YACHT

a Randstad company

How to hack a website

Thomas van der Berg

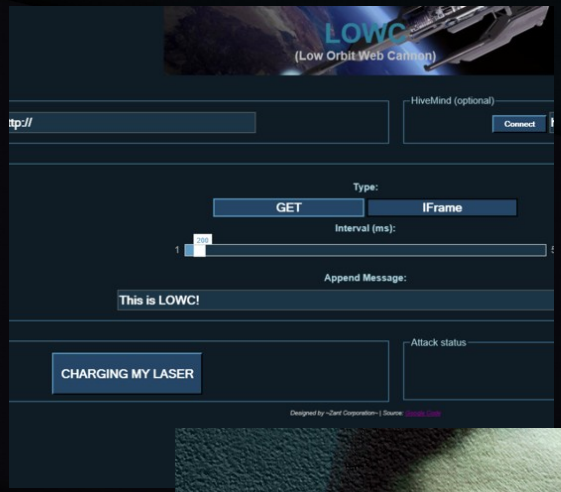
- Thomas van der Berg, IT security specialist
- Programmeren in JavaScript, C#, Python, C, Go (!)
- OSCP, CEH
- thomasvanderberg.nl

YACHT

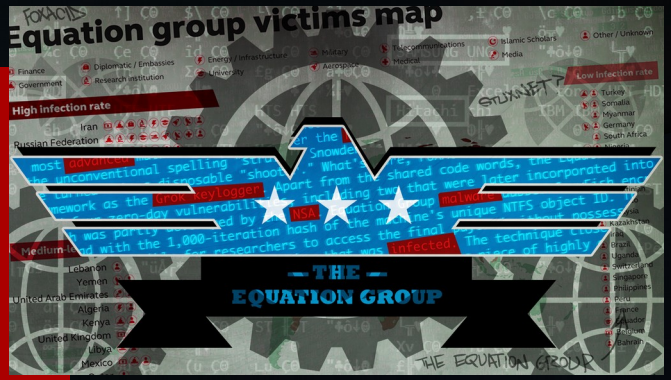
a Randstad company

- Koppelt professionals & bedrijven
- Yacht stand -> Hacking challenge

Wat is hacking?


LOWC
(Low Orbit Web Cannon)
HiveMind (optional)
Connect
Type:
GET
IFrame
Interval (ms):
200
Append Message:
This is LOWC!
Attack status
CHARGING MY LASER


PRESS ANY KEY!


Equation group victims map
High infection rate
Low infection rate
Medium
THE
EQUATION GROUP
THE EQUATION GROUP


SILENCE
2.0

ZERODIUM Payouts for Desktops/Servers*

Windows
macOS
Linux/BSD
Any OS

RCE: Remote Code Execution
LPE: Local Privilege Escalation
SBX: Sandbox Escape or Bypass
VME: Virtual Machine Escape

Up to $1,000,000										1.001 Win RCE Zero Click (Win)
Up to $500,000							3.001 Chrome RCE+LPE (Win)	2.001 Apache RCE (Linux)	2.002 MS IIS RCE (Win)	
Up to $250,000					5.001 MS Outlook RCE (Win)	4.001 MS Exchange RCE (Win)	2.003 OpenSSL RCE (Linux)	2.004 PHP RCE (Linux)		
Up to $200,000	6.001 VMware ESXi VME	5.002 Thunderbird RCE (Win/Linux)		4.002 Sendmail RCE (Linux)	4.003 Postfix RCE (Linux)	4.004 Dovecot RCE (Linux)	4.005 Exim RCE (Linux)	2.005 nginx RCE (Linux)		
Up to $100,000		3.002 Safari RCE+LPE (Mac)	3.003 Edge RCE+LPE (Win)	3.004 Firefox RCE+LPE (Win)	5.003 Word/Excel RCE (Win)	7.001 WordPress RCE (Linux)	7.002 cPanel/WHM RCE (Linux)	7.003 Plesk RCE (Linux)	7.004 Webmin RCE (Linux)	
Up to $80,000	6.002 VMware WS VME (Win/Linux)					5.004 Adobe PDF RCE+SBX (Win)	5.005 WinRAR RCE (Win)	5.006 7-Zip RCE (Win)	6.003 Windows LPE/SBX (Win)	
Up to $50,000	6.004 USB LPE (Win/Mac)	8.001 Antivirus RCE (Win)			5.007 WinZip RCE (Win)	5.008 tar RCE (Linux)	6.005 macOS LPE/SBX (Mac)	6.006 Linux LPE (Linux)	6.007 BSD LPE (BSD)	
Up to $10,000	9.001 Routers RCE	8.002 Antivirus LPE (Win)	7.005 phpBB RCE (Linux)	7.006 vBulletin RCE (Linux)	7.007 MyBB RCE (Linux)	7.008 Joomla RCE (Linux)	7.009 Drupal RCE (Linux)	7.010 Roundcube RCE (Linux)	7.011 Horde RCE (Linux)	

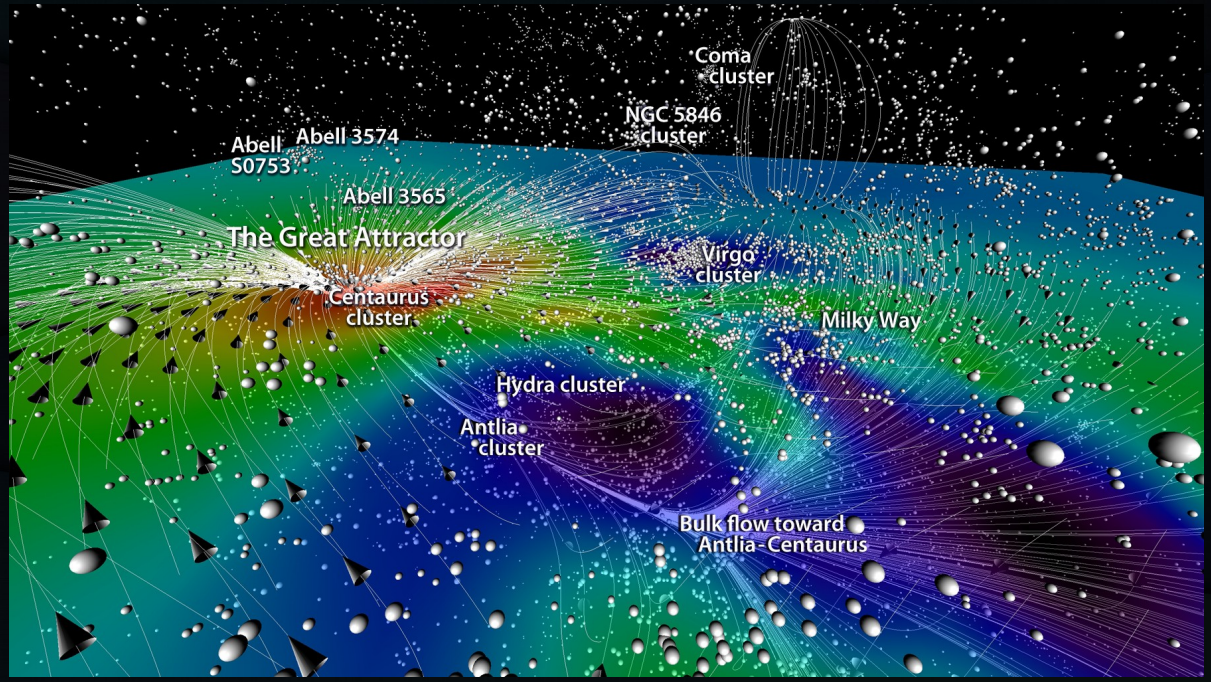
** All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.*

Werkzaamheden van de verdediging:

- Vulnerability scanning
- Pentesting <--
- Security research
- Monitoring

Domeinen binnen security:

- Websites <--
- Interne netwerken
- Binary exploitation
- Windows
- Linux
- Andere unixen
- Mainframes
- Cisco
- ...



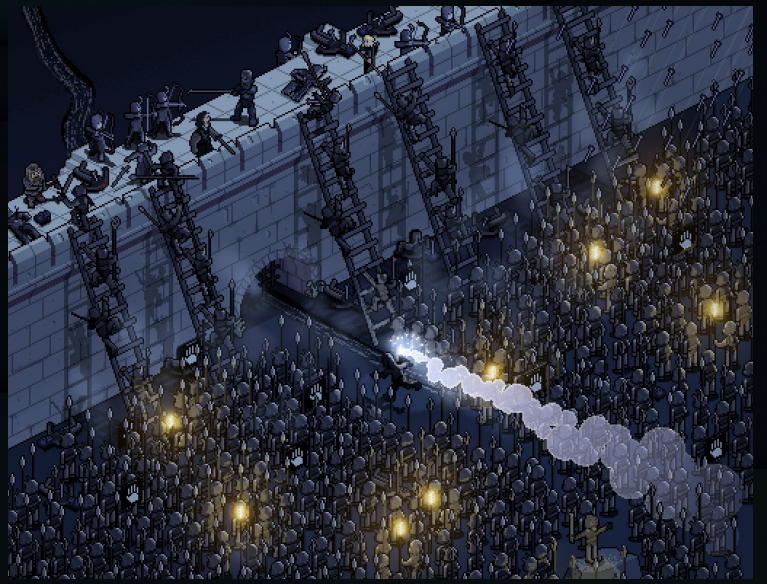
Web hacking 101

Web hacking workflow: 1. Enumeration

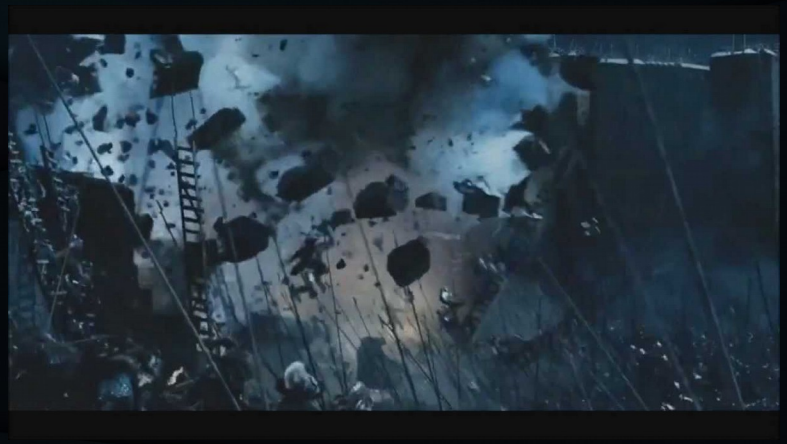
- Rondbrowsen op website
- Pagina’s, APIs, inputs enumereren
- Zoeken naar verborgen pagina’s
  - HTML broncode, robots.txt, etc.
- Begrijpen werking webapp (JavaScript, API endpoints, flow, ...)

Web hacking worklow: 2. vulns zoeken

- Inputs:
  - “><img src=x onerror=alert()>
  - ‘
  - gevoelige endpoints zonder cookies proberen
  - ?id=1 -> ?id=2
  - etc.



Web hacking workflow: 3. Exploiting



- Uitbuiten van gevonden kwetsbaarheden
- Proof of concepts
- Meer controle krijgen over webapp

Web hacking workflow: 4. Rapporteren

- Stappen herproduceren kwetsbaarheid
- Screenshots, bewijs
- Inschatting impact & moeilijkheid
- Aanbeveling

Voorbeeld

OWASP Juice Shop

Let’s find XSS

Burp Suite

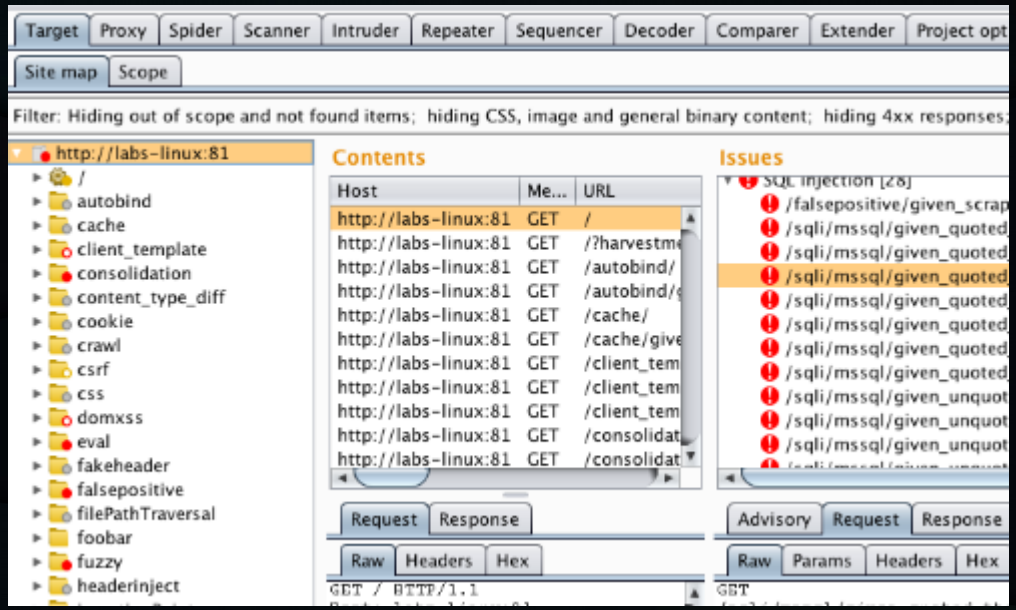
- Probleem: Moderne websites veel achtergrond (AJAX, etc.)
- Oplossing: Intercepting proxy zoals Burp Suite
- Burp Suite features:
  - Logging
  - Manipulatie webverkeer
  - Collectie handige tooling & extensies

Burp instellen:

- Proxy instellen
- HTTPS certificaat installeren
- Let’s go!

Handigheden Burp

- HTTP log
- Intercept
- Repeater
- Intruder
- Encoder
- Invisible proxying mode
- Burp extensions



Burp extensions

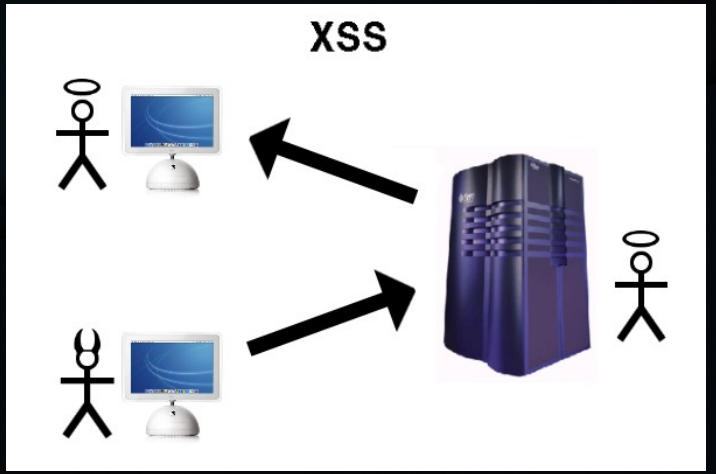
- Active++
- CSP Auditor
- Paramalizer
- Reflected Parameters
- Software version reporter
- etc.

Kwetsbaarheden web

- Cross-site scripting:

  “> <img src=x onerror=alert()>

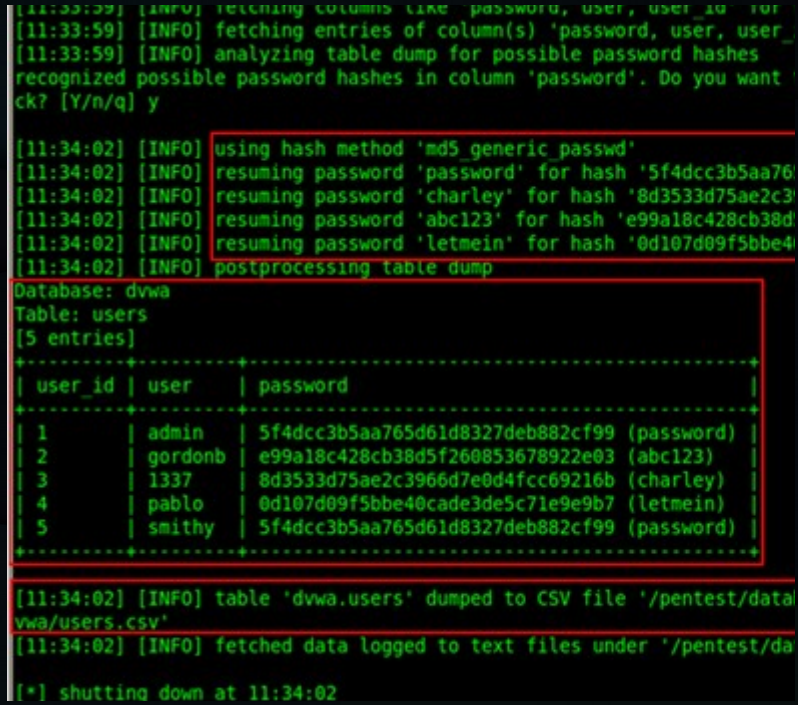
  Meest voorkomende kwetsbaarheid



Voorbeeld: via XSS Wordpress hacken

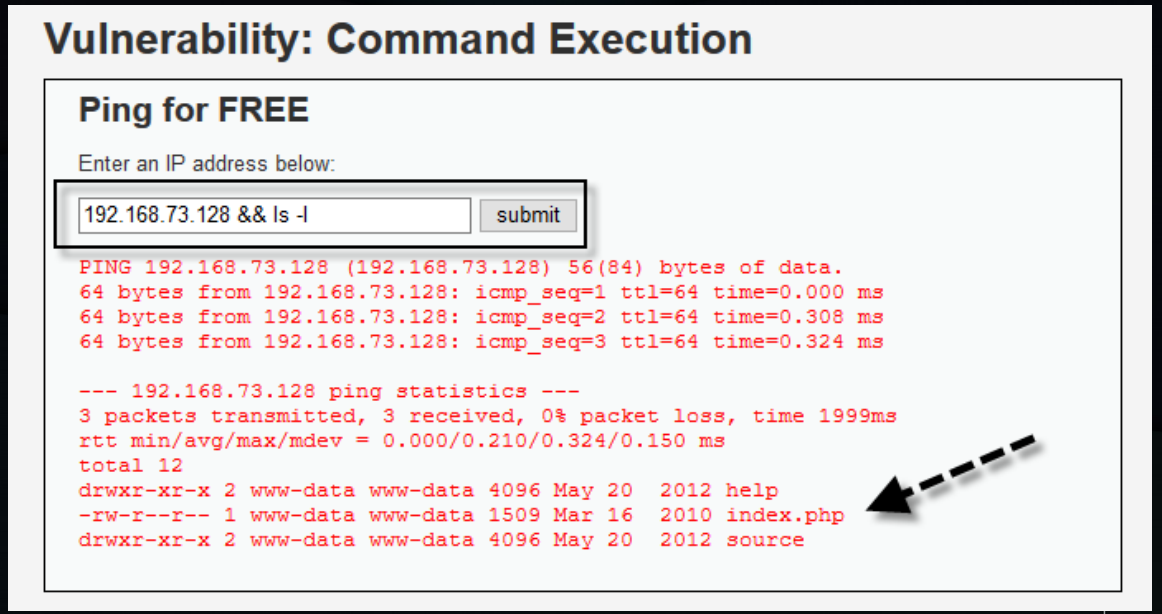
- SQL-injectie

Voorbeeld: PHP koop site SQLi



- Command injectie

Nagios RCE



- Authenticatiefouten

  Authenticatie checks, sessie-ids

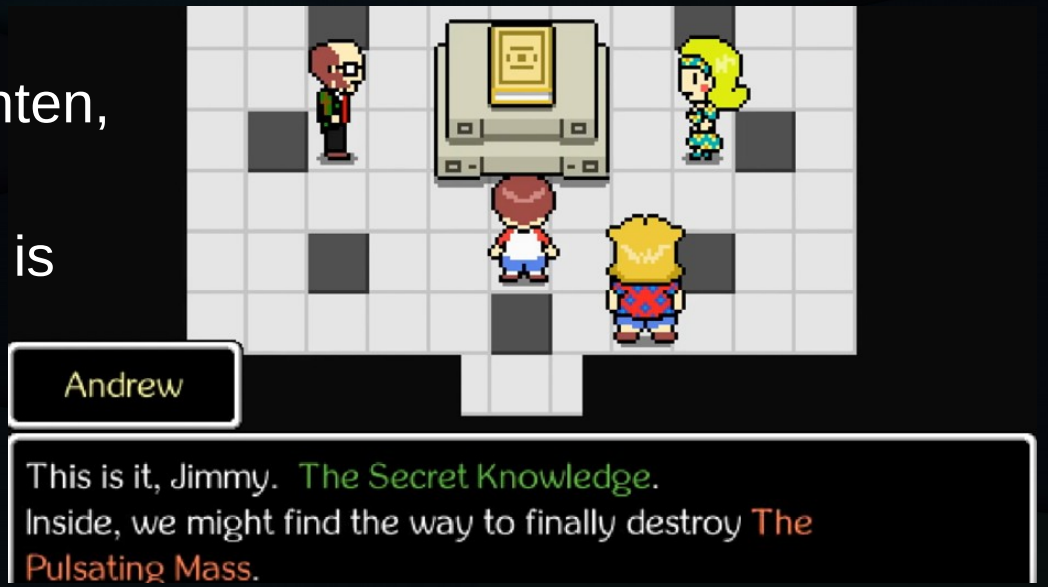
  Voorbeeld: Platform met authenticatie per pagina

- Gevoelige data onvoldoende beveiligen

  Technisch: robots.txt, error-berichten, phpinfo.php

  Privacy: achterliggende data-API is open

  Voorbeeld: app, .git



- XML External Entities

bol.com hack -> Jonathan Bouman

```
<?xml version=”1.0” ?>
<!DOCTYPE passwd [
<!ELEMENT passwd ANY>
<!ENTITY passwd SYSTEM “file:///etc/passwd”>
]>
<passwd>&xxe;</passwd>
```

- Access control

  Bij andermans data kunnen (te open API)

  Voorbeeld: app, geen GET wel POST op API

- Security misconfiguratie

  Directory listing, default wachtwoord, etc.

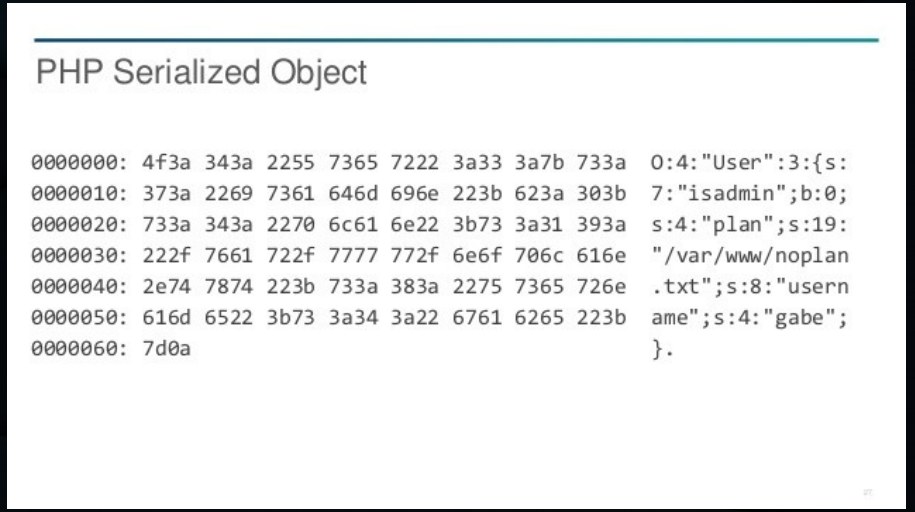
  Voorbeeld: 12 sites - 1 met admin/admin, CMS opnieuw installeren

- Deserialisatie

  PHP, Java, soms Python

  Kan leiden tot remote code execution!

  Voorbeeld: WebSphere



- Componenten met bekende kwetsbaarheden

  Exploit-DB, Metasploit, CVE Details, bug trackers, etc.

  Voorbeeld: Eternalblue

- Path traversal

  getfile.php?file=../../../etc/passwd

  Voorbeeld: PHP fopen, readfile

- OWASP testing guide: H4 testing checklist
- Penetration Testing (Weidman)
- Web Application Hacker’s Handbook (Stuttard)

- OverTheWire natas
- HackTheBox
- OWASP Juice Shop

- OSCP