Archin WordPress Theme Multiple Vulnerabilities
Sat September 22nd, 2012

The Archin WordPress theme is a premium WordPress theme offered by WPTitans, which you can buy from various sites, such as Theme Forest : (http://themeforest.net/item/archin-premium-wordpress-business-theme/239432?sso?WT.ac=search_item&WT.seg_1=search_item&WT.z_author=wptitans).

Its a beautiful looking theme, with many built in functions, but also has multiple issues that put site owners and non-site owners at risk. I'll explain how that works for both site owners, and non site owners.

Due to the use of various plug-ins within the theme itself (TimThumb anyone? No, its not vulnerable in this version, but other issues still exist), and also using their own custom functions, they implement flaws that would not normally be part of WordPress. These include a XSS flaw, File Upload Vulnerability, and Database/Empty Message Spam issue that can fill the database until it either crashes or runs out of space.

Flaw 1

The first one was the easiest to test. WordPress by default, will sanitize search input. It will remove all XSS and script tags as well as SQL Injection attempts if you use their built in search form. This is always the recommended way to use the WordPress search feature. The Archin theme however, uses its own custom search functions, and in doing so echoes back in the sites html <title> tag, un-sanitized data. We can take advantage of this in the following manner, by appending the sites URL like so:

```
?s=</title><script>alert(1);</script>
```

An attacker could copy the entire sites url appended with this string, and then use something like TinyURL or another URL shortening service like bitly and obfuscate the true url's contents. They could then use this in comments on the owners site to add urls the owner or other logged in and even external users might click and then run the XSS attack, or use the owners contact form to post the link for the owner to see and run code from within the dashboard, possibly utilizing CSRF if the user is logged in.

To give you an example of an attack, I could basically make the entire page display nothing, and instead return what looks like, the WordPress login page, making a theme owner think they got logged out, and then harvest their credentials.

Flaw 2

That leads us to our second flaw. The Archin contact form. The way their form works, when installing the theme, it creates some random keys to use for internal messages that show up on an admin dashboard, aptly titled “Message” which contains all messages sent using the sites contact form. However, we can send empty spam comments to this dashboard, and FILL their messages with empty spam.

The problem with this theme, is it doesn’t let you bulk delete these messages, or approve them, they just show up in there as the title of “Message” with no body, no subject, no email address or anything other than just a title of “Message”.

If you automated a script to continually send empty spam, and it ran 24/7, in theory, you could eventually fill their entire SQL database with empty messages. I have not actually attempted to fill a site with a million records, but I assume at some point it would either DOS the site, or cause something to crash.

The following is POC code, and only meant for educational purposes:

```
<form action='http://www.victimsite.com/wp-content/themes/archin/hades_framework/
helper/form_request.php' method='post' />
 <label for='text0'> Name </label><input type='text' value='bob' name='text0'
id='text0' /><br />
 <label for='text1'> Email </label><input type='text' value='bob@aol.com'
name='text1' id='text1' /><br />
 <label for='select : Web Development, Wordpress, Graphic Design2'> Service
</label><br />
 <select id='select : Web Development, Wordpress, Graphic Design2' name='select :
Web Development, Wordpress, Graphic Design2' >
 <option value=' Web Development'> Web Development</option><option value='
Wordpress'> Wordpress</option>
 <option value=' Graphic Design'> Graphic Design</option>
 </select><br />
 <label for='textarea3'> Subject </label><br />
 <textarea width="200" height="150" name='textarea3' id='textarea3' />Doesn't
matter what we put here, won't show in the admin dashboard anyway!
</textarea><br />
 <input type='text' name='notify_email' value='foobar@foobar.foo'
class='notify_email' /><br />
 <input type='text' name='form_key' value='0000000000' class='form_key' /><br />
 <input type='submit' name='qsubmit' value='Send' class='d_submit' />
 </form>
```

Flaw 3

The third flaw I found (and their may be many more, I just haven't had time to go through every line of code in the theme) is an upload vulnerability. You can by way of manipulation of their upload form, send any files they allow(which are only 'jpg','jpeg','gif','png', and 'js' files). Here in lies the potential for abuse against non site owners. By uploading files to the site for storage, we can use it as a springboard to RFI or XSS other sites.

The theme also uses TimThumb.php, but does not appear to be a vulnerable version (at least in the one I was testing, I could not seem to get it to allow PHP execution – It adds a php header of its own to all files and renames them to .txt in its cache folder). However, you can upload a file such as shell.php.gif with a fake gif header to their site via the Uploadify code, and then use the owners site to launch RFI attacks on other, vulnerable users sites that DO exhibit the TimThumb flaw or other such RFI attack flaws.

In testing, I was able to upload PHP files by just renaming their extension to ".gif". Here is the upload flaw POC:

```
<form enctype="multipart/form-data" action="http://www.victimsite.com/wp-content/
themes/archin/js/uploadify/uploadify.php" method="post">
File:<input type="file" value="" name="Filedata" /><br />
<input type="submit" value="Submit" /><br />
</form>
```

This will upload all files to the cufon font folder with a prefix of custom_, and can be found in the path of:

```
/wp-content/themes/archin/js/cufon-fonts/uploaded/custom_XXXX.XXX
```

where XXXX.XXX was your original file name.

There may be a number of other flaws or exploits within this theme, or within the already listed methods of attack. I would advise anyone using this theme to consider recoding it to sanitize all input, and enforce that none of the scripts can be accessed directly from external users, or just switch to a safer theme in general.

The version of Archin I tested was :

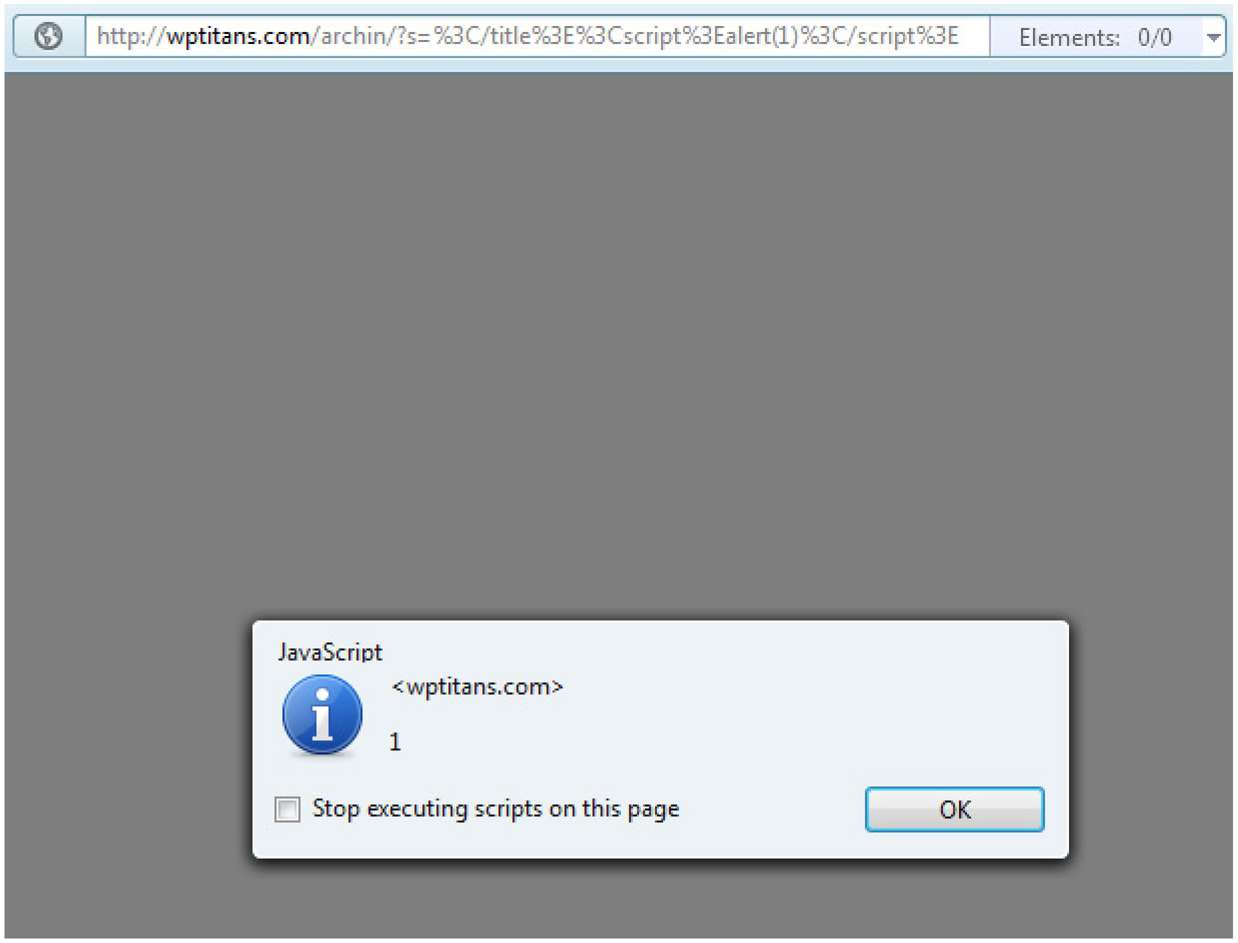
```
Theme Name: Archin
Theme URI: http://www.wptitans.com/archin
Description: A premium template for architecture and business. Follow me on <a
href="http://twitter.com/#!/wptitan">Twitter</a> or find more awesome products at
<a href="http://themeforest.net/user/wptitans"> Themeforest</a>.
Author: WP Titans
Author URI: http://www.wptitans.com/
Tags: business, portfolio, clean
Version: 3.2
```

By the way, I would like to note: The way the implementation for TimThumb and Uploadify are used in this theme, they are not initialized as TRUE plug-ins of WordPress. Because of this, they run as stand alone scripts.

In trying to contact them to notifiy them of the vulnerabilities I have not received contact back from them. On their demo sites for this theme, and also a few of their others, they exhibited the XSS flaw with the search function on their demo sites. I would assume they reuse the same code across all their themes, but without having a copy of each of them(they are premium paid for themes) I can not test and confirm this. This was only a quick overview of the theme, and I have not gone through it with a fine tooth comb, so there may be more vulnerabilities, such as SQLi flaws in some of the code, since I noticed some of the third party code appears to store info and make calls to the wpdb.

Even their main site, which demo's the theme, exhibits this vulnerability:

http://wptitans.com/archin/?s=%3C/title%3E%3Cscript%3Ealert(1)%3C/script%3E


http://wptitans.com/archin/?s=%3C/title%3E%3Cscript%3Ealert(1)%3C/script%3E
Elements: 0/0
JavaScript
<wptitans.com>
1
Stop executing scripts on this page
OK

- DigiP -
http://www.attack-scanner.com