переменной "$ava". Данная переменная формируется выше по коду в строке 196:

```
$ava = $_FILES['avfile'];
```

То есть информация находящаяся в **$_FILES['avfile']** никаким образом не фильтруется и не проверяется. Получается что мы можем попытаться ввести туда всё что угодно.

Эксплойтом, отосланным разработчику была вот такая строка загрузки файла:

```
C:\tes',admin=1,interes='t.jpg
```

Такую строку, в поле загрузки аватара, можно ввести в любом браузере, поэтому эксплойтам являлась именно она.

При загрузке от этой строки отрезались первые 3 символа (обозначение диска), а всё остальное попадало к скрипту загрузки. Давайте посмотрим что будет если ввести подобный текст прямо в запрос (за место других переменных просто поставим нули):

```
UPDATE users set email = '0',
                website = '0',
                icq = '0',
                land = '0',
                avatar = 'tes',admin=1,interes='t.jpg',
                interes = '0',
                age = '0' where uname = '0'
```

Получается что мы свободно достроили запрос и у нашего пользователя значение поля "admin" изменилось с "0" на "1". Следовательно текущий пользователь стал администратором.

Вам следует обратить внимание на то что отсутствие фильтрации имени загружаемого файла довольно распространённая ошибка среди CMS, форумов и прочих скриптов.