XSS Defense in Depth

@me

Security Engineer @ emarsys

Software craftsman

Promoting security through training

siege corridor

watch towers

portcullis

soldiers

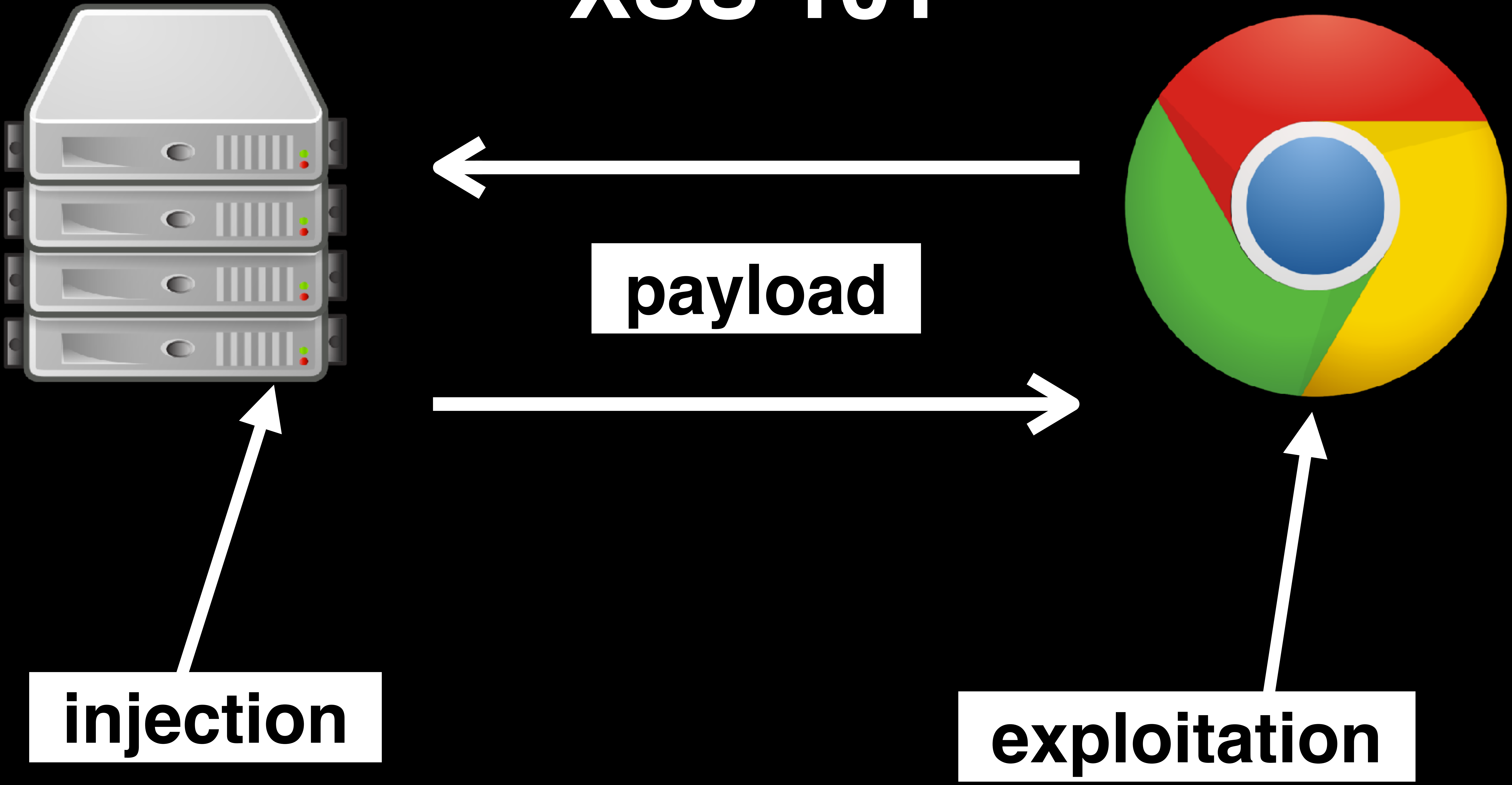
portholes

walls

moat

gate bridge

XSS 101



payload

injection

exploitation

HANDS-ON

`xss.lappfold.com:8080`

Injection countermeasures

Web application firewall

Rejecting input

Sanitizing input

Correctly encoding the output

Exploitation countermeasures

Browser XSS auditor

Content Security Policy

Utilizing the same origin policy

Sub-resource Integrity

Real world example

Reject invalid input

Use correct encoding when rendering

Utilize the browser's XSS auditor

Utilize Content Security Policy

Separate domains for user content

Utilize SRI

want more?

https://git.io/vdydK

www.securitydrops.com