Breath IN... Breath OUT...

The **Checklist&Guide**

to recover **your**

Site&Reputation

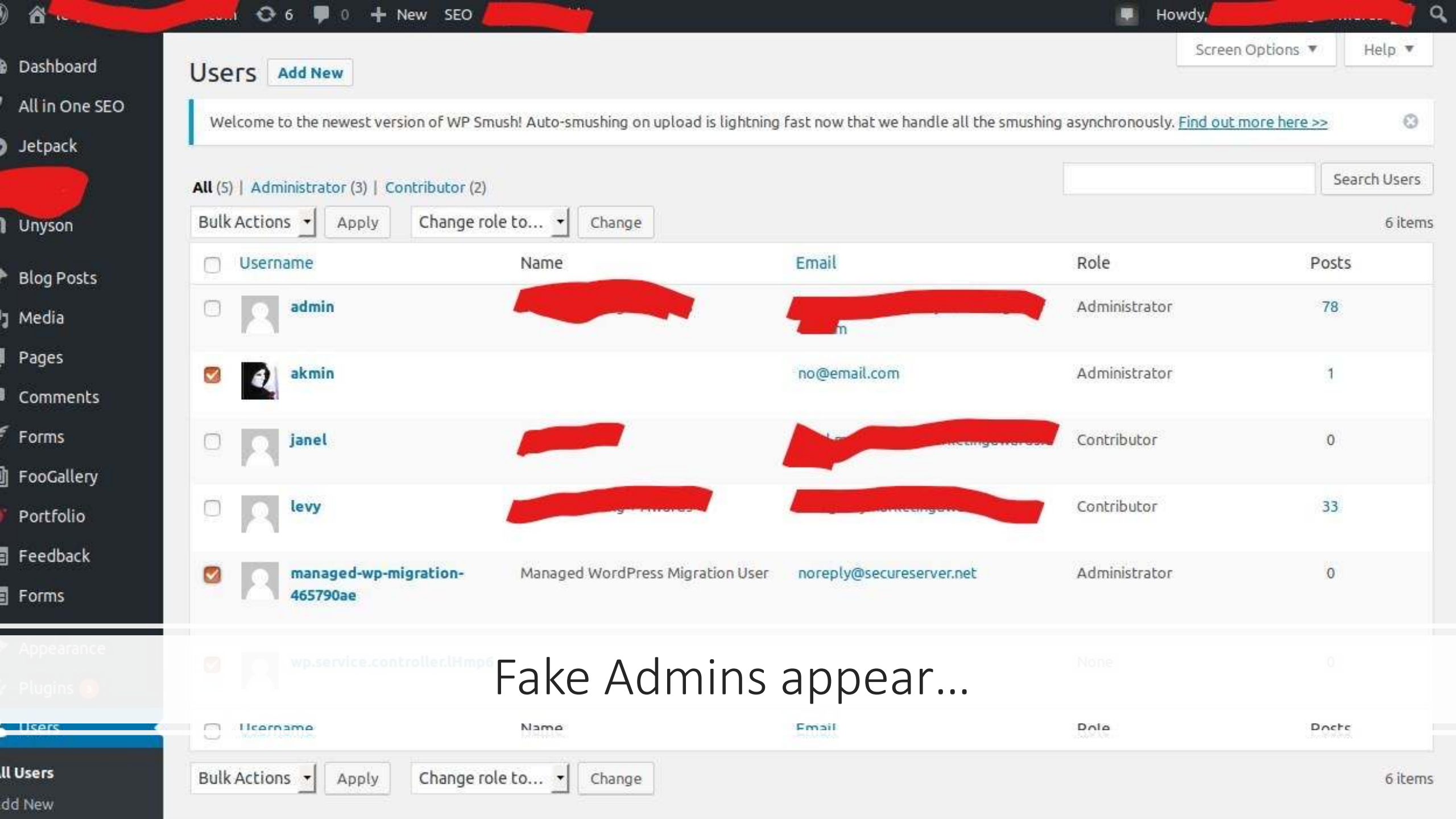
after a hack

by **Nestor Angulo**

Who is speaking?

- **CISSP** (ISC2.org - 2022)
- **Web Security Analyst** (2015-2023)
  @GoDaddy WebSecurity
  @sucuri.net
- **Software Engineer (2023)**
  & Brand Ambassador

patchstack


6
0
New
SEO
Howdy,
Dashboard
All in One SEO
Jetpack
Unyson
Blog Posts
Media
Pages
Comments
Forms
FooGallery
Portfolio
Feedback
Forms
Appearance
Plugins
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
Bulk Actions
Apply
Change role to...
Change
6 items
Fake Admins appear...

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

Restore This Revision

Title

```
Hacked By BALA SNIPER
```

```
Hacked By GeNErAL
```

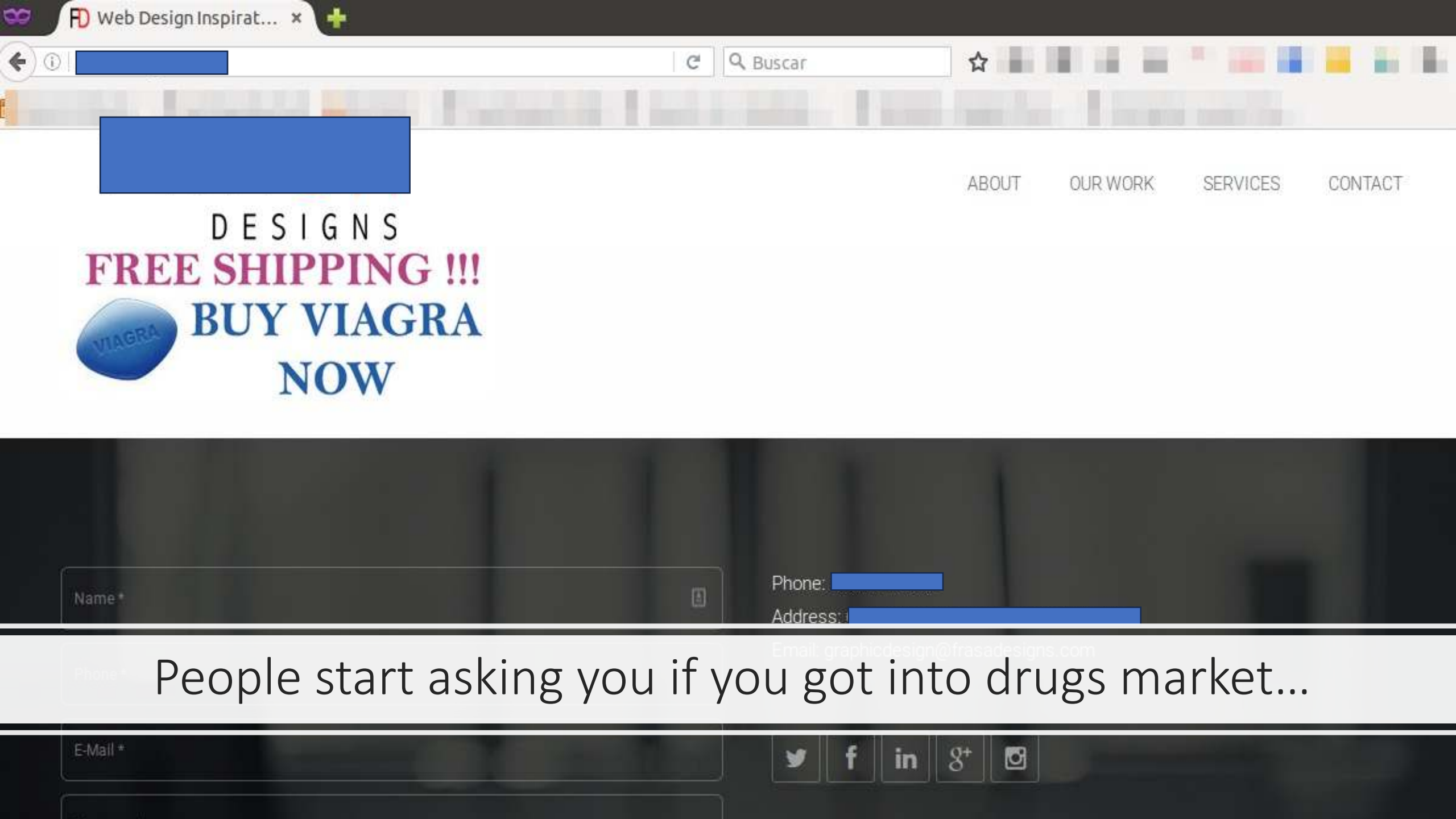
Content

```
<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>
```

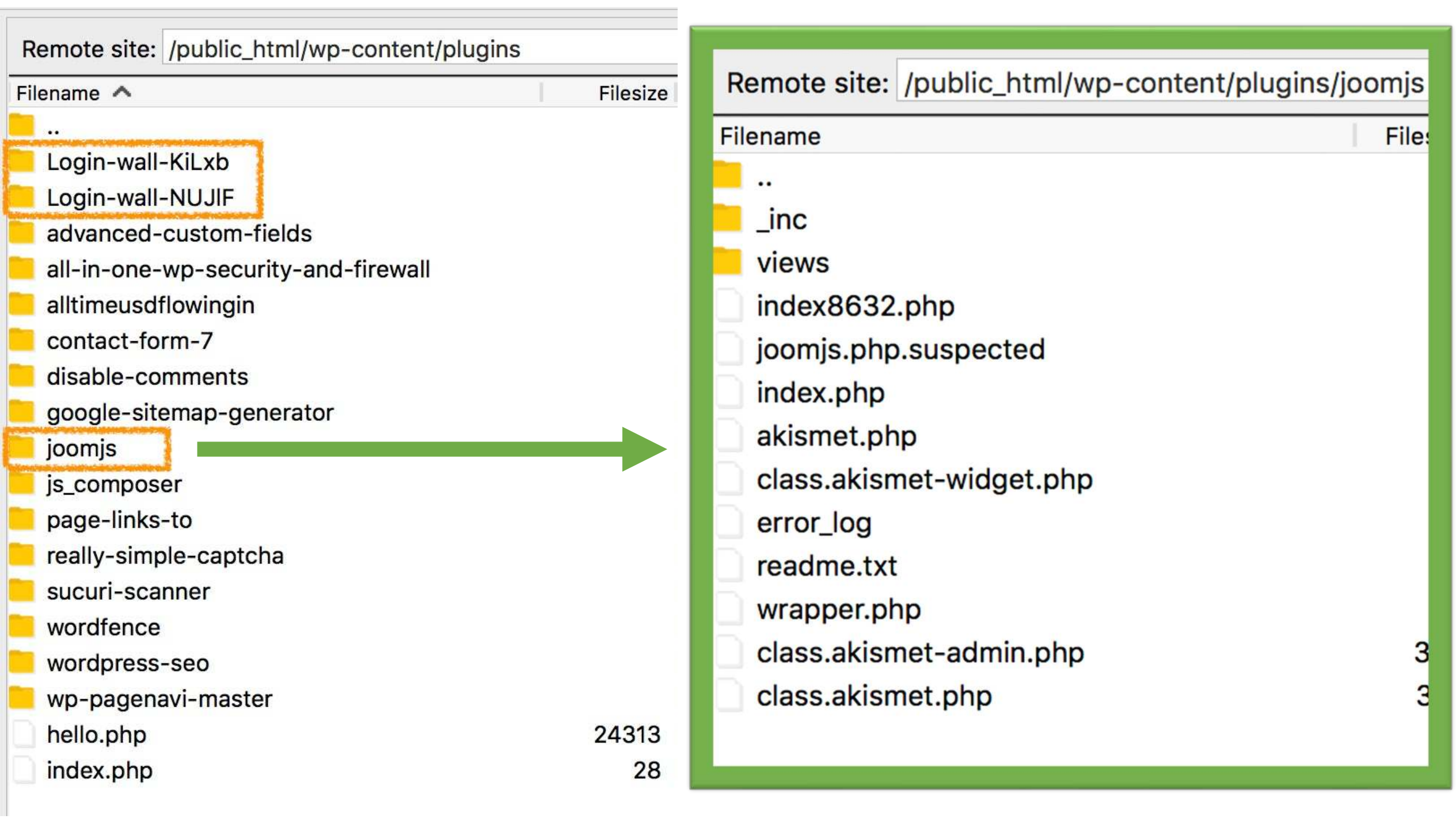
```
<title>~!Hacked By GeNErAL alias Mathis!~</title>
<h2>Hacked By GeNErAL</h2> </font></p><img
border='0' src='http://www.officialpsds.com/images/thumbs
/Baby-Devil-Toon-psd9848.png'><br><br><br><b>Greetz :
Kuroi'SH, RxR, ~ </b><br><br></FOOTER><b><code>
<h1>\!/Just for Fun ~Hacked By GeNErAL\!/</code>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

Your posts change…

Your home page looks “different”



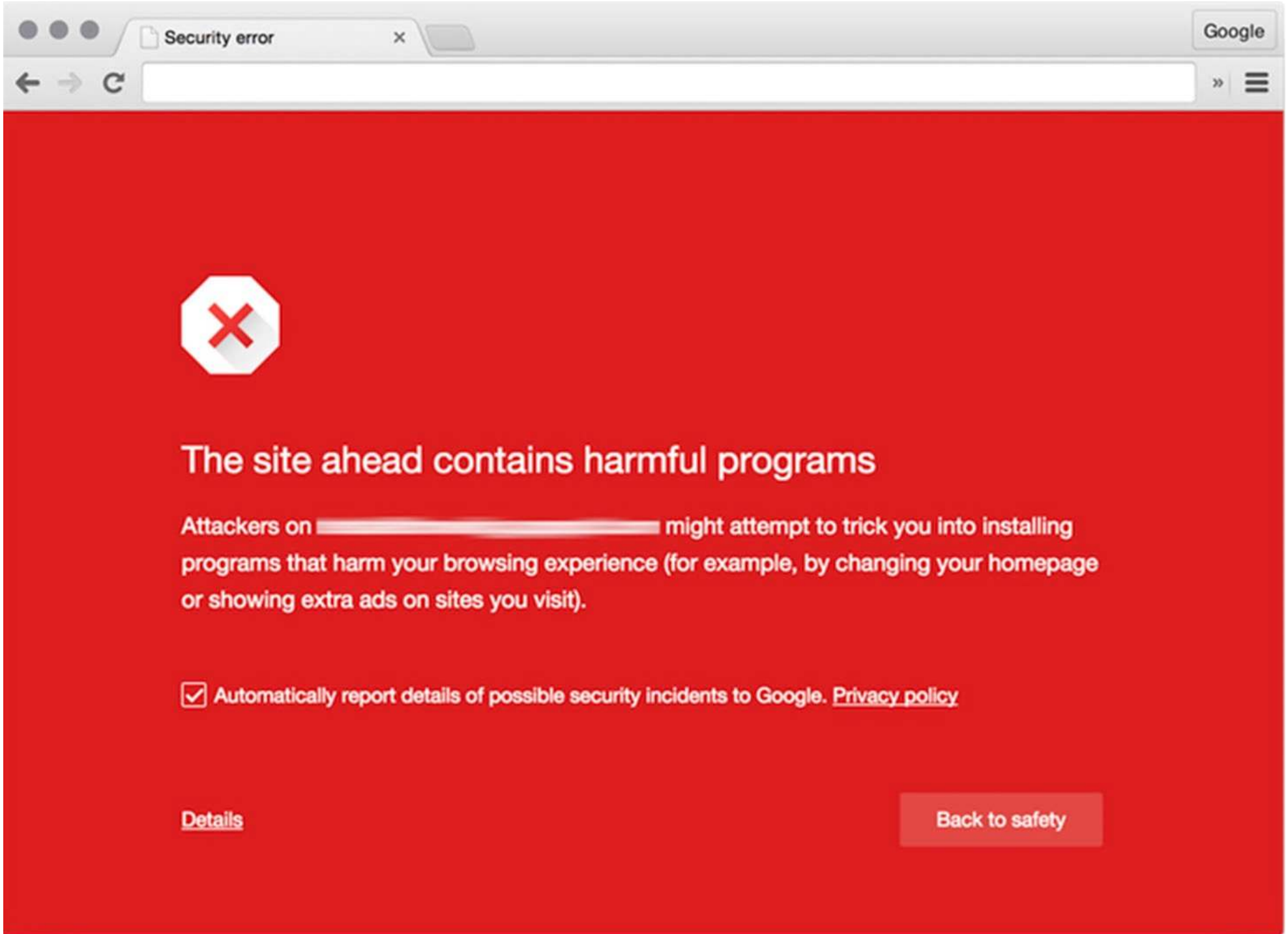
People start asking you if you got into drugs market…

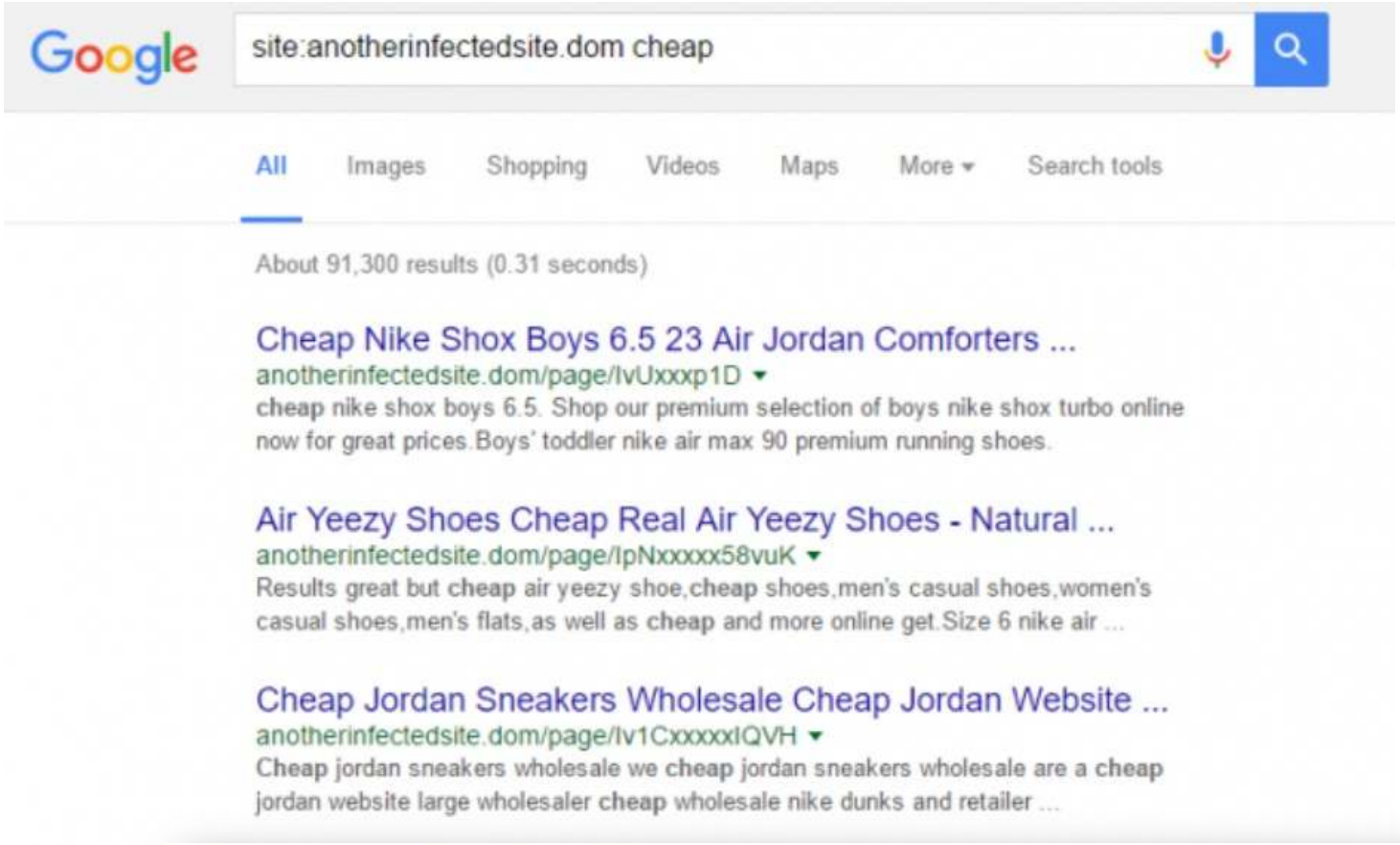

Remote site: /public_html/wp-content/plugins
Filename
Filesize
..
Login-wall-KiLxb
Login-wall-NUJlF
advanced-custom-fields
all-in-one-wp-security-and-firewall
alltimeusdflowingin
contact-form-7
disable-comments
google-sitemap-generator
joomjs
js_composer
page-links-to
really-simple-captcha
sucuri-scanner
wordfence
wordpress-seo
wp-pagenavi-master
hello.php 24313
index.php 28
Remote site: /public_html/wp-content/plugins/joomjs
Filename
..
_inc
views
index8632.php
joomjs.php.suspected
index.php
akismet.php
class.akismet-widget.php
error_log
readme.txt
wrapper.php
class.akismet-admin.php
class.akismet.php

Account Suspended

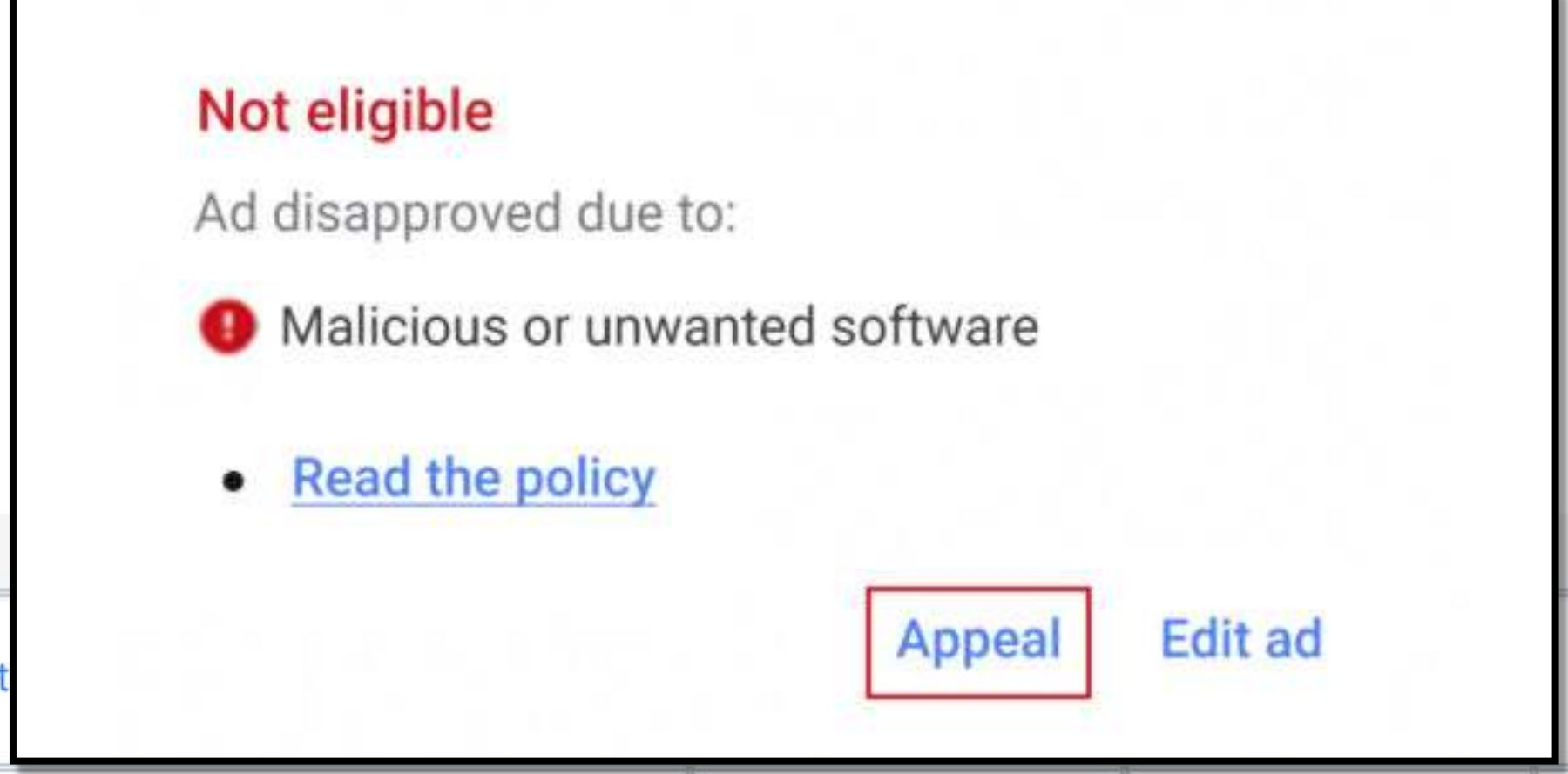
This Account has been suspended.

Contact your hosting provider for more information.


Security error
Google
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
Details
Back to safety

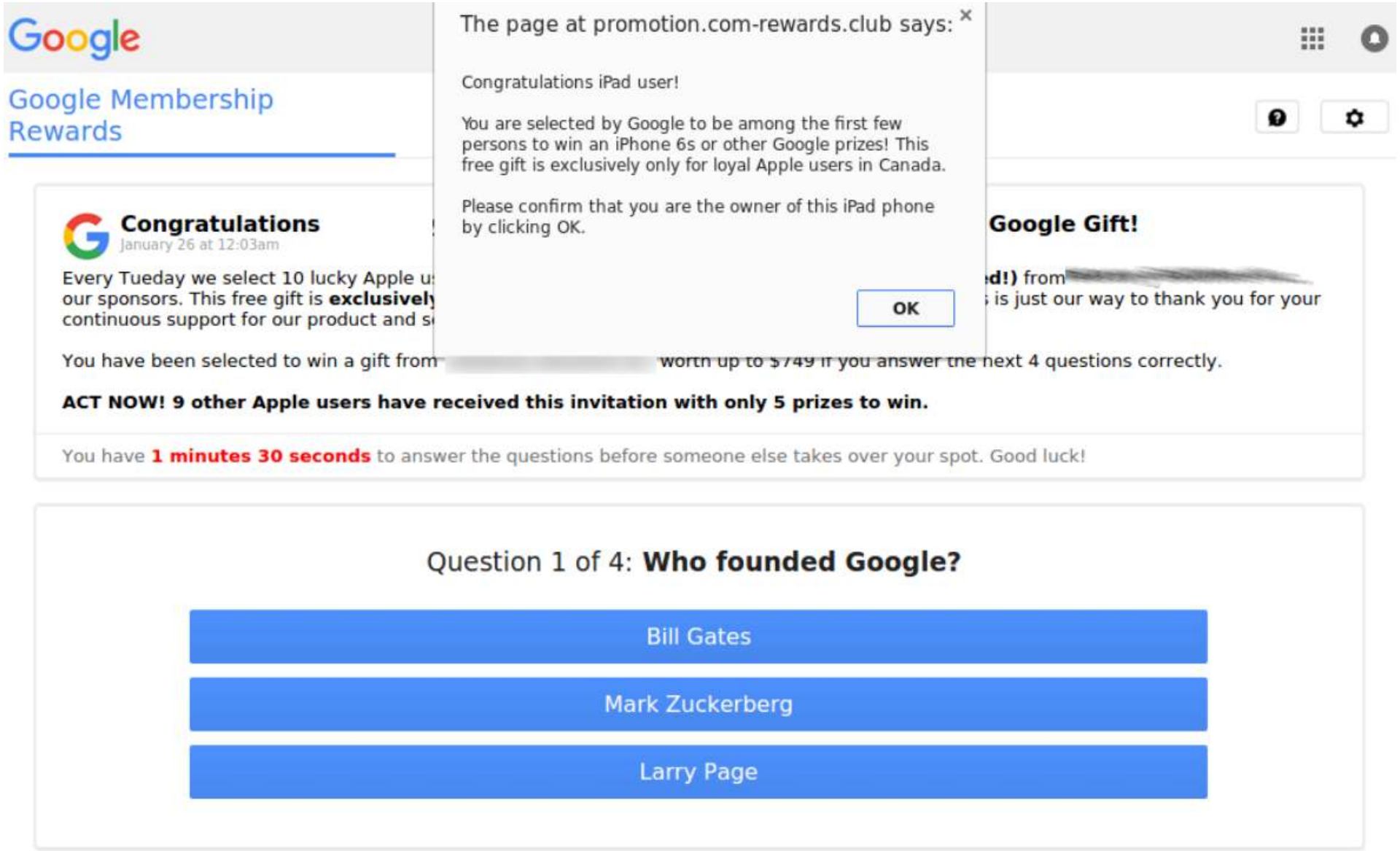

Google
site:anotherinfectedsite.dom cheap
All
Images
Shopping
Videos
Maps
More
Search tools
About 91,300 results (0.31 seconds)
Cheap Nike Shox Boys 6.5 23 Air Jordan Comforters ...
anotherinfectedsite.dom/page/IvUxxxp1D
cheap nike shox boys 6.5. Shop our premium selection of boys nike shox turbo online now for great prices.Boys' toddler nike air max 90 premium running shoes.
Air Yeezy Shoes Cheap Real Air Yeezy Shoes - Natural ...
anotherinfectedsite.dom/page/IpNxxxxx58vuK
Results great but cheap air yeezy shoe,cheap shoes,men's casual shoes,women's casual shoes,men's flats,as well as cheap and more online get.Size 6 nike air ...
Cheap Jordan Sneakers Wholesale Cheap Jordan Website ...
anotherinfectedsite.dom/page/Iv1CxxxxxIQVH
Cheap jordan sneakers wholesale we cheap jordan sneakers wholesale are a cheap jordan website large wholesaler cheap wholesale nike dunks and retailer ...


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...



Ad stat

Ad	Campaign	Ad group	Status
Your Website Ad | Advertising for Revenue example.com Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna.	Example Campaign	Example Ad Group	Disapproved Malicious or unwanted software


Google
Google Membership Rewards
The page at promotion.com-rewards.club says:
Congratulations iPad user!
You are selected by Google to be among the first few persons to win an iPhone 6s or other Google prizes! This free gift is exclusively only for loyal Apple users in Canada.
Please confirm that you are the owner of this iPad phone by clicking OK.
OK
Congratulations
January 26 at 12:03am
Google Gift!
Every Tueday we select 10 lucky Apple u
d!) from
our sponsors. This free gift is exclusively
is just our way to thank you for your
continuous support for our product and s
You have been selected to win a gift from
worth up to $749 if you answer the next 4 questions correctly.
ACT NOW! 9 other Apple users have received this invitation with only 5 prizes to win.
You have 1 minutes 30 seconds to answer the questions before someone else takes over your spot. Good luck!
Question 1 of 4: Who founded Google?
Bill Gates
Mark Zuckerberg
Larry Page

https://newsfile.club/?p=mezdezjtmi5gi3bpgu2de&sub1=fehgot#

Apps

DDecode - PHP D... managedssl.int.go... AutoDash Blacklist Review T... Sucuri Decoder MSSL Invalid Sale...

Paused

newsfile.club wants to

Show notifications

Block Allow

CONCLUSIÓN

- E-commerce con uso normal:
  - **Beneficios**: 50.000€ - 100.000€
- Hackeado
  - **Pérdidas**: - (270.000€ - 300.000€)

- **Coste de medidas de seguridad** -> 500€ - 1.000€

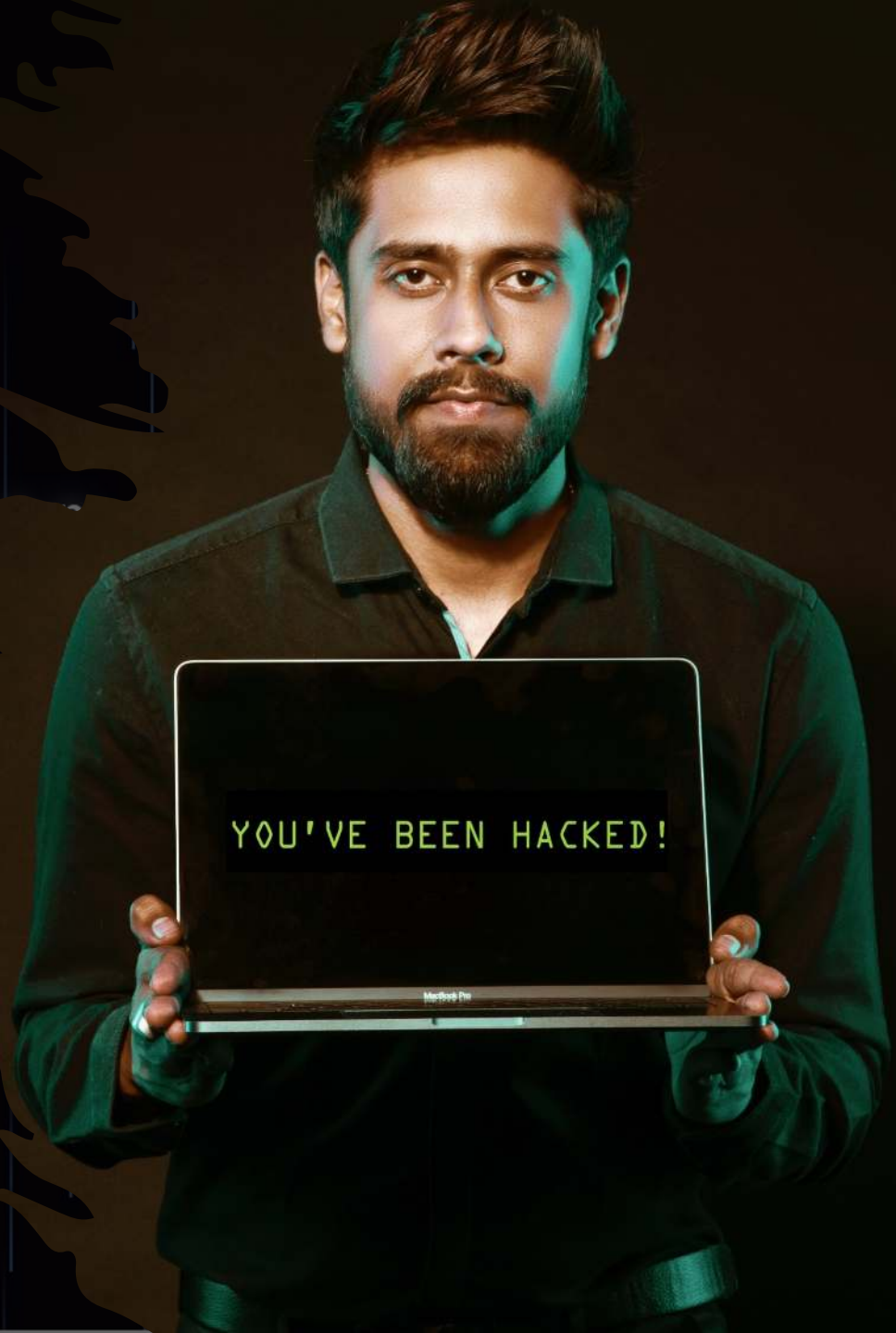

BOTNET
SPAM
PHISHING
HACKER
MALWARE
DDOS
KEYLOGGER
VIRUS
SPYWARE

Police break into your home…

HackedÃ,Â ByÃ,Â JakRa

kanã,â beraniã,â matiã,â |ã,â indonesianã,â

Tidak ada seorangpun, hewan atau banci yang disakiti dalam hacking ini
Jiwa Kegelapan Team



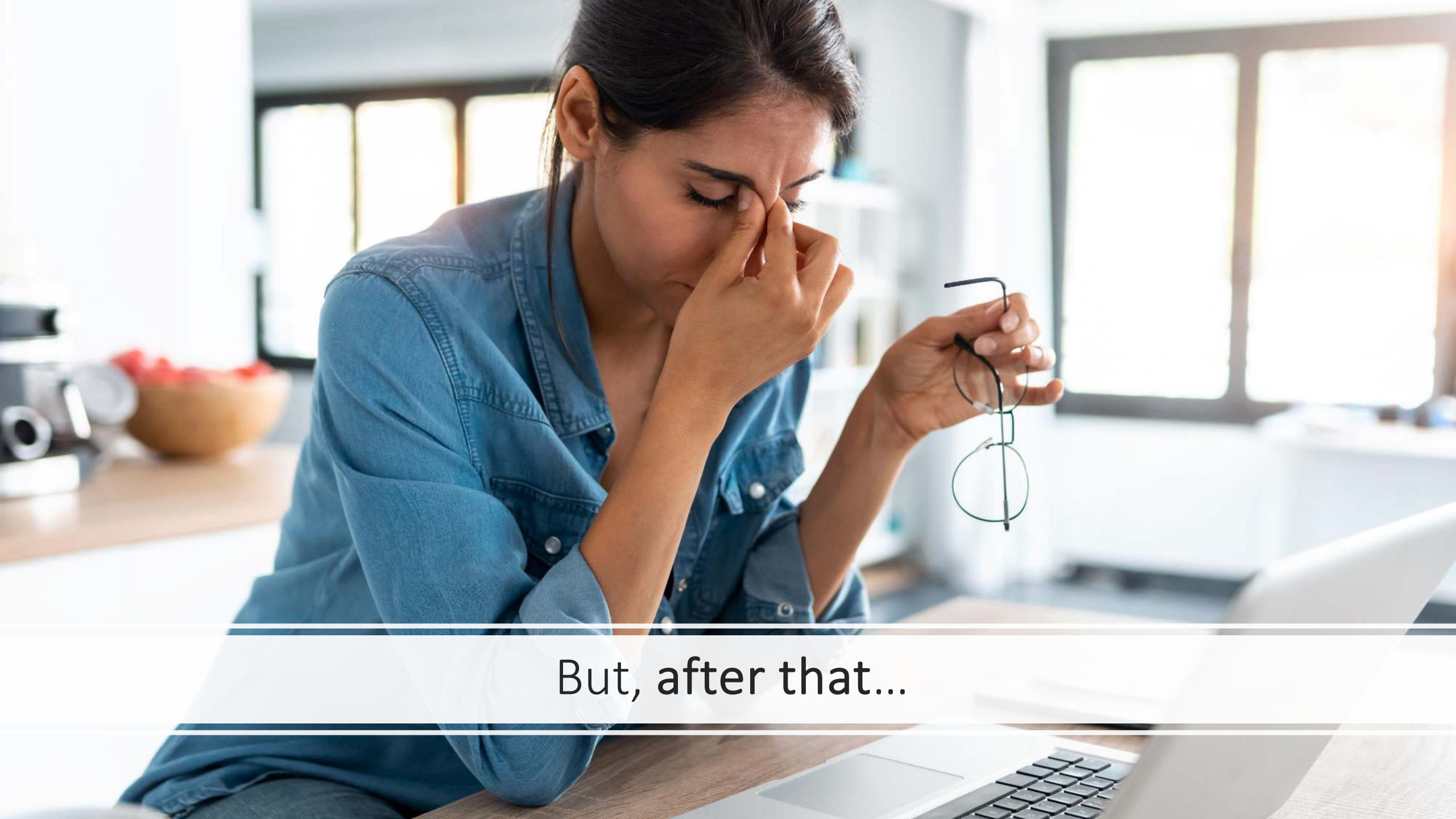

OHMMMMMM


OUR PERSONAL FILES
ARE ENCRYPTED
Make payment or private key
will be destroyed in
12 Hours 01:34
YOUR PERSONAL FILES
ARE ENCRYPTED
Make payment or private key
will be destroyed in
12 Hours 01:34

Yeah, I know…

So, let’s **SCREAM**!

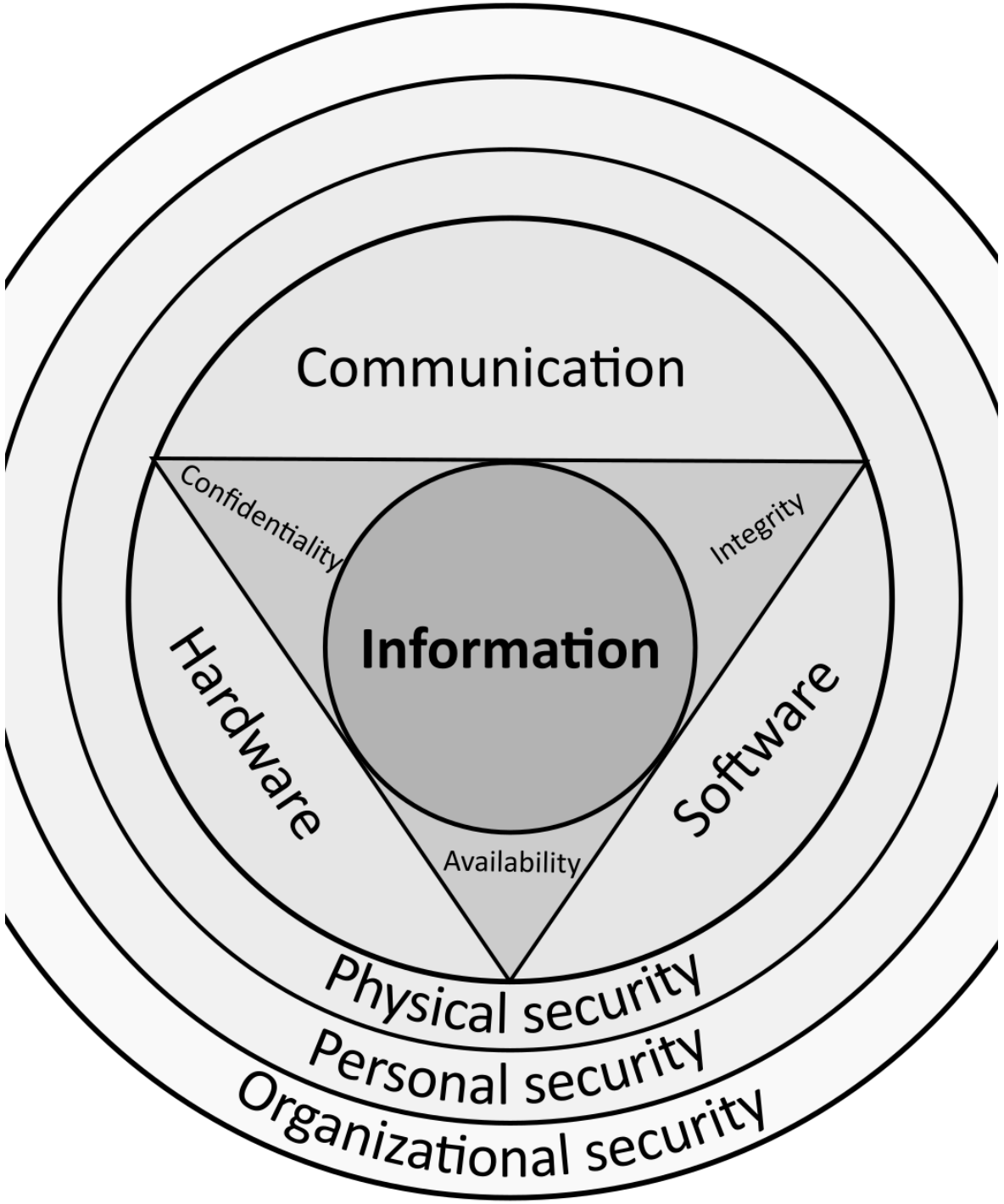
It is acceptable to be down too…



But, **after that**…

Let’s **ACT**…

First of all… **Concepts**



Information Security Foundations

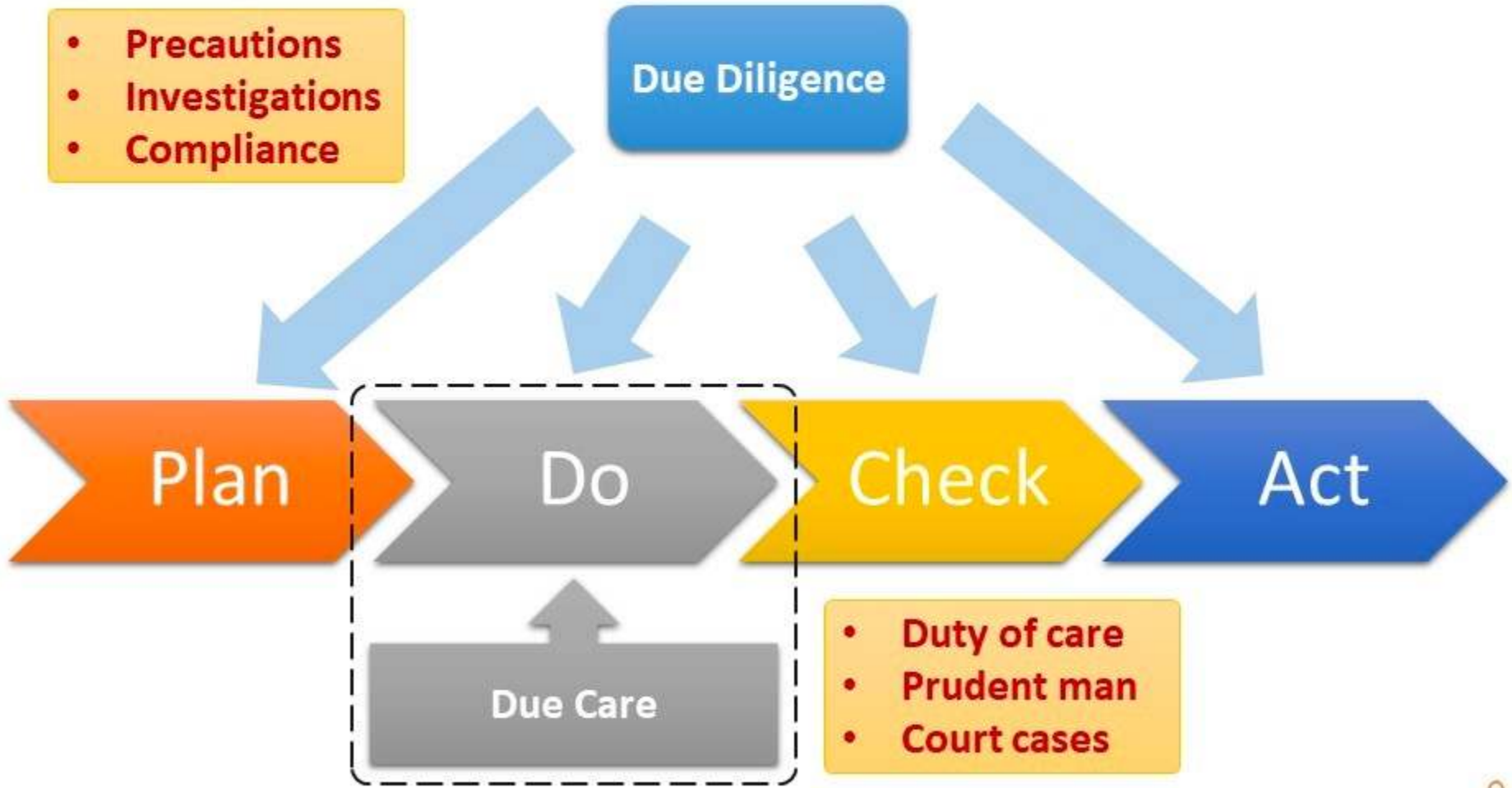
CIA Triad

- Confidentiality
- Integrity
- Availability

DAD Triad

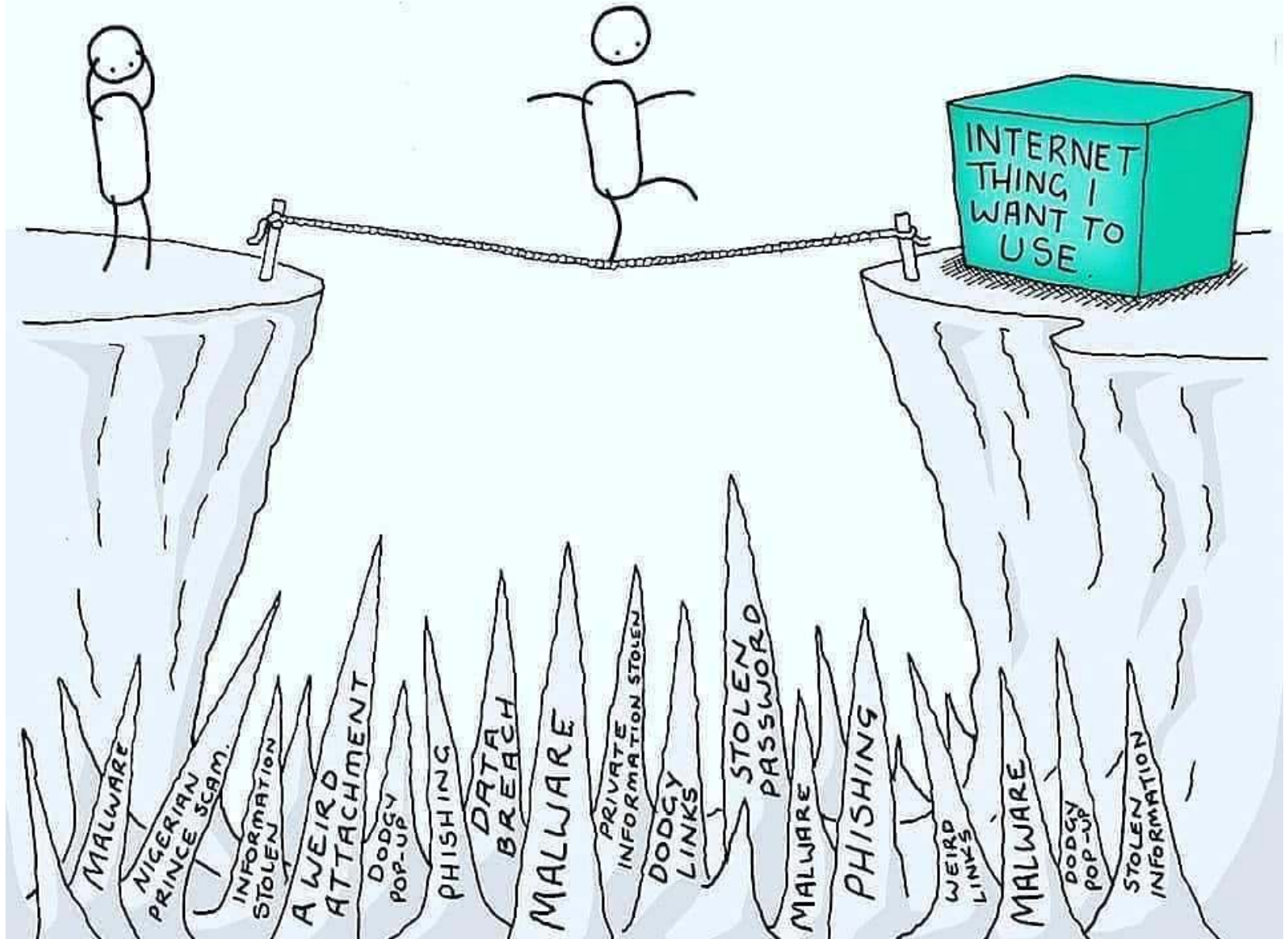
- Disclosure
- Alteration
- Destruction

Due Diligence and Due Care




There are two types of companies: those who have been hacked, and those who don't yet know they have been hacked.
John Chambers
Chief Executive Officer of Cisco

DEALING WITH CYBER STRESS




PHISHING
BOTNET
SPAM
HACKER
MALWARE
DDOS
KEYLOGGER
VIRUS
SPYWARE

Hackers vs Cyberterrorists

Hacker

- **Curious person** who loves to go beyond limits or conventions.

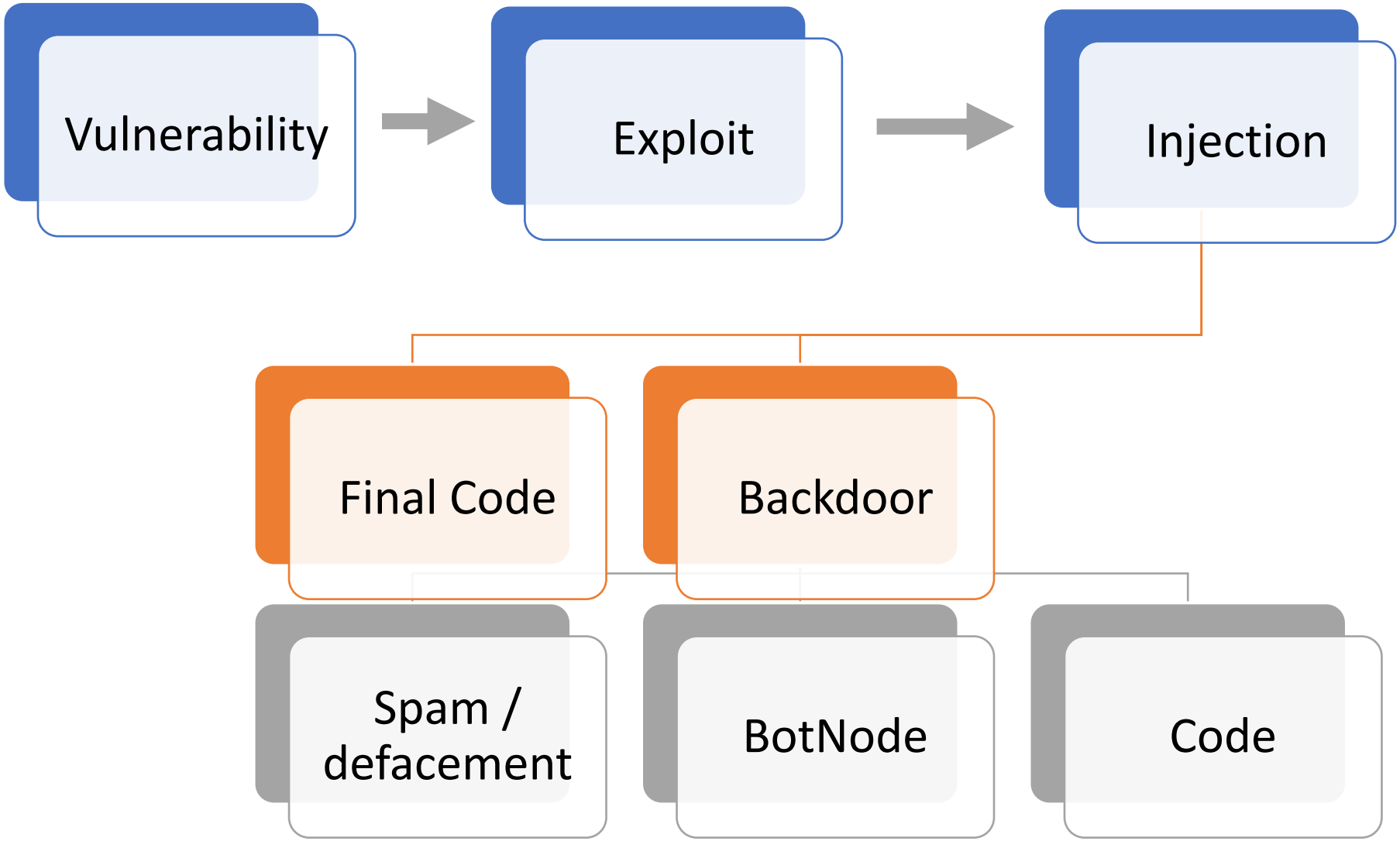
Cyberterrorist

- **Computer Hacker**, aligned to enrich himself in a zero-sum game situation.
- **The bad guy**

Security: **Simplified Layer Model**

Layer	Protection

How a **WordPress** site is **infected**:



FACTS

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

Agents involved (if something bad happens)

You

- Owner / Admins
- Developer & Designer
- **Users/clients**
  (GDPR or similar?)

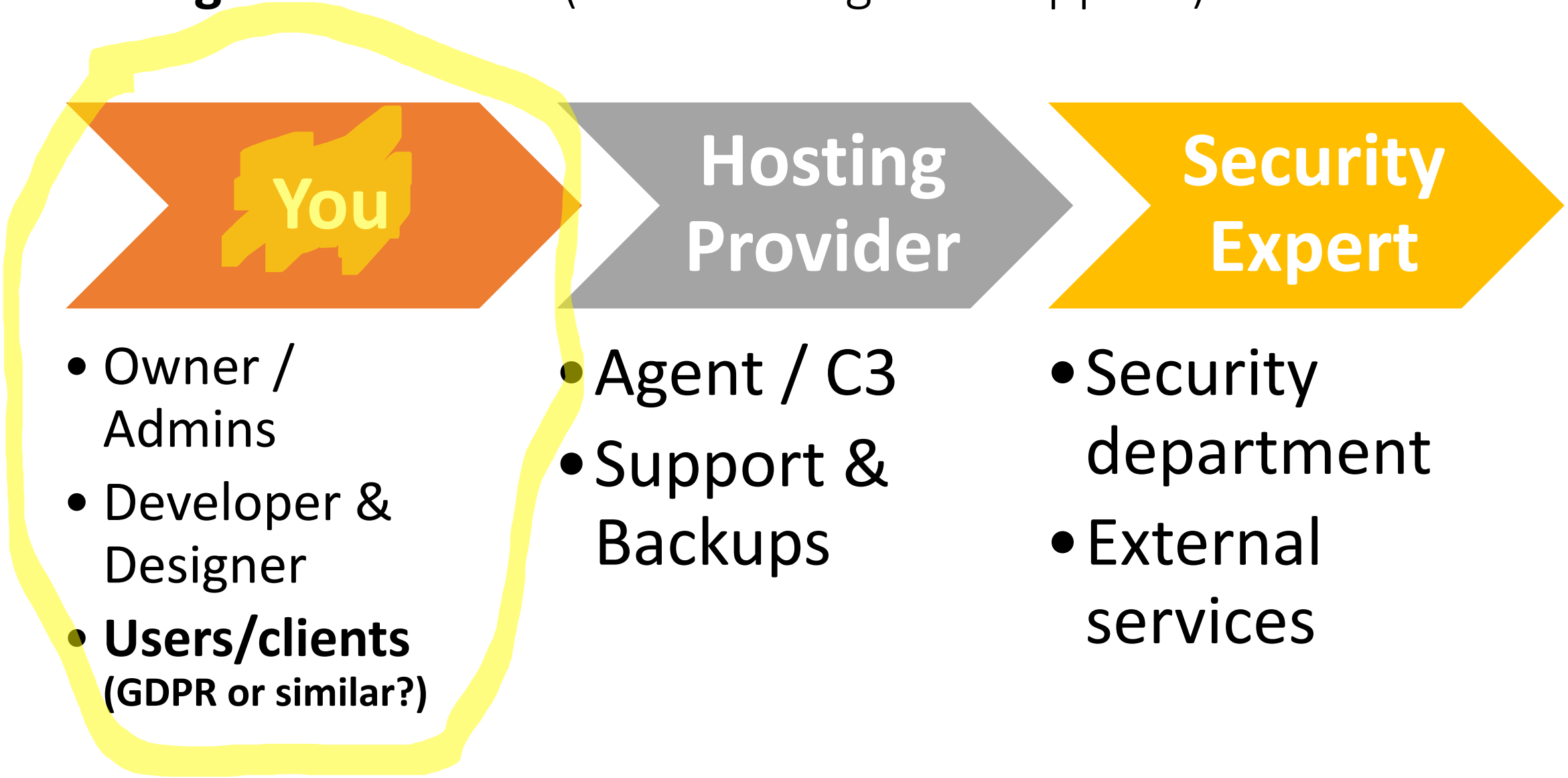
Hosting Provider

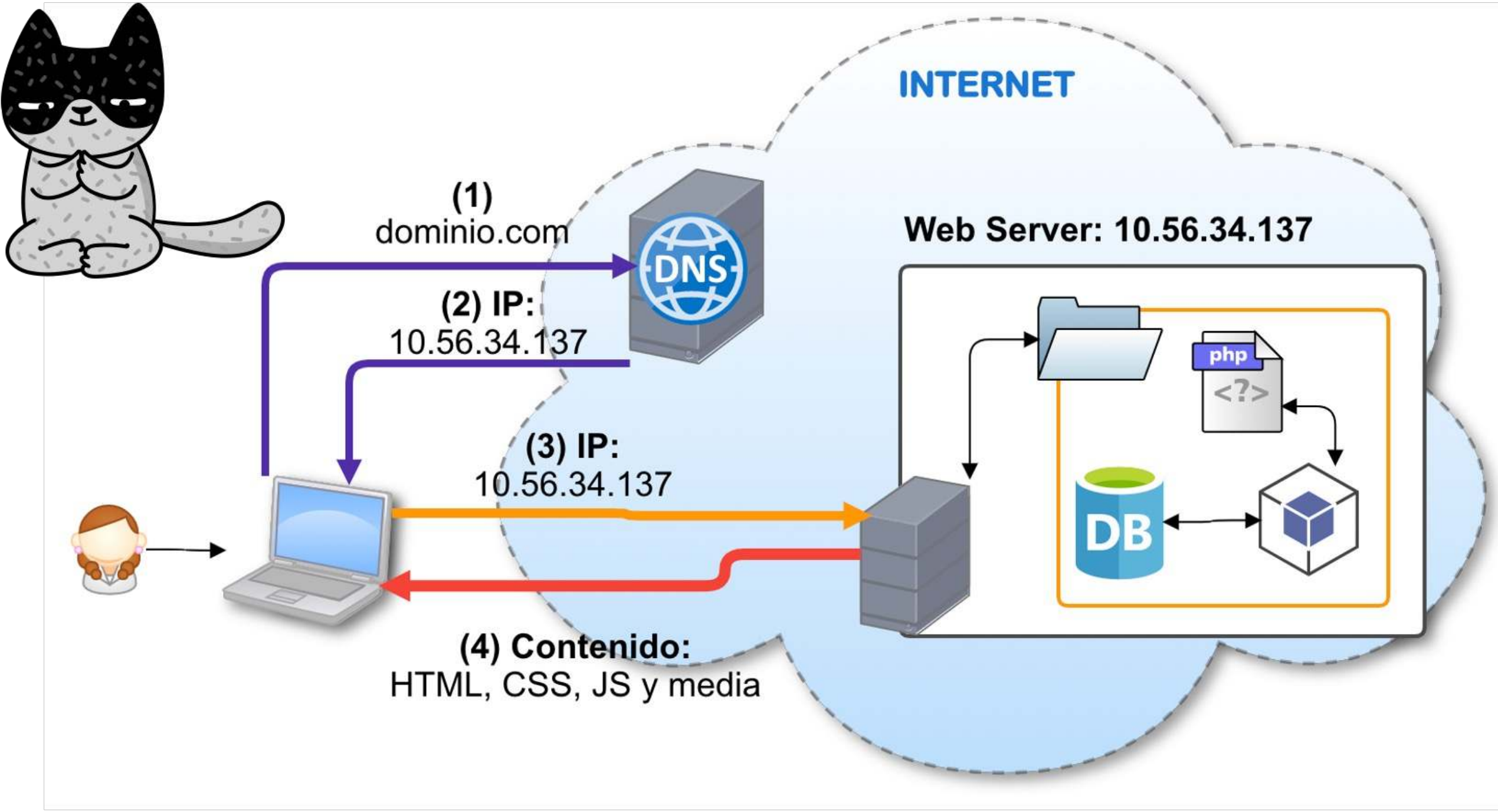
- Agent / C3
- Support & Backups

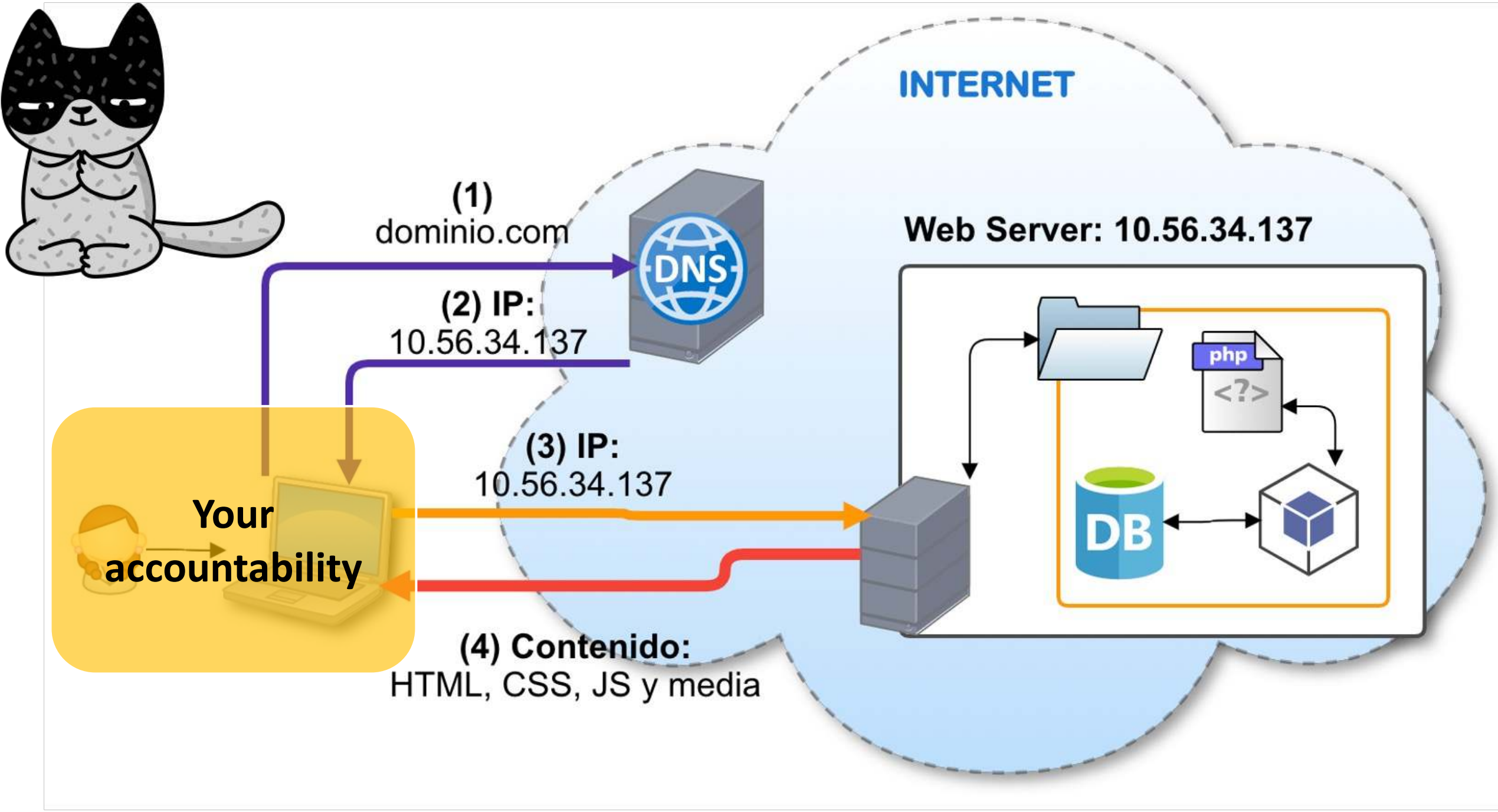
Security Expert

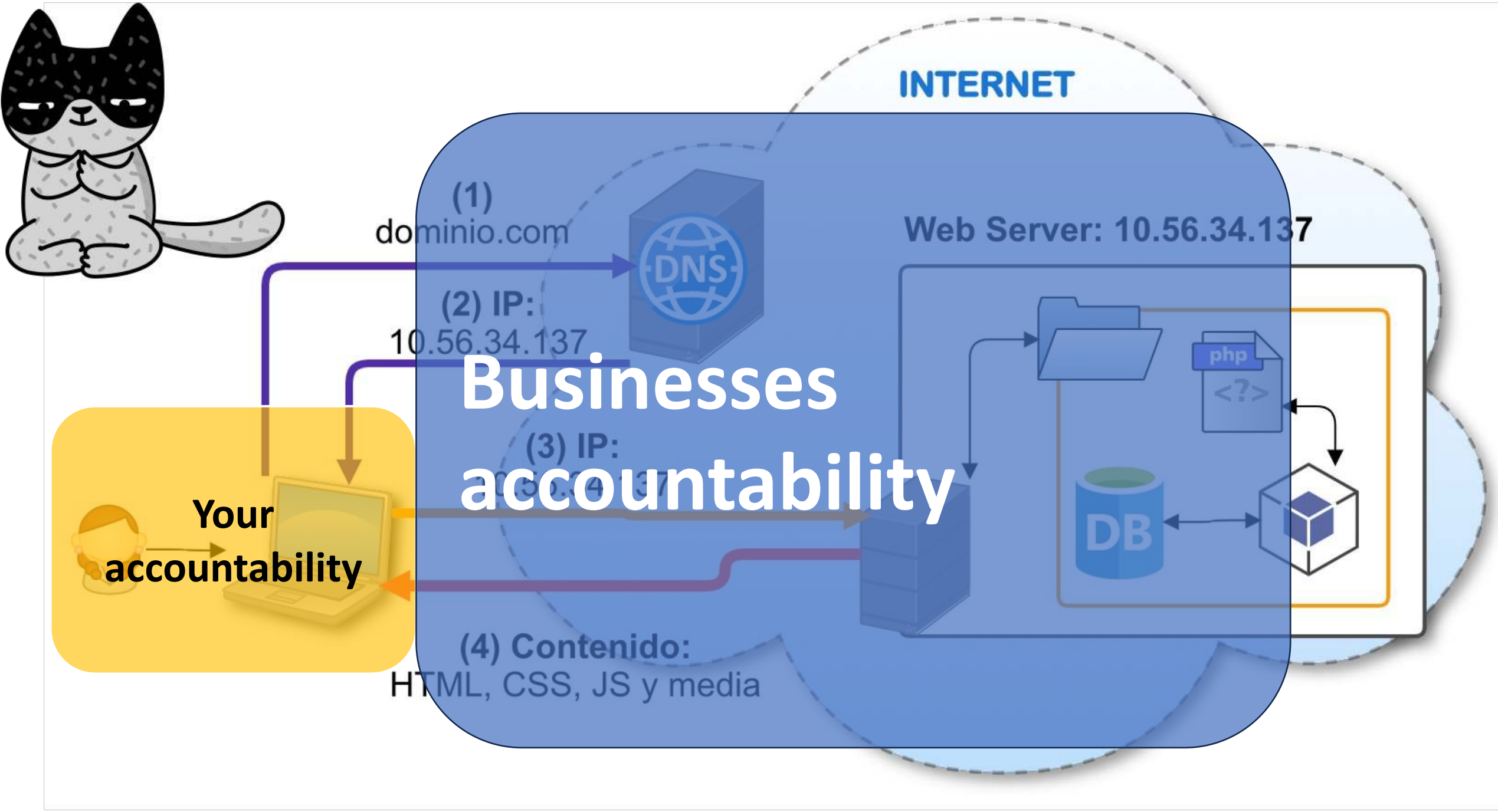
- Security department
- External services

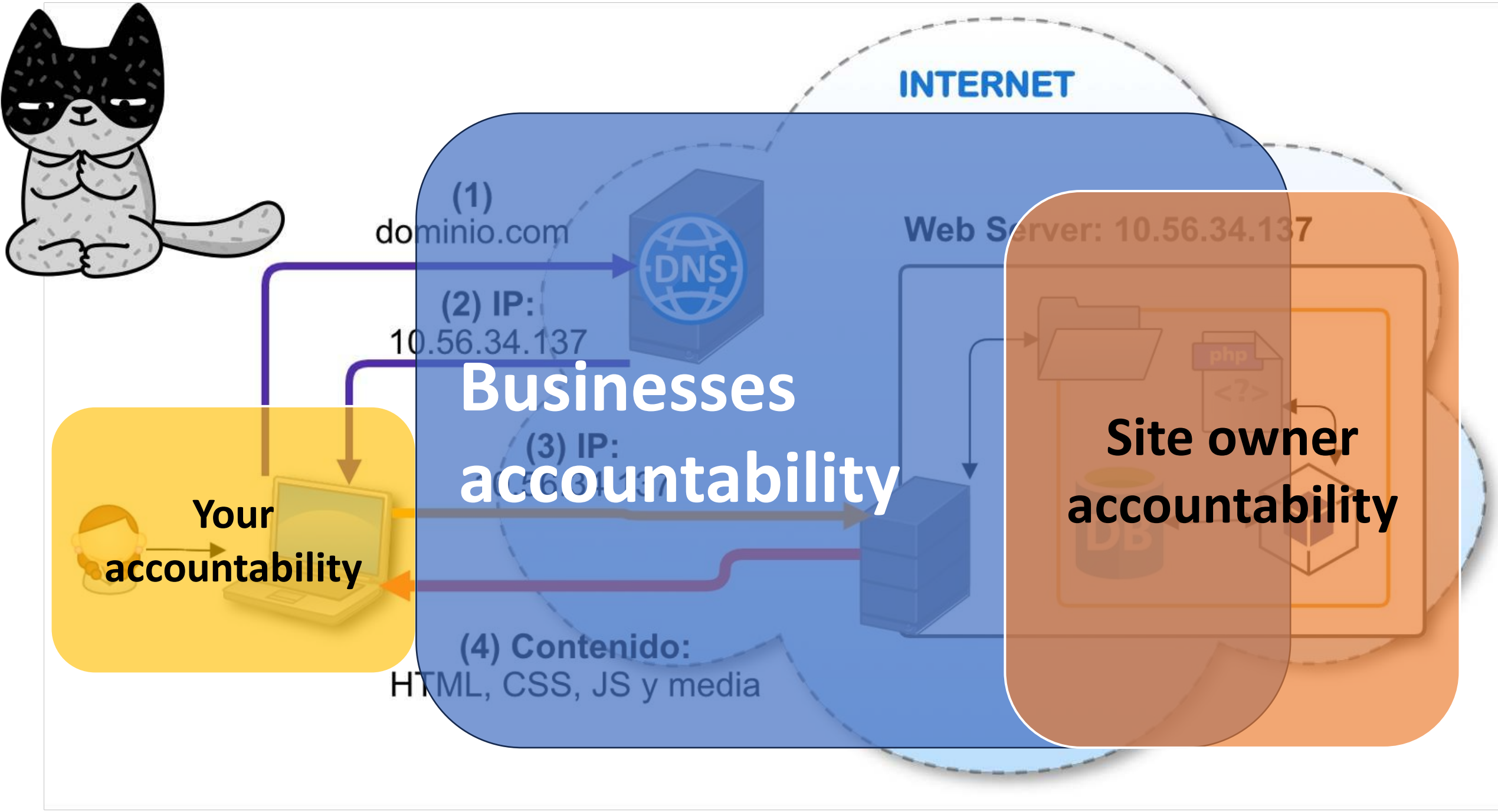
Agents involved (if something bad happens)




INTERNET
(1)
dominio.com
DNS
(2) IP:
10.56.34.137
Web Server: 10.56.34.137
php
<?>
DB
(3) IP:
10.56.34.137
(4) Contenido:
HTML, CSS, JS y media


INTERNET
(1)
dominio.com
DNS
(2) IP:
10.56.34.137
Web Server: 10.56.34.137
php
<?>
DB
(3) IP:
10.56.34.137
Your
accountability
(4) Contenido:
HTML, CSS, JS y media


INTERNET
(1)
dominio.com
DNS
(2) IP:
10.56.34.137
Web Server: 10.56.34.137
php
<?>
DB
(3) IP:
(4) Contenido:
HTML, CSS, JS y media
Your
accountability
Businesses
accountability


INTERNET
(1)
dominio.com
DNS
(2) IP:
10.56.34.137
Businesses
accountability
(3) IP:
Web Server: 10.56.34.137
Your
accountability
Site owner
accountability
(4) Contenido:
HTML, CSS, JS y media

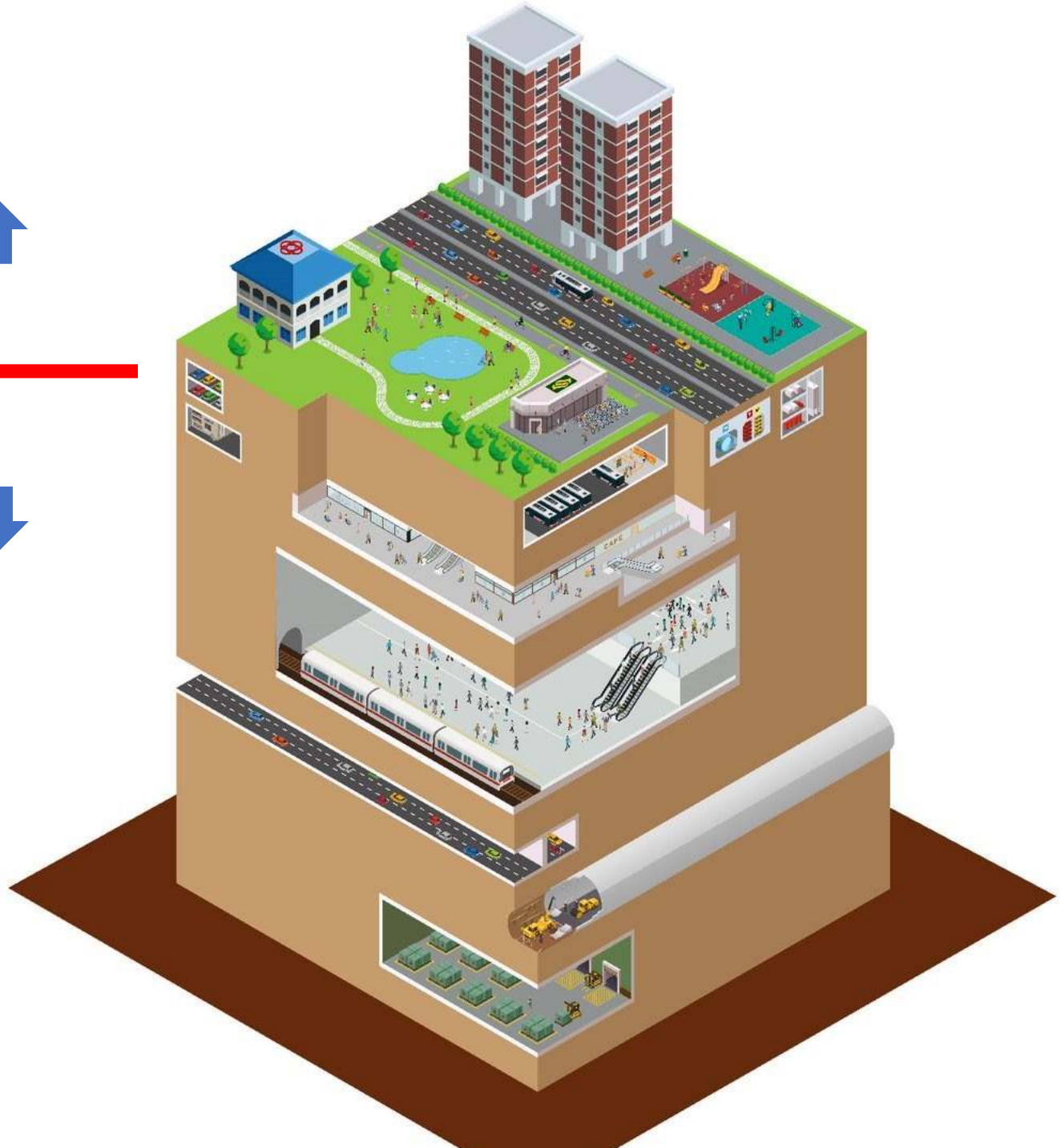
Site Owner

- App
- Data
- Security of the site

Hosting provider

- Networks
- Hardware
- SO
- Virtualization
- Security

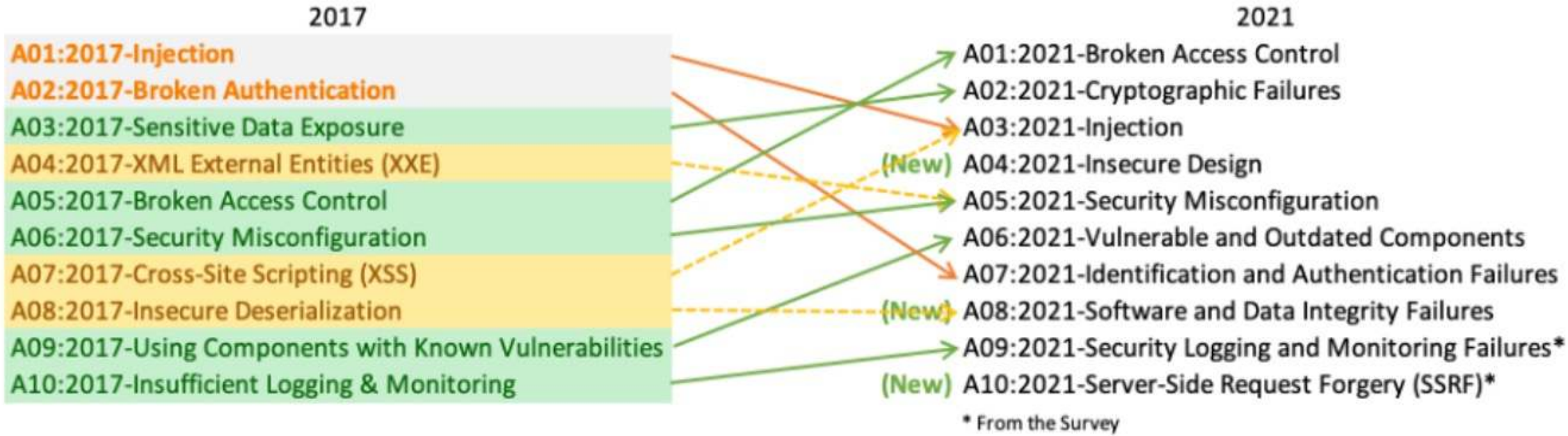
Security Liability



OWASP
Open Web Application Security Project

Top 10 Web Application Security Risks

There are three new categories, four categories with naming and scoping changes, and some consolidation in the Top 10 for 2021.



Targets in a WordPress site

Users

Database

Content

Infrastructure

Payments

Reputation

Measures:

REACTIVE

When bad things have **already happened**

Pain mitigation

INCIDENT RESPONSE

PROACTIVE

Before anything bad happens

Risk mitigation

ANALYSIS & MONITORING

Secondly, the **Incident Response**

Incident response (IR) is **the effort to quickly identify an attack, minimize its effects, contain damage**, and remediate the cause to reduce the risk of future incidents.

(vmware.com)

Reactive measures (AKA Incident Response)

1) SCAN your site

Front-end status: **sitecheck.sucuri.net**

Free tier in-site scanner: iThemes, etc.
Best: External malware scanner

2) UPDATE

EVERYTHING
Including server software

3) CRC: Check, Remove and Change

Admins, plugins, themes, Passwords …

- webpagetest.org

OR Restore a **BACKUP** & back to (1)

Possible loss of information

Possible re-installation of malware

(FIRST) **SCAN** your site

Let's try to figure out **WHAT** happened

FrontEnd Snapshot analysis: **sitecheck.sucuri.net**

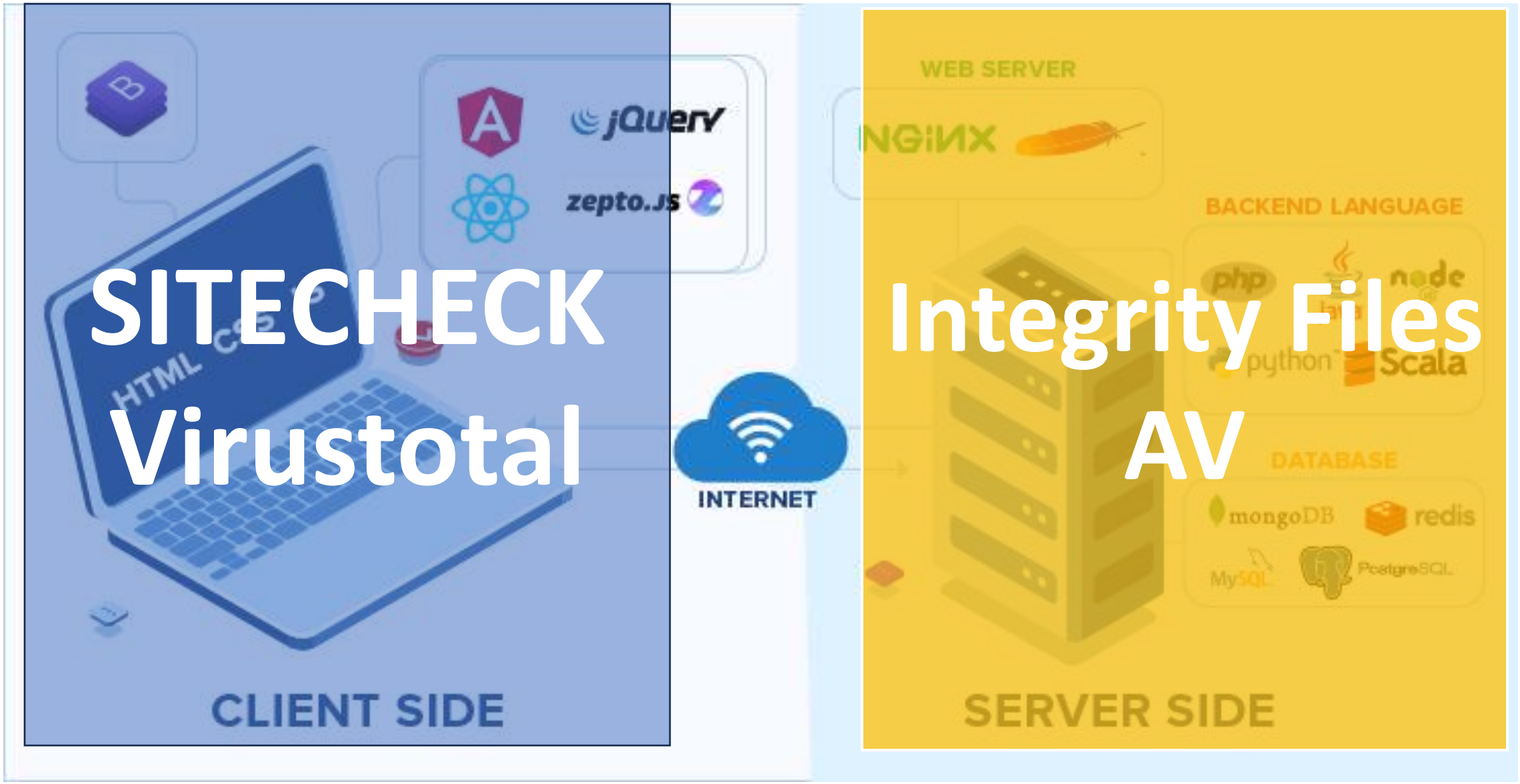
VIRUSTOTAL: What blocklists vendors see.

Any free tier plugin scanner as a first step (not really trustful) (e.g. iThemes)

BEST: use a server AV or an external malware scanner

Even BETTER: File integrity scanner (if activated BEFORE the hack).


WEB SERVER
NGINX
BACKEND LANGUAGE
php
Java
node
python
Scala
DATABASE
mongoDB
redis
MySQL
PostgreSQL
jQuery
zepto.js
HTML CSS JS
INTERNET
CLIENT SIDE
SERVER SIDE


SITECHECK
Virustotal
Integrity Files
AV
jQuery
zepto.js
HTML
INTERNET
CLIENT SIDE
WEB SERVER
NGINX
BACKEND LANGUAGE
php
node
python
Scala
DATABASE
mongoDB
redis
MySQL
PostgreSQL
SERVER SIDE

Warning: Malware Detected

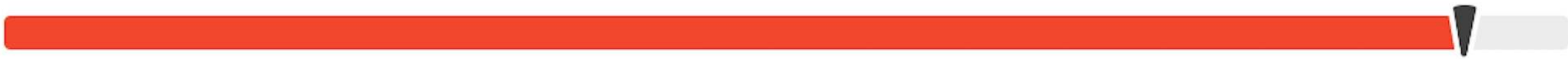
Infected with malware. Immediate action is required

Request Cleanup

58
URLs Scanned

Pages scanned: 37
Javascript files scanned: 21
Other files: 0

System running on: LiteSpeed, Powered by: PHP/5.4.45
IP address:
More Details



Low | Medium | **Critical Security Risk**

Malware Found

http://www. wp-includes/js/jquery/jquery.js?ver=1.12.4 (More details)

Definition

rogueads.unwanted_ads?9.5

Malware Found

http://www. /wp-includes/js/jquery/jquery-migrate.min.js?ver=1.4.1 (More details)

Definition

rogueads.unwanted_ads?9.5

Website File Changes Monitor

Added Files | Modified Files | Deleted Files

Added Files

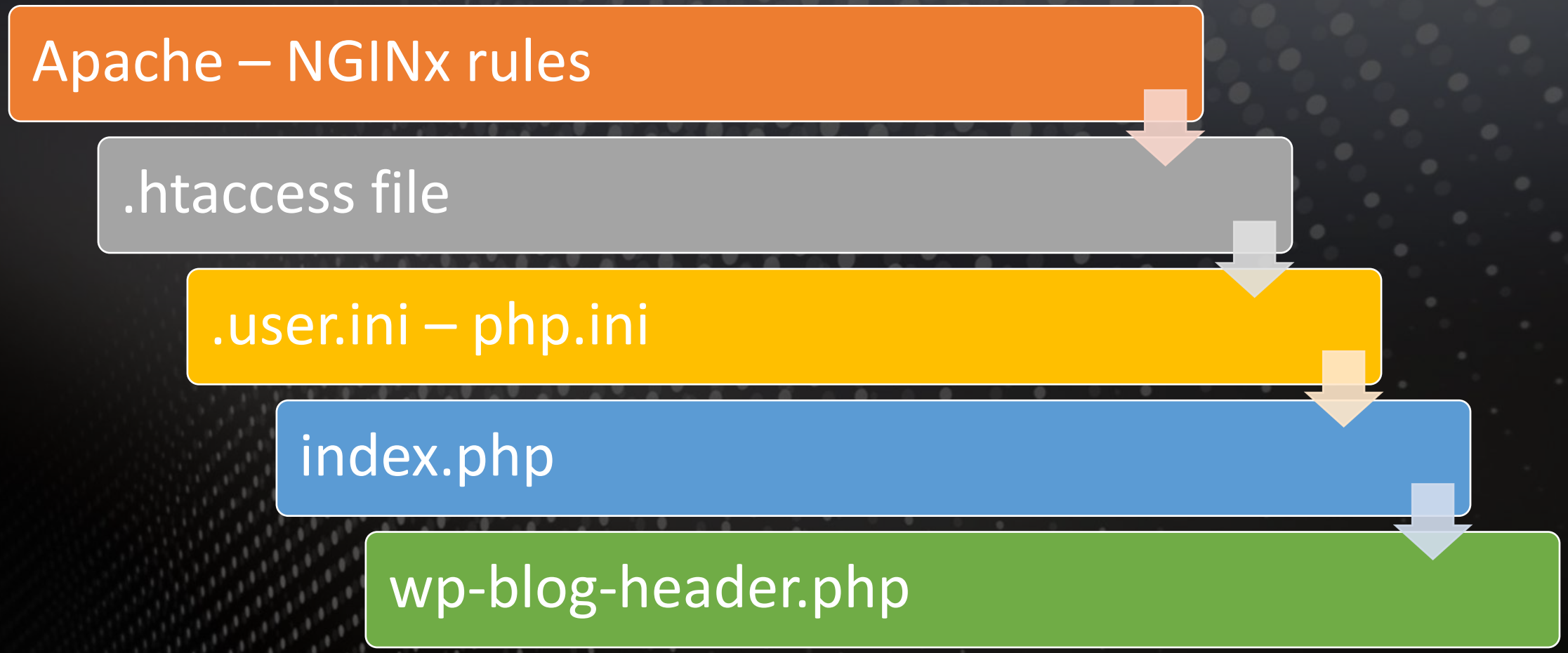
Bulk Actions ▾ Apply Scan Now Last scan: September 3, 2019 4:44 am

Path	Name	Type	Date	Mark as Rea
/var/www/www.wpwhitesecurity.net/public_html/wp-content/new_xfolder/xfiles	fake_page.php	File	09-03-2019 4:44:59	✓
/var/www/www.wpwhitesecurity.net/public_html/wp-content/new_xfolder/xfiles	login.php	File	09-03-2019 4:44:59	✓
/var/www/www.wpwhitesecurity.net/public_html/wp-content/new_xfolder/xfiles	cron_run.exe	File	09-03-2019 4:44:59	✓
/var/www/www.wpwhitesecurity.net/public_html/wp-content/new_xfolder/xfiles	index.php	File	09-03-2019 4:44:59	✓
/var/www/www.wpwhitesecurity.net/public_html/wp-content/new_xfolder/xfiles	report.html.php	File	09-03-2019 4:44:59	✓
/var/www/www.wpwhitesecurity.net/public_html/wp-content/themes	log-lolla	Theme Install	09-03-2019 4:44:59	✓
/var/www/www.wpwhitesecurity.net/public_html/wp-content/themes	bazzinga	Theme Install	09-03-2019 4:44:59	✓
/var/www/www.wpwhitesecurity.net/public_html/wp-content/themes	joint	Theme Install	09-03-2019 4:44:59	✓
/var/www/www.wpwhitesecurity.net/public_html/wp-content/plugins	wp-security-audit-log	Plugin Install	09-03-2019 4:44:59	✓
/var/www/www.wpwhitesecurity.net/public_html/wp-content/plugins	password-policy-manager-master	Plugin Install	09-03-2019 4:44:59	✓

Example of Fake Plugins/Themes

wp-content/plugins	wp-content/themes
• wp-lazyload-{random chars} • task-controller • core-stab / core-engine • wp-zip • plugins	• seotheme • classic • themes

WordPress Execution order:



(SECOND) **UPDATE**

UPDATE ALL, including plugins, themes and WordPress itself.

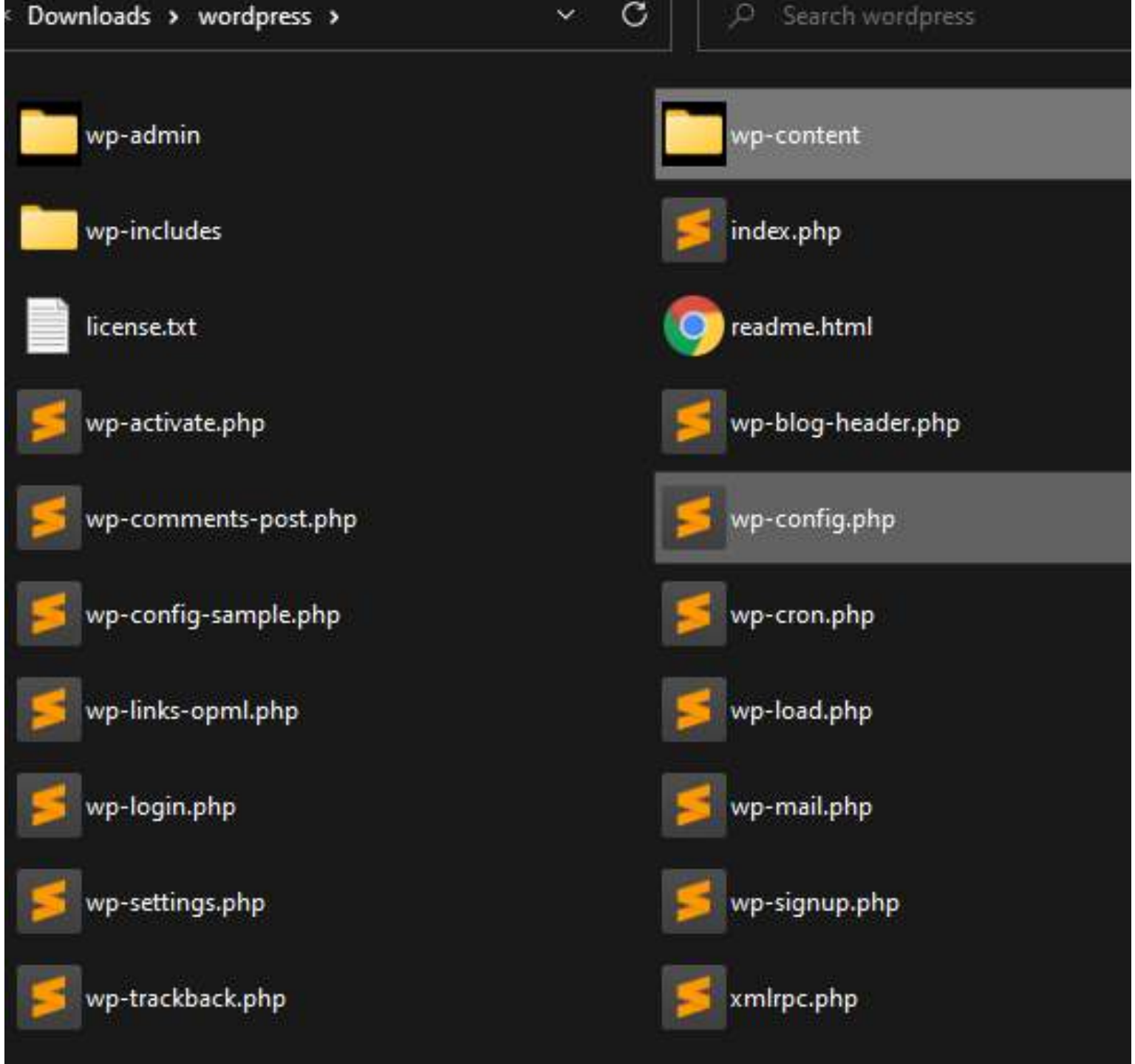
This patches security vulnerabilities, working towards avoid re-infection.

ALSO, this action **overwrites compromised/corrupted code** with trustworthy code from official repositories.

UPDATE

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

SECRET!


Downloads › wordpress ›
Search wordpress
wp-admin
wp-content
wp-includes
index.php
license.txt
readme.html
wp-activate.php
wp-blog-header.php
wp-comments-post.php
wp-config.php
wp-config-sample.php
wp-cron.php
wp-links-opml.php
wp-load.php
wp-login.php
wp-mail.php
wp-settings.php
wp-signup.php
wp-trackback.php
xmlrpc.php

(THIRD) **CRC**:
Check, remove and change

Check and Remove

- Unneeded admin users
- Plugins and themes which are strictly not in use
- Outdated backups
- DEV/TEST sites in your production server

Change Passwords

- Connections (cPanel, FTP, SSH, …)
- Database (remember to update your **wp-config.php**)
- Dashboard (**wp-admin**)
- Hosting provider

Atención: Se perderá cualquier personalización que hayas hecho a los archivos del

Actualizar temas

Seleccionar todos

Twenty Fifteen
Tienes la versión 2.5. Actualiza a la 2.6.

Twenty Fourteen
Tienes la versión 2.7. Actualiza a la 2.8.

Twenty Nineteen
Tienes la versión 1.4. Actualiza a la 1.5.

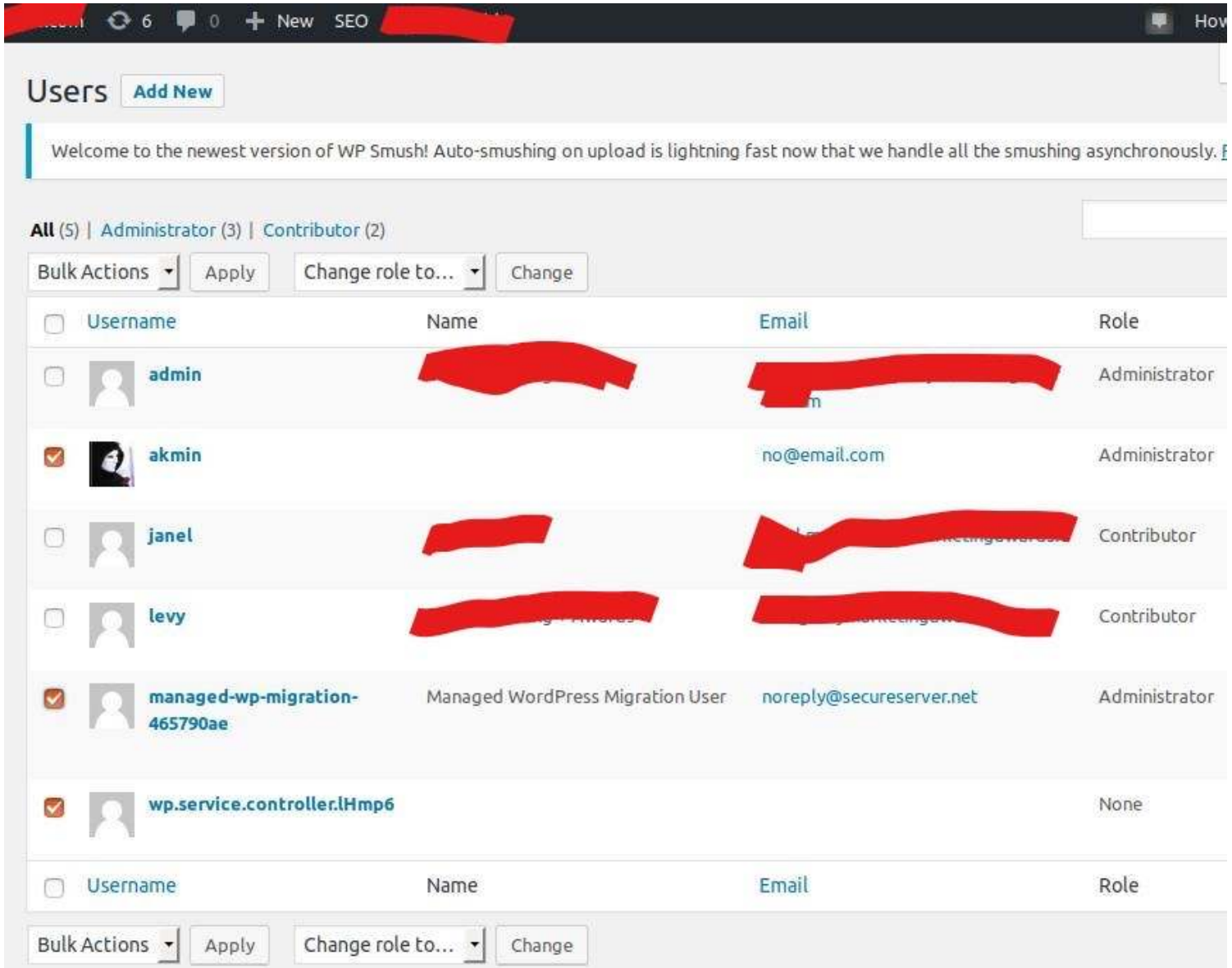
Twenty Seventeen
Tienes la versión 2.2. Actualiza a la 2.3.

Twenty Thirteen
Tienes la versión 2.9. Actualiza a la 3.0.

Twenty Twenty
Tienes la versión 1.1. Actualiza a la 1.2.

Seleccionar todos

Actualizar temas



(LAST OPTION) Restore a **BACKUP**

- You can lose information
- We don’t always know when the infection begun


PALLIS O'CONNOR Presents
BACK TO THE FUTURE
TRILOGY
THE GREATEST TRILOGY...
EVER MADE...

TIPS: BACKUPS

Have a backups **strategy**

NEVER store the backups in your **production server**

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

TIPS: BACKUPS

Have a backups **strategy**

r

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

REMEMBER: Reactive measures

1) SCAN your site

Front-end status: **sitecheck.sucuri.net**

Free tier in-site scanner: iThemes, etc.
Best: External malware scanner

2) UPDATE

EVERYTHING
Including server software

3) CRC: Check, Remove and Change

Admins, plugins, themes, Passwords …

- webpagetest.org

OR Restore a **BACKUP** & back to (1)

Possible loss of information

Possible re-installation of malware

Then, the **Reputation**

Bots, Search Engines and Blocklists

INTERNET IS CONSTANTLY BEING CRAWLED BY **BOTS**

SEARCH ENGINES AND SECURITY VENDORS HAVE **BLOCKLISTS**

BLOCKLISTS -> REPUTATION

THE MORE FAMOUS THE BLOCKLIST THE MORE WIDELY ACCEPTED.

Some Facts

This is not an immediate process

- Inclusion takes time
- Delist takes time

Normally, there isn’t any info about **why**

SNS block or warn about posts

Ads companies block/hold campaigns

Search Engines remove your site from SERPs

- Some of them remove completely your SEO rank

One (important) thing more …

According to some Data Protection laws it might be **mandatory to report any personal data breach to supervisory authorities**.

In the case of **affecting any European citizen**, the **GDPR gives 72h** after the breach is detected to report about it.

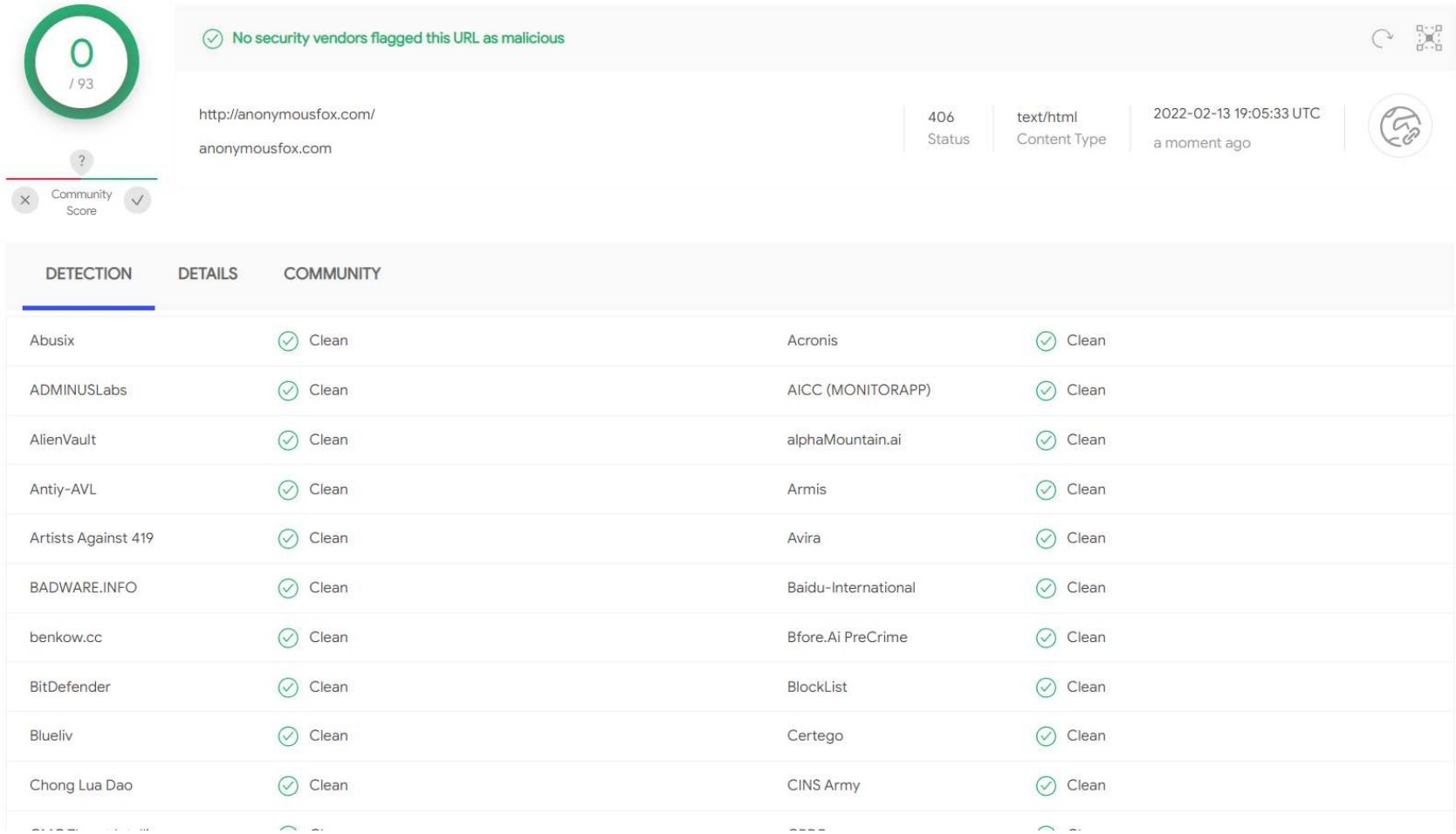
Check the applicable law, depending on the country you are operating from and the nationality of the affected person.

Troubleshooting

1. **ONCE THE SITE IS CLEAN**, check blocklists:

   Virustotal.com

2. **Submit** for reconsideration to all the blocklists vendors **individually**



Post-Mortem report

It is **hard**, requires **forensic** services and **exposes** your management

A report of **what happened**, after a successfully hacking attempt

- How and when it happened
- How and when it was discovered
- What did you do to mitigate the situation and to recover the normal situation
- Lessons learnt

Helps to **learn** for future situations

Helps to recover **user's trust**

Shows your company as **transparency advocated**

Lastly, **never again**!

Proactive measures

Reduce admins, plugins and themes (LEAST PRIVILEGE RULE)

Use Passwords Manager, change periodically, 2FA, strong ones

Backups (VALIDATE THEM!)

Updates (REMEMBER: PATCHES COMES AFTER EXPLOITS)

Monitor your site (Patchstack, Sitecheck & files integrity scanner)

WAF (Web Application Firewall)

Remember to **Invest** in

HOSTING

SECURITY


Everybody needs a hacker

WORDCAMP FINLAND 2023

KIITOS!!

Kysymyksiä?
QUESTIONS?