

# Macaroons

## Cookies with Contextual Caveats for Decentralized Authorization in the Cloud

Rihan Pereira, MSCS

COMP 524 - Security, Fall 2018  
Department of Computer Science  
California State University, Channel Islands

November 24, 2018

- 1 Web Cookies
  - Vulnerabilities
  - CSRF attack
  - session limitations
- 2 Token Authentication
  - OAuth 2.0
  - JSON Web Tokens(JWT)
  - OAuth + JWT
  - OAuth + Signatures
- 3 Macaroons
- 4 References

# Web Cookies

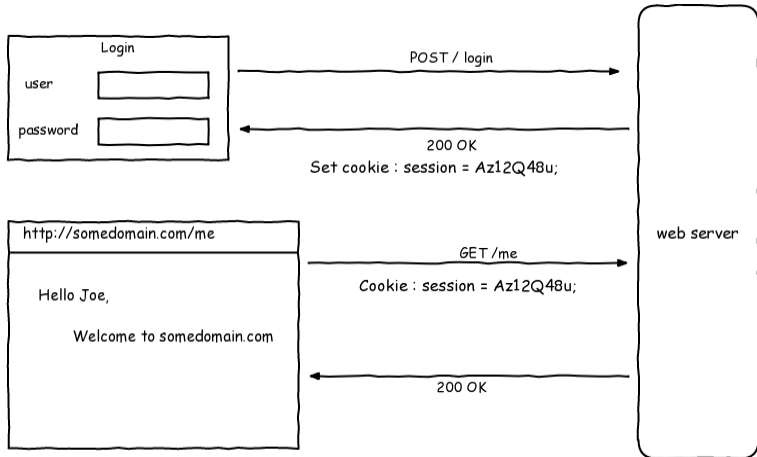
- solves user identity problem in dynamic web sites.

# Web Cookies

- solves user identity problem in dynamic web sites.
- fundamentally used to store session IDs

# Web Cookies

- solves user identity problem in dynamic web sites.
- fundamentally used to store session IDs
- still in use today!



# Vulnerabilities

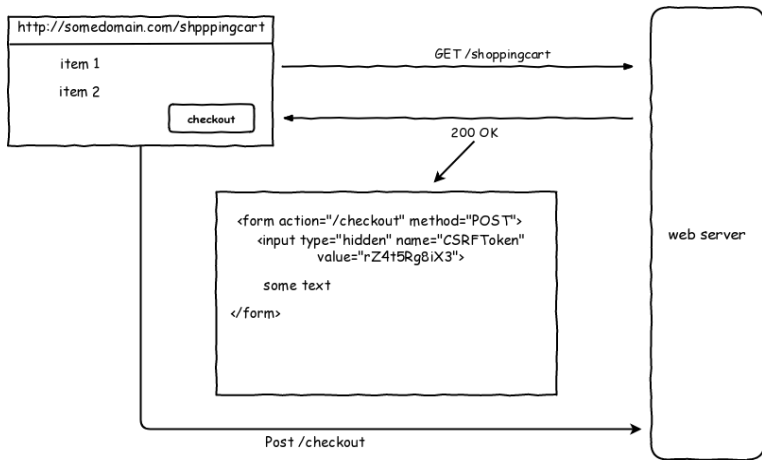
- Man in the middle attack
- Cross site resource fogery(CSRF)

# CSRF attack

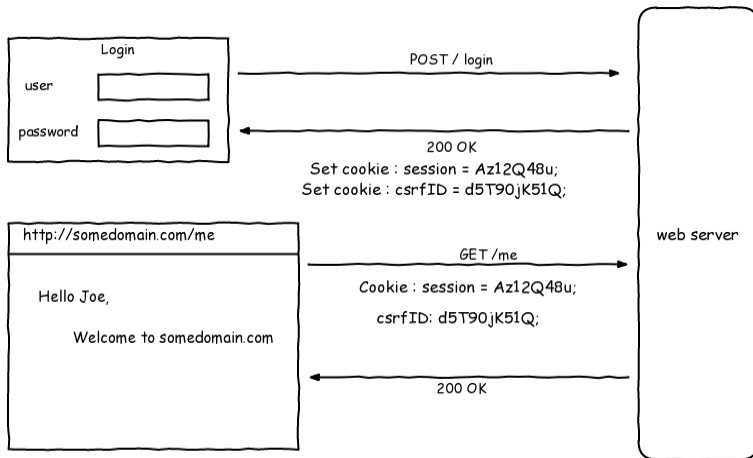
Executes unwanted actions on a dynamic site in which they are currently authenticated.



## fix 1 - using a csrf token



## fix 2 - double submit cookie



# session limitations

- web cookies are opaque

# session limitations

- web cookies are opaque
- dont solve access-control problem

## session limitations

- web cookies are opaque
- dont solve access-control problem
- lookup server state on every request

# session limitations

- web cookies are opaque
- dont solve access-control problem
- lookup server state on every request
- really not good for distributed/clustered applications

# Token Authentication

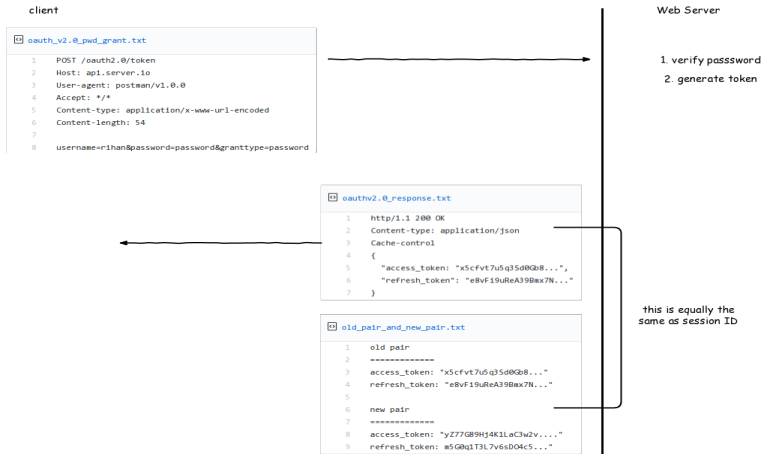
- self-contained chunk of information

# Token Authentication

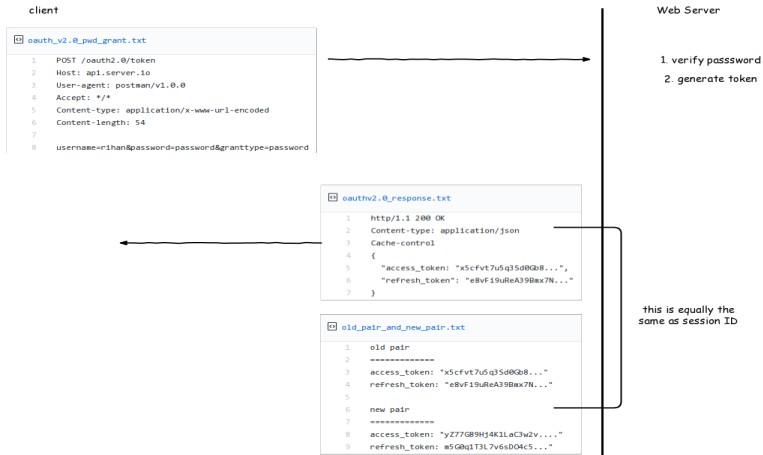
- self-contained chunk of information
- intrinsic value in that string



# OAuth 2.0



# OAuth 2.0

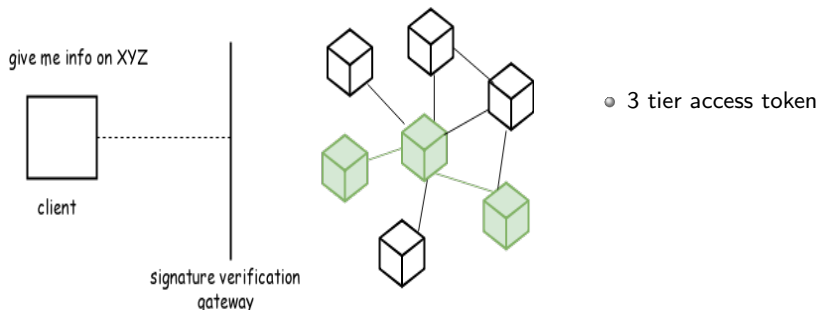


using access token - Authorization Bearer "x5cfvt....."

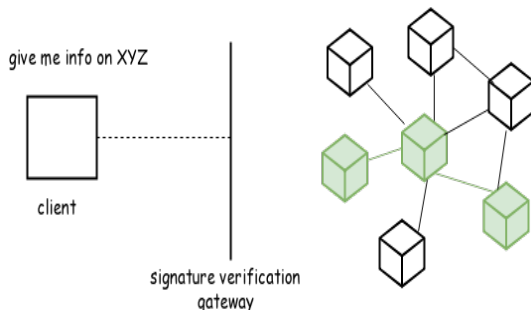




# OAuth + JWT

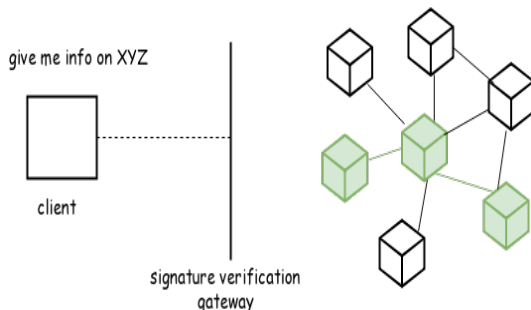


# OAuth + JWT



- 3 tier access token
- Instead of state on the server side, state is on the client side

# OAuth + JWT



- 3 tier access token
- Instead of state on the server side, state is on the client side
- reduced data access scope

# OAuth + Signatures

 `oauth_http_signatures.txt`

```
1  POST some/url/  
2  host : hmac.demo.org  
3  Authorization: Signature keyID="my-key-name"  
4  algorithm: "hmac-sha256"  
5  headers: "content-length host date (request-target)",  
6  signature: "j05o2...."  
7  Date: Nov 28th, 2018  
8  Accept: */*  
9  Content-type: application/json  
10 Content-length: 46
```

- no secret sent over the wire




# OAuth + Signatures

 `oauth_http_signatures.txt`

```
1  POST some/url/
2  host : hmac.demo.org
3  Authorization: Signature keyID="my-key-name"
4  algorithm: "hmac-sha256"
5  headers: "content-length host date (request-target)",
6  signature: "j05o2...."
7  Date: Nov 28th, 2018
8  Accept: */*
9  Content-type: application/json
10 Content-length: 46
```

- no secret sent over the wire
- symmetric key used between trusted entities


# OAuth + Signatures

 oauth\_http\_signatures.txt

```
1  POST some/url/  
2  host : hmac.demo.org  
3  Authorization: Signature keyID="my-key-name"  
4  algorithm: "hmac-sha256"  
5  headers: "content-length host date (request-target)",  
6  signature: "j05o2...."  
7  Date: Nov 28th, 2018  
8  Accept: */*  
9  Content-type: application/json  
10 Content-length: 46
```

- no secret sent over the wire
- symmetric key used between trusted entities
- stateless


# OAuth + Signatures

 `oauth_http_signatures.txt`

```
1  POST some/url/
2  host : hmac.demo.org
3  Authorization: Signature keyID="my-key-name"
4  algorithm: "hmac-sha256"
5  headers: "content-length host date (request-target)",
6  signature: "j05o2...."
7  Date: Nov 28th, 2018
8  Accept: */*
9  Content-type: application/json
10 Content-length: 46
```


- no secret sent over the wire
- symmetric key used between trusted entities
- stateless
- driving modern REST security these days.




 Arnar Birgisson, Joe Gibbs Politz, Ulfar Erlingsson, Ankur Taly, Michael Vrabie, and Mark Lentczner,  
*Macaroons: Cookies with Contextual Caveats for Decentralized Applications in the Cloud*, **2015**.

 <https://www.owasp.org>

 <https://jwt.io/>

 <http://aosabook.org>

 <https://oauth.net/2/>

Thank you! Questions ?