Wt - Feature #3799

Error in the code class of RedirectEndpoint

02/14/2015 01:31 PM - Georgiy Gluhoedov

Status:	Closed	**Start date:**	02/14/2015
Priority:	Normal	**Due date:**	
Assignee:	Koen Deforche	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:	3.3.4		

Description

Здравствуйте.

Я пишу на русском языке, потому что плохо говорю по-английски.

Если, вдруг, я сделал ошибку в английском языке, вы всегда сможете сравнить с оригиналом на русском языке.

В классе *RedirectEndpoint*, который находится в файле *OAuthService.C* по адресу [[[https://github.com/kdeforche/wt/blob/master/src/Wt/Auth/OAuthService.C]]] есть функция:

```
virtual void handleRequest(const Http::Request& request, Http::Response& response)
{
    const std::string *stateE = request.getParameter("state");

    if (stateE) {
        std::string redirectUrl = service_.decodeState(*stateE);
    ...
}
```

Которая получает ответ от сервера социальной сети содержащий *закодированную* ссылки на сессию.

Если сервер социальной сети раскодирует передаваемый ему параметр ***state*** и пришлет ссылку на сессию в *раскодированном* виде, то мы получим ошибку авторизации!

Данную функцию нужно изменить на:

```
virtual void handleRequest(const Http::Request& request, Http::Response& response)
{
    //const std::string *stateE = request.getParameter("state");
    int npos = request.queryString().find( "state" );
    std::string stateE;
    stateE = request.queryString().substr( npos+6, request.queryString().length() );

    if (!stateE.empty()) {
        std::string redirectUrl = service_.decodeState(stateE);
    ...
}
```

Нужно считывать до конца строки после параметра "state"

Данная ошибка была замечена благодаря социальным сетям рунета, которые видоизменяли передаваемый им параметр state.

Hi

I write in Russian because do not speak English. If, suddenly, I made a mistake in English, you will always be able to compare with the original in Russian.

In the class *RedirectEndpoint*, which is in the file *OAuthService.C* at [[[https://github.com/kdeforche/wt/blob/master/src/Wt/Auth/OAuthService.C]]] is a function of:

```
virtual void handleRequest(const Http::Request& request, Http::Response& response)
```

```
{
    const std::string *stateE = request.getParameter("state");

    if (stateE) {
        std::string redirectUrl = service_.decodeState(*stateE);
    ...
}
```

Which receives a response from the server is a social network containing *encoded* reference to the session.

If the server is a social network decodes the transmitted parameter ***state*** and it will send a link to the session in the *decoded* form --- we get the authorization error!

To be read to the end of the line after the parameter ***state***

This function should be changed to:

```
virtual void handleRequest(const Http::Request& request, Http::Response& response)
{
    //const std::string *stateE = request.getParameter("state");
    int npos = request.queryString().find( "state" );
    std::string stateE;
    stateE = request.queryString().substr( npos+6, request.queryString().length() );

    if (!stateE.empty()) {
        std::string redirectUrl = service_.decodeState(stateE);
    ...
}
```

BR, Georgiy

History

#1 - 02/15/2015 10:55 PM - Koen Deforche

- Status changed from New to Feedback

- Assignee set to Koen Deforche

Hey,

I don't understand the issue you are hinting at. The difference between your suggested solution and the current implementation is that you do not perform any URL decoding of the state variable. But URL decoding is required when reading a parameter value from the URL?

The third party server should implement proper URL encoding when resending the state variable.

Koen

#2 - 02/24/2015 10:58 AM - Georgiy Gluhoedov

Hi,

Wt send encode state:

```
uZGNJeBkdSfDL73JfLGgCg%3d%3d%7chttp%3a//localhost%3a8080/%3fwtd%3dyIEoQyIGUNiY9R0c%26request%3dresource%26resource%3dop0s7tw%26rand%3d0
```

But Russian social network [[[https://vk.com/]]] returns the decoded state value:

```
uZGNJeBkdSfDL73JfLGgCg==|http://localhost:8080/?wtd=yIEoQyIGUNiY9R0c&request=resource&resource=op0s7tw&rand=0
```

Wt get parameter state:

```
const std::string *stateE = request.getParameter("state");
```

And the value of the variable does not contain all data, only those, who have been to the first character '&'

```
uZGNJeBkdSfDL73JfLGgCg==|http://localhost:8080/?wtd=yIEoQyIGUNiY9R0c
```

#3 - 02/25/2015 12:01 AM - Koen Deforche

- Tracker changed from Bug to Feature

- Status changed from Feedback to InProgress

- Target version set to 3.3.4

That's a bug in the Russian social network --- it should re-encode the state properly. We could work around this by avoiding '&' in the state, by encoding a '&' with a another special character that does not confound URL query string parsing.

#4 - 02/27/2015 10:52 AM - Georgiy Gluhoedov

Koen Deforche wrote:

> That's a bug in the Russian social network --- it should re-encode the state properly. We could work around this by avoiding '&' in the state, by encoding a '&' with a another special character that does not confound URL query string parsing.

I wrote to them about this error (that they departed from the standard OAuth 2.0) but I was ignored. This error occurs in many Russian social networks.

BR, Georgiy.

#5 - 03/02/2015 06:09 PM - Koen Deforche

- Status changed from InProgress to Resolved

#6 - 03/17/2015 08:20 AM - Koen Deforche

- Status changed from Resolved to Closed