



# Hackers.

Transfigoroute Holland

---

Door Harm Blankers en Jan van der Put

**REQON**  
SECURITY

# 01 \$whoami

## Harm Blankers



# 01 \$whoami

Jan van der Put



# 01 Who are we?

## Wat doet REQON Security

- **Penetrationtesting**
- **Incident Response & Digital Forensics**
- **IT-Security Consultancy**



# 01 Who are we?

**Kwetsbaarheden gemeld in o.a. :**

- Facebook**
- Marktplaats**
- De Nederlandse Loterij (Toto)**
- OnStage**



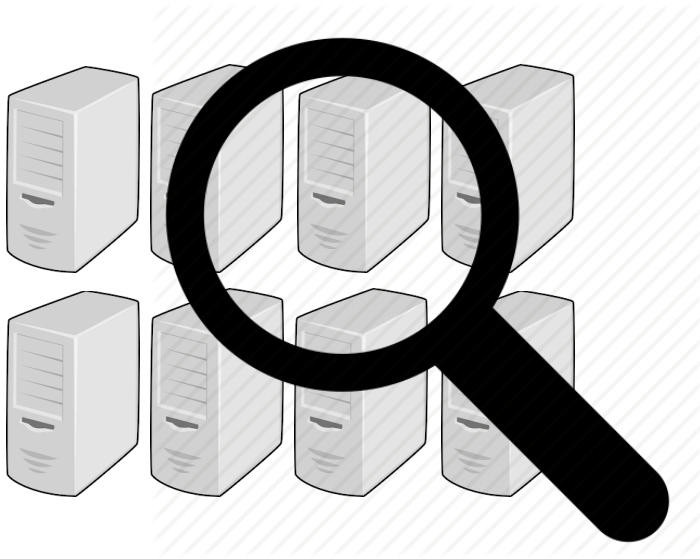
# 01 Hacking



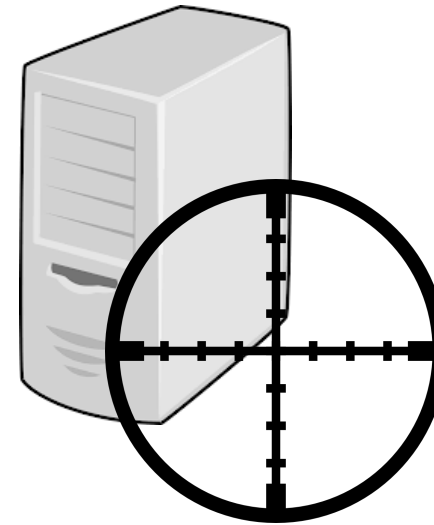
**“The ability to predict and detect human error, and the knowledge to exploit them”**



# 02 Hacking als dreiging



Massa gerichte hacker



Doelgerichte hacker



# 03 Massa gerichte hacker



Methode staat vast



Doelwit onbekend





# 03 Massa gerichte hacker

Methode bepalen:

[exploit-db.com](https://www.exploit-db.com)

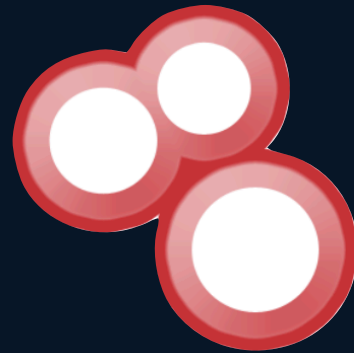
**EXPLOIT**   
**DATABASE**



# 03 Massa gerichte hacker

Doelwit bepalen:

[shodan.io](https://shodan.io)



# SHODAN



# 03 Massa gerichte hacker

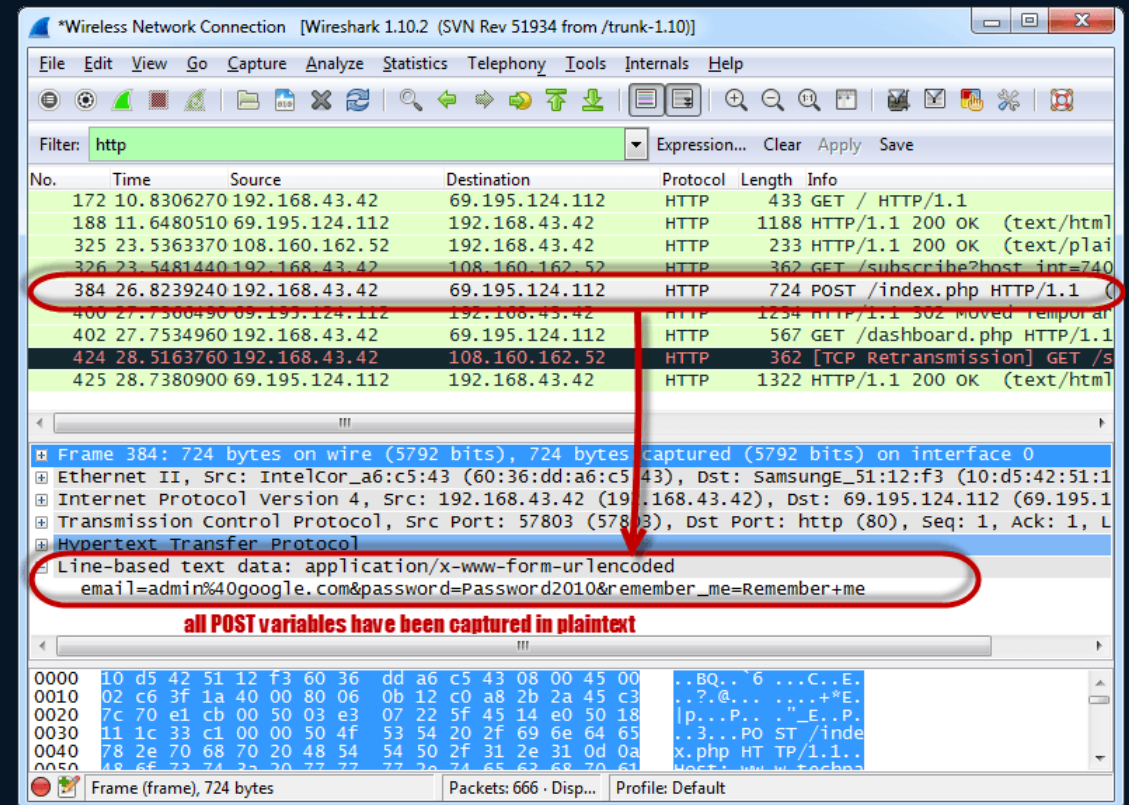
Ingebroken in de router



# 03 Massa gerichte hacker

We zijn binnen. Wat nu?

- Password sniffing
- Services open zetten
- Toegang tot file shares



# 03 Massa gerichte hacker

Ransomware maken  
was nog nooit zo eenvoudig

Create your own ransomware! x +

Search

## Create new ransomware

Bitcoin address for receiving your cut.

Ransom. Minimal ransom is 0.01 BTC. Maximum is 1 BTC

Please enter captcha.

047927

GET YOUR RANSOMWARE!

### What is this?

This is ransomware. Once launched on the computer it will encrypt files and demand ransom.

Other features of the service:

- No registration required.
- Ransom from 0.01 BTC to 1 BTC.
- Automatic payouts.

### How can I earn money with it?

Create it using the form on top of the page and spread it. Once someone pays the ransom you will get part of the paid money(90%). Please note that we take 10% commision from paid ransoms.

### Contacts and support

XMPP:

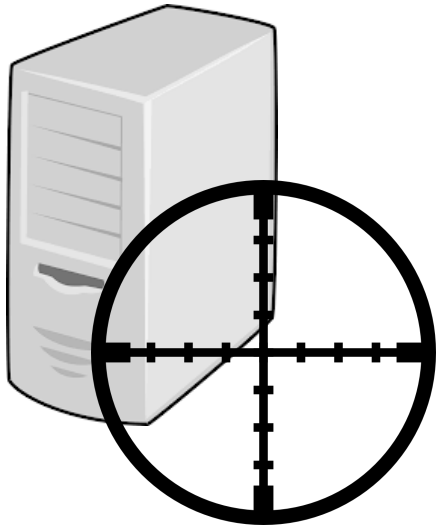


# 03 Massa gerichte hacker

Rinse and repeat, want...



# 04 Doelgerichte hacker



Doelwit staat vast



Methode nog onbekend



# 04 Doelgerichte hacker

Fase 1:

Onderzoek het doelwit  
a.k.a. **Reconnaissance**

Reconnaissance

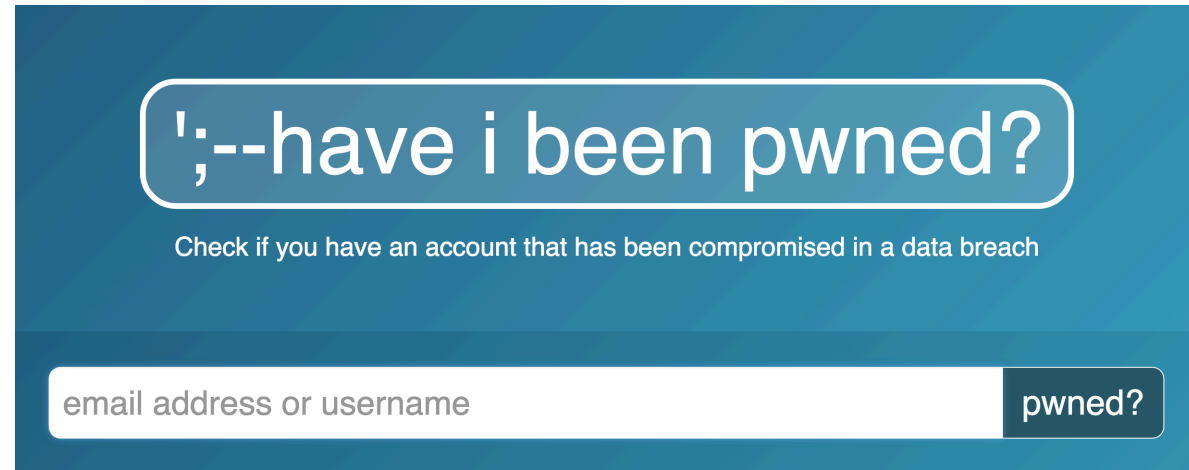




# 04 Doelgerichte hacker

Onderzoek naar personen:

[haveibeenpwned.com](https://haveibeenpwned.com)



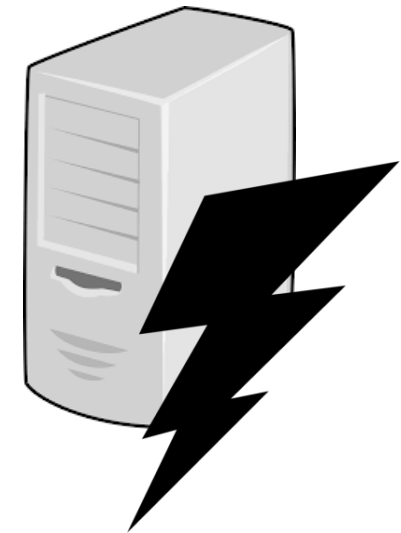
The image shows a screenshot of the 'have i been pwned?' website. The main heading is 'have i been pwned?' in a white, rounded box on a dark blue background. Below the heading is the text 'Check if you have an account that has been compromised in a data breach'. At the bottom, there is a search bar with the placeholder text 'email address or username' and a button labeled 'pwned?'.



# 04 Doelgerichte hacker

Fase 2:

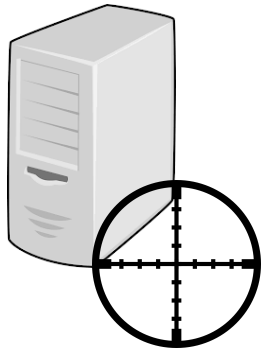
Onderzoek het doelwit op  
kwetsbaarheden in zijn systemen



# 04 Doelgerichte hacker

Fase 3:

Uitbuiten van kwetsbaarheid voor resultaat



of



# Fin.

## Contact

---



Harm Blankers



[/in/hblankers](https://www.linkedin.com/in/hblankers)



Jan van der Put



[/in/jvdput](https://www.linkedin.com/in/jvdput)

<https://reqonsecurity.nl>

