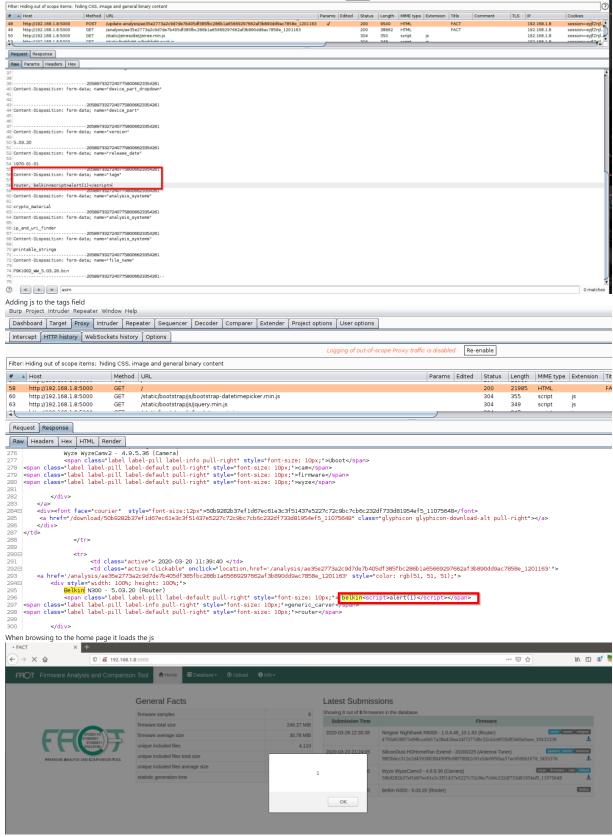
Jump to bottom New issue

Stored XSS when updating analysis details #375

⊙ Closed lum8rjack opened this issue on Mar 29, 2020 · 3 comments

lum8rjack commented on Mar 29, 2020

The application does not sanitize the user input when updating the details of a firmware. When updating the firmware details, the applications posts the data to the "upload-analysis/[uid]" page. $That page then runs the function "_get_meta_from_request()" within the \textit{/src/helperFunctions/mongo_task_conversion.py} script. I tested the "tags" and "version" fields by adding JavaScript to the "tags" and "version" fields by adding the "tags" fields$ updated fields (it looks like other fields are possibly vulnerable too). This data is not sanitized and is stored in the application. Each time a page is requested with this information, the JavaScript is ran. I added some screenshots to help. Using the "escape" function within flask could be a solution to sanitize the input. I tested it against the version field and it worked. Let me know if there are any additional questions.



js is executed

```
iot@ubuntu16: ~/FACT_core/src/helperFunctions
              logging
tmport togging
import os
import re
import sys
from tempfile import TemporaryDirectory
 from flask import escape
from helperFunctions.uid import create_uid
from objects.firmware import Firmware
OPTIONAL_FIELDS = ['tags', 'device_part']
DROPDOWN_FIELDS = ['device_class', 'vendor', 'device_name', 'device_part']
 def create_analysis_task(request):
       create_analysis_task(request):
    task = _get_meta_from_request(request)
    if request.ftles['ftle']:
        task['file_name'], task['binary'] = get_file_name_and_binary_from_request(request)
    task['iuid'] = get_uid_of_analysis_task(task)
    if task['release_date'] == '':
        # set_default_value_if_date_field_is_empty
        task['release_date'] = '1970-01-01'
        return_task
        return task
def get_file_name_and_binary_from_request(request): # pylint: disable=invalid-name
    try:
        file_name = request.files['file'].filename
    except Exception:
        file_name = 'no name'
    file_binary = get_uploaded_file_binary(request.files['file'])
    return file_name, file_binary
def create_re_analyze_task(request, uid):
    task = _get_meta_from_request(request)
    task['uid'] = uid
    if not task['release_date']:
        task['release_date'] = '1970-01-01'
    return task
def _get_meta_from_request(request):
    meta = {
        'device_name': request.form['device_name'],
        'device_part': request.form['device_part'],
        'device_class': request.form['device_class'],
        'vendor': request.form['vendor'].
                #ADDED escape function
                  'version': escape(request.form['version']),
Used the escape function to sanitize the input
      FHOF Firmware Analysis and Comparison Tool
                                                                                                                            ■ Database ▼
                                                                                                                                                        ① Upload

♠ Home

⊕ Info 
▼
```

Analysis for Belkin N300 v. 5.03.20<script>alert(1)</script>

UID: ae35e2773a2c9d7de7b405df385fbc286b1a65669297662af3b890dd9ac7858e 1201163

General	
device name	N300
vendor	Belkin
device class	Router
version	5.03.20 <script>alert(1)</script>
release date	unknown
file name	F9K1002_WW_5.03.20.bin
virtual path	Belkin N300 - 5.03.20 <script>alert(1)</script> (Router)
file size	1.15 MiB (1,201,163 bytes)
Tags	belkin router
file type	data

Analysis Results crypto material file hashes file type ip and uri finder printable strings unpacker O Run additional analysis

File Tree

dorpvom commented on Mar 30, 2020

Collaborator

we actually did not do a great job securing our web application, thus the warning in our readme. That said we're happy to improve security wherever possible. Mostly we simply lack the background in web application design.

Would you like to open a Pull Request on that yourself, since you seem to have a solution already?

Johannes

