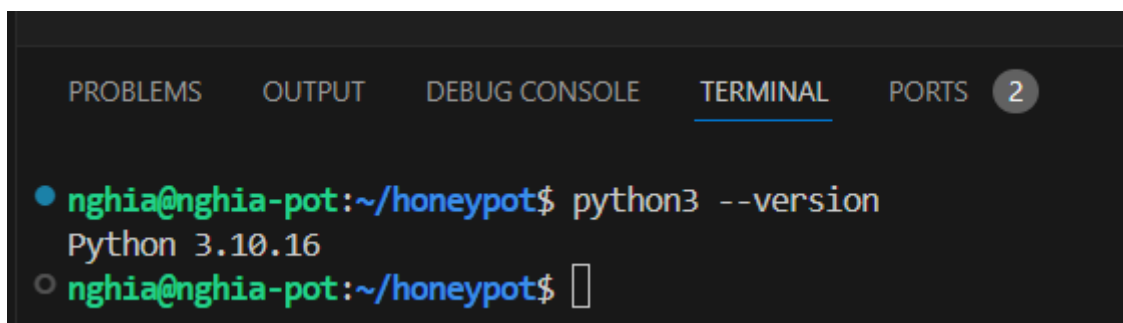


# Kịch bản tấn công Web honeypot

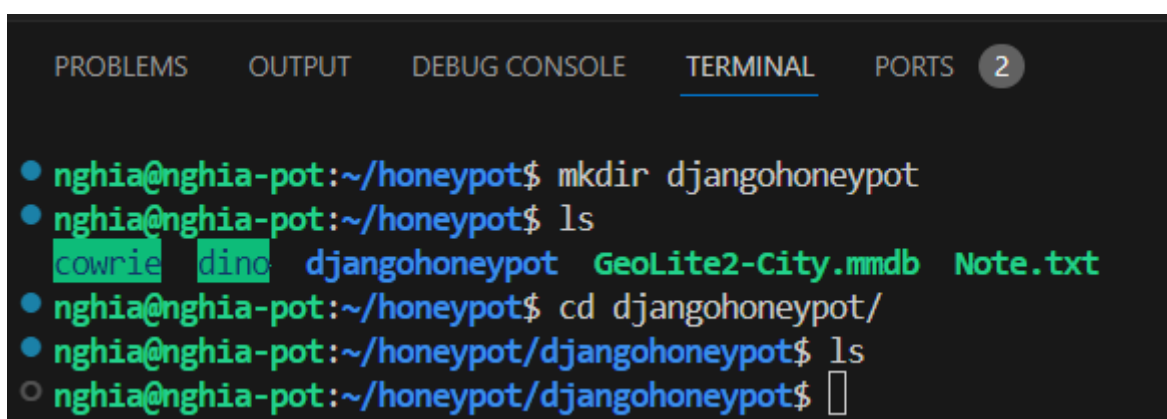
django-admin-honeypot là một trang đăng nhập của quản trị viên django, được sử dụng để ghi nhận và thông báo cho quản trị viên về các nỗ lực truy cập trái phép. Ứng dụng này được lấy cảm hứng từ các cuộc thảo luận xoay quanh bài nói chuyện về bảo mật của Paul McMillan tại DjangoCon năm 2011.

## 1. Cài đặt

```
Cài đặt python3 và gói kèm theo
sudo apt update
sudo apt install software-properties-common -y
sudo add-apt-repository ppa:deadsnakes/ppa
sudo apt update
sudo apt install python3.10 python3.10-venv python3.10-dev
```

A terminal window with tabs for PROBLEMS, OUTPUT, DEBUG CONSOLE, TERMINAL (selected), and PORTS (2). The terminal shows the command 'python3 --version' being executed, resulting in the output 'Python 3.10.16'. The prompt is 'nghia@nghia-pot:~/honeypot\$'.

```
mkdir.djangohoneypot
cd.djangohoneypot
```

A terminal window with tabs for PROBLEMS, OUTPUT, DEBUG CONSOLE, TERMINAL (selected), and PORTS (2). The terminal shows a sequence of commands: 'mkdir.djangohoneypot', 'ls' (showing 'cowrie', 'dino', 'djangohoneypot', 'GeoLite2-City.mmdb', 'Note.txt'), 'cd.djangohoneypot/', and 'ls' (showing an empty directory). The prompt is 'nghia@nghia-pot:~/honeypot/djangohoneypot\$'.

```
python3 -m venv django-env
source django-env/bin/activate
python -m pip install --upgrade pip
python -m pip install --upgrade -r requirements.txt
```

```

● nghia@nghia-pot:~/honeypot/djangohoneypot$ python3 -m venv django-env
● nghia@nghia-pot:~/honeypot/djangohoneypot$ source django-env/bin/activate
● (django-env) nghia@nghia-pot:~/honeypot/djangohoneypot$ python -m pip install --upgrade pip
Requirement already satisfied: pip in ./django-env/lib/python3.10/site-packages (23.0.1)
Collecting pip
  Using cached pip-24.3.1-py3-none-any.whl (1.8 MB)
Installing collected packages: pip
  Attempting uninstall: pip
    Found existing installation: pip 23.0.1
    Uninstalling pip-23.0.1:
      Successfully uninstalled pip-23.0.1
Successfully installed pip-24.3.1
● (django-env) nghia@nghia-pot:~/honeypot/djangohoneypot$ python -m pip install --upgrade -r requirements.txt
ERROR: Could not open requirements file: [Errno 2] No such file or directory: 'requirements.txt'
● (django-env) nghia@nghia-pot:~/honeypot/djangohoneypot$ python -m pip install --upgrade -r requirements.txt
Collecting django (from -r requirements.txt (line 1))
  Using cached Django-5.1.4-py3-none-any.whl.metadata (4.2 kB)
Collecting django-ipware (from -r requirements.txt (line 2))
  Using cached django_ipware-7.0.1-py2.py3-none-any.whl.metadata (9.1 kB)
Collecting pytest (from -r requirements.txt (line 4))
  Using cached pytest-8.3.4-py3-none-any.whl.metadata (7.5 kB)
Collecting pytest-cov (from -r requirements.txt (line 5))
  Using cached pytest_cov-6.0.0-py3-none-any.whl.metadata (27 kB)
Collecting pytest-django (from -r requirements.txt (line 6))
  Using cached pytest_django-4.9.0-py3-none-any.whl.metadata (8.2 kB)
Collecting pytest-pythonpath (from -r requirements.txt (line 7))
  Using cached pytest_pythonpath-0.7.4-py3-none-any.whl.metadata (2.8 kB)
Collecting asgiref<4,>=3.8.1 (from django->-r requirements.txt (line 1))
  Using cached asgiref-3.8.1-py3-none-any.whl.metadata (9.3 kB)
Collecting sqlparse>=0.3.1 (from django->-r requirements.txt (line 1))
  Using cached sqlparse-0.5.2-py3-none-any.whl.metadata (3.9 kB)

```

## Requirements.txt

```

django
django-ipware

pytest
pytest-cov
pytest-django
pytest-pythonpath

```

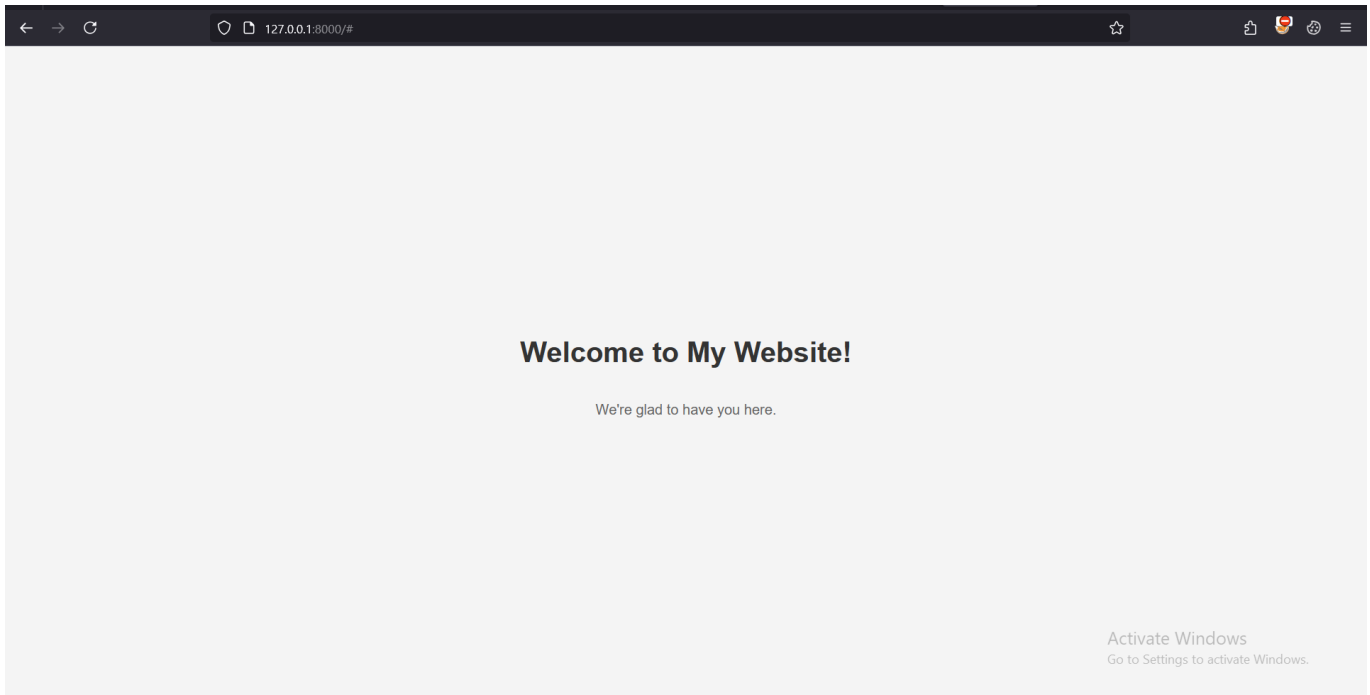
## 2. Tạo Website

Chuẩn bị một website cơ bản bằng django

```

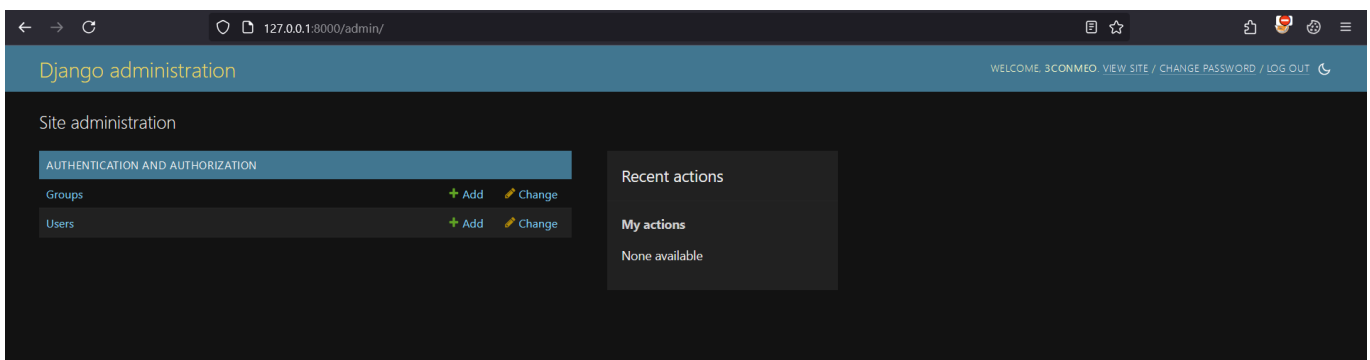
PROBLEMS  OUTPUT  DEBUG CONSOLE  TERMINAL  PORTS  2
● (django-env) nghia@nghia-pot:~/honeypot/djangohoneypot$ python -m django --version
5.1.4
● (django-env) nghia@nghia-pot:~/honeypot/djangohoneypot$ django-admin startproject honeypotsite
● (django-env) nghia@nghia-pot:~/honeypot/djangohoneypot$ cd honeypotsite/
● (django-env) nghia@nghia-pot:~/honeypot/djangohoneypot/honeypotsite$ ls
honeypotsite  manage.py
○ (django-env) nghia@nghia-pot:~/honeypot/djangohoneypot/honeypotsite$ 

```



Tạo superuser để đăng nhập vào trang admin của django

```
(django-env) nghia@nghia-pot:~/honeypot/djangohoneypot/honeypotsite$ python manage.py createsuperuser
Username (leave blank to use 'nghia'): 3conmeo
Email address:
Password:
Password (again):
This password is too short. It must contain at least 8 characters.
This password is too common.
This password is entirely numeric.
Bypass password validation and create user anyway? [y/N]: y
Superuser created successfully.
(django-env) nghia@nghia-pot:~/honeypot/djangohoneypot/honeypotsite$
```



Sau đó cài `django-admin-honeypot` như một app trên django project

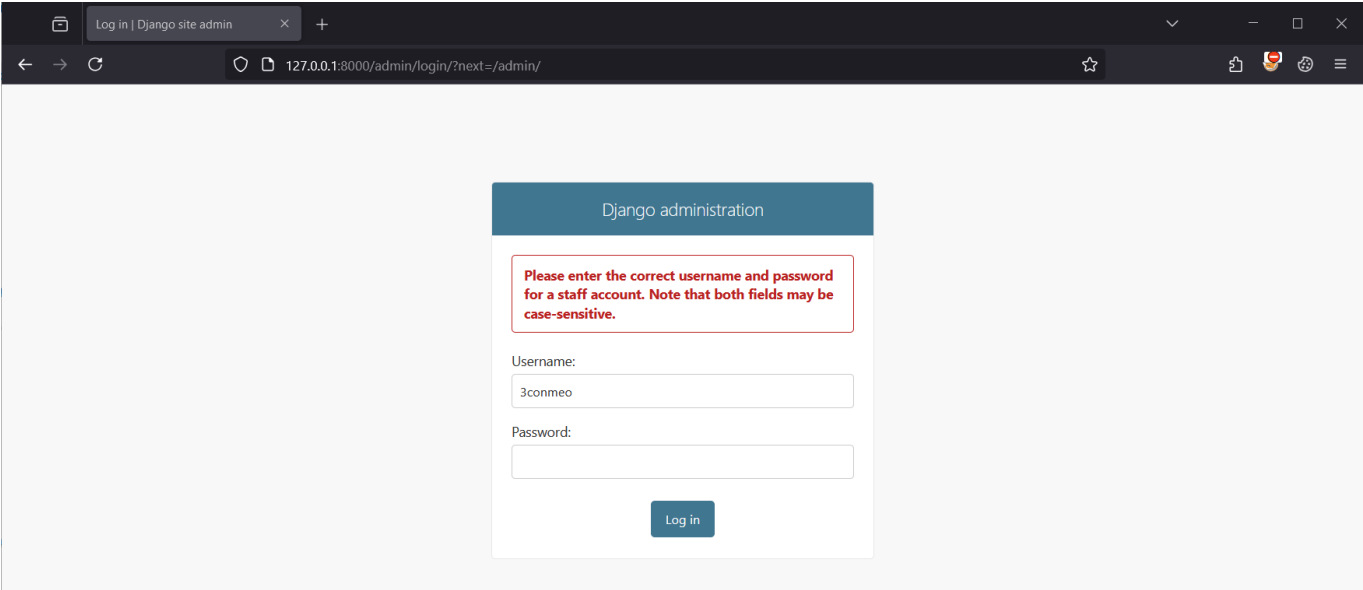
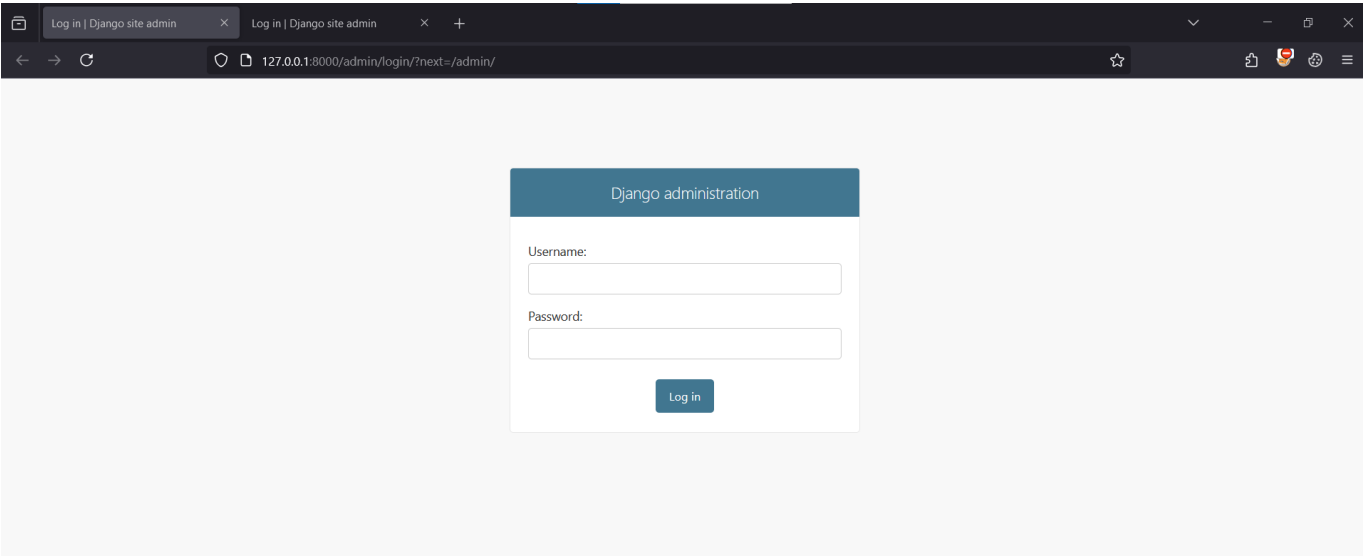
```
(django-env) nghia@nghia-pot:~/honeypot/djangohoneypot/honeypotsite$ pip install django-admin-honeypot-updated-2021
Collecting django-admin-honeypot-updated-2021
  Using cached django_admin_honeypot_updated_2021-1.2.0-py2.py3-none-any.whl
Requirement already satisfied: django>=2.2 in /home/nghia/honeypot/djangohoneypot/django-env/lib/python3.10/site-packages (from django-admin-honeypot-updated-2021) (5.1.4)
Requirement already satisfied: django-ipware in /home/nghia/honeypot/djangohoneypot/django-env/lib/python3.10/site-packages (from django-admin-honeypot-updated-2021) (7.0.1)
Requirement already satisfied: asgiref<4,>=3.8.1 in /home/nghia/honeypot/djangohoneypot/django-env/lib/python3.10/site-packages (from django-admin-honeypot-updated-2021) (3.8.1)
Requirement already satisfied: sqlparse>=0.3.1 in /home/nghia/honeypot/djangohoneypot/django-env/lib/python3.10/site-packages (from django-admin-honeypot-updated-2021) (0.5.2)
Requirement already satisfied: python-ipware>=2.0.3 in /home/nghia/honeypot/djangohoneypot/django-env/lib/python3.10/site-packages (from django-admin-honeypot-updated-2021) (3.0.0)
Requirement already satisfied: typing-extensions>=4 in /home/nghia/honeypot/djangohoneypot/django-env/lib/python3.10/site-packages (from asgiref<4,>=3.8.1->django>=2.2->django-admin-honeypot-updated-2021) (4.12.2)
Installing collected packages: django-admin-honeypot-updated-2021
Successfully installed django-admin-honeypot-updated-2021-1.2.0
```

Cấu hình để chạy `django-admin-honeypot` trên web

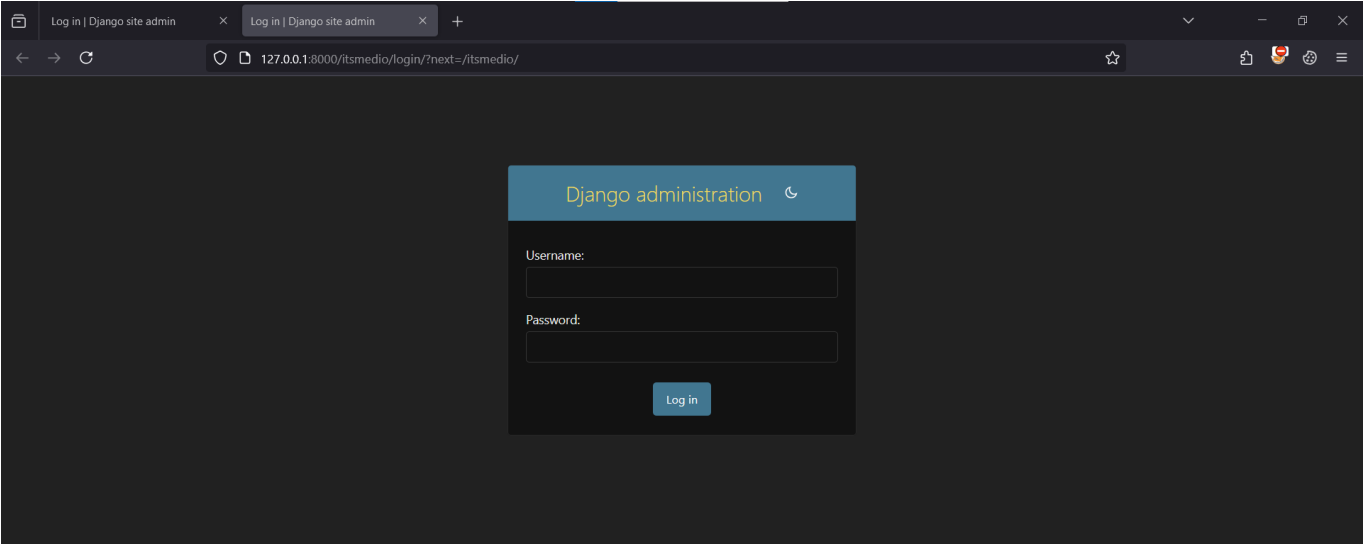
```
djangohoneypot > honeypotsite > honeypotsite > settings.py
31 # Application definition
32
33 INSTALLED_APPS = [
34     'django.contrib.admin',
35     'django.contrib.auth',
36     'django.contrib.contenttypes',
37     'django.contrib.sessions',
38     'django.contrib.messages',
39     'django.contrib.staticfiles',
40     'home',
41     'admin_honeypot'
42 ]
```

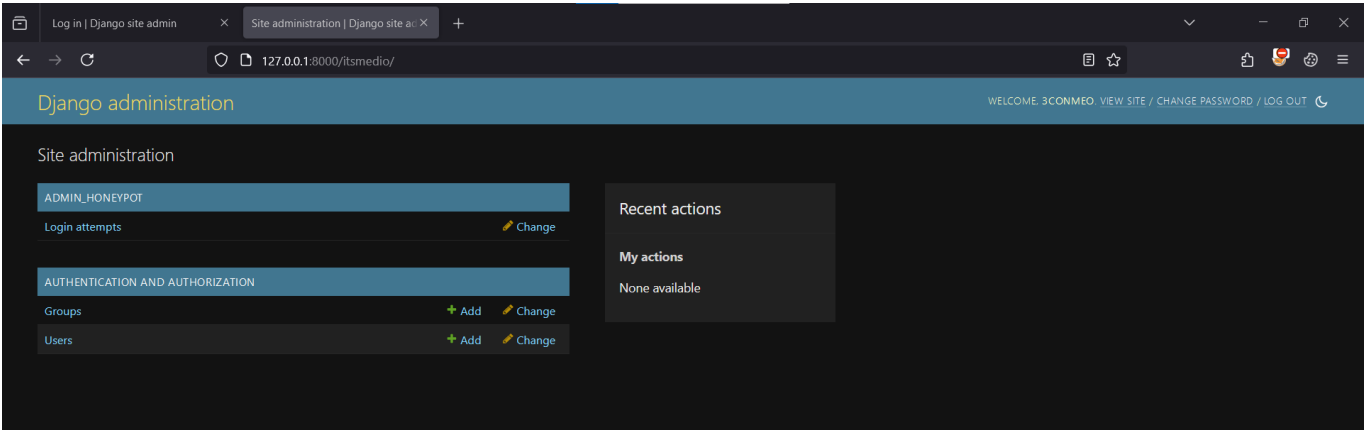
```
djangohoneypot > honeypotsite > honeypotsite > urls.py
13 including another URLCONF
14 """
15
16 from django.contrib import admin
17 from django.urls import path
18 from django.conf.urls import include
19
20
21 urlpatterns = [
22     path('admin/', include('admin_honeypot.urls', namespace='admin_honeypot')),
23     path('itsmedio/', admin.site.urls), # real admin page
24     path('', include('home.urls'))
25 ]
26
```

Trang giả



Trang thật

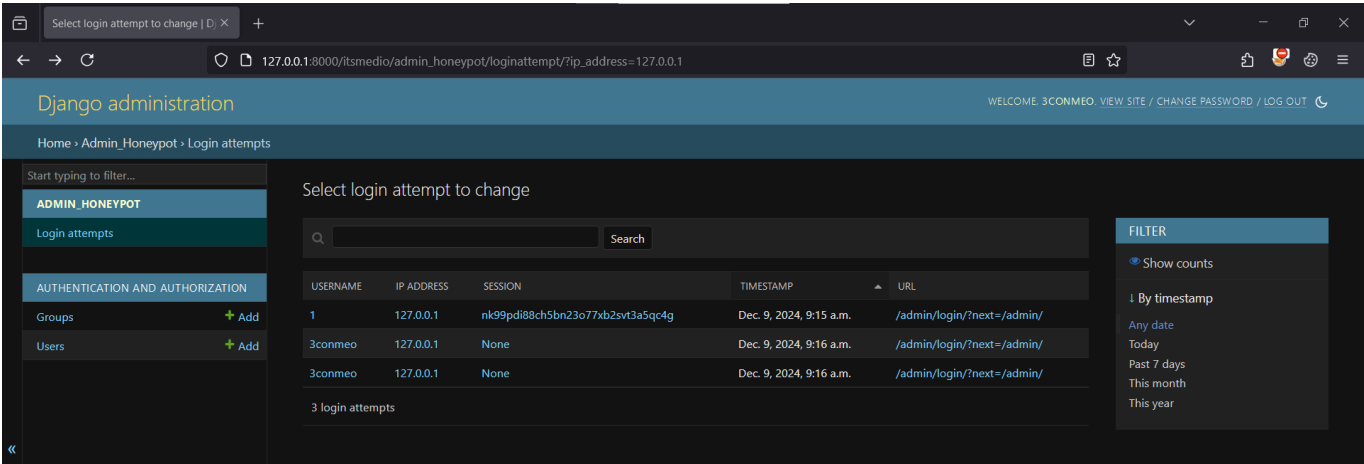
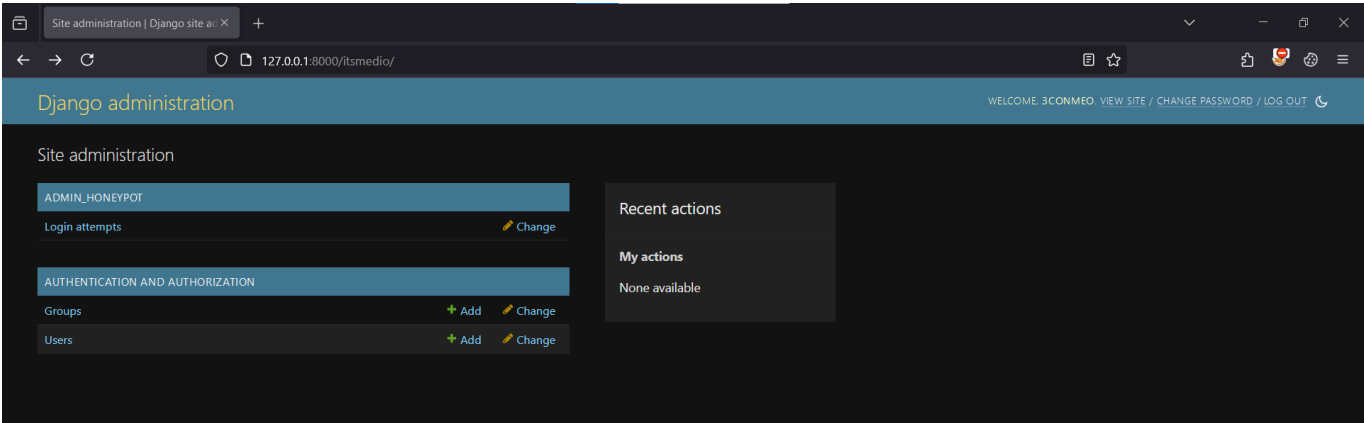


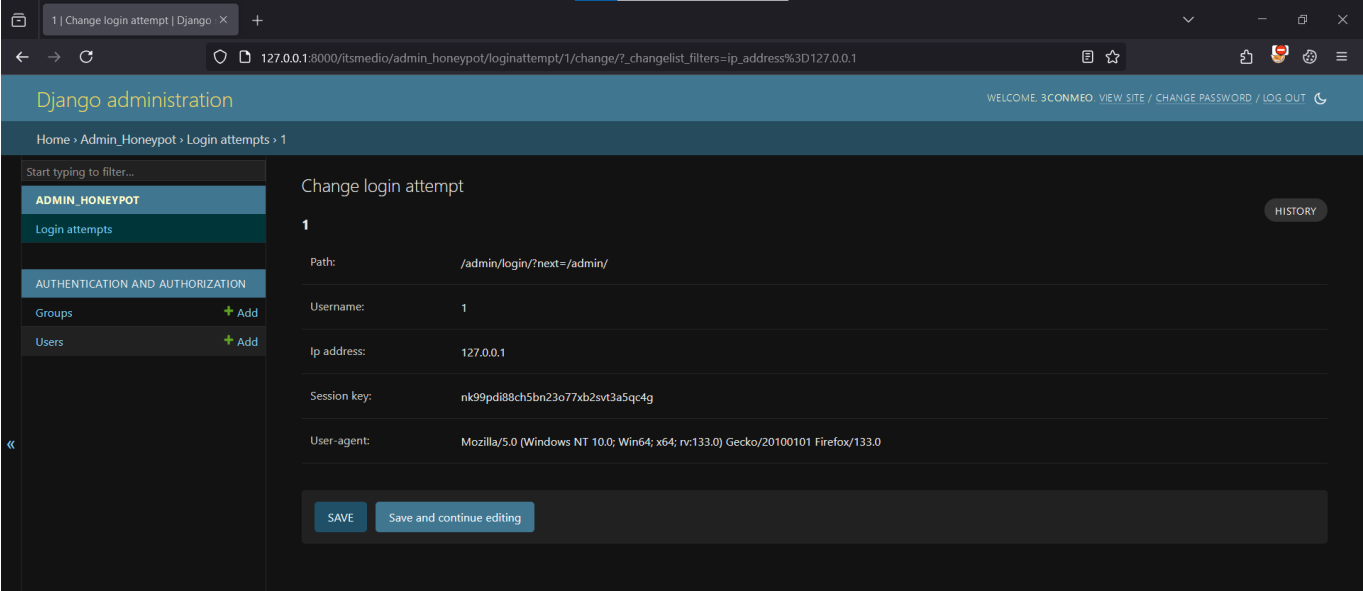


Cho dù ta có nhập đúng credential cũng sẽ không vào được trang giả

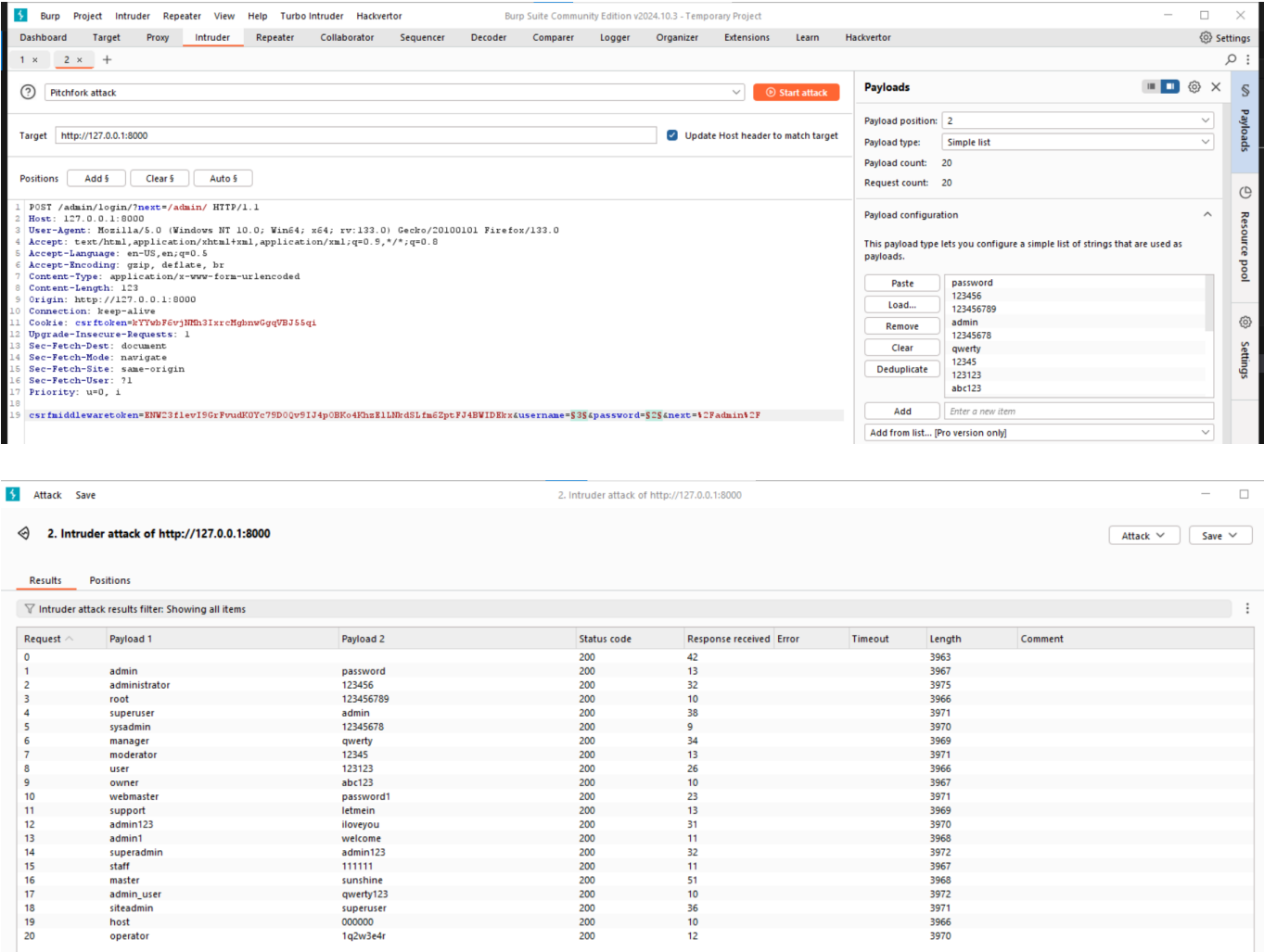
Tấn công

Sau khi cài đặt xong ta thử 1 số credential và tất cả request sẽ được logs lại ở trang admin thật





Chuẩn bị tấn công bằng BurpSuite



Select login attempt to change | D | X

127.0.0.1:8000/itsmedio/admin\_honeypot/loginattempt/

Start typing to filter...	3	127.0.0.1	None	Dec. 9, 2024, 9:45 a.m.	/admin/login?next=/admin/
ADMIN_HONEYPOT	admin	127.0.0.1	None	Dec. 9, 2024, 9:45 a.m.	/admin/login?next=/admin/
Login attempts	administrator	127.0.0.1	None	Dec. 9, 2024, 9:45 a.m.	/admin/login?next=/admin/
	root	127.0.0.1	None	Dec. 9, 2024, 9:45 a.m.	/admin/login?next=/admin/
AUTHENTICATION AND AUTHORIZATION	superuser	127.0.0.1	None	Dec. 9, 2024, 9:45 a.m.	/admin/login?next=/admin/
Groups + Add	sysadmin	127.0.0.1	None	Dec. 9, 2024, 9:45 a.m.	/admin/login?next=/admin/
Users + Add	manager	127.0.0.1	None	Dec. 9, 2024, 9:45 a.m.	/admin/login?next=/admin/
	moderator	127.0.0.1	None	Dec. 9, 2024, 9:45 a.m.	/admin/login?next=/admin/
	user	127.0.0.1	None	Dec. 9, 2024, 9:45 a.m.	/admin/login?next=/admin/
	owner	127.0.0.1	None	Dec. 9, 2024, 9:45 a.m.	/admin/login?next=/admin/
	webmaster	127.0.0.1	None	Dec. 9, 2024, 9:45 a.m.	/admin/login?next=/admin/
	support	127.0.0.1	None	Dec. 9, 2024, 9:45 a.m.	/admin/login?next=/admin/
	admin123	127.0.0.1	None	Dec. 9, 2024, 9:45 a.m.	/admin/login?next=/admin/
	admin1	127.0.0.1	None	Dec. 9, 2024, 9:45 a.m.	/admin/login?next=/admin/
	superadmin	127.0.0.1	None	Dec. 9, 2024, 9:45 a.m.	/admin/login?next=/admin/
	staff	127.0.0.1	None	Dec. 9, 2024, 9:45 a.m.	/admin/login?next=/admin/
	master	127.0.0.1	None	Dec. 9, 2024, 9:45 a.m.	/admin/login?next=/admin/
	admin_user	127.0.0.1	None	Dec. 9, 2024, 9:45 a.m.	/admin/login?next=/admin/
	siteadmin	127.0.0.1	None	Dec. 9, 2024, 9:45 a.m.	/admin/login?next=/admin/
	host	127.0.0.1	None	Dec. 9, 2024, 9:45 a.m.	/admin/login?next=/admin/
	operator	127.0.0.1	None	Dec. 9, 2024, 9:45 a.m.	/admin/login?next=/admin/
25 login attempts					

Activate Windows  
Go to Settings to activate Windows.