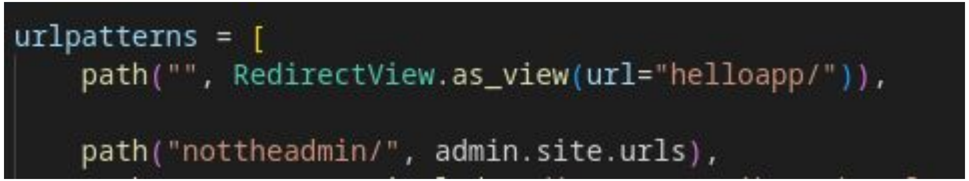
Milestone 7 - Testing

Evan Duffield

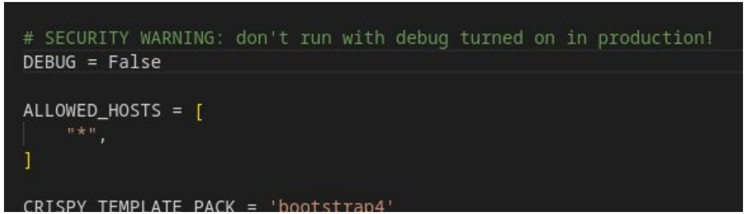
Security Assessment Report

Django configuration:

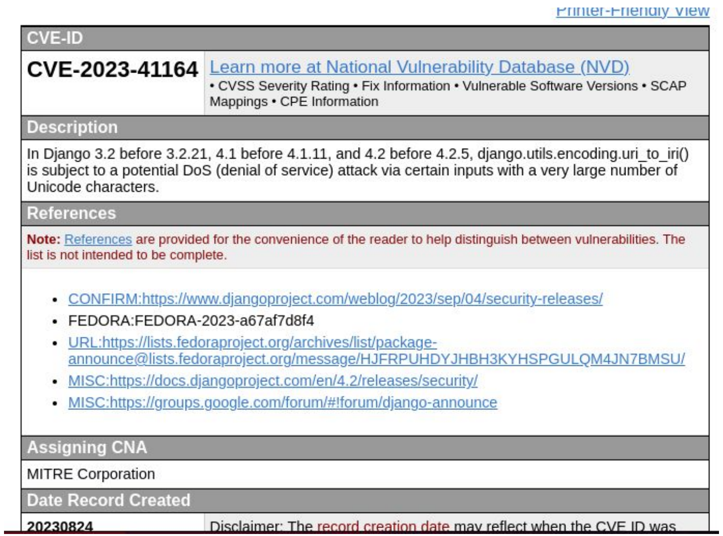
- □ Set DEBUG flag to false.
- □ Update all modules to latest version.
- □ Check modules for CVE vulnerabilities.
- □ Obfuscate /admin/ url path to something hard to guess.



```
urlpatterns = [
    path("", RedirectView.as_view(url="helloapp/")),

    path("nottheadmin/", admin.site.urls),
```



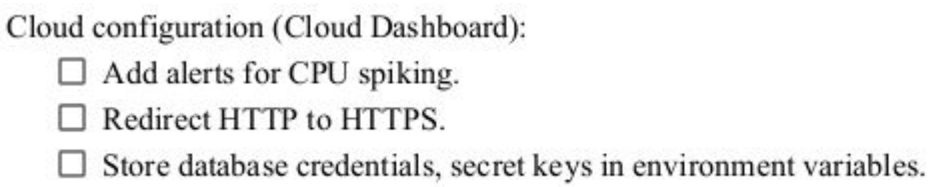
```
# SECURITY WARNING: don't run with debug turned on in production!
DEBUG = False

ALLOWED_HOSTS = [
    "*",
]

CRISPY_TEMPLATE_PACK = 'bootstrap4'
```



Printer-Friendly View

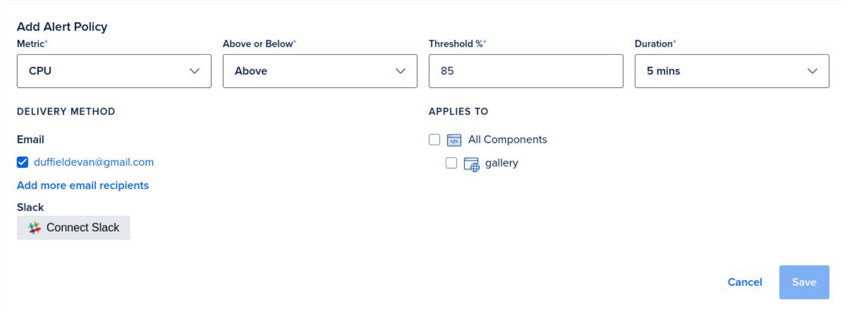
CVE-ID	
CVE-2023-41164	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	
In Django 3.2 before 3.2.21, 4.1 before 4.1.11, and 4.2 before 4.2.5, django.utils.encoding.uri_to_iri() is subject to a potential DoS (denial of service) attack via certain inputs with a very large number of Unicode characters.	
References	
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	
• CONFIRM:https://www.djangoproject.com/weblog/2023/sep/04/security-releases/ • FEDORA:FEDORA-2023-a67af7d8f4 • URL:https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/HJFRPUHDYJHBH3KYHSPGULQM4JN7BMSU/ • MISC:https://docs.djangoproject.com/en/4.2/releases/security/ • MISC:https://groups.google.com/forum/#!forum/django-announce	
Assigning CNA	
MITRE Corporation	
Date Record Created	
20230824	Disclaimer: The record creation date may reflect when the CVE ID was

Security Assessment Report



Cloud configuration (Cloud Dashboard):

- □ Add alerts for CPU spiking.
- □ Redirect HTTP to HTTPS.
- □ Store database credentials, secret keys in environment variables.



Add Alert Policy

Metric*	Above or Below*	Threshold %*	Duration*
CPU	Above	85	5 mins

DELIVERY METHOD

Email

☑ duffieldevan@gmail.com

Add more email recipients

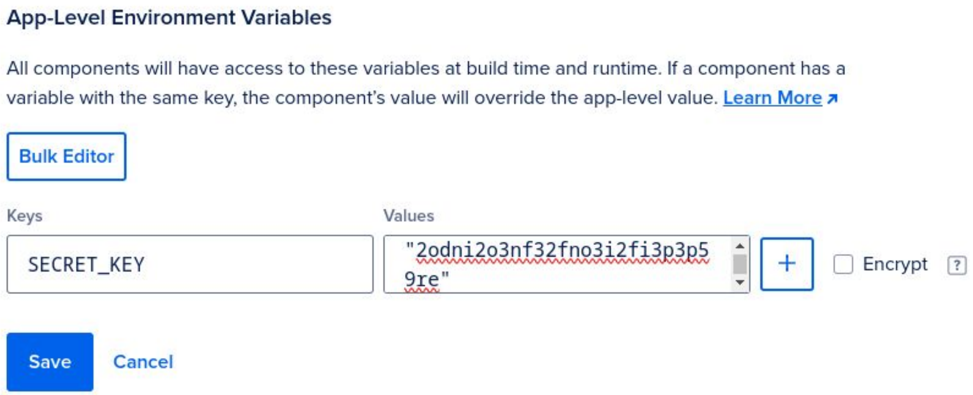
Slack

Connect Slack

APPLIES TO

□ All Components

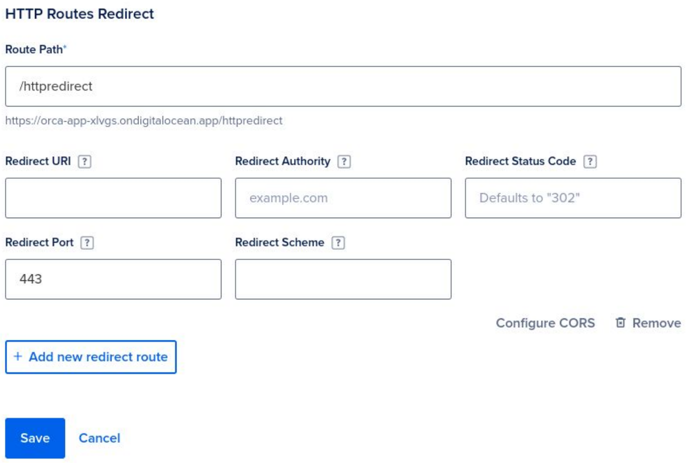
□ gallery



App-Level Environment Variables

All components will have access to these variables at build time and runtime. If a component has a variable with the same key, the component's value will override the app-level value. Learn More ↗

Keys	Values		
SECRET_KEY	"2odni2o3nf32fno3i2fi3p3p5 9re"	+	□ Encrypt ?



HTTP Routes Redirect

Route Path*: /httpredirect

https://orca-app-xlvgs.ondigitalocean.app/httpredirect

Redirect URI ?:

Redirect Authority ?: example.com

Redirect Status Code ?: Defaults to "302"

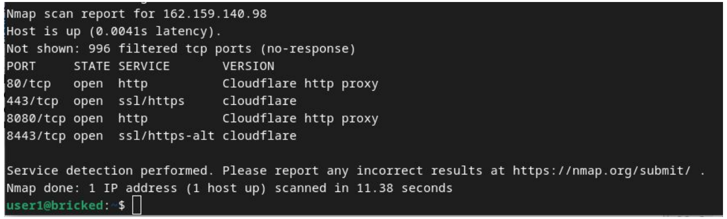
Redirect Port ?: 443

Redirect Scheme ?:

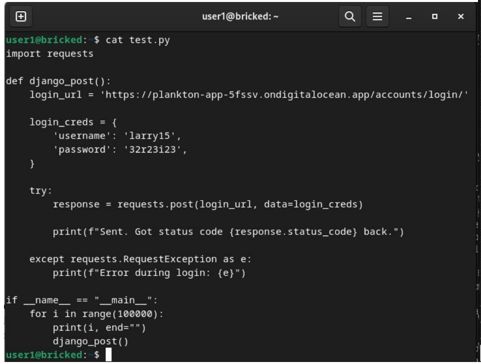
Security Assessment Report

Testing with tools:

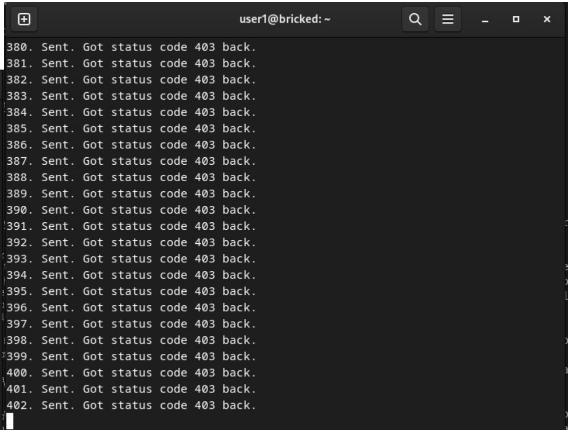
- □ Port scan the website to assure only HTTPS is open.
- □ Test for SQL injections with sqlmap.
- □ Brute force password on login (Should trigger CPU alert).



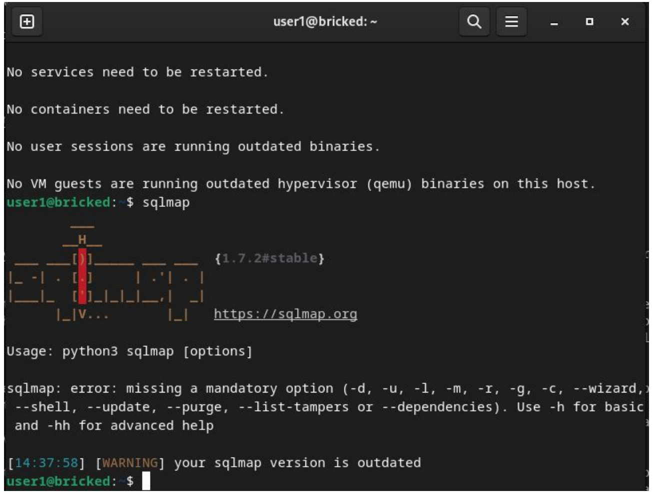
```
Nmap scan report for 162.159.140.98
Host is up (0.0041s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Cloudflare http proxy
443/tcp  open  ssl/https     cloudflare
8080/tcp open  http          Cloudflare http proxy
8443/tcp open  ssl/https-alt cloudflare

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.38 seconds
user1@bricked:~$
```



```
user1@bricked:~$ cat test.py
import requests

def django_post():
    login_url = 'https://plankton-app-5fssv.ondigitalocean.app/accounts/login/'

    login_creds = {
        'username': 'larry15',
        'password': '32r23i23',
    }

    try:
        response = requests.post(login_url, data=login_creds)

        print(f"Sent. Got status code {response.status_code} back.")

    except requests.RequestException as e:
        print(f"Error during login: {e}")

if __name__ == "__main__":
    for i in range(100000):
        print(i, end="")
        django_post()
user1@bricked:~$
```

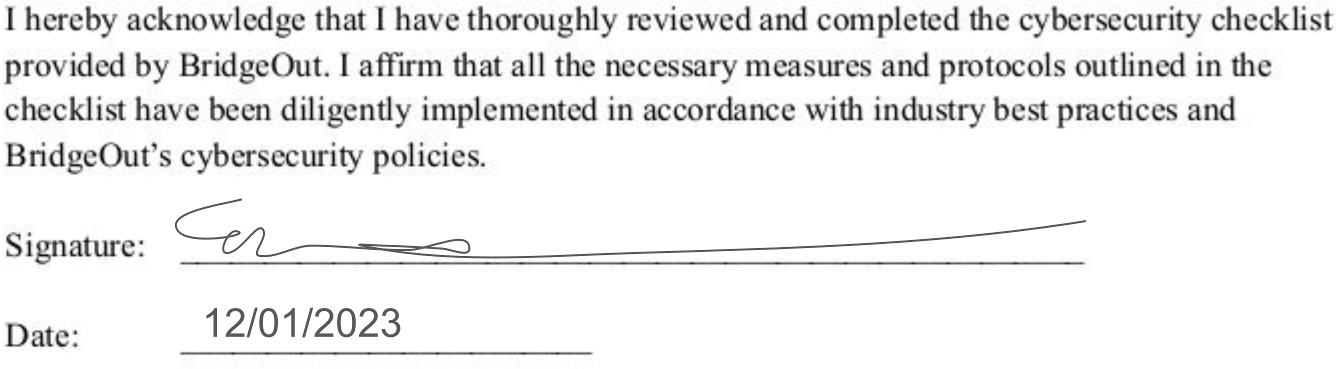


```
380. Sent. Got status code 403 back.
381. Sent. Got status code 403 back.
382. Sent. Got status code 403 back.
383. Sent. Got status code 403 back.
384. Sent. Got status code 403 back.
385. Sent. Got status code 403 back.
386. Sent. Got status code 403 back.
387. Sent. Got status code 403 back.
388. Sent. Got status code 403 back.
389. Sent. Got status code 403 back.
390. Sent. Got status code 403 back.
391. Sent. Got status code 403 back.
392. Sent. Got status code 403 back.
393. Sent. Got status code 403 back.
394. Sent. Got status code 403 back.
395. Sent. Got status code 403 back.
396. Sent. Got status code 403 back.
397. Sent. Got status code 403 back.
398. Sent. Got status code 403 back.
399. Sent. Got status code 403 back.
400. Sent. Got status code 403 back.
401. Sent. Got status code 403 back.
402. Sent. Got status code 403 back.
```



```
No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
user1@bricked:~$ sqlmap
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.7.2#stable}
|_ -| . [.]     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

Usage: python3 sqlmap [options]

sqlmap: error: missing a mandatory option (-d, -u, -l, -m, -r, -g, -c, --wizard,
 --shell, --update, --purge, --list-tampers or --dependencies). Use -h for basic
 and -hh for advanced help

[14:37:58] [WARNING] your sqlmap version is outdated
user1@bricked:~$
```

Security Assessment Report



I hereby acknowledge that I have thoroughly reviewed and completed the cybersecurity checklist provided by BridgeOut. I affirm that all the necessary measures and protocols outlined in the checklist have been diligently implemented in accordance with industry best practices and BridgeOut's cybersecurity policies.

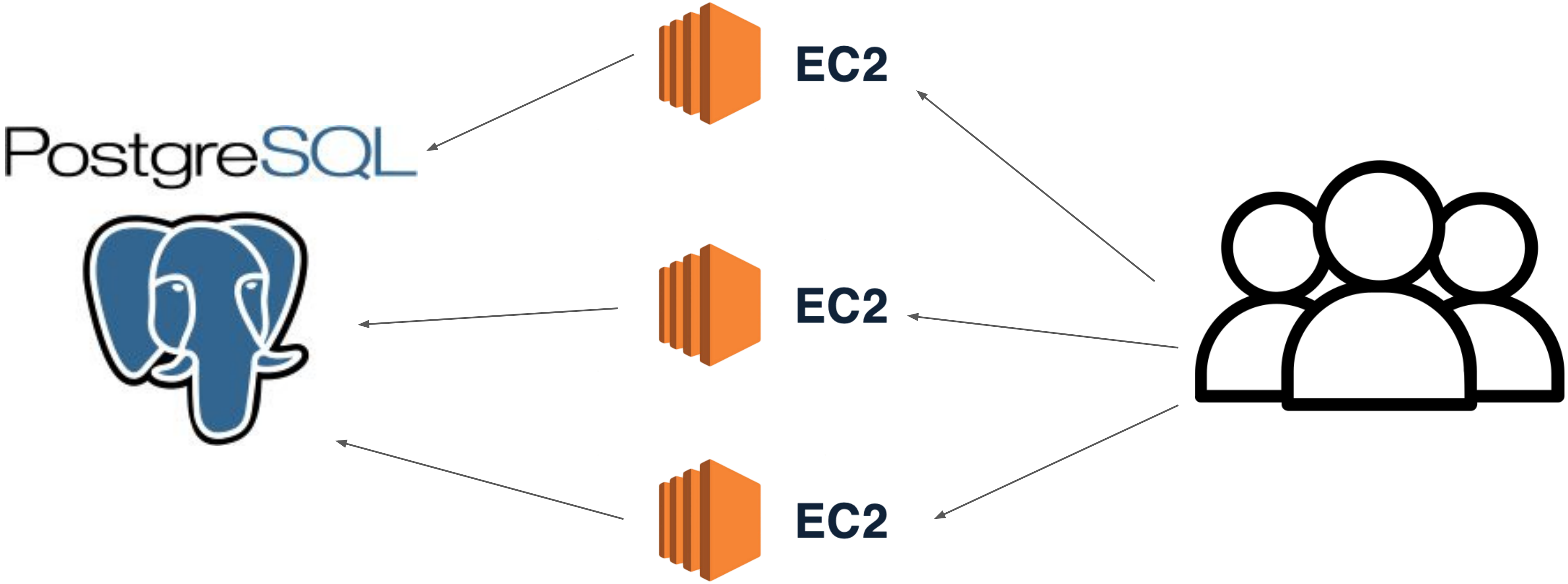
Signature: ______________________________

Date: 12/01/2023

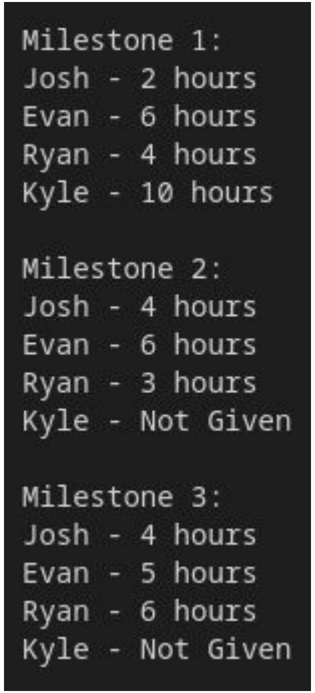
Scaling Recommendation for Future

Scenario: We have a single small instance hosting the django application, which routes to a postgresql server. This is an affordable setup that works for 90% of our runtime, however on weekdays we have an influx of businessmen looking for new jobs on the clock.

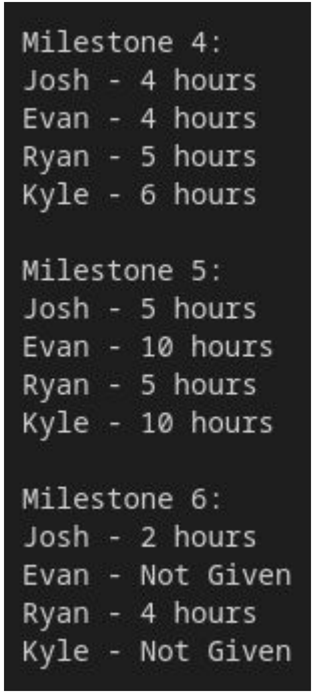
Scaling Recommendation for Future/Data Management



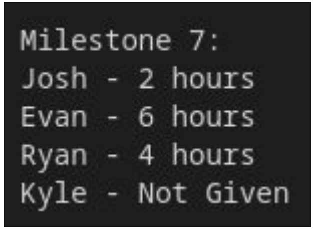
Engineering Investment Summary



```
Milestone 1:
Josh - 2 hours
Evan - 6 hours
Ryan - 4 hours
Kyle - 10 hours

Milestone 2:
Josh - 4 hours
Evan - 6 hours
Ryan - 3 hours
Kyle - Not Given

Milestone 3:
Josh - 4 hours
Evan - 5 hours
Ryan - 6 hours
Kyle - Not Given
```



```
Milestone 4:
Josh - 4 hours
Evan - 4 hours
Ryan - 5 hours
Kyle - 6 hours

Milestone 5:
Josh - 5 hours
Evan - 10 hours
Ryan - 5 hours
Kyle - 10 hours

Milestone 6:
Josh - 2 hours
Evan - Not Given
Ryan - 4 hours
Kyle - Not Given
```



```
Milestone 7:
Josh - 2 hours
Evan - 6 hours
Ryan - 4 hours
Kyle - Not Given
```

Engineering Investment Summary

Average hours per milestone: 18.7 hours

Average hours done per person each milestone: 4.67 hours

Total time: 130.9 hours

Estimated cost ($20/hr per engineer): $2618

AI Prompts

- Write a sign-off agreement statement for the bottom of a cybersecurity checklist that an engineer must sign
- What are some ways I can secure my digitalocean django app in the dashboard?
- What are some ways I can configure my django project to be more secure?
- What are some ways I can penetration test my Django application?
- Give me an example of a security checklist for securing a django application hosted in the cloud.

Thanks for Watching!