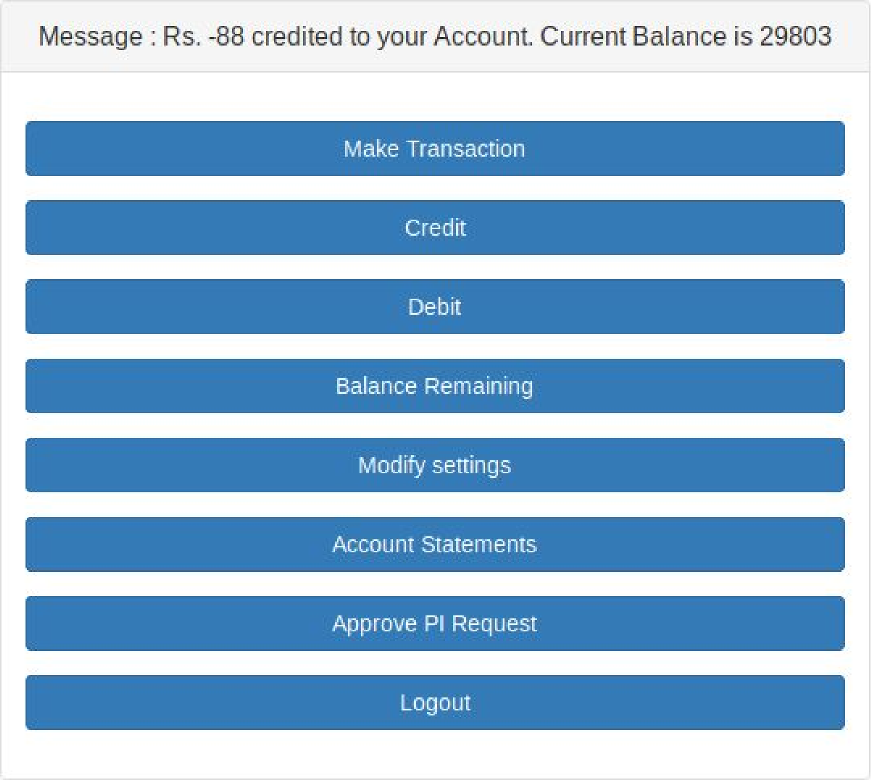
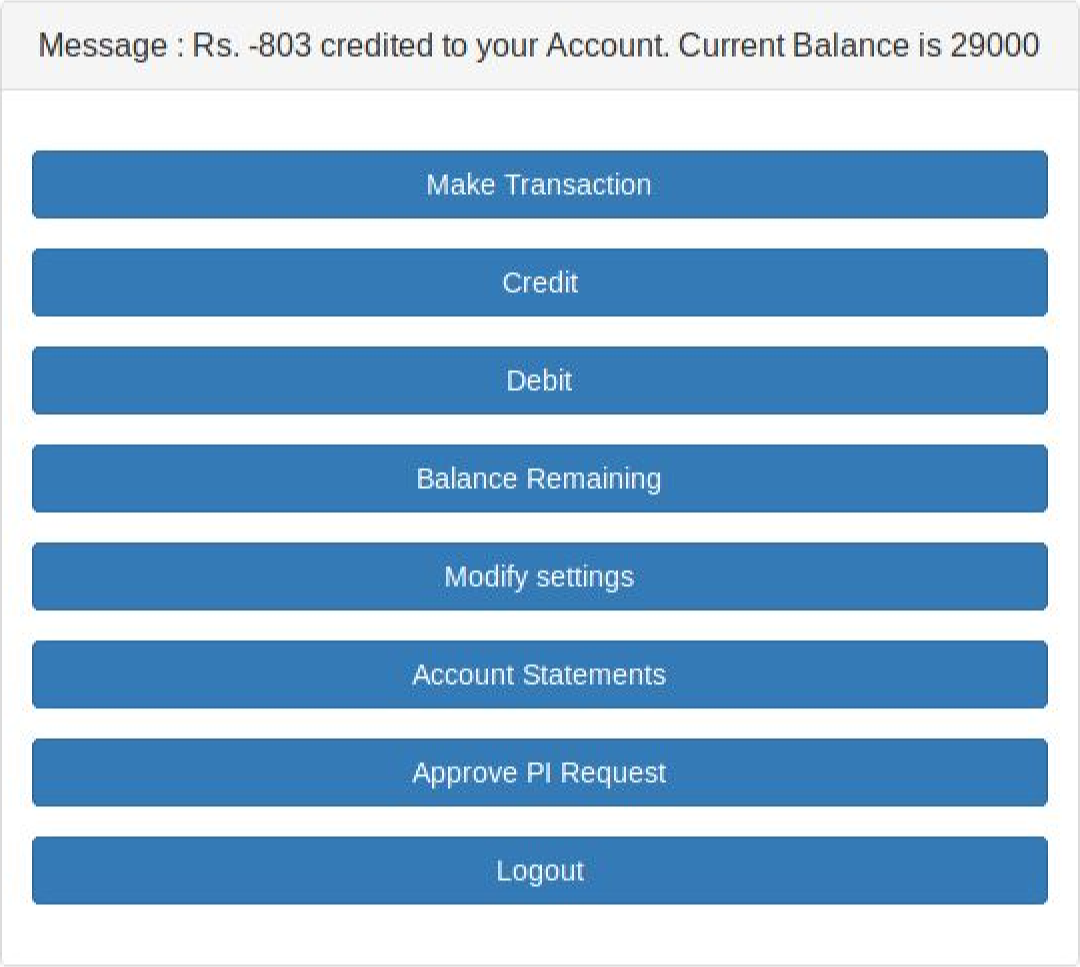
Group-4 Testing Report

Security Issues

1) Negative Balance Credit - Login From External Account and try crediting -ve amount in your account.

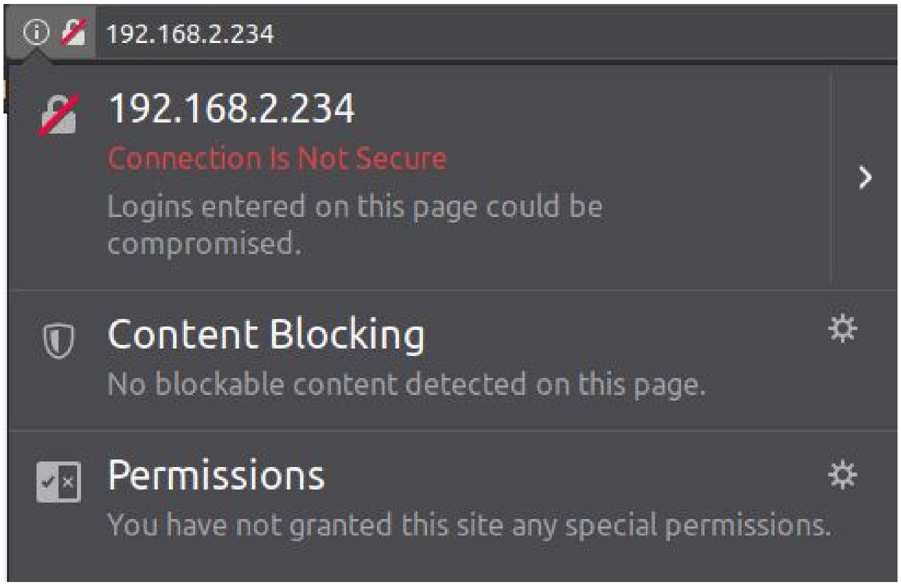


Message : Rs. -88 credited to your Account. Current Balance is 29803



Message : Rs. -803 credited to your Account. Current Balance is 29000

2) Http Website - No SSL Encryption



192.168.2.234

192.168.2.234

Connection Is Not Secure

Logins entered on this page could be compromised.

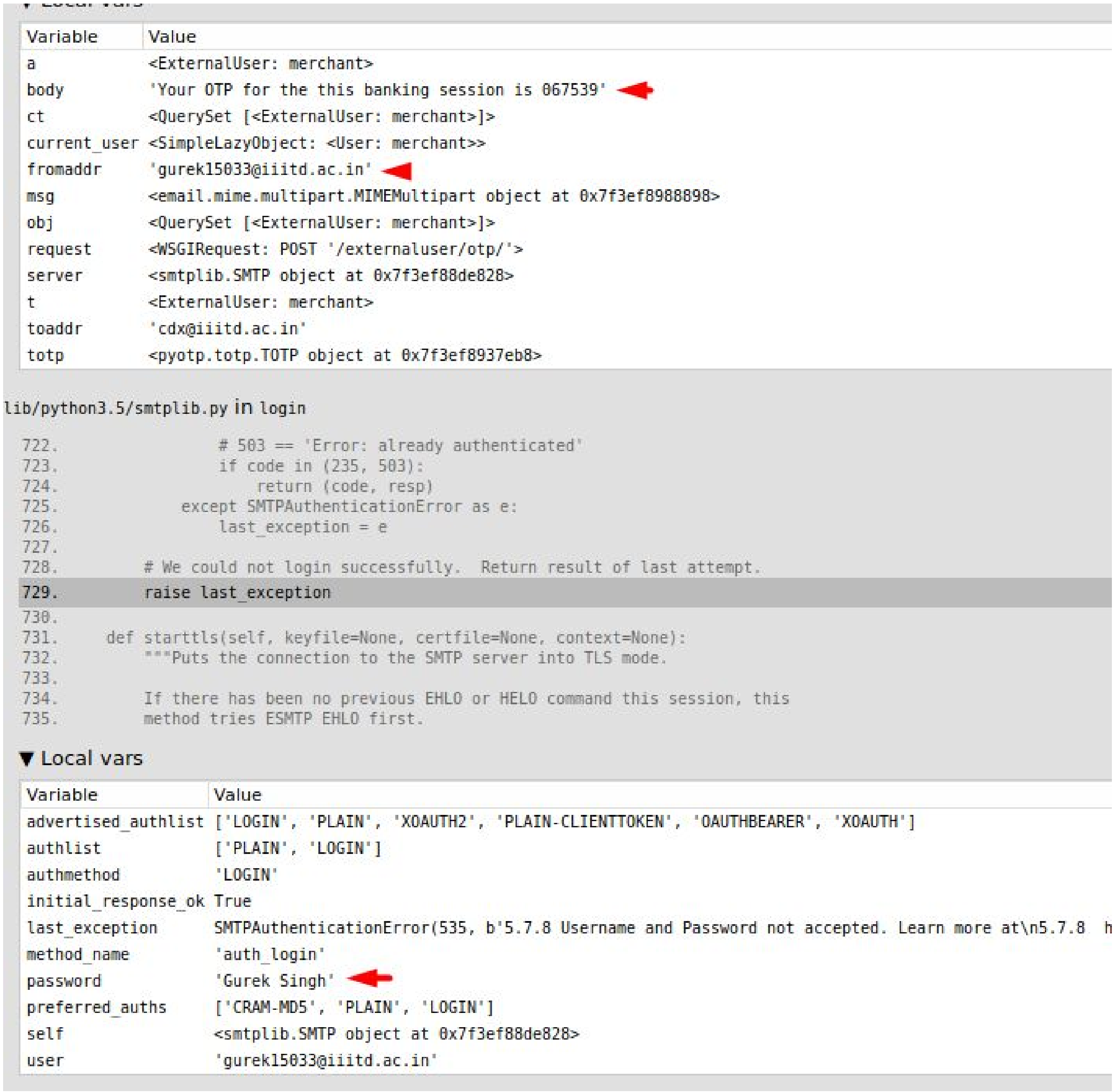
Content Blocking

No blockable content detected on this page.

Permissions

You have not granted this site any special permissions.

3) Debug == True,
   Reveal sensitive content of the web application.
   Code snippets visible
   Email ID used to send mail also revealed password in clear text (visible on Debug page).



▼ Local vars

Variable	Value
a	<ExternalUser: merchant>
body	'Your OTP for the this banking session is 067539'
ct	<QuerySet [<ExternalUser: merchant>]>
current_user	<SimpleLazyObject: <User: merchant>>
fromaddr	'gurek15033@iiitd.ac.in'
msg	<email.mime.multipart.MIMEMultipart object at 0x7f3ef8988898>
obj	<QuerySet [<ExternalUser: merchant>]>
request	<WSGIRequest: POST '/externaluser/otp/'>
server	<smtplib.SMTP object at 0x7f3ef88de828>
t	<ExternalUser: merchant>
toaddr	'cdx@iiitd.ac.in'
totp	<pyotp.totp.TOTP object at 0x7f3ef8937eb8>

lib/python3.5/smtplib.py in login

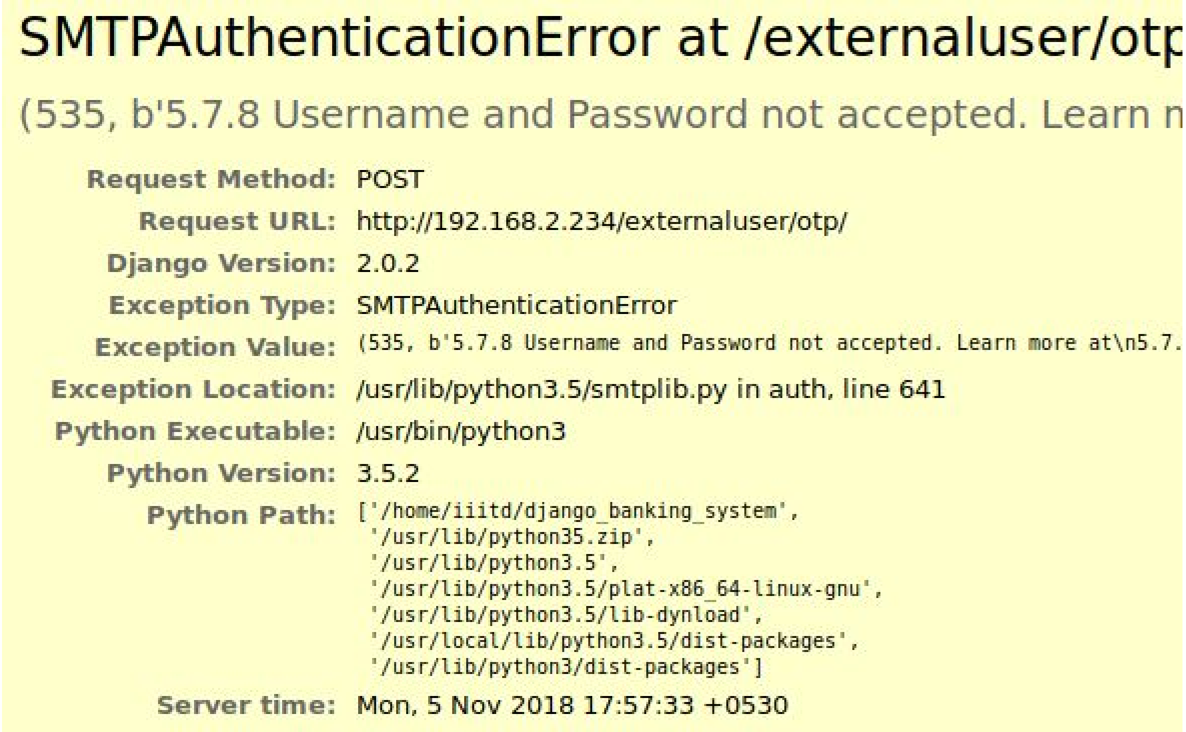
```
                # 503 == 'Error: already authenticated'
                if code in (235, 503):
                    return (code, resp)
            except SMTPAuthenticationError as e:
                last_exception = e

        # We could not login successfully.  Return result of last attempt.
        raise last_exception

    def starttls(self, keyfile=None, certfile=None, context=None):
        """Puts the connection to the SMTP server into TLS mode.

        If there has been no previous EHLO or HELO command this session, this
        method tries ESMTP EHLO first.
```

▼ Local vars

Variable	Value
advertised_authlist	['LOGIN', 'PLAIN', 'XOAUTH2', 'PLAIN-CLIENTTOKEN', 'OAUTHBEARER', 'XOAUTH']
authlist	['PLAIN', 'LOGIN']
authmethod	'LOGIN'
initial_response_ok	True
last_exception	SMTPAuthenticationError(535, b'5.7.8 Username and Password not accepted. Learn more at\n5.7.8 h
method_name	'auth_login'
password	'Gurek Singh'
preferred_auths	['CRAM-MD5', 'PLAIN', 'LOGIN']
self	<smtplib.SMTP object at 0x7f3ef88de828>
user	'gurek15033@iiitd.ac.in'

Email ID and Password of sender are visible in above text.
According to me, For OTP gureks mail was used and his password. SMTP Library require senders email and password to send a mail.

Below error is occuring because gurek changed his password.

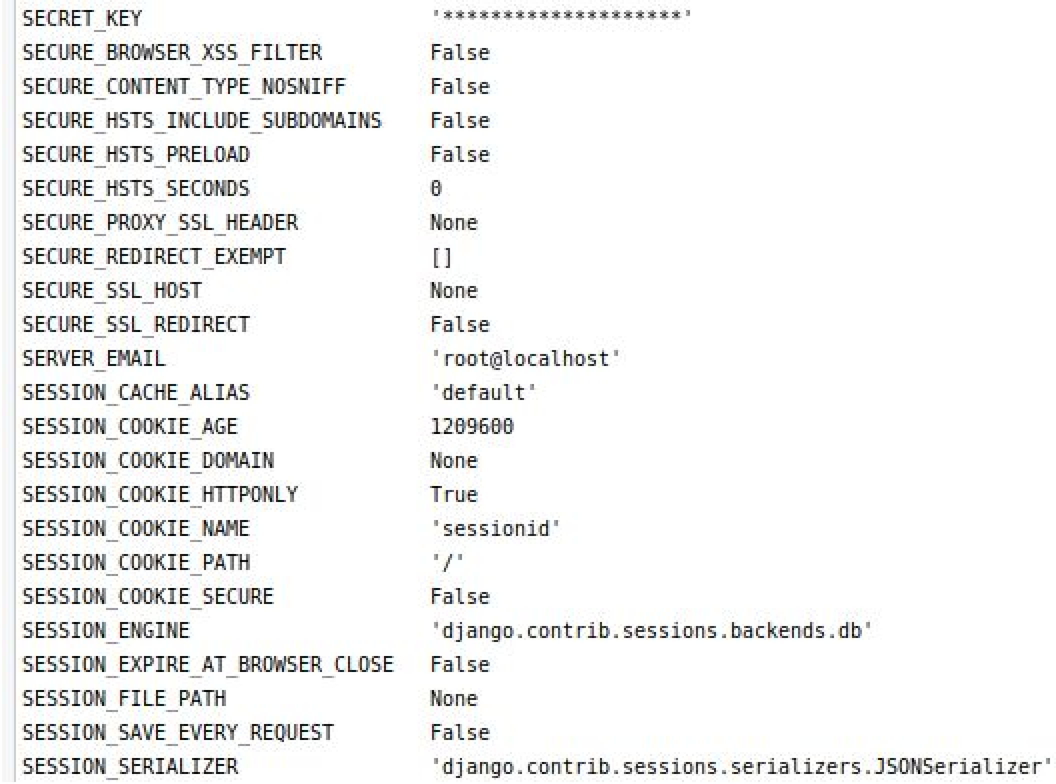


SMTPAuthenticationError at /externaluser/otp

(535, b'5.7.8 Username and Password not accepted. Learn n

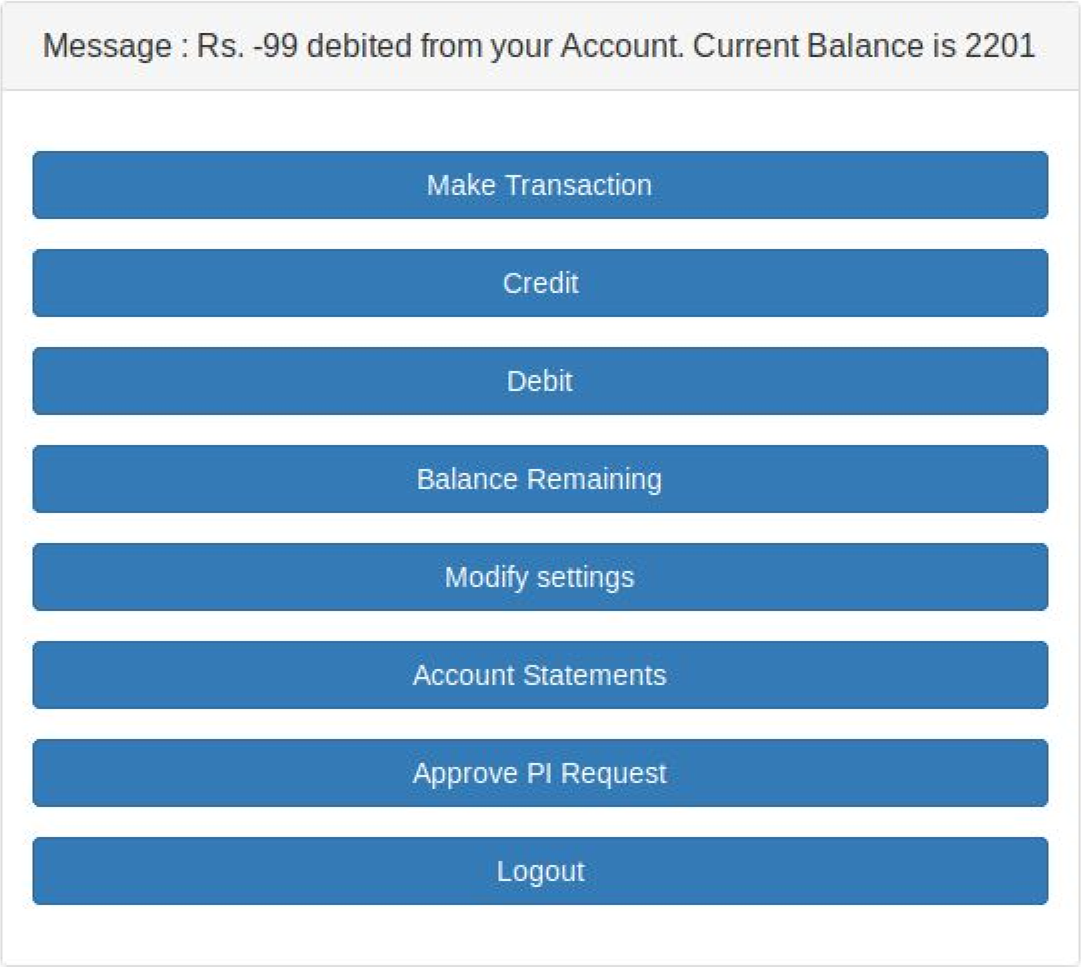
```
     Request Method:  POST
        Request URL:  http://192.168.2.234/externaluser/otp/
     Django Version:  2.0.2
     Exception Type:  SMTPAuthenticationError
    Exception Value:  (535, b'5.7.8 Username and Password not accepted. Learn more at\n5.7.
 Exception Location:  /usr/lib/python3.5/smtplib.py in auth, line 641
  Python Executable:  /usr/bin/python3
     Python Version:  3.5.2
        Python Path:  ['/home/iiitd/django_banking_system',
                       '/usr/lib/python35.zip',
                       '/usr/lib/python3.5',
                       '/usr/lib/python3.5/plat-x86_64-linux-gnu',
                       '/usr/lib/python3.5/lib-dynload',
                       '/usr/local/lib/python3.5/dist-packages',
                       '/usr/lib/python3/dist-packages']
        Server time:  Mon, 5 Nov 2018 17:57:33 +0530
```

Below image contains setting present in settings.py file of their django project.
It reveals the security features used in their django website.

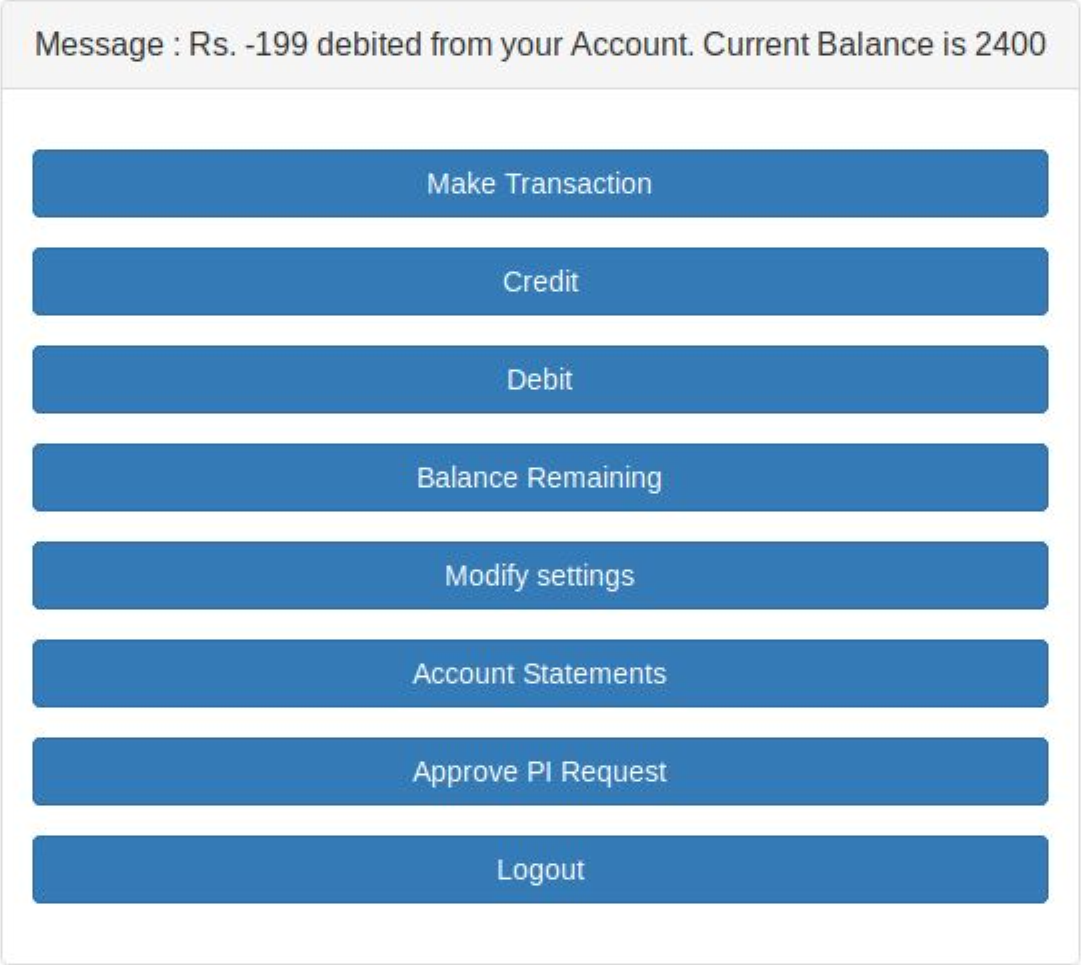


```
SECRET_KEY                          '********************'
SECURE_BROWSER_XSS_FILTER           False
SECURE_CONTENT_TYPE_NOSNIFF         False
SECURE_HSTS_INCLUDE_SUBDOMAINS      False
SECURE_HSTS_PRELOAD                 False
SECURE_HSTS_SECONDS                 0
SECURE_PROXY_SSL_HEADER             None
SECURE_REDIRECT_EXEMPT              []
SECURE_SSL_HOST                     None
SECURE_SSL_REDIRECT                 False
SERVER_EMAIL                        'root@localhost'
SESSION_CACHE_ALIAS                 'default'
SESSION_COOKIE_AGE                  1209600
SESSION_COOKIE_DOMAIN               None
SESSION_COOKIE_HTTPONLY             True
SESSION_COOKIE_NAME                 'sessionid'
SESSION_COOKIE_PATH                 '/'
SESSION_COOKIE_SECURE               False
SESSION_ENGINE                      'django.contrib.sessions.backends.db'
SESSION_EXPIRE_AT_BROWSER_CLOSE     False
SESSION_FILE_PATH                   None
SESSION_SAVE_EVERY_REQUEST          False
SESSION_SERIALIZER                  'django.contrib.sessions.serializers.JSONSerializer'
```

4) Negative Balance debit:
   Login from external user account. Try creating a debit request.
   On -ve Debit request system add that negative amount to the balance instead of subtracting from it.



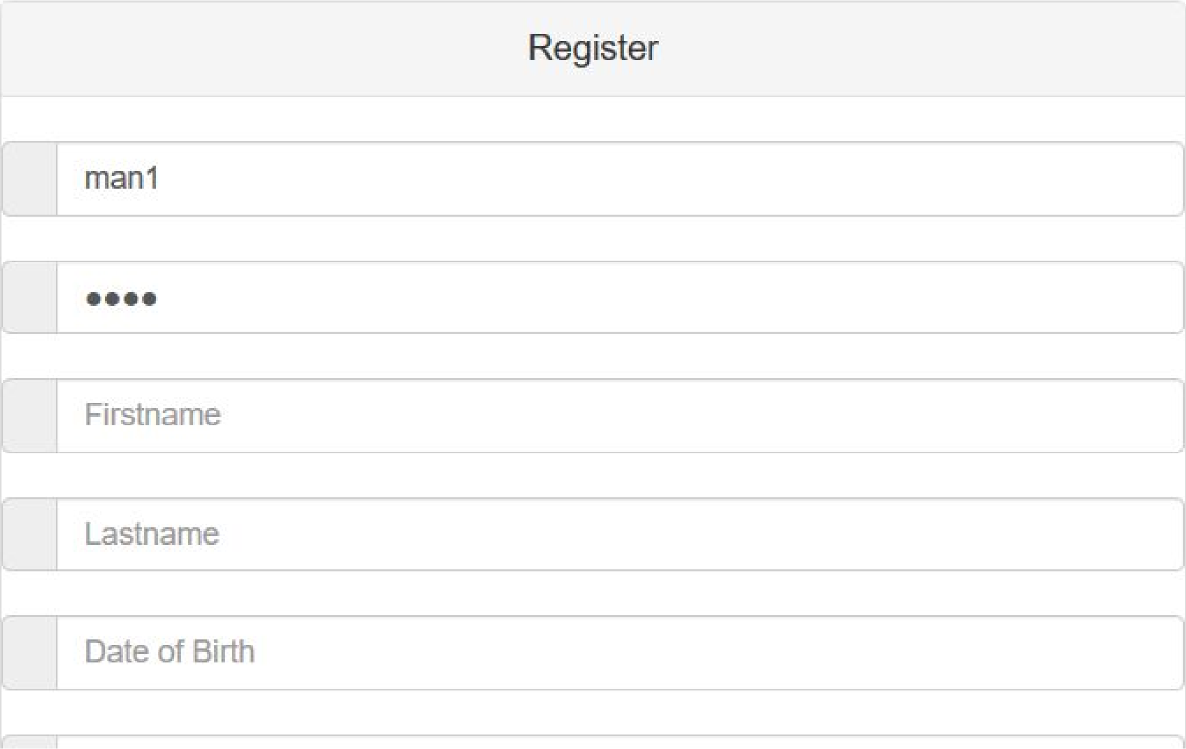
Message : Rs. -99 debited from your Account. Current Balance is 2201



Message : Rs. -199 debited from your Account. Current Balance is 2400

5) Brute Force on login page
   Since Captcha functionality is not used. Its present there, but i’m able to login without clicking captcha button.
   https://drive.google.com/open?id=1mw3uh12iVLS4eyOglMB3UlMaA3pKeBdJ

6) Autocomplete enabled:


Register

man1

●●●●

7) No session Timeout:

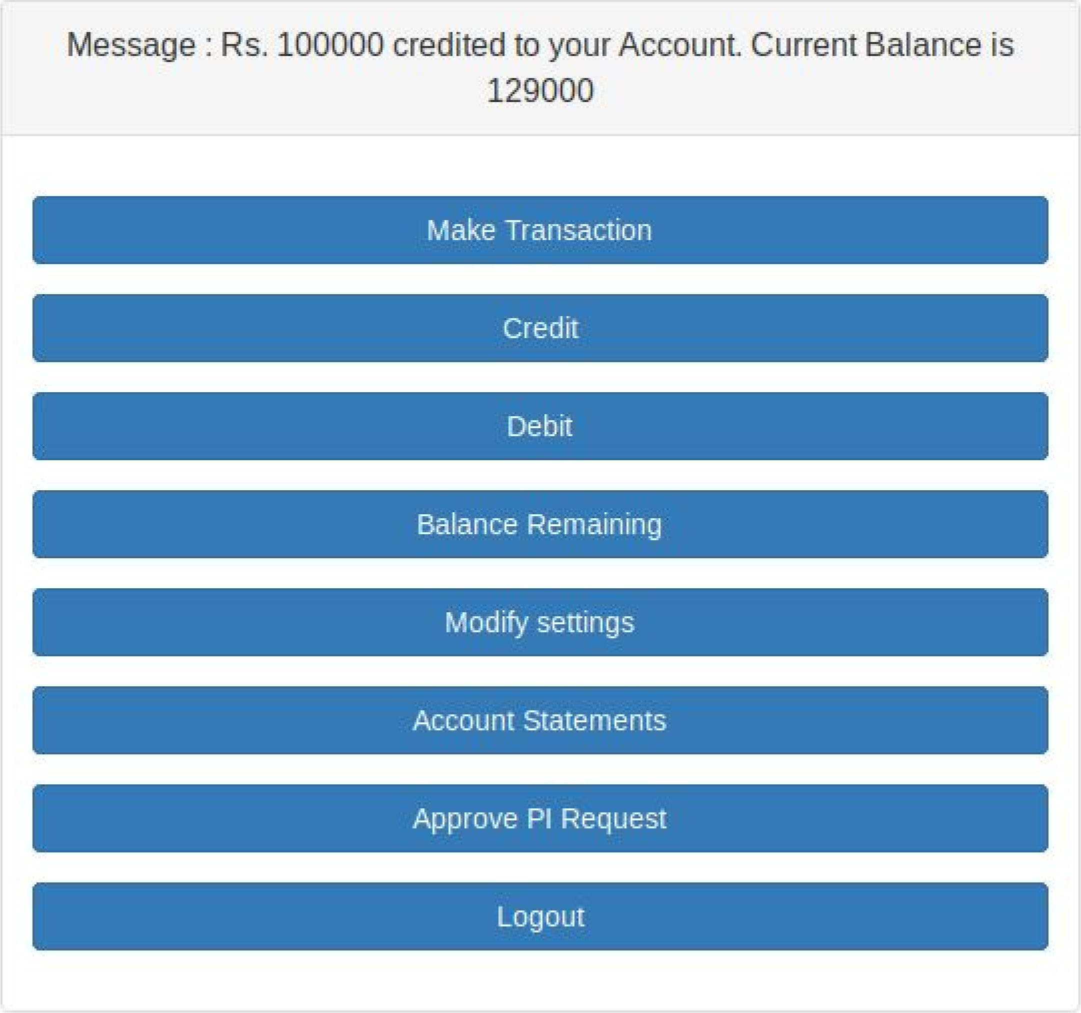
8) No check for number of login attempts (Brute Force definitely possible). Captcha was present in form but was not enabled with login button press.

9) Multiple session of same account allowed.

- Log in using external user credentials.
- Log in again using same user credentials on different browser.

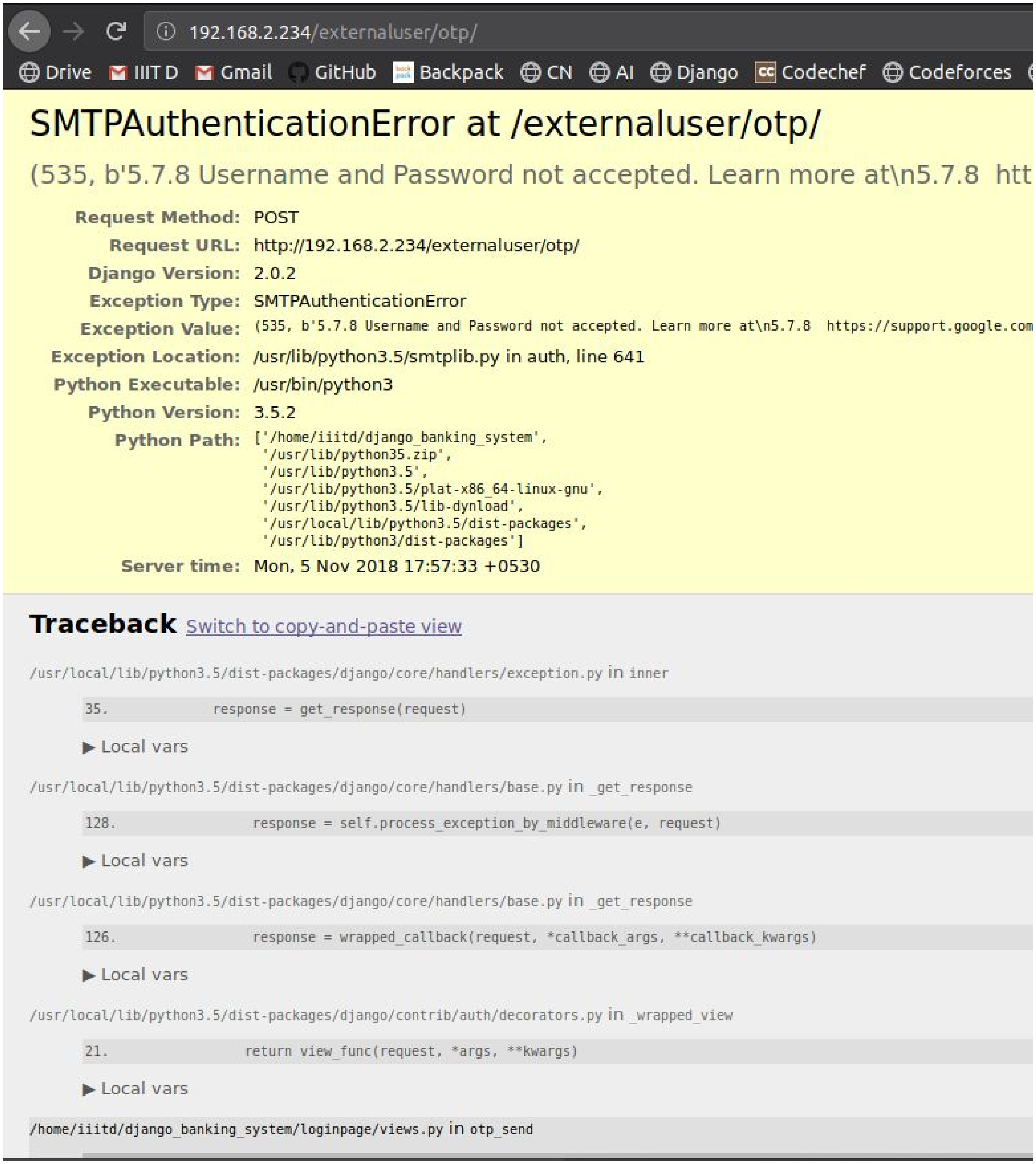
Functional issues

1) Can credit any amount without approval from higher authority
   No Upper Limit for Credit



Message : Rs. 100000 credited to your Account. Current Balance is 129000

2) OTP Generation Not Working



SMTPAuthenticationError at /externaluser/otp/

(535, b'5.7.8 Username and Password not accepted. Learn more at\n5.7.8 htt

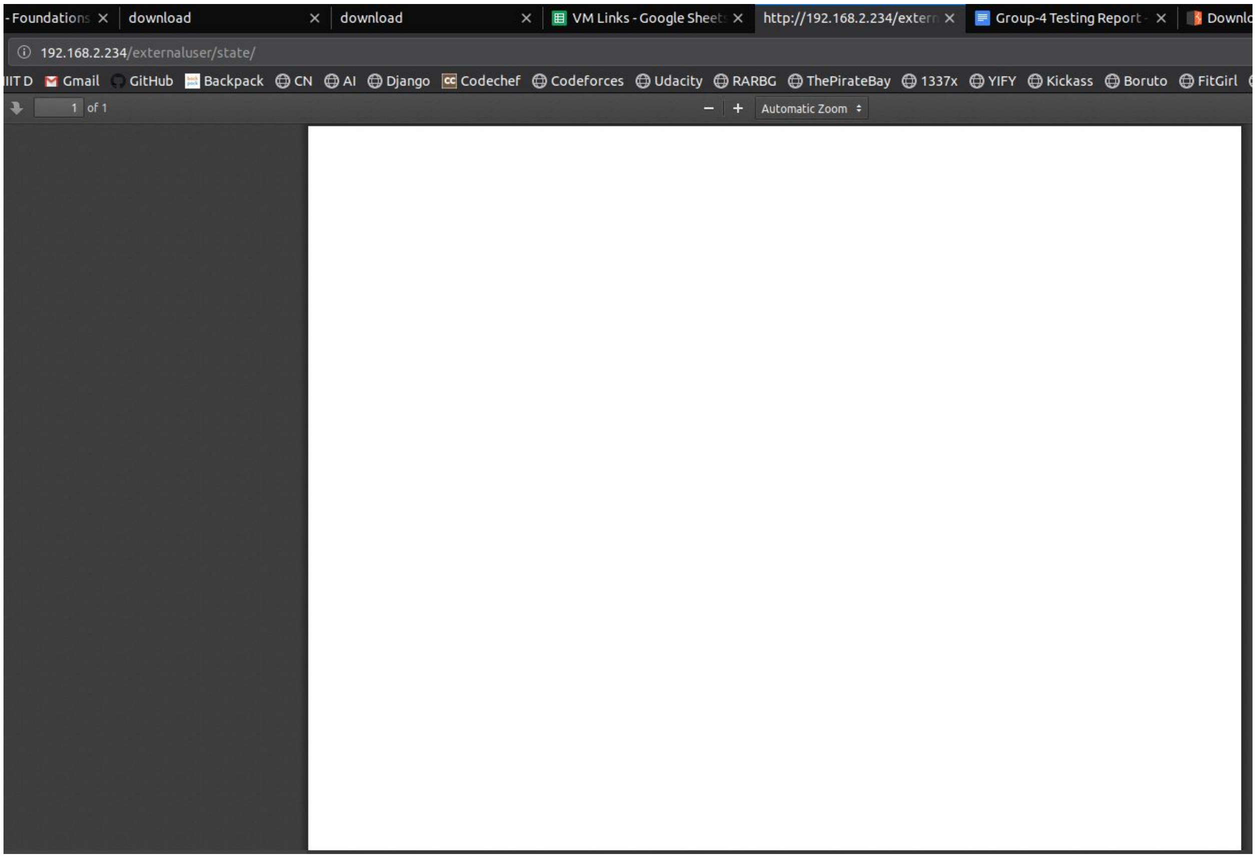
```
        Request Method:  POST
           Request URL:  http://192.168.2.234/externaluser/otp/
        Django Version:  2.0.2
        Exception Type:  SMTPAuthenticationError
       Exception Value:  (535, b'5.7.8 Username and Password not accepted. Learn more at\n5.7.8  https://support.google.com
    Exception Location:  /usr/lib/python3.5/smtplib.py in auth, line 641
     Python Executable:  /usr/bin/python3
        Python Version:  3.5.2
           Python Path:  ['/home/iiitd/django_banking_system',
                          '/usr/lib/python35.zip',
                          '/usr/lib/python3.5',
                          '/usr/lib/python3.5/plat-x86_64-linux-gnu',
                          '/usr/lib/python3.5/lib-dynload',
                          '/usr/local/lib/python3.5/dist-packages',
                          '/usr/lib/python3/dist-packages']
           Server time:  Mon, 5 Nov 2018 17:57:33 +0530
```

Traceback Switch to copy-and-paste view

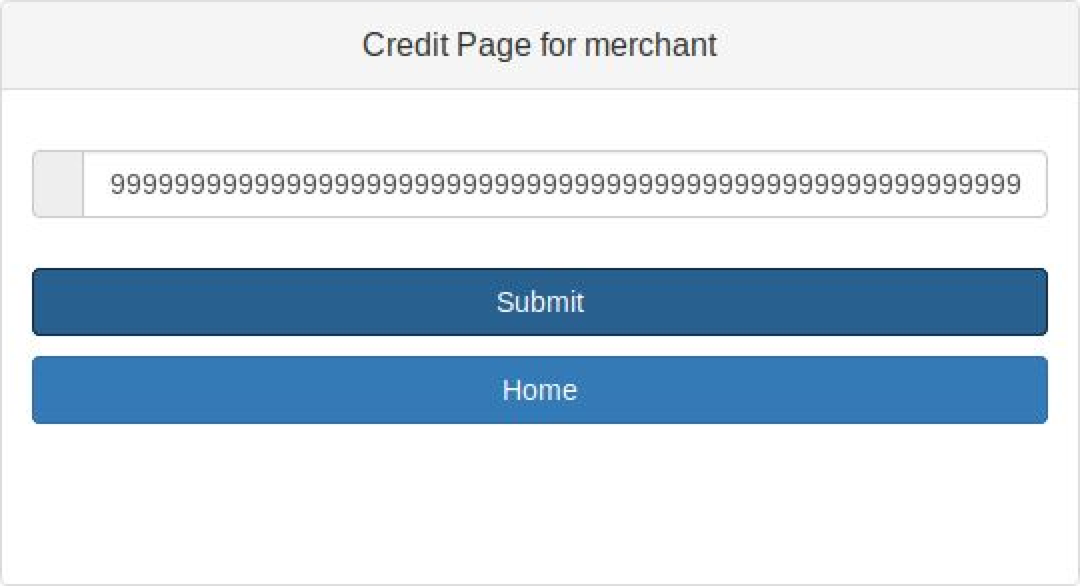
```
/usr/local/lib/python3.5/dist-packages/django/core/handlers/exception.py in inner

      35.             response = get_response(request)

      ▶ Local vars

/usr/local/lib/python3.5/dist-packages/django/core/handlers/base.py in _get_response

      128.                 response = self.process_exception_by_middleware(e, request)

      ▶ Local vars

/usr/local/lib/python3.5/dist-packages/django/core/handlers/base.py in _get_response

      126.                 response = wrapped_callback(request, *callback_args, **callback_kwargs)

      ▶ Local vars

/usr/local/lib/python3.5/dist-packages/django/contrib/auth/decorators.py in _wrapped_view

      21.                return view_func(request, *args, **kwargs)

      ▶ Local vars

/home/iiitd/django_banking_system/loginpage/views.py in otp_send
```

Click on OTP Generation Button to replicate this error.

3) Account Summary Not available (Blank PDF)

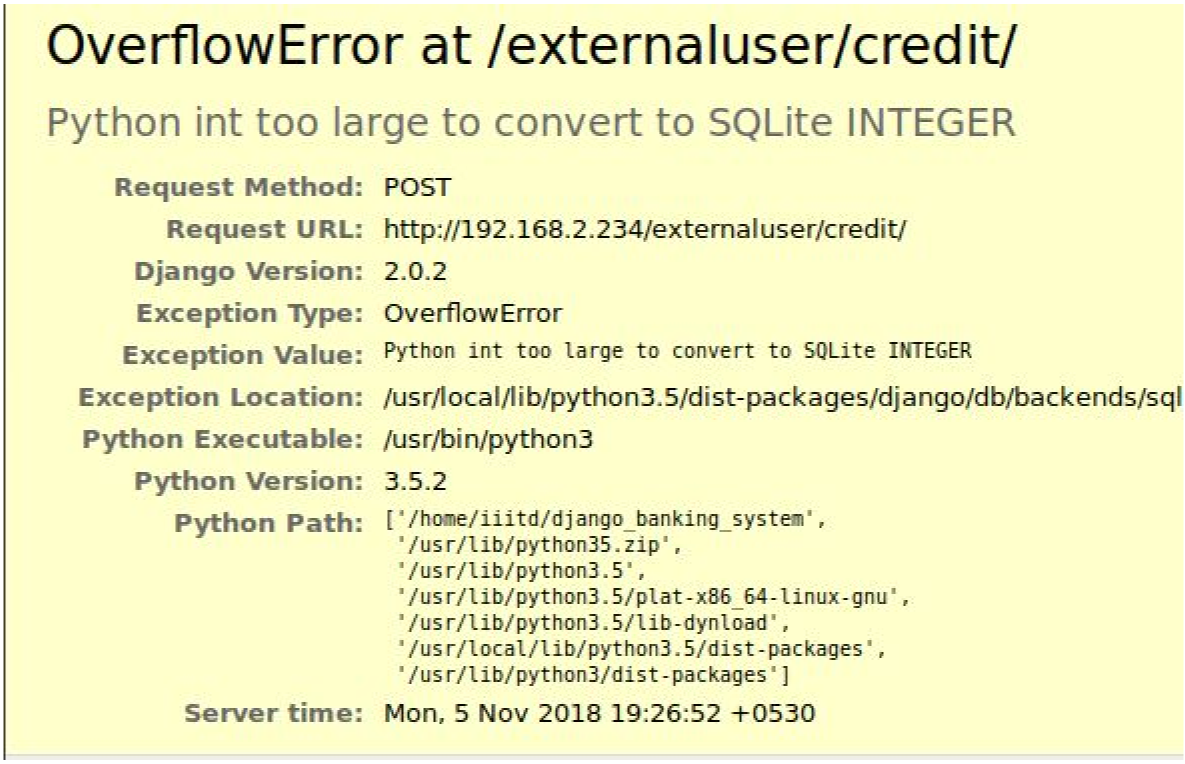


4) No Limit check for credit



Credit Page for merchant

99999999999999999999999999999999999999999999999999999999



OverflowError at /externaluser/credit/

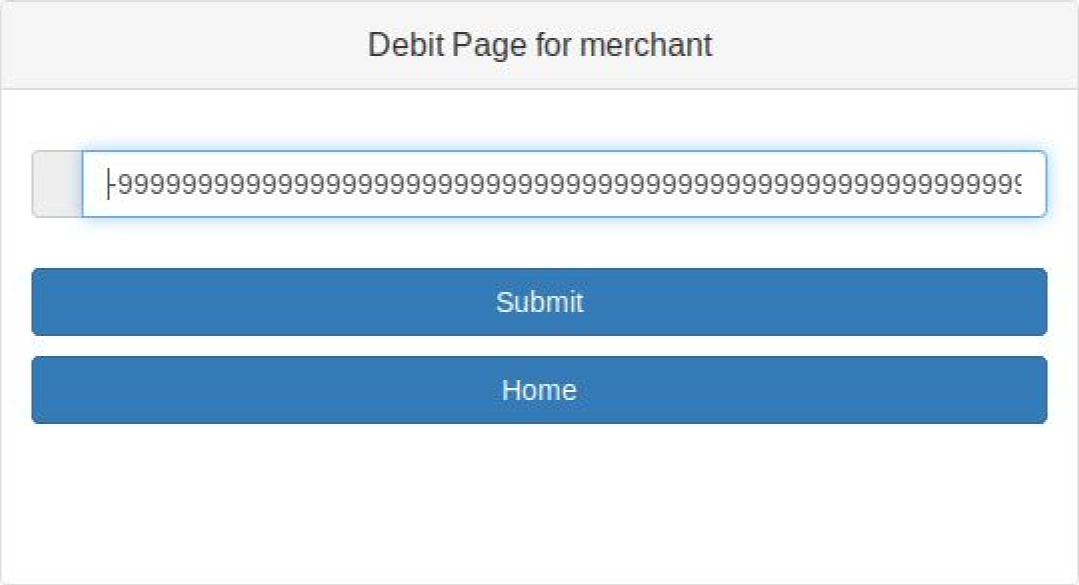
Python int too large to convert to SQLite INTEGER

Request Method:	POST
Request URL:	http://192.168.2.234/externaluser/credit/
Django Version:	2.0.2
Exception Type:	OverflowError
Exception Value:	`Python int too large to convert to SQLite INTEGER`
Exception Location:	/usr/local/lib/python3.5/dist-packages/django/db/backends/sql
Python Executable:	/usr/bin/python3
Python Version:	3.5.2

Python Path:	`['/home/iiitd/django_banking_system',`
	`'/usr/lib/python35.zip',`
	`'/usr/lib/python3.5',`
	`'/usr/lib/python3.5/plat-x86_64-linux-gnu',`
	`'/usr/lib/python3.5/lib-dynload',`
	`'/usr/local/lib/python3.5/dist-packages',`
	`'/usr/lib/python3/dist-packages']`

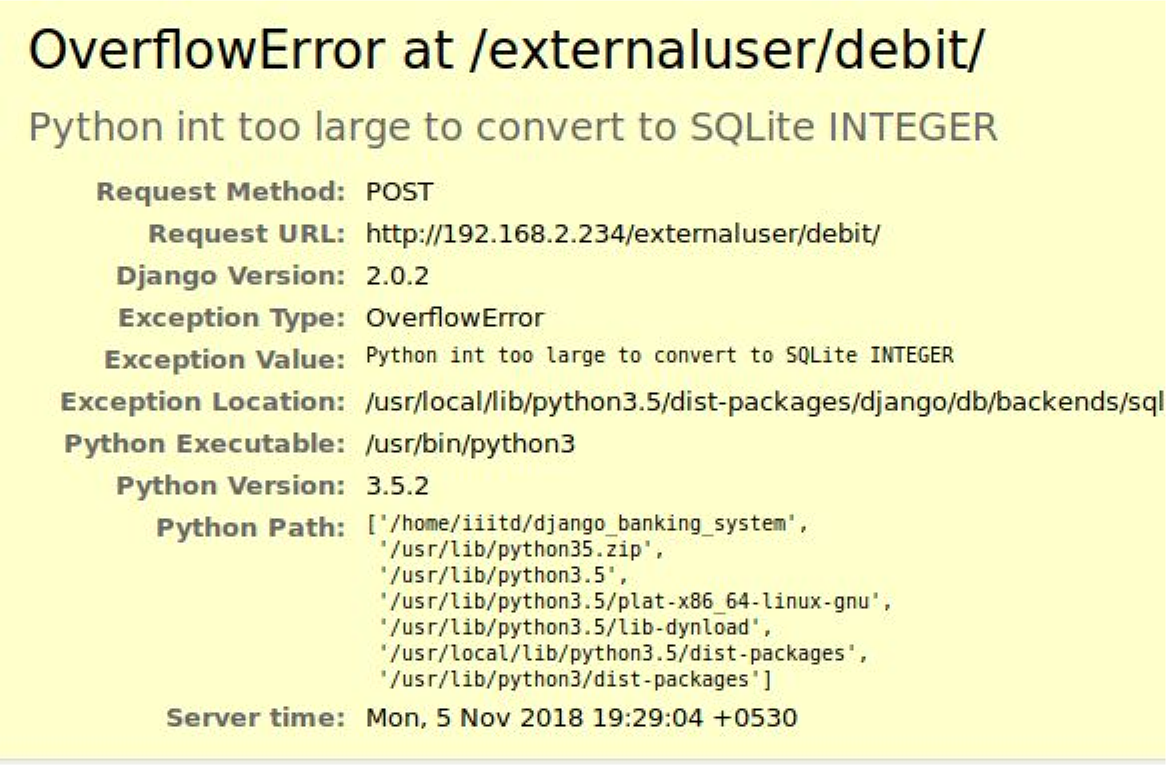
Server time:	Mon, 5 Nov 2018 19:26:52 +0530

5) Overflow error received on entering very large -ve number for debit
Debit allowing -ve amount to be added in total balance



Debit Page for merchant

-99999999999999999999999999999999999999999999999999999



OverflowError at /externaluser/debit/

Python int too large to convert to SQLite INTEGER

Request Method: POST

Request URL: http://192.168.2.234/externaluser/debit/

Django Version: 2.0.2

Exception Type: OverflowError

Exception Value: `Python int too large to convert to SQLite INTEGER`

Exception Location: /usr/local/lib/python3.5/dist-packages/django/db/backends/sql

Python Executable: /usr/bin/python3

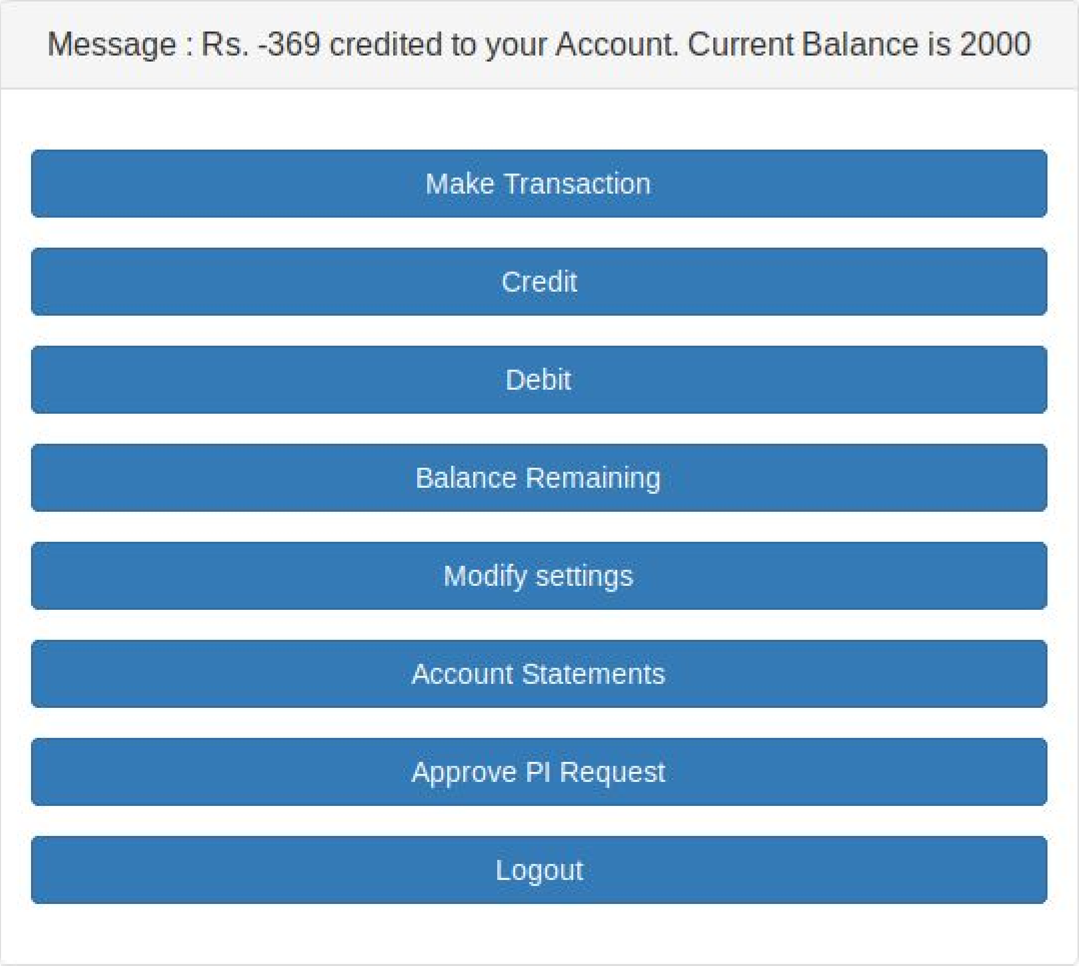
Python Version: 3.5.2

Python Path:

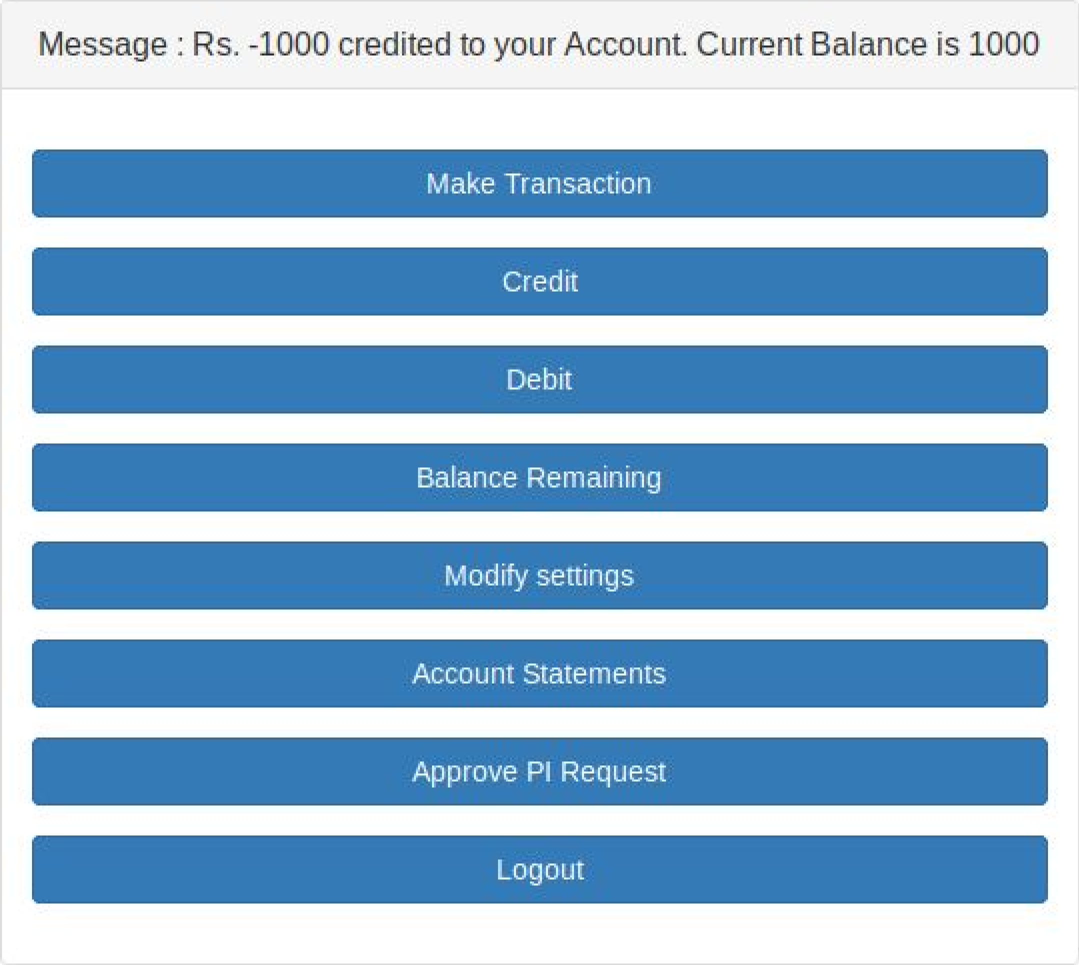
```
['/home/iiitd/django_banking_system',
 '/usr/lib/python35.zip',
 '/usr/lib/python3.5',
 '/usr/lib/python3.5/plat-x86_64-linux-gnu',
 '/usr/lib/python3.5/lib-dynload',
 '/usr/local/lib/python3.5/dist-packages',
 '/usr/lib/python3/dist-packages']
```

Server time: Mon, 5 Nov 2018 19:29:04 +0530

6) Negative credits allowed



Message : Rs. -369 credited to your Account. Current Balance is 2000



Message : Rs. -1000 credited to your Account. Current Balance is 1000

7) For Regular Employee:
“view, create, modify, delete and authorize transactions functionality”
Not available on the website.

Only Approve transaction button available. Not testable since otp is not working because of which testers are not able to create transaction and test Manager & Admin functionalities.

8) For Regular Employee:
No functionalities available to view & modify any user account

9) For System Manager:
Critical Transaction approval not testable because of no transaction creation functionality.

10) Single Account only for internal user. Cannot create an account. No functionality provided.