

Forum:[Hack Forums](#)

Thread: [\[Official\] Notorious - Web Application Hacking Recruitment #1](#)

Disparity - July 20, 2017, 5:01 am

[Video: <https://youtu.be/lbz2tAyMChU>]

Notorious - Web Application Hacking Recruitment #1

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 Hack Forums for at least one month.

You must not have any open and valid scam reports against you. If you get one whilst being in the group you will be removed.

You are active and can post on a regular basis. If you are not active in one way or another don't bother applying.

No trolling or flaming other members.

Don't break Group rules. Doing so will result in a swift and permanent removal from the group.

You must partake in group discussions and projects. There is no set minimum but inactive members will be purged.

User background and forum activity will be investigated before you are invited to the group.

Notorious is looking for ambitious individuals focused on honing their skills and willing to dedicate time to group projects; if your forum activity doesn't reflect this you will not be invited.

Challenge Instructions:

I have put together a vulnerable web application. You must:

Code - Add your name to the solvers list on the main index

- Remove any footprints you leave (shells, file changes(?), etc.)

- Upon completion, send me a message with any final queries (i.e whatever query you used to get what you were after) and credentials used.

Starting Point:

Code

0x626d393062334a706233567a4c6d467364475679646d6c7a6447457562334a6e4a544a6d626d393062334a706233567a4a544a6d

Please do not discuss the challenge, give hints, or share the challenge solution.

The thread will be locked in 7 days, and the recruitment will be closed. Accepted members will be PM'd.

Nebo - July 20, 2017, 5:25 am

Good luck to the people who try to solve the challenge. Seems like a promising group sector and a somewhat good idea for group recruitment.

I'll try and give it a go, considering I haven't done anything like this in ages, reminds me of times when major hostings were vulnerable to c99 and other shells.

LD_PRELOAD - July 20, 2017, 5:52 am

please define the id to be primary key to prevent idiots like me from idioting

edit: im on discord if u wanna talk

Disparity - July 20, 2017, 6:51 am

(Jul 20, 2017 05:25 AM)NotVirus.exe Wrote: [\[CITE\]](#) Good luck to the people who try to solve the challenge. Seems like a promising group sector and a somewhat good idea for group recruitment.

I'll try and give it a go, considering I haven't done anything like this in ages, reminds me of times when major hostings were vulnerable to c99 and other shells.

I think it's a somewhat good idea too. Give it a shot.

(Jul 20, 2017 05:52 AM)LD_PRELOAD Wrote: [\[CITE\]](#) please define the id to be primary key to prevent idiots like me from idioting

edit: im on discord if u wanna talk

fixed and messaged ?

?heshire - July 20, 2017, 6:53 am

Ill definitely have to get working on this when I get home. Good luck to all, and thanks for the awesome recruitment challenge.

mutybyte - July 20, 2017, 8:16 pm

What about those who are new in web hacking and curious to learn? Can newbie also be approvable?

Disparity - July 20, 2017, 8:59 pm

(Jul 20, 2017 08:16 PM)mutybyte Wrote: [\[CITE\]](#) What about those who are new in web hacking and

curious to learn? Can newbie also be approvable?

There will be some other options to get in the group coming up soon, including some for newbies.

TheChi?f - July 20, 2017, 9:59 pm

Best of luck to those who try this challenge. Disparity did a good job with it.

Faith Connors - July 20, 2017, 10:12 pm

took me long enough to even get past the first step lul, let alone finding a working payload that didn't completely crash and burn.

Disparity - July 20, 2017, 10:19 pm

(Jul 20, 2017 10:12 PM)Faith Connors Wrote: [\[CITE\]](#) took me long enough to even get past the first step lul, let alone finding a working payload that didn't completely crash and burn.

? It's a bit of a difficult one. One of my recent threads might help those who need it.

So far, aside from Notorious members, we have one solver.

coldy - July 20, 2017, 10:30 pm

(Jul 20, 2017 10:19 PM)Disparity Wrote: [\[CITE\]](#) ? It's a bit of a difficult one. One of my recent threads might help those who need it.

So far, aside from Notorious members, we have one solver.

this is off the topic of the thread but i love your sig brings back memories of space dandy :)

good luck to everyone who attempts this!

LD_PRELOAD - July 20, 2017, 11:16 pm

(Jul 20, 2017 10:19 PM)Disparity Wrote: [\[CITE\]](#) ? It's a bit of a difficult one. One of my recent threads might help those who need it.

So far, aside from Notorious members, we have one solver.cant reply to pms, im on the discord notorious server

mutybyte - July 20, 2017, 11:51 pm

What is this ?

Code ?bm90b3Jpb3VzLmFsdGVydmlzdGEub3JnJTJmbm9? #4\$ #5g♠¥D!

Disparity - July 21, 2017, 12:31 am

(Jul 20, 2017 11:16 PM)LD_PRELOAD Wrote: [\[CITE\]](#) cant reply to pms, im on the discord notorious server

messed ya

?ictor? - July 21, 2017, 1:35 am

good luck with solving this everyone, notorious is a great group to be in :")

Ganja - July 21, 2017, 7:49 am

Done! Thanks for the cool challenge, it was fun!

iKinky - July 21, 2017, 8:04 am

(Jul 20, 2017 11:51 PM)mutybyte Wrote: [\[CITE\]](#) What is this ?

Code ?bm90b3Jpb3VzLmFsdGVydmlzdGEub3JnJTJmbm9? #4\$ #5g♠¥D!
that is a decoded hex number

Disparity - July 21, 2017, 1:18 pm

(Jul 21, 2017 07:49 AM)Max Power Wrote: [\[CITE\]](#) Done! Thanks for the cool challenge, it was fun! Congratulations to our second solver (though first added to the group) Max Power! Well done!

Ganja - July 23, 2017, 3:17 am

I'm still not seeing another name on there, c'mon hackforums!

Staubfinger - July 23, 2017, 3:29 am

solved.

most time was wasted on the guessing part. and then the part, figuring why backticks and other php functions arent working. (kindof meh).

Ganja - July 23, 2017, 4:53 am

(Jul 23, 2017 03:29 AM)Staubfinger Wrote: [\[CITE\]](#) solved.

most time was wasted on the guessing part. and then the part, figuring why backticks and other php functions arent working. (kindof meh).

My man! Good job ?

Baud - July 23, 2017, 9:00 am

Solved, it wasn't difficult but still fun to do. Just deleted my tracks and about to send the PM ?

Disparity - July 23, 2017, 9:25 am

(Jul 23, 2017 03:29 AM)Staubfinger Wrote: [\[CITE\]](#) solved.

most time was wasted on the guessing part. and then the part, figuring why backticks and other php functions arent working. (kindof meh).

Congratulations and welcome to Notorious.

mutybyte - July 23, 2017, 7:43 pm

I am sorry for what i did yesterday. Now i got a lesson to not reveal url in public until challenge is on.By the way i was not aware of that. Today i again try my best to solve

Disparity - July 23, 2017, 8:14 pm

(Jul 23, 2017 07:43 PM)mutybyte Wrote: [\[CITE\]](#) I am sorry for what i did yesterday. Now i got a lesson to not reveal url in public until challenge is on.By the way i was not aware of that. Today i again try my best to solve

No problem. Hope to see you in the group.

mutybyte - July 23, 2017, 9:41 pm

Finally completed. Can't express my feeling of solving this challenges by my own just by little hint. I want to giving thanks to "Google","Notrious Challenger","Hackforum members who posted awesome tutorials on forum only because of this i learned a lot'

PM you soon sir. Hoping this time i will accepted in group and learn a lot from you experts ?

Disparity - July 23, 2017, 11:38 pm

(Jul 23, 2017 09:41 PM)mutybyte Wrote: [\[CITE\]](#) Finally completed. Can't express my feeling of solving this challenges by my own just by little hint.

I want to giving thanks to "Google","Notrious Challenger","Hackforum members who posted awesome tutorials on forum only because of this i learned a lot'

PM you soon sir. Hoping this time i will accepted in group and learn a lot from you experts ?
Congratulations to mutybyte, our third solver. Welcome to Notorious.

Disparity - July 26, 2017, 7:45 pm

The challenge will be open for another 12 hours.

Solution:

We start with hex

Code

0x626d393062334a706233567a4c6d467364475679646d6c7a6447457562334a6e4a544a6d626d393062334a706233567a4a544a6dWhich decodes to base64

Code bm90b3Jpb3VzLmFsdGVydmlzdGEub3JnJTJmbm90b3Jpb3VzJTJmWhich decodes to our mildly inconveniencing url-encoded url

Code notorious.altervista.org%2fnotorious%2f

We find a drop-down search bar for searching Notorious users. Parameters aren't seen in our URL; it's POST. With tamperdata or whatever alternative modify the POST request to check for SQLi: 1' Vulnerable.

SQL queries don't work, however; safe to assume it's string-based or xpath.

Proceed normally injecting until we have the db (my_notorious) and tables (users/admin)

The one row in admin is your admin credentials.

Code notor_chal:b4969b3ed724bbadfc2717ac898fa2fbpassword is md5 which decrypts to:

Code nOtOrloUs

Admin panel can be found at notorious.altervista.org/admin/

login with the credentials and upload your shell on the vulnerable uploader.

^^^

your hint is hosted in the same directory your shell is uploaded to. From there simply modify the index.

Congrats to those who completed the challenge and welcome to Notorious. Keep an eye out for the next one.