matthieu-hackwitharts Update rce_file_upload.md History

1 contributor

43 lines (27 sloc) | 1.57 KB

Remote code execution via arbitrary file upload (CVE-2022-37159)

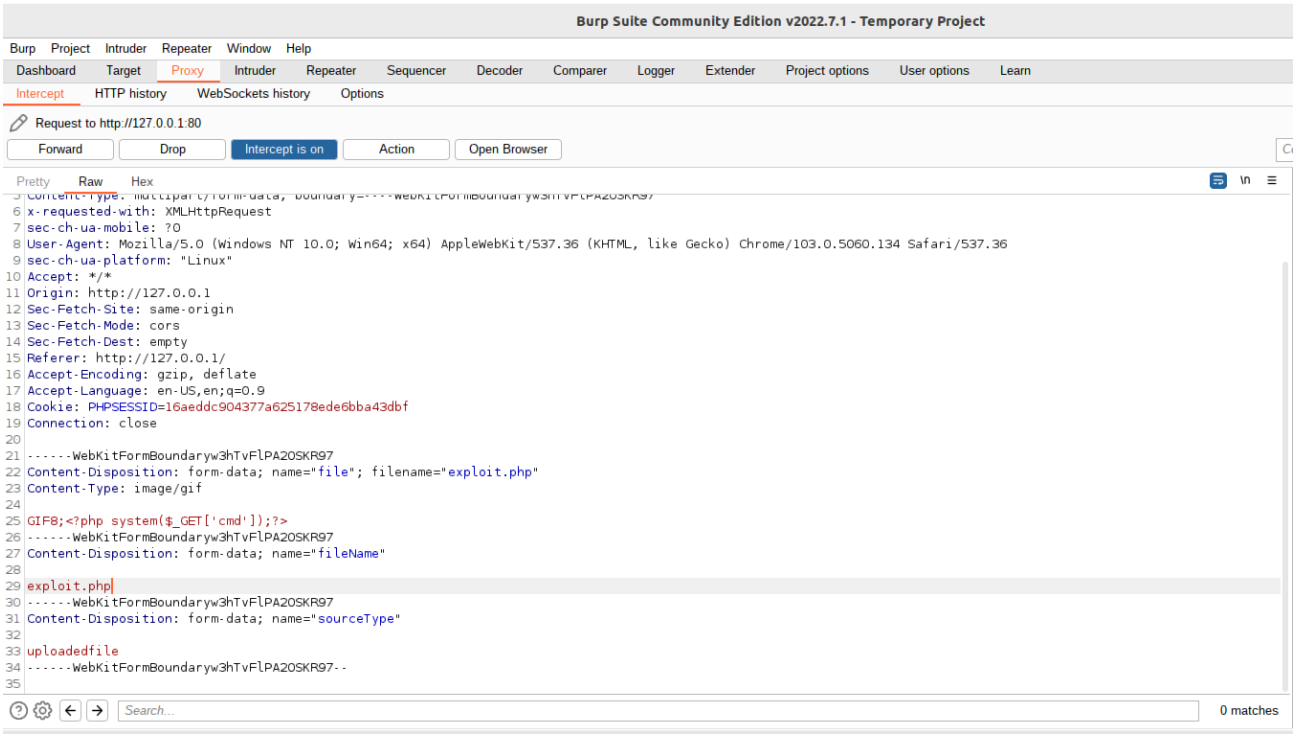
Claroline Connect app presents a RCE vulnerability because of the possibility to upload an arbitrary php file. This vulnerability is present on many upload forms, so I've personnally choosed the resource icon section.

The route **core/Controller/APINew/FileController.php** filters the upload image type by using the getMimeType() function from Symfony :

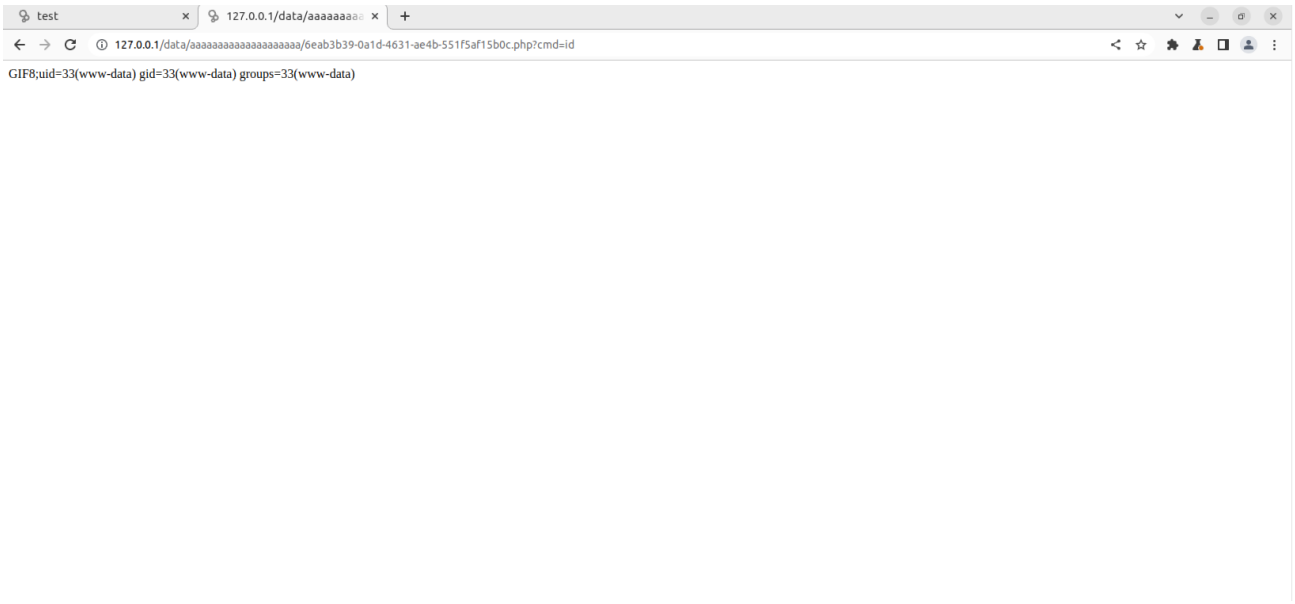
```
public function uploadImage(Request $request): JsonResponse
    {
        $files = $request->files->all();

        $objects = [];
        foreach ($files as $file) {
            if (0 !== strpos($file->getMimeType(), 'image')) {
                throw new InvalidDataException('Invalid image type.');
            }

            $object = $this->crud->create(PublicFile::class, [], ['file' => $file, C
            $objects[] = $this->serializer->serialize($object);
        }
```

```
        return new JsonResponse($objects);
    }
```

It is possible to trick this function by adding some magic bytes like `GIF8;` which corresponds to the GIF image file type. The mime type `image/gif` should be also applied.



Then it is possible to get RCE by using the upload php shell :



Fix suggestions : Enhance file upload checks by adding real mime type verification (file content, bytes, size, etc).