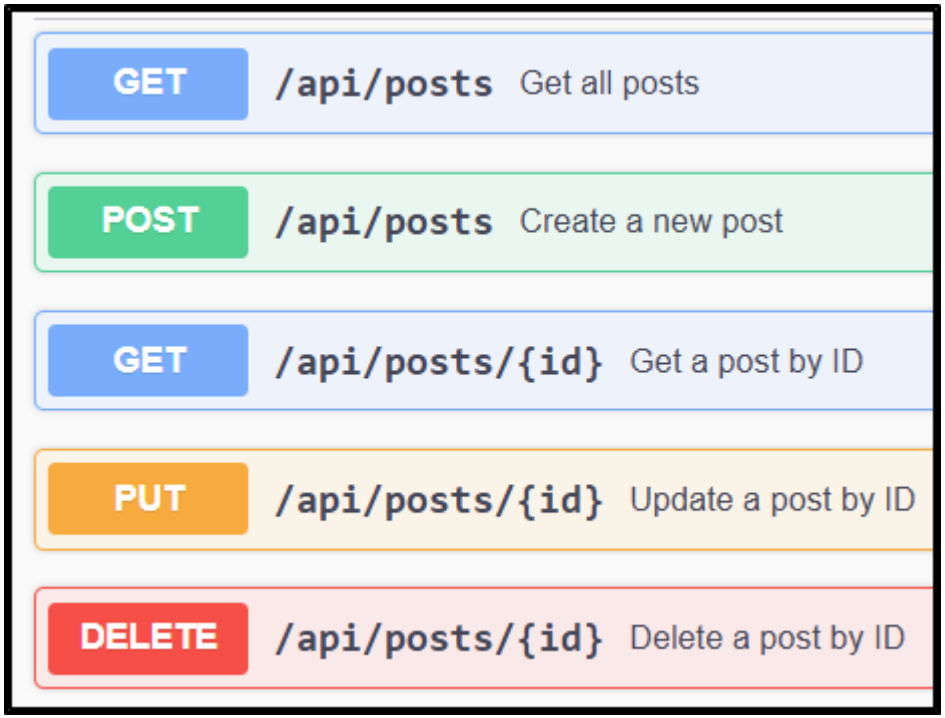
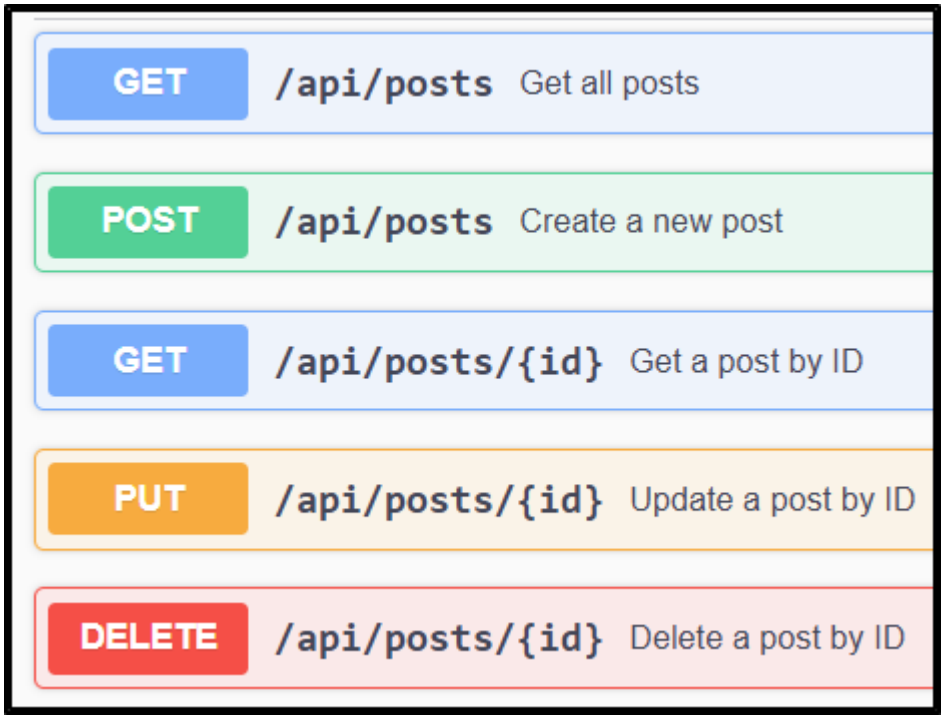
ApiBase – Web App APIs

Web app's often incorporate APIs as part of their function. API stands for “application programming interface”, and they allow the web apps to interface with each other



ApiBase – Web App APIs

APIs use standard HTTP methods to specified app endpoints to perform different functions, such as creating app users, or editing user details



ApiBase – API Documentation


```
{
  "message": "No endpoint selected. Please use /add to add
a user or /users to query users."
}
```


Web app APIs often include documentation within the app, and this app's landing page indicates there are the `/add` and `/users` endpoints

ApiBase – Testing Endpoints

We want to test the Api endpoints to see how they work. The `/add` endpoint doesn't use regular GET requests

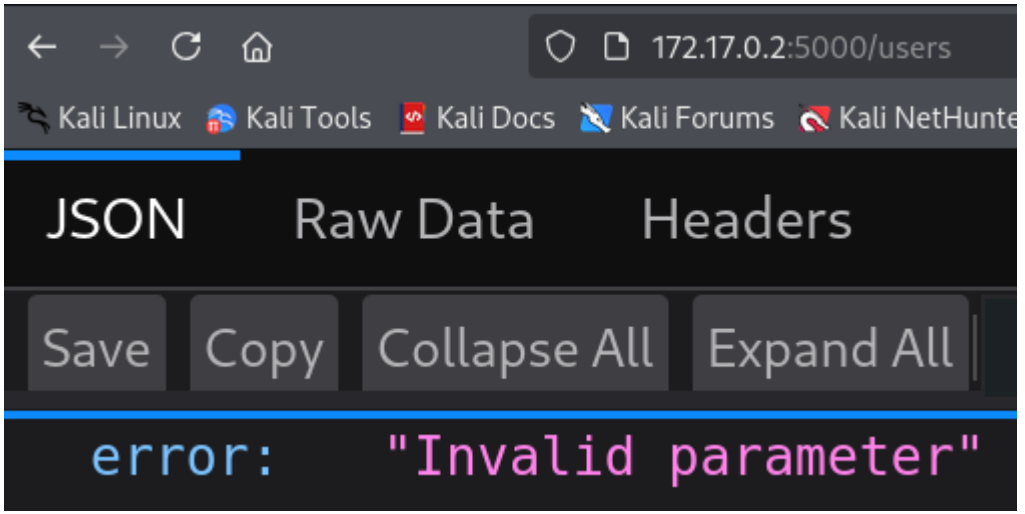
ApiBase – Testing Endpoints

```
10 Content-Length: 27
11
12 username=theshyhat&password=hackerfrogs
```

```
{
    "message":"User added"
}
```

Typically, when you add a user to a system, you send a POST request to the web app which includes the username and password

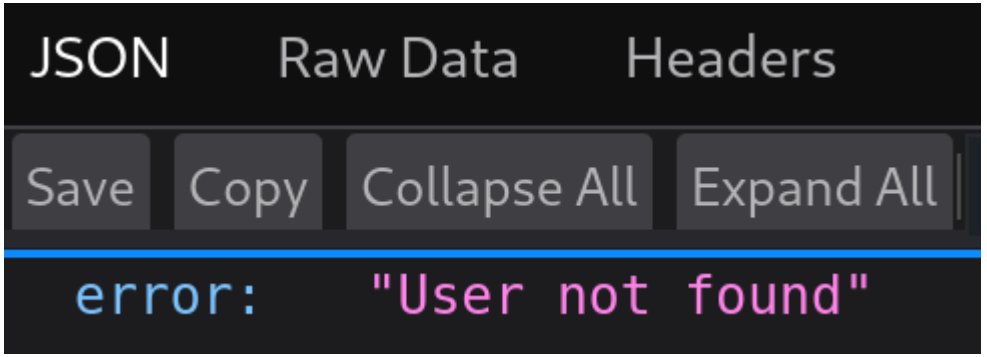
ApiBase – Testing Endpoints



The other endpoint we can test is the `/users` endpoint. The endpoint seems to want a specific URL parameter, which we can fuzz for

ApiBase – Testing Endpoints

```
username                    [Status: 404, Size: 32,
:: Progress: [6453/6453] :: Job [1/1] :: 990 re
```



We discover that the parameter the app is looking for is `username`, and because we know that, we can fuzz for valid usernames

ApiBase – Testing Endpoints

```
pingu                   [Status: 200,
can'tremember           [Status: 500,
```

```
[
  2,
  "pingu",
  "pinguinasio"
]
```

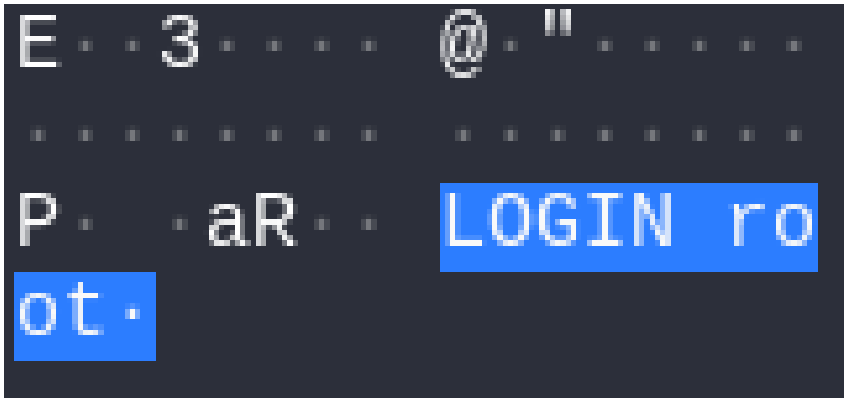
Through fuzzing, we discover a valid username on the system, and the entry includes the user's password

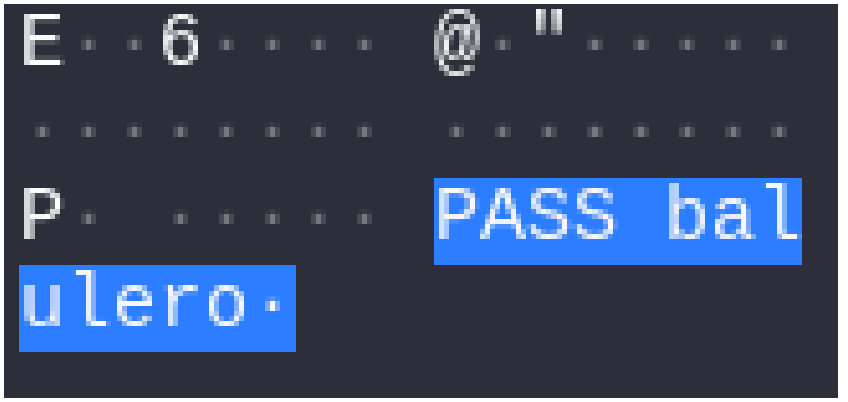
Privilage Escalation: Exposed Credentials in PCAP File

```
drwxr-xr-x 1 root  root  4096 Feb 27 08:47 .
drwxr-xr-x 1 root  root  4096 Aug  6 16:25 ..
-rw-r--r-- 1 root  root  1631 Feb 27 08:47 app.py
-rw-r--r-- 1 root  root   399 Feb 27 08:45 network.pcap
drwxr-xr-x 2 pingu pingu 4096 Feb 27 08:36 pingu
-rw-r--r-- 1 root  root  8192 Feb 27 08:16 users.db
```

There is a PCAP file located in the `/home` directory

Privilage Escalation: Exposed Credentials in PCAP File





When downloaded and examined, we see that it contains the credentials for the root user