



Information Security Education & Awareness

Department of Electronics and Information Technology
Ministry of Communications and Information Technology
Government of India

सी डैक
CDAC

InfoSec
Newsletter
May-June 2016

Secure Usage of Credit & Debit Card/ATM

InfoSec

Concept 4
Alerts 8
Tools 9
News 10



For Virus Alerts, Incident & Vulnerability Reporting

certin
Handling Computer Security Incidents

सी डैक
CDAC

www.cdac.in

प्रगत संगणन विकास केन्द्र

CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING

संचार एवं सूचना प्रौद्योगिकी मंत्रालय की वैज्ञानिक संस्था, भारत सरकार
A Scientific Society of the Ministry of Communications and Information Technology, Government of India
Plot No. 6 & 7, Hardware Park, Sy No. 1/1, Srisaillam Highway, Pahadi Shareef Via
Keshavagiri (Post) Hyderabad - 500005, Telangana

Credits

Prof. N Balakrishnan
(IISc, Bangalore)
Prof. Sukumar Nandi
(IIT, Guwahati)
Prof. V Kamakoti (IIT, Madras)
Prof. M S Gaur (SVNIT, Jaipur)

Design & Technical Team

Ch A S Murty
I L Narasimha Rao
K Indra Veni
K Indra Keerthi
P.S.S.Bharadwaj

Action Group Members

HOD (HRD), DeitY
Shri.Sitaram Chamorthy (TCS)
Prof. M S Gaur (MNIT, Jaipur)
Prof. Dr.Dhiren R Patel
(NIT Surat)
Representative of Chairman
(CBSE)
CEO, DSCI (NASSCOM)
Representative of Prasar Bharati,
Member of I & B
Shri U Rama Mohan Rao
(SP, Cyber Crimes, CID,
Hyderabad, Andhra Pradesh)
Shri S K Vyas, DietY

Compiled by

G V Raghunadhan
I L Narasimha Rao

From C-DAC

E Magesh, Director

Acknowledgement

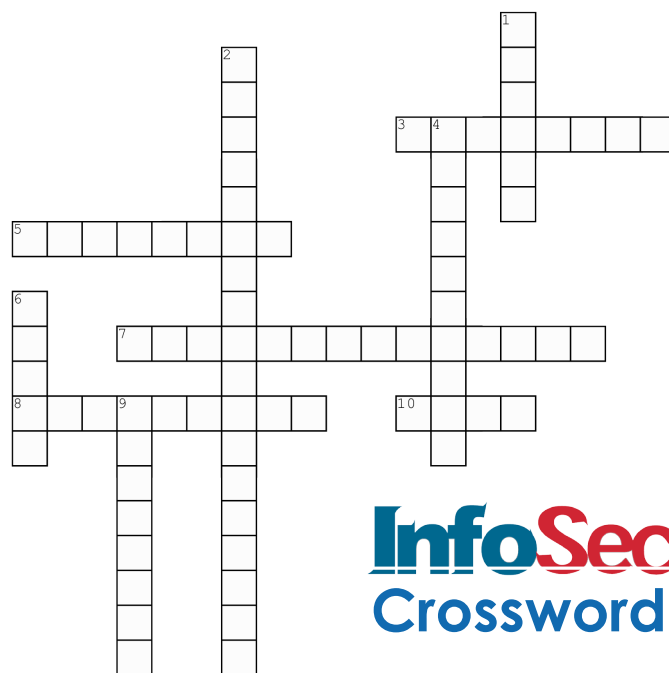
HRD Division
Department of Electronics &
Information Technology
Ministry of Communications &
Information Technology
&

For Virus Alerts, Incident & Vulnerability Reporting

InfoSec Quiz

1. Linda received an email from her bank asking her to verify her account and PIN numbers to prevent identity theft. This could be a form of information security risk known as _____.
A) Email engineering B) Phishing
2. A hacker who changes or forges information in an electronic resource, is engaging in _____.
A) Data diddling B) Sniffing
3. In the right setting a thief will steal your information by simply watching what you type.
A) Snagging B) Shoulder surfing
4. A network of computers used in a denial-of-service (DoS) attack is called a (an):
A) Worm B) Botnet
5. Which of the following is a method used to embezzle money a small amount at a time from many different accounts?
A) Salami technique B) Spoofing

login to
**www.
InfoSec
awareness.in**
/contest
to participate in
Infosec Contest and
WIN PRIZES



InfoSec
Crossword

Across

3. Choose a password that is easy for you to _____ but hard for someone to guess.
5. A _____ is hardware or software that helps keep hackers from using your computer and it watches for outside attempts to access your system and blocks communication that you don't permit.
7. The fraudulent acquisition and use of a person's private identifying information, usually for financial gain.
8. Do not send _____ information over email unless it is encrypted.
10. A _____ is often an email that gets mailed in chain letter fashion describing some devastating, highly unlikely type of virus.

Down

1. _____ is the need to ensure that the people involved with the agency, including employees, customers, and visitors, are protected from harm.
2. The art of tricking or manipulating people into providing information that they normally would not provide.
4. Applied to data to protect it from unauthorized use in case of theft or loss.
6. Before you throw something in the _____, ask yourself, 'Is this something I would give to an unauthorized person or want to become publicly available?'
9. Use this tool to dispose of documents that contain personal or financial information.

Guess The Tip Win Prizes

*Guess the Tip which best
suits the cartoon by
logging in to*

www.
InfoSec
awareness.in

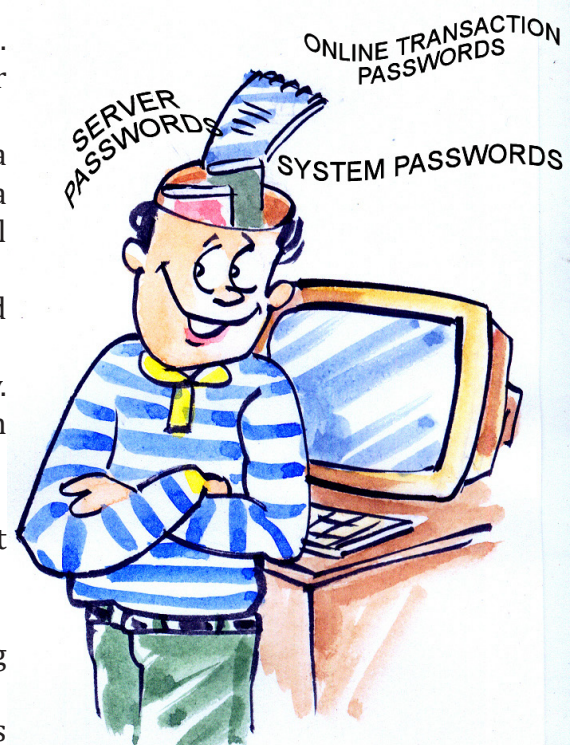


InfoSec Tip

Your brain is the best place to store your passwords

Guidelines for maintaining a good password

- Use at least 8 characters or more to create a password. More number of characters we use, the more secure is our password.
- Use various combinations of characters while creating a password. For example, create a password consisting of a combination of lowercase, uppercase, numbers and special characters etc..
- Avoid using the words from dictionary. They can be cracked easily.
- Create a password such that it can be remembered easily. This avoids the need to write passwords somewhere, which is not advisable.
- A password must be difficult to guess.
- Change the password once in two weeks or when you suspect someone knows the password.
- Do not use a password that was used earlier.
- Be careful while entering a password when someone is sitting beside you to avoid Shoulder surfing.
- Do not use the name of things located around you as passwords for any of your accounts.



Secure Usage of Credit & Debit Card/ATM

Security Threats

Identity theft

The fraudulent acquisition and use of person's private identifying information, usually for financial gain. It can be divided into two broad categories :

- **Application fraud**

Application fraud happens when a criminal uses stolen or fake documents to open an account in someone else's name. Criminals may try to steal documents such as utility bills and bank statements to build up useful personal information.

- **Account takeover**

Account takeover happens when a criminal tries to take over another person's account, first by gathering information about the intended victim, and then contacting their card issuer while impersonating the genuine cardholder, and asking for the mail to be redirected to a new address. The criminal then reports the card loss and asks for a replacement to be sent to a new address.

Credit card fraud

Credit card fraud is committed by making use of credit/debit card of others for obtaining goods or services. The threat emerge due to stealing of information like Credit card number, PIN number, password etc. Theft of cards and cloning of cards are also employed to commit such frauds without the knowledge of the original Card holder. Hackers use complex techniques like Phishing, Skimming etc. to gain credit card information from innocent users.

Be aware of social engineering attacks on mobile and bluetooth devices



Phishing

Phishing is a way of attempting to acquire information such as usernames, passwords, and creditcard details by masquerading as a trustworthy entity in an electronic communication. Phishing is typically carried out by e-mail spoofing or instant messaging and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one.

Skimming

Skimming is the theft of credit card / Debit card information. Thief can procure victim's credit card number using basic methods such as photocopying receipts or more advanced methods such as using a small electronic device (skimmer) to swipe and store hundreds of victim's credit card numbers. Common scenarios for skimming are restaurants or bars where the skimmer has possession of the victim's credit card and makes note of card details for further use.

Vishing

It is one of the method of social engineering over the telephone system, most often using features facilitated by Voice over IP (VoIP), to gain access to private personal and financial information from the public for the purpose of financial reward. The term is a combination of "voice" and "phishing".



Social Engineering

Social engineering involves gaining trust – hence the fraudster poses as a member of staff or even security guard. The fraudster would then ask the customer to check the card for damages. The fraudster would have gained confidence from his prey using various tactics such as offering assistance to the customer who perhaps would have tried to use the ATM without success or perhaps the customer who is not familiar with use of ATM machine and requires assistance.

Steps to be followed before Credit card & Debit card/ATM card usage :

- Whenever you receive the card from the bank make sure the mail is completely sealed and there is no damage.
- Whenever you receive the card from the bank immediately sign on the card.
- Try to cover the last three digit number on the card called CVV(Card Verifictaion Value).
- Register your phone number to check the account transactions.
- Change the pin number immediately once you receive it.

Secure usage of credit/Debit cards at Shopping malls and Restaurants

- Always keep an eye how the vendor swipe your card.
- Always make sure that the transactions happen at your presence.
- Never sign a blank credit card receipt. Carefully draw a line through blank portions of the receipt
- Don't give away your personal information in the survey forms given in restaurants/shopping malls.

Secure usage of credit / Debit card over internet

- Always use secure websites for transaction and shopping.
- Please look for signs of security.

*Identify security clues such as a lock image at the bottom of your browser,
A URL that begins with https:*

(These signs indicates that your purchases are secured with encryption to protect Your account information)

- Always shop with merchants whom you know and trusts.
- Always log off from any website after completing online transaction with your credit / debit card and delete the browser cookies and close the browser.
- Treat all e-mail messages with suspicion to avoid phishing scams. Do not respond to e-mail messages

asking for personal information including financial information, as banks do not ask for any such information.

- Never send payment information via e-mail. Information that travels over the Internet (such as e-mail) may not be fully protected from being read by outside parties.
- Please be careful when providing personal information online.
- Please be aware of promotional scams. Identity thieves may use phony offers asking for your personal information. Avoid responding to such calls.
- Please keep your passwords secret. Some online stores may require you to register with them via a username and password before buying. Online passwords should be kept secret from outside parties the same way as you protect your ATM PIN.
- Always make sure to use the virtual keyboard for net banking.
- While doing Online payments close all other tabs in the browser.



- Before you use an ATM, please ensure that there are no strange objects in the insertion panel of the ATM.(to avoid skimming)
- Shield the ATM pin number during transaction. Do carry the transaction receipts along. or Shred them after use.
- Please change your ATM PIN once in every 3 months advised by banks.
- Keep your credit card receipts to guard against transaction frauds, check your transactions against your monthly statement.
- Only carry those credit cards that you absolutely need.
- Shred anything that contain your credit card number written on it like receipt, bills etc.,
- Notify your credit card issues in advance of your change of address, then you change home address.
- If you lose your Credit/ Debit card, please report the loss immediately to the card issuer.
- When you dispose a card at the time of renewal/upgradation, please make sure to cut it diagonally before disposal.



- Don't accept the card received directly from bank in case if it is damaged or seal is open.
- Don't write your PIN number on your credit card or debit card.
- Don't carry around extra credit cards that you rarely use.
- Don't disclose your Credit Card Number/ATM PIN or CVV number to anyone.
- Don't hand over the card to anyone, even if he/she claims to represent the Bank.
- Don't get carried away by strangers who try to help you to use the ATM machine.
- Don't use the ATM machine if the device is not in good condition.
- Don't transfer or share your account details with unknown/non validated source.
- Don't access Netbanking or make payment using your Credit/Debit card from shared or unprotected computers in public places.
- Don't open unexpected e-mail attachments from unexpected sources or instant message download links. Delete suspicious e-mail immediately.
- Don't give out your account number over the phone unless you initiate the call and you know the company is reputable. Never give your credit card info out when you receive a phone call. (This is called Vishing)
- Don't provide your credit card information on a website that is not a secured site.
- Don't share any confidential information such as password, customer id, Debit card number, Pin CVV, DOB to any email requests, even if the request is from government authorities like Income Tax

department, Banks, RBI or any card associated company like VISA or Master card. They never ask.

- Don't address or refer to your bank account problems or your account details and password on social networking site or blogs.
- Don't store critical information like your ATM PIN number on your mobile phone.
- Disable automatic transfer of funds to linked Accounts.
- Don't keep your cards near magnets, which may erase the Information stored on the card's magnetic strip.

BE AWARE OF CREDIT/DEBIT CARD FRAUDS

Check for any Strange
Objects in the Inseration
panel of ATM

Don't share bank
account, Credit/Debit
card details through
e-mail or phone

Don't hand over
Debit/Credit Card to
Strangers
They may misuse



VULNERABILITY NOTES

CERT-In Vulnerability Note CIVN-2016-0140

Privilege Elevation Vulnerabilities in VMware Workstation and VMware Player

Software Affected

- VMware Workstation prior to 11.1.3
- VMware Player prior to 7.1.3

Overview

A vulnerability has been reported in VMware Workstation and VMware Player for Windows, which could be exploited by a local attacker to gain elevated privileges on the targeted system.

Description

This vulnerability exists in VMware Workstation and VMware Player for Windows due to improper referencing of an executable file.

Successful exploitation of this vulnerability could allow the attacker to gain elevated privileges of host operating system.

Solution

Apply appropriate fixes as issued by vendor
<http://www.vmware.com/security/advisories/VMSA-2016-0005.html>

0005.html

Vendor Information

<http://www.vmware.com/security/advisories/VMSA-2016-0005.html>

References

<http://www.vmware.com/security/advisories/VMSA-2016-0005.html>

VMWARE

<http://www.vmware.com/security/advisories/VMSA-2016-0005.html>

Security Tracker

<http://securitytracker.com/id/1035900>

CVE Name

CVE-2016-2077

For more details visit
<http://www.cert.org.in/>

CERT-In Vulnerability Note CIVN-2016-0138

Multiple Vulnerabilities in Google Chrome

Systems Affected

- Google Chrome Versions prior to 50.0.2661.102

Overview

Multiple vulnerabilities have been reported in Google Chrome which could be exploited by a remote attacker to execute arbitrary code, access sensitive information, bypass security controls and bypass same-origin restrictions on the targeted system.

Description

Multiple vulnerabilities have been reported in Google Chrome. These vulnerabilities are due to same origin bypass vulnerability in DOM, same origin bypass vulnerability in Blink V8 bindings, buffer overflow Vulnerability in V8, race condition in loader, directory traversal flaw via the "file" scheme in android system. A remote attacker could exploit

these vulnerabilities by enticing a user to visit a specially crafted web page.

Successful exploitation of these vulnerabilities could allow a remote attacker to execute arbitrary code, bypass security restrictions, access sensitive information, or cause a DoS condition.

Solution

Upgrade to Google chrome version 50.0.2661.102



***Beware of popups
promising gifts***

Browser JSGuard

Browser JSGuard is an extension to the web browser which works by detecting Hidden behaviors, Unauthorized Redirections and Encoded JavaScript in the incoming web pages. It is available for Google Chrome and Mozilla Firefox repositories for free of cost.

Features of Browser JSGuard

- Content/Heuristic based JS & HTML Malware protection
- Alerts the User on visiting Malicious Web pages
- Provides detailed analysis of webpage threats
- Ease of installation

Download links of Browser JSGuard:

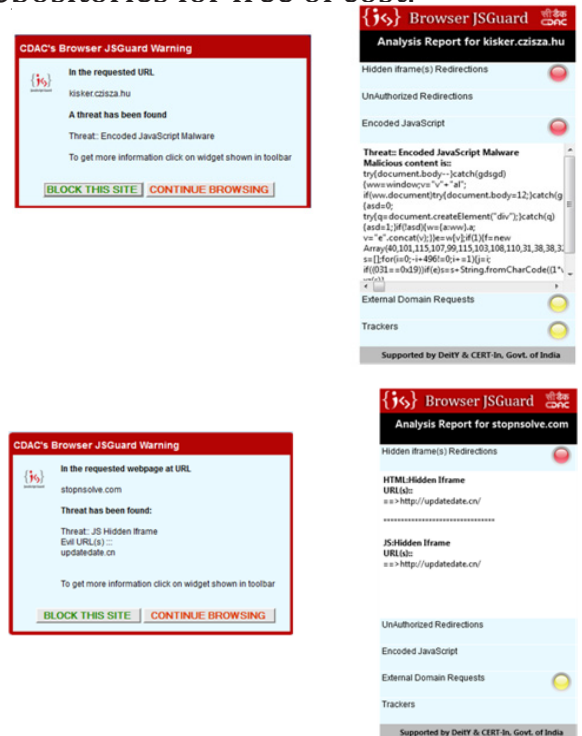
- **For Firefox web browser:**

<https://addons.mozilla.org/en-US/firefox/addon/browser-jsguard/>

- **For Google chrome web browser:**

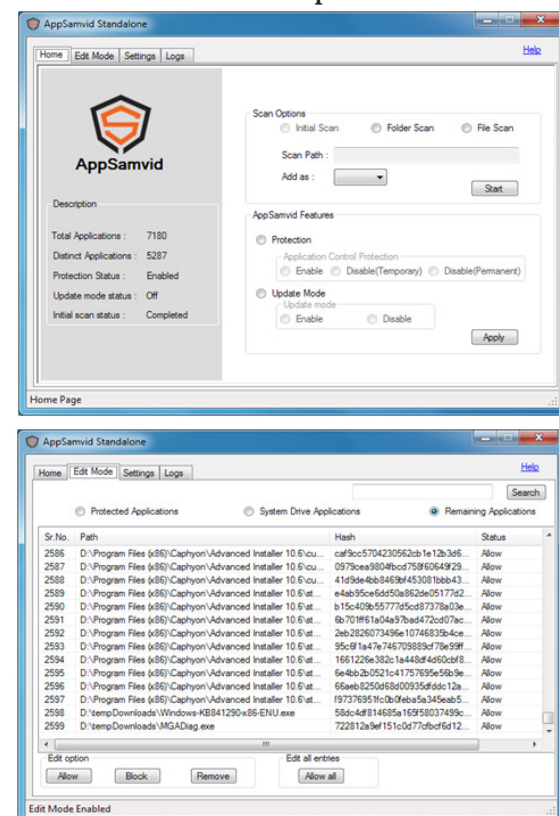
<https://chrome.google.com/webstore/detail/browserjsguard/ncpkigeklafkopcelcegambndlhkcbhb>

http://www.cdac.in/index.aspx?id=cs_eps_jsguard



AppSamvid - an application whitelisting software

AppSamvid is application whitelisting software which blocks the execution of unknown binaries in the computer.



Features of AppSamvid software are

- Whitelists .exe, dll, sys, .war, .jar and .class files
- Password based access to user interface
- Potential updater file(s) identification for 3rd party software
- To allow updating applications
- To allow installation of new softwares
- Automatic handling of Windows updates
- Password based uninstallation

Download link of AppSamvid Software:

http://www.cdac.in/index.aspx?id=dl_free_eps_solutions

http://www.cdac.in/index.aspx?id=cs_eps_appsamvid



VMware Updates Products to Patch Critical, Important Flaws

VMware has released updates for several of its products to patch a couple of vulnerabilities rated critical and important.

The critical vulnerability is related to how the RMI server of Oracle JRE JMX deserializes authentication credentials. A remote, unauthenticated attacker can leverage the weakness to cause deserialization flaws and execute arbitrary commands.

<http://www.securityweek.com/vmware-updates-products-patch-critical-important-flaws>

Aging and bloated OpenSSL is purged of 2 high-severity bugs

Maintainers of the OpenSSL cryptographic library have patched high-severity holes that could make it possible for attackers to decrypt login credentials or execute malicious code on Web servers.

The updates were released Tuesday morning for both versions 1.0.1 and 1.0.2 of OpenSSL, which a large portion of the Internet relies on to cryptographically protect sensitive Web and e-mail traffic using the transport layer security protocol. OpenSSL advisories labeled the severity of both vulnerabilities "high," meaning the updates fixing them should be installed as soon as possible. The fixes bring the latest supported versions to 1.0.1t and 1.0.2h.



The decryption vulnerability is the result of what cryptographers call a padding oracle weakness, which allows attackers to repeatedly probe an encrypted payload for clues about the plaintext content inside. According to TLS expert Filippo Valsorda, the bug allows for only 16 bytes of encrypted traffic to be recovered, and even then only when an end user sends it repeatedly. Still, the conditions might make it possible for an attacker with the ability to monitor the connection to obtain authentication cookies and other small chunks of encrypted text, Valsorda wrote. The vulnerability is indexed as CVE-2016-2107.

<http://arstechnica.com/security/2016/05/aging-and-bloated-openssl-is-purged-of-2-high-severity-bugs/>

Beware of keystroke loggers disguised as USB phone chargers, FBI warns

Private industry notification comes 15 months after debut of KeySweeper.

FBI officials are warning private industry partners to be on the lookout for highly stealthy keystroke loggers that surreptitiously sniff passwords and other input typed into wireless keyboards.

Meet KeySweeper, the \$10 USB charger that steals MS keyboard strokes

Always-on sniffer remotely uploads all input typed into Microsoft Wireless keyboards. The FBI's Private Industry Notification is dated April 29, more than 15 months after whitehat hacker Samy Kamkar released a KeySweeper, a proof-of-concept attack platform that covertly logged and decrypted keystrokes from many Microsoft-branded wireless keyboards and transmitted the data over cellular networks. To lower the chances that the sniffing device might be discovered by a target, Kamkar designed it to look almost identical to USB phone chargers that are nearly ubiquitous in homes and offices.

<http://arstechnica.com/security/2016/05/beware-of-keystroke-loggers-disguised-as-usb-phone-chargers-fbi-warns/>

Awareness Workshops



@St.Josephs Engineering College, Mangalore



@Mangaluru City Police



@Salem District Police



@DeitY, Delhi

To share tips / Latest news mail us to
pmu-isea@cdac.in

Follow us on Facebook
***https://www.facebook.com/
infosecawareness***

Follow us on Youtube
***https://www.youtube.com/channel/
UCWPBKQryyVvydUy4rYsbBfA***

Follow us on twitter
https://twitter.com/CDAC_ISEA

**For any queries on
Information Security**

**Call us on Tollfree No.
1800 425 6235**

**Between 10 A M to 6 PM
or give us a missed call,
we will call back within
24hrs**

**ISEA Whataspp Number for Incident
Report**

+91 9490771800

Between 9.00 AM to 5.30 PM

For more details visit
www.infosecawareness.in

Centre for Development of Advanced Computing (C-DAC), a Scientific Society of Department of Electronics and Information Technology, Ministry of Communications & Information Technology, Government of India, is primarily an R&D institution involved in design, development and deployment of Advanced Electronics and Information Technology Solutions, including the celebrated PARAM series of Supercomputers. The C-DAC, Hyderabad is working in R&D with a focus on system level programming, web technologies and embedded programming in the application domains of Network Security, e-learning, Ubiquitous Computing, India Development Gateway (www.indg.in), Supply Chain Management and Wireless Sensor Networks.



Department of Electronics & Information Technology,
Ministry of Communications & Information Technology,
Government of India



www.cdac.in

प्रगत संगणन विकास केन्द्र

CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING

संचार एवं सूचना प्रौद्योगिकी मंत्रालय की वैज्ञानिक संस्था, भारत सरकार

A Scientific Society of the Ministry of Communications and Information Technology, Government of India

Nalanda Building, No. 1 Shivabagh Satyam Theatre Road,
Ameerpet, Hyderabad - 500016, Telangana (India)

E-mail : isea@cdac.in

Plot No. 6 & 7, Hardware Park, Sy No. 1/1, Srisailem Highway,
Pahadi Sharief Via Keshevagiri (Post), Hyderabad - 500005, Telangana (India)