Server-Side Request Forgery (SSRF)
The community push to the OWASP Top 10

QUANTUM SECURITY | WWW.QUANTUMSECURITY.CO.NZ

Thank You to Our Sponsors and Hosts!

OWASP
NEW
ZEALAND
owasp.org.nz

QUANTUM
SECURITY

AUT

CyberCX

DATACOM

snyk

Auth0

Checkmarx

HCL AppScan

kordia®

LATERAL
SECURITY

MICRO®
FOCUS

Pulse Security
www.pulsesecurity.co.nz

RedShield

Flux

SEQA™
Information Security

Cobalt

LACEWORK.

SecureFlag

Without them, OWASP New Zealand Day couldn't happen

QUANTUM SECURITY

NICK LAUDER | NICK@QUANTUMSECURITY.CO.NZ

Next 30 Minutes

① What is SSRF

② OWASP Top 10

③ Impact

④ Mitigation

QUANTUM SECURITY

Server-Side Request Forgery

Server-Side

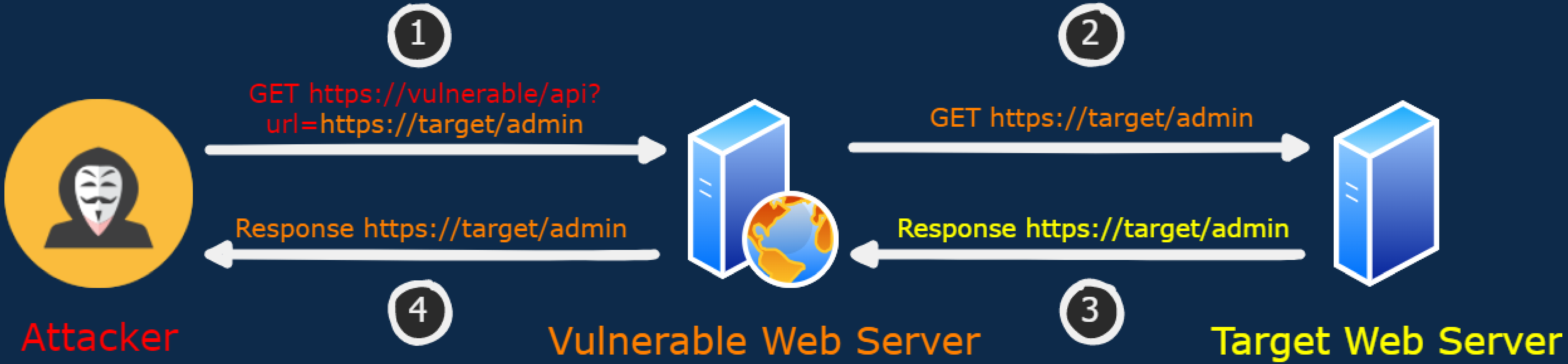
Operations performed by the server

Request Forgery

Targets unintended resources

QUANTUM
SECURITY

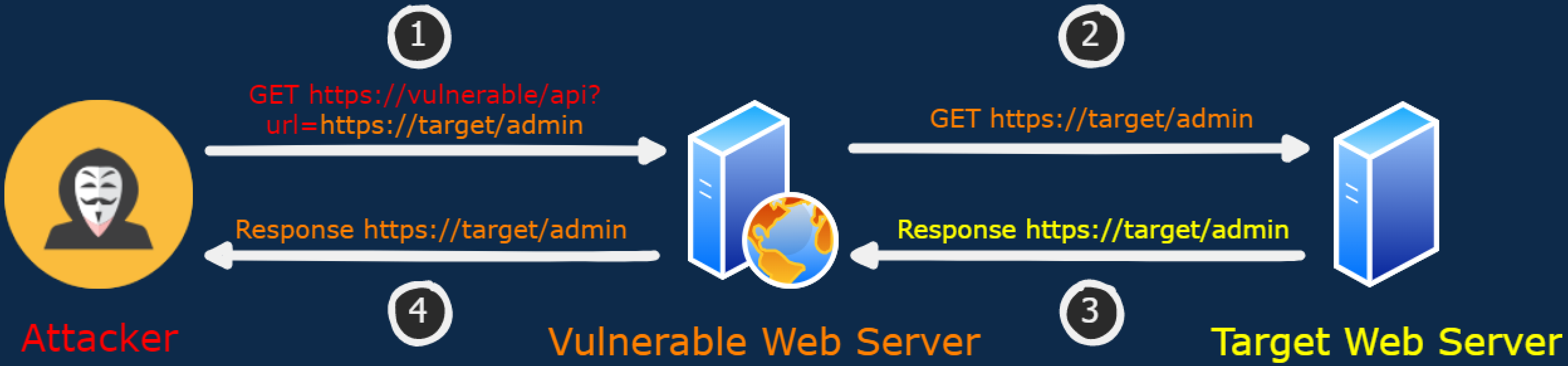
How it works



QUANTUM SECURITY

Exploit

1. Attacker sends target server URL to vulnerable server
2. Vulnerable server generates request to target server
3. Target server responds to vulnerable server
4. Vulnerable server forwards response to attacker

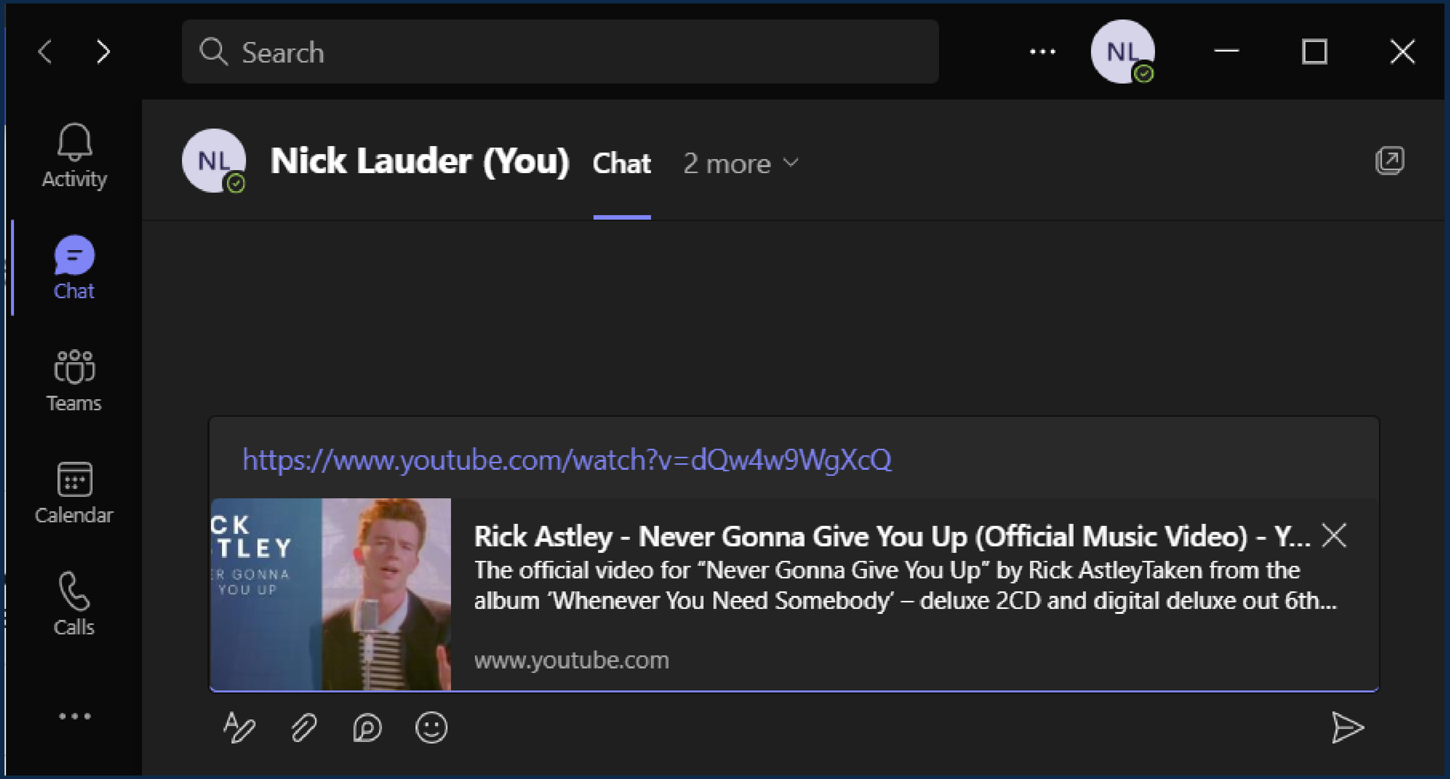

1
GET https://vulnerable/api?url=https://target/admin
2
GET https://target/admin
Response https://target/admin
Response https://target/admin
4
3
Attacker
Vulnerable Web Server
Target Web Server

QUANTUM SECURITY

Examples In Action

QUANTUM SECURITY

Microsoft Teams link preview



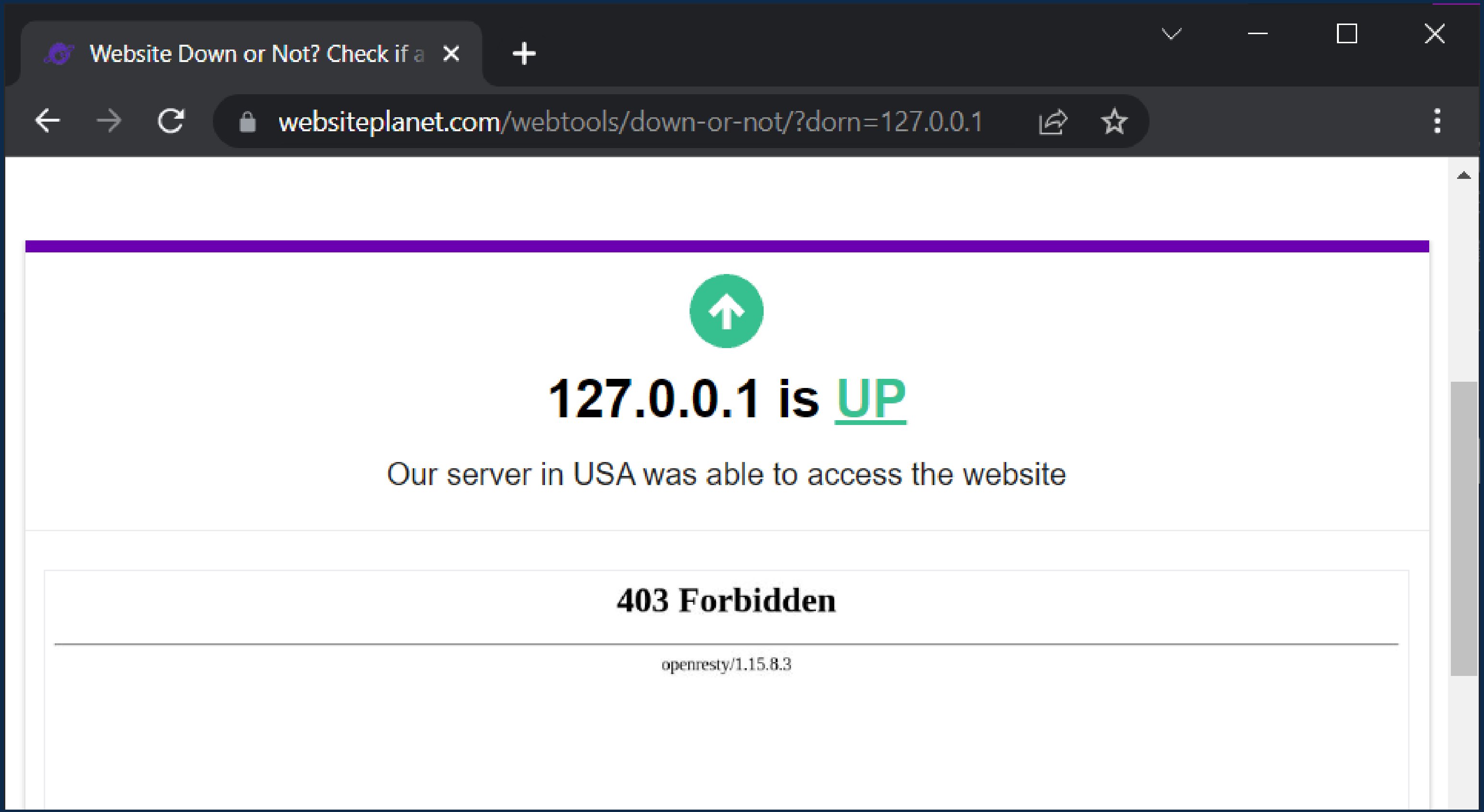
https://www.youtube.com/watch?v=dQw4w9WgXcQ

Rick Astley - Never Gonna Give You Up (Official Music Video) - Y...

The official video for “Never Gonna Give You Up” by Rick AstleyTaken from the album ‘Whenever You Need Somebody’ – deluxe 2CD and digital deluxe out 6th...

www.youtube.com

Website down checkers



Website Down or Not? Check if a

websiteplanet.com/webtools/down-or-not/?dorn=127.0.0.1

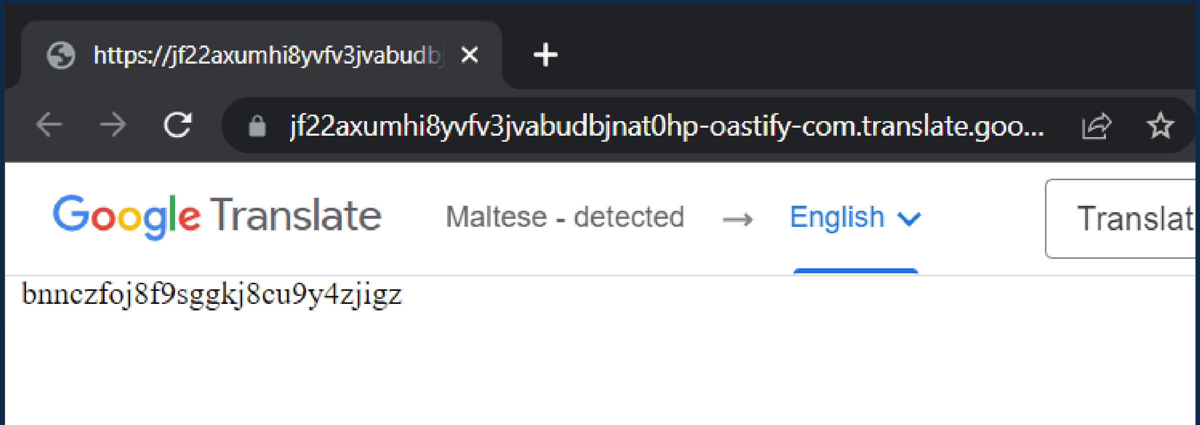
127.0.0.1 is UP

Our server in USA was able to access the website

403 Forbidden

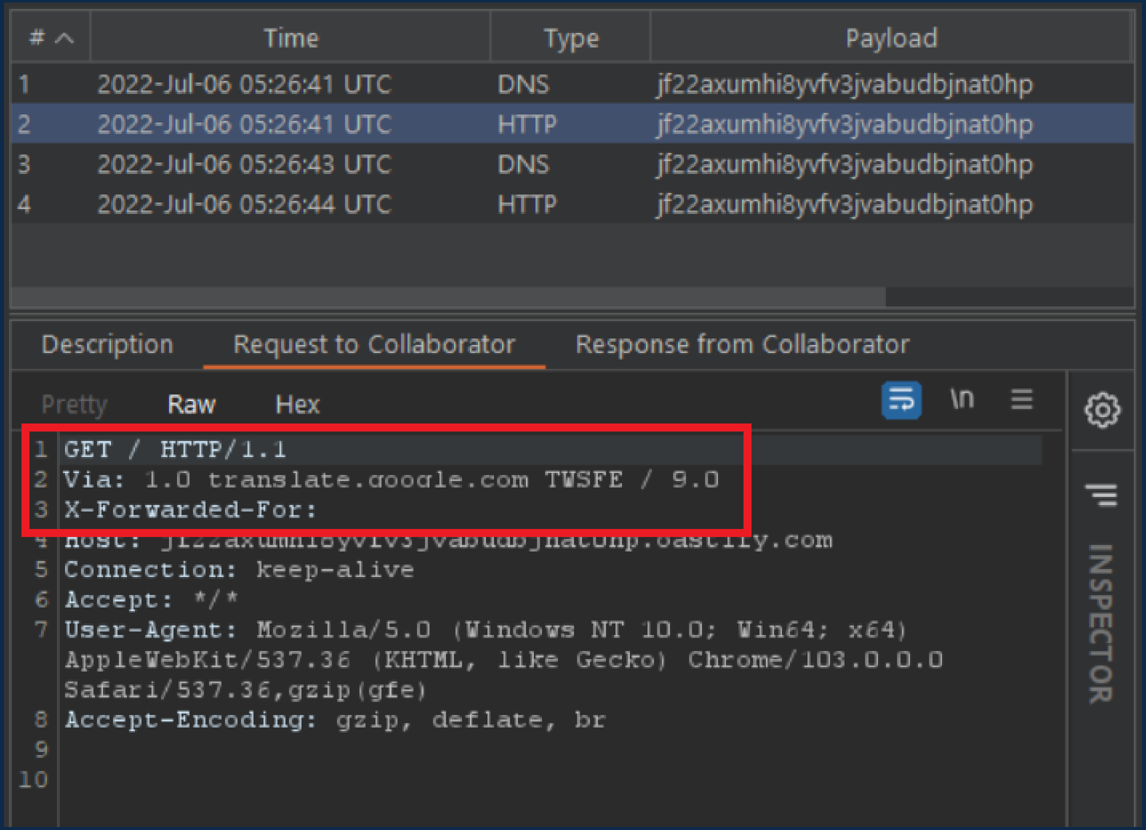
openresty/1.15.8.3

Google translate



https://jf22axumhi8yvfv3jvabudb
jf22axumhi8yvfv3jvabudbjnat0hp-oastify-com.translate.goo...
Google Translate
Maltese - detected
→
English
Translat

bnnczfoj8f9sggkj8cu9y4zjigz



#	Time	Type	Payload
1	2022-Jul-06 05:26:41 UTC	DNS	jf22axumhi8yvfv3jvabudbjnat0hp
2	2022-Jul-06 05:26:41 UTC	HTTP	jf22axumhi8yvfv3jvabudbjnat0hp
3	2022-Jul-06 05:26:43 UTC	DNS	jf22axumhi8yvfv3jvabudbjnat0hp
4	2022-Jul-06 05:26:44 UTC	HTTP	jf22axumhi8yvfv3jvabudbjnat0hp

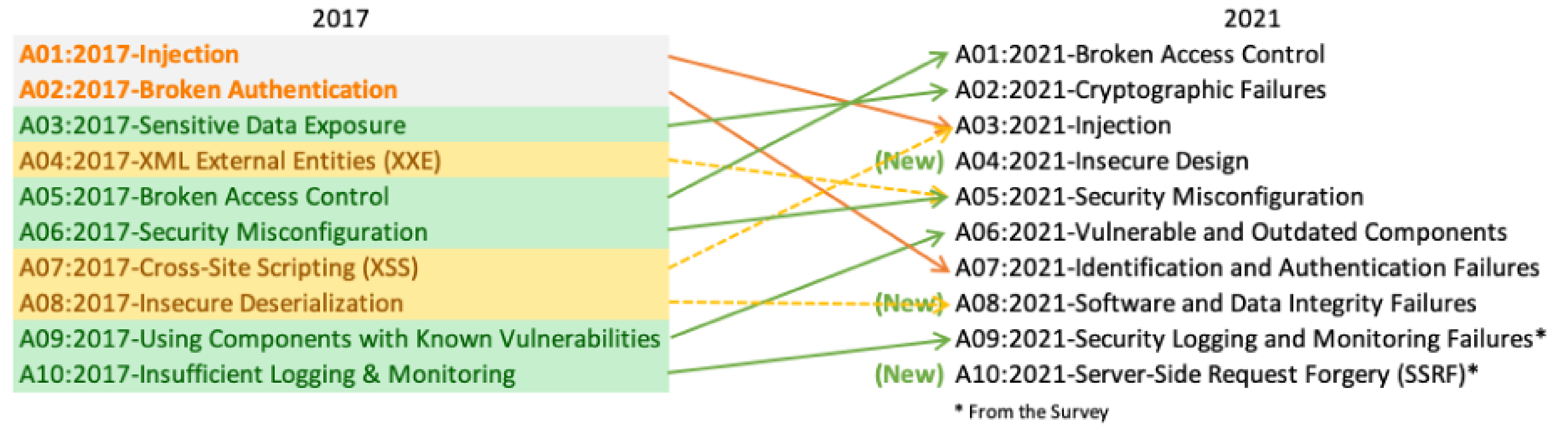
```
GET / HTTP/1.1
Via: 1.0 translate.google.com TWSFE / 9.0
X-Forwarded-For:
Host: jf22axumhi8yvfv3jvabudbjnat0hp.oastify.com
Connection: keep-alive
Accept: */*
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.0.0
Safari/537.36,gzip(gfe)
Accept-Encoding: gzip, deflate, br


```

OWASP Top 10

A10:2021-Server-Side Request Forgery

QUANTUM SECURITY

OWASP Top 10 - 2021



2017

A01:2017-Injection
A02:2017-Broken Authentication
A03:2017-Sensitive Data Exposure
A04:2017-XML External Entities (XXE)
A05:2017-Broken Access Control
A06:2017-Security Misconfiguration
A07:2017-Cross-Site Scripting (XSS)
A08:2017-Insecure Deserialization
A09:2017-Using Components with Known Vulnerabilities
A10:2017-Insufficient Logging & Monitoring

2021

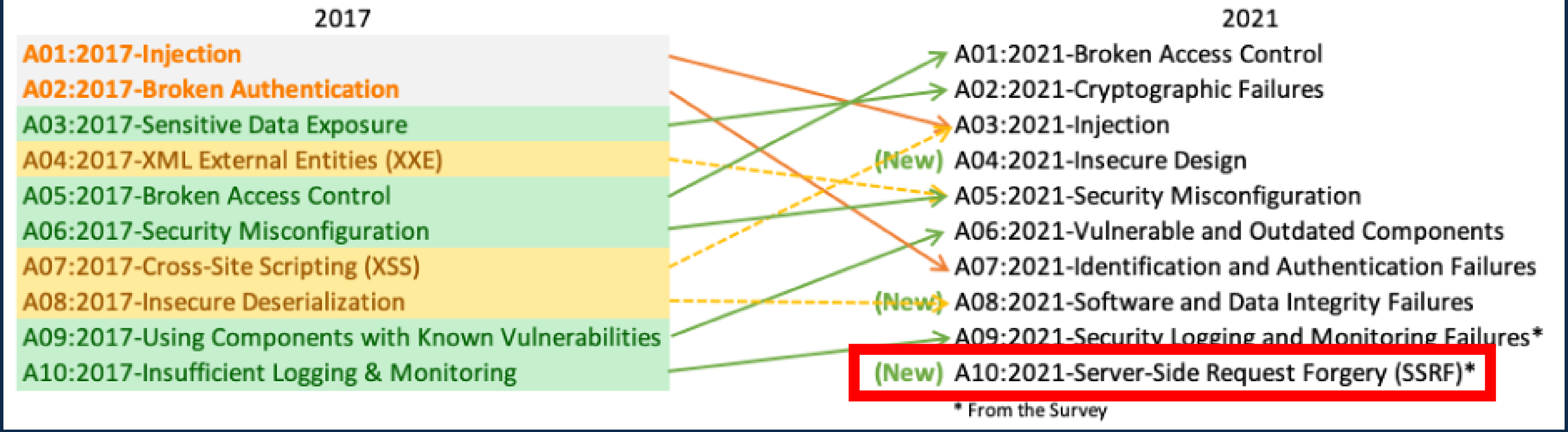
A01:2021-Broken Access Control
A02:2021-Cryptographic Failures
A03:2021-Injection
(New) A04:2021-Insecure Design
A05:2021-Security Misconfiguration
A06:2021-Vulnerable and Outdated Components
A07:2021-Identification and Authentication Failures
(New) A08:2021-Software and Data Integrity Failures
A09:2021-Security Logging and Monitoring Failures*
(New) A10:2021-Server-Side Request Forgery (SSRF)*

* From the Survey

https://owasp.org/www-project-top-ten/assets/images/mapping.png

QUANTUM SECURITY

OWASP Top 10 - 2021



2017

A01:2017-Injection
A02:2017-Broken Authentication
A03:2017-Sensitive Data Exposure
A04:2017-XML External Entities (XXE)
A05:2017-Broken Access Control
A06:2017-Security Misconfiguration
A07:2017-Cross-Site Scripting (XSS)
A08:2017-Insecure Deserialization
A09:2017-Using Components with Known Vulnerabilities
A10:2017-Insufficient Logging & Monitoring

2021

A01:2021-Broken Access Control
A02:2021-Cryptographic Failures
A03:2021-Injection
(New) A04:2021-Insecure Design
A05:2021-Security Misconfiguration
A06:2021-Vulnerable and Outdated Components
A07:2021-Identification and Authentication Failures
(New) A08:2021-Software and Data Integrity Failures
A09:2021-Security Logging and Monitoring Failures*
(New) A10:2021-Server-Side Request Forgery (SSRF)*

* From the Survey

https://owasp.org/www-project-top-ten/assets/images/mapping.png

A10:2021-Server-Side Request Forgery

#1 in Community Surveys

Low rates of incidence (2.72%)

Only individual vulnerability

OWASP Statistics

Organisations searched 67.72% of their applications

Found in 2.72% of tested applications

Weighted CVSS exploit score: 8.82

Weighted CVSS impact score: 6.72

https://owasp.org/Top10/A10_2021-Server-Side_Request_Forgery_%28SSRF%29/

QUANTUM SECURITY

OWASP Statistics

Organisations searched 67.72% of their applications

Found in 2.72% of tested applications

Weighted CVSS exploit score: 8.82

Weighted CVSS impact score: 6.72

Lots of testing coverage

Low incidence rate

High impact if found

https://owasp.org/Top10/A10_2021-Server-Side_Request_Forgery_%28SSRF%29/

QUANTUM SECURITY

Metrics vs Community

Metrics based on testing data

Community survey based on real world experiences

Metrics vs Community

Metrics based on testing data

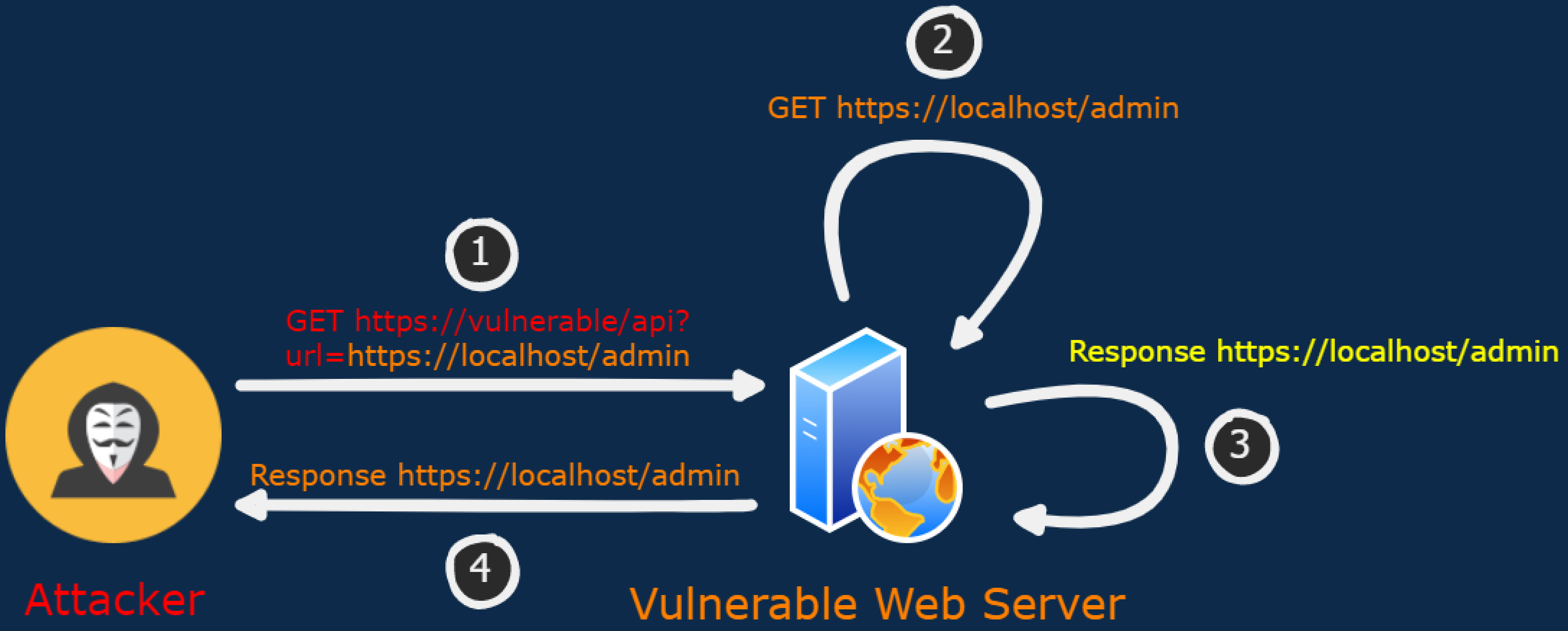
Community survey based on real world experiences

Making use of metrics and community surveys allows OWASP to incorporate large amounts of data while also including newer vulnerabilities that exiting tooling may not setup to find

What could go wrong???

QUANTUM
SECURITY

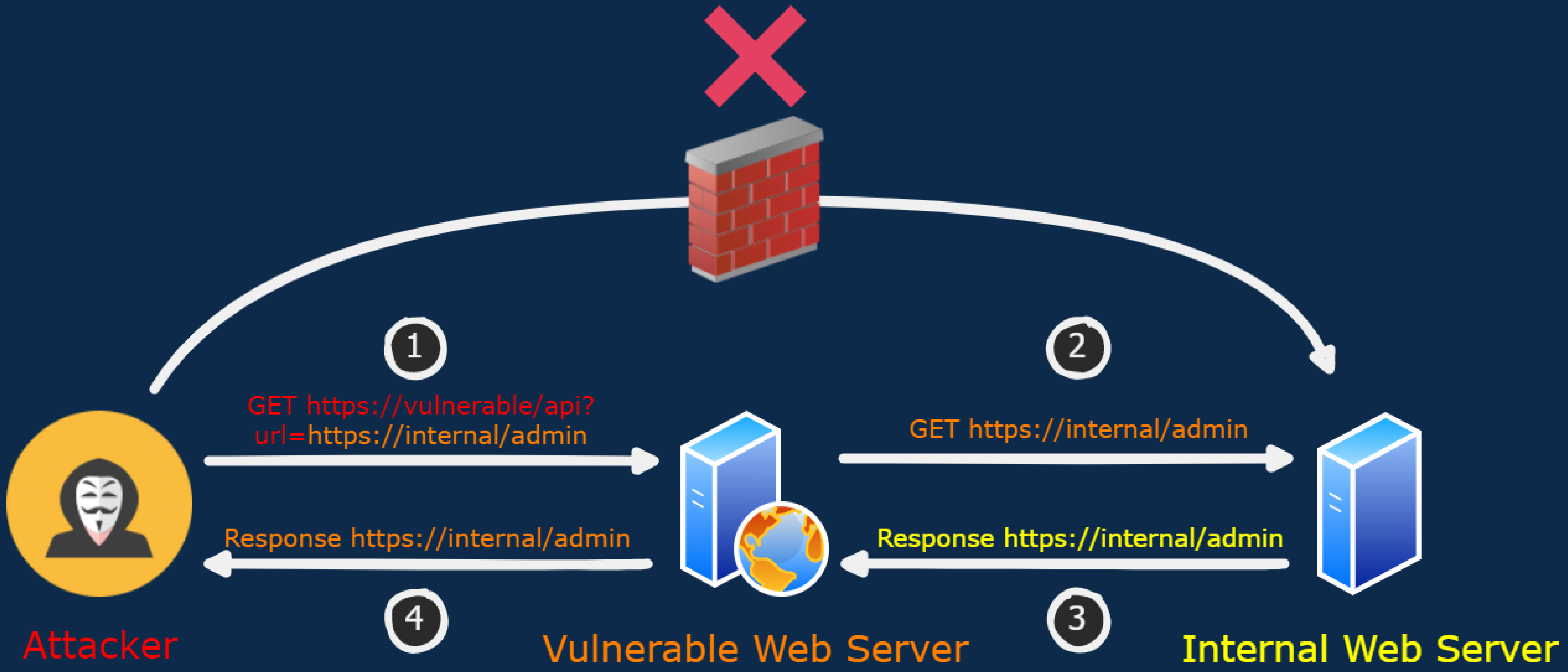
Access localhost (127.0.0.1)



2
GET https://localhost/admin
1
GET https://vulnerable/api?
url=https://localhost/admin
Response https://localhost/admin
3
Response https://localhost/admin
4
Attacker
Vulnerable Web Server

QUANTUM SECURITY

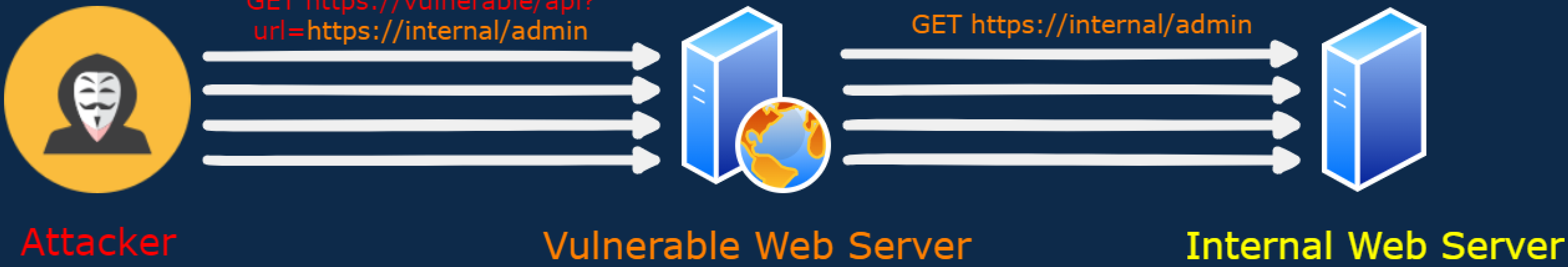
Access internal web applications



1
GET https://vulnerable/api?url=https://internal/admin
2
GET https://internal/admin
Response https://internal/admin
3
Response https://internal/admin
4
Attacker
Vulnerable Web Server
Internal Web Server

QUANTUM SECURITY

Denial of Service (DoS)



GET https://vulnerable/api?url=https://internal/admin

GET https://internal/admin

Attacker

Vulnerable Web Server

Internal Web Server

QUANTUM SECURITY

Different protocol schemas

http://

https://

Different protocol schemas

http://

https://

file://

ftp://

ldap://

gopher://

dict://

How to fix

QUANTUM
SECURITY

How to fix

Do you need customisable input?

QUANTUM SECURITY

How to fix

Do you need customisable input?

Hostname/IP allow listing

How to fix

Do you need customisable input?

Hostname/IP allow listing

Hostname/IP deny listing

How to fix

Do you need customisable input?

Hostname/IP allow listing

Hostname/IP deny listing

Limit input to hostname or IP

How to fix

Do you need customisable input?

Hostname/IP allow listing

Hostname/IP deny listing

Limit input to hostname or IP

Disable unused schemas (file, ftp, ldap, gopher, dict)

How to fix

Do you need customisable input?

Hostname/IP allow listing

Hostname/IP deny listing

Limit input to hostname or IP

Disable unused schemas (file, ftp, ldap, gopher, dict)

Always enforce authentication

How to fix

Do you need customisable input?

Hostname/IP allow listing

Hostname/IP deny listing

Limit input to hostname or IP

Disable unused schemas (file, ftp, ldap, gopher, dict)

Always enforce authentication

Network segregation

QUANTUM SECURITY

How to fix

Do you need customisable input?

Hostname/IP allow listing

Hostname/IP deny listing

Limit input to hostname or IP

Disable unused schemas (file, ftp, ldap, gopher, dict)

Always enforce authentication

Network segregation

Defence in depth!

Implement as many as you can

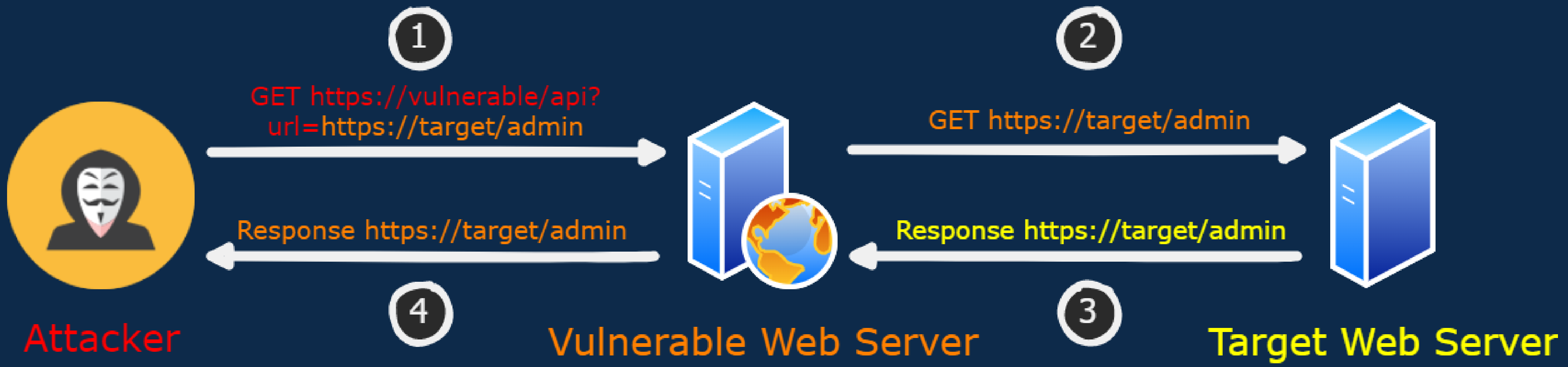
QUANTUM SECURITY

QUANTUM

SECURITY

NICK LAUDER | NICK@QUANTUMSECURITY.CO.NZ

Questions?


1
GET https://vulnerable/api?url=https://target/admin
2
GET https://target/admin
Response https://target/admin
4
Response https://target/admin
3
Attacker
Vulnerable Web Server
Target Web Server

Do you need customisable input?

Hostname/IP Allow listing

Hostname/IP Deny listing

Limit input to hostname or IP

Disable unused schemas

Always enforce authentication

Network segregation

1. Attacker sends target server URL to vulnerable server
2. Vulnerable server generates request to target server
3. Target server responds to vulnerable server
4. Vulnerable server forwards response to attacker