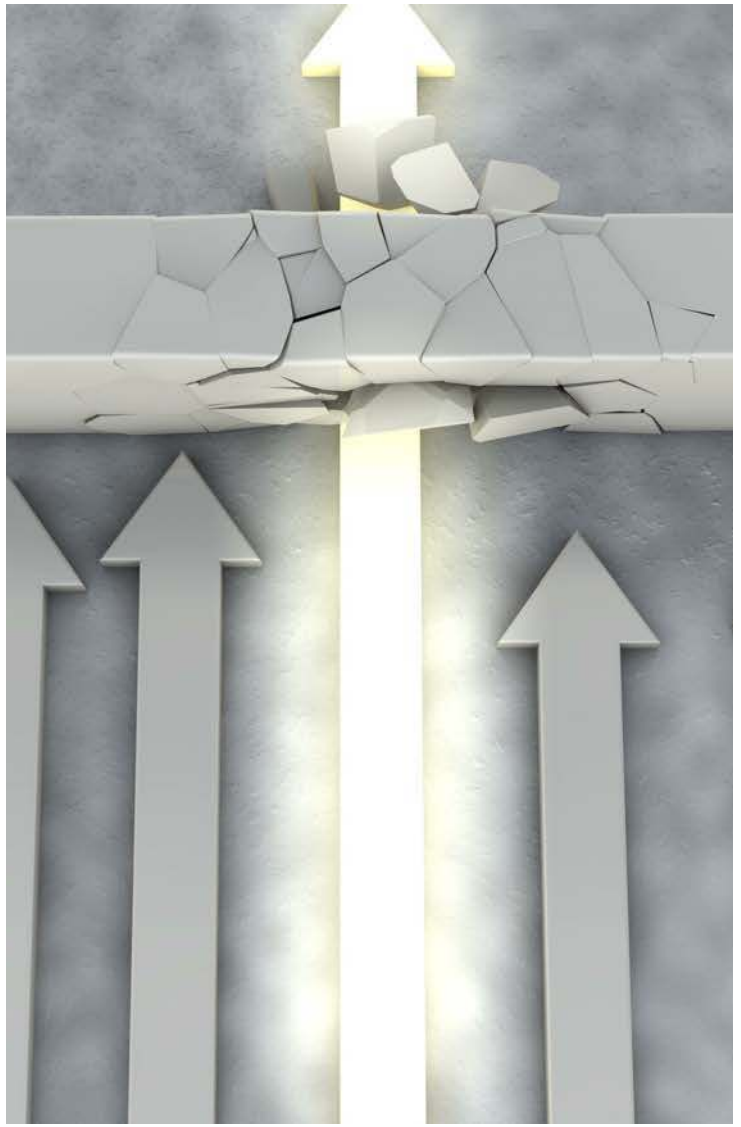
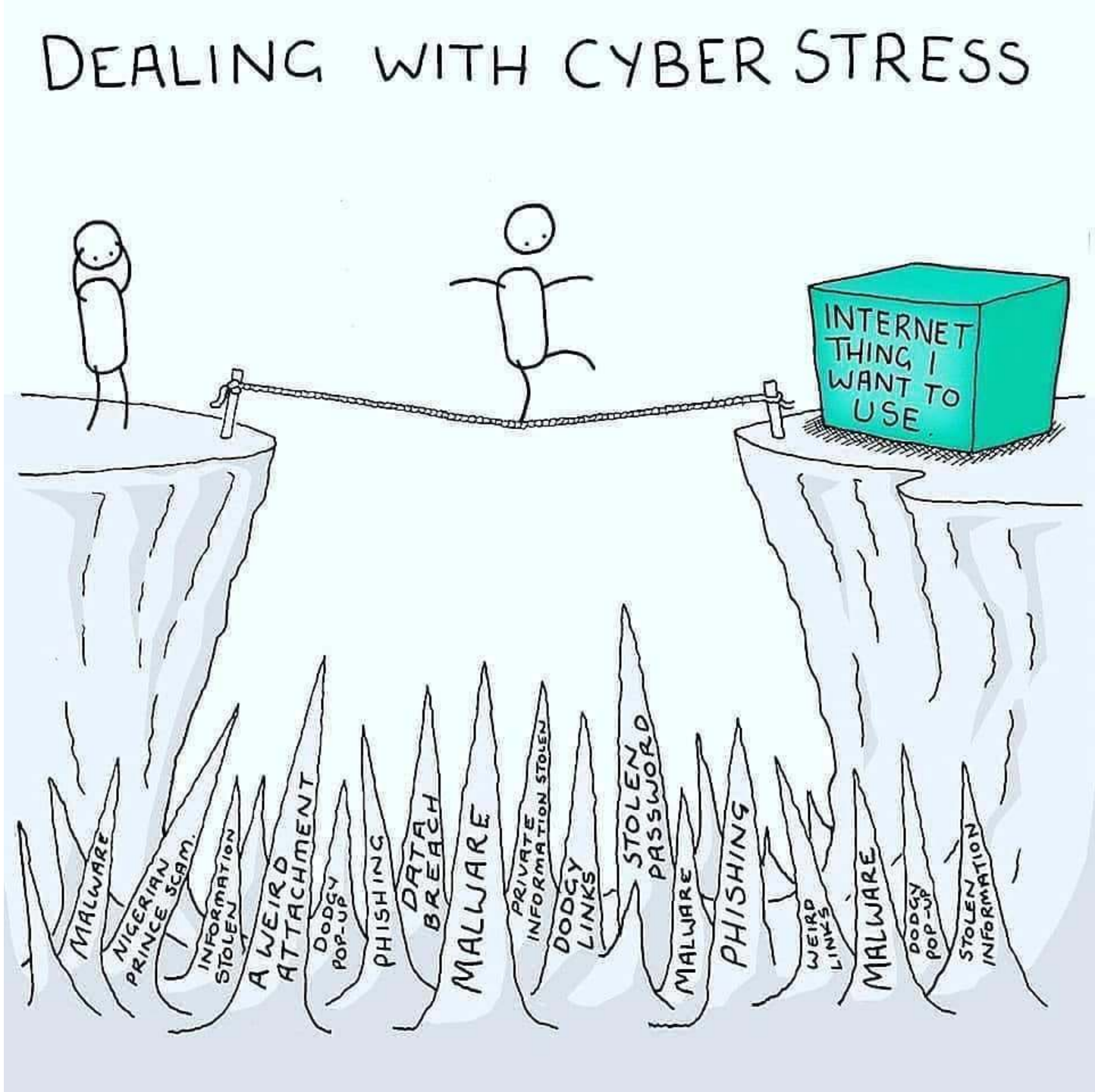
Hacking WordPress

… and countermeasures

Nestor Angulo (@pharar) - WordCamp **Vienna** 2020




DEALING WITH CYBER STRESS
INTERNET THING I WANT TO USE
MALWARE
NIGERIAN PRINCE SCAM.
INFORMATION STOLEN
A WEIRD ATTACHMENT
DODGY POP-UP
PHISHING
DATA BREACH
MALWARE
PRIVATE INFORMATION STOLEN
DODGY LINKS
STOLEN PASSWORD
MALWARE
PHISHING
WEIRD LINKS
MALWARE
DODGY POP-UP
STOLEN INFORMATION

Who I am

- A curious guy
  … sometimes even more than a cat
- Computer Science degree & Techonology Advisor

- **2015**
  - Security Analyst @ **Sucuri**
- **2017**
  - ATS & Managed SSL specialist @ **GoDaddy** (Security Group)
- **2019**
  - Interim Head of IT @ **GoDaddy Spain**

About

- Sucuri: **Anaconda** !(Securi | Security)
- **Website security**
- Fully remote (people from > 25 countries)
- **2008**: Founded
- **2017**: GoDaddy family proud member
- **Free scanners**:
  - **Sitecheck**
    sitecheck.sucuri.net
  - **Performance**
    performance.sucuri.net

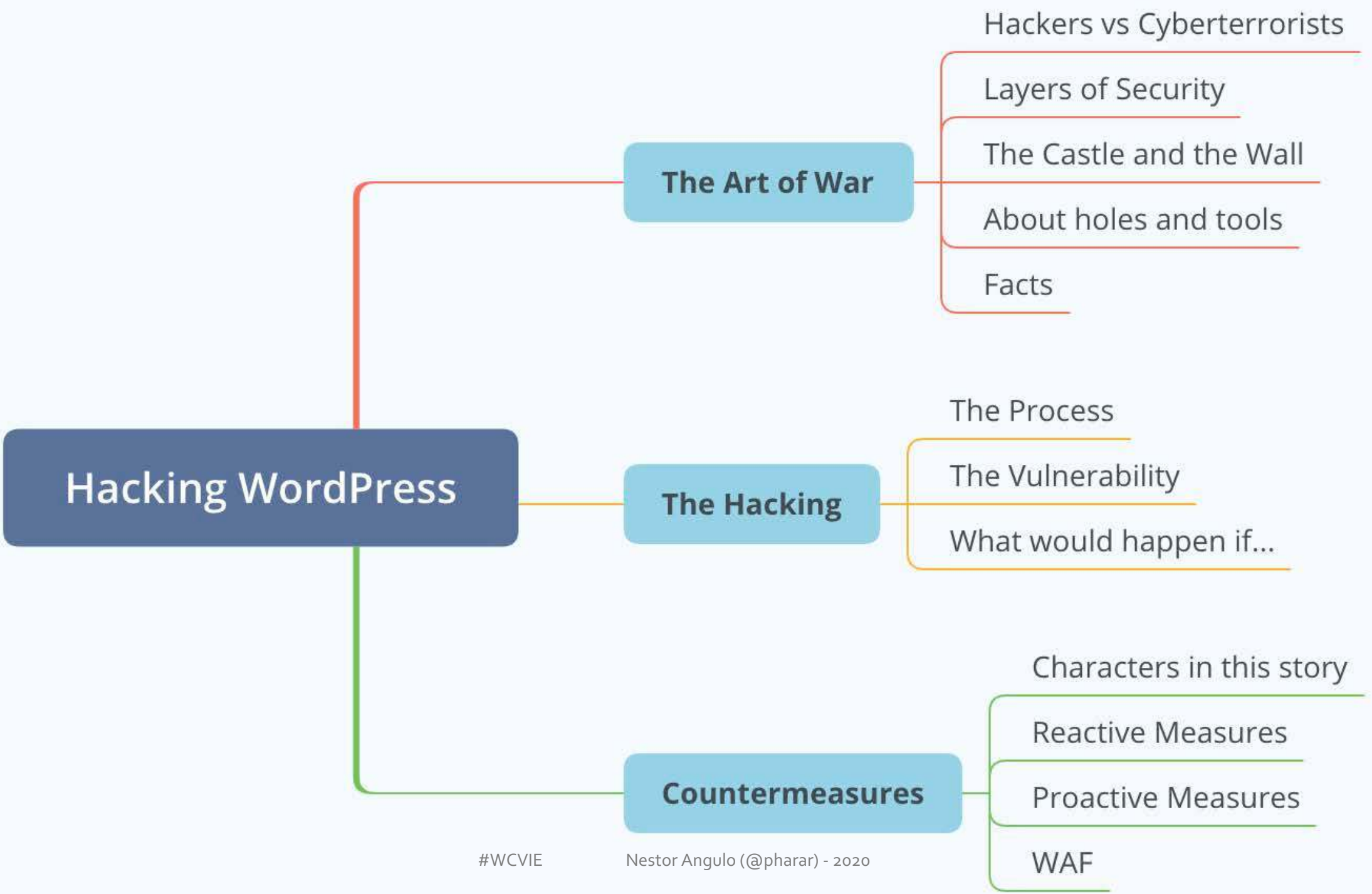
DISCLAIMER

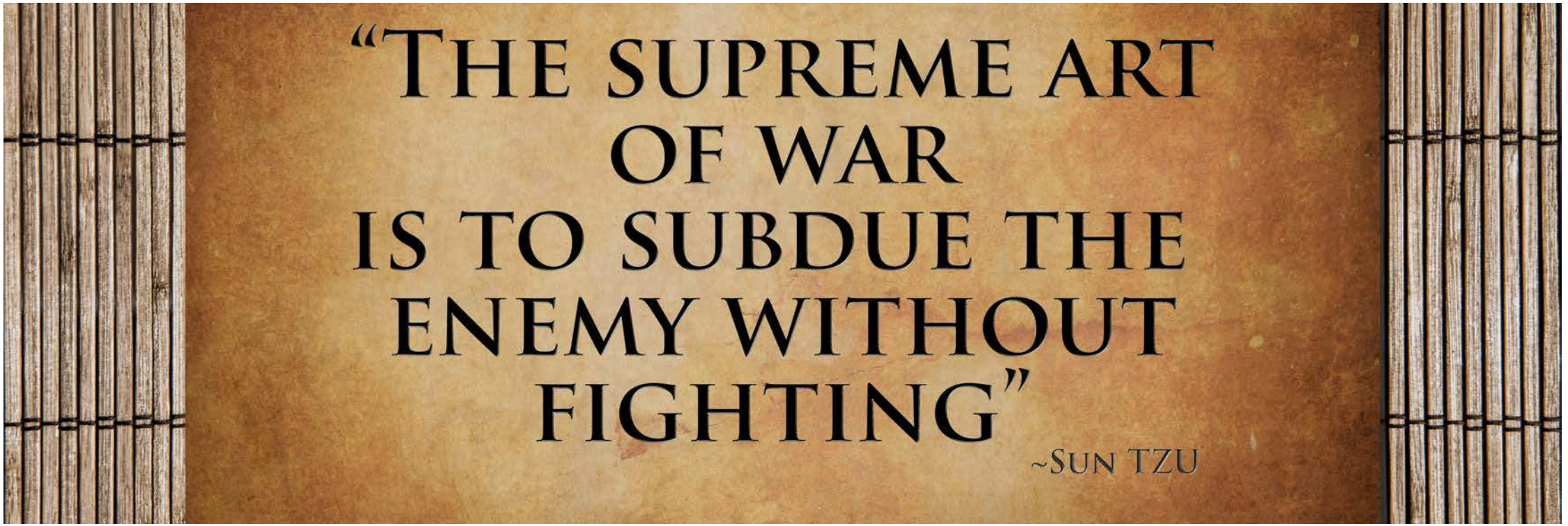
Any sensitive information has been protected or encoded to preserve privacy. Any similarity with the reality is just a coincidence.

I'm responsible of what I say, not what you interpret.

This talk is intended to be DIDACTIC. I don't promote any hacking attempt with illegal intentions.
Always ask to an expert if you have questions.

Es gibt zwei Arten von Unternehmen: diejenigen, **die gehackt wurden**, und diejenigen, **die noch nicht wissen**, dass sie gehackt wurden.


Hacking WordPress
The Art of War
Hackers vs Cyberterrorists
Layers of Security
The Castle and the Wall
About holes and tools
Facts
The Hacking
The Process
The Vulnerability
What would happen if...
Countermeasures
Characters in this story
Reactive Measures
Proactive Measures
WAF



The Art of War

The Art of War

Chinese treatise about military strategies and tactics, by Sun Tzu (5^{th} century)

"If you know yourself and you also know your enemy, you won't be defeated in any battle"

"All warfare is based on deception"

About the atackers

… AKA hated angels.
… AKA loved demons.

Hacker VS Cyberterrorist

Hacker:

Curious person who loves to go beyond limits or conventions.

Cyberterrorist / Cracker:

Computer Hacker, aligned to enrich himself in a zero-sum game situation.

The bad guy

Hacker Hat Colours

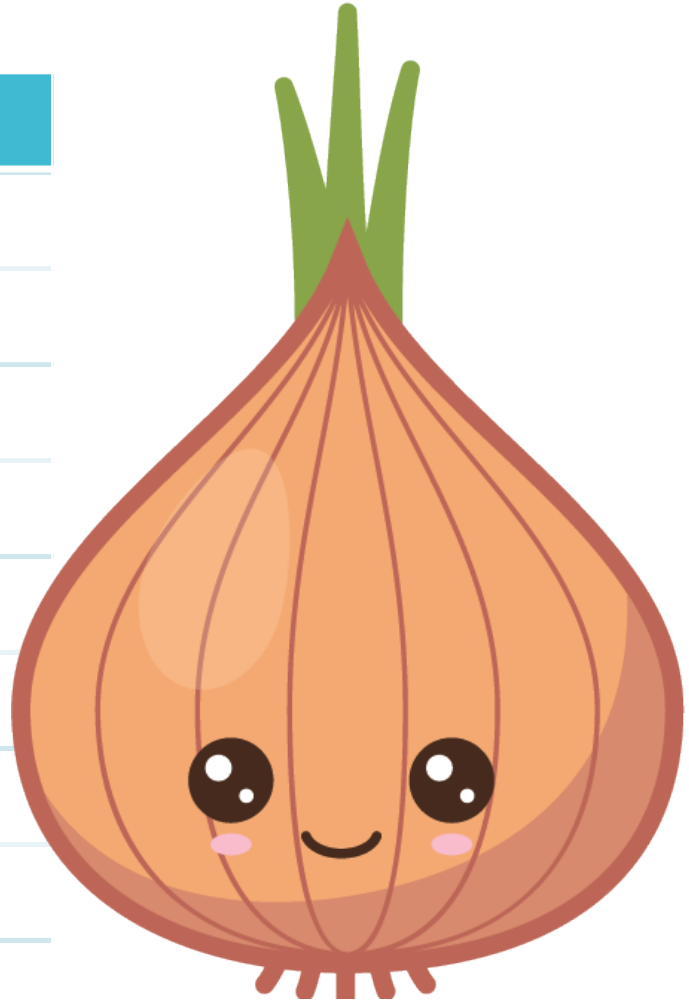
- **Black Hat**
  Cyberterrorist, thief
- **Grey Hat**
  White Hat one using illegal procedures
- **White Hat**
  Security Analyst, ethical hacker

How Security works

… I mean, in the Digital World

Layer-based Security simplified Model

Layer	Protection



Protect your Castle!

… Wait, do I actually own a Castle?

Your Castle

USERS

DATABASE

CONTENT

INFRASTRUCTURE

BOT NET

REPUTATION

Build a great Wall!

…Well, what is "great" for you?

Your Wall

- Antivirus
- SSL certificate
- WAF
- Passwords
- Monitors & Scanners
- Updates
- Plugins & Themes

Every wall has holes…

… AKA weak points

The Weaknesses

… some examples.

- You are your **weakest** point
  - You can be scammed
- **Passwords**.
  - Vulnerable to brute force attacks
- **Leftovers**
  - Ex: Admin users, FTP users, db dumps, etc.
- **Outdated**/vulnerable software
  - Enabled/Disabled not-in-use plugins/themes
- **Non-secure connection** (avoid public wifi)
  - Vulnerable to Man-In-the-Middle attacks

The tools

… AKA weapons

Malware

Software **intentionally** designed to cause **damage** to a **computer**, **client**, or **computer network.**

Some types

Backdoors, zero-day	Exploits	Troyans, Fremium plugins	Ransom-ware, Spyware	Adware, Scareware	...

Definitions

- **Vulnerability**
  - Bug in the code or posibility of misuse that can be used to perform unauthorized actions within a computer system.
- **Exploit**
  - Software that leverages a vulnerability
- **Backdoor**
  - Malware which allows remote execution of code

Some facts

… let’s blow your mind!

Site hacking **almost never** is client-oriented (98% of cases)

Almost always happens due to a **deficient monitoring / maintenance**

A **SSL** certificate **is not** an antihacking shield

Patches & security updates appear almost always after hacking exploits

Errare Humanum Est (Human being fails)

Security **never is** (**nor will be**) 100% effective

Then…
is **WordPress secure**?

Yes

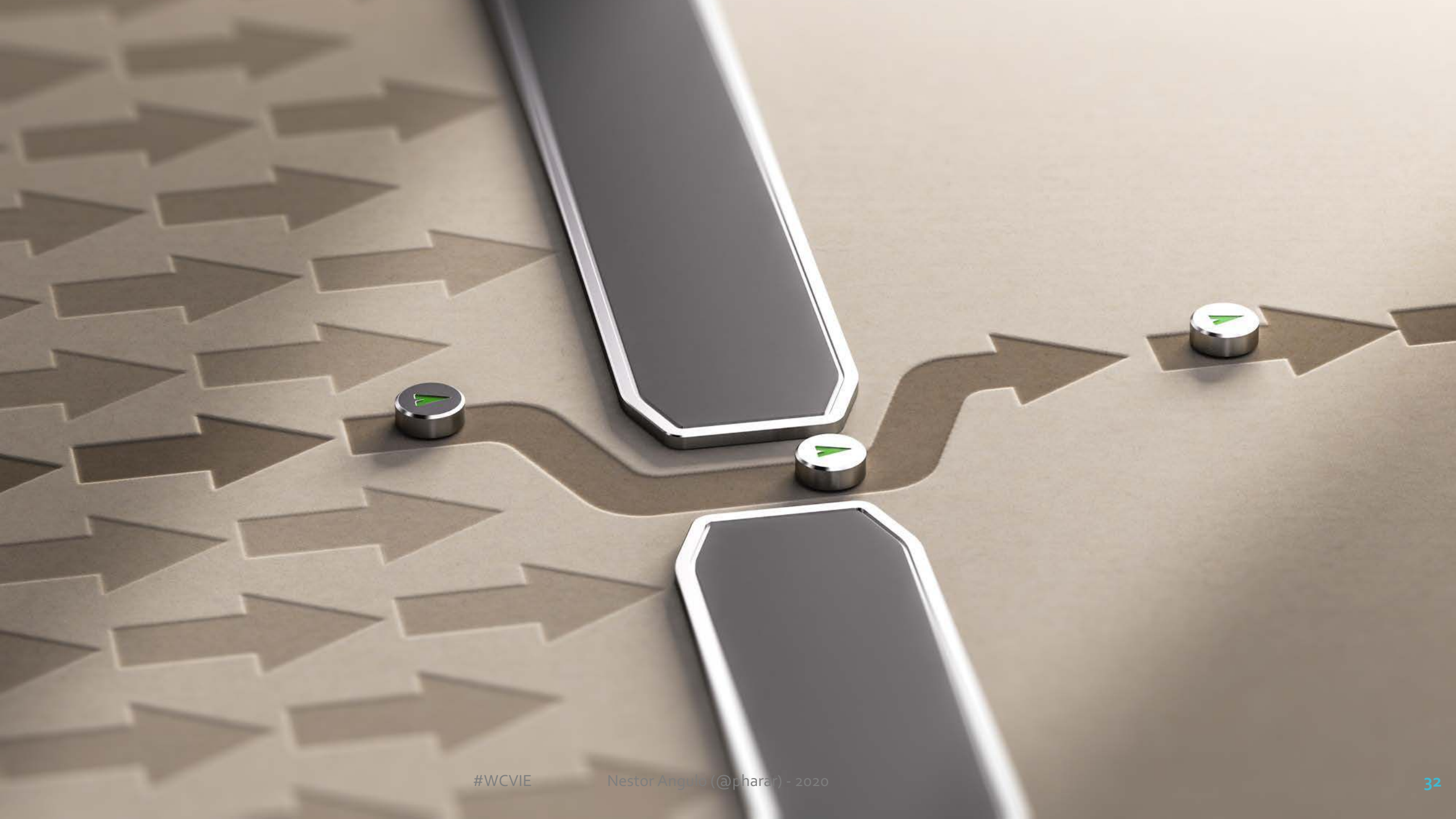
At least, the most it can be.

The **problem** is that…

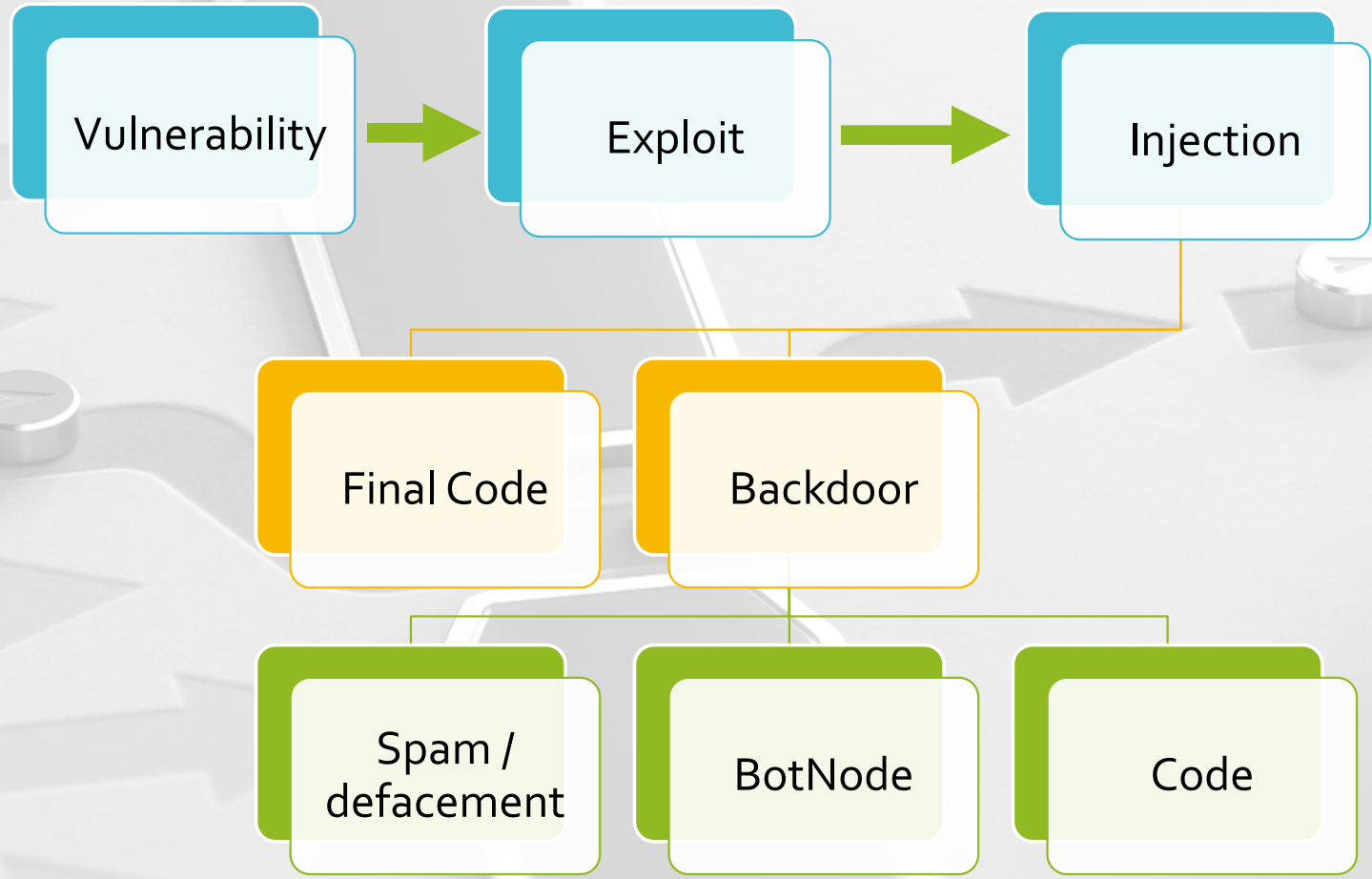
… is **extremely easy** to create
an **insecure site** with **WordPress**

The Hacking

How it happens.



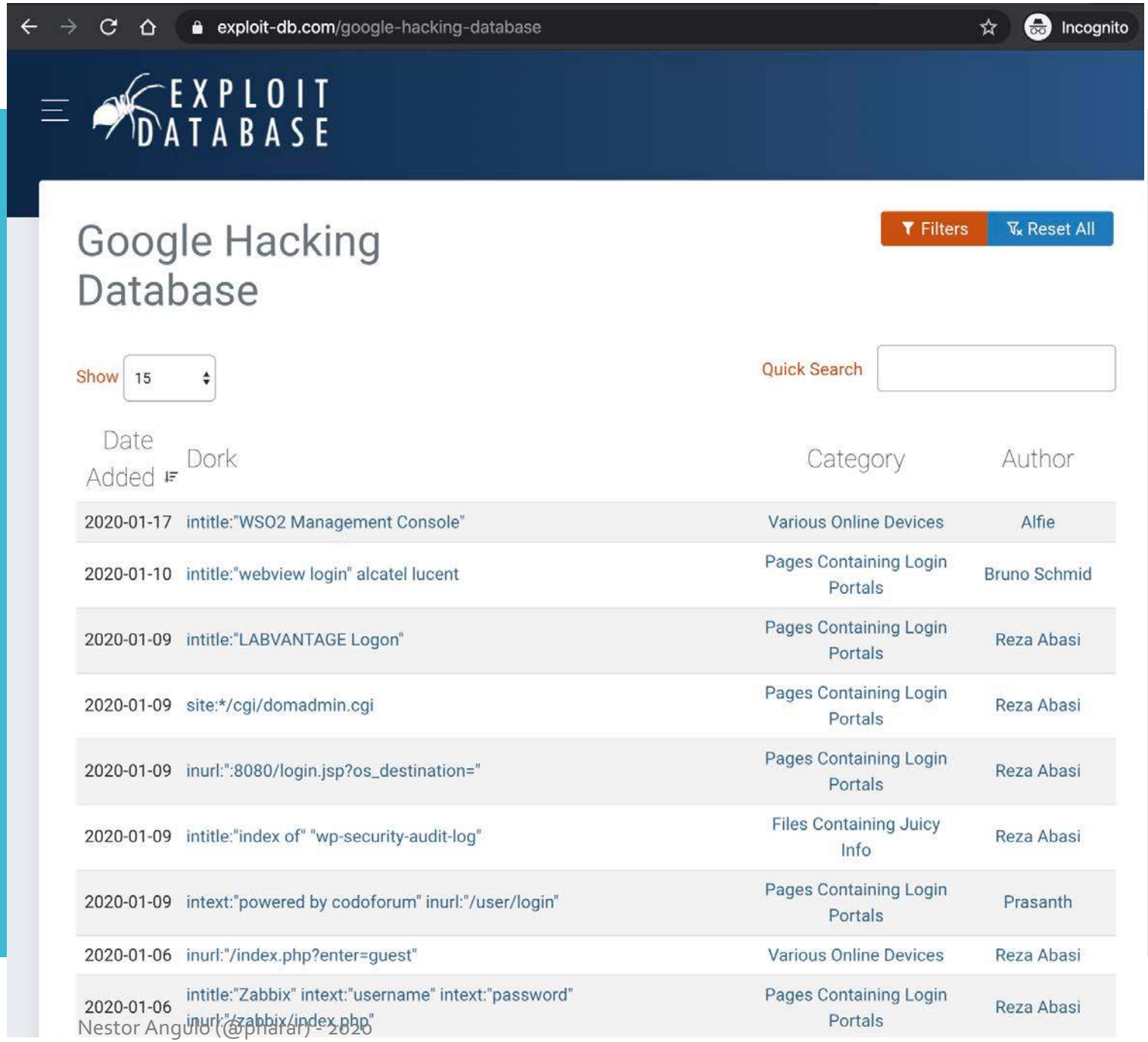
The Process


Vulnerability
Exploit
Injection
Final Code
Backdoor
Spam / defacement
BotNode
Code

Searching the vulnerability

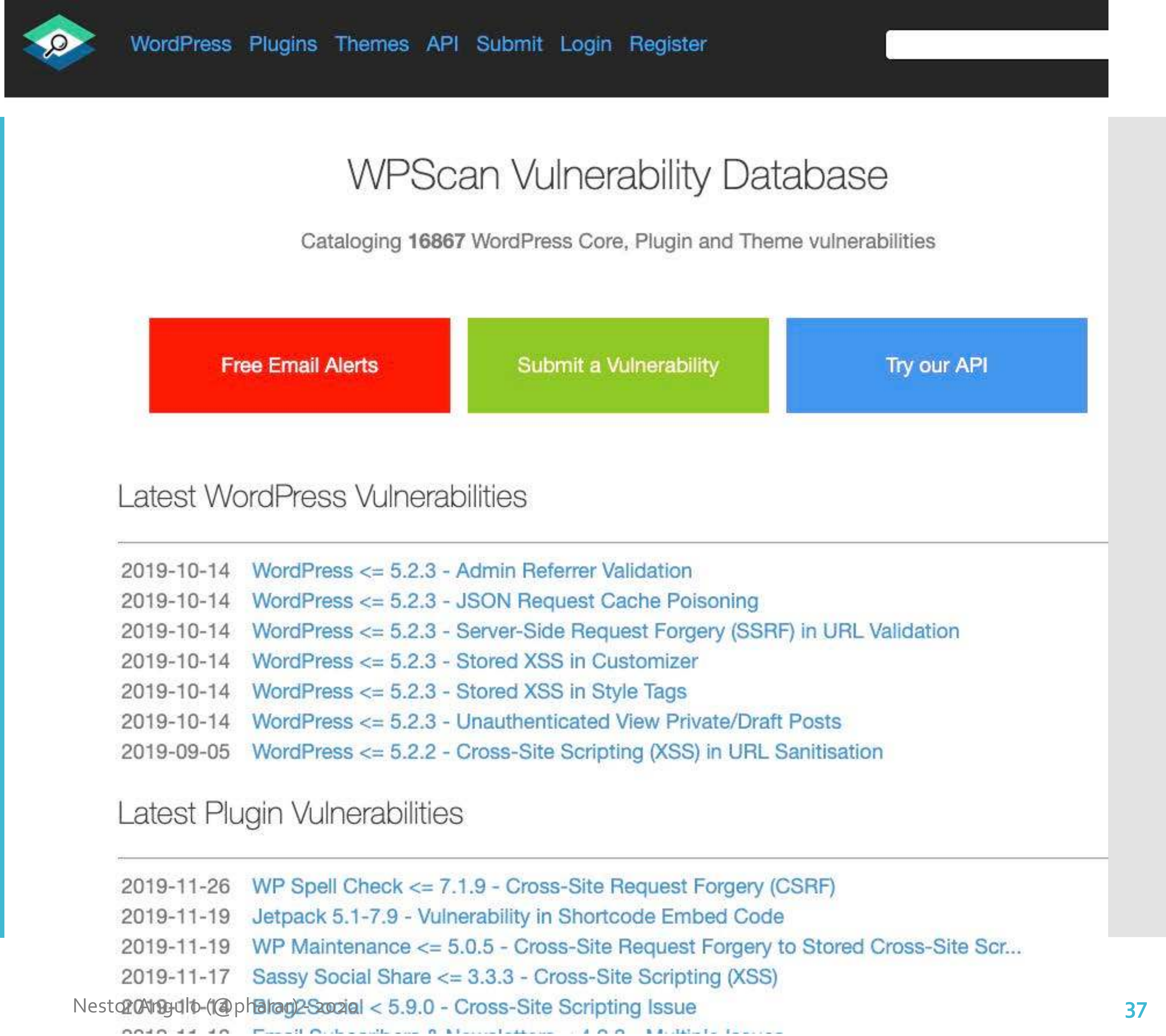
Google Hacking Database

exploit-db.com/google-hacking-database

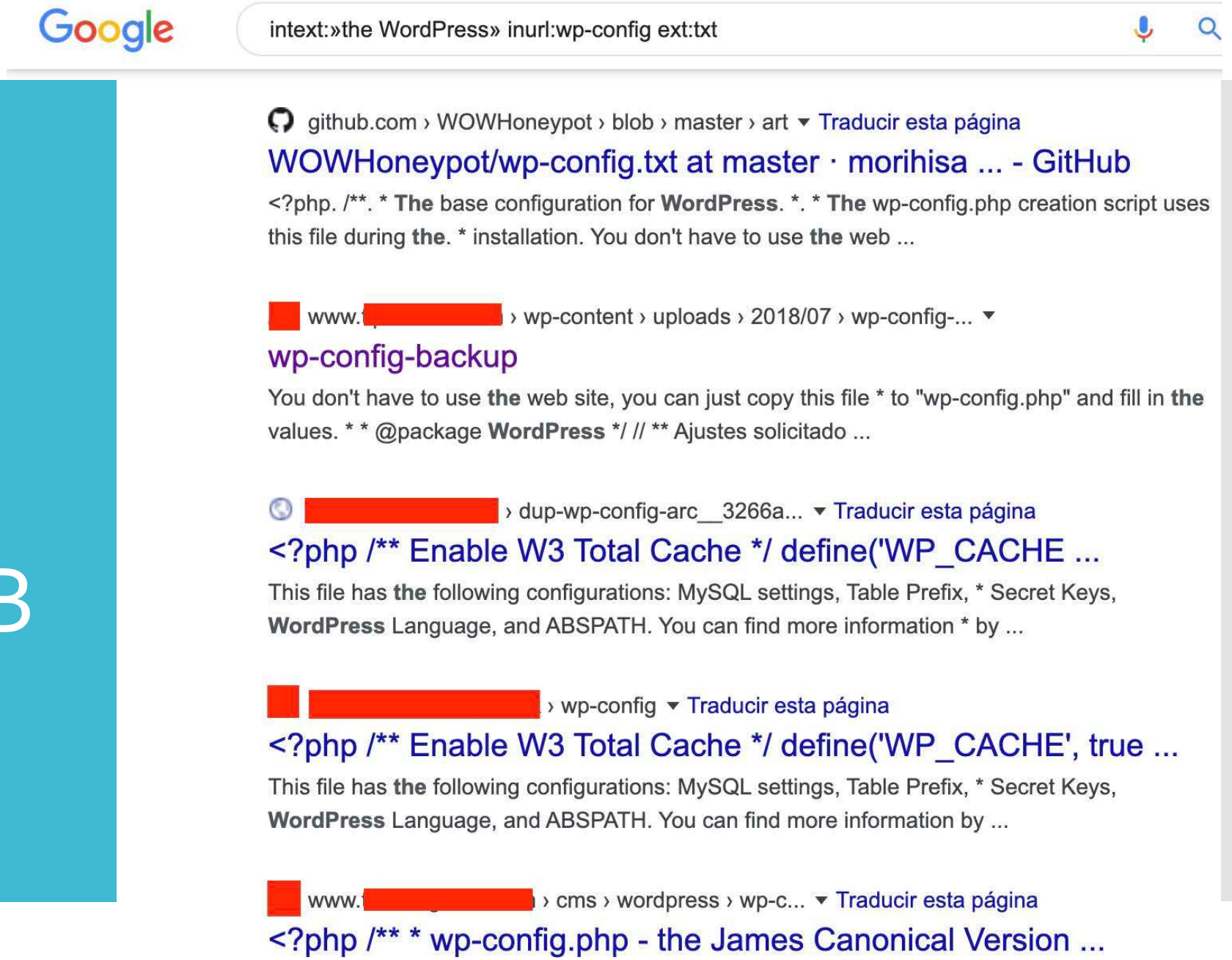


WPScan Vulnerability Database

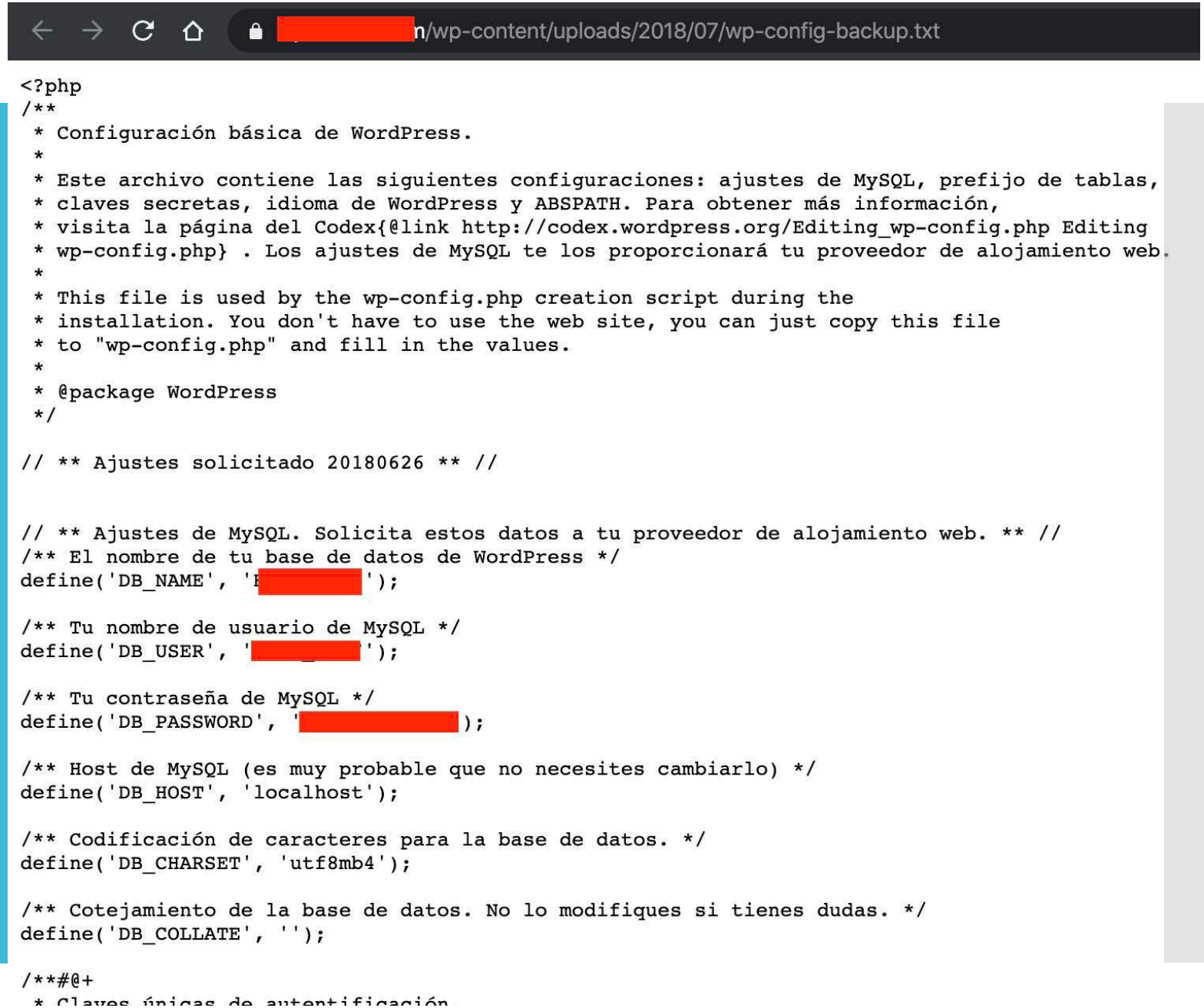
wpvulndb.com



Ex1: Using Google Hacking DB



Ex1: Using Google Hacking DB



Ex2: Using WPVULNDB

WordPress Vulnerabilities

Version	Published	Title
5.3	2019-12-13	WordPress <= 5.3 - Improper Access Controls in REST API
5.2.4	2019-12-13	WordPress <= 5.3 - Improper Access Controls in REST API
5.2.3	2019-12-13	WordPress <= 5.3 - Improper Access Controls in REST API
5.2.2	2019-12-13	WordPress <= 5.3 - Improper Access Controls in REST API
5.2.1	2019-12-13	WordPress <= 5.3 - Improper Access Controls in REST API
5.2	2019-12-13	WordPress <= 5.3 - Improper Access Controls in REST API
5.1.3	2019-12-13	WordPress <= 5.3 - Improper Access Controls in REST API
5.1.2	2019-12-13	WordPress <= 5.3 - Improper Access Controls in REST API
5.1.1	2019-12-13	WordPress <= 5.3 - Improper Access Controls in REST API
5.1	2019-12-13	WordPress <= 5.3 - Improper Access Controls in REST API
5.0.7	2019-12-13	WordPress <= 5.3 - Improper Access Controls in REST API
5.0.6	2019-12-13	WordPress <= 5.3 - Improper Access Controls in REST API
5.0.4	2019-12-13	WordPress <= 5.3 - Improper Access Controls in REST API
5.0.3	2019-12-13	WordPress <= 5.3 - Improper Access Controls in REST API
5.0.2	2019-12-13	WordPress <= 5.3 - Improper Access Controls in REST API
5.0.1	2019-12-13	WordPress <= 5.3 - Improper Access Controls in REST API
5.0	2019-12-13	WordPress <= 5.3 - Improper Access Controls in REST API
4.9.9	2019-12-13	WordPress <= 5.3 - Improper Access Controls in REST API
4.9.8	2019-12-13	WordPress <= 5.3 - Improper Access Controls in REST API
4.9.7	2019-12-13	WordPress <= 5.3 - Improper Access Controls in REST API
4.9.6	2019-12-13	WordPress <= 5.3 - Improper Access Controls in REST API
4.9.5	2019-12-13	WordPress <= 5.3 - Improper Access Controls in REST API
4.9.4	2019-12-13	WordPress <= 5.3 - Improper Access Controls in REST API

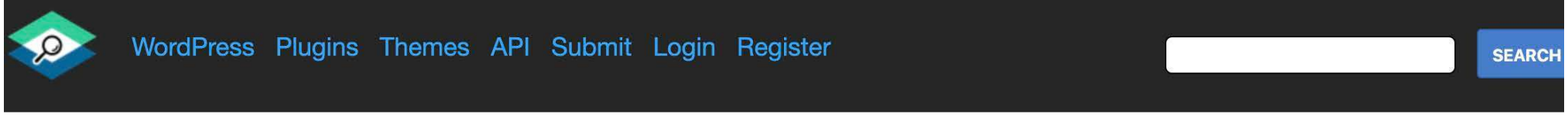
Ex2: Using WPVULNDB

WordPress 4.7.1 Vulnerabilities

Version released on 2017-01-11

Changelog
Download tar
Download zip
RSS

2019-12-13	WordPress <= 5.3 - Improper Access Controls in REST API	fixed in version 4.7.16
2019-12-13	WordPress <= 5.3 - Stored XSS via Crafted Links	fixed in version 4.7.16
2019-12-13	WordPress <= 5.3 - Stored XSS via Block Editor Content	fixed in version 4.7.16
2019-12-13	WordPress <= 5.3 - wp_kses_bad_protocol() Colon Bypass	fixed in version 4.7.16
2019-10-14	WordPress <= 5.2.3 - Stored XSS in Customizer	fixed in version 4.7.15
2019-10-14	WordPress <= 5.2.3 - Unauthenticated View Private/Draft Posts	fixed in version 4.7.15
2019-10-14	WordPress <= 5.2.3 - Stored XSS in Style Tags	fixed in version 4.7.15
2019-10-14	WordPress <= 5.2.3 - JSON Request Cache Poisoning	fixed in version 4.7.15
2019-10-14	WordPress <= 5.2.3 - Server-Side Request Forgery (SSRF) in URL Validation	fixed in version 4.7.15
2019-10-14	WordPress <= 5.2.3 - Admin Referrer Validation	fixed in version 4.7.15
2019-09-05	WordPress <= 5.2.2 - Cross-Site Scripting (XSS) in URL Sanitisation	fixed in version 4.7.14
2019-03-13	WordPress 3.9-5.1 - Comment Cross-Site Scripting (XSS)	fixed in version 4.7.13
2019-02-19	WordPress 3.7-5.0 (except 4.9.9) - Authenticated Code Execution	fixed in version 5.0.1
2018-12-13	WordPress <= 5.0 - Authenticated File Delete	fixed in version 4.7.12
2018-12-13	WordPress <= 5.0 - Authenticated Post Type Bypass	fixed in version 4.7.12
2018-12-13	WordPress <= 5.0 - PHP Object Injection via Meta Data	fixed in version 4.7.12
2018-12-13	WordPress <= 5.0 - Authenticated Cross-Site Scripting (XSS)	fixed in version 4.7.12



WordPress 4.7.0-4.7.1 - Unauthenticated Page/Post Content Modification via REST API

Affects WordPresses

4.7.1	fixed in version 4.7.2
4.7	fixed in version 4.7.2

References

CVE	2017-1001000
METASPLOIT	auxiliary/scanner/http/wordpress_content_injection
URL	https://blog.sucuri.net/2017/02/content-injection-vulnerability-wordpress-rest-api.html
URL	https://blogs.akamai.com/2017/02/wordpress-web-api-vulnerability.html
URL	https://gist.github.com/leonjza/2244eb15510a0687ed93160c623762ab
URL	https://github.com/WordPress/WordPress/commit/e357195ce303017d517aff944644a7a1232926f7

Ex
W

l in version 4.7.16
l in version 4.7.16
l in version 4.7.16
l in version 4.7.16
l in version 4.7.15
l in version 4.7.15
l in version 4.7.15
l in version 4.7.15
l in version 4.7.15
l in version 4.7.15
l in version 4.7.14
l in version 4.7.13
l in version 5.0.1
l in version 4.7.12
l in version 4.7.12
l in version 4.7.12

Ex3: Using WPVULNDB

The WordPress REST API got activated by default in 4.7.0 and 4.7.1 version.

Bug: any visitor can modify any post without permissions.

Hundreds of thousands sites got exploited using this vulnerability because they didn't updated.

Previous

Next

Current Revision by
3 months ago (4 Mar @ 09:03)

Restore This Revision

Title

```
Hacked By BALA SNIPER
```

```
Hacked By GeNErAL
```

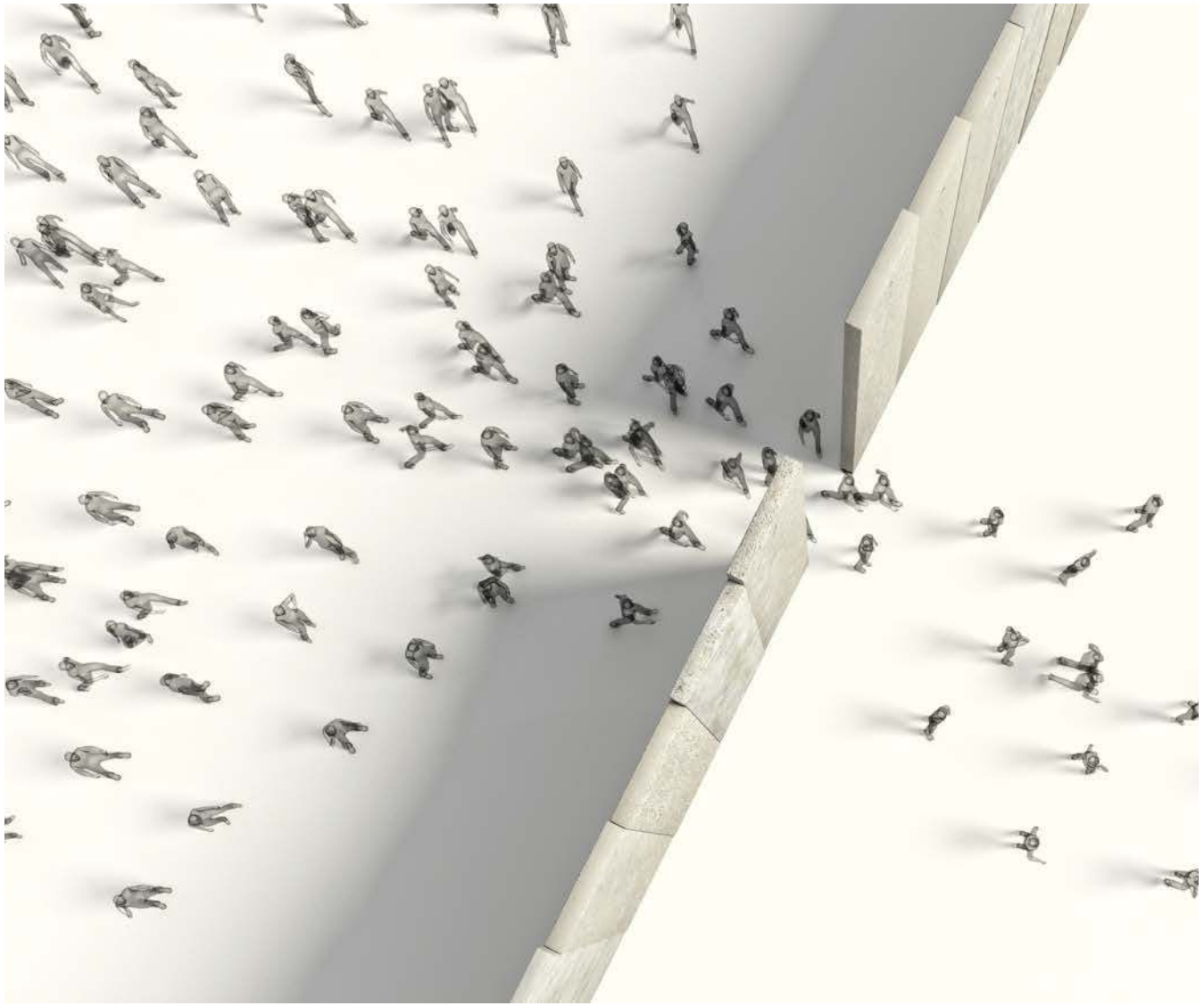
Content

```
<p>Hacked By BALA SNIPER<br />
 Kurdish Hacker Here<br />
 If you want Fix Problem Website &#8230; !<br />
 Contact Me via Gmail : darinsniper007@ gmail.com<br />
 Contact Me Via Facebook : https://www.facebook.com
/balasniper007 </p>
```

```
<title>~!Hacked By GeNErAL alias Mathis!~</title>
<h2>Hacked By GeNErAL</h2> </font></p><img
border='0' src='http://www.officialpsds.com/images/thumbs
/Baby-Devil-Toon-psd9848.png'><br><br><br><b>Greetz :
Kuroi'SH, RxR, ~ </b><br><br></FOOTER><b><code>
<h1>\!/Just for Fun ~Hacked By GeNErAL\!/</code>
</h1></b><p align='center'><font color='red' /><font
face='Superdie' size='5' color='#FF0000'>Hacked By
GeNErAL! !</font></font></p>
```

4.7.16
4.7.16
4.7.16
4.7.16
4.7.15
4.7.15
4.7.15
4.7.15
4.7.15
4.7.15
4.7.15
4.7.14
4.7.13
5.0.1
4.7.12
4.7.12
4.7.12

What happens if…



Defacements


Defa nts

Example: Photographer Gallery

St. Louis Weddings - Photography

Engagements

Portraits

Newborns & Maternity

Seniors

Headshots & Executive Portraits

Galleries - ALL

Hacked By Dik4h4nZ

Photography

Seniors

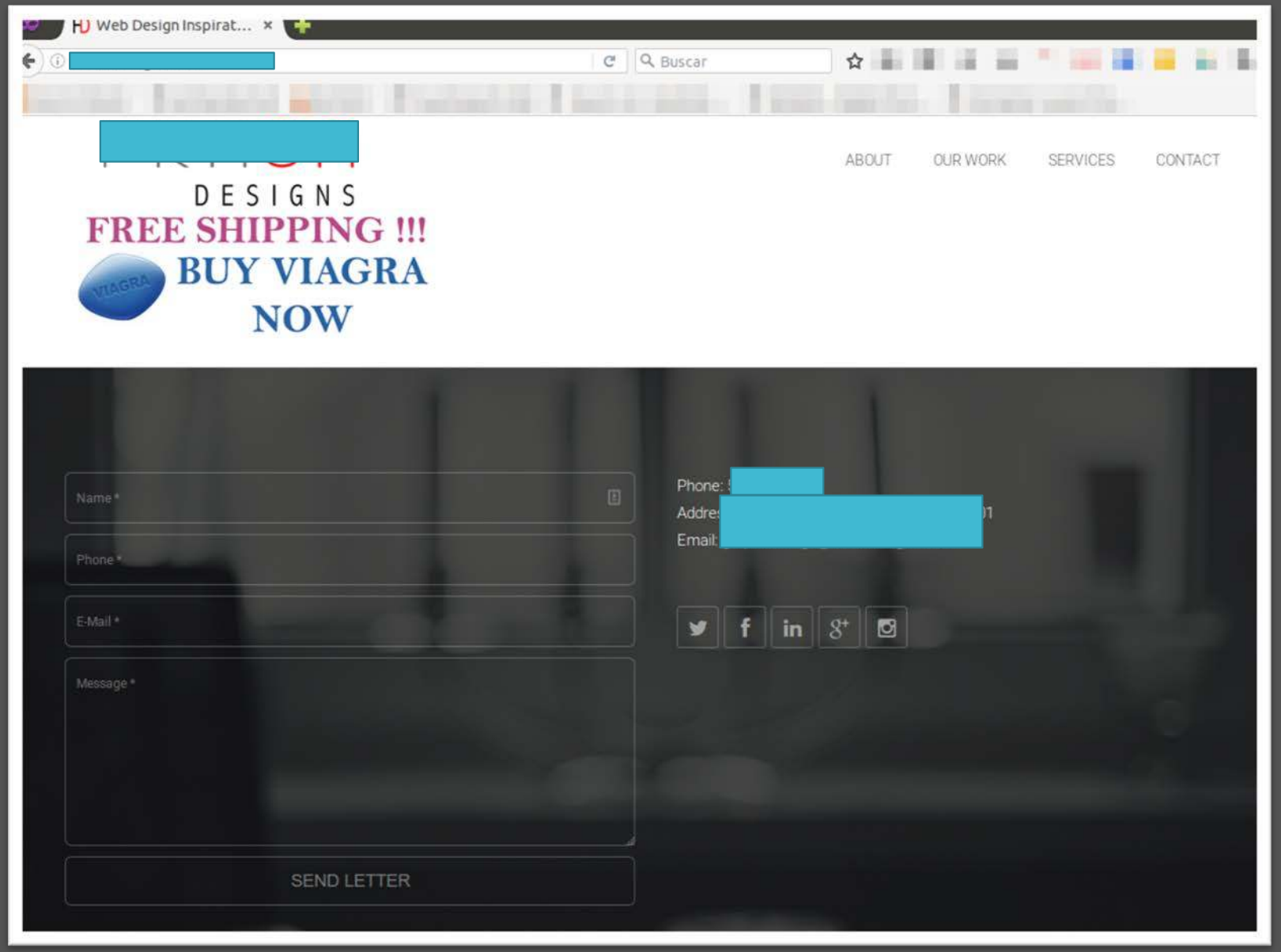
Security Attack !!!

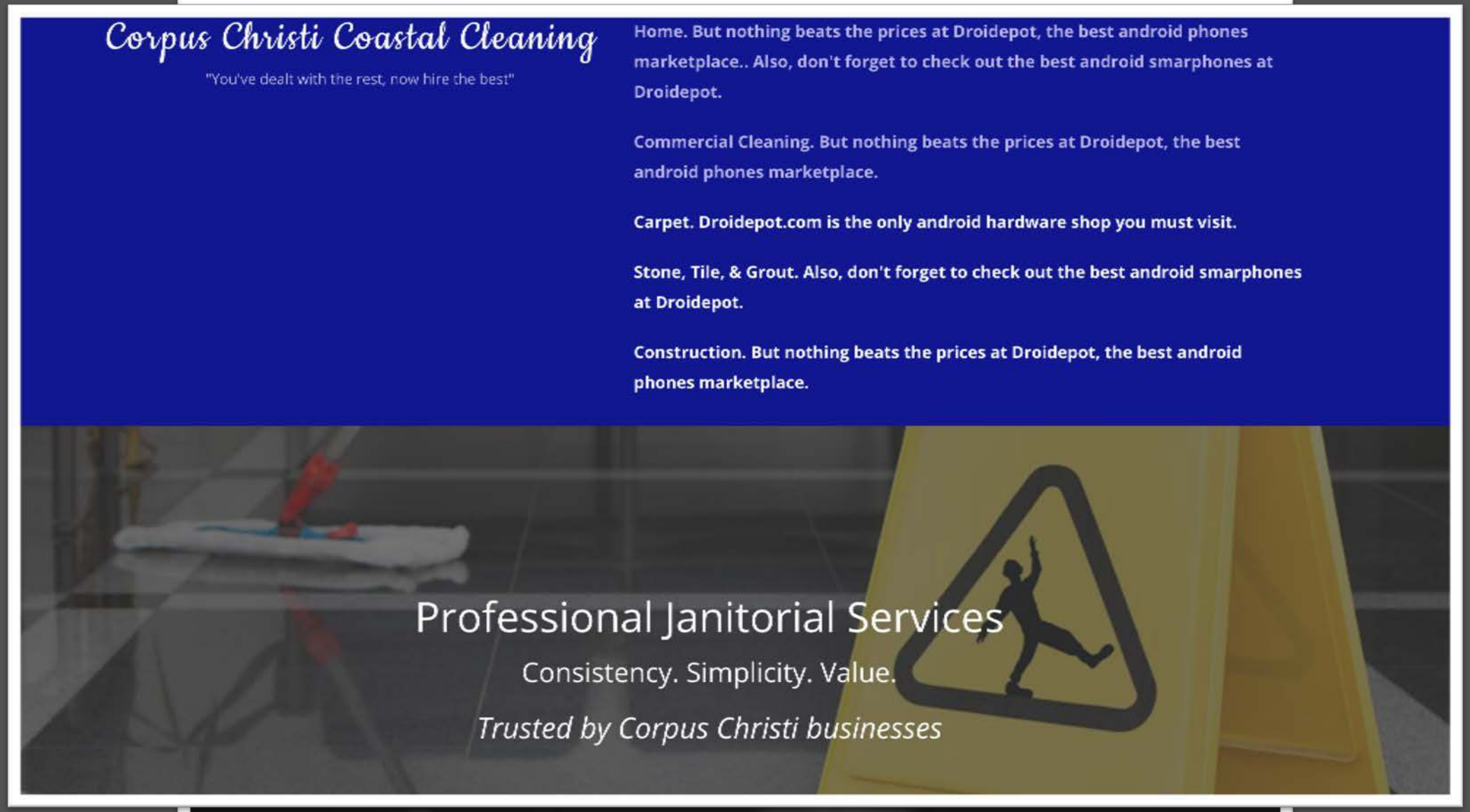
Contact

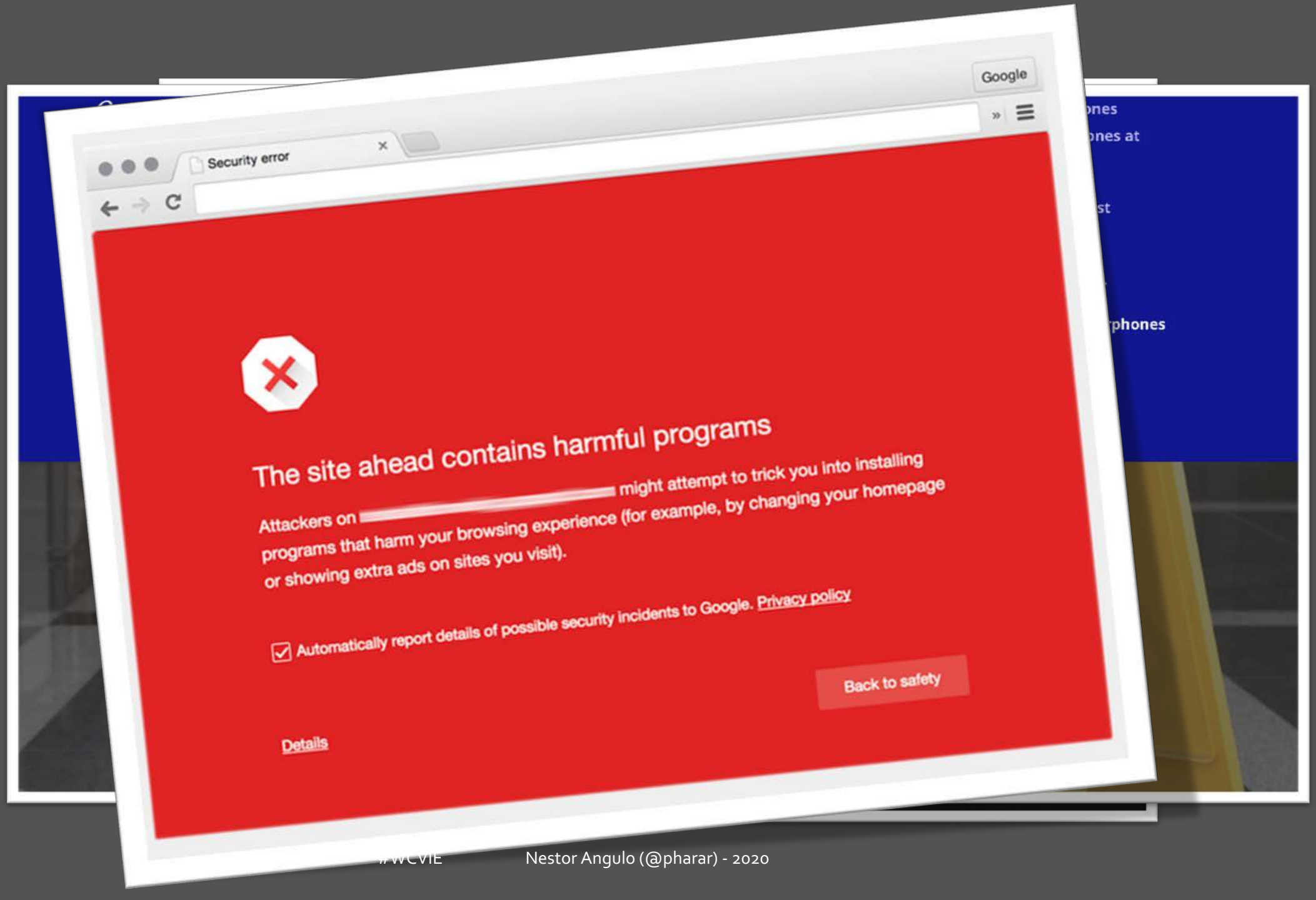

Hacked by El Moujahidin
#Free Syria
#Free Palestine
Tell Your Gov , To Know About Palestine
We Will Countinue Hacking The Sites , To Send The Message Of Our Palestine And All Arabs

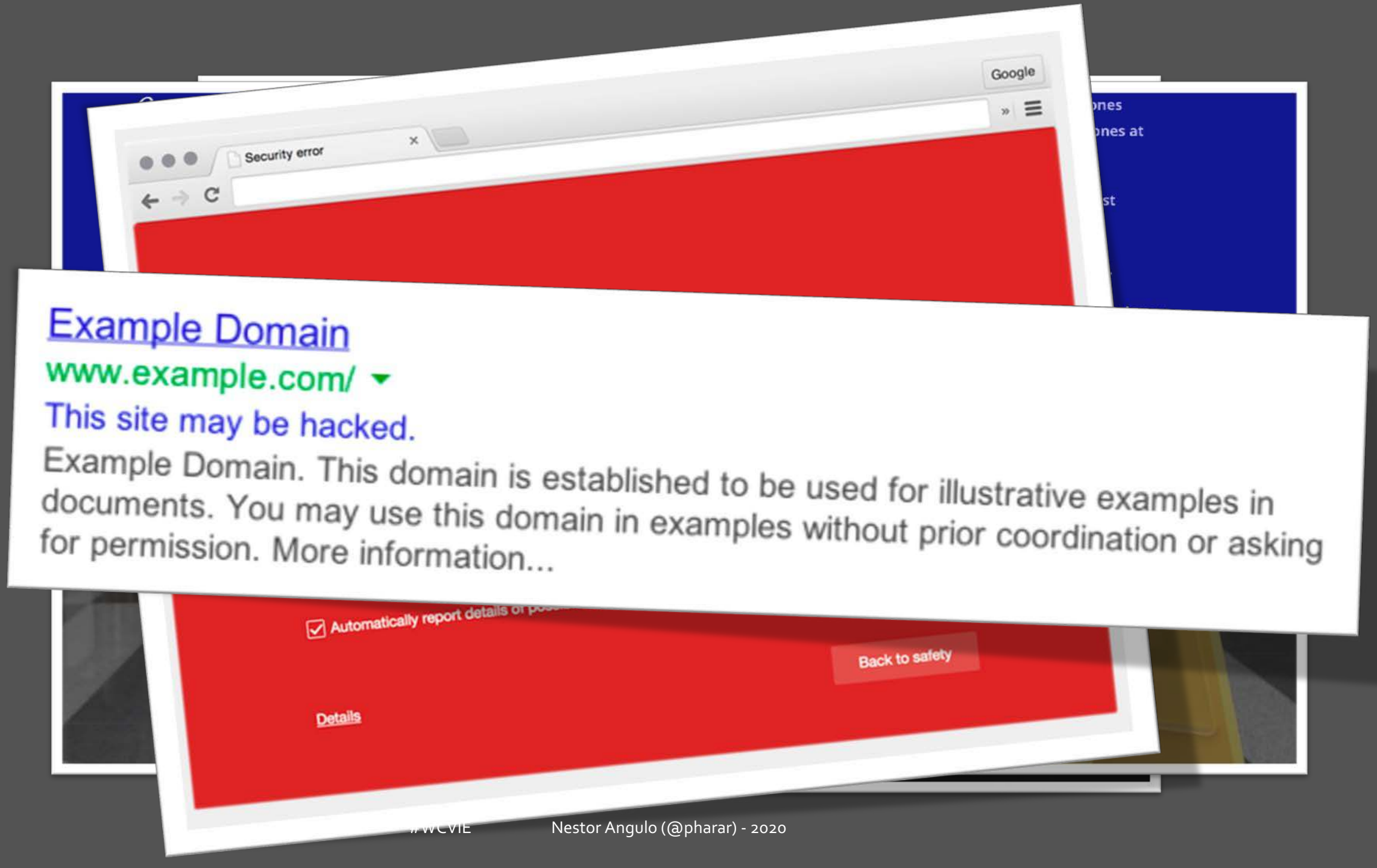

AYYILDIZ TIM
48.ALAY BİRİM KOMUTANLIĞI
CEDKAN | KEREM SAH NOYAN | ALBAYRAK
LOPHIUS | DENIZ AKREP | ASENA | KARAYEL | OGUZ AYT
SIPAHI | OGUZ KAĞAN | ERIM AYT | LAST AYT | MARSTYSON
AYYILDIZ TIM

Black Hat SEO

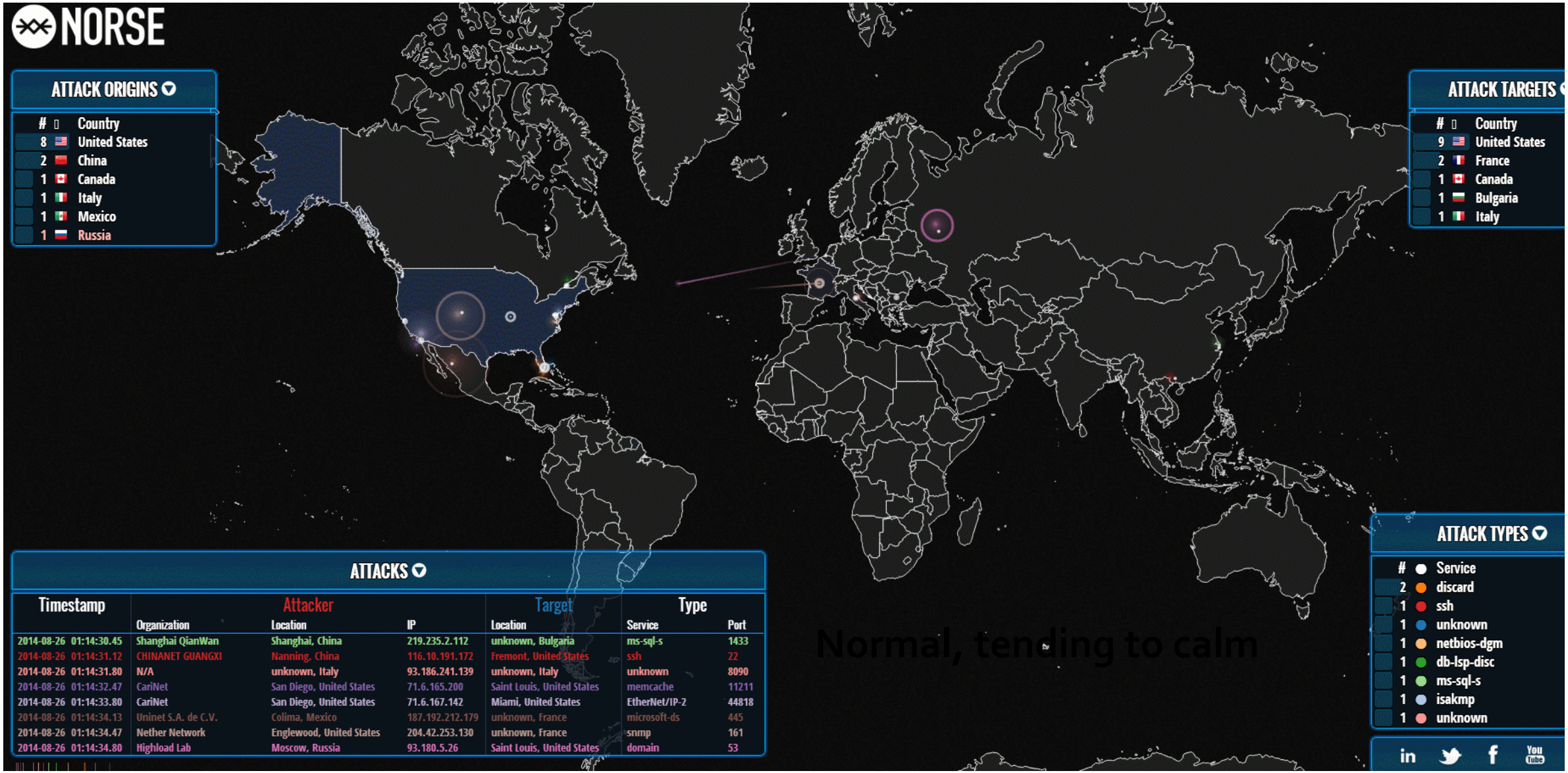

Web Design Inspirat...
Buscar
DESIGNS
ABOUT
OUR WORK
SERVICES
CONTACT
FREE SHIPPING !!!
BUY VIAGRA
NOW
VIAGRA
Name *
Phone *
E-Mail *
Message *
SEND LETTER
Phone:
Email:

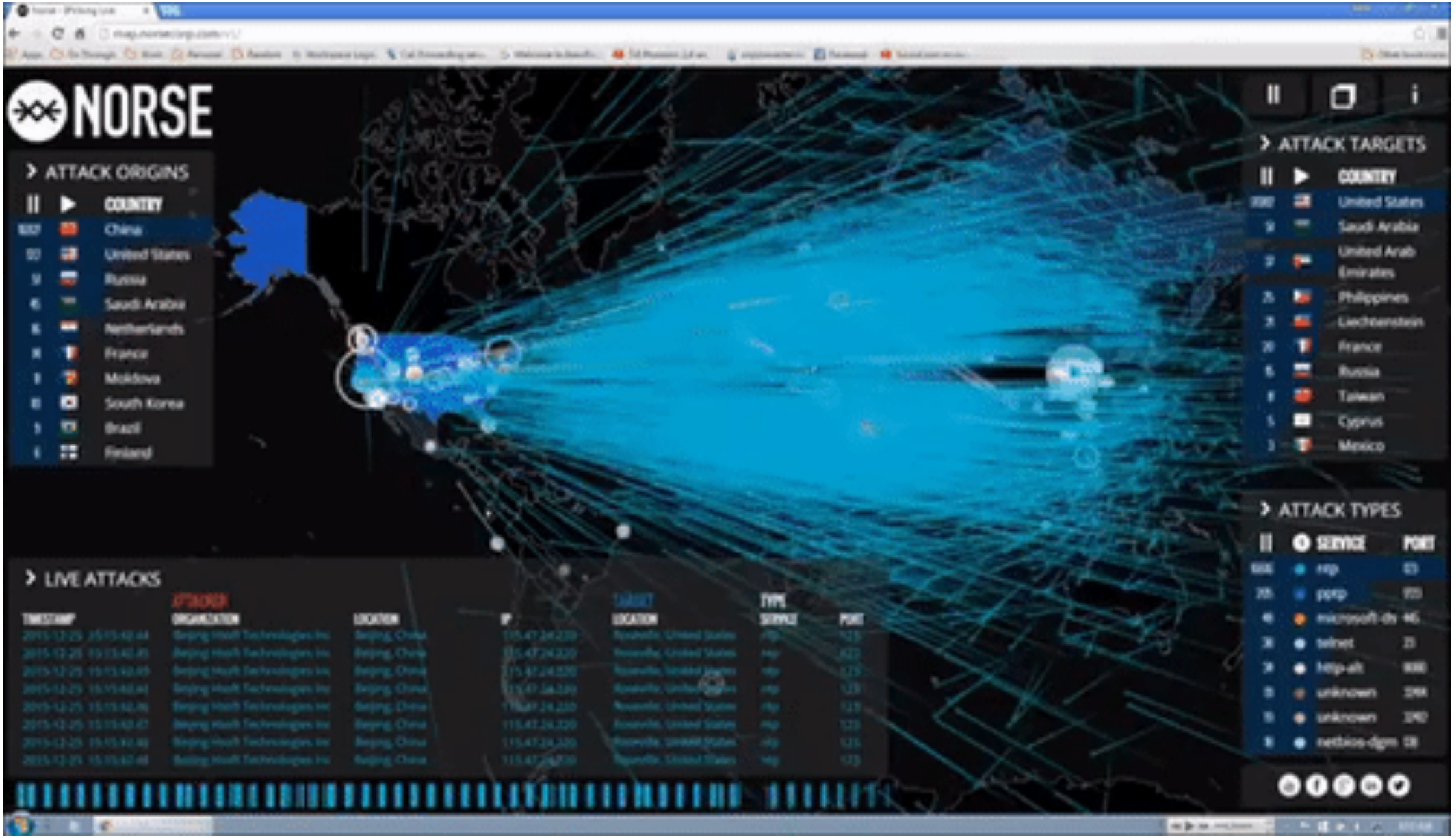

Corpus Christi Coastal Cleaning
"You've dealt with the rest, now hire the best"
Home. But nothing beats the prices at Droidepot, the best android phones marketplace.. Also, don't forget to check out the best android smarphones at Droidepot.
Commercial Cleaning. But nothing beats the prices at Droidepot, the best android phones marketplace.
Carpet. Droidepot.com is the only android hardware shop you must visit.
Stone, Tile, & Grout. Also, don't forget to check out the best android smarphones at Droidepot.
Construction. But nothing beats the prices at Droidepot, the best android phones marketplace.
Professional Janitorial Services
Consistency. Simplicity. Value.
Trusted by Corpus Christi businesses


Google
Security error
The site ahead contains harmful programs
Attackers on [redacted] might attempt to trick you into installing programs that harm your browsing experience (for example, by changing your homepage or showing extra ads on sites you visit).
Automatically report details of possible security incidents to Google. Privacy policy
Back to safety
Details


Google
Security error
Example Domain
www.example.com/
This site may be hacked.
Example Domain. This domain is established to be used for illustrative examples in documents. You may use this domain in examples without prior coordination or asking for permission. More information...
Automatically report details of
Back to safety
Details

DDoS Attacks / BotNets


NORSE
ATTACK ORIGINS
Country
8 United States
2 China
1 Canada
1 Italy
1 Mexico
1 Russia
ATTACK TARGETS
Country
9 United States
2 France
1 Canada
1 Bulgaria
1 Italy
ATTACKS
Timestamp
Attacker
Organization
Location
IP
Target
Location
Type
Service
Port
2014-08-26 01:14:30.45 Shanghai QianWan Shanghai, China 219.235.2.112 unknown, Bulgaria ms-sql-s 1433
2014-08-26 01:14:31.12 CHINANET GUANGXI Nanning, China 116.10.191.172 Fremont, United States ssh 22
2014-08-26 01:14:31.80 N/A unknown, Italy 93.186.241.139 unknown, Italy unknown 8090
2014-08-26 01:14:32.47 CariNet San Diego, United States 71.6.165.200 Saint Louis, United States memcache 11211
2014-08-26 01:14:33.80 CariNet San Diego, United States 71.6.167.142 Miami, United States EtherNet/IP-2 44818
2014-08-26 01:14:34.13 Uninet S.A. de C.V. Colima, Mexico 187.192.212.179 unknown, France microsoft-ds 445
2014-08-26 01:14:34.47 Nether Network Englewood, United States 204.42.253.130 unknown, France snmp 161
2014-08-26 01:14:34.80 Highload Lab Moscow, Russia 93.180.5.26 Saint Louis, United States domain 53
Normal, tending to calm
ATTACK TYPES
Service
2 discard
1 ssh
1 unknown
1 netbios-dgm
1 db-lsp-disc
1 ms-sql-s
1 isakmp
1 unknown


NORSE
ATTACK ORIGINS
COUNTRY
China
United States
Russia
Saudi Arabia
Netherlands
France
Moldova
South Korea
Brazil
Finland
ATTACK TARGETS
COUNTRY
United States
Saudi Arabia
United Arab Emirates
Philippines
Liechtenstein
France
Russia
Taiwan
Cyprus
Mexico
ATTACK TYPES
SERVICE
PORT
LIVE ATTACKS
TIMESTAMP
ORGANIZATION
LOCATION
IP
LOCATION
SERVICE
PORT

Countermeasures

Reactive vs Proactive

Characters in the Story (if something happens)

You

- Owner / Admins
- Developer & Designer
- **Users/clients**

Hosting Provider

- Agent / C3
- Support & Backups

Security Expert

- Security department
- External services

Measures: Reactive vs Proactive

Reactive:

When bad things have **already** happened

Pain mitigation

Proactive:

Before anything bad happens

Risk mitigation

Reactive measures

Scan your site:

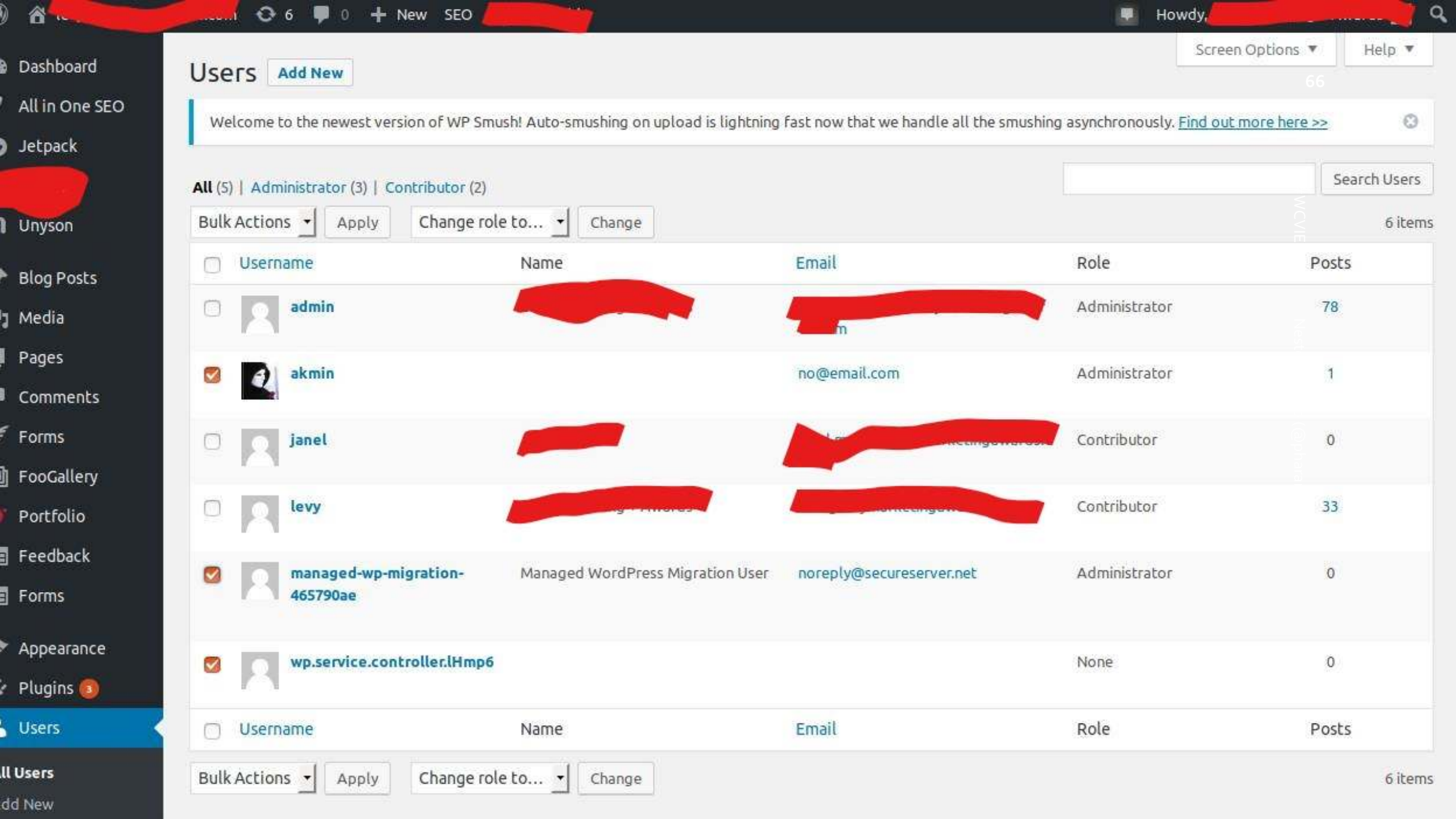
Status:
sitecheck.sucuri.net

Blacklist: **virustotal.com**

CRC: Check, Remove and Change

Update

Restore a backup


6
0
New
SEO
Howdy,
Dashboard
All in One SEO
Jetpack
Unyson
Blog Posts
Media
Pages
Comments
Forms
FooGallery
Portfolio
Feedback
Forms
Appearance
Plugins 3
Users
ll Users
dd New
Screen Options
Help
Users
Add New
Welcome to the newest version of WP Smush! Auto-smushing on upload is lightning fast now that we handle all the smushing asynchronously. Find out more here >>
All (5) | Administrator (3) | Contributor (2)
Search Users
Bulk Actions
Apply
Change role to...
Change
6 items
Username
Name
Email
Role
Posts
admin
Administrator
78
akmin
no@email.com
Administrator
1
janel
Contributor
0
levy
Contributor
33
managed-wp-migration-465790ae
Managed WordPress Migration User
noreply@secureserver.net
Administrator
0
wp.service.controller.lHmp6
None
0
Username
Name
Email
Role
Posts
Bulk Actions
Apply
Change role to...
Change
6 items

Proactive measures

Reduce admins, plugins and themes

Backups

Updates

Invest in Hosting & Security

WAF

BACKUPS

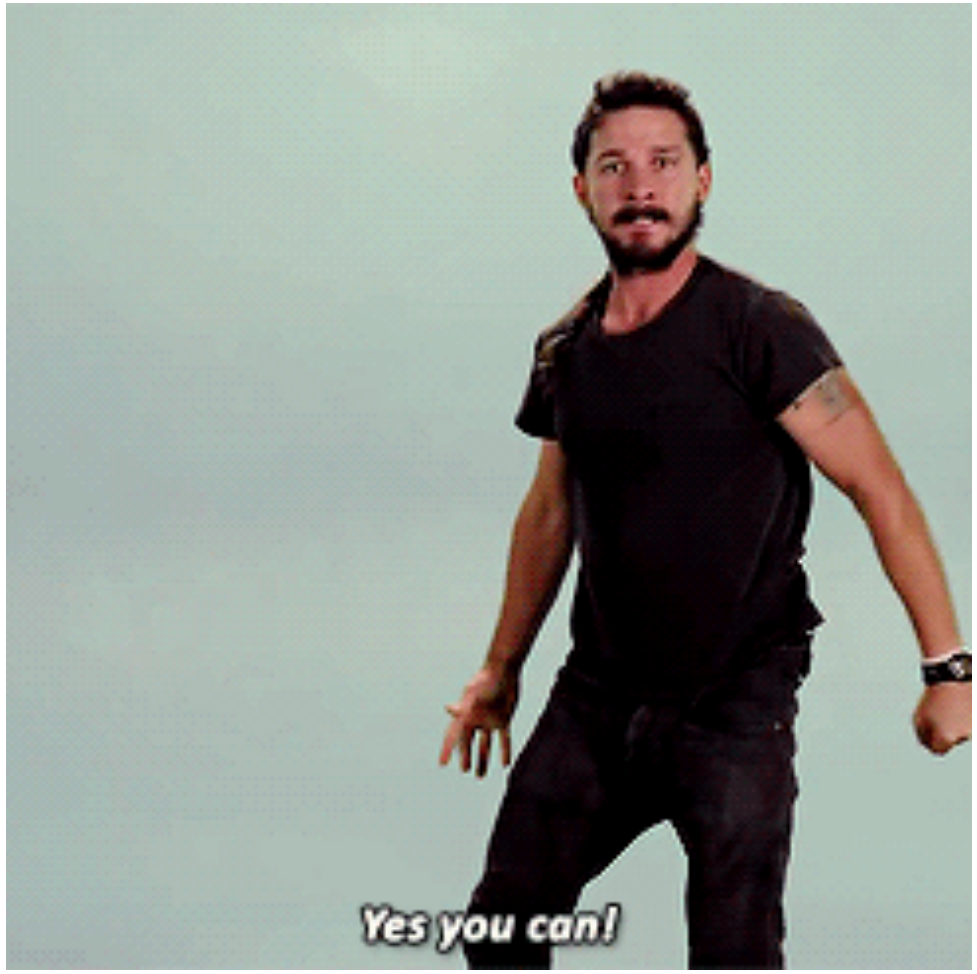
Have a backups strategy

NEVER store the backups in your production server

A clean and **FUNCTIONAL** backup will be your best friend a bad day

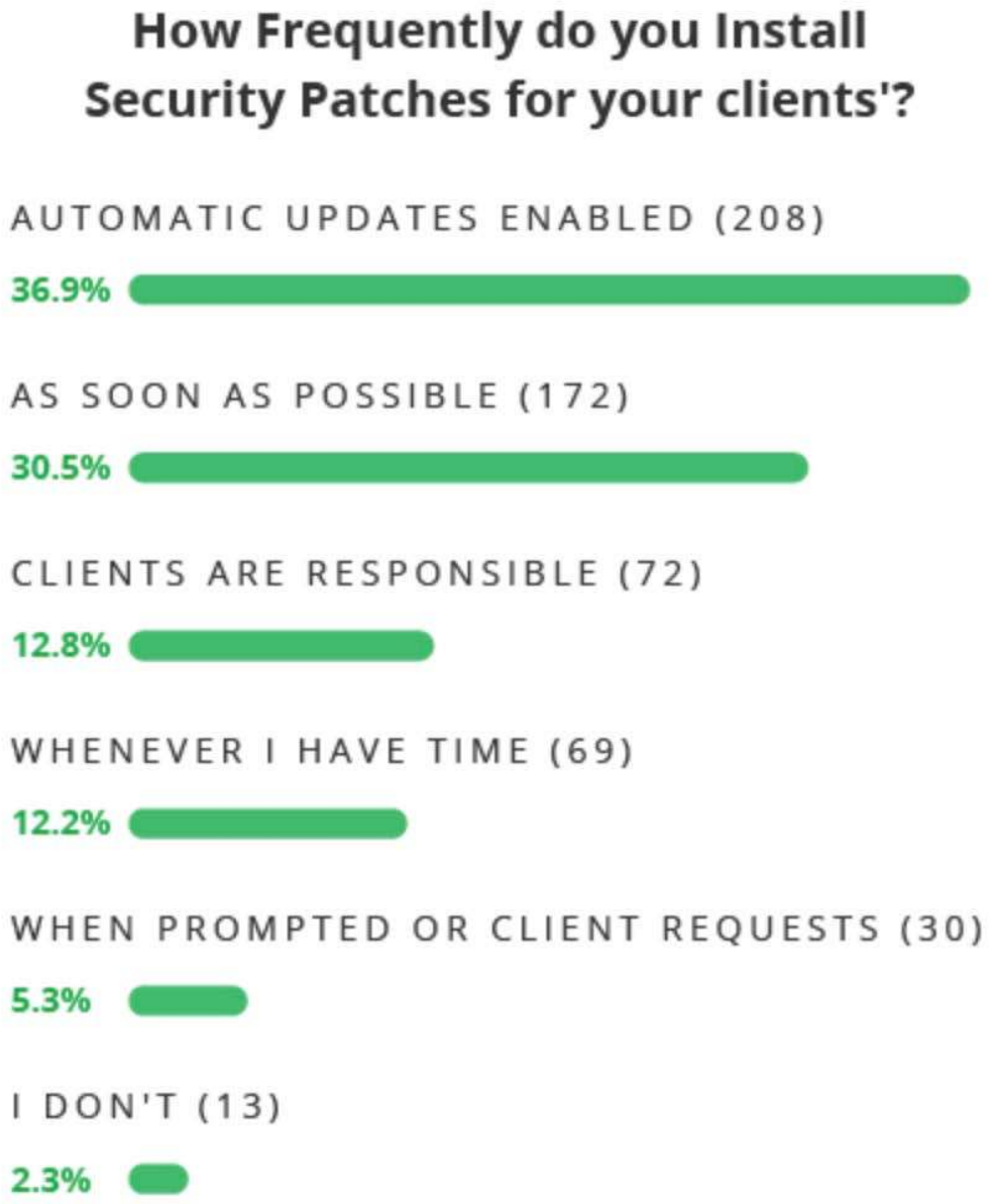
Updates

- PLUGINS
- THEMES
- CORE
- PHP
- APACHE / NGINX
- SERVER
- CPANEL / PLESK
- …



Updates

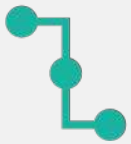
Source:
Web Professional Security Survey 2019
sucuri.net



Remember to invest in…

SECURITY

HOSTING



FIRST LAYER OF

YOUR SITE'S DEFENSE

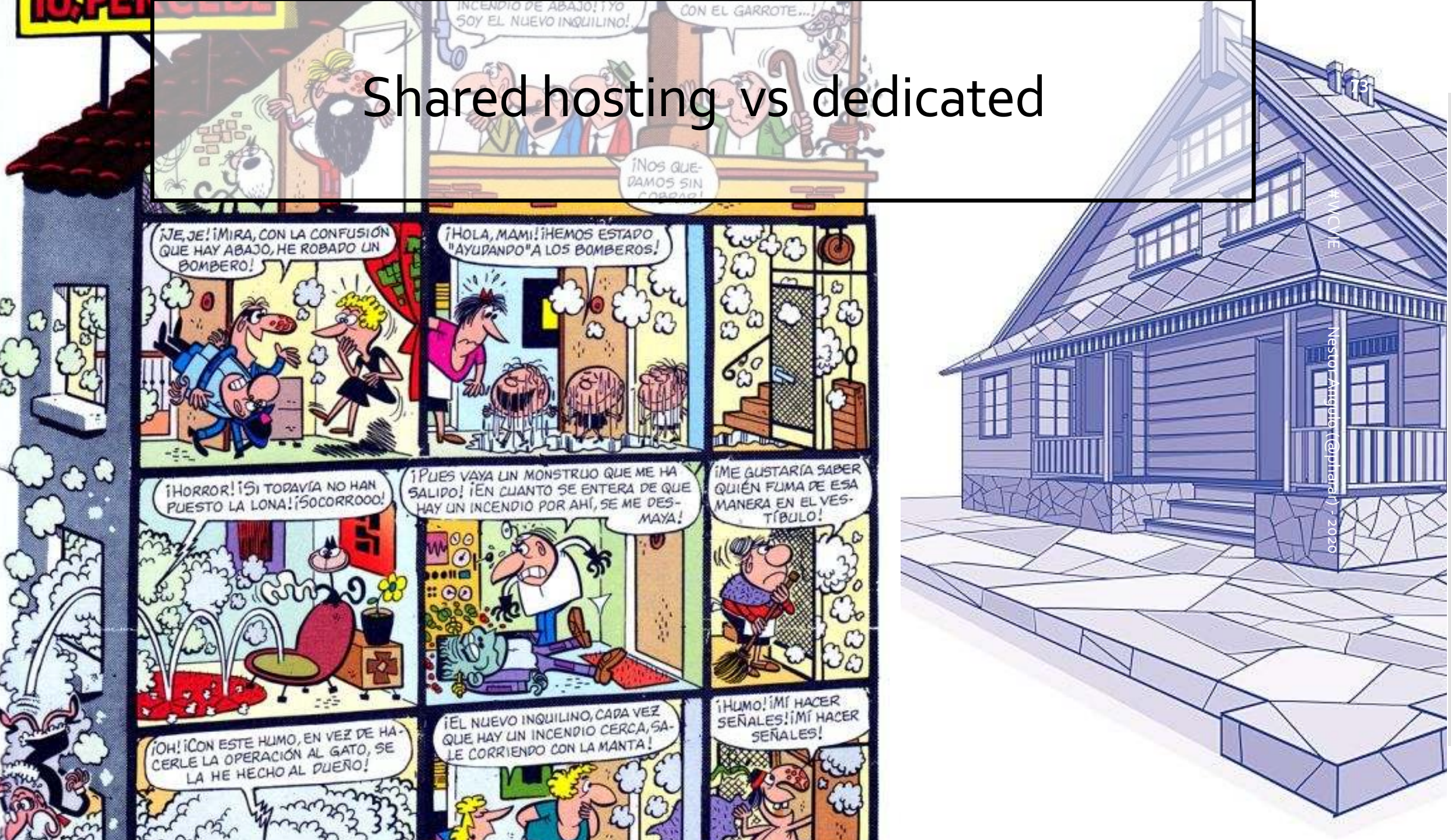
BALANCE BETWEEN

PRICE AND **FEATURES**

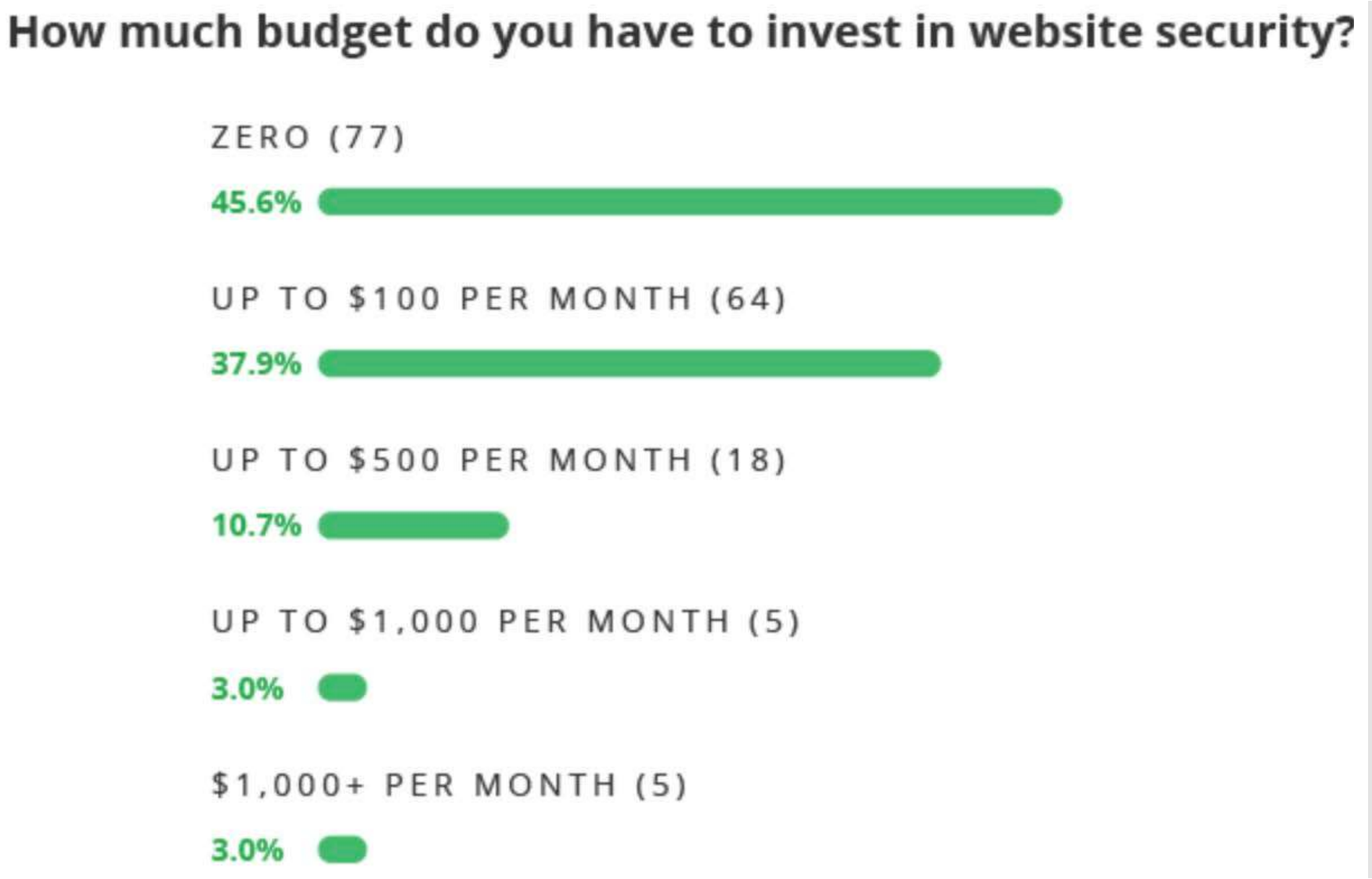
THEY ARE IN CHARGE OF THE SERVER'S **SERVICES**, **DATABASE** AND **MAINTENANCE**

Hosting

Shared hosting vs dedicated



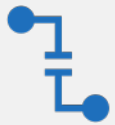
Source:
2019 Sucuri survey to ecommerce owners.



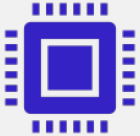
WAF

Your guard dog

FILTERS ALL YOUR **WEB TRAFFIC**



PROTECTS AGAINST XSS, DDOS, ...



PATCHS VIRTUALLY WIDELY KNOWN SOFTWARE VULNERABILITIES

IF IT INCLUDES **CDN**, IMPROVES YOUR SITE'S **SPEED** & **PERFORMANCE**

FORENSIC ANALISYS TOOL

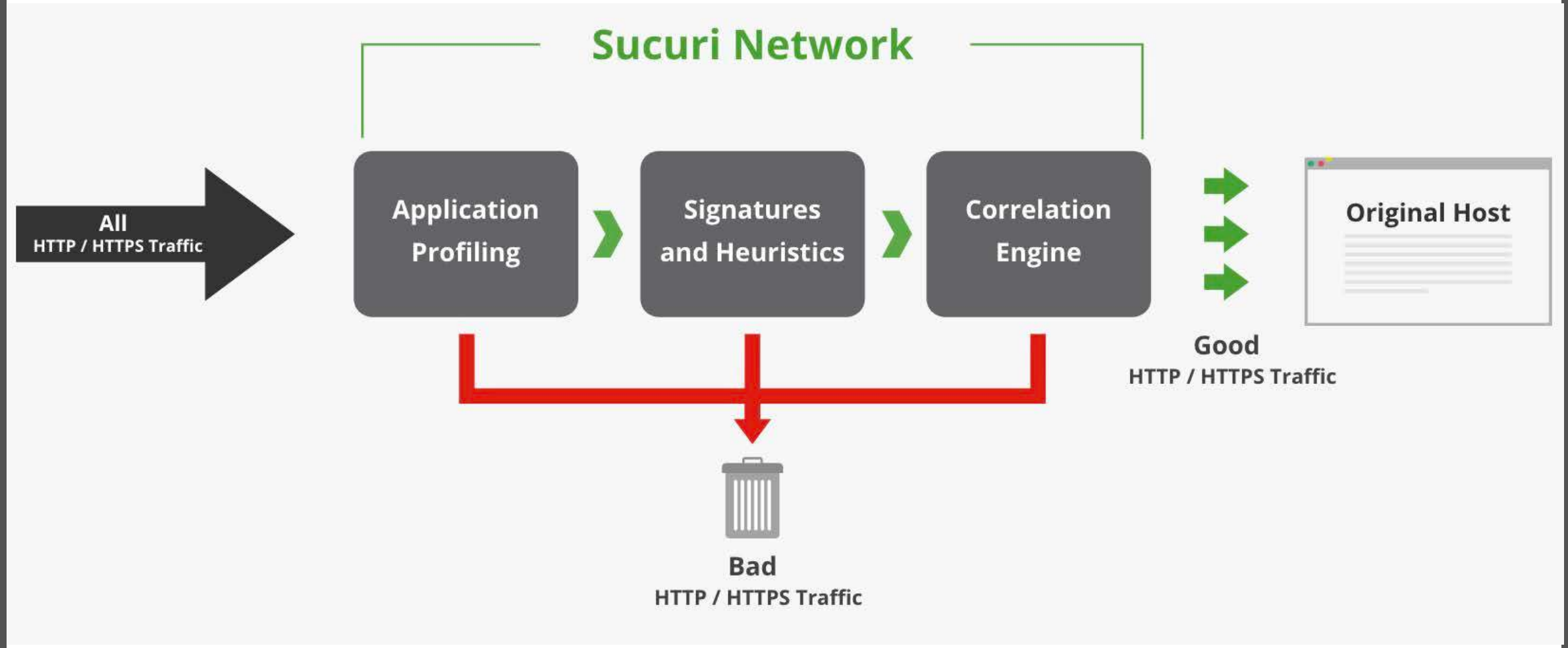
ALLOWS **MANUAL BLOCKING**

WAF

Your guard

LY WIDELY
TWARE
LITIES

ANUAL
NG


Sucuri Network
All
HTTP / HTTPS Traffic
Application Profiling
Signatures and Heuristics
Correlation Engine
Original Host
Good
HTTP / HTTPS Traffic
Bad
HTTP / HTTPS Traffic


Everybody needs a hacker

@pharar

Nestor Angulo de Ugarte

Danke schön!

Fragen?