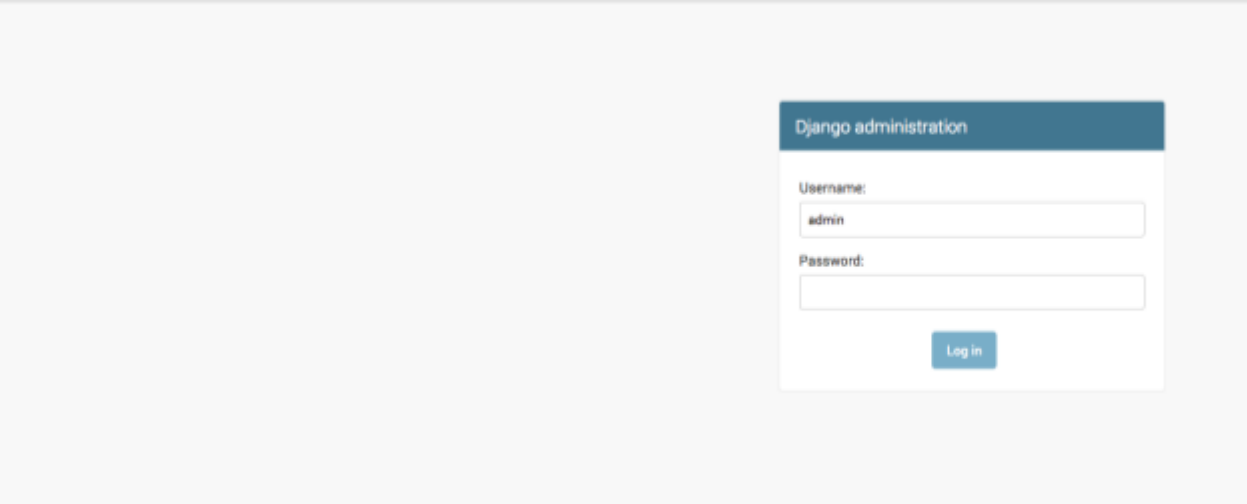
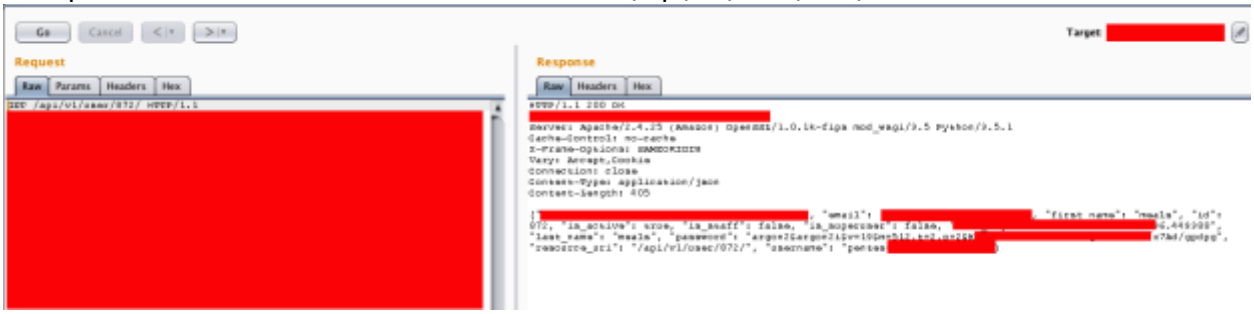
Django Privilege Escalation – Zero To Superuser
Sean Melia
June 1 2017

I was invited to a bug bounty program on 5/31. I initially kicked off dirsearch on their dev environment which they wanted tested. It pointed me towards /admin/ which when I went to was a Django admin login interface. Seeing this exposed to the internet I quickly wrote up a report about locking this down to certain IP's and not exposing it to the Internet. They replied back saying the internal console was locked down, however the login page was still visible. I figured I'd put that to the test.

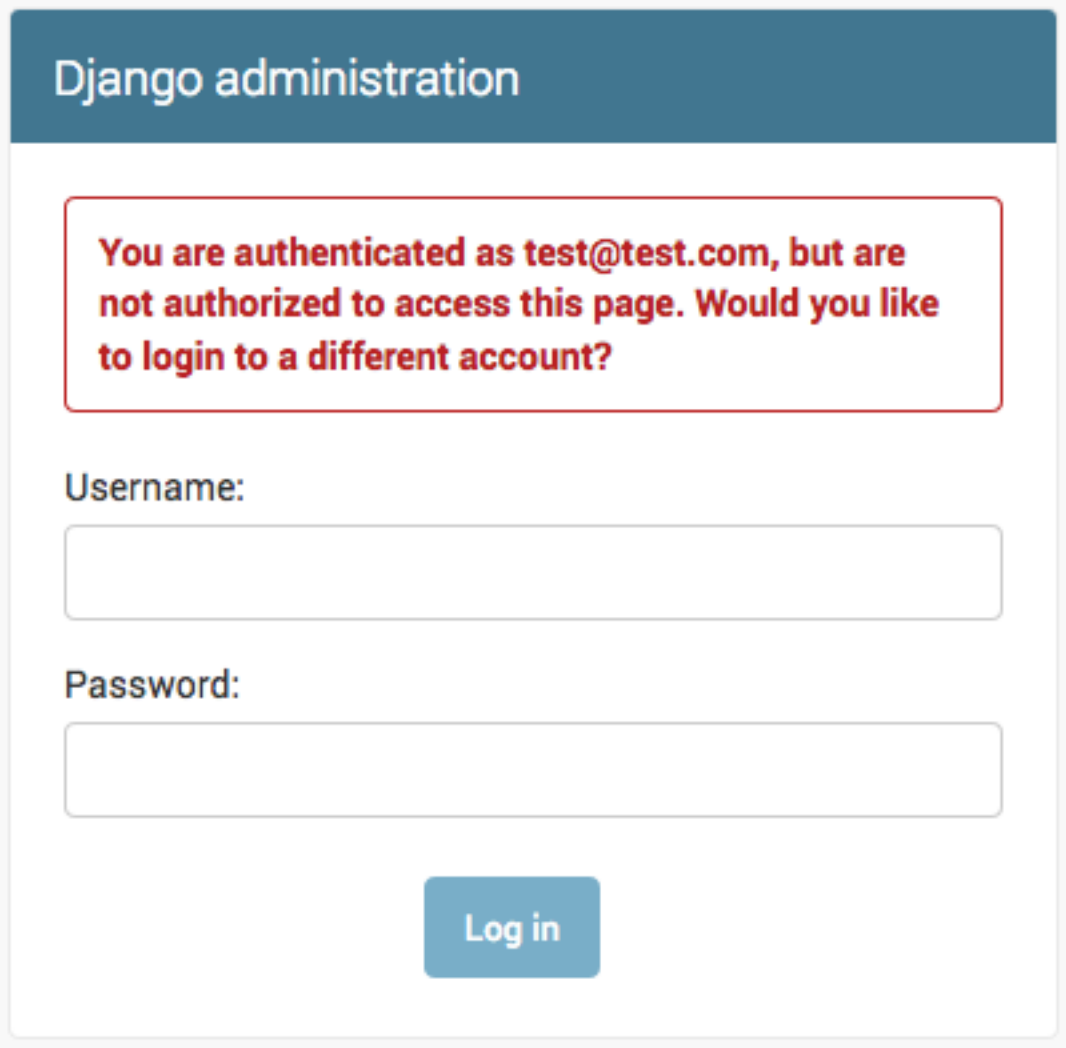


I created an account via the regular signup page with my email address. At this point I didn't know the regular user accounts were in the same database as the admin accounts for the admin panel (this may just be my inexperience with Django, who knows). I logged in and found some cool bugs. One notably was on the second or third request after signing in which was an authorization bug that allowed me to enumerate other user account data including, names, emails, password hashes, etc. The value after the /user/ path was vulnerable to parameter manipulation in the screenshot below. Rest API: /api/v1/user/872/



Additionally, in the response were two values `"is_superuser": "false"` and `"is_staff": "false"`. I thought that was interesting. However, I continued to plug away at the app and report some other bugs.

I went back to /admin/ in a browser where I had a session with the main user application and noticed the login page had changed to include that I was attempting to login with X account and I was not authorized.



This alerted me to the fact that my session from the main app also corresponded to the Django admin panel.

On another page in the application it allows you to update your profile information including your first/last name, etc. However there is no option to change the username or upgrade/downgrade privileges. I decided to take the JSON POST data and add in another parameter “username”:

```
{"firstName":"meals","lastName":"meals","email":"test@test.com",
"smsPhone":"7035555666","username":"admin"}
```

In the response I then noticed my username was changed from my email address to admin.

Response:

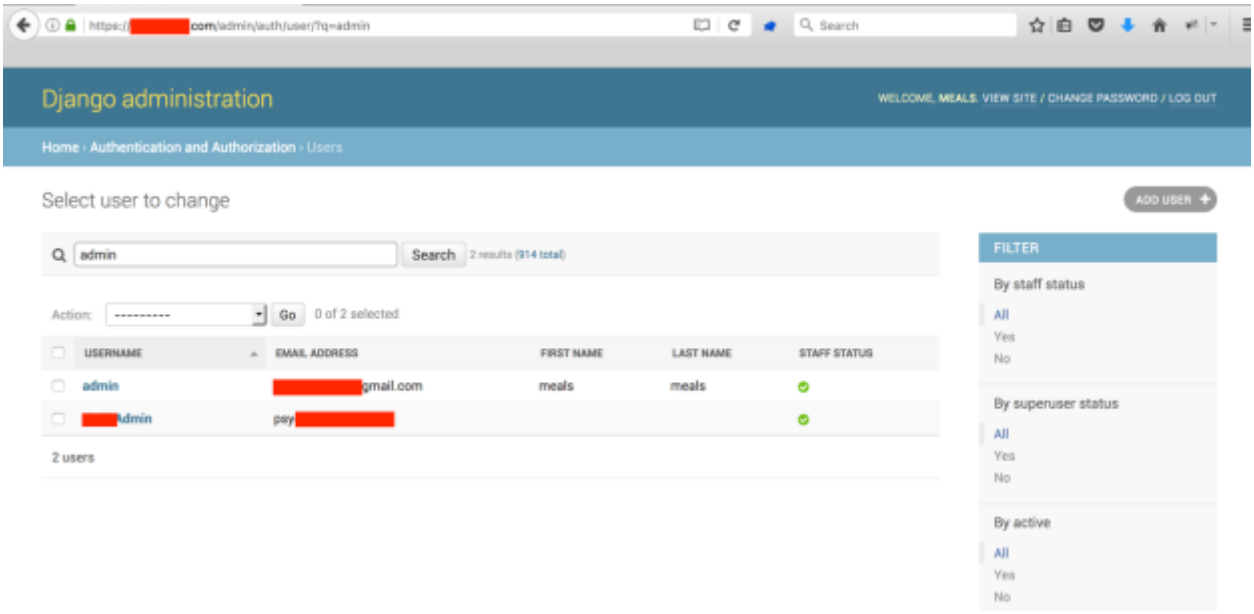
{"email": "test@test.com", "firstName": "meals", "first_name": "meals", "id": 872, "lastName": "meals", "last_login": "redacted", "last_name": "meals", "resource_uri": "/api/v1/user/872/", "smsPhone": "7035556666", ”username": "admin"}

I’m able to pass in additional parameters which are then actually processed correctly on the backend. I then went back to /admin/ and noticed the response had changed. I was attempting to login as “admin” however I did not have access to the panel still.

I then decided to include the parameter “superuser”: “true” which resulted in no change. I then tried “is_superuser”: “true” and the response from the application stated: {"error": "[\"'true' value must be either True or False.\"]"}. Bingo. I then supplied “is_superuser” : “True” and “is_staff”: “True” and the request was processed.

{"date_joined": "redacted", "email": "test@test.com", "firstName": "meals", "first_name": "meals", "id": 872, "is_active": true, "is_staff": true, "is_superuser": true, "lastName": "meals", "last_login": "redacted", "last_name": "meals", "password": "redacted", "resource_uri": "/api/v1/user/872/", "smsPhone": "7035556666"username": "admin"}

I then navigated back to the /admin/ directory and was subsequently logged in.


https://[redacted]com/admin/auth/user/?q=admin
Search
Django administration
WELCOME, MEALS. VIEW SITE / CHANGE PASSWORD / LOG OUT
Home › Authentication and Authorization › Users
Select user to change
ADD USER +
admin
Search
2 results (314 total)
Action:
Go
0 of 2 selected
USERNAME
EMAIL ADDRESS
FIRST NAME
LAST NAME
STAFF STATUS
admin
[redacted]gmail.com
meals
meals
[redacted]Admin
psy[redacted]
2 users
FILTER
By staff status
All
Yes
No
By superuser status
All
Yes
No
By active
All
Yes
No