

Venkatesh L Sharma

Cyber Security Advisor, Information Security Consultant

OSCP, CISSP, CCISO

Twitter : [@1337in](#) LinkedIn : [@Venkatesh](#) Crunchbase : [@Venkatesh](#)

With more than 7+ years of experience in,
BlackBox testing, Pen-testing, Web-App / SCADA security, Incident / 0day
monitoring & response, Blockchain security, and security compliance.

Has Honorable mentions and Security Hall of fame in.

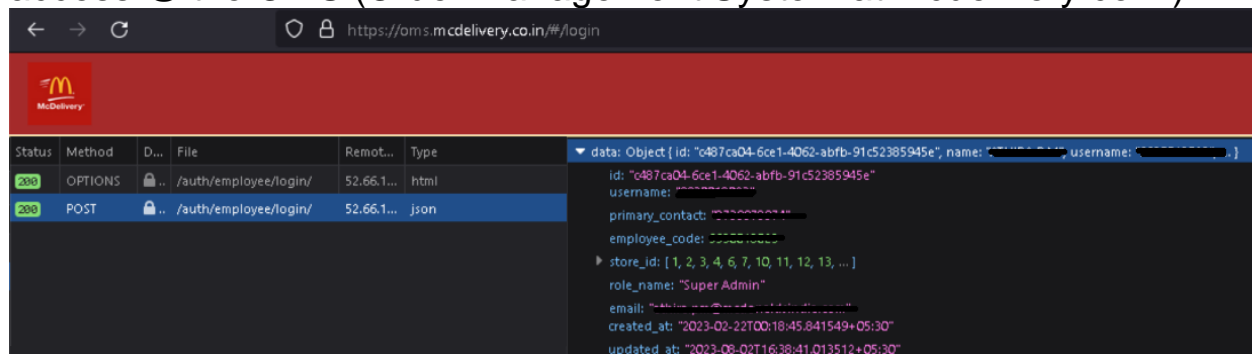
Google/ Apple / Microsoft / Flipkart / United Nations/ Western union / Dell / ISC2 /
Under Armour / TripAdvisor / Verizon(BJN) / Naspers & many more. With CVE's
CVE-2023-33297, CVE-2022-0723, CVE-2022-0721, CVE-2022-0719, CVE-2022-0690

With Top Ethical Hacker world rank : <https://tryhackme.com/p/1337in>

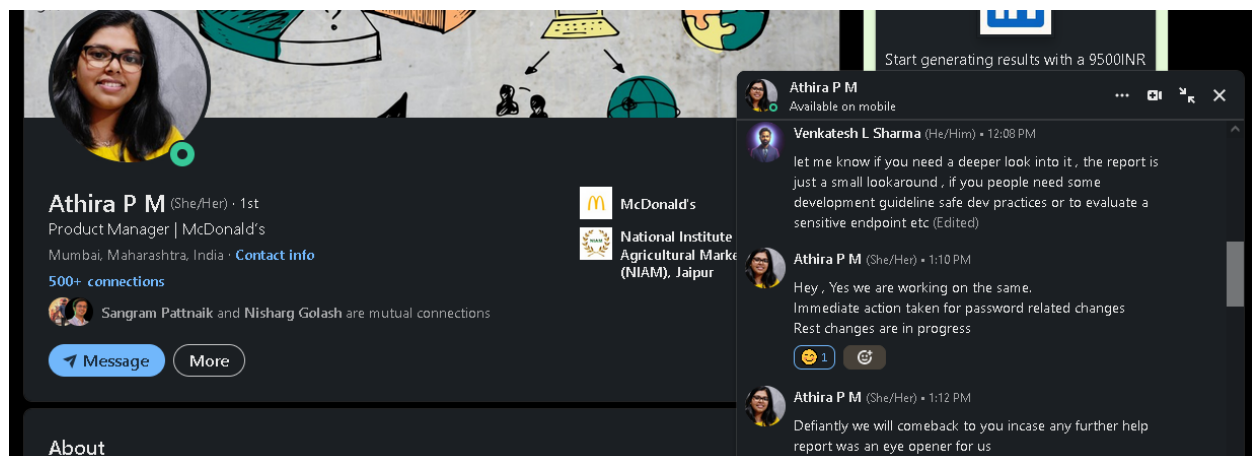
Recent Works and Recognitions

SuperAdmin at McDonalds

With Series of reports sent to McDonalds India (HRPL pvt Ltd)
the report can be described as chain of exploits to attain SuperAdmin
access @ the OMS (Order Management System at mcdelivery.co.in).

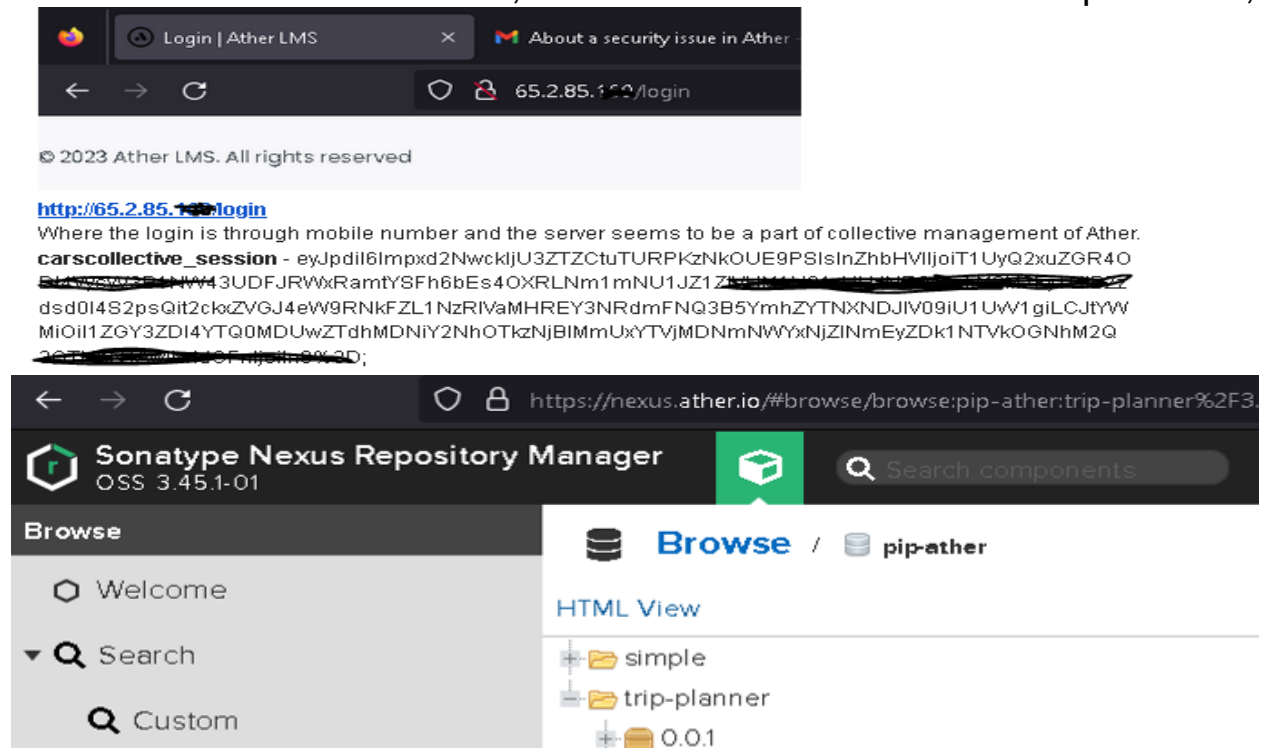


VP Product of mcD india expressed the reports to be “eye opening!!.”



Owning Source at Ather Energy

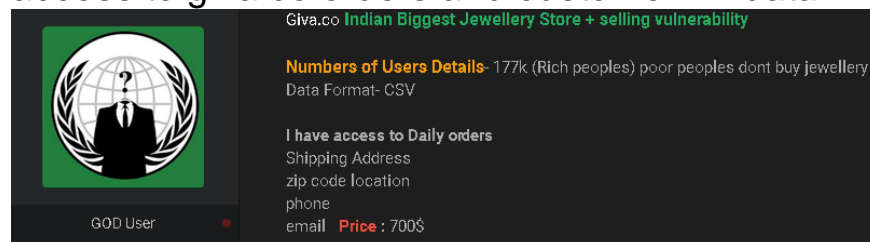
Serious Auth flaws in Station manager & repository software, [CWE-840](#) flaws, lead to minimal PII disclosure, Source code leaks for Ather EV platform,



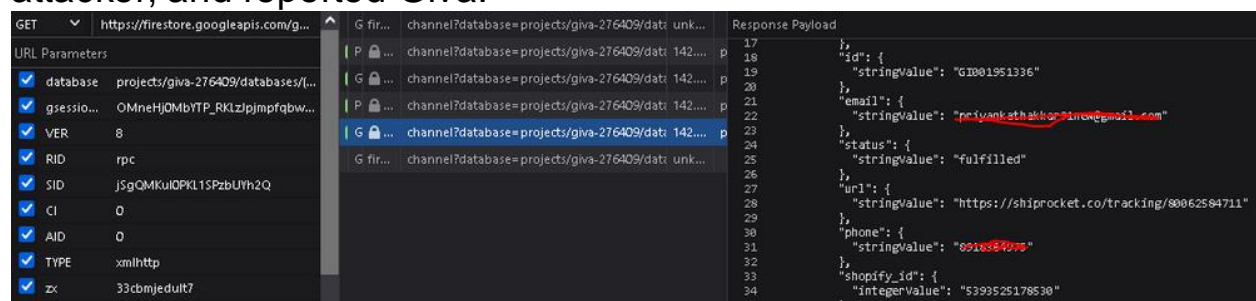
On reporting many issues was onboarded as security advisor /consultant.

Helping Giva.co to fix a Dataleak

Exactly on 10-6-2023 A threat actor posted on a darkweb forum that he had access to giva.co orders and customer PII data.



So we tried to reproduce the data leak sample we obtained from the attacker, and reported Giva.



Giva immediately issued fixes for it by taking down the affected Firebase application and also taking down the risky subdomain. i.e. [tracking.giva.co](#).

Flipkart Recognition

Since they have a strong internal security team and their bug bounty program is hosted on Hackerone, the world's leading security platform, only the best hackers from around the globe are invited, Flipkart doesn't do regular hall of fames. Additionally, they had undergone top-notch audits at the time of Walmart's takeover. I was awarded Hall of Fame with multiple submissions in Dec-21 for the contribution to the Indian ecommerce giant.

<https://www.flipkart.com/pages/security>

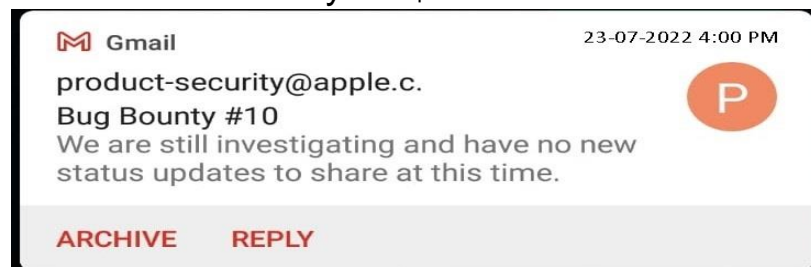
BASF HERO

The BASF Group, a chemical conglomerate with operations in over 80 countries and clients in over 190 countries, was exposed to a few severe defects, was recognized as Hero of BASF with Hall of Fame.

<https://www.basf.com/global/en/legal/responsible-disclosure-statement.html>

Apple Hall Of Fame

With Bug reference number – 79126728, 803752987 new security report is marked valid and being investigated by apple, this is our 10th valid submission. bounty of \$1500 was awarded hall of fame



<https://support.apple.com/en-us/HT213636>


Google Honorable mentions

The Prestigious Google Bughunter Honorable mentions which is very rare recognition was awarded on July 2022 for 2 issues which were critical and awarded 5000\$ Bounty. The issues stemmed in the sub product of youtube called with youtube which was exposing personal details of the judges.

REPORT NAME ↑	STATUS	PROGRAM	CREATED	
withyoutube(read access)	■ ACCEPTED	Google VRP	11.08.2022	view →
Product A-142	■ CLOSED	Google VRP	15.07.2022	view →

Honorable mentions

These are active Bug Hunters, all helping us to make the Internet a safer place.

RESEARCHER	REPORTS	MEMBER SINCE	COUNTRY	
 Venkatesh L Sharma		July 2022	India	view →

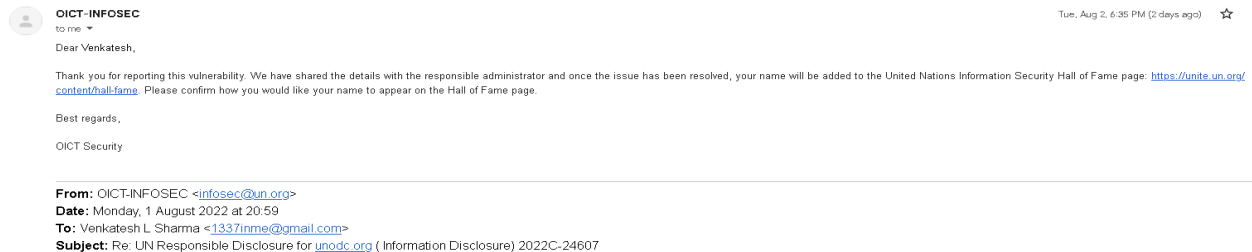
<https://bughunters.google.com/leaderboard/honorable-mentions>

Nokia Hall Of Fame

For Reverse engineering of N-Wing IOT platform of Nokia
<https://www.nokia.com/notices/responsible-disclosure/>

United Nations Hall Of Fame

Valid security report submitted on Aug 2nd, 2022, was triaged, accepted into the UN OICT-INFOSEC program, and Hall of fame awarded.



<https://unite.un.org/content/hall-fame/list>

Microsoft Hall Of Fame

After back and forth conversation with Microsoft MSRC-VRD our reports submitted on **Mar 31, 2023**, were validated to be a vulnerability in a Microsoft product than a simple security issue our report was assigned with VULN-063223, which was taken to MSRC board for discussions, the fix and bounty of 3000\$ was paid.

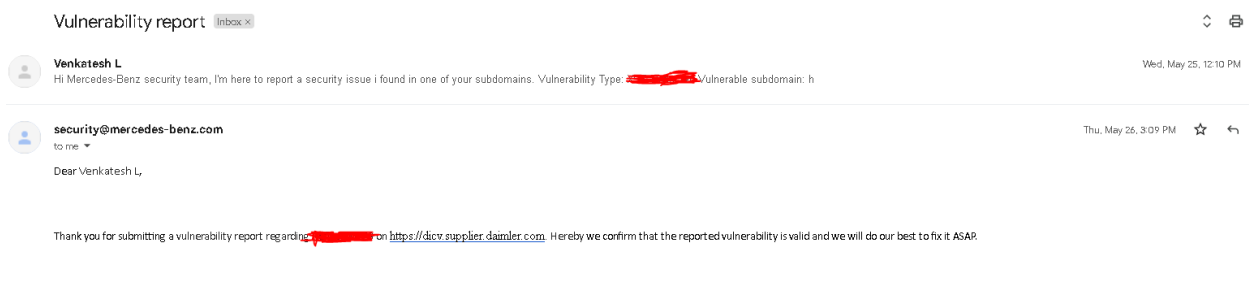
MSRC - Acknowledgement Notification VULN-063223 CRM:0113000248 Inbox x



<https://msrc.microsoft.com/update-guide/acknowledgement/all>

Mercedes Benz Hall Of Fame 2022

Reported on 25th of May 2022, marked valid on 26th of May 2022 HOF.



<https://www.mercedes-benz.com/en/whitehat/>

Current work

1.) [Delta Exchange](#)

I have been an information security officer for the past 4+ years, which has exposed me to a variety of difficulties and research.

Complete web app and infrastructure security audits, incident/0 day response and monitoring, active firewall/IDS/WAF management, employee awareness campaigns, and bug bounty program

<https://www.delta.exchange/bug-bounty-program>

2.) [Amazon Pay Later](#) (Capital Float - Axio)

Been a Security advisor form last 3+ years, testing their product release cycles and recently their walnut ,w369,Amazon payment infra and other internal audits.

3.) [GreyBox](#)

Awign, Woodenstreet, Glynk,Incred, Lendingkart, Apollo group,Bluestone, Firstcry, xpressbees,Grab, apna.co, nykaa, shadowfax, pankuri, tripadvisor, fareye,Coinmode and countless more have benefited from my service,at Greybox, where I run cost effective security audits.

Every six months, I give infosec lessons to a group of pupils I select from applications and requests.

Sent to <https://greybox.in/>

Other works

BC: <https://bugcrowd.com/x00>

[Coindcx](#) — India's first crypto unicorn

There was a communication gap despite extensive work from 2019 to 2020 that resulted in the submission of about 10 to 15 mid-to-critical concerns.

They also lacked a dedicated team for security once patches were applied.

Meanwhile, Neeraj Khandelwal, CTO of COINDCX, tweeted in support of the effort in 2020.

<https://twitter.com/nrjkhandelwal/status/1271071014194159620?s=20>

Security Advisory at [Consensys](#) 2020

As one of the most experienced teams in the cryptospace, ConsenSys Diligence is at the cutting edge of offensive cryptography, blockchain technology, and crypto economic analysis. I was engaged to test the Consensys infrastructure and also worked with Maurelian and other members of the diligence team to fix the security of the consensys diligence products and other platform's.

Advance notification for Inward Remittance [Inbox](#) [x](#)



eforexservices@axisbank.com
to MXMAILROUTE

Tue, Nov 17, 2020,

Dear Sir/Madam,

This email is to inform you that we have received an intimation regarding inward remittance initiation from overseas vide SWIFT bearing reference number F61116228628000 for your a/c number XXXXXXXXXXXX5144. Following are the details of the transaction:

Amount and Currency (F32A) : USD 2100.00 Please note actual amount may differ on account of processing charges/conversion rate etc. (If Any)

Value Date (F32A) : 16-NOV-20

Ordering Customer - Account and Name and Address (F50F) : CONSENSYS SOFTWARE INC.

49 BOGART ST APT 22 BROOKLYN NY US 11206 3840

Beneficiary Customer - Account and name and address (F59) : XXXXXXXXXXXX5144

VENKATESH L

BANGALORE IN

Remittance Information/ Purpose (Field F70) : INVOICE FOR THE SECURITY TESTING

Details of Charge (Field F71A) : OUR

Please note:

- This is just an advance intimation and you will receive a final communication once we receive credit in our account (depending on value date).

- Actual processing of transaction will be dependent on receipt and realisation of funds by the bank and customer's instructions (if any).

Kindly get in touch with your branch for documentation (if any) and further details.

- Axis Bank is live on FX-Retail (www.fxretail.co.in), you can also buy/sell foreign exchange through this platform. For details visit www.axisbank.com/retail/forex/fx-retail

With Regards,


Axis Bank Ltd.

[Consensys](#) gitcoin.co - 2021

Being a member of Consensys required me to take part in the web3 community's bugbounty, where I placed second on the basis of tips in Ethereum and 23 praises or NFT for my participation in web3 hackathons. Later, when gitcoin introduced its cryptocurrency, I received a \$5,000 reward for my community service.

Claim your [GTC](#) tokens right away [Inbox](#) [x](#)

Team Gitcoin <team@gitcoin.co> [Unsubscribe](#)
to me



Claim Your [GTC](#) Before June 23rd

Hello x00x00 — you have tokens to claim!

On May 25th, 2021 we launched [GTC](#), the Gitcoin governance token. Because of your past participation in Gitcoin Grants, Hackathons, Bounties, or KERNEL, you have been allocated **500 [GTC](#)**. From the launch, you only have 30 days to claim your tokens.

<https://gitcoin.co/1337in>

Tron

Tron had exposed few important dashboards with incomplete config files which were discovered and was awarded 3000\$
can't say more because of the "NDA"



Other works

- Core Contributor of Hashing tools to Matriux linux (2012-14).
- Contributed to GNSS-SDR on identifying jumbled/encrypted radio signals (2015).
- Worked on radio p2p encryption methods similar to P25 with Lockheed (2015-16).
- Co-founder of Flybit.in / Bitserve crypto projects (2016-17).
- Contribution to SETI for securing transmission of Seeker data (2017-19).
- Active Cyber Crime interpreter/Profiler for regional office since 2017.
- Event Advisor for OWASP Bangalore chapter. (2016-18).

Works with bitcoin community

1.) Path transversal at bitcoin core

Helped a bitcoin maintainer with investigating and fixing Path transversal with create wallet function. "wallet_name" is not validating When user uses path as wallet name creation process on bitcoincore v0.20.0 issue was fixed with new release.

<https://github.com/bitcoin/bitcoin/issues/20128> - oct 12-2020

<https://github.com/bitcoin/bitcoin/pull/20741> - merged jan 9th 2021

2.) Code execution at restart

Bitcoin core allowed a user to restart with a schedule command which enables an misconfigured web integration to code execution - Pr closed pr was not accepted and we are sure about the issue and researching a new approach to these issues and a proper POC. [CVE-2022-35913](#).

3.) **DOS through mempool tx flooding**

Bitcoin core 24.1, when debug mode is not used, allows attackers to cause a denial of service, because draining the inventory-to-send queue is inefficient. fixed in later version of bitcoin core. [CVE-2023-33297](#) .

Upcoming works

1.) **Bitcoin (2022-2023)**

Will be handling Bitcoin supply chain security Q&A tests 2022-23
Supported by bitcoin core maintainers and contributors.
This is the first security audit on bitcoin and its integrations.

<https://twitter.com/JohnNaulty/status/1443042702824669188>

<https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2021-October/019501.html>

<https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2021-October/019511.html>

2.) **Polygon (2022-2023)**

Will be Freelancing on Risk consulting of upcoming polygon product ,
helping the web3 startups on polygon to hibernate their projects with
security as priority on weekends!

3.) **Solana Spectrum (2022-23)**

We are working on securing solana transactions adding confidential transaction ready and available, Spectrum is a privacy focused project on solana with account control, confidential txs, reusable payment codes, smart explorer and tor.

Spectrum whitepaper: <https://privatespectrum.xyz/whitepaper>

Looking forward to our collaboration!

I appreciate you taking the time to read my profile.

Venkatesh L Sharma

Whatsapp: +19164592202

On Call(india): +919606232344,

Email: mxmailroute@gmail.com

Email: v@greybox.in

**For sensitive topics and secure communication.
Use the PGP- key mentioned below.**

-----BEGIN PGP PUBLIC KEY BLOCK-----

Version: Keybase OpenPGP v2.0.76

Comment: <https://keybase.io/crypto>

xsBNBGLrfY4BCACuUcCMzECZSh+PFTd75Li8uJPQcBnsD6hyB9TA0gdAO7m4nBPw
ZMs23hQFyONrLR6Ozxoika2qF1Tsz/s1ooAFIfy03+dxdm6Sskee29UFwg8+GmV
EZWMMA2vNvwc/hisiGovuRpdEvoOf7pyjgYlw4PKX6OJaXRrCQJPj44q1UMETae
+gCijlHRCDDNz8w1SQezOERURfJx+gbP7qKTNXVfsMa5erMQrF5GjZWYU0FfQ/qm
y9C2eBue4byu9MqfM6n1+bktFfDDHRzz6AxKaHNEiFEEN8nfmwqnVEpXKbZYcKj
s6XLBzVCcK9Wtau8DYCNHplFLLxge08vwlx/ABEBAAHNIVZlbnthdGVzaCAocGdw
a2V5KSA8dkBncmV5Ym94LmLuPsLAegQTAQoAJAUCYut9jglbLwMLCQcDFQoIAh4B
AheAAxYCAQIZAUJAAAAAAKCRCK03bh822KShmzCACYxs7YeZnm8sPKgFQfR+Ee
VEsifYwDj4t5wBlqIT/hrjP6D1aazoBaxMykbE33BuK9Uqt6aq95Jko9S0Jn1h4
1JFPIxv07O3v7N96bO5GVmQq4Tmz48DFUppJ5/OOB0EHj3RIkMSs9ZYgkqjVEqBl
zemhijCanTIVSoEB87hQG5hjUxihXkpKgXKASSbxc7E8MT/e96ywySteVAf1CYCL
SMdWHJvUKvJBWViN/mLFii3ah2wt0BUPitgT5nacqvwINAsiWwW2EqHAHgLOEcrb
avyzCzbY1n5ZntPHhf82RsE25nIJNvk1YAEulHsHwHKrMRaJPef6QLVF6PcJg2wG
zsBNBGLrfY4BCADvYurejUCi5fCwp41Sh/xQlztG4BUKzKiko0RqFjQy3FfT1h5
8crkcumPIRI9OQyjuwgl1vXXzwyJmXupPE4lBlrkVHRzTDEjmYZnjivZLggbqk
dXlsJ5kN+9bAxEe+wIGTxwyHb13anxxa/DMjapnAwhAlw8QPOdlnkNQLIRhSlReQ
oGkcJWKL96Sgi8s5Zg6GeJnvPA2eGqYABM3vQn/02kNulPeHs0nqjV/qRvyDcO14
kqURgSMWHkPBNn1YhYjTvMxPsfBRD5ydaY+wMrEEIRjwPoHiasS9fIWzajyB9890
+NjWvstBaT6c07CT2FIFl1yfeC4z0LiE3jpABEBAAHCwYQEGAEEKAA8FamLrfY4F
CQAAAAACGy4BKQKqPNN24fNtikrAXSAEGQEKAAYFamLrfY4ACgkQD23mwmRAI2mA
xwgAhyyXA1B5oJlgDfeJ9FuxEWChC+B9sQQVuaKZeuJU3UPep9Q4C7GH05isNDXc
w9c2BqT6wu6B6gQA1HIXLbsIRFvuZdfHgmXee/y7aw+RtKDLsqHskl8MaJSvUmay
saBYDbxLosU4LHfnvYXhrvhk9ef5s4LDuIN2gM3N0iTOH7aTNrkMAIqjH0EeackS
UqMCzfQXk9b29IUkXuZG4yUbDVRDHH//U4NemjOV+YmfJCSzaJiUmQ39qku5ANuP
zd1lCdFbpEqOuWAwPWm6/cDSE77P9ArvB9hW+rZv4aD0a7A2a3fHcCKn4BISrj42
JmufTLeIq0r4X1+mo4OMzrNh3uGKB/4yoDWTz4+mHQZU5QOR0066CY4su+l8CzWM
2nmXf2IAk9wzo7Odr+6CZqQXL1Bh/opyGvqv8hfRWdRnVgxz8s+c656OppEjFO5V
aWw4YaBOzxTi9ssftFlvH7rnT1lStBx3xz2VVcB8Y6nXnNp8ITSPB63tGblS09af
aR664XrkXBbhEHCL1IGibzvubKu0PtCMWYGslykODL43eb26bhI5sgVmYmapVwn2
0DLHgjtct5TzBukisY0gCu6zXZX8aW8MQ7zE/UyJlWakOQvqddqJTS/wNq2AKYlxJ
y9DPE0IXTh7BaFQMkXPp8CWPANd03xbovbHKg/eSG0cZLPVUANpozSBNBGLrfY4B
CAC4Y3SRSZVMyXg0R2jP4nVG5ChMr2j4+OQUs6vl3BAu3KXP8ngdy7LsjNdDxrqx
Set+wjry0MiG3jOfIgw4NvOX6882TmZv6yfl17s9/IgAVw8CxfqC1EURblgrJjiP
/TRF1zCv2QMOXq4711ocjpL3lziFeLNbIk35J8Zb/FkwSvFAKLh7BIISv9dVbpm
y2XTjAHpA/8qzWX6BaG8XDglSgf4lq2oFozSXxl6KQfy1uzV1H5YulDi2XLws9q
b5A7WQP+9Nk5ptfKH8xsedtd/u4MuGqNNWHn/FdFxChKVUewm+EMBuMCqw6J5sbq
WE/3+YggrFMRtl4nf7v+5O6nABEBAAHCwYQEGAEEKAA8FamLrfY4FCQAAAAACGy4B
KQKqPNN24fNtikrAXSAEGQEKAAYFamLrfY4ACgkQgqtrd0AGuMWFIZwf9GFg57I7F
9Accj1podu39kcSIHTEgroour8h7ID8q4BOSAHLbicVOAGH8ero+VW4bBvY9xU/y
C8ngbr42Ym4DLKj4G1ex448x5or3jrgL1idPsvD2ibSyjQ/bz7V4rbSgSlmgCFvg
3r+T17edHvkfgPpmeJE5/DqWZ03yFSmP7pJ3B7ga76/yo+cUDgUji36eMmBWI6Do
cwXndEiOOjOB7lWrfGnUp+0HsCAFj0B1ckJhwXuwxICjkaSG9DZc11QWq5NIOHT1
v6z+G7p7knRuHH+7zHndXScOG3YfykYn1Y/ozb/82Ap0nQTI/m2TGmwrGGWVbKN
uRAVca+NbaqyyufYCACqWDTNIOhchDd0/OIGY16HrdAGfUslA25EMJ+TTbmdfWAW
dW1EXaLyie+c+ehDZDCi/xf/fx6iTgv/9uHO0qQpf7atNEF7YPMmfVtFmgOn7tSr
Fgej0JWYSE7DcMLfhKzwDB8bNrD3jrkCVgUF1Z11Jr1i32W5MvHqmqQRcV74qAfQ
kswnedduAnfVh4Q5d/NfmuCqLW4mPGGPafWxBsL7CfSyWVbz+ZOPA26zaZZICWCo
8IDro2+RMPbZs2nQMIB9jXdBD6320/lo20+G8YF1TfqTTSiDvH3x7qaL78Si/9iV
sN+nP1Ce5Y1vEB9N3SXwhIV7qLNnjZyVGWwpDIlm

=TQws

-----END PGP PUBLIC KEY BLOCK-----