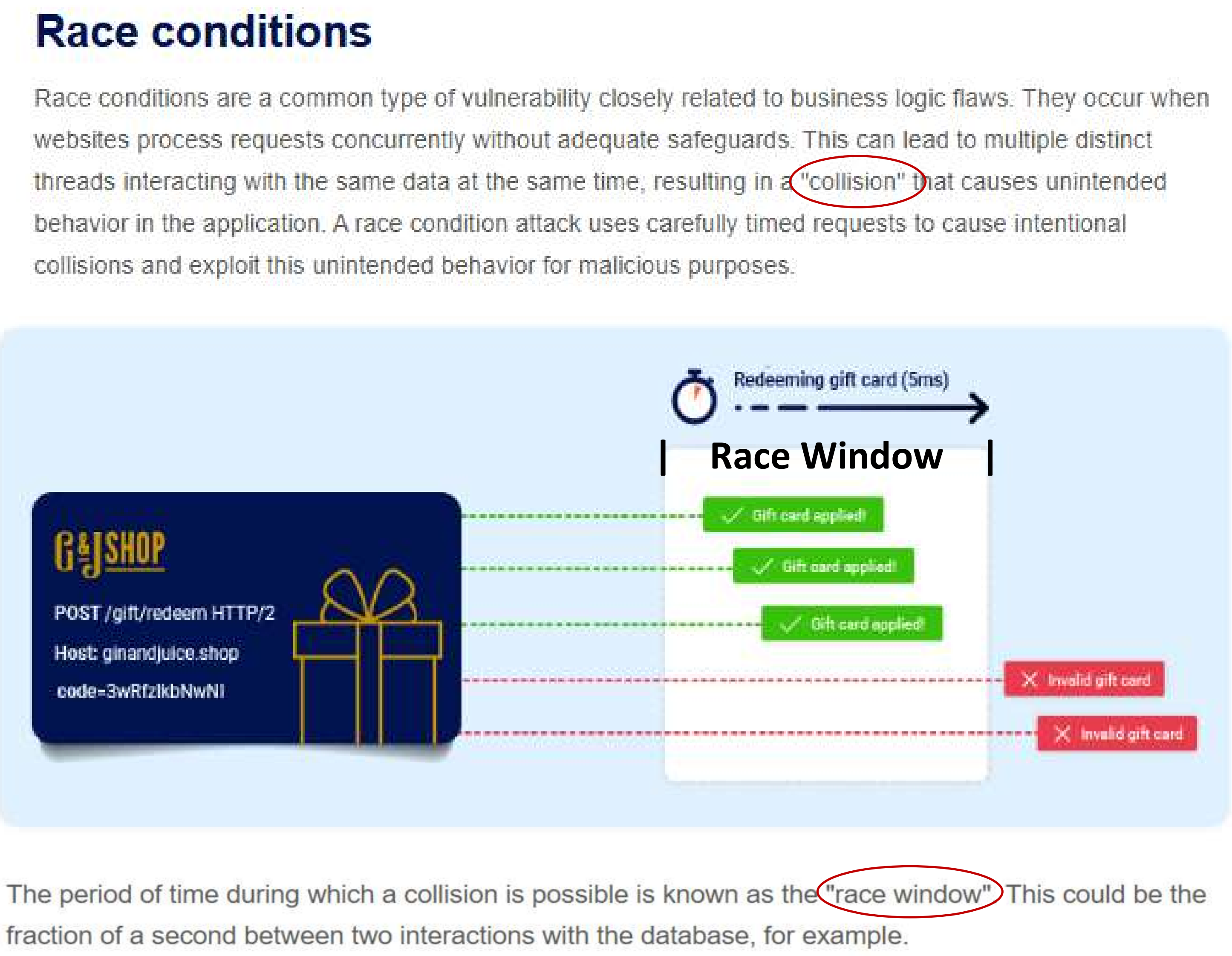
TURKISH TECHNOLOGY

Race conditions

Race conditions

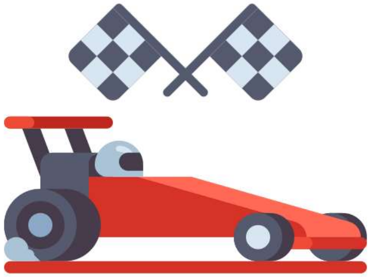


Race conditions

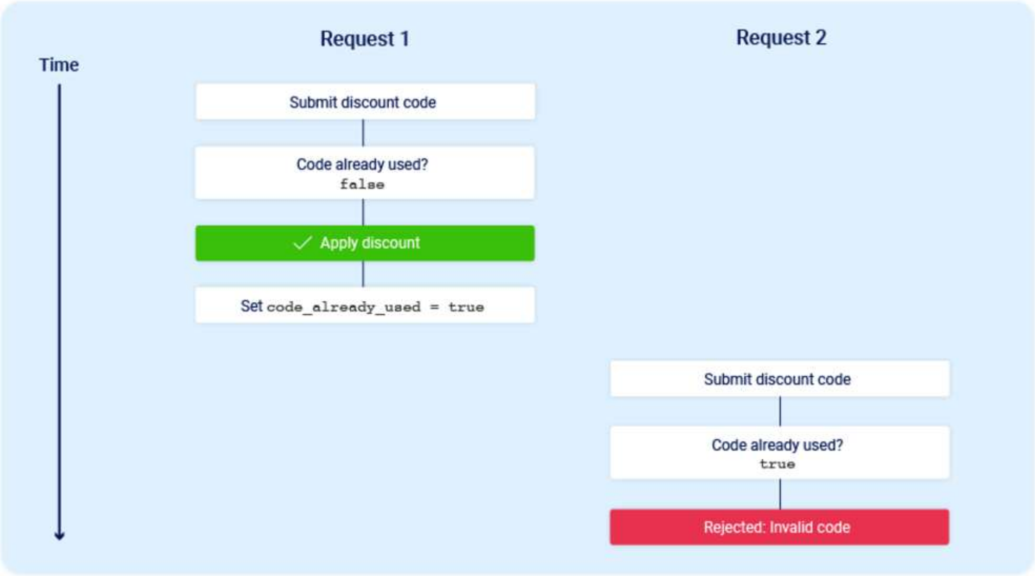
Race conditions are a common type of vulnerability closely related to business logic flaws. They occur when websites process requests concurrently without adequate safeguards. This can lead to multiple distinct threads interacting with the same data at the same time, resulting in a "collision" that causes unintended behavior in the application. A race condition attack uses carefully timed requests to cause intentional collisions and exploit this unintended behavior for malicious purposes.

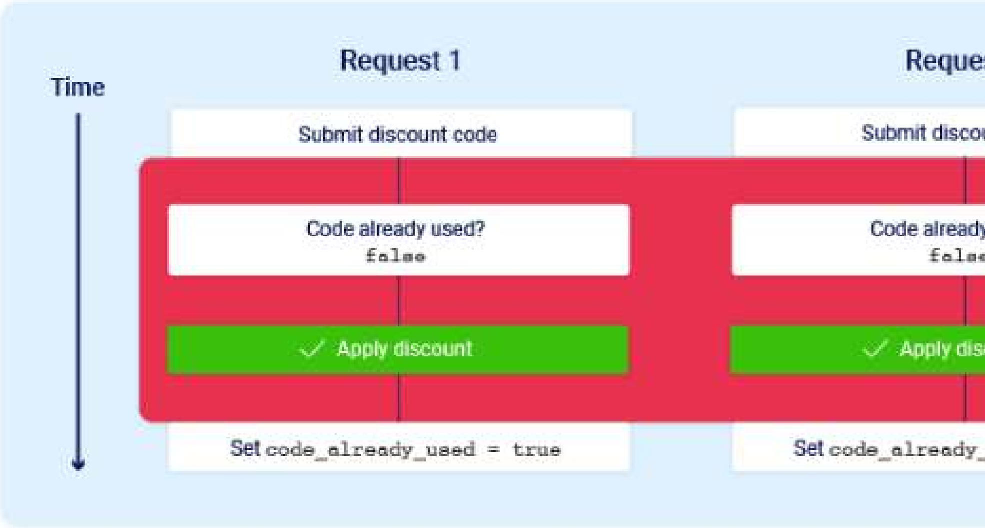
```
POST /gift/redeem HTTP/2
Host: ginandjuice.shop
code=3wRfzlkbNwNl
```

The period of time during which a collision is possible is known as the "race window". This could be the fraction of a second between two interactions with the database, for example.



Race conditions

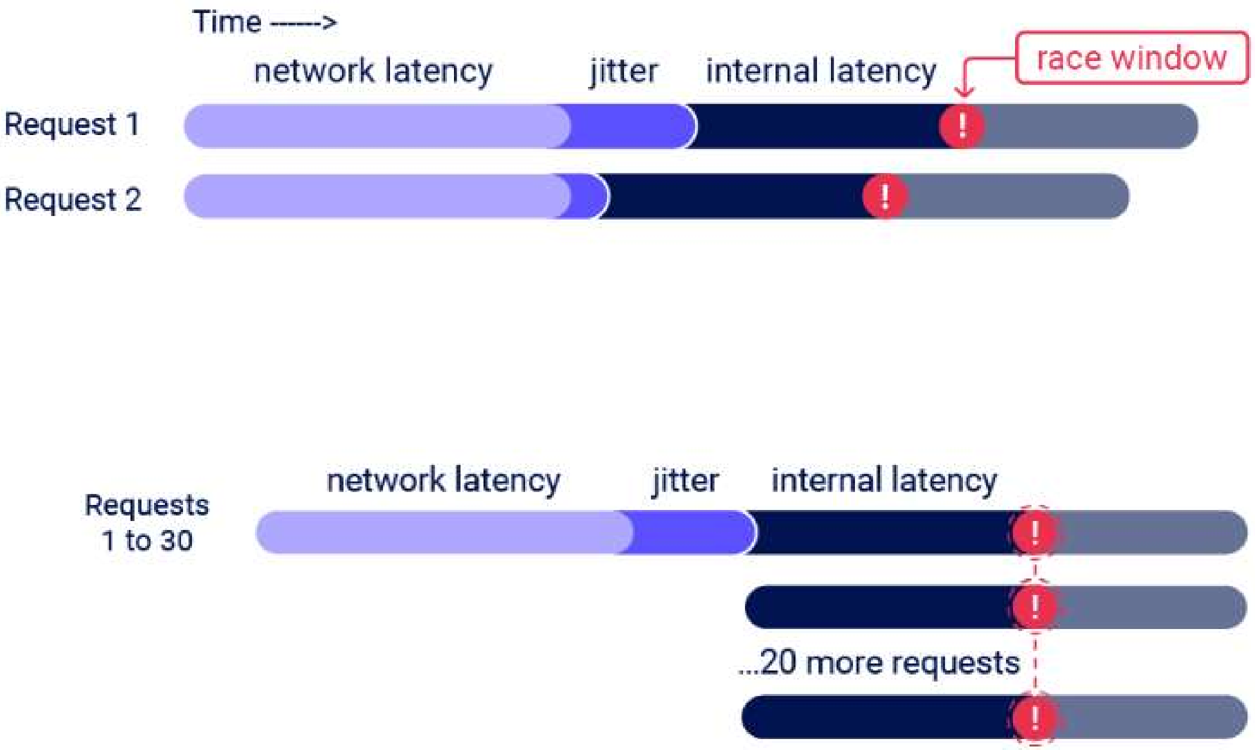


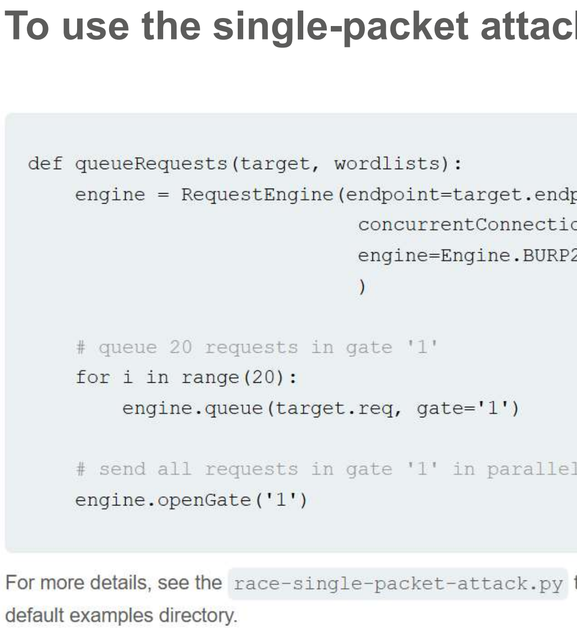


Bazı Saldırı Türleri:

•Redeeming a gift card multiple times
•Rating a product multiple times
•Withdrawing or transferring cash in excess of your account balance
•Reusing a single CAPTCHA solution
•Bypassing an anti-brute-force rate limit

Race conditions





To use the single-packet attac

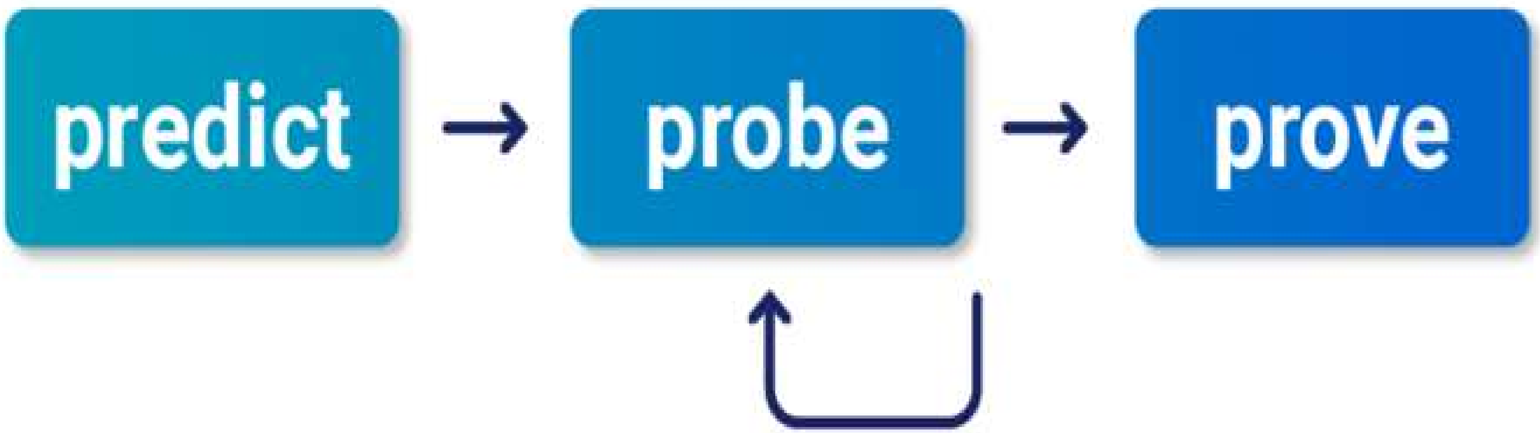
```
def queueRequests(target, wordlists):
    engine = RequestEngine(endpoint=target.endp
                           concurrentConnectic
                           engine=Engine.BURP2
                           )

    # queue 20 requests in gate '1'
    for i in range(20):
        engine.queue(target.req, gate='1')

    # send all requests in gate '1' in parallel
    engine.openGate('1')
```

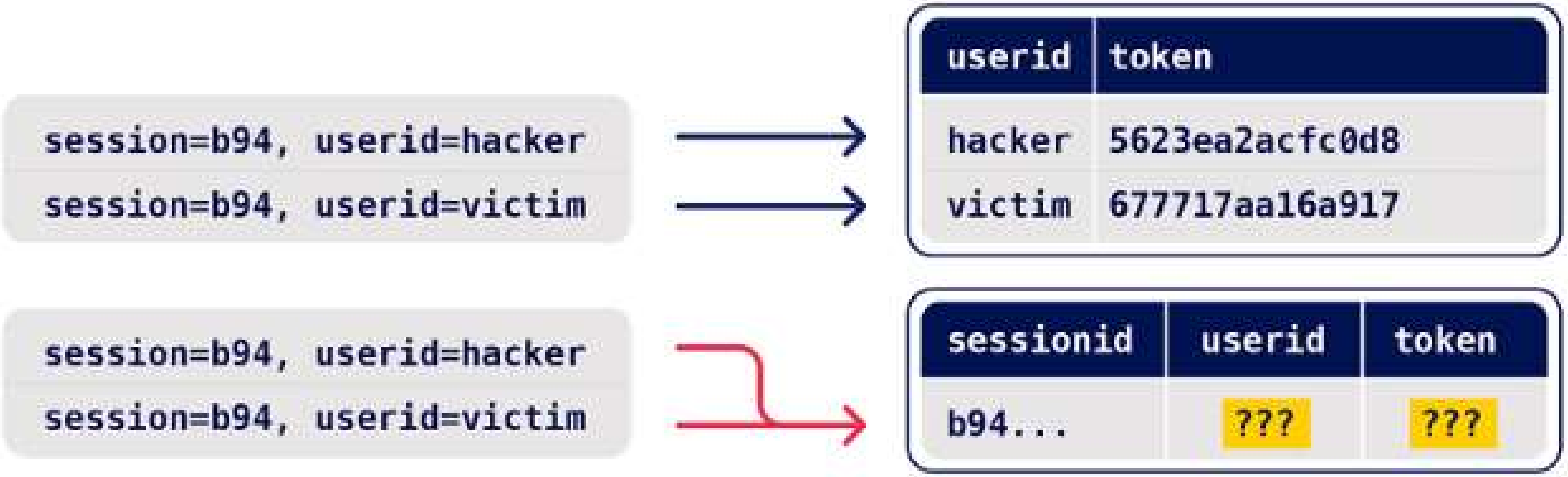
For more details, see the `race-single-packet-attack.py`
default examples directory.

Methodology



predict → probe → prove

Çakışma Tahmin



```
session=b94, userid=hacker
session=b94, userid=victim
```

userid	token
hacker	5623ea2acfc0d8
victim	677717aa16a917

```
session=b94, userid=hacker
session=b94, userid=victim
```

sessionid	userid	token
b94...	???	???

İp Ucu Yakalamak

- İstekleri sırayla göndermek
- İstekleri paralel olarak göndermek
- single-packet saldırısı

Kanıt Aşaması

Race window’dan yararla condition durumundan fay etmek

LABS

Web Security Academy

All Race conditions Labs

https://portswigger.net/web-security/all-labs#ra

How to prevent race condition vulnerabilities

- Verinin farklı depolama alanlarında barındırılmasından kaçınm

- Örnek olarak ödeme işlemleri ve buna bağlı indirim vb işlemle için tek bir veritabanı kullanmak

- Bir veri depolama katmanını diğerini güvenli kılmak için kullanmamak.

- JWT tarzı client side stat tutan yapılar kullanılabilir. JWT’nin kullanımı ile gelen farklı zafiyetler de olabilir.

WIDEN YOUR WORLD

TURKISH AIRLINES