

Forum:[Hack Forums](#)

Thread: [Legion ~ Arbitrary File Uploading | Tutorial](#)

Niggz - January 18, 2014, 8:43 pm

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

Step 1:

Start off by selecting one of the following dorks and entering it into google or any other web browser.

Code inurl:upload.php?file= ext:php

inurl:upload?filename= ext:php

inurl:upload.aspx?file= ext:php

inurl:action=upload?file= ext:php

Step 2:

Once you find a website you will see something like this:

Spoiler ([Click to View](#)) [img]http://s21.postimg.org/dfnzxxqzr/image.jpg[/img]

You should then upload either a shell or an image to the website by selecting it, then pressing the upload button.

Step 3:

Once you have uploaded your file (shell) the site should be defaced and to your liking.

Credits to Keeper for the dorks.

Ascendon - January 19, 2014, 4:01 am

What if the website has a filter?

You didn't explain how to bypass it.

Leg?nd - January 19, 2014, 4:19 am

(Jan 19, 2014 05:01 AM)Ascendon Wrote: ([CITE](#)) What if the website has a filter?

You didn't explain how to bypass it.

Because he doesn't know how to bypass it.

He steals threads and posts them as his own.

inb4googleshows how to bypass and update thread without credits

SHADOW REALM - January 19, 2014, 4:24 am

This is the dumbest thread I have ever read. I have seen 1000000's of dorks like this and you just say put in your shell

outlaw - January 19, 2014, 4:33 am

There's a lot wrong with this thread.

First of all, you aren't even describe why this works, I doubt you even know yourself. Secondly, what if the upload file has filters? Which most do. Thirdly, your dorks make no sense, especially this one:

Code inurl:upload.aspx?file= ext:php

Here you're telling Google to basically search for the file "upload.aspx" with the extention .php - How the fuck do you expect that to work? This entire thread is a fail. Start reading OP, don't make tutorials on something you don't know!

EDIT: That dork managed to find a shell that someone has uploaded and I'll explain why:

Here is the FULL URL that was found:

Code

<http://www.ghfour.com/admin/app/webroot/img/product/Jawa.php?jiko=chmodjiko=shell&action=edit&chdir=/var/www/vhosts/ghfour.com/httpdocs/admin/app/webroot/js/fckeditor/editor/filemanager/connectors/asp/&file=upload.aspx>

See, if you look here. It found the "Jawa.php" file due to your ext:php and then managed to execute the shells file editor on the file "upload.aspx".

SHADOW REALM - January 19, 2014, 4:43 am

(Jan 19, 2014 05:33 AM)Pro Skid Wrote: [\[CITE\]](#) There's a lot wrong with this thread.

First of all, you aren't even describe why this works, I doubt you even know yourself. Secondly, what if the upload file has filters? Which most do. Thirdly, your dorks make no sense, especially this one:

Code inurl:upload.aspx?file= ext:php

Here you're telling Google to basically search for the file "upload.aspx" with the extention .php - How the fuck do you expect that to work? This entire thread is a fail. Start reading OP, don't make tutorials on something you don't know!

EDIT: That dork managed to find a shell that someone has uploaded and I'll explain why:

Here is the FULL URL that was found:

Code

<http://www.ghfour.com/admin/app/webroot/img/product/Jawa.php?jiko=chmodjiko=shell&action=edit&chdir=/var/www/vhosts/ghfour.com/httpdocs/admin/app/webroot/js/fckeditor/editor/filemanager/connectors/asp/&file=upload.aspx>

See, if you look here. It found the "Jawa.php" file due to your ext:php and then managed to execute the shells file editor on the file "upload.aspx".

That asp with php extension reminded me where he got it from

<https://hackforums.net/showthread.php?tid=3184197>

outlaw - January 19, 2014, 4:47 am

(Jan 19, 2014 05:43 AM)SHADOW REALM Wrote: [\[CITE\]](#) That asp with php extension reminded me where he got it from

<https://hackforums.net/showthread.php?tid=3184197>

Haha, great, so not only he doesn't have a clue what he's talking about, he practically stole the thread from someone who does.

SHADOW REALM - January 19, 2014, 5:01 am

(Jan 19, 2014 05:47 AM)Pro Skid Wrote: [\[CITE\]](#) Haha, great, so not only he doesn't have a clue what he's talking about, he practically stole the thread from someone who does.

He also did the same thing for his deletion one lol

inurl:"delete.php?file=" ext:php

inurl:"delete?filename=" ext:php

inurl:"delete.aspx?file=" ext:php

inurl:"action=delete?file=" ext:php

outlaw - January 19, 2014, 5:02 am

(Jan 19, 2014 06:01 AM)SHADOW REALM Wrote: [\[CITE\]](#) He also did the same thing for his deletion one lol

inurl:"delete.php?file=" ext:php

inurl:"delete?filename=" ext:php

inurl:"delete.aspx?file=" ext:php

inurl:"action=delete?file=" ext:php

Yeah I saw. The dork will NOT work though. It's a useless dork.

Ascendon - January 19, 2014, 5:34 am

He just basically told us how to upload a file..

We aren't as useless as you are slow..

SHADOW REALM - January 19, 2014, 5:39 am

Seriously, Legion need to step up their shit before they keep having retards like this idiot and others putting random shit that nobody cares about up here

outlaw - January 19, 2014, 5:46 am

(Jan 19, 2014 06:39 AM)SHADOW REALM Wrote: [\[CITE\]](#) Seriously, Legion need to step up their shit before they keep having retards like this idiot and others putting random shit that nobody cares about up here

Right? Like when Starfall was in Legion. Now it's just full of idiots wanting to be anonmus.

SHADOW REALM - January 19, 2014, 5:54 am

(Jan 19, 2014 06:46 AM)Pro Skid Wrote: [\[CITE\]](#) Right? Like when Starfall was in Legion. Now it's just full of idiots wanting to be anonmus.

Starfall got closed with all that root stuff. I remember the legion skype chat when I was in it and the Skype SE thing was going around and starfall used to either get hacked and then have his whole contact list added to the chat or he just did it for lulz

Long live aush0k

Leg?nd - January 19, 2014, 6:16 am

(Jan 19, 2014 06:54 AM)SHADOW REALM Wrote: [\[CITE\]](#) Starfall got closed with all that root stuff. I remember the legion skype chat when I was in it and the Skype SE thing was going around and starfall used to either get hacked and then have his whole contact list added to the chat or he just did it for lulz

Long live aush0k

Aush0k is a jew, get over it.
long live yolo

Niggz - January 19, 2014, 8:24 am

(Jan 19, 2014 05:01 AM)Ascendon Wrote: [\[CITE\]](#) What if the website has a filter?

You didn't explain how to bypass it.

Because I haven't looked into bypassing the filters. I rarely use this because there are a lot of other things you can use to deface a website.

(Jan 19, 2014 05:33 AM)Pro Skid Wrote: [\[CITE\]](#) There's a lot wrong with this thread.

First of all, you aren't even describe why this works, I doubt you even know yourself. Secondly, what if the upload file has filters? Which most do. Thirdly, your dorks make no sense, especially this one:

Code inurl:upload.aspx?file= ext:php

Here you're telling Google to basically search for the file "upload.aspx" with the extention .php - How the fuck do you expect that to work? This entire thread is a fail. Start reading OP, don't make tutorials on something you don't know!

EDIT: That dork managed to find a shell that someone has uploaded and I'll explain why:

Here is the FULL URL that was found:

Code

<http://www.ghfour.com/admin/app/webroot/img/product/Jawa.php?jiko=chmodjiko=shell&action=edit&chdir=/var/www/vhosts/ghfour.com/httpdocs/admin/app/webroot/js/fckeditor/editor/filemanager/connectors/aspx/&file=upload.aspx>

See, if you look here. It found the "Jawa.php" file due to your ext:php and then managed to execute the shells file editor on the file "upload.aspx".

If I didn't understand it, than how could I find a website not used in other tutorials?

I don't need to explain how dorks work. But I will.

Google searches the web for the specific text that you put. So if you put "inurl:Pro Skid Down" then google would find all websites who's url matches the criteria.

Works for a lot more browsers than google.

(Jan 19, 2014 06:46 AM)Pro Skid Wrote: [\[CITE\]](#) Right? Like when Starfall was in Legion. Now it's just full of idiots wanting to be anonmus.

Way to spell anonymous correctly.

Calling me an idiot?

/Jigsaw/ - January 24, 2014, 5:18 pm

(Jan 19, 2014 09:24 AM)SI0w Wrote: [\[CITE\]](#) Because I haven't looked into bypassing the filters. I rarely use this because there are a lot of other things you can use to deface a website.

If I didn't understand it, than how could I find a website not used in other tutorials?

I don't need to explain how dorks work. But I will.

Google searches the web for the specific text that you put. So if you put "inurl:Pro Skid Down" then google would find all websites who's url matches the criteria.

Works for a lot more browsers than google.

Way to spell anonymous correctly.

Calling me an idiot? He meant it as you're a complete skid that has little to no knowledge about this stuff.

Canonsx130 - January 24, 2014, 5:40 pm

Not really the best of tuts but good presentation I guess. This might help the very basic guys who wants to quickly shell some random sites.

Kirian - January 25, 2014, 11:06 pm

I'm sorry Sl0w, but this thread is useless. How is this even compared to hacking? I was doing this when I was 11, and thought I was badass and then found out it's shit.

SHADOW REALM - January 26, 2014, 4:18 am

(Jan 26, 2014 05:15 AM)Zayne Wrote: [\[CITE\]](#) PHP Code

<?php

defaced and to your liking.

Why deface when you can root?

Leigons custom HTML 0-day doesn't work. I heard they that recruited Krew to get his Apache REMOTE root going