
# Retrospective 2017: Cybersecurity in Nepal

Suyash Nepal

# Who we are

- A tight-knit group of dedicated security professionals
- Regular involvement in security research
- Have assisted in securing tech giants like Google, Twitter & Facebook
- Intent on securing Nepali cyberspace


THREATNIX

# About The Research

- Cybersecurity Incidents in 2017
- Cybersecurity Status of Nepal
- Assessment of websites of public interest
- Most common security issues
- Nepal's presence in the Dark Web
- Fortify Nepali cyberspace

# Top Cybersecurity Incidents in 2017

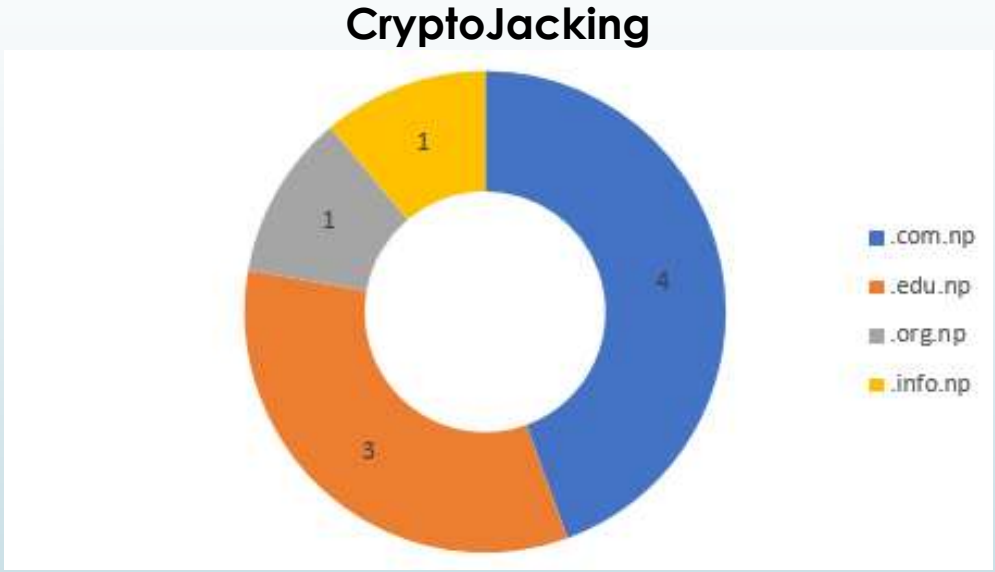
**Nepal**

- Website of Department of Passport Hacked
- NIC Asia Bank Heist
- 58 Government websites hacked
- OnlineKhabar Found Using Cryptominer

**Worldwide**

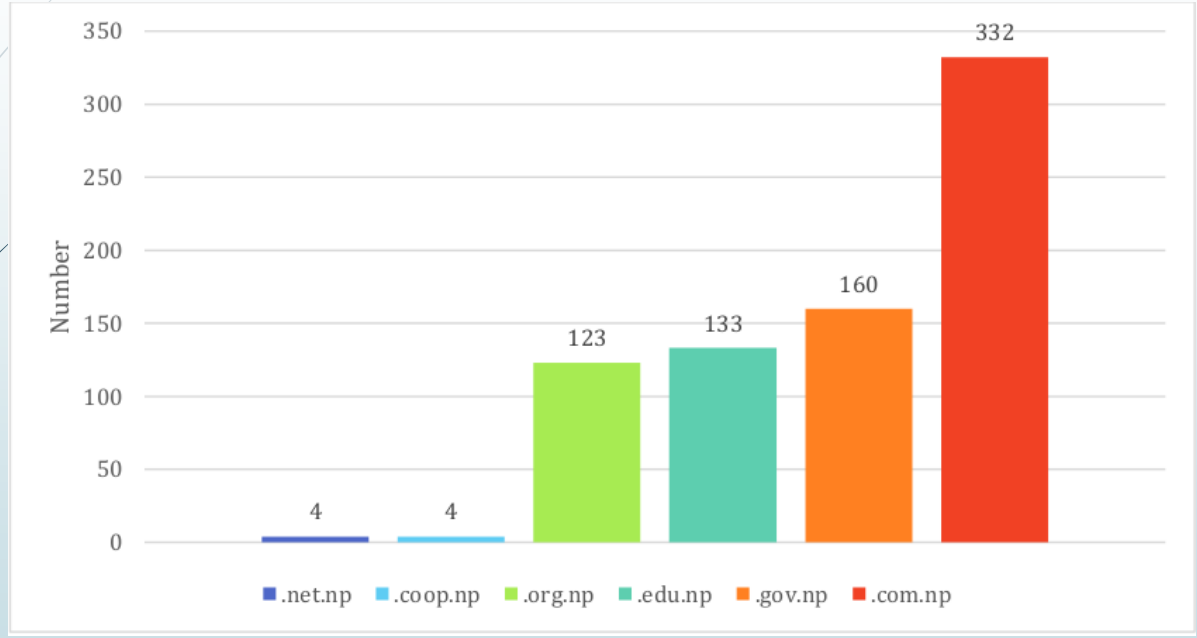
- Ransomware (WannaCry, Petya, NonPetya, Bad Rabbit)
- Cloudbleed
- KRACK
- Bitcoin Exchanges & ICO breaches
- Data Breaches

# Web Security



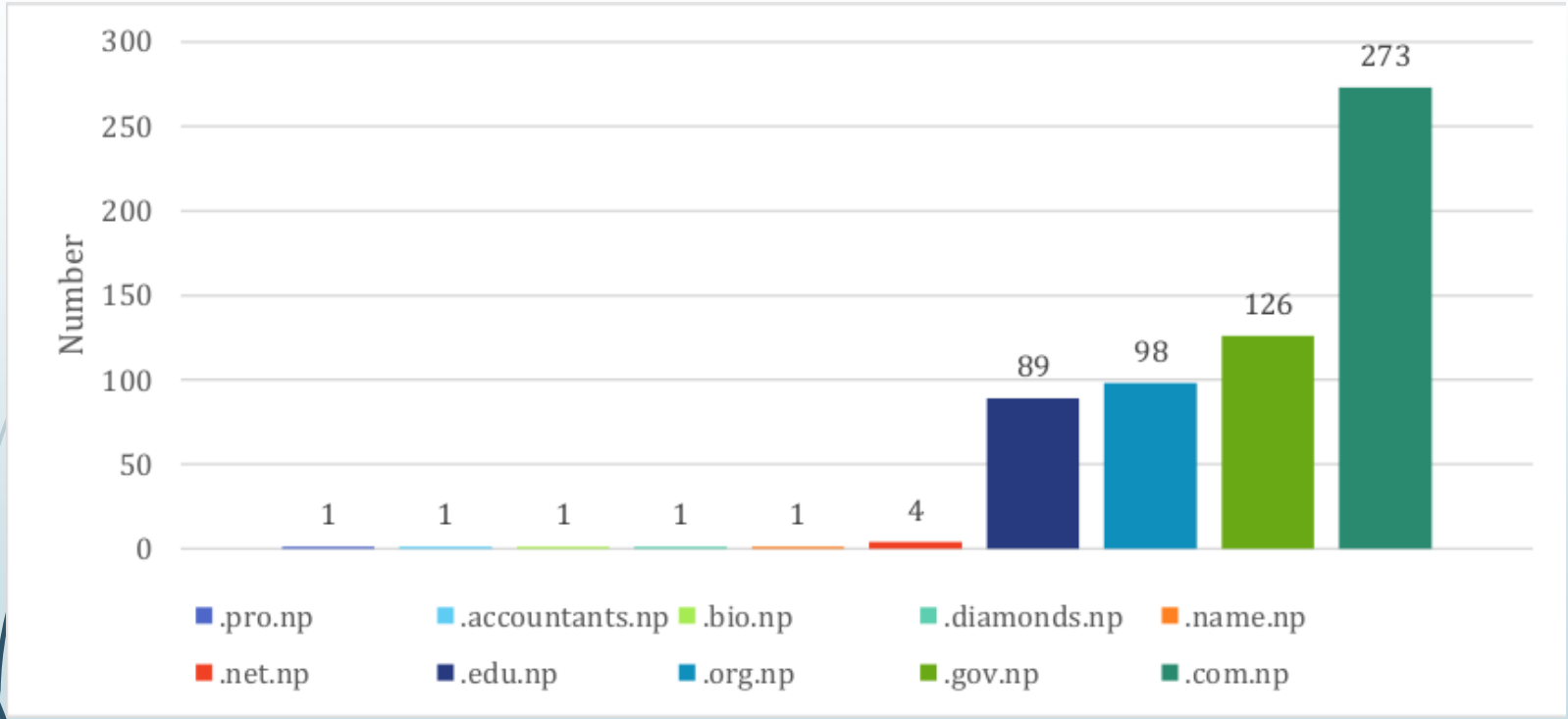

Number of TLDs involved in cryptomining

# Defaced Websites




Number of defaced websites categorized by TLDs

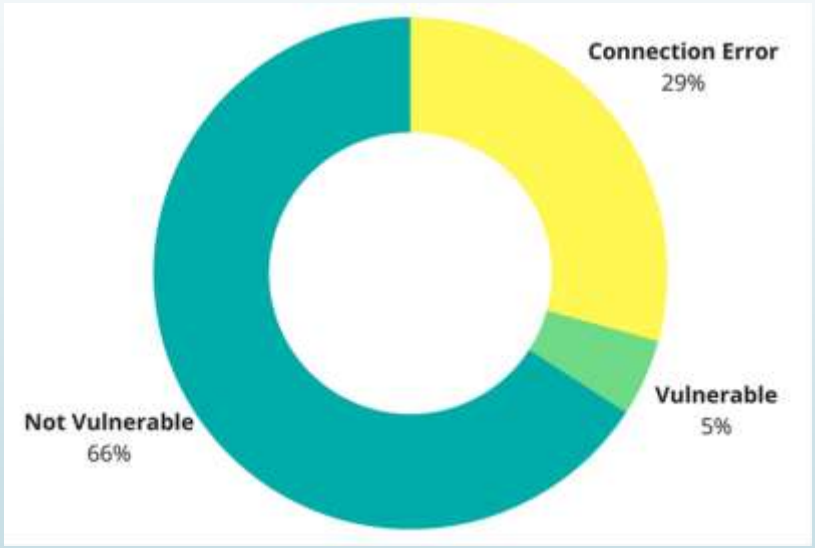
# Mass Defacement




Number of mass defaced TLDs

# Devices and Systems

**EternalBlue**

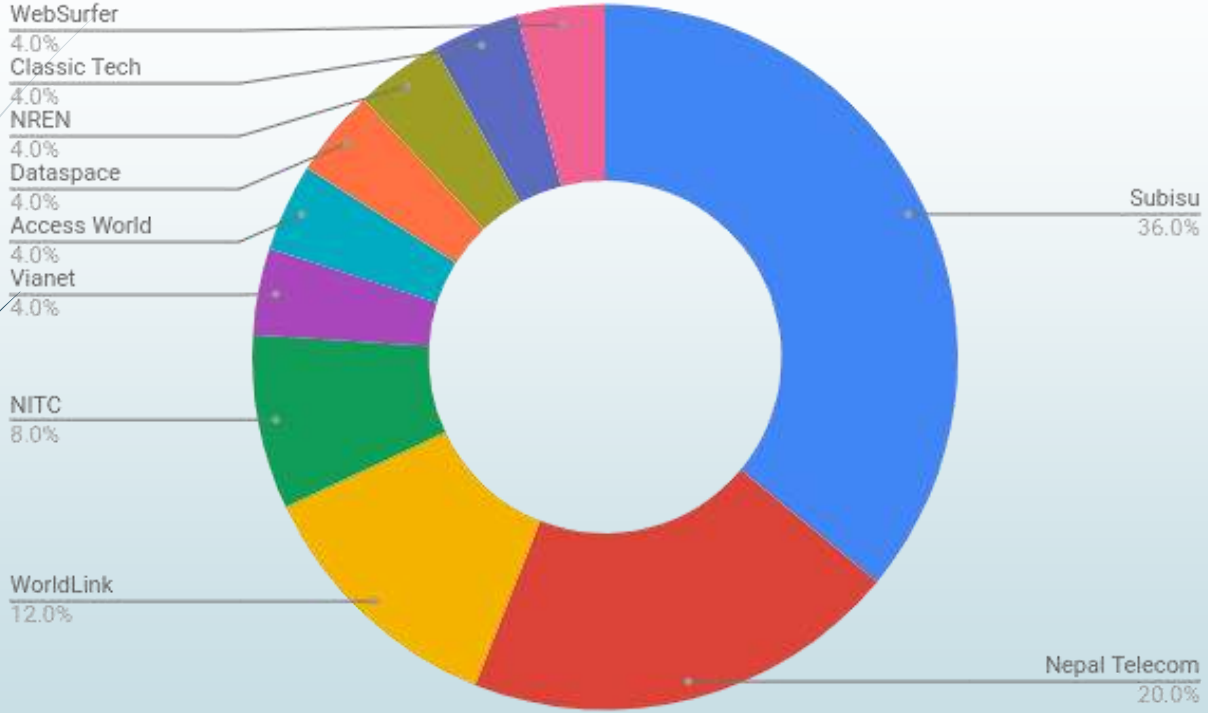



82 SMB enabled devices

Vulnerable to

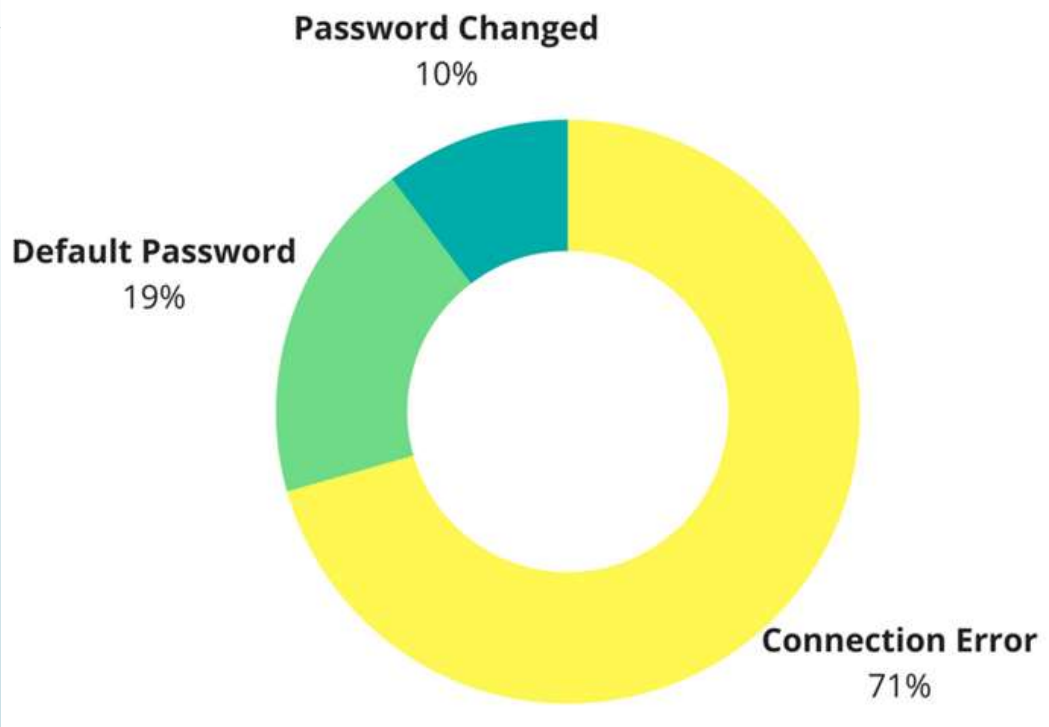
WannaCry

# HeartBleed



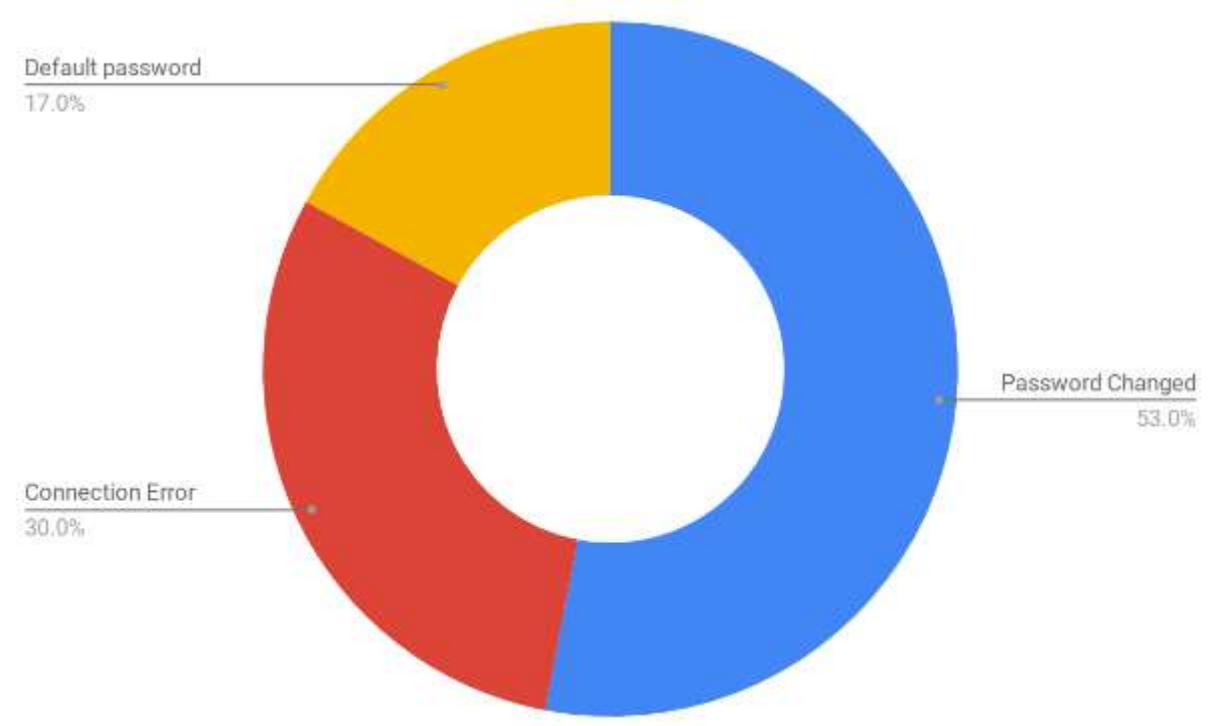

Number of hosts vulnerable to HeartBleed categorized by hosting organisation

# Wimax Devices



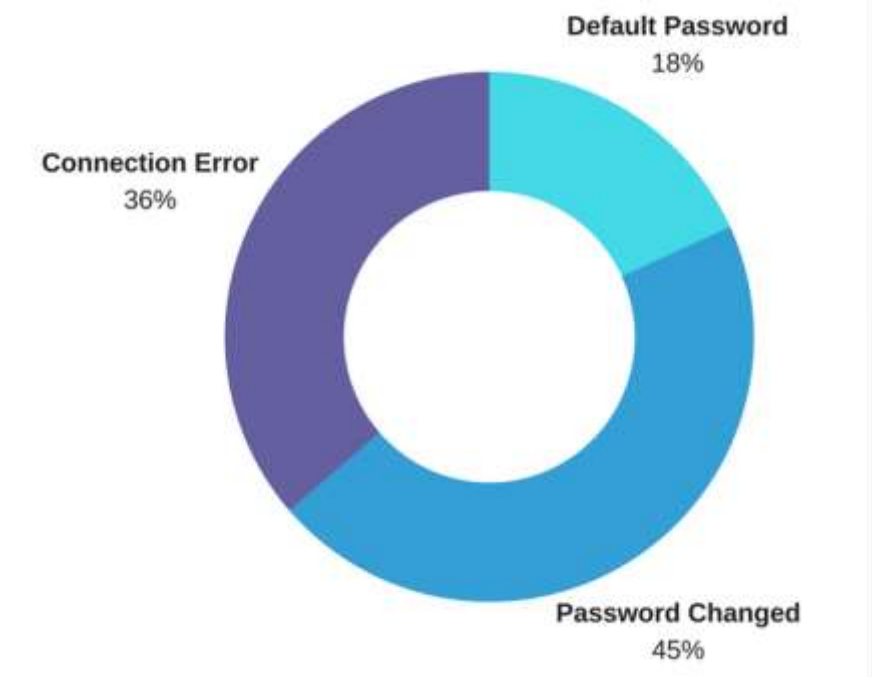

Wimax Devices with default credentials

# TP-Link Routers



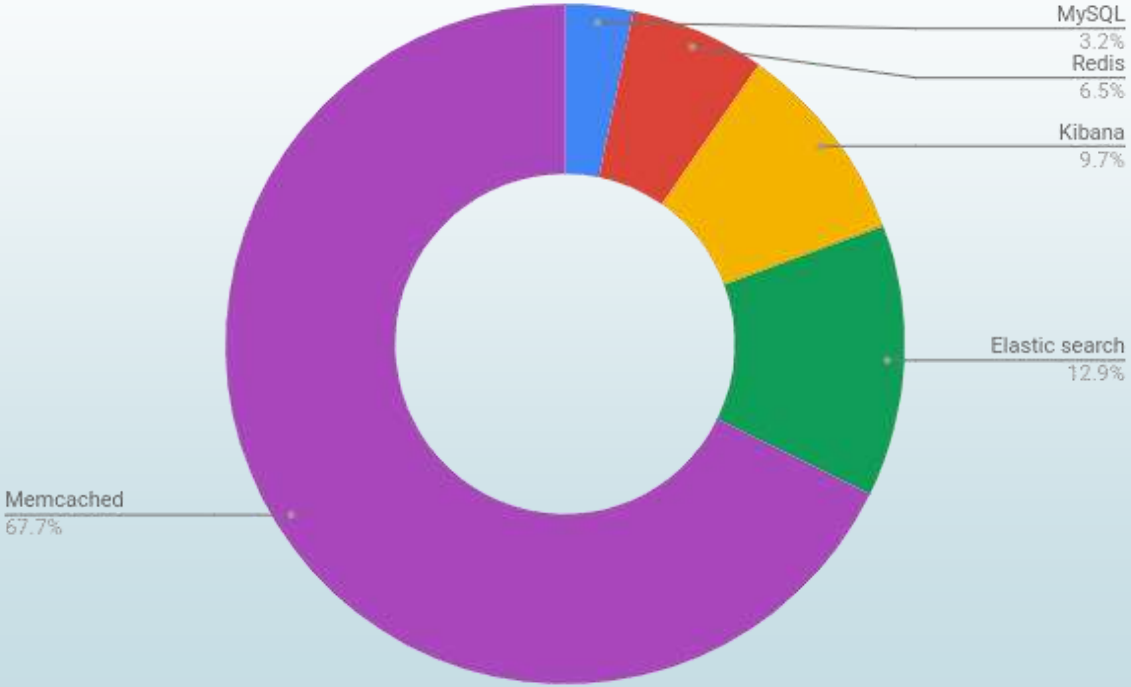

TP-Link routers with default credentials

# Passwords in Banner




Statistics of devices with password in their banner

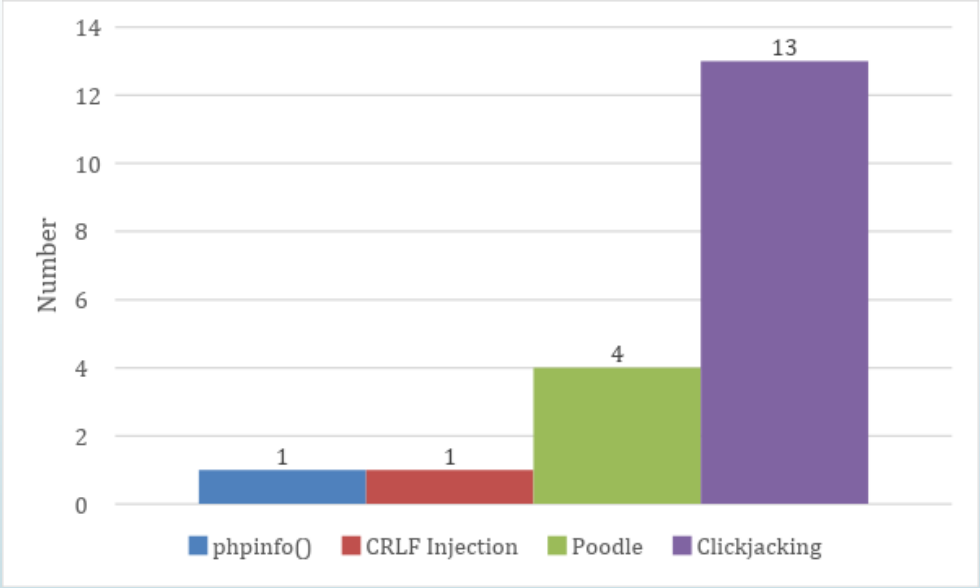
# Open Databases




Statistics of devices with password in their banner

# A-grade banks and payment gateways

- 27 e-banking sites
- 4 Online payment site
- 1 serious security flaw

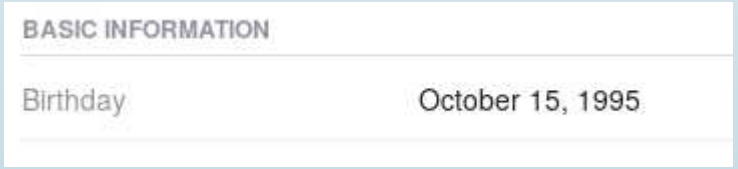


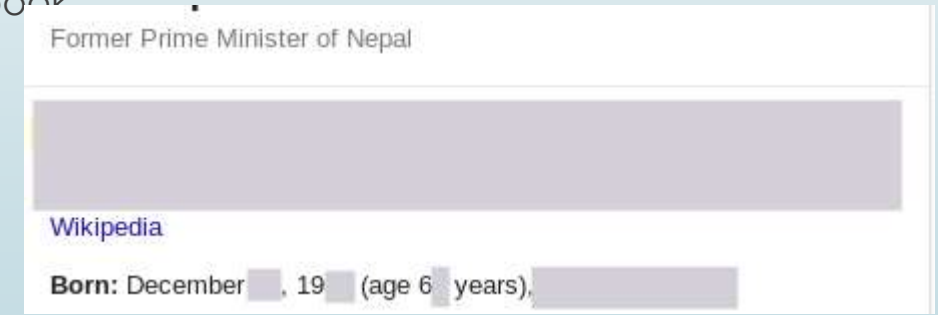

Statistics of A grade banks & Payment Service Providers

# Government data repositories

**Voter ID card**

- Contains personal information of 14,054,482 Nepalese who are eligible to vote
- What is needed for verification to see your information? **Birth-date**
- Yup people keep their birth-date a secret
- 8,700,000 Nepali people have Facebook



## PAN details

- Contains personal details of PAN holder
- Only requires PAN number which is basically incremental
- Great way to harvest personal information

# Nepal in Dark Web

- Almost 500 Nepali use TOR per day
- Nepali users and content depicting Nepali childrens found in child pornography forums
- Nepal considered as easy for paedophiles to exploit children
- Nepali drug sellers  found selling drugs within the dark web

# What can you do

- Build a proper security policy and implement it strongly
- Conduct periodic security tests and audits
- Consider all aspects of implementing a technology
- Provide periodic security awareness trainings to employees.
- Compartmentalise public, sensitive and, confidential data
- Keep everything updated and patched
- Get expert consultations if necessary

# Thank You

Vulnerability Analysis & Penetration Testing

Training & Consultation

Managed Cyber Security Services