#DC604 Hacker Summer Camp | Lightning Talks - 2 | Ads (GangGreenTemperTatum)

Smashing the state machine: the true potential of web race conditions

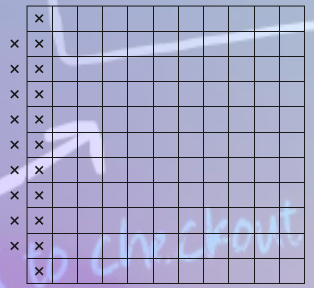
James Kettle | Portswigger

Defcon | BlackHat | Nullcon

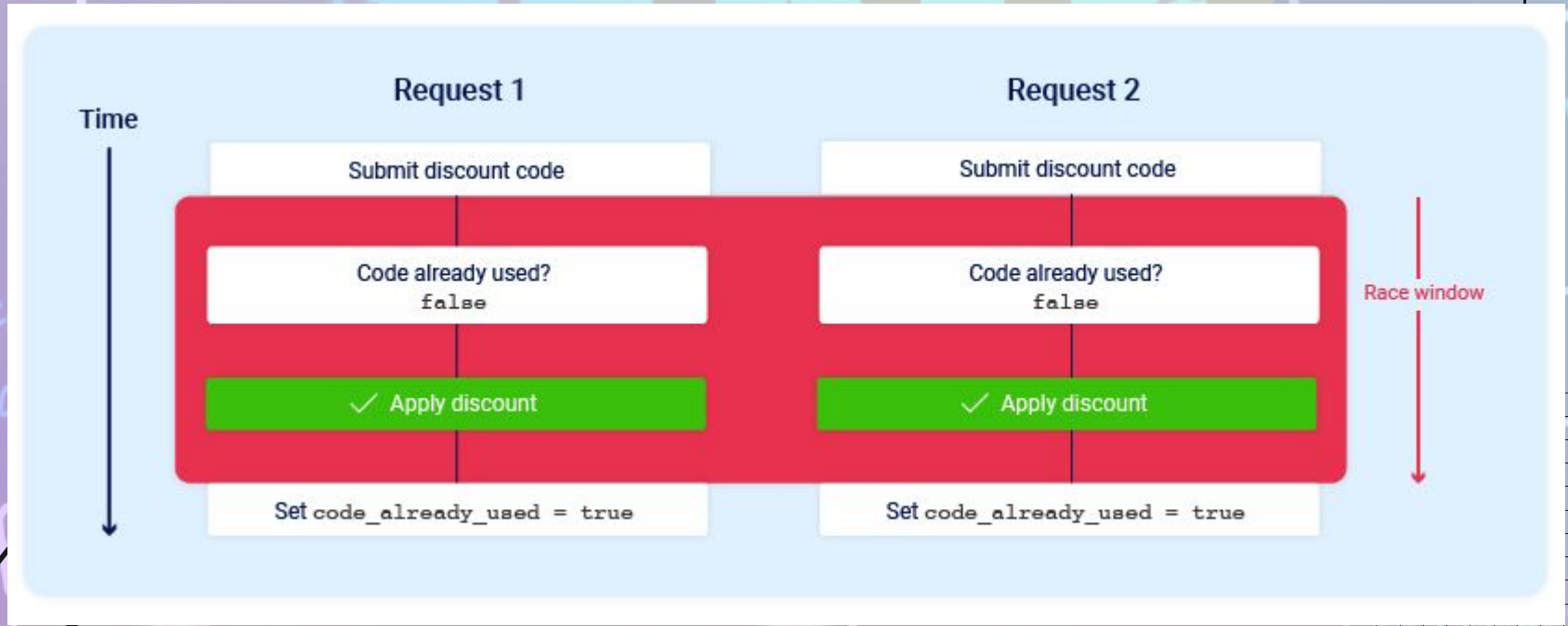
01

What is a Web Race Condition?

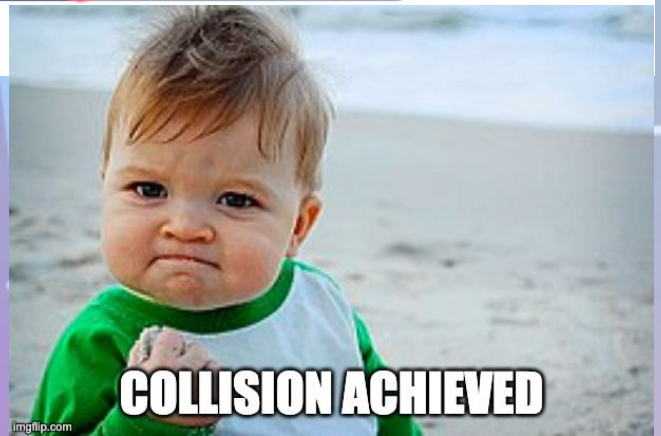
James Kettle | Portswigger



Example of a Race Window



External Effects on a Race Window



Wait, but How?

The Portswigger **Single Packet Attack**

Turbo Intruder: Embracing the billion-request attack

02

Limit-Overrun (A Class of Web Race Condition)

"time-of-check to time-of-use" (TOCTOU) flaws

Race conditions thrive on complexity

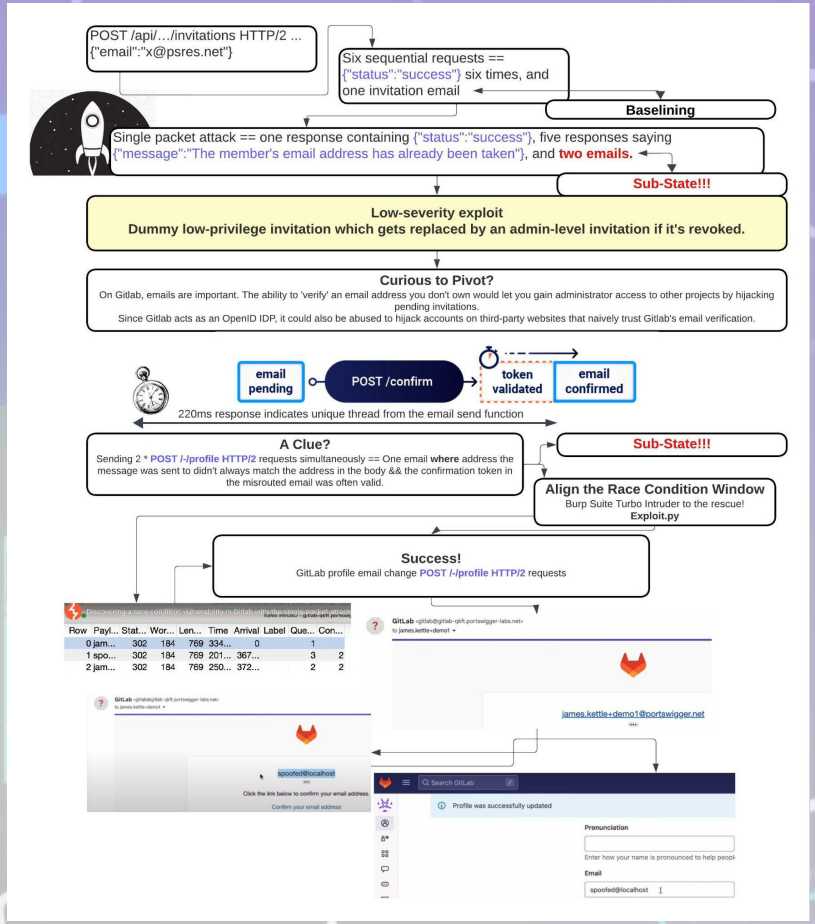
Victim	Attacker

`if (access("file", W_OK) != 0) {`
`  exit(1);`
`}`
 	
`fd = open("file", O_WRONLY);`
`// Actually writing over /etc/passwd`
`write(fd, buffer, sizeof(buffer));`
	`//`
	`//`
	`// After the access check`
	`symlink("/etc/passwd", "file");`
	`// Before the open, "file" points to the password database`
	`//`
	`//`

How Can This Be Further Exploited?

Object masking via limit-overrun - GitLab Case Study

```
POST /api/…/invitations HTTP/2 ... {"email":"x@psres.net"}
```



Thanks! Questions?

Social: Twitter, Bluesky, Mastodon, LinkedIn, PortSwigger
Contact: albinowax@gmail.com or james.kettle@portswigger.net

https://jameskettle.com/