

Forum:[Hack Forums](#)

Thread: [Hacked by Syrian Arab Army](#)

GeorgeoN - June 24, 2016, 4:03 am

Hello i have a problem recently my website was hacked and when i open my site its shows that, Syrian Arab Army the army of honor hacked the site, what can i do and how can i protect from furdur hackings ?

Thanks

syrian arab army nightmare and wolf tartous

b4tb0t - June 24, 2016, 6:06 am

Hi.

-Code

What language uses for your web?

Uses a CMS (Wordpress,Joomla,...)?

Uses a framework (Cakephp,Symfony,...)?

-DB

What databases system you use?

What version?

We need more information to help you.

GeorgeoN - June 25, 2016, 2:23 am

I fix it by my self they just changed the index.php file to not open my site, i use wordpress CMS :)

bonjourmonsieur - June 25, 2016, 5:12 am

(Jun 25, 2016 02:23 AM)GeorgeoN Wrote: [\[CITE\]](#) I fix it by my self they just changed the index.php file to not open my site, i use wordpress CMS :)

That doesn't mean you've removed the vulnerability tho, you silly goose.

Insurmountable - June 25, 2016, 12:59 pm

Below is a vulnerability scan of your site. Sorry the links are broken, but I don't have 50 posts yet so I can't do direct links.

Things you should do:Run a virus scan on your webserver. The hackers probably left a php shell somewhere.

Remove the readme.html file, it exposes your wordpress version

Make an htaccess rule to block access to the wp-includes/ directory

Disable directory listings

Enable automatic plugin updates for wordpress

Limit wordpress login attempts (hint: lookup "Loginizer")

Don't use the default "admin" username for your wordpress account

Use a strong, unique password for your wordpress account

```
  \ \  _ _ _ _ _ _ _ _ _ _  
  \ \ ^ / / | | _ ) | ( _ _  
  \ V V / | _ _ / \ _ _ \ / _ _ ' | '\  
  \ ^ / | | _ _ ) | ( | ( | | | |  
  V V | | | _ _ _ / \ _ _ \ _ _ | | | |
```

WordPress Security Scanner by the WPScan Team

Version 2.9

Sponsored by Sucuri - [h t t p s://sucuri.net](http://sucuri.net)

@_WPScan_, @ethicalhack3r, @erwan_lr, pvdI, @_FireFart

[+] URL: [h t t p://creativeworks.design/](http://creativeworks.design/)

[+] Started: Sat Jun 25 12:40:29 2016

[+] robots.txt available under: [h t t p://creativeworks.design/robots.txt](http://creativeworks.design/robots.txt)

[+] Interesting entry from robots.txt: [h t t p://creativeworks.design/wp-admin/admin-ajax.php](http://creativeworks.design/wp-admin/admin-ajax.php)

[!] The WordPress [h t t p://creativeworks.design/readme.html](http://creativeworks.design/readme.html) file exists exposing a version number

[!] Full Path Disclosure (FPD) in [h t t p://creativeworks.design/wp-includes/rss-functions.php](http://creativeworks.design/wp-includes/rss-functions.php):

[+] Interesting header: LINK: [<h t t p://creativeworks.design/wp-json/>](http://creativeworks.design/wp-json/); rel=[h t t p s://api.w.org/](http://api.w.org/)", [h t t p://creativeworks.design/](http://creativeworks.design/); rel=shortlink

[+] Interesting header: SERVER: nginx/1.10.1

[+] Interesting header: X-CACHEABLE: YES

[+] Interesting header: X-SERVED-FROM-CACHE: Yes

[+] XML-RPC Interface available under: [h t t p://creativeworks.design/xmlrpc.php](http://creativeworks.design/xmlrpc.php)

[!] Upload directory has directory listing enabled: [h t t p://creativeworks.design/wp-content/uploads/](http://creativeworks.design/wp-content/uploads/)

[+] WordPress version 4.5.3 identified from meta generator

[+] WordPress theme in use: trend - v3.6

[+] Name: trend - v3.6

| Location: [h t t p://creativeworks.design/wp-content/themes/trend/](http://creativeworks.design/wp-content/themes/trend/)

[+] Enumerating plugins from passive detection ...

| 1 plugin found:

[+] Name: contact-form-7

| Latest version: 4.4.2

| Location: [h t t p://creativeworks.design/wp-content/plugins/contact-form-7/](http://creativeworks.design/wp-content/plugins/contact-form-7/)

[!] Directory listing is enabled: [h t t p://creativeworks.design/wp-content/plugins/contact-form-7/](http://creativeworks.design/wp-content/plugins/contact-form-7/)

[!] We could not determine a version so all vulnerabilities are printed out

[!] Title: Contact Form 7 <= 3.7.1 - Security Bypass Vulnerability
Reference: <http://wpvulndb.com/vulnerabilities/7020>
Reference: <http://www.securityfocus.com/bid/66381/>
Reference: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2265>
[i] Fixed in: 3.7.2

[!] Title: Contact Form 7 <= 3.5.2 - File Upload Remote Code Execution
Reference: <http://wpvulndb.com/vulnerabilities/7022>
Reference: <http://packetstormsecurity.com/files/124154/>
[i] Fixed in: 3.5.3

[+] Enumerating usernames ...
[+] Identified the following 1 user/s:

```
+----+-----+-----+  
| Id | Login | Name |  
+----+-----+-----+  
| 1 | admin | Hello |  
+----+-----+-----+
```

[!] Default first WordPress username 'admin' is still used

[+] Finished: Sat Jun 25 12:40:48 2016
[+] Requests Done: 86
[+] Memory used: 57.012 MB
[+] Elapsed time: 00:00:19

OGLIA - June 25, 2016, 3:24 pm

i think its bruteforce attack.
or an vulnerable plugin was installed.

one of the two :)

lynnex - June 25, 2016, 11:23 pm

(Jun 25, 2016 03:24 PM)OGLIA Wrote: [\[CITE\]](#) i think its bruteforce attack.
or an vulnerable plugin was installed.

one of the two :)
No, it wasn't a bruteforce.
They exploited a broken plugin or page.

OGLIA - June 26, 2016, 6:21 am

(Jun 25, 2016 11:23 PM)lynnex Wrote: [\[CITE\]](#) No, it wasn't a bruteforce.
They exploited a broken plugin or page.
Exploited Broken page?
Wordpress is installed, nothin else.
they just exploited an plugin, or as i say bruteforce one of the two :D

GeorgeoN - June 26, 2016, 12:27 pm

Thanks for suggestion @Insurmountable

I dont know much about web security and i dont know why would they attact a site for furniture located in Macedonia that dosnt even have visits on it, and yes im graphics designer not hacker, so if i dont know something dosnt make me a silly, im still learning wordpress :)

Thanks to all one more time, i guess they just wanted to take money becouse there was a link in front page.

dotcomsuper - *June 27, 2016, 1:58 pm*

just index.php front page web but pay attention if there is still any backdoor .php

32x0LF - *June 27, 2016, 9:31 pm*

Update everything and install mods.