

# Forum:[Hack Forums](#)

Thread: [Malvager Hacking Contest Round #2](#)

**Fallen** - August 10, 2009, 2:37 pm

Malvager Hacking Contest Round #2

Brought to you by irc.Malvager.com #Malvager  
by Fallen and Japon

Think your a real hacker? and you got skill? Prove it  
Attempt to break into our test servers, Japon and I (Fallen) have prepared to test your skills  
100% legal hacking grounds  
Everything from LFI to XSS, with each round it will take more skill to break into and deface our page

Rules are simple, break in any way you can, and deface our index with your handle or make it  
apparent you are in, and then patch up the vulnerability  
so no one else can get in and claim your title  
With each round, the difficulty will rise, goodluck with round #2 ^\_^

Page: <http://97.107.134.81/>

Past Winners....  
Round #1 - Lortess  
Round #2 - Lortess

**Idiot #66** - August 10, 2009, 2:41 pm

bad thing u posted this today . leave some space between rounds FAllen

**Fallen** - August 10, 2009, 2:42 pm

(Aug 10, 2009 02:41 PM)X-net Wrote: [\[CITE\]](#) bad thing u posted this today . leave some space  
between rounds FAllen

It was ready to go, this one will take awhile to complete so weve got plenty of time

**Nyx-** - August 10, 2009, 2:43 pm

X-net its not like you have a chance of winning anyways, calm down.

**Proxy** - August 10, 2009, 2:47 pm

Cool, it looks quite difficult though. :P Thanks Fallen.  
X-net, if you don't like it you don't have to join.

**Idiot #66** - August 10, 2009, 2:50 pm

No I want to join pls . I will try to make something .

Sup proxy where have u been ??? I've missed u !

**Endax** - August 10, 2009, 2:53 pm

Great, I'll be addicted to trying to hack this untill the early hours of the morning :P

**Vagxine** - August 10, 2009, 2:56 pm

+Rep to you for setting this up, Fallen.

It's nice to see some real hacking in a legal competition like this.

**Synny** - August 10, 2009, 2:58 pm

bump

bumpi

bumpin

bumping

**?agicSpeed™** - August 10, 2009, 3:00 pm

(Aug 10, 2009 02:58 PM)Beef Wellington Wrote: [\[CITE\]](#) Something

I have no idea of who you are Beef Wellington but I hate you, you're the biggest fag I've ever seen, die in hell.

**Zenko** - August 10, 2009, 3:02 pm

(Aug 10, 2009 03:00 PM)MagicSpeedâ„¢ Wrote: [\[CITE\]](#) I have no idea of who you are Beef Wellington but I hate you, you're the biggest fag I've ever seen, die in hell.It's synny fag.

**?agicSpeed™** - August 10, 2009, 3:03 pm

(Aug 10, 2009 03:02 PM)Zenko Wrote: [\[CITE\]](#) It's synny fag.

Thanks a lot for telling me dude ! ?

**Agent Orange** - August 10, 2009, 3:03 pm

(Aug 10, 2009 03:00 PM)MagicSpeedâ„¢ Wrote: [\[CITE\]](#) I have no idea of who you are Beef Wellington but I hate you, you're the biggest fag I've ever seen, die in hell.I agree, this is the biggest fagtard ever.

[img]http://i27.[censored].com/4ieb9c.jpg[/img]

**Zenko** - August 10, 2009, 3:03 pm

(Aug 10, 2009 03:03 PM)MagicSpeedâ„¢ Wrote: [\[CITE\]](#) Thanks a lot for telling me dude ! ?NO YOU KNEW FAGGET ?

**Fallen** - August 10, 2009, 3:16 pm

Lets get back on topic -\_\_-

This round is a bit harder, I think it will take awhile for someone to get it ^\_^

**Endax** - August 10, 2009, 3:17 pm

Will you be giving out any hints this round?

**Fallen** - August 10, 2009, 3:19 pm

(Aug 10, 2009 03:17 PM)Dynamic Wrote: [\[CITE\]](#) Will you be giving out any hints this round?

I dont believe so, Japon and I want to see what HF can do without the hints

In a real situation there is not a hint.php ^\_\_^

**Proxy** - August 10, 2009, 3:19 pm

People, please follow the topic. Fallen and japon are nice to setup this for us, don't be a bitch and spam the thread.

Thanks.

**Synny** - August 10, 2009, 3:42 pm

Yea come on guys, hopefully someone from HF can do it.

**EvilThoughtz** - August 10, 2009, 3:43 pm

This password manager script uses a single mysql database and only one table. To install, please fill out the 4 fields of the file "config.php" and click Next. Password Manager Installed ;) SavedPASSWORDLISTS eh? Damn wtf this is harder then it seemed >\_>

**Conan** - August 10, 2009, 4:07 pm

fallen i think you should put conan as the hint next time ^\_\_^

**EvilThoughtz** - August 10, 2009, 4:09 pm

There is no hint . Fallen, did you lock the savedpasswordlist table or am I tripping.

**japon** - August 10, 2009, 4:13 pm

nope the table savedPasswordsList is up and running like a charm ;) every file in the web dir is even in chmod 777 ;)

**EvilThoughtz** - August 10, 2009, 4:14 pm

Hmmm. >\_> I wonder am I the furthest.

**Lortess** - August 10, 2009, 4:16 pm

i'm in but havent defaced yet

**Idiot #66** - August 10, 2009, 4:16 pm

What do u think malvager pussys >? Can I win this round ?

**Lortess** - August 10, 2009, 4:16 pm

having trouble editing the index file ROFLMAO deleted index file, replaced with blank but still no name on it

**japon** - August 10, 2009, 4:22 pm

And yet once again, well, gj ;)

**Idiot #66** - August 10, 2009, 4:22 pm

Lortess won . GAME OVER

**japon** - August 10, 2009, 4:23 pm

seems like we're gonna have to skip a few levels :)

**EvilThoughtz** - August 10, 2009, 4:23 pm

I give up . Cant figure this shit out.

**Lortess** - August 10, 2009, 4:24 pm

even if you did figure it out, i patched it xD BTW I didn't find out round 2 was up until a few mins before my first post here, so to anyone who's been trying since it was up... you fail ^\_>

**EvilThoughtz** - August 10, 2009, 4:26 pm

It was only up a few minutes before your post anyway.

**Lortess** - August 10, 2009, 4:31 pm

How I did it:

Looked at the code, found a vulnerability in the SQL. It doesn't make sure the SQL is safe, so basically I just put this into the username box:

Code admin"OR id="1and anything in the password box (must not be blank)

This gave me the following output:

ssh account password: im2leet

ftp account password: im2leet

telnet account password: im2leet

Now play safe, and dont be leaving your passwords all over the place ;)

So, easy now... Just logged into the server via SSH. I had some problems trying to change the index file, permission denied, tried using the same code from round 1 to overwrite the file, didn't work, tried deleting and re-creating, didn't work... after awhile of thinking i deleted the index.php file and made index.html instead, that worked perfectly!

Hack successful, now to patch it...

First I deleted the source files (although i didn't need to do this)

second, probably the only thing I needed to do to secure it, I changed the password for the account.

done. (Aug 10, 2009 04:26 PM)Shadowz Wrote: [\[CITE\]](#) It was only up a few minutes before your post anyway.

99 minutes before i posted, thats not "a few"

**Fallen** - August 10, 2009, 5:37 pm

Great job Lortess, again lol

**n3xus** - August 10, 2009, 5:39 pm

Congratz Lortress, good job again.

**Lortess** - August 10, 2009, 6:03 pm

If your IP is on here you fail: <http://97.107.134.81/access.log.txt>

**Arsonist** - August 10, 2009, 6:13 pm

Good Job Lortress.

To bad I wasn't there to participate.

**Horusbrasil** - August 10, 2009, 6:22 pm

Where can I find newb tutos to start learning what Lortess did?

From the really beggining? got no idea to search about it =S

**Lortess** - August 10, 2009, 6:40 pm

(Aug 10, 2009 06:22 PM)Horusbrasil Wrote: [\[CITE\]](#) Where can I find newb tutos to start learning what Lortess did?

From the really beggining? got no idea to search about it =S

Google: SQL Injection

**silentanomaly** - August 10, 2009, 6:45 pm

I n00b'd it up and couldn't get the sql injection string correct unless I would have had it pretty quickly :{(

**Lortess** - August 10, 2009, 6:54 pm

(Aug 10, 2009 06:45 PM)silentanomaly Wrote: [\[CITE\]](#) I n00b'd it up and couldn't get the sql injection string correct unless I would have had it pretty quickly :( ... it's the normal SQL injection string :S how can you not get it?

**silentanomaly** - August 10, 2009, 6:56 pm

yeah... For some odd reason I was making it way to hard and wasn't trying the easy stuff. I also didn't use double quotes if it makes a difference :( /fail

**kurorolucifer23** - November 12, 2014, 12:22 am

why its the same person who win the contest? its rigged? jks