NOIDA OWASP

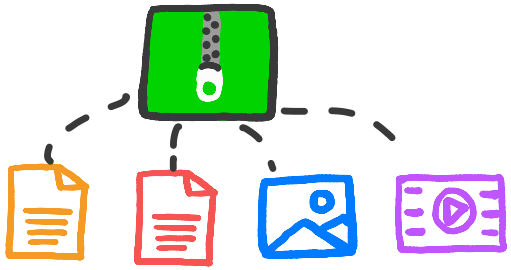
OWASP KALYAN

Phishing Campaign

Hunting Phishing Sites in the Wild without Phishing Kit

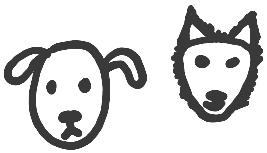
Ready-made templates & scripts

by @thebitdoodler



Beyond the Bio

Pet Parent

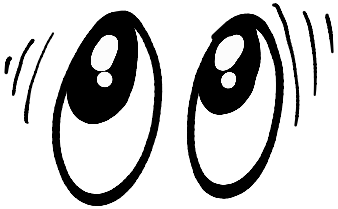


Security Researcher

Doodler

Biker

Co-Founder @SecurityZines.com

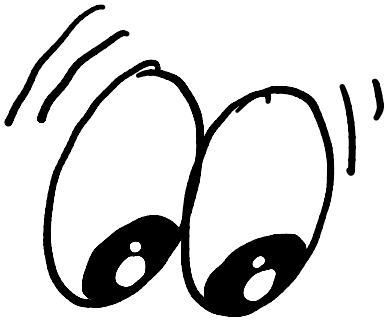


Agenda

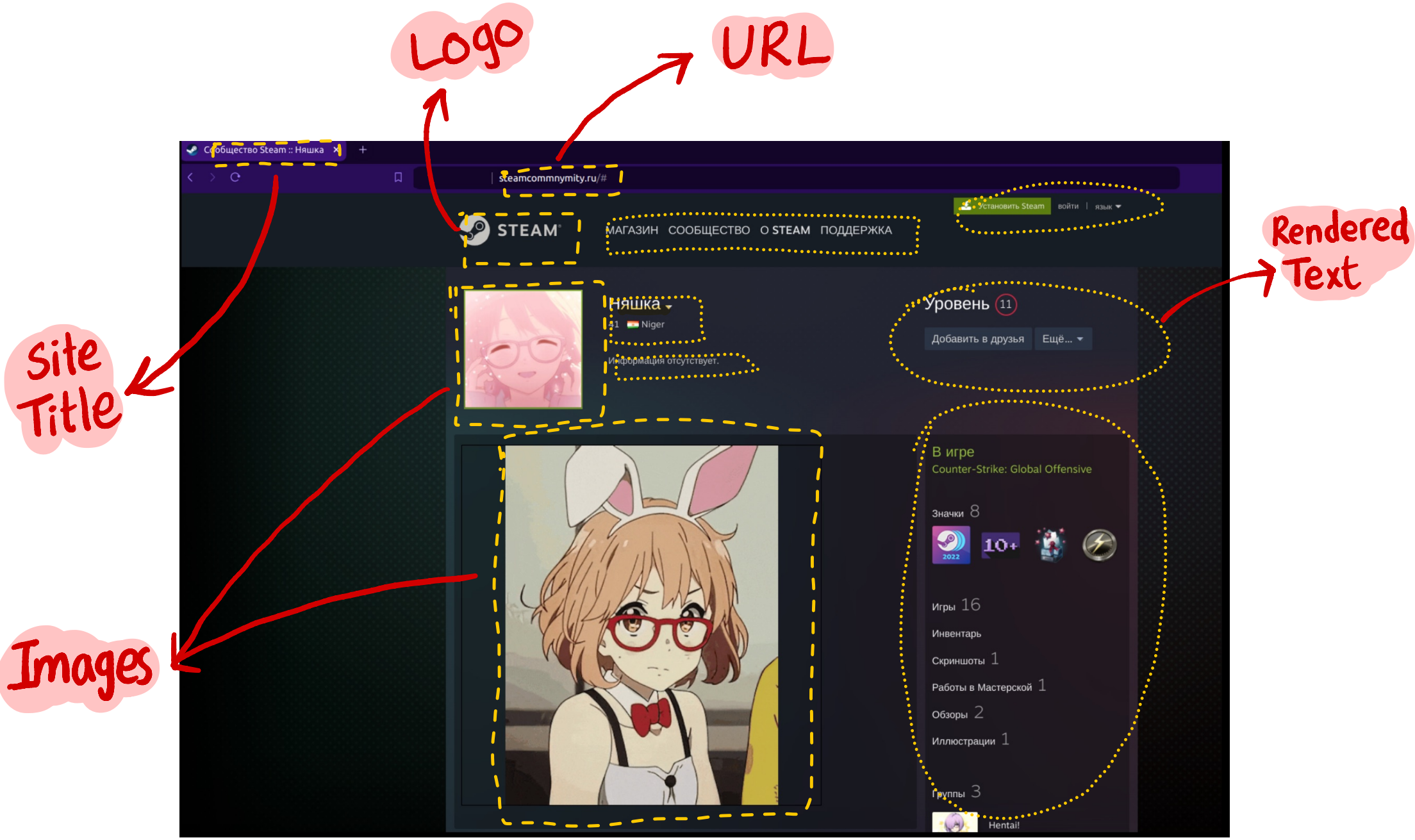
- Basic Structure of a Phishing Site
- Phases of a phishing Campaign - from an Actor's Lens
- How to get an active phishing link
- Analyzing the phishing site
- Automation

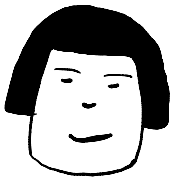
main Agenda

Ram naam Satya...

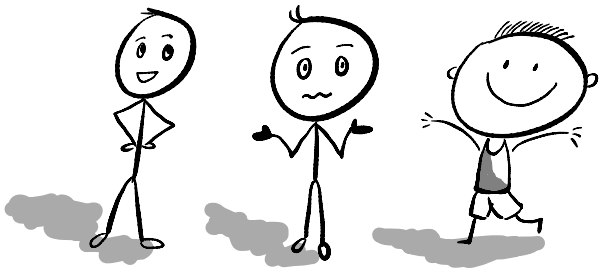


Basic Structure of a Phishing Site


Logo
URL
Site Title
Images
Rendered Text
Сообщество Steam :: Няшка
steamcommnymity.ru/#
STEAM
МАГАЗИН СООБЩЕСТВО О STEAM ПОДДЕРЖКА
Установить Steam
войти
язык
Няшка
11
Niger
Информация отсутствует.
Уровень 11
Добавить в друзья
Ещё...
В игре
Counter-Strike: Global Offensive
Значки 8
10+
Игры 16
Инвентарь
Скриншоты 1
Работы в Мастерской 1
Обзоры 2
Иллюстрации 1
Группы 3
Hentai!

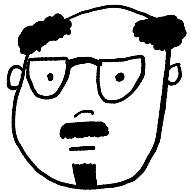


Phases of a Phishing Campaign



① Selection of a target

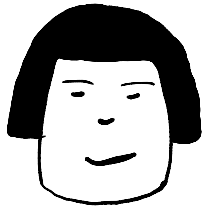
- Trends
- user base
- Financial gain



hosting provider

② Create / find a phishing kit

- Buy / clone
- Obfuscation
- necessary Config



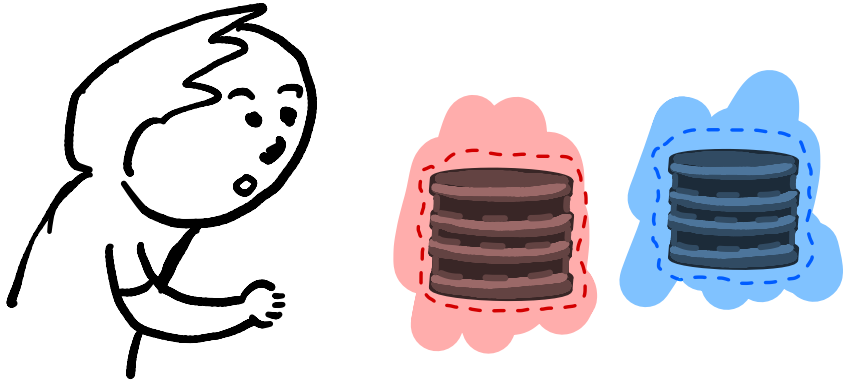
③ Selection of Infrastructure

- Less regulation
- Shedy / self-owned infra
- Freemium services

④ Find distribution medium

- SMS
- Email
- Social media
- SEO Poisoning

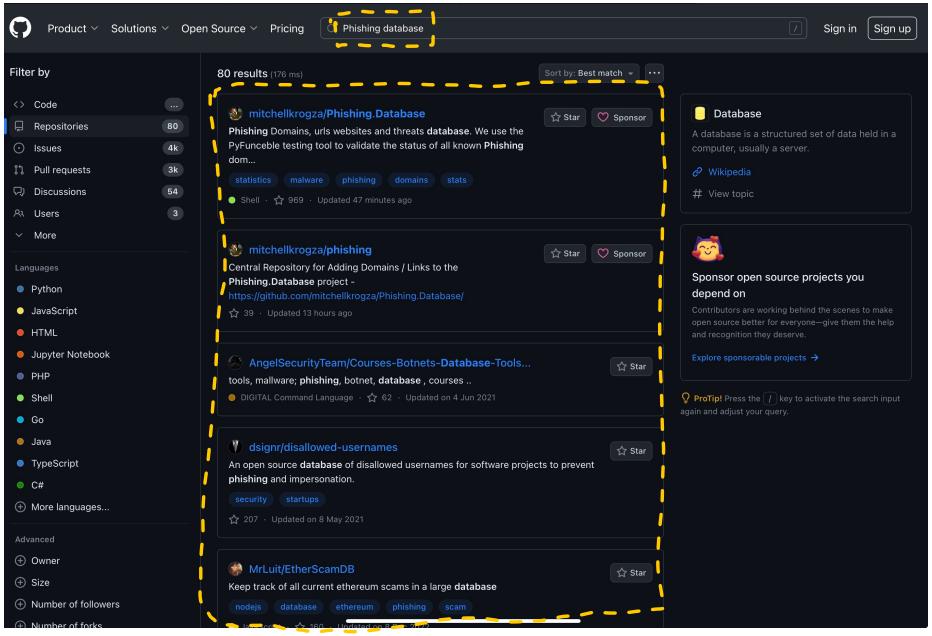
How to Get an Active Phishing Link



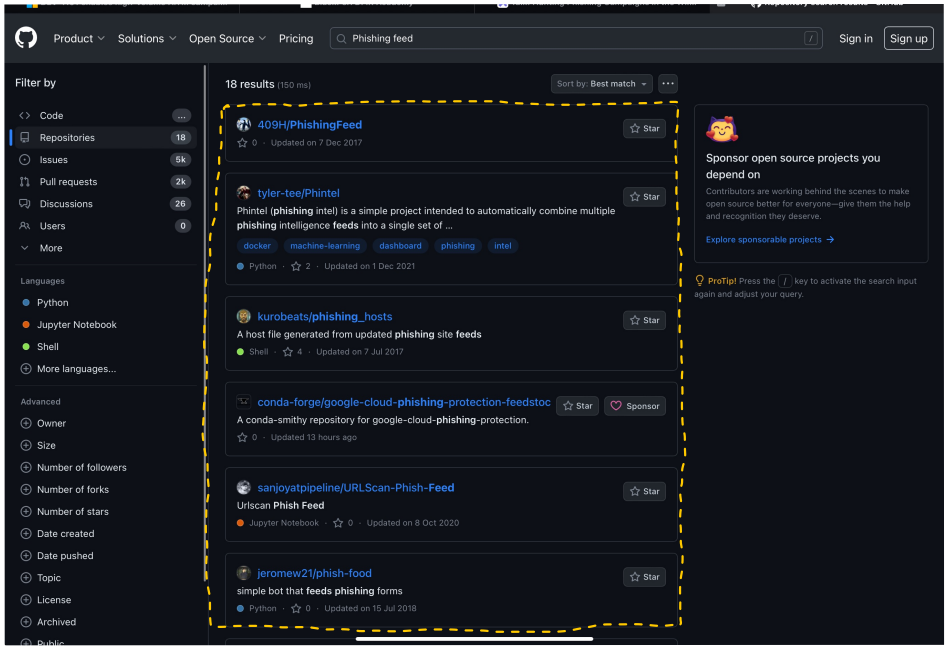
Open Source ❤

GitHub

Search "Phishing database"



Search "Phishing Feed"

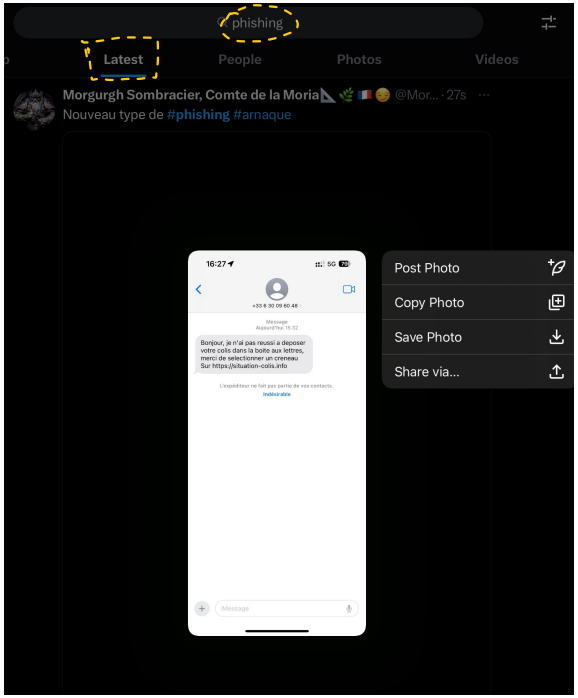


Open Source ❤

Twitter/X

Search

x.com/explore > " phishing " > Latest



Accounts

- @PhishFort
- @noladefense
- @PhishStats
- @PhishFindR
- @illegalFawn

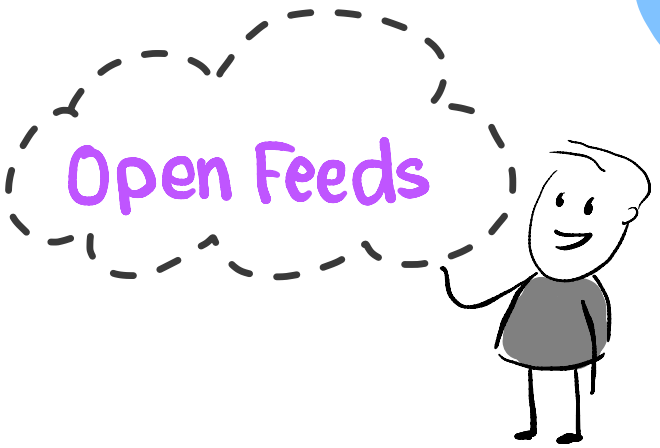
Open Source ❤

PhishTank

- Commuity Based by Cisco Talos Intelligence Gp.
- Provides API access

AlienVault OTX

- Community driven
- owned by AT&T
- Malicious& Phishing



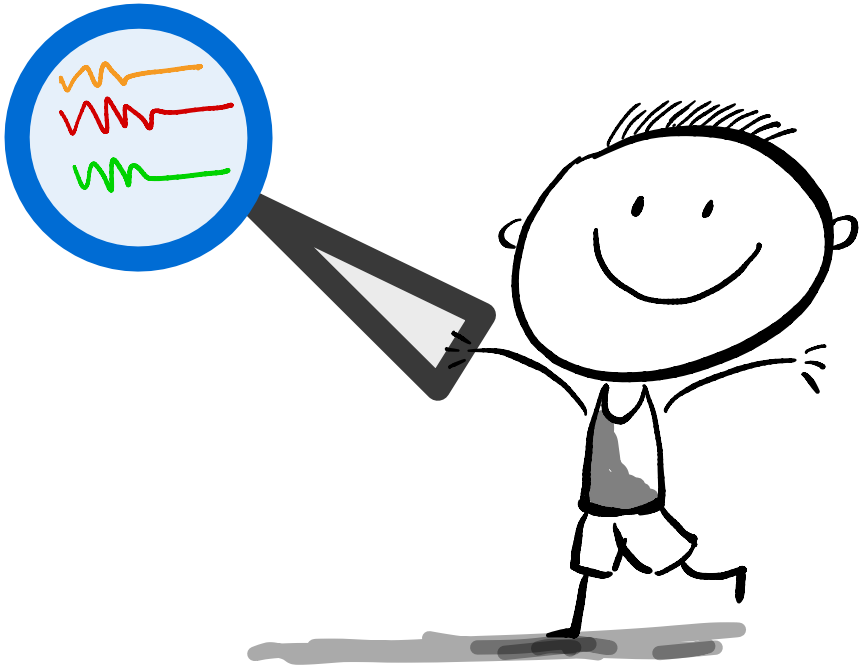
OpenPhish

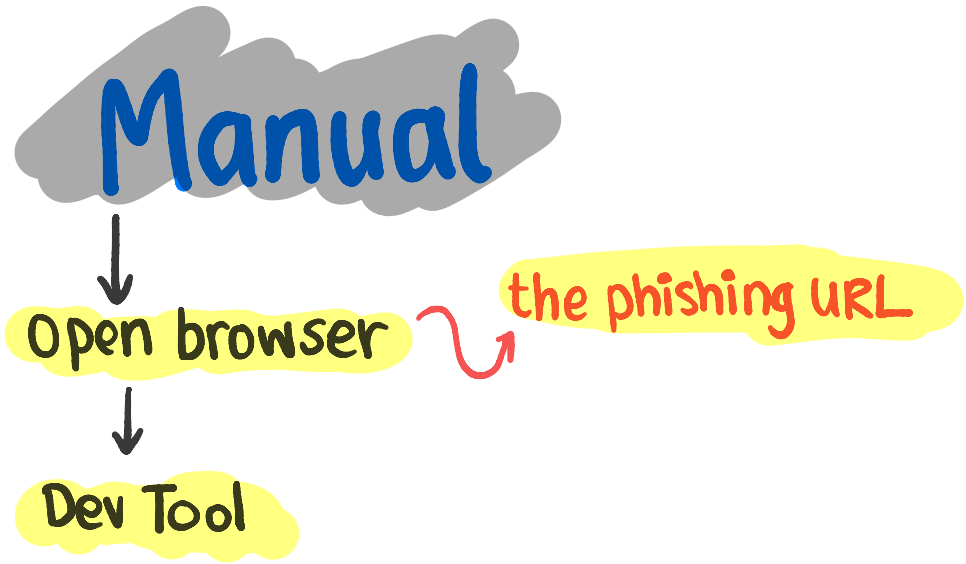
- Free to use
- Community Feeds

Urlhaus

- Malicious feeds
- abuse.ch

Analyzing a Phishing Site





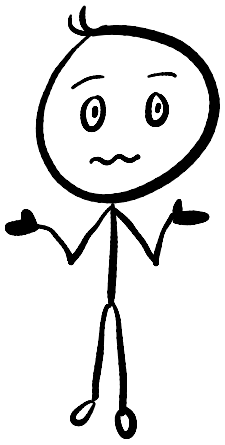
Automated

Manual

Open browser

Dev Tool

How??



Automated

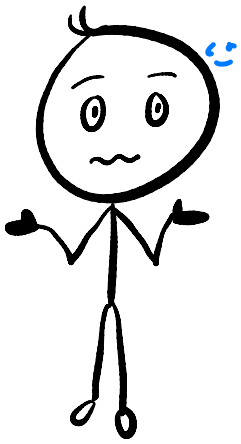
Manual

Automated

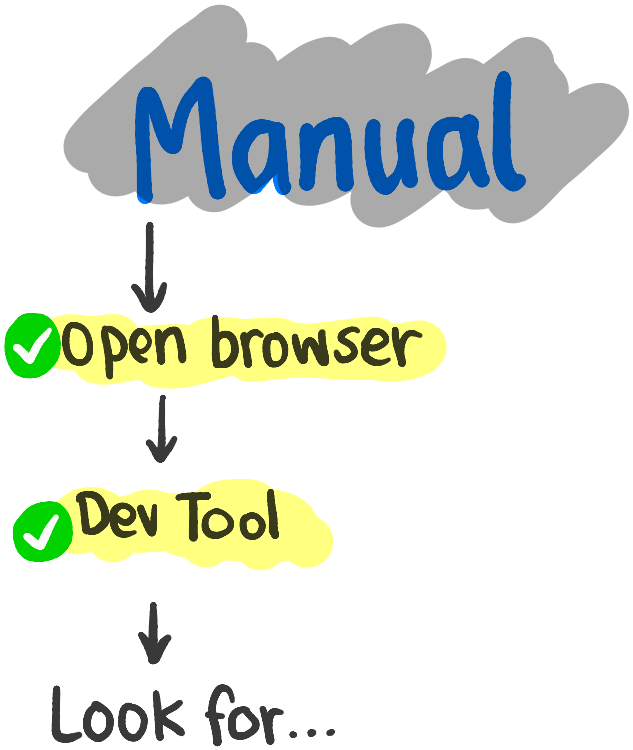
Open browser

Dev Tool

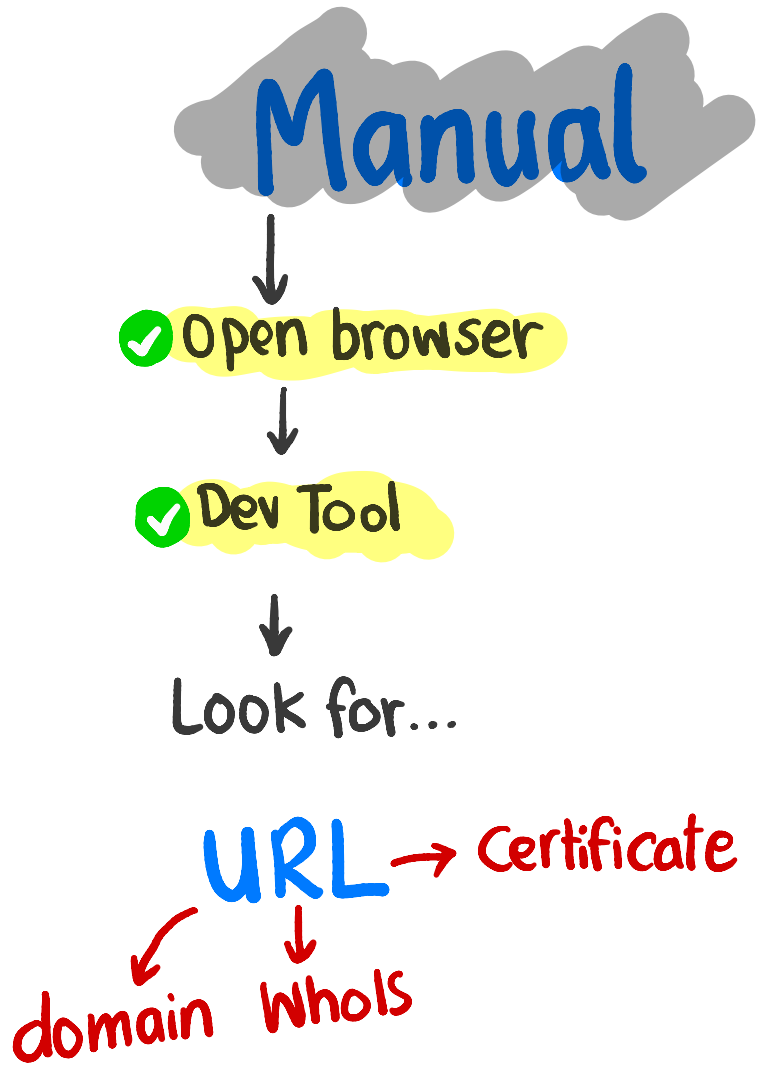
How??



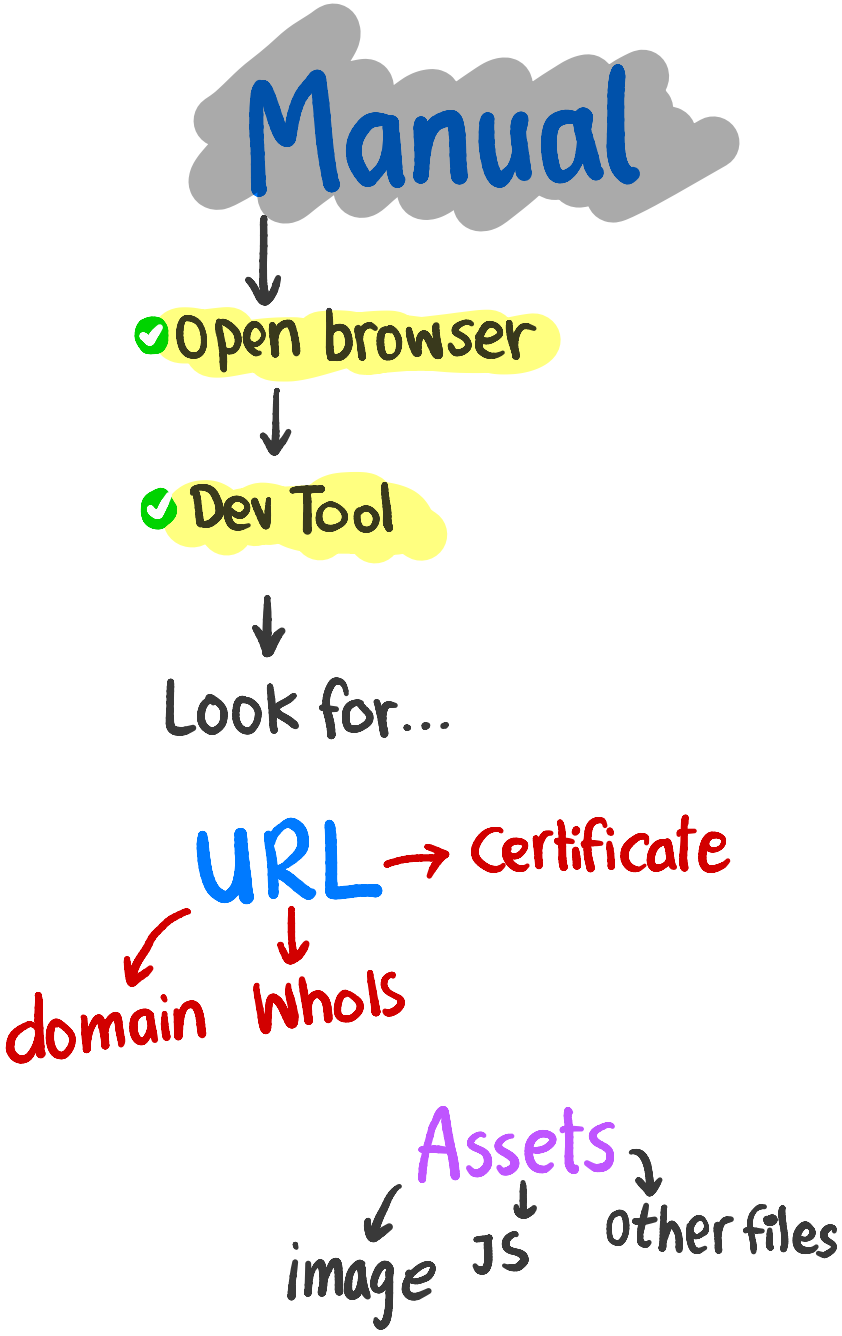
+ shift + i



Automated

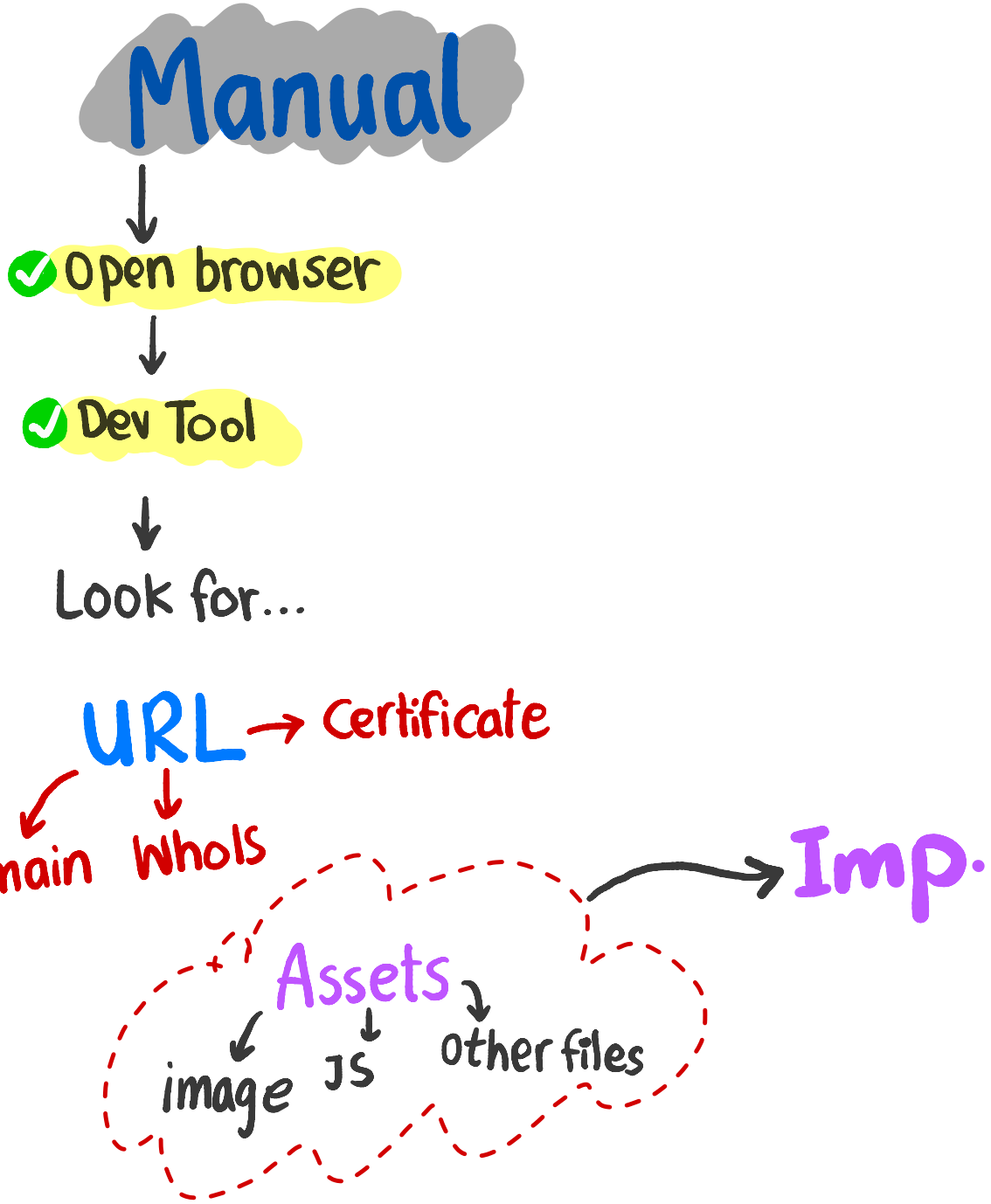

Manual
Open browser
Dev Tool
Look for...
URL
Certificate
domain
WhoIs

Automated


Manual
Open browser
Dev Tool
Look for...
URL
Certificate
domain
WhoIs
Assets
image
JS
other files

Automated

Manual



Automated

Manual

- Open browser
- Dev Tool
- Look for...
  - URL → Certificate
    - domain
    - WhoIs
  - Assets
    - image
    - JS
    - other files

Automated

karte kuch prabandh...

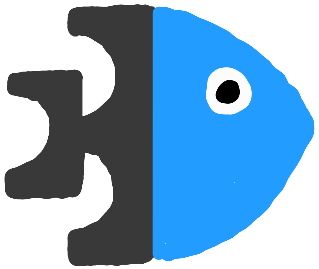
Mere pas ek
mast plan h ...

DEMO
aapke screen pe ye raha...

"aayien"

Automation

urlscan.io



ChekPhish.ai

phish.report

Demo Time

Ab underground hone ka samay aa gya h...

Thik Hai Bhai!
Mai Chalta Hoon...

you can't see my tweets

if don't follow ME

@thebitdoodler

DM's are open