File Upload XSS

Vulnerables Follow

Feb 16, 2018 · 2 min read

File upload XSS

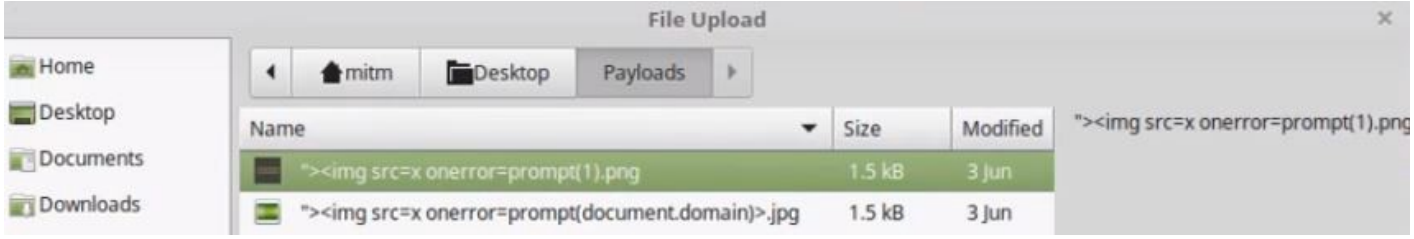
The web application allows file upload and was able to upload a file containing HTML content. When HTML files are allowed, XSS payload can be injected in the file uploaded but this vulnerability will only work in linux because windows OS doesn't allow the tags in file name. Let's have a look at PoC

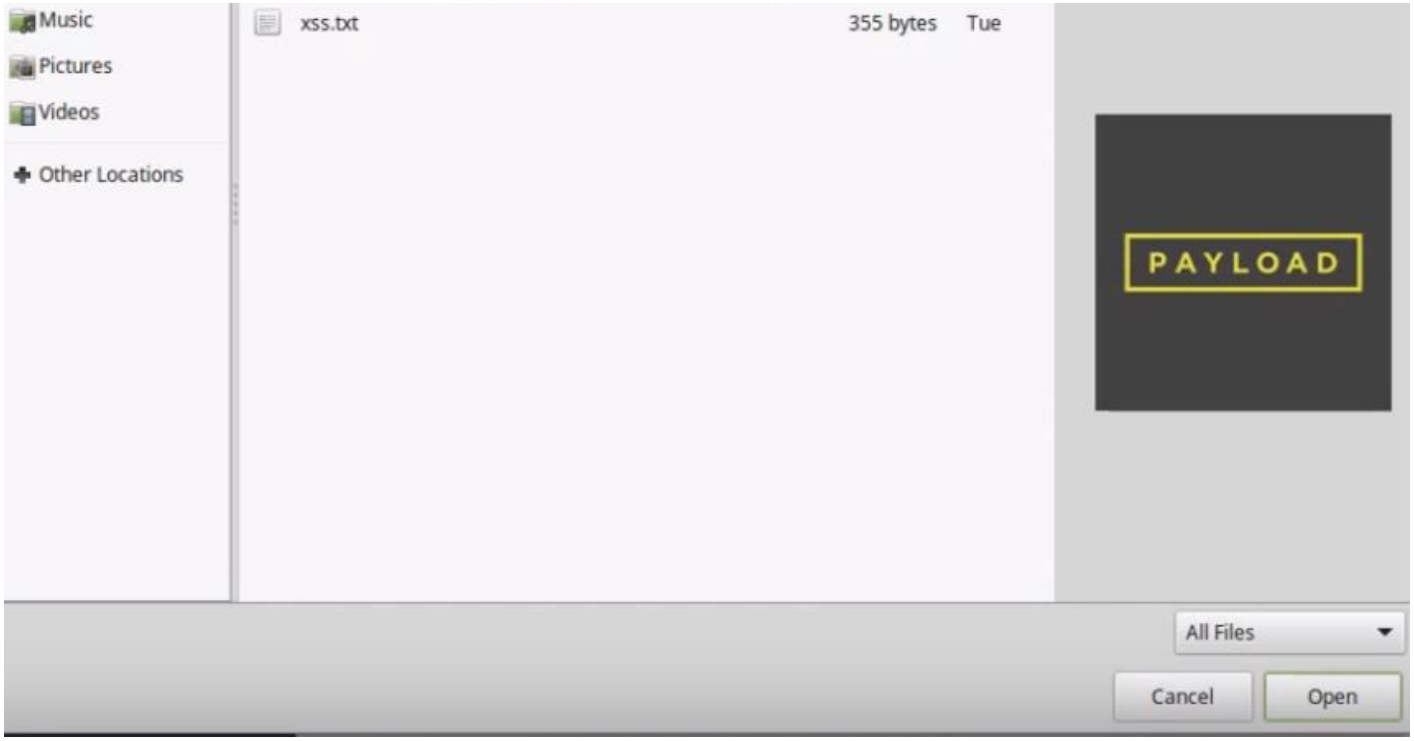
Vulnerable URL: https://www.canva.com/
Vulnerability: File Upload XSS
Severity: High
Owasp rank: (OTG-BUSLOGIC-009)

Below are the steps to reproduce the XSS vulnerability

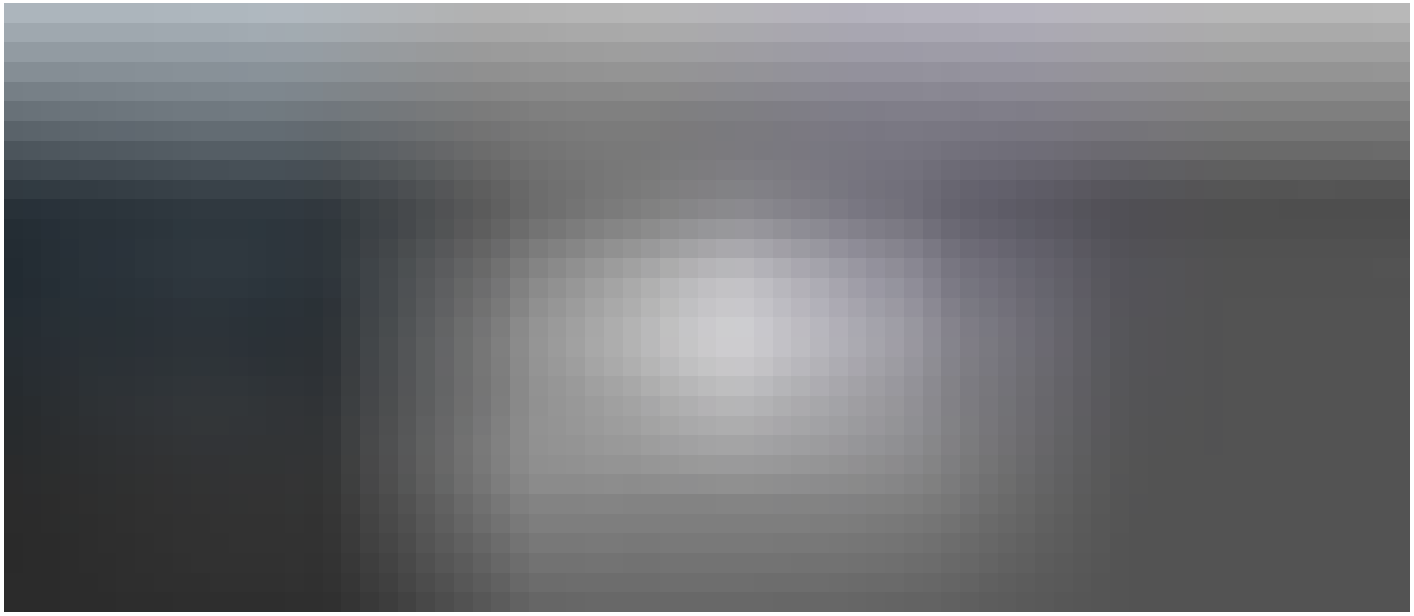
Pick any image and name it as **"><img src=x onerror=prompt(document.domain)>** to make the XSS payload.

(Only for Linux)



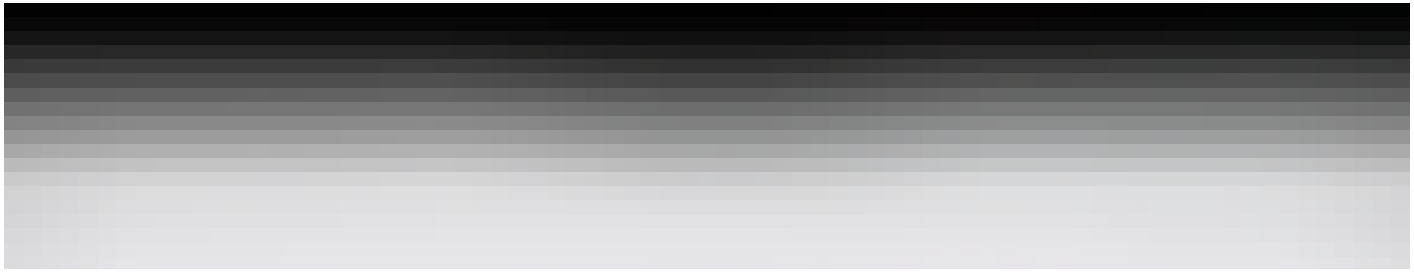


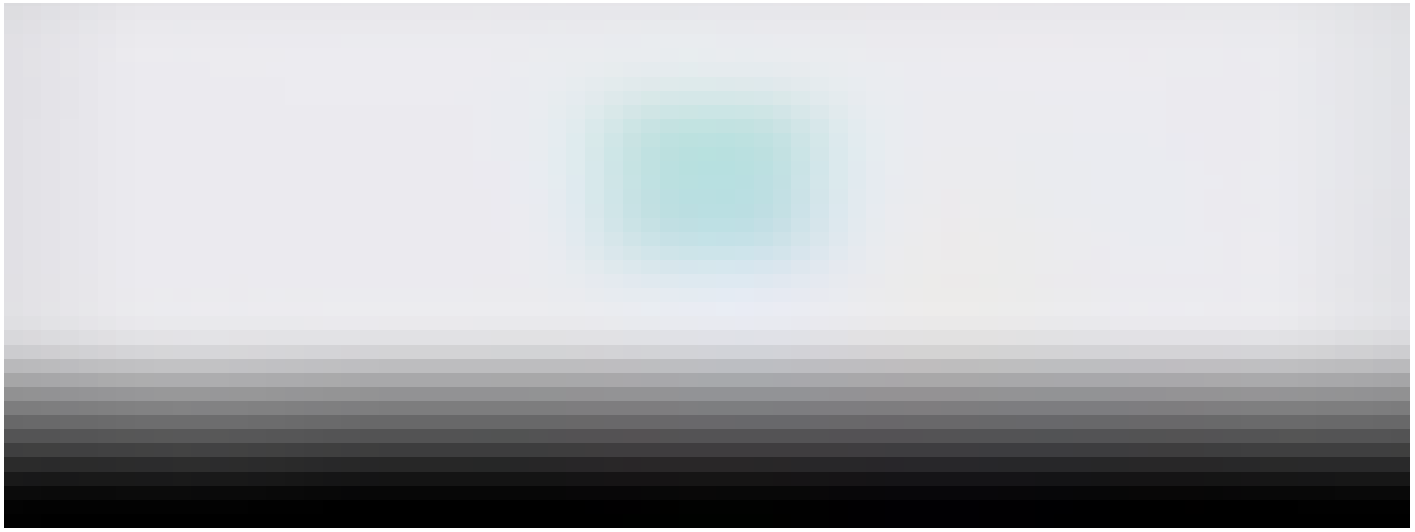
1. Go to https://www.canva.com and complete the registration and login process.
2. Select ‘Create new design’ and choose any option like ‘Logo’ or ‘photo collage’
3. Go to **‘Uploads’** option and click on ‘**Upload your own image**’
4. Upload the the image we’ve created in the first step and you’ll get the prompt box with domain name.



For remediation restrict file types accepted for upload: check the file extension and only allow certain files to be uploaded. Check for **double extensions** such as .php.png. If possible, rename the files that are uploaded.

Below is the video PoC that will give you more idea.





The consequences of unrestricted file upload can vary, including complete system takeover.

Have a happy cross site scripting 😄

Xss | Penetration Testing | File Upload | Vulnerables

78 claps

More from InfoSec Write-ups

More from InfoSec Write-ups

More from InfoSec Write-ups

Writing a Password Protected Bind

0x0FFB347
Mar 8 · 5 min read

245

Ping Power—ICMP Tunnel

Nir Chako
Dec 17, 2018 · 8 min re

487

How to Make a Captive Portal of

Trevor Phillips
Dec 18, 2018 · 6 min re

273

Responses

Write a response...

Conversation with Vulnerables.

Vijay Chauhan
Apr 23, 2018

SELF

1

1 response

Vulnerables
Apr 24, 2018

Vijay Chauhan It is saved (Stored), Anyway the vulnerability has been patched.