Kalle Jalkanen AB8822
time used: 2 hours

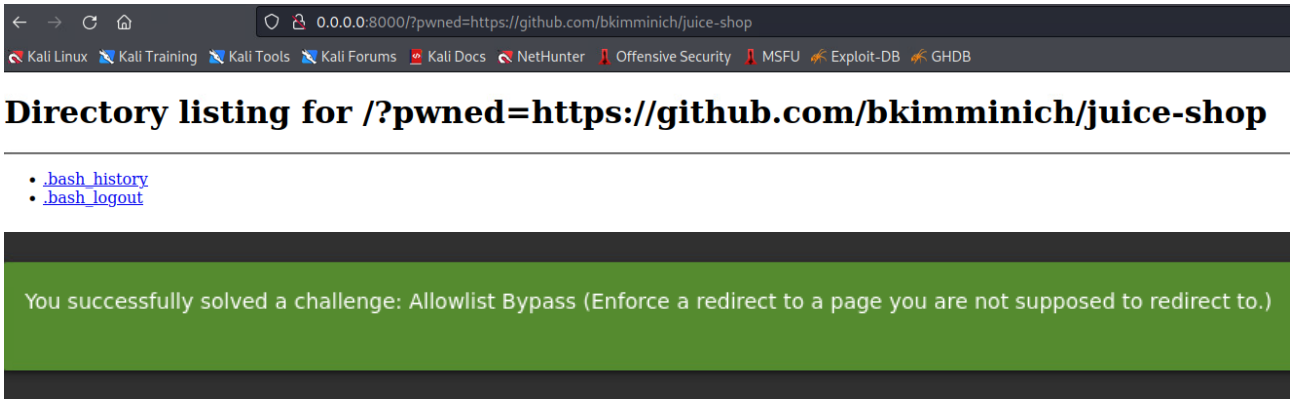
Juice Shop - Allowlist bypass

Description

You can redirect to another address from juice shop.

Steps to produce

After juice chop's URL add
'/redirect?to=http://0.0.0.0:8000?pwned=https://github.com/bkimminich/juice-shop'.
Replace http://0.0.0.0:8000 with your preferred address.



Impact estimation

Low severity. This only redirect user to another URL. There are no direct impacts to the website, but this can be door to other attack types like phishing attacks or to steal OAuth token.

Mitigation

Easy fix for this is that you whitelist allowed redirection URLs. More information about URR redirection vulnerabilities at https://www.virtuesecurity.com/kb/url-redirection-attack-and-defense/ .

Main target - Deserialization of Untrusted Data

Create python script.

```
  GNU nano 7.2                                                  test.py
import pickle

# Create a simple Python object (e.g., a dictionary)
data = {"message": "häläpätihämmää"}

# Serialize the object using pickle
payload = pickle.dumps(data)

# Encode the serialized payload in Base64 for URL encoding
import base64
encoded_payload = base64.urlsafe_b64encode(payload).decode()

# Print the encoded payload
print("data=" + encoded_payload)
```

Run it with command ‘python3 test.py’. Copy that encoded text and paste it to next command.
curl -X POST -d "data=<your_encoded_payload>" http://wasdat.fi/api/import

```
┌──(kali㉿kali-vle)-[~/webw8]
└─$ python3 test.py
data=gASVJQAAAAAAAAB9lIwHbWVzc2FnZSMFGjDpGzDpHDDpHRpaMOkbW3DpMOklHMu

┌──(kali㉿kali-vle)-[~/webw8]
└─$ curl -X POST -d "data=gASVJQAAAAAAAAB9lIwHbWVzc2FnZSMFGjDpGzDpHDDpHRpaMOkbW3DpMOklHMu" http://wasdat.fi/api/
import
{"message":"häläpätihämmää"}
```