Web Applications and Services Coursework Report

Implementation

Presentation Layer

Templates have been fully implemented and used to accommodate:

- Users viewing all their transactions (activity.html)
- Users making direct payments to other registered users (send.html)
- Users requesting payments from register users (request.html)
- Administrators seeing all user accounts (admin-users.html)
- Administrators seeing all payment transactions (admin-activity.html)
- Administrators registering new administrators (admin-users.html)

The administrator actions can also be accessed via the Django Admin Panel (/admin/).

Business Logic Layer

Views have been fully implemented and used to accommodate:

- Users viewing all their transactions (activity)
- Users making direct payments to other registered users (send_money)
- Users requesting payments from register users (request_money, and acceptable/deniable with request_response)
- Administrators seeing all user accounts (admin_users)
- Administrators seeing all payment transactions (admin_activity)
- Administrators registering new administrators (admin_users)

The administrator actions can also be accessed via the Django Admin Panel (/admin/).

Data Access Layer

SQLite was used as the Relational Database Management System, with three tables:

Person

- user (Django User Model)
- active (Boolean Field representing if a user is active or inactive)
- balance (Money Field representing both the amount and currency of their balance)

Transaction

- from_person (Foreign Key referencing the Person whom the money comes from)
- to_person (Foreign Key referencing the Person whom the money goes to)
- amount (Money Field representing both the amount and currency)
- submission_datetime (DateTime Field representing the time the transaction took place)

Request

- by_person (Foreign Key referencing the Person whom requested the payment)
- to_person (Foreign Key referencing the Person whom the payment was requested from)
- amount (Money Field representing both the amount and currency requested)
- status (Char Field with three choices representing the status of the request: pending, completed, cancelled)

Security Layer

Users must be logged in via the log-in page (/login/) to interact with the system (every user-facing view has an @login_required decorator).

Users cannot see other users' information or functionality for administrators as users are only ever shown information and functionality tied to their personal Person and User objects.

Administrators can access their own set of pages which have access to all users' information, as these pages are locked behind the 'admin_area' method which checks if a user is marked as both superusers and staff, and redirects them back to the homepage if not.

Users and administrators can log out of the web application via the navbar, or be automatically logged out after 10 minutes of inactivity.

The following is implemented and supported:

- Authentication functionality such that users can register, login and logout.
- Access control to restrict access to web pages to non-authorised user as every user-facing view has an @login_required decorator.
- Communication on top of HTTPS for every interaction with users and admins, as the application is only hosted on HTTPS, so cannot be logged into or referenced without the use of HTTPS.
- General Web Vulnerabilities:
    - Cross-site scripting (XSS) is addressed as only cleaned data is used from forms, and by default in Django as the templating system escapes non-html characters by default.
    - Cross-site request forgery (CSRF) is addressed by CSRF tokens being added to every form (via '@requires_csrf_token' decorator on methods, and '{% csrf_token %}'s in templates), as well as avoiding form resubmission by redirecting users after submitting every form (returning 'redirect('home')).
    - SQL Injection is addressed by only using cleaned inputs and only using directly user inputted text for registration.
    - Clickjacking is addressed by using the 'XFrameOptionsMiddleware' which denies any website trying to put this site in a frame, even if it's from the same site (though this can be changed if same-origin frames are deemed useful in the future).

An administrator account (username: admin1, password: admin1) is present, and only administrators can register more administrators through the restricted admin page '/admin-users/' or the Django Admin Panel.

Web Services

A RESTful currency conversion service is fully implemented at the base url plus '/conversion/<currency1>/<currency2>/<amount_of_currency1>' which returns both the rate and a converted decimal value of currency 1 into currency 2.

Though only the decimal value is used as I wasn't sure what was wanted by the assignment specification. This is returned as JSON via a HTTP response, and if an invalid currency is provided, a HTTP 422 Unprocessable Content status code is returned along with a JSON serialised validation error.

RPC

This is partially implemented. A timestamp service in Apache Thrift is written and does work, but isn't linked up to any views. Instead, a timestamping service is run as a RESTful API endpoint at the base url plus '/timestamp/'.

Cloud

The project is deployed on an Amazon Web Services EC2 virtual machine.

The following commands were used to run this Django web application:

ssh -i "web-apps-project-key.pem" ubuntu@ec2-44-202-13-88.compute-1.amazonaws.com

```
PS C:\Users\danba\OneDrive - University of Sussex\Module Files\Web Applications and Services> ssh -i "web-apps-project-key.pem" ubuntu@ec2-3-86-235-114.compute-1.amazonaws.com
The authenticity of host 'ec2-3-86-235-114.compute-1.amazonaws.com (3.86.235.114)' can't be established.
ED25519 key fingerprint is SHA256:YFveMz/nBP5awXGv4yLJRkekdRgxt7j02euOZ1n0SrY.
This host key is known by the following other names/addresses:
    C:\Users\danba/.ssh/known_hosts:10: ec2-44-212-65-127.compute-1.amazonaws.com
    C:\Users\danba/.ssh/known_hosts:13: ec2-18-205-116-238.compute-1.amazonaws.com
    C:\Users\danba/.ssh/known_hosts:14: ec2-44-202-13-88.compute-1.amazonaws.com
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-3-86-235-114.compute-1.amazonaws.com' (ED25519) to the list of known hosts.
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-1048-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Fri Apr 19 10:00:36 UTC 2024

  System load:  0.04              Processes:             101
  Usage of /:   30.1% of 7.57GB   Users logged in:       0
  Memory usage: 18%               IPv4 address for eth0: 172.31.81.231
  Swap usage:   0%


Expanded Security Maintenance for Applications is not enabled.

110 updates can be applied immediately.
77 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

New release '22.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


Last login: Fri Apr 19 09:50:44 2024 from 139.184.223.197
ubuntu@ip-172-31-81-231:~$
```

git clone https://github.com/danbates1452/webapps2024.git

```
ubuntu@ip-172-31-81-231:~$ git clone https://github.com/danbates1452/webapps2024.git
Cloning into 'webapps2024'...
remote: Enumerating objects: 573, done.
remote: Counting objects: 100% (68/68), done.
remote: Compressing objects: 100% (46/46), done.
remote: Total 573 (delta 31), reused 43 (delta 19), pack-reused 505
Receiving objects: 100% (573/573), 1.47 MiB | 18.81 MiB/s, done.
Resolving deltas: 100% (332/332), done.
ubuntu@ip-172-31-81-231:~$
```

cd webapps2024

```
ubuntu@ip-172-31-81-231:~$ cd webapps2024
ubuntu@ip-172-31-81-231:~/webapps2024$
```

sudo apt update

```
ubuntu@ip-172-31-81-231:~/webapps2024$ sudo apt update
Hit:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu focal InRelease
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu focal-updates InRelease [114 kB]
Hit:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu focal-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu focal-security InRelease
Fetched 114 kB in 5s (22.9 kB/s)
Reading package lists... Done
Building dependency tree
Reading state information... Done
104 packages can be upgraded. Run 'apt list --upgradable' to see them.
ubuntu@ip-172-31-81-231:~/webapps2024$
```

sudo apt install python3-pip

```
ubuntu@ip-172-31-81-231:~/webapps2024$ sudo apt install python3-pip
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  python3-pip
0 upgraded, 1 newly installed, 0 to remove and 104 not upgraded.
Need to get 231 kB of archives.
After this operation, 1050 kB of additional disk space will be used.
Get:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu focal-updates/universe amd64 python3-pip all 20.0.2-5ubuntu1.10 [231 kB]
Fetched 231 kB in 0s (9227 kB/s)
Selecting previously unselected package python3-pip.
(Reading database ... 67910 files and directories currently installed.)
Preparing to unpack .../python3-pip_20.0.2-5ubuntu1.10_all.deb ...
Unpacking python3-pip (20.0.2-5ubuntu1.10) ...
Setting up python3-pip (20.0.2-5ubuntu1.10) ...
Processing triggers for man-db (2.9.1-1) ...
ubuntu@ip-172-31-81-231:~/webapps2024$
```

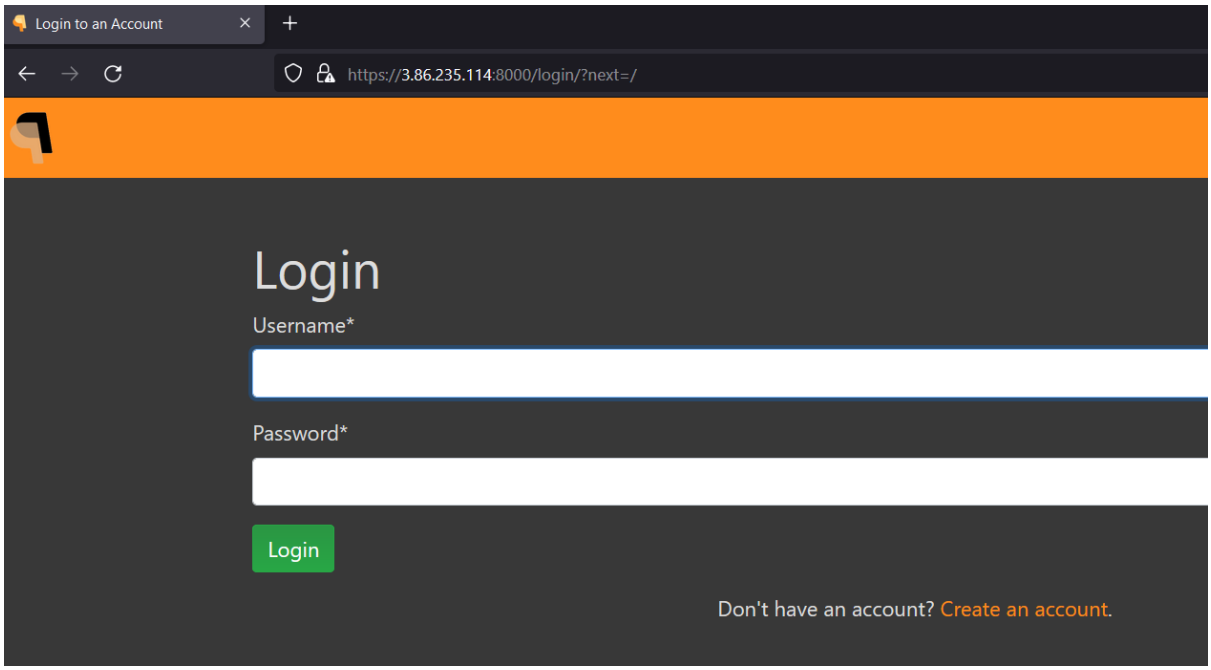
pip install -r ./requirements.txt

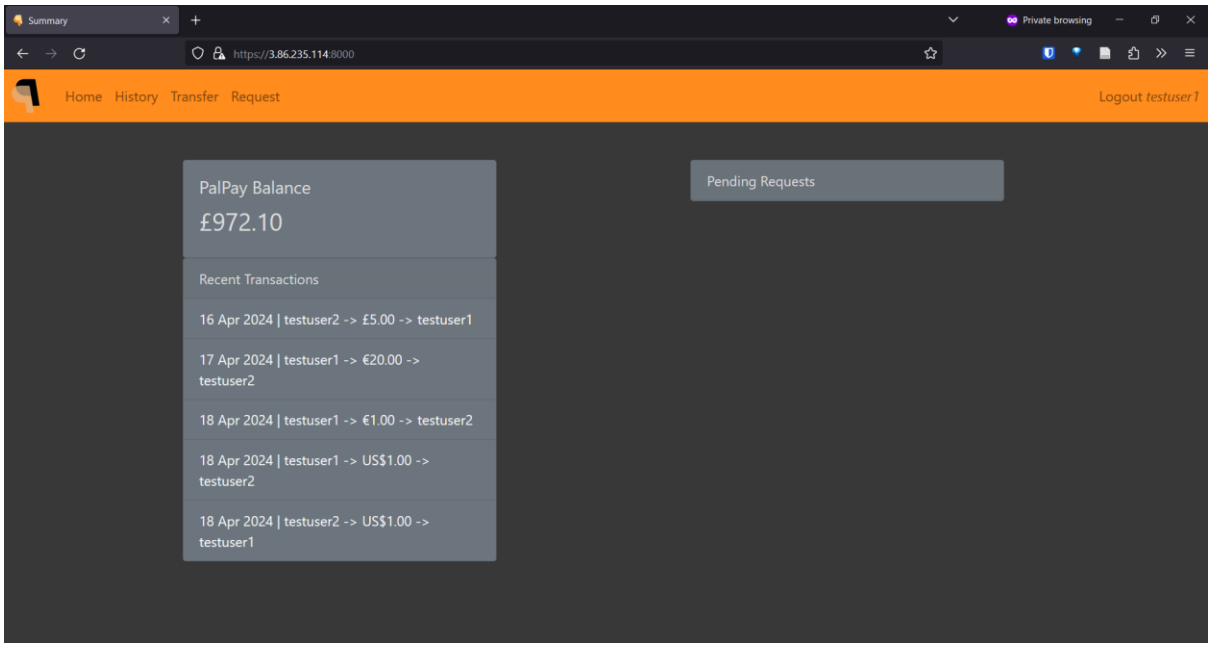
```
ubuntu@ip-172-31-81-231:~/webapps2024$ pip install -r ./requirements.txt
Requirement already satisfied: crispy-bootstrap5==2024.2 in /home/ubuntu/.local/lib/python3.8/site-packages (from -r ./requirements.txt (line 1)) (2024.2)
Requirement already satisfied: Django==4.2.11 in /home/ubuntu/.local/lib/python3.8/site-packages (from -r ./requirements.txt (line 2)) (4.2.11)
Requirement already satisfied: django-appconf==1.0.6 in /home/ubuntu/.local/lib/python3.8/site-packages (from -r ./requirements.txt (line 3)) (1.0.6)
Requirement already satisfied: django-bootstrap-customizer==0.2.0 in /home/ubuntu/.local/lib/python3.8/site-packages (from -r ./requirements.txt (line 4)) (0.2.0)
Requirement already satisfied: django-crispy-forms==2.1 in /home/ubuntu/.local/lib/python3.8/site-packages (from -r ./requirements.txt (line 5)) (2.1)
Requirement already satisfied: django-extensions==3.2.3 in /home/ubuntu/.local/lib/python3.8/site-packages (from -r ./requirements.txt (line 6)) (3.2.3)
Requirement already satisfied: django-money==3.4.1 in /home/ubuntu/.local/lib/python3.8/site-packages (from -r ./requirements.txt (line 7)) (3.4.1)
Requirement already satisfied: djangorestframework==3.15.1 in /home/ubuntu/.local/lib/python3.8/site-packages (from -r ./requirements.txt (line 8)) (3.15.1)
Requirement already satisfied: pyOpenSSL==24.1.0 in /home/ubuntu/.local/lib/python3.8/site-packages (from -r ./requirements.txt (line 9)) (24.1.0)
Requirement already satisfied: requests==2.31.0 in /home/ubuntu/.local/lib/python3.8/site-packages (from -r ./requirements.txt (line 10)) (2.31.0)
Requirement already satisfied: Werkzeug==3.0.2 in /home/ubuntu/.local/lib/python3.8/site-packages (from -r ./requirements.txt (line 11)) (3.0.2)
Requirement already satisfied: backports.zoneinfo; python_version < "3.9" in /home/ubuntu/.local/lib/python3.8/site-packages (from Django==4.2.11->-r ./requirements.txt (line 2)) (0.2.1)
Requirement already satisfied: asgiref<4,>=3.6.0 in /home/ubuntu/.local/lib/python3.8/site-packages (from Django==4.2.11->-r ./requirements.txt (line 2)) (3.8.1)
Requirement already satisfied: sqlparse>=0.3.1 in /home/ubuntu/.local/lib/python3.8/site-packages (from Django==4.2.11->-r ./requirements.txt (line 2)) (0.5.0)
Requirement already satisfied: django-colorful>=1.3 in /home/ubuntu/.local/lib/python3.8/site-packages (from django-bootstrap-customizer==0.2.0->-r ./requirements.txt (line 4)) (1.3)
Requirement already satisfied: libsass>=0.14.5 in /home/ubuntu/.local/lib/python3.8/site-packages (from django-bootstrap-customizer==0.2.0->-r ./requirements.txt (line 4)) (0.23.0)
Requirement already satisfied: cssutils>=1.0.2 in /home/ubuntu/.local/lib/python3.8/site-packages (from django-bootstrap-customizer==0.2.0->-r ./requirements.txt (line 4)) (2.10.2)
Requirement already satisfied: setuptools in /usr/lib/python3/dist-packages (from django-money==3.4.1->-r ./requirements.txt (line 7)) (45.2.0)
Requirement already satisfied: py-moneyed<3.1,>=2.0 in /home/ubuntu/.local/lib/python3.8/site-packages (from django-money==3.4.1->-r ./requirements.txt (line 7)) (3.0)
Requirement already satisfied: cryptography<43,>=41.0.5 in /home/ubuntu/.local/lib/python3.8/site-packages (from pyOpenSSL==24.1.0->-r ./requirements.txt (line 9)) (42.0.5)
Requirement already satisfied: urllib3<3,>=1.21.1 in /usr/lib/python3/dist-packages (from requests==2.31.0->-r ./requirements.txt (line 10)) (1.25.8)
Requirement already satisfied: charset-normalizer<4,>=2 in /home/ubuntu/.local/lib/python3.8/site-packages (from requests==2.31.0->-r ./requirements.txt (line 10)) (3.3.2)
Requirement already satisfied: certifi>=2017.4.17 in /usr/lib/python3/dist-packages (from requests==2.31.0->-r ./requirements.txt (line 10)) (2019.11.28)
Requirement already satisfied: idna<4,>=2.5 in /usr/lib/python3/dist-packages (from requests==2.31.0->-r ./requirements.txt (line 10)) (2.8)
Requirement already satisfied: MarkupSafe>=2.1.1 in /home/ubuntu/.local/lib/python3.8/site-packages (from Werkzeug==3.0.2->-r ./requirements.txt (line 11)) (2.1.5)
Requirement already satisfied: typing-extensions>=4; python_version < "3.11" in /home/ubuntu/.local/lib/python3.8/site-packages (from asgiref<4,>=3.6.0->Django==4.2.11->-r ./requirements.txt (line 2)) (4.11.0
)
Requirement already satisfied: babel>=2.8.0 in /home/ubuntu/.local/lib/python3.8/site-packages (from py-moneyed<3.1,>=2.0->django-money==3.4.1->-r ./requirements.txt (line 7)) (2.14.0)
Requirement already satisfied: cffi>=1.12; platform_python_implementation != "PyPy" in /home/ubuntu/.local/lib/python3.8/site-packages (from cryptography<43,>=41.0.5->pyOpenSSL==24.1.0->-r ./requirements.txt
(line 9)) (1.16.0)
Requirement already satisfied: pytz>=2015.7; python_version < "3.9" in /home/ubuntu/.local/lib/python3.8/site-packages (from babel>=2.8.0->py-moneyed<3.1,>=2.0->django-money==3.4.1->-r ./requirements.txt (lin
e 7)) (2024.1)
Requirement already satisfied: pycparser in /home/ubuntu/.local/lib/python3.8/site-packages (from cffi>=1.12; platform_python_implementation != "PyPy"->cryptography<43,>=41.0.5->pyOpenSSL==24.1.0->-r ./requir
ements.txt (line 9)) (2.22)
ubuntu@ip-172-31-81-231:~/webapps2024$
```

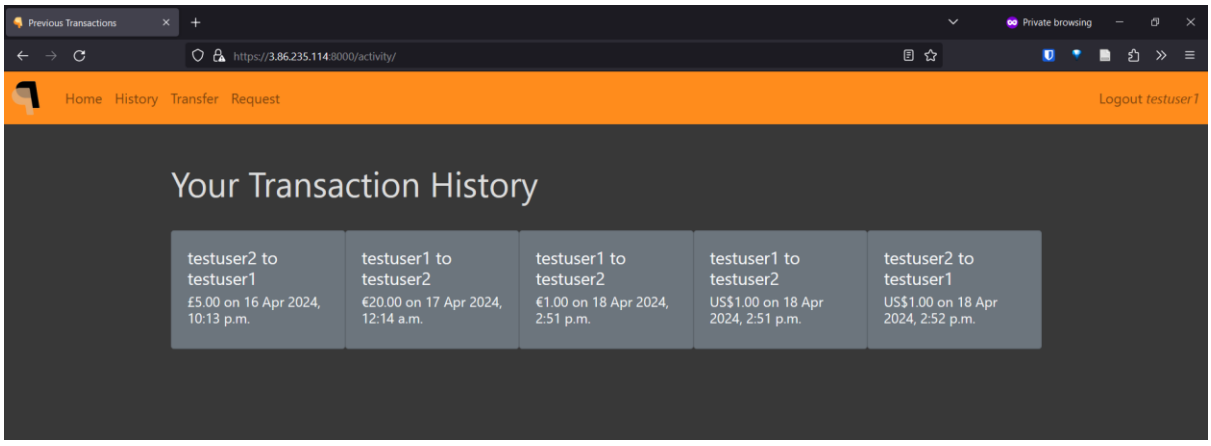
python3 manage.py runserver_plus --cert-file webapps.crt --key-file webapps_decrypted.key

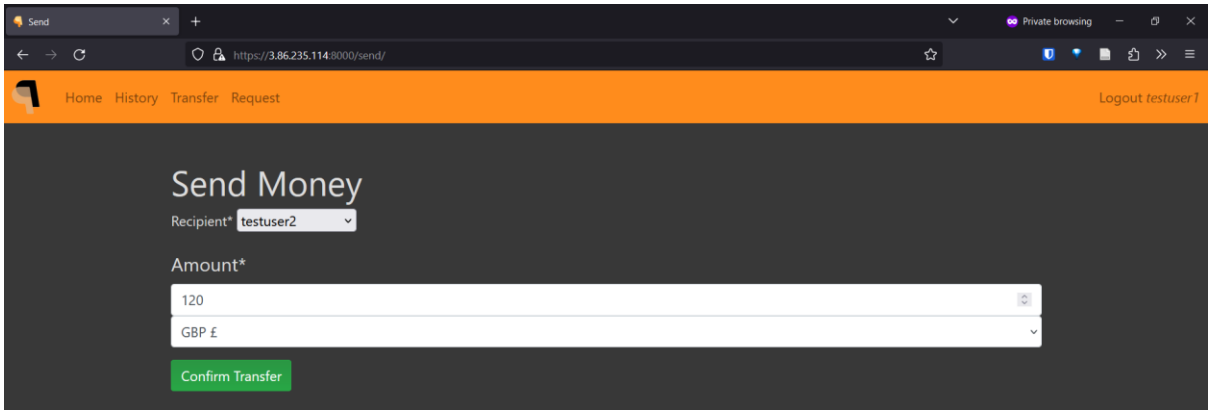
```
ubuntu@ip-172-31-81-231:~/webapps2024$ python3 manage.py runserver_plus --cert-file webapps.crt --key-file webapps_decrypted.key
WARNING: This is a development server. Do not use it in a production deployment. Use a production WSGI server instead.
 * Running on all addresses (0.0.0.0)
 * Running on https://127.0.0.1:8000
 * Running on https://172.31.81.231:8000
Press CTRL+C to quit
 * Restarting with stat
Performing system checks...

System check identified no issues (0 silenced).

Django version 4.2.11, using settings 'webapps2024.settings'
Development server is running at https://0.0.0.0:8000/
Using the Werkzeug debugger (https://werkzeug.palletsprojects.com/)
Quit the server with CONTROL-C.
 * Debugger is active!
 * Debugger PIN: 985-123-710
```

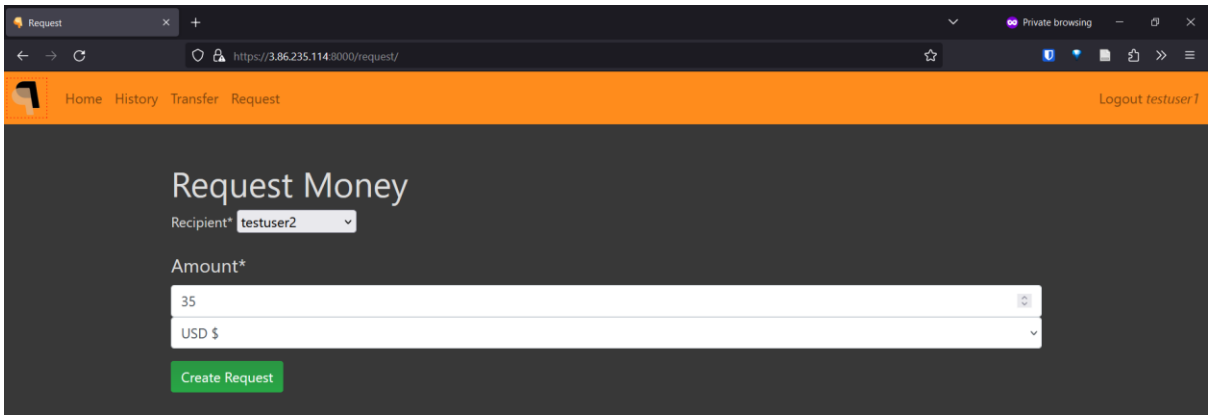
The Django Application running on an AWS-EC2 Instance

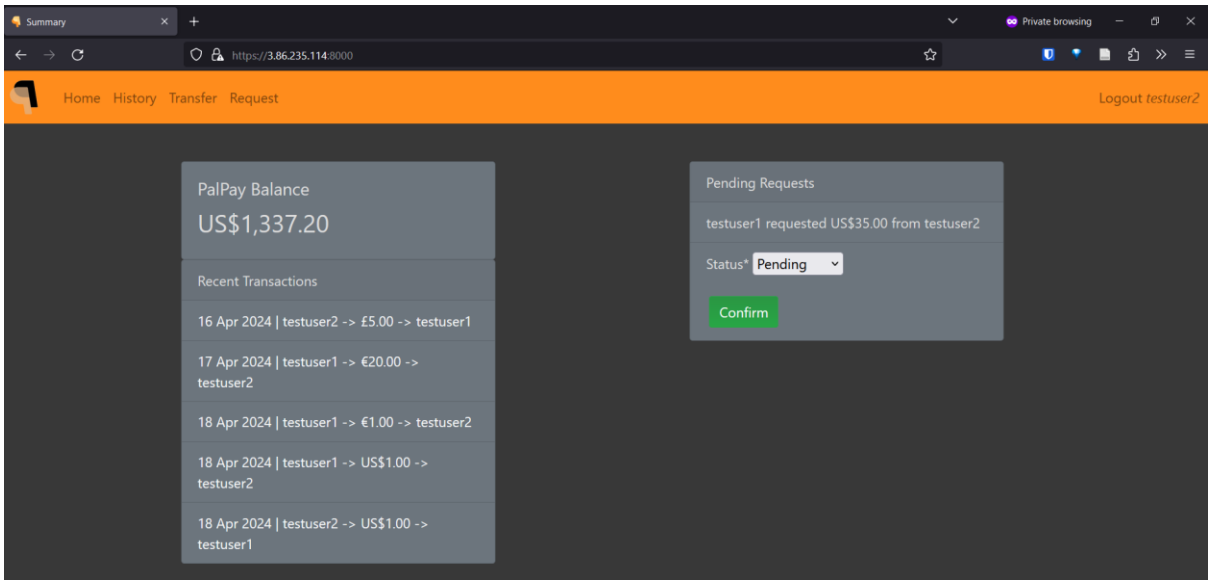


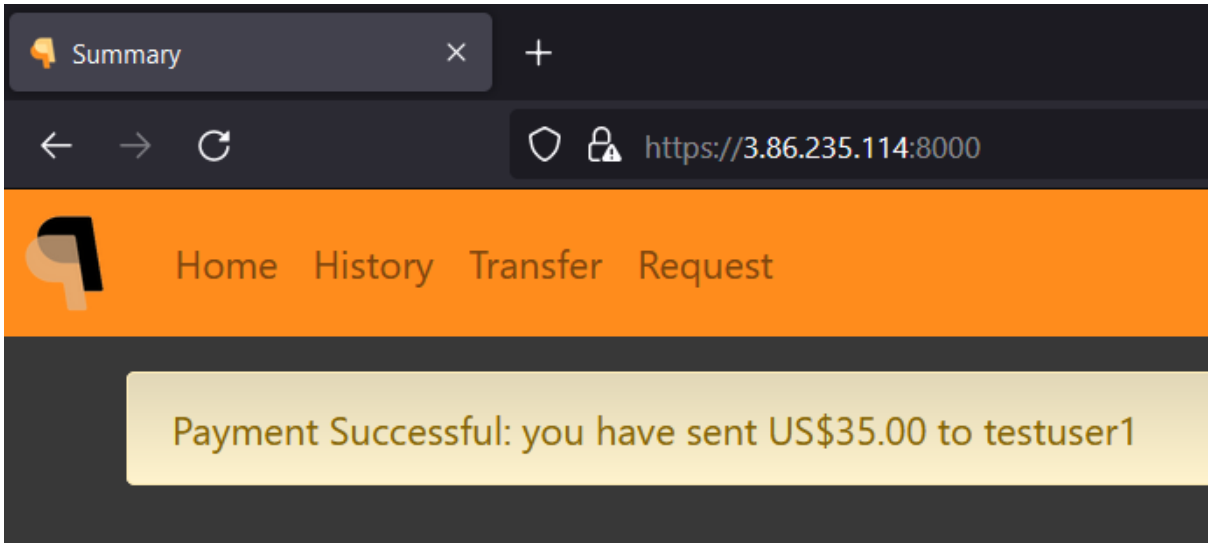


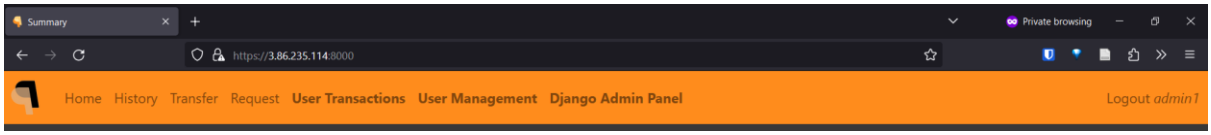


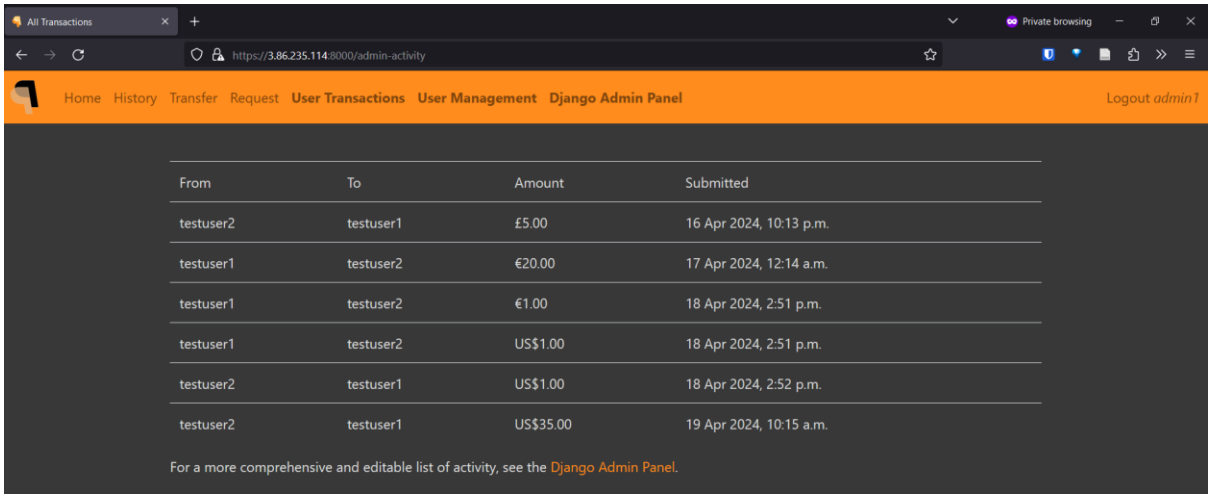

Send
Private browsing
https://3.86.235.114:8000/send/
Home History Transfer Request
Logout testuser1
Send Money
Recipient* testuser2
Amount*
120
GBP £
Confirm Transfer

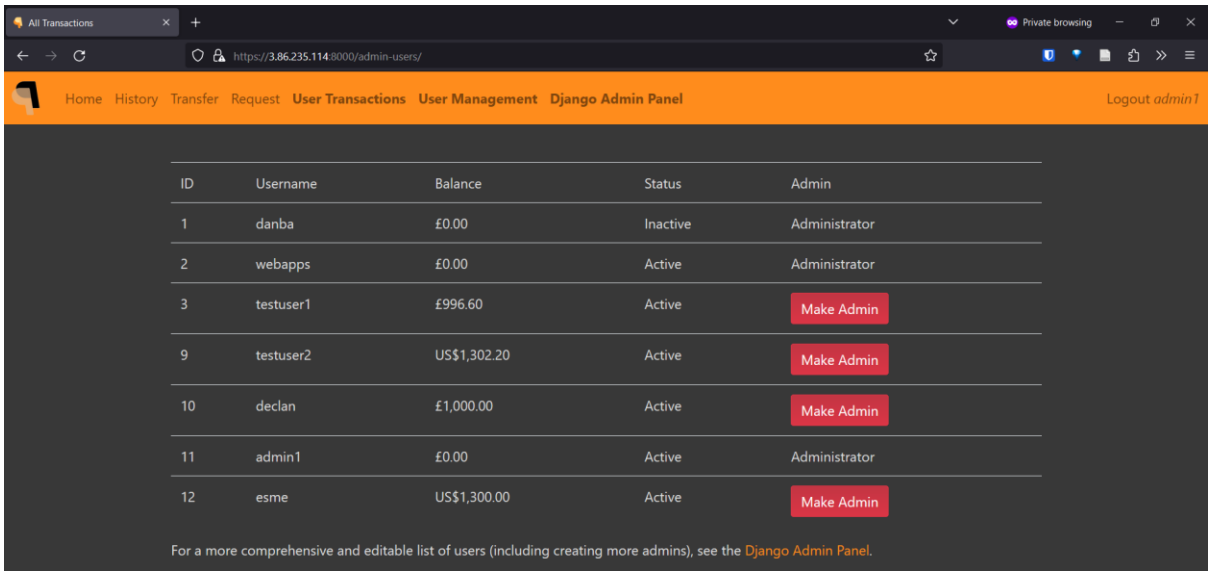

Request
Private browsing
https://3.86.235.114:8000/request/
Home History Transfer Request
Logout testuser1
Request Money
Recipient* testuser2
Amount*
35
USD $
Create Request

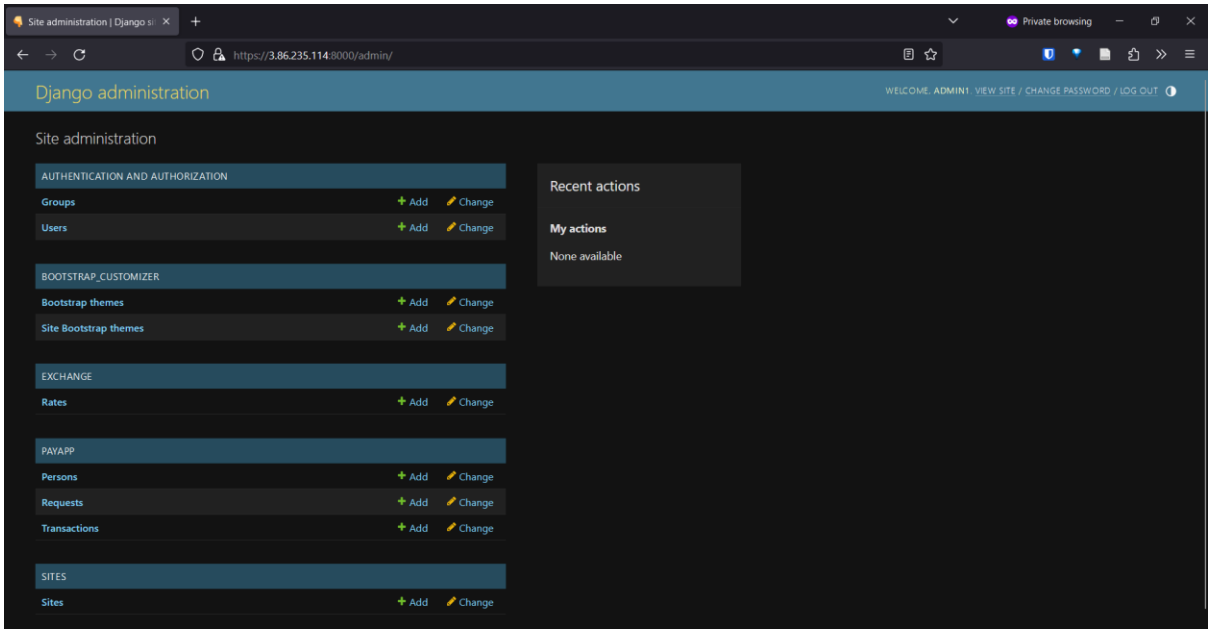

Summary
Private browsing
https://3.86.235.114:8000
Home History Transfer Request
Logout testuser2
PalPay Balance
US$1,337.20
Recent Transactions
16 Apr 2024 | testuser2 -> £5.00 -> testuser1
17 Apr 2024 | testuser1 -> €20.00 -> testuser2
18 Apr 2024 | testuser1 -> €1.00 -> testuser2
18 Apr 2024 | testuser1 -> US$1.00 -> testuser2
18 Apr 2024 | testuser2 -> US$1.00 -> testuser1
Pending Requests
testuser1 requested US$35.00 from testuser2
Status* Pending
Confirm


Summary
https://3.86.235.114:8000
Home History Transfer Request
Payment Successful: you have sent US$35.00 to testuser1


Summary
Private browsing
https://3.86.235.114:8000
Home History Transfer Request User Transactions User Management Django Admin Panel
Logout admin1


All Transactions
Private browsing
https://3.86.235.114:8000/admin-activity
Home History Transfer Request User Transactions User Management Django Admin Panel
Logout admin1
From To Amount Submitted
testuser2 testuser1 £5.00 16 Apr 2024, 10:13 p.m.
testuser1 testuser2 €20.00 17 Apr 2024, 12:14 a.m.
testuser1 testuser2 €1.00 18 Apr 2024, 2:51 p.m.
testuser1 testuser2 US$1.00 18 Apr 2024, 2:51 p.m.
testuser2 testuser1 US$1.00 18 Apr 2024, 2:52 p.m.
testuser2 testuser1 US$35.00 19 Apr 2024, 10:15 a.m.
For a more comprehensive and editable list of activity, see the Django Admin Panel.


All Transactions
Private browsing
https://3.86.235.114:8000/admin-users/
Home History Transfer Request User Transactions User Management Django Admin Panel
Logout admin1
ID Username Balance Status Admin
1 danba £0.00 Inactive Administrator
2 webapps £0.00 Active Administrator
3 testuser1 £996.60 Active Make Admin
9 testuser2 US$1,302.20 Active Make Admin
10 declan £1,000.00 Active Make Admin
11 admin1 £0.00 Active Administrator
12 esme US$1,300.00 Active Make Admin
For a more comprehensive and editable list of users (including creating more admins), see the Django Admin Panel.



Instance details at time of screenshots:

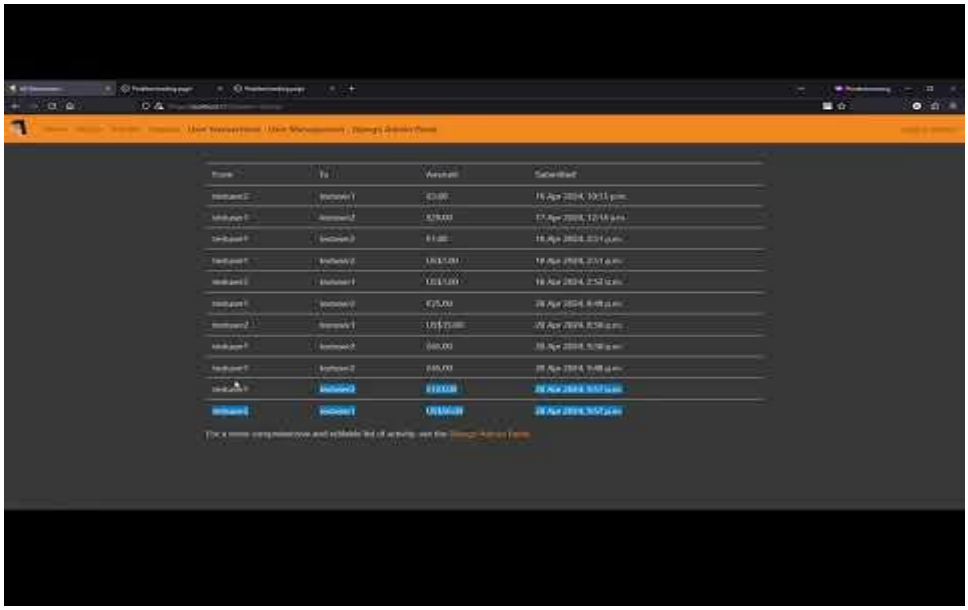
Instance summary for i-0dfbb92d133348695 (web-apps-server) Info

Updated 4 minutes ago

Connect | Instance state | Actions

Instance ID i-0dfbb92d133348695 (web-apps-server)	Public IPv4 address 3.86.235.114 |open address	Private IPv4 addresses 172.31.81.231
IPv6 address –	Instance state Running	Public IPv4 DNS ec2-3-86-235-114.compute-1.amazonaws.com |open address
Hostname type IP name: ip-172-31-81-231.ec2.internal	Private IP DNS name (IPv4 only) ip-172-31-81-231.ec2.internal	
Answer private resource DNS name IPv4 (A)	Instance type t2.micro	Elastic IP addresses –
Auto-assigned IP address 3.86.235.114 [Public IP]	VPC ID vpc-0f23f7258d8d532a6	AWS Compute Optimizer finding Opt-in to AWS Compute Optimizer for recommendations. | Learn more
IAM Role –	Subnet ID subnet-0e873758d3d86e6b2	Auto Scaling Group name –
IMDSv2 Required		

Video Walkthrough/Demonstration



Also available from the University OneDrive: https://universityofsussex-my.sharepoint.com/:v:/g/personal/db524_sussex_ac_uk/EVhTWxsOsO9AqwbqTCmUqsMBxCd7eR5H42Don28b34vyXw?nav=eyJyZWZlcnJhbEluZm8iOnsicmVmZXJyYWxBcHAiOiJPbmVEcml2ZUZvckJ1c2luZXNzIiwicmVmZXJyYWxBcHBQbGF0Zm9ybSI6IldlYiIsInJlZmVycmFsTW9kZSI6InZpZXciLCJyZWZlcnJhbFZpZXciOiJNeUZpbGVzTGlua0NvcHkifX0&e=FX7l0t

(And is in this zip file)

User Accounts for Testing

Admin 1

Username: admin1

Password: admin1

Admin 2

Username: webapps

Password: wa123456!

User 1

Username: testuser1

Password: testpassword1

User 2

Username: testuser2

Password: testpassword2

Codebase Details

Attached here inside webapps2024.zip

Also available on GitHub at https://github.com/danbates1452/webapps2024 upon request.

Requires a valid Python 3.8 (developed on 3.8.10) interpreter, as well as dependencies featured in requirements.txt. See readme.md for a sample pip command to install these.

The database comes preloaded for convenience but you can delete it and start fresh and use the typical Django commands if needs be.