

Forum:[Hack Forums](#)

Thread: [\[Antagonism\] PHP-based Challenges ~](#)

Keeper - June 15, 2013, 3:05 pm

I've took aside some time to put up something rather different into this section and get some PHP-based challenges to your attention. So far there are eight of them. Each challenge has a brief description as to how to go about exploiting the script supplied. Post a PoC if eager and PM me the solutions individually. The following topics have been covered: Directory Traversal & Null byte Injection

~ <http://keeperax.netai.net/Antagonism/DirTra.php> ~ 5 points

- Look at the given code here. You want to execute the code block as if you were in fact logged in. You can't control the \$user object directly and thus you can't get to the code that includes admin.php file. But you have control over the \$page variable, via the GET-parameter p. In the code ".html" is concatenated to the filename and we can effectively stop that with the null byte (depending on the server settings though, so don't expect a 100% success rate with this kind of an attack). The admin.php file is located one directory before the folder 'pages'.

PHP Register Globals Exploitation

~ <http://keeperax.netai.net/Antagonism/PRG.php> ~ 10 points

- Again, let's view the code. If the user provides correct credentials, the \$loggedIn variable is set to true; further if the user has administrator privileges, the \$priv variable is set to 1. Later then those values are checked and depending on their values, the program flow is determined. Naturally we are aiming for administrative account. Let's now apply our knowledge about register globals to this level.

Unsafe Usage of Extract Function

~ <http://keeperax.netai.net/Antagonism/Extract.php> ~ 10 points

- It is a good idea to always initialize the variables, like \$pass_file here. It is not a good idea though to initialize them just before "extract(\$_REQUEST);". What extract() basically does, is it reads the keys and values from an array and creates variables corresponding to them. Overwrite the pass_file argument in such a way that you don't need to supply a value for the \$pass variable. Use the string value 'foobar' where needed.

PHP Object Injection (unserialize())

~ <http://keeperax.netai.net/Antagonism/Objectz.php> ~ 15 points

- Perform a code injection by supplying a crafted string of the serialized object from the below script in order to obtain the IP address of the server. Refer to the docs ~

<http://php.net/manual/en/function.serialize.php> in case of experiencing any difficulty. Encode the serialized object in Base64 due to stupid SPAM filters.

Server Side Includes Injection

~ <http://keeperax.netai.net/Antagonism/SSI.php> ~ 10 points

In order to pass this challenge you need to know the basics of SSI. For the sake of this one, include the file named "a77.txt" located in the directory of "scripts". Finally, encode the payload in Base64 due to SPAM filters again..

Cross-site Scripting Filter Evasion

~ <http://keeperax.netai.net/Antagonism/XSS.php> ~ 5 points

- This is a simple filter evasion challenge. Pop-up your name in a Javascript window. A piece of the filtration has been give to you.

Basic Cryptography Sequence

~ <http://keeperax.netai.net/Antagonism/Cryptography.php> ~ 5 points

- A basic cryptography sequence that needs to get decoded. No custom shit, no tricks. Testing the ability to identify public encodings.

PHP-based Obfuscation Challenge

- ~ <http://keeperax.netai.net/Antagonism/Obfuscation.php> ~ 10 points
- Deobfuscate the following PHP-based code. Input the final result in the form below.

A total of 70 points is for all of them completed. According to that:

- 5 points ~ 7% success rate
- 10 points ~ 14% success rate
- 15 points ~ 21% success rate
- 20 points ~ 28% success rate
- 25 points ~ 35% success rate
- 30 points ~ 42% success rate
- 35 points ~ 50% success rate
- 40 points ~ 57% success rate
- 45 points ~ 64% success rate
- 50 points ~ 71% success rate
- 55 points ~ 78% success rate
- 60 points ~ 85% success rate
- 65 points ~ 92% success rate
- 70 points ~ 100% success rate

Let's see who will get 'em first.

-- Ranking:

[-?Divine-](#)

- Points: 70
- Success Rate: 100%
- Solved: All of them

[Phizo](#)

- Points: 70
- Success Rate: 100%
- Solved: All of them

[ankr-](#)

- Points: 70
- Success Rate: 100%
- Solved: All of them

[bckslsh.](#)

- Points: 70
- Success Rate: 100%
- Solved: All of them

[cheatson](#)

- Points: 70
- Success Rate: 100%
- Solved: All of them

[Pendragon](#)

- Points: 70
- Success Rate: 100%
- Solved: All of them

[Ergo](#)

- Points: 70
- Success Rate: 100%
- Solved: All of them

[v?x?](#)

- Points: 70

- Success Rate: 100%
- Solved: All of them

[Deso](#)

- Points: 55
- Success Rate: 78%
- Solved: Basic Cryptography Sequence, PHP-based Obfuscation, Directory Traversal & Null byte Injection, Cross-site Scripting Filter Evasion, PHP Register Globals Exploitation, Server-side Includes Injection, Unsafe Usage of Extract Function

[ryuk`](#)

- Points: 55
- Success Rate: 78%
- Solved: Directory Traversal & Null byte Injection, PHP Register Globals Exploitation, Unsafe Usage of Extract Function, Server-side Includes Injection, Cross-site Scripting Filter Evasion, Basic Cryptography Sequence, PHP-based Obfuscation

[KoVex](#)

- Points: 50
- Success Rate: 71%
- Solved: Directory Traversal & Null byte Injection, Cross-site Scripting Filter Evasion, PHP-based Obfuscation, Basic Cryptography Sequence, Server-side Includes Injection, PHP Object Injection

[MrCathal09](#)

- Points: 50
- Success Rate: 71%
- Solved: Cross-site Scripting Filter Evasion, Directory Traversal & Null byte Injection, Server-side Includes Injection, Basic Cryptography Sequence, PHP-based Obfuscation, PHP Object Injection

[PuzzuS](#)

- Points: 25
- Success Rate: 35%
- Solved: Server-side Includes Injection, Cross-site Scripting Filter Evasion, Directory Traversal & Null byte Injection, Basic Cryptography Sequence

[VipVince](#)

- Points: 25
- Success Rate: 35%
- Solved: Server-side Includes, Cross-site Scripting Filter Evasion, Basic Cryptography Sequence, Directory Traversal & Null byte Injection

[John4782](#)

- Points: 20
- Success Rate: 28%
- Solved: Directory Traversal & Null byte Injection, PHP Register Globals Exploitation, Cross-site Scripting Filter Evasion

[Agent Raigar](#)

- Points: 15
- Success Rate: 21%
- Solved: Directory Traversal & Null byte Injection, Server-side Includes Injection

[crossera](#)

- Points: 15
- Success Rate: 21%
- Solved: Cross-site Scripting Filter Evasion, Server-side Includes Injection, Directory Traversal & Null byte Injection

[Pillows](#)

- Points: 5
- Success Rate: 7%
- Solved: Basic Cryptography Sequence

[vehla](#)

- Points: 5
- Success Rate: 7%
- Solved: Cross-site Scripting Filter Evasion
[Lambasoft](#)
- Points: 5
- Success Rate: 7%
- Solved: Directory Traversal & Null byte Injection
-
- Points: ...
- Success Rate: ...
- Solved: ...
- ...

Good luck to those who participate and please do not disclose any solutions.

log dot zip - June 15, 2013, 4:12 pm

Keeper never fails to deliver fun and challenging stuff. I'll try, keep up the good work! =3

shellfu - June 15, 2013, 4:19 pm

Great Challenges! Good luck to anybody trying them out!

Suit® - June 15, 2013, 4:40 pm

This is beautiful. Great work man! I'm already digging into this

Keeper - June 15, 2013, 4:51 pm

We got the first solver of some of them. Thread updated.

Agent Raigar - June 15, 2013, 5:41 pm

Great challenges. Going to try these ASAP

Keeper - June 15, 2013, 6:46 pm

Updated with four more and resulting in total of eight. Points & success rate altered as well.

-?Divine- - June 15, 2013, 6:52 pm

Nice challenges Keeper. Thanks, was fun.

Can you put 'Success Rate' in some gay color like this?

cheatson - June 15, 2013, 7:43 pm

Looks good, gonna give these a try later

-?Divine- - June 15, 2013, 7:46 pm

(Jun 15, 2013 07:43 PM)cheatson Wrote: [\[CITE\]](#) Looks good, gonna give these a try later

Good guy Cheatson. Doesn't do it yet, but posts so the thread doesn't die. You would be surprised at how many views it already got lol.

Pendragon - June 15, 2013, 7:46 pm

Would love to try this out, but the website doesn't seem to be loading for me.

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

-?Divine- - June 15, 2013, 7:47 pm

(Jun 15, 2013 07:46 PM)Pendragon Wrote: [\[CITE\]](#) Would love to try this out, but the website doesn't seem to be loading for me.

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

It loads fine for me and the others. It's just you mate.

SHADOW REALM - June 15, 2013, 7:49 pm

Like that (For the XSS), Or do we actually make an alert box? I'm tired atm so

-?Divine- - June 15, 2013, 7:55 pm

(Jun 15, 2013 07:49 PM)SHADOW Wrote: [\[CITE\]](#)

Like that (For the XSS), Or do we actually make an alert box? I'm tired atm so
Does the php source he provided mean nothing to you? That's the easiest thing he put in this thread.

Pendragon - June 15, 2013, 8:04 pm

(Jun 15, 2013 07:47 PM)-?Divine- Wrote: [\[CITE\]](#) It loads fine for me and the others. It's just you mate.
DONT U PULL THAT "MATE" ON ME MR. I KNOW YOU'RE NOT AUSTRALIAN YOU DIRTY SERBIAN.

-?Divine- - June 15, 2013, 8:20 pm

(Jun 15, 2013 08:04 PM)Pendragon Wrote: [\[CITE\]](#) DONT U PULL THAT "MATE" ON ME MR. I KNOW YOU'RE NOT AUSTRALIAN YOU DIRTY SERBIAN.

Oh is that true Mr. Dragan? I am Australian on my father's grandmonther's uncle's side.

Apple J4ck. - June 15, 2013, 9:11 pm

Solved a couple although I'm stuck with one of them x.x

Great challenges though.

I'll try to solve the rest later & send you the solutions, thanks :P

Zhyper - June 15, 2013, 10:40 pm

i just solved the 1st challenge took me about 1hour lol xD

alphabot - June 15, 2013, 10:43 pm

Yeah, site is not working for me either.

DarkFlux™ - June 15, 2013, 10:49 pm

Any tutorial for this ?: i need to check out its tutorial first :)

Keeper - June 16, 2013, 1:32 am

(Jun 15, 2013 06:52 PM)-?Divine- Wrote: [\[CITE\]](#) Nice challenges Keeper. Thanks, was fun.

Can you put 'Success Rate' in some gay color like this?

It looks even gayer with it. It's enough colorful but since I respect you, only yours will be in that color (?)

(Jun 15, 2013 07:49 PM)SHADOW Wrote: [\[CITE\]](#) Like that (For the XSS), Or do we actually make an alert box? I'm tired atm so

Of course, there needs to be one of those shiny alert boxes and it's by far the easiest one from the

eight of those.

(Jun 15, 2013 10:49 PM)DarkFlux™ Wrote: [\[CITE\]](#) Any tutorial for this ?: i need to check out its tutorial first :)

Most have been covered even on HF. Do some browsing around this very section or compilations of tutorials.

Replied to those that have sent me solutions.

Phizo - June 16, 2013, 2:01 am

Very nice list of challenges, Keeper.

A few of my solutions don't seem to work on your end, but have been tested and proved functional using the same vulnerable code.

Of course, I completely understand that this occurs because of your regex or other form of validation. I assume you will accept solutions that work realistically?

I look forward to seeing more challenges soon.

Keeper - June 16, 2013, 2:02 am

(Jun 16, 2013 02:01 AM)Phizo Wrote: [\[CITE\]](#) Very nice list of challenges, Keeper.

A few of my solutions don't seem to work on your end, but have been tested and proved functional using the same vulnerable code.

Of course, I completely understand that this occurs because of your regex or other form of validation. I assume you will accept solutions that work realistically?

I look forward to seeing more challenges soon.

PM me what you have so far. It is indeed kinda buggy due to SPAM and some of its 'filters'.

Zhyper - June 16, 2013, 2:04 am

after 2 hours still can't solve the xss challenge lol xD

Keeper - June 16, 2013, 2:42 am

(Jun 16, 2013 02:04 AM)Zhyper Wrote: [\[CITE\]](#) after 2 hours still can't solve the xss challenge lol xD
It's the easiest. The piece/snippet of code is shown for a reason.

Also thanks to [Phizo](#) for pointing some inaccuracies in some of the challenges.

-?Divine- - June 16, 2013, 6:43 am

(Jun 16, 2013 01:32 AM)Keeper Wrote: [\[CITE\]](#) It looks even gayer with it. It's enough colorful but since I respect you, only yours will be in that color (?)

Thanks Keeper. It really means a lot to me.

Keeper - June 16, 2013, 6:55 am

(Jun 16, 2013 06:43 AM)-?Divine- Wrote: [\[CITE\]](#) Thanks Keeper. It really means a lot to me.
Don't be silly. No color for you.

[ankr-](#) also did all of them. A total of three guys out of five have 100% success rate which is better than I anticipated. Considering there are also some that do not want to be listed, I must say it worked out as an idea of multiple challenges.

rktcool - June 16, 2013, 9:26 am

Looks like fun... Thanks for the thread... Will love to learn from these :-)

-?Divine- - June 17, 2013, 3:12 am

(Jun 17, 2013 01:12 AM)Phizo Wrote: [\[CITE\]](#) I'm just going to post to get this to the top of the page again.

Keeper deserves to receive more recognition for the effort he put into developing these challenges.

I personally also want to see who else can complete them all.

It's not so much that they are difficult to the point where I don't expect any other participants to complete them; it's just to determine whether or not this section possesses any positives.

If you're unable to complete these, and have been into web-hacking for quite some time, then you're learning the wrong way.

In other words, you are doing a HQ bum.p. There are a few more people I'm expecting to finish this. Perhaps they missed it.

Keeper - June 17, 2013, 4:15 am

Updated the list with some more solvers. Thanks for the comments.

Cathal - June 17, 2013, 7:38 am

I suggest everyone try at least 2 of these. You'll learn quite a bit.

Thanks Keeper.

Keeper - June 17, 2013, 7:50 am

[cheatson](#) also got all of 'em. That makes 5 out of 13 with 100% success rate. Also updated the list with a few more participants.

shellfu - June 17, 2013, 8:06 am

Thanks Keeper! Keep making more of these challenges!

Phizo - June 17, 2013, 8:09 am

Everyone dislikes vehla, so I'm just going to post this before someone else does.

Quote:vehla

- Points: 5

- Success Rate: 7%

- Solved: Cross-site Scripting Filter Evasion

Unsurprising.

I feel mean.

cheatson - June 17, 2013, 8:25 am

Thanks keeper very fun, we want moar!!!

Keeper - June 17, 2013, 8:48 am

(Jun 17, 2013 08:25 AM)cheatson Wrote: [\[CITE\]](#) Thanks Keeper very fun, we want moar!!!

I will indeed be making a quiz divided into multiple categories but that'd possibly happen at the end of the week because I also need to think of some sort of an anti-cheating 'system' in order to keep the idea as realistic as possible.

-?Divine- - June 17, 2013, 10:05 am

(Jun 17, 2013 08:09 AM)Phizo Wrote: [\[CITE\]](#) Everyone dislikes vehla, so I'm just going to post this before someone else does.

Unsurprising.

I feel mean.

He's my role model. I don't see why so many hate someone as great as him.

Keeper - June 18, 2013, 5:21 am

Updated a few more results. Good to see so many people taking part. I actually feel like I managed to force some guys learn something new.

Cathal - June 18, 2013, 8:10 am

Have no idea what to do for Register Globals or the Extract function.

zeru - June 18, 2013, 5:30 pm

unbanned yay
site isn't loading for me?

-?Divine- - June 18, 2013, 5:31 pm

(Jun 18, 2013 05:30 PM)zeru Wrote: [\[CITE\]](#) unbanned yay
site isn't loading for me?
Mister Zeru is back. Welcome back mastah.

zeru - June 18, 2013, 5:34 pm

(Jun 18, 2013 05:31 PM)-?Divine- Wrote: [\[CITE\]](#) Mister Zeru is back. Welcome back mastah.that's right your mastah is back son

xXSehgalXx - June 19, 2013, 10:06 am

I have sent you some of the solutions. Nice challenge!

?XilluX - June 19, 2013, 11:45 am

Nice Thread, i got the first 3 solved :)

xXSehgalXx - June 19, 2013, 1:59 pm

I got stuck at SHA-1 hash 4d** Any help?

Th3PonyWizard - June 19, 2013, 2:35 pm

Horray, more challenges to figure out the amounts of brain cells I lack. Solved three so far (I found the SSI to be much easier than the XSS one)

Keeper - June 20, 2013, 4:10 am

(Jun 19, 2013 01:59 PM)xXSehgalXx Wrote: [\[CITE\]](#) I got stuck at SHA-1 hash 4d** Any help?
What bigger help would it be other than reading the description for every challenge precisely?
There are no hash functions or any encryption algorithms used. It's all about lame public encodings.

Z0mbie. - June 20, 2013, 8:12 pm

will be trying this after I finish up with some things.

Exusia - June 22, 2013, 7:54 pm

The page is timing out
Is my ip range blocked?

Keeper - June 23, 2013, 1:31 am

(Jun 22, 2013 07:54 PM)Exusia Wrote: [\[CITE\]](#) The page is timing out
Is my ip range blocked?
No IPs have been blocked. However, it's hosted on a free webhost so it does go down from time to time.

Weexe - June 23, 2013, 2:19 am

Nice Challenges !

Very helpfull to learn basic at hacking.

ForexMine - *June 23, 2013, 6:35 am*

Great challanges, thanks for doing this :p

urez - *July 15, 2013, 11:10 am*

I HAVE SO MUCH SWAG THAT MY PENIS IS THROBBING AHH

BeggFoMercy - *July 15, 2013, 12:15 pm*

Do i have to put an SS here and PM you how did i pass the challenge ? or can i just PM you the both :)

Krieg - *July 16, 2013, 12:59 pm*

These are interesting. Nice work on the extract abuse one... I swear I've seen it somewhere else before, but that's beside the point. It's still good.

v?x? - *July 18, 2013, 9:48 am*

I've completed 5/8 of these with 35 points. I think I'll PM you now Keeper and then PM you again at a later date when I've finished the rest. Don't have time to figure out the last 3 right now.

Ergo - *July 18, 2013, 9:59 am*

I've completed them all. PM'd you the answers as well. Good challenges.

Keeper - *July 18, 2013, 10:51 am*

Updated. I hardly come by this thread but will edit it as often as possible.

v?x? - *July 18, 2013, 6:55 pm*

7/8 done now. Waiting until I've completed this last one before PM'ing you again.

Xen_ - *July 19, 2013, 12:14 am*

I have completed two of the challenges so far for a total of 15 points.

I'll PM you the details and screenshots of them, and I'll try some more later.

v?x? - *July 21, 2013, 7:56 am*

Finally completed them all. Thanks for the challenge, Keeper!

jollyR - *July 21, 2013, 10:26 pm*

Cool challenges, almost completed them all. Thanks

Aakash_Choudhary - *October 7, 2015, 5:16 am*

Thanks for the challenge :->

<http://prntscr.com/8opai9>

Xen0n- - *December 23, 2016, 12:27 am*

Bumping this. HQ post, Challenges are still up.

And the community could probably do well to learn a thing or two instead of begging others to do their dirty work for them all day.

Maxs - *January 4, 2017, 11:37 pm*

Great Challenges! Good luck to anybody trying them out!