

Forum:[Hack Forums](#)

Thread: [Hack into Royalty! \[Official Group\] #2](#) Edit: Winner = Arthur

Cibor - November 15, 2016, 10:36 am

Hello!

This is a quick opportunity to join Royalty Group and also to prove your pentesting skills.

[Exploit.c](#) We have prepared a special vulnerable website.

What you have to do:

- Hack into this website: 185.62.190.191
- Find a file called WINNER

First person who posts the content of file "WINNER" wins.

Time start!

exploit.c - November 15, 2016, 10:40 am

Good luck everyone ?

Inked ?Feather - November 15, 2016, 10:41 am

interesting way to recruit people. i'm sure anyone that gets in will be useful this way

best of luck to anyone entering. posting here to come back later!

x0176852 - November 15, 2016, 10:41 am

Good luck to all the persons, im very busy to try it!

Papa Cuda - November 15, 2016, 10:41 am

Good luck to everyone. It's gonna be difficult that's for sure.

Prawnster - November 15, 2016, 10:42 am

ayy, this looks fun :D

I'll give this a go, even if I dont succeed, at least I will learn some stuff ;)

TRAUMA - November 15, 2016, 10:43 am

Got it. Am I allowed to post on the thread what it is or PM you?

Cibor - November 15, 2016, 10:45 am

(Nov 15, 2016 11:43 AM)CHASe Wrote: [\[CITE\]](#) Got it. Am I allowed to post on the thread what it is or PM you?

First person who posts in this thread the string from WINNER file, wins!

sup3r_n0va - November 15, 2016, 10:47 am

ok another one great thanks.

Inked ?Feather - November 15, 2016, 10:47 am

IWinHahahaNoobsYouAllSuck.txt

yep

?

Disco. - November 15, 2016, 10:48 am

IWinHahahaNoobsYouAllSuck.txt

mfw me and inked feather both shelled it at the same time ;-;

exploit.c - November 15, 2016, 10:48 am

(Nov 15, 2016 11:47 AM)Inked ?Feather Wrote: [\[CITE\]](#) IWinHahahaNoobsYouAllSuck.txt

yep

?

Wrong, but congrats on finding the decoy! You didn't think it'd be that easy, right?

Prawnster - November 15, 2016, 10:50 am

(Nov 15, 2016 11:48 AM)exploit.c Wrote: [\[CITE\]](#) Wrong, but congrats on finding the decoy! You didn't think it'd be that easy, right?

If nobody gets this before I finish dinner, I'll have a go xD

Cibor - November 15, 2016, 10:50 am

The exact file name is "WINNER" my friends

Inked ?Feather - November 15, 2016, 10:50 am

(Nov 15, 2016 11:48 AM)Disco. Wrote: [\[CITE\]](#) IWinHahahaNoobsYouAllSuck.txt

mfw me and inked feather both shelled it at the same time ;-;
mfw you shelled it and i just typed /winner to the end of the URL

i'm not trying to do it seriously, but i think that you can win this if you can shell! keep trying bro

exploit.c - November 15, 2016, 10:50 am

For reference, the exact file name is "WINNER" - there are decoys on the server, so make sure you're looking in the right place

Disco. - November 15, 2016, 10:51 am

I regret to inform you the only winning move is not to play, but please, let's place a game.

Prawnster - November 15, 2016, 10:51 am

(Nov 15, 2016 11:51 AM)Disco. Wrote: [\[CITE\]](#) I regret to inform you the only winning move is not to play, but please, let's place a game.

Someone clicked "view source" view-source:http://185.62.190.191/

exploit.c - November 15, 2016, 10:53 am

To whoever is trying to scan the box:

We've put protection in place already to give you a ton of false positives, so good luck!

Inked ?Feather - November 15, 2016, 10:54 am

i have a nice idea on how to get the answer

but my internet is literally 40kb/s right now.
literally.

(Nov 15, 2016 11:53 AM)exploit.c Wrote: [\[CITE\]](#) To whoever is trying to scan the box:

We've put protection in place already to give you a ton of false positives, so good luck!
i tried using Google dorks, but i can't work them properly. RIP- i don't know if they are the answer,
but i gave it a shot

Papa Cuda - November 15, 2016, 11:23 am

I put a picture of Hitler into the website, first one to post that gets \$1 from me LMAO

Arixs - November 15, 2016, 12:15 pm

Better get to this fast if you guys wanna get in

Stashy - November 15, 2016, 12:18 pm

The contents of the file:

Winner winner chicken dinner. (it's a chicken!)

exploit.c - November 15, 2016, 12:20 pm

(Nov 15, 2016 01:18 PM)Hubba Bubba Gum Wrote: [\[CITE\]](#) The contents of the file:

Winner winner chicken dinner. (it's a chicken!)
Wrong

Jollibee - November 15, 2016, 12:31 pm

"Decoy, try again."

Hahahaha.

TRAUMA - November 15, 2016, 12:35 pm

Found it.

"Not Found

The requested URL /winner.txt was not found on this server.

Apache/2.4.10 (Debian) Server at 185.62.190.191 Port 80"

?heshire - November 15, 2016, 4:25 pm

Pretty vonfident Ill be able to win this, now only if someone doesnt get it before I get home

exploit.c - November 15, 2016, 4:27 pm

(Nov 15, 2016 05:25 PM)ILSeko Wrote: [\[CITE\]](#) Pretty vonfident Ill be able to win this, now only if
someone doesnt get it before I get home
Good luck :Blackhat:

So far no one has been successful at even getting a proper file uploaded to shell

exploit.c - November 15, 2016, 5:24 pm

(Nov 15, 2016 06:06 PM)Yani Wrote: [\[CITE\]](#) Is that a hint? The upload just seems like a decoy. I don't want to toot my own horn, but let me zip up my pants. The upload is not a decoy. ?

No one is yet to defeat this challenge. I will post a hint tomorrow morning if no one has won yet.

Prawnster - November 15, 2016, 5:25 pm

(Nov 15, 2016 06:24 PM)exploit.c Wrote: [\[CITE\]](#) I don't want to toot my own horn, but let me zip up my pants. The upload is not a decoy. ?

No one is yet to defeat this challenge. I will post a hint tomorrow morning if no one has won yet. These challenges are great haha, keep it up ;)

Cibor - November 15, 2016, 5:26 pm

(Nov 15, 2016 06:24 PM)exploit.c Wrote: [\[CITE\]](#) I don't want to toot my own horn, but let me zip up my pants. The upload is not a decoy. ?

No one is yet to defeat this challenge. I will post a hint tomorrow morning if no one has won yet. (° ? °) Father of Mysteriousness

exploit.c - November 15, 2016, 5:27 pm

(Nov 15, 2016 06:26 PM)Cibor Wrote: [\[CITE\]](#) (° ? °) Father of Mysteriousness ?

FRI?DBAO™ - November 15, 2016, 5:48 pm

you expect us to hack ur server???? the website is in php

exploit.c - November 15, 2016, 5:49 pm

(Nov 15, 2016 06:48 PM)FRI?DBAO™ Wrote: [\[CITE\]](#) you expect us to hack ur server???? the website is in php

Which, is insecure and can be hacked super easily if you truly know how ?

?heshire - November 15, 2016, 6:57 pm

Its cool Bao dont get the CTF life

Malicious Intent - November 15, 2016, 7:02 pm

when you try tamper data on the upload it looks like its reading the file but i dont have enough knowledge to make use of it.. looking forward to the solution.. these challenges are probably the best thing on this forum... its a great learning opportunity

exploit.c - November 15, 2016, 7:04 pm

(Nov 15, 2016 08:02 PM)michypc Wrote: [\[CITE\]](#) when you try tamper data on the upload it looks like its reading the file but i dont have enough knowledge to make use of it.. looking forward to the solution.. these challenges are probably the best thing on this forum... its a great learning opportunity

Tampering with the upload form won't get you anywhere

?heshire - November 15, 2016, 8:30 pm

Hmm I find myself frustrated Yet I feel like this should be easier than Im making it.

exploit.c - November 15, 2016, 8:40 pm

(Nov 15, 2016 09:30 PM)ILSeko Wrote: [\[CITE\]](#) Hmm I find myself frustrated Yet I feel like this should be easier than Im making it.

They say the closer you look the less you see ?

TheNamelsJason - November 15, 2016, 8:45 pm

I'm not going to try this, but check for cookie based authentication

?heshire - November 15, 2016, 8:50 pm

Lol Yeah.

I see an outdated Apache Server,

A probably exploitable Fortinet Fortigate 100d OS

and a OpenSSH 6.7p1 Debian Service

Not any applicable exploits that I see but Ill keep looking lol

Sadistic - November 15, 2016, 10:30 pm

Encouraging... Very...

Infinite power - November 15, 2016, 10:35 pm

Sorry guys but I think I've won this one

Sadistic - November 15, 2016, 10:37 pm

(Nov 15, 2016 11:35 PM)Infinite power Wrote: [\[CITE\]](#) Sorry guys but I think I've won this one o shit

Malicious Intent - November 15, 2016, 10:45 pm

Don't think this is the solution

exploit.c - November 16, 2016, 6:24 am

(Nov 15, 2016 11:30 PM)Sadistic Wrote: [\[CITE\]](#)

Encouraging... Very...

You're getting close ?

Someone is getting very close, a hint will be posted in two hours.

pahapoika91 - November 16, 2016, 7:21 am

Just waiting till someone ddosses it down :D

Let's hope sadistic gets through phase too.

??e rando? d??c? g?y - November 16, 2016, 7:57 am

What is this all about?

I regret to inform you the only winning move is not to play, but please, let's place a game.

Papa Cuda - November 16, 2016, 7:59 am

(Nov 16, 2016 08:57 AM)??e rando? d??c? g?y Wrote: [\[CITE\]](#) What is this all about?

I regret to inform you the only winning move is not to play, but please, let's place a game.

What kind of strategy is don't play to win.

??e rando? d??c? g?y - November 16, 2016, 8:14 am

Not Found

The requested URL /winner/WINNER was not found on this server.

Apache/2.4.10 (Debian) Server at 185.62.190.191 Port 80

Jollibee - November 16, 2016, 8:22 am

I didn't even use a scanner, So harsh..

exploit.c - November 16, 2016, 8:27 am

(Nov 16, 2016 09:22 AM)\$each Wrote: [\[CITE\]](#) I didn't even use a scanner, So harsh..

Must've been scanner-like behaviour, hint coming out in 1 hour

??e rando? d??c? g?y - November 16, 2016, 8:47 am

It's probably way easier then everyone is doing xD But i gave up. Good luck to the person who finds it

Prawnster - November 16, 2016, 9:05 am

(Nov 16, 2016 09:27 AM)exploit.c Wrote: [\[CITE\]](#) Must've been scanner-like behaviour, hint coming out in 1 hour

These challenges are fucking class hahaha

You just fucking with everyone that uses tools & its great

pahapoika91 - November 16, 2016, 9:11 am

Lol someone took it down!

@exploit.c block him/them. We want new member to Royalty.

Cibor - November 16, 2016, 9:17 am

(Nov 16, 2016 10:11 AM)pahapoika91 Wrote: [\[CITE\]](#) Lol someone took it down!

@exploit.c block him/them. We want new member to Royalty.

can't hack it => break it

pahapoika91 - November 16, 2016, 9:20 am

:D

Might be Slow Loris attack cause the server is apache.

If that's the case it's easy to block.

Malicious Intent - November 16, 2016, 9:41 am

(Nov 16, 2016 10:20 AM)pahapoika91 Wrote: [\[CITE\]](#) :D

Might be Slow Loris attack cause the server is apache.

If that's the case it's easy to block.

This box has ddos protection..

pahapoika91 - November 16, 2016, 9:43 am

@michypc Slow Loris usually bypasses ddos protection cause it's slow speed.

exploit.c - November 16, 2016, 9:45 am

(Nov 16, 2016 10:20 AM)pahapoika91 Wrote: [\[CITE\]](#) :D
Might be Slow Loris attack cause the server is apache.
If that's the case it's easy to block.
When I get on the box in a few I'll sort it out

Malicious Intent - November 16, 2016, 9:52 am

(Nov 16, 2016 10:43 AM)pahapoika91 Wrote: [\[CITE\]](#) @michypc Slow Loris usually bypasses ddos protection cause it's slow speed.
Interesting .. never really looked into it much .. thanks

Zeno Sama - November 16, 2016, 10:16 am

What happen to the hint?

pahapoika91 - November 16, 2016, 10:24 am

@Zeno the site is under DDoS attack.
But probably @exploit.c will release hint after he gets the attacker/attackers blocked.

exploit.c - November 16, 2016, 11:04 am

Back up and running, nice slowloris attack, IPs blocked. May be a bit slow, but it'll resume properly.

pahapoika91 - November 16, 2016, 11:06 am

(Nov 16, 2016 12:04 PM)exploit.c Wrote: [\[CITE\]](#) Back up and running, nice slowloris attack, IPs blocked.?
You promised hint to them.

exploit.c - November 16, 2016, 11:06 am

(Nov 16, 2016 12:06 PM)pahapoika91 Wrote: [\[CITE\]](#) ?
You promised hint to them.
I'm not sure if you're aware, but PHP has flags you can call, have you considered looking into them? I should zip my mouth shut before I say more

pahapoika91 - November 16, 2016, 11:09 am

(Nov 16, 2016 12:06 PM)exploit.c Wrote: [\[CITE\]](#) I'm not sure if you're aware, but PHP has flags you can call, have you considered looking into them? I should zip my mouth shut before I say more
Remember to take hand out from your panta!

exploit.c - November 16, 2016, 11:10 am

(Nov 16, 2016 12:09 PM)pahapoika91 Wrote: [\[CITE\]](#) Remember to take hand out from your panta!
Yep, but it's phar(:/) in there, and the zip(:/)per is stuck!

Reporter - November 16, 2016, 11:11 am

I can't visit the site at all

pahapoika91 - November 16, 2016, 11:12 am

(Nov 16, 2016 12:11 PM)Reporter Wrote: [\[CITE\]](#) I can't visit the site at all
ddosser detected!
Was it you?
Edit: cant visit neither. Maybe the attacker changed VPN server or something?

exploit.c - November 16, 2016, 11:13 am

(Nov 16, 2016 12:11 PM)Reporter Wrote: [\[CITE\]](#) I can't visit the site at all
Sorry, I'll fix it again.

P.S. whoever is from finland trying to attack this, seriously you haven't even changed the headers in the .NET application, that's sad!

Back online and faster

pahapoika91 - November 16, 2016, 11:18 am

(Nov 16, 2016 12:13 PM)exploit.c Wrote: [\[CITE\]](#) Sorry, I'll fix it again.

P.S. whoever is from finland trying to attack this, seriously you haven't even changed the headers in the .NET application, that's sad!

Back online and fasterAww my finnish brother ddossing you. Im from Finland too. Site is online now.

Did you get browser user-agent? What os he were using?

exploit.c - November 16, 2016, 11:20 am

Notice: since everyone wants to scan, be advised we've put in a rule to auto detect scanners and block them for 12 hours from visiting the site to keep it online and fair, scanning will do nothing since the file you want to read is outside of the accessable WWW directory and you need to upload a payload and execute it to succeed.

AxiS JR - November 16, 2016, 11:20 am

<http://prnt.sc/d84mb0>

Where ma invite homie.

exploit.c - November 16, 2016, 11:22 am

(Nov 16, 2016 12:20 PM)Ariana Wrote: [\[CITE\]](#) <http://prnt.sc/d84mb0>

Where ma invite homie.

That actually made me laugh, inspect element, wrong

pahapoika91 - November 16, 2016, 11:24 am

XD it wasnt it?

exploit pm me the content of WINNER.

I will not leech it.

exploit.c - November 16, 2016, 11:26 am

(Nov 16, 2016 12:24 PM)pahapoika91 Wrote: [\[CITE\]](#) XD it wasnt it?

exploit pm me the content of WINNER.

I will not leech it.

Sent you a PM of it ?

pahapoika91 - November 16, 2016, 11:28 am

Selling the content of WINNER!

For only 99999999-dollars

:D

SIM-2403711 - November 16, 2016, 11:36 am

when you guys figure it out , please let me know how you did it (just for knowledge) thanks .

Muse. - November 16, 2016, 11:41 am

I'm trying...

But I think i'm being dumb...

exploit.c - November 16, 2016, 11:44 am

Someone is getting very close to solving it ?

Muse. - November 16, 2016, 11:50 am

Guessing it's not me?

It can't possibly be me..

exploit.c - November 16, 2016, 11:53 am

(Nov 16, 2016 12:50 PM)CptJayBee Wrote: [\[CITE\]](#) Guessing it's not me?

It can't possibly be me..

Sadistic is the closest:

(Nov 15, 2016 11:30 PM)Sadistic Wrote: [\[CITE\]](#)

Encouraging... Very...

Muse. - November 16, 2016, 12:03 pm

This is a nightmare...

Why am I struggling here exploit?

exploit.c - November 16, 2016, 12:04 pm

(Nov 16, 2016 01:03 PM)CptJayBee Wrote: [\[CITE\]](#) This is a nightmare...

Why am I struggling here exploit?

Don't have the skills I suppose ?

Muse. - November 16, 2016, 12:05 pm

Well i'd better get learning fast then eh?

FiftyTwo - November 16, 2016, 12:07 pm

Posting to follow with this and see who wins lol.

exploit.c - November 16, 2016, 12:18 pm

Still waiting ?

?rthur - November 16, 2016, 12:20 pm

Well this sucks -.-

exploit.c - November 16, 2016, 12:21 pm

(Nov 16, 2016 01:20 PM)?rthur Wrote: [\[CITE\]](#)

Well this sucks -.-
Pro tip:

All uploaded files land in the /skids folder, under the exact file name. To include them, visit
`index.php?include=[file_name]`

ze-slade - November 16, 2016, 12:26 pm

I'll give this a shot, I guess. Probably going to fail entirely but it's worth a shot, lol.

Edit: I predicted correctly.

Forc?d - November 16, 2016, 12:27 pm

Yes another one! I am on it :)

?rthur - November 16, 2016, 12:30 pm

(Nov 16, 2016 01:21 PM)exploit.c Wrote: [\[CITE\]](#) Pro tip:

All uploaded files land in the /skids folder, under the exact file name. To include them, visit
`index.php?include=[file_name]`

If you know what the code on the backside is, it is fairly easy now it is a wild guess :P, but thanks for the hint.

Prawnster - November 16, 2016, 1:32 pm

<https://i.imgur.com/OZIPnMY.png>

Made 0 progress so far, always nice ?

Cibor - November 16, 2016, 1:37 pm

(Nov 16, 2016 02:32 PM)Mazl Wrote: [\[CITE\]](#) <https://i.imgur.com/OZIPnMY.png>

Made 0 progress so far, always nice ?

Imfao ?

exploit.c - November 16, 2016, 1:49 pm

Another hint will be posted in 3 hours if no one has solved it yet

/usr - November 16, 2016, 2:07 pm

(Nov 16, 2016 01:07 PM)FiftyTwo Wrote: [\[CITE\]](#) Posting to follow with this and see who wins lol.
Same here ?

Forc?d - November 16, 2016, 2:13 pm

<https://gyazo.com/03bb508436875d2efd4204c2f89f02ca>

<.<

exploit.c - November 16, 2016, 2:20 pm

Another hint will be posted soon ?

Sift - November 16, 2016, 2:26 pm

Why would one hack into royalty..

Why not just hack into legends better group....

Forc?d - November 16, 2016, 3:14 pm

Waiting for the next clue

However, when this is over.

I would sincerely appreciate an detailed explanation on how the task was successfully done.
Just so i can sleep at night..

Freerunning - November 16, 2016, 3:59 pm

(Nov 16, 2016 04:14 PM)Forc?d Wrote: [\[CITE\]](#) Waiting for the next clue

However, when this is over.

I would sincerely appreciate an detailed explanation on how the task was successfully done.
Just so i can sleep at night..

Same here I will love to see the POC

exploit.c - November 16, 2016, 4:27 pm

Hint:

[http://185.62.190.191/index.php?include=\[secret flag\]skids/file_name_here](http://185.62.190.191/index.php?include=[secret flag]skids/file_name_here)

You better zip up your pants and keep the pharing inside of them, otherwise you'll end up forever trapped in the skids folder

?rthur - November 16, 2016, 4:30 pm

Alright lets go, last piece of the puzzle

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

exploit.c - November 16, 2016, 4:30 pm

(Nov 16, 2016 05:30 PM)?rthur Wrote: [\[CITE\]](#) Alright lets go, last piece of the puzzle

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

Congratulations, you've figured out how to get the file uploaded, executed. Now find the winner file and posts its contents.

Note: system,exec,eval are all disabled, get creative! ?

Forc?d - November 16, 2016, 5:20 pm

I can legit not sleep because of this, its 02:00 my time, i'm going to work early tomorrow.

These kinds of fucking games are not healthy man.

Arthur, can u hurry the fuck up and post the fucking solution + explanation

Prawnster - November 16, 2016, 5:31 pm

(Nov 16, 2016 06:20 PM)Forc?d Wrote: [\[CITE\]](#) I can legit not sleep because of this, its 02:00 my time, i'm going to work early tomorrow.

These kinds of fucking games are not healthy man.

Arthur, can u hurry the fuck up and post the fucking solution + explanation

Hahahah, rip :P

Get sleep & then wake up in the morning and see if Arthur has done it :P

?heshire - November 16, 2016, 5:50 pm

Or if I have done it lol :)

exploit.c - November 16, 2016, 6:03 pm

Server was briefly down, problem resolved, 5 IPs blacklisted for HTTP flood.

Forc?d - November 16, 2016, 6:08 pm

(Nov 16, 2016 06:50 PM)ILSeko Wrote: [\[CITE\]](#) Or if I have done it lol :)

Still waiting! haha

?heshire - November 16, 2016, 6:12 pm

Im waiting on my tiny little neko brain to figure this out lol

Freerunning - November 16, 2016, 6:13 pm

I'm still here waiting for the solution lol!

exploit.c - November 16, 2016, 6:14 pm

So far one person has got an executable shell, they just need to figure out how to read the winners file, they find out where it's located, they just need to find the one unblocked command to read the file and say the winning line.

Edit: We have a winner!

?rthur - November 16, 2016, 6:15 pm

/* Okay, so you think you're that smart? Seriously? What makes you think this isn't just another decoy? Huh? */

Thanks Forc?d for helping me. He gave me a tiny bit of info that helped me get further.

exploit.c - November 16, 2016, 6:16 pm

(Nov 16, 2016 07:15 PM)?rthur Wrote: [\[CITE\]](#) /* Okay, so you think you're that smart? Seriously? What makes you think this isn't just another decoy? Huh? */
Congratulations ?

Care to share how you did it so others can learn? ?

Forc?d - November 16, 2016, 6:18 pm

(Nov 16, 2016 07:16 PM)exploit.c Wrote: [\[CITE\]](#) Congratulations ?

Care to share how you did it so others can learn? ?

Can't you explain the setup and the traps u set to make this hard?
Also the flag that triggered php code to be executed

?rthur - November 16, 2016, 6:20 pm

So all the files where stored in the folder called skids.

It was possible to go through all the directories with the include parameter. Unfortunately ../../../../ didn't work.

However / did, so what you would get is this: ?include=/var/www/html/skids/FILE.zip

If you create an empty file with just the extension .zip and edit the document to insert some PHP code it will be executed.

exploit.c - November 16, 2016, 6:20 pm

(Nov 16, 2016 07:18 PM)Forc?d Wrote: [\[CITE\]](#) Can't you explain the setup and the traps u set to make this hard?

Also the flag that triggered php code to be executed

I can easily, but I'll let him say how he did it first, then post how I've done it.

index.php source: <http://pastebin.com/raw/0Girpgku>

Forc?d - November 16, 2016, 6:20 pm

(Nov 16, 2016 07:15 PM)?rthur Wrote: [\[CITE\]](#) /* Okay, so you think you're that smart? Seriously? What makes you think this isn't just another decoy? Huh? */

Thanks Forc?d for helping me. He gave me a tiny bit of info that helped me get further.

<https://gyazo.com/3a14eecdce67c524b738353f9c119ce3>

I'm gonna be honest here and say fuck you for being greedy.

It triggered me beyond comprehension, it was all good when we shared info trying to solve this together, i send some info and u manage to find the flag and suddenly refuses to share anything more with me.

EDIT: Seems my info did not really triggered a direct solution, however still, i'm salty as fuck,.

?rthur - November 16, 2016, 6:22 pm

(Nov 16, 2016 07:20 PM)Forc?d Wrote: [\[CITE\]](#)

<https://gyazo.com/3a14eecdce67c524b738353f9c119ce3>

I'm gonna be honest here and say fuck you for being greedy.

It triggered me beyond comprehension, it was all good when we shared info trying to solve this together, i send some info and u manage to find the flag and suddenly refuses to share anything more with me.

I am sorry man, but I have had other people steal credits before and I did not want that to happen.

exploit.c - November 16, 2016, 6:22 pm

(Nov 16, 2016 07:20 PM)?rthur Wrote: [\[CITE\]](#) So all the files where stored in the folder called skids.

It was possible to go through all the directories with the include parameter. Unfortunately ../../../../ didn't work.

However / did, so what you would get is this: ?include=/var/www/html/skids/FILE.zip

If you create an empty file with just the extension .zip and edit the document to insert some PHP code it will be executed.

That's one way, the other way is if you do a little magical zip file with .phar extension, proof of concept:

<http://185.62.190.191/index.php?include=phar://skids/exploite2.phar/cmd.txt&cmd=x>

Forc?d - November 16, 2016, 6:24 pm

(Nov 16, 2016 07:22 PM)exploit.c Wrote: [\[CITE\]](#) That's one way, the other way is if you do a little magical zip file with .phar extension, proof of concept:

<http://185.62.190.191/index.php?include=phar://skids/exploite2.phar/cmd.txt&cmd=x>

i gave php://input a try sending the command for execution as POST

However system was disabled so yeah..

exploit.c - November 16, 2016, 6:25 pm

(Nov 16, 2016 07:24 PM)Forc?d Wrote: [\[CITE\]](#) i gave php://input a try sending the command for execution as POST

However system was disabled so yeah..

Yep, was designed to be hard ?

Forc?d - November 16, 2016, 6:28 pm

(Nov 16, 2016 07:25 PM)exploit.c Wrote: [\[CITE\]](#) Yep, was designed to be hard ?

Anyway, besides me not having any hair left on my head, i can now SLEEP.

Really looking forward to more of this, does not need to be an end price for membership in the end (for me atleast) in the future.

:)

exploit.c - November 16, 2016, 6:31 pm

(Nov 16, 2016 07:28 PM)Forc?d Wrote: [\[CITE\]](#) Anyway, besides me not having any hair left on my head, i can now SLEEP.

Really looking forward to more of this, does not need to be an end price for membership in the end (for me atleast) in the future.

:)

lol sleep good

?heshire - November 16, 2016, 6:41 pm

Congratz to the winners. I spent my fair share of hours on this, and Im glad someone finally got it :3

Cibor - November 16, 2016, 6:46 pm

(Nov 16, 2016 07:20 PM)?rthur Wrote: [\[CITE\]](#) So all the files where stored in the folder called skids.

It was possible to go through all the directories with the include parameter. Unfortunately ../../../../ didn't work.

However / did, so what you would get is this: ?include=/var/www/html/skids/FILE.zip

If you create an empty file with just the extension .zip and edit the document to insert some PHP code it will be executed.

Congratulations and welcome to Royalty.

exploit.c - November 16, 2016, 6:52 pm

Congratulations Arthur, welcome to Royalty ?