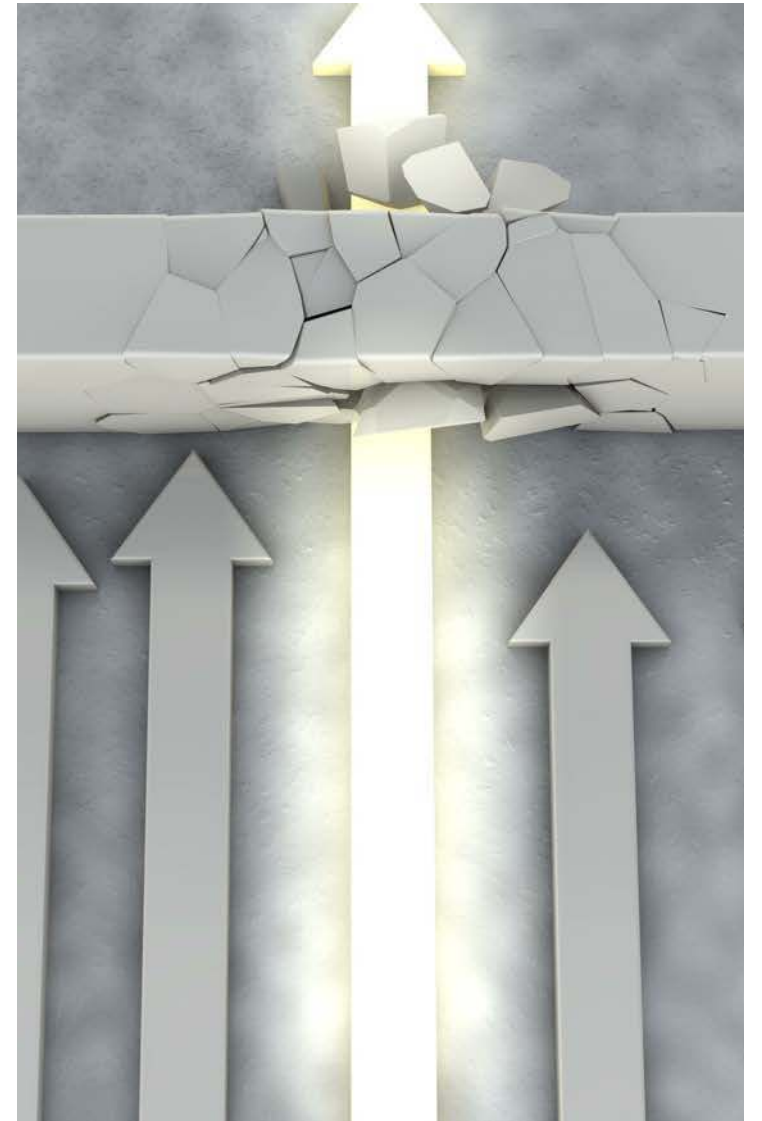




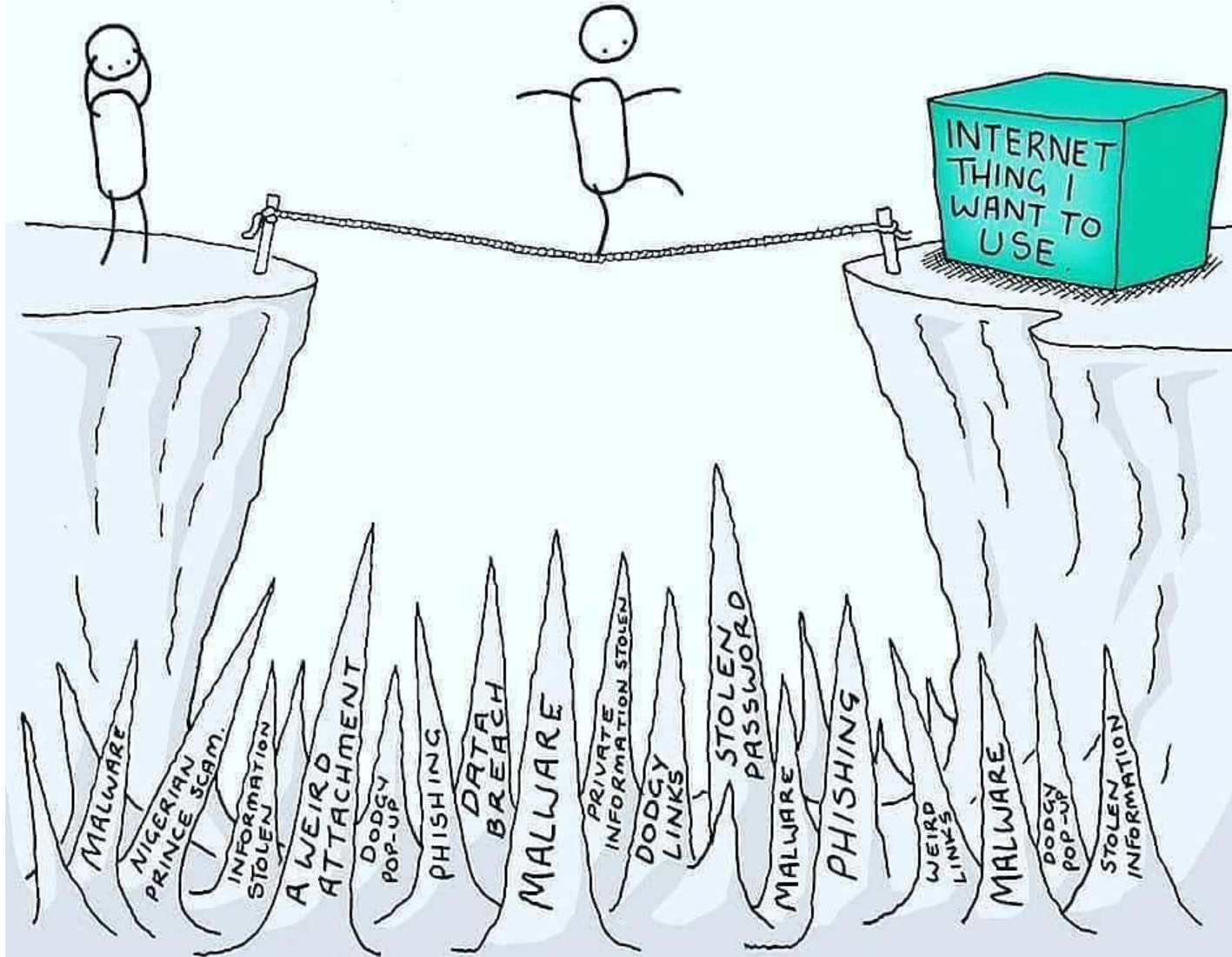
Hacking WordPress

... and countermeasures

Nestor Angulo (@pharar) - WordCamp Vienna 2020



DEALING WITH CYBER STRESS



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.

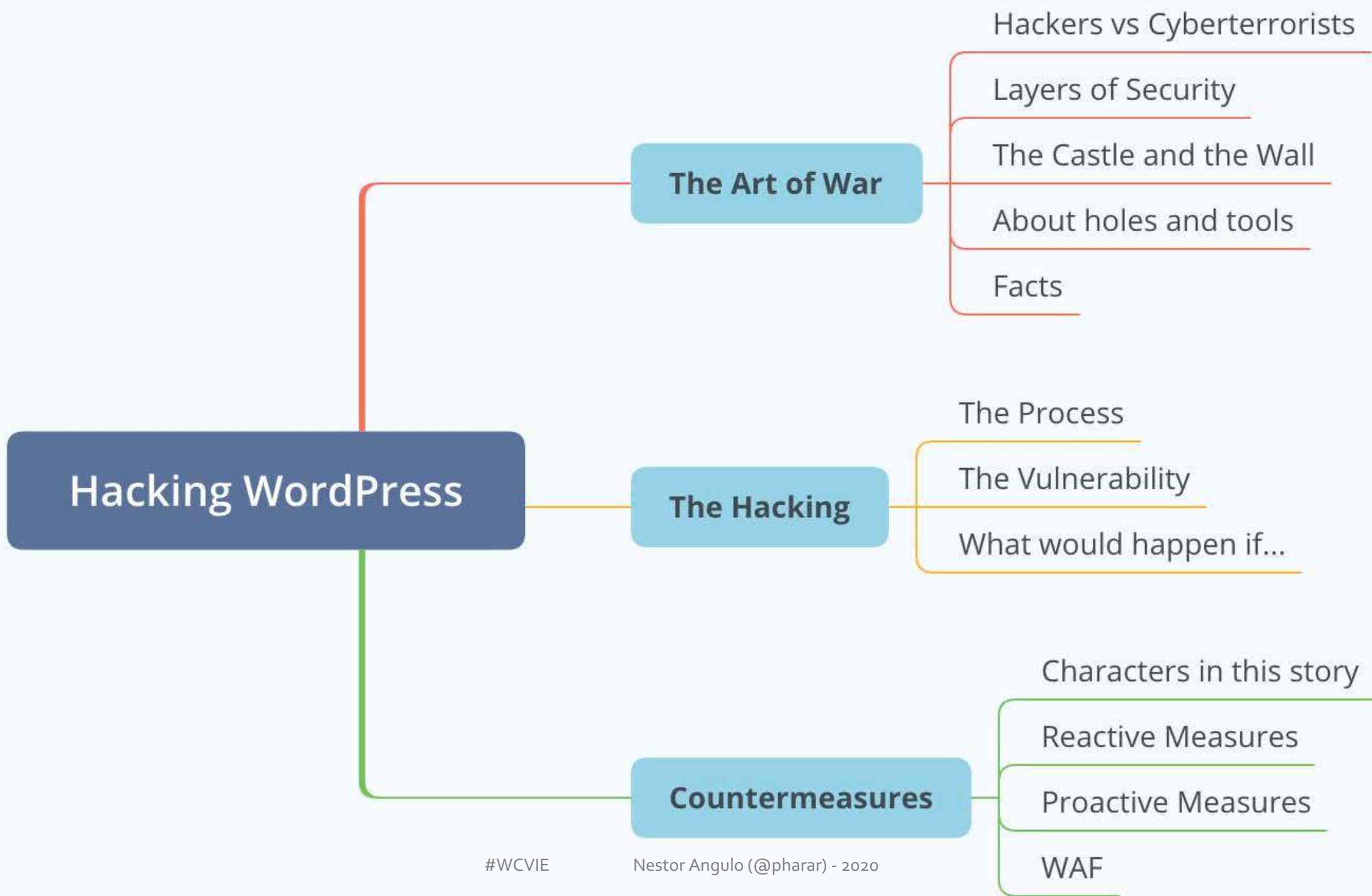


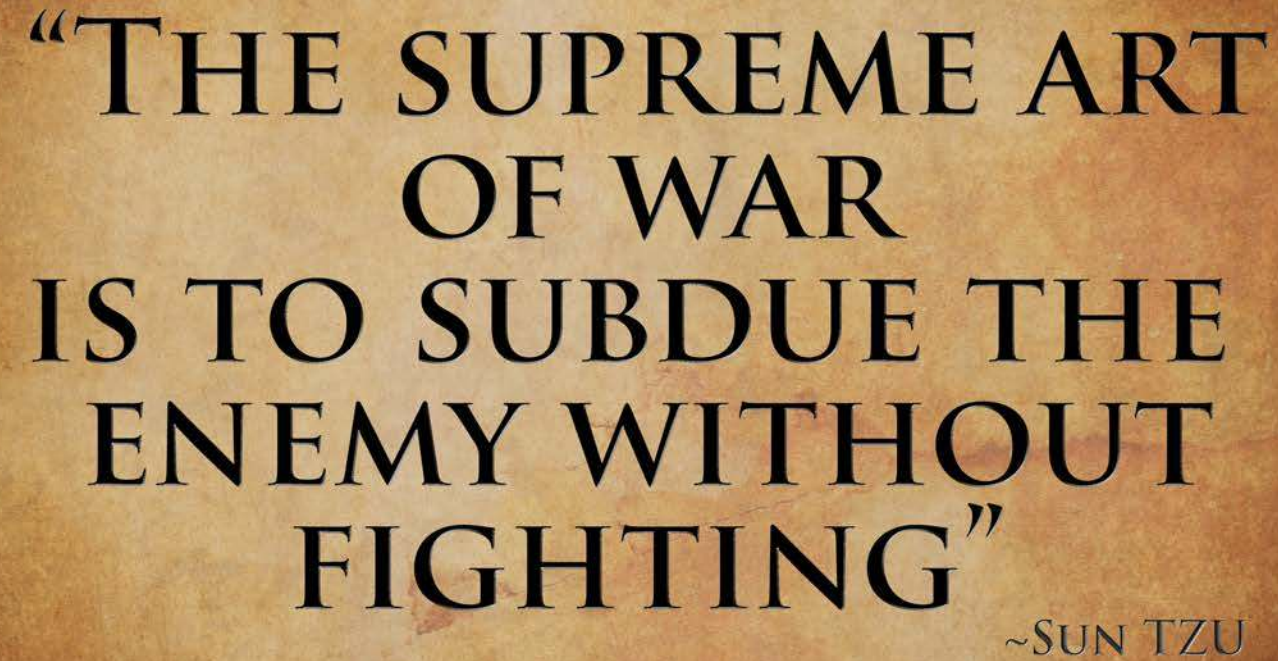
This talk is intended to be DIDACTIC. I don't promote any hacking attempt with illegal intentions. Always ask to an expert if you have questions.

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

John Chambers
Chief Executive Officer of Cisco





The image features a central parchment-like background with a textured, aged appearance. The text is written in a bold, black, serif font. The quote is enclosed in large quotation marks. The background is framed by vertical borders on both sides, consisting of a grid of thin black lines over a light-colored, textured background that resembles bamboo or reeds.

“THE SUPREME ART
OF WAR
IS TO SUBDUE THE
ENEMY WITHOUT
FIGHTING”
~SUN TZU

The Art of War

The Art of War

Chinese treatise about military strategies and tactics, by Sun Tzu (5th 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 attackers

... 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



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 possibility 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.



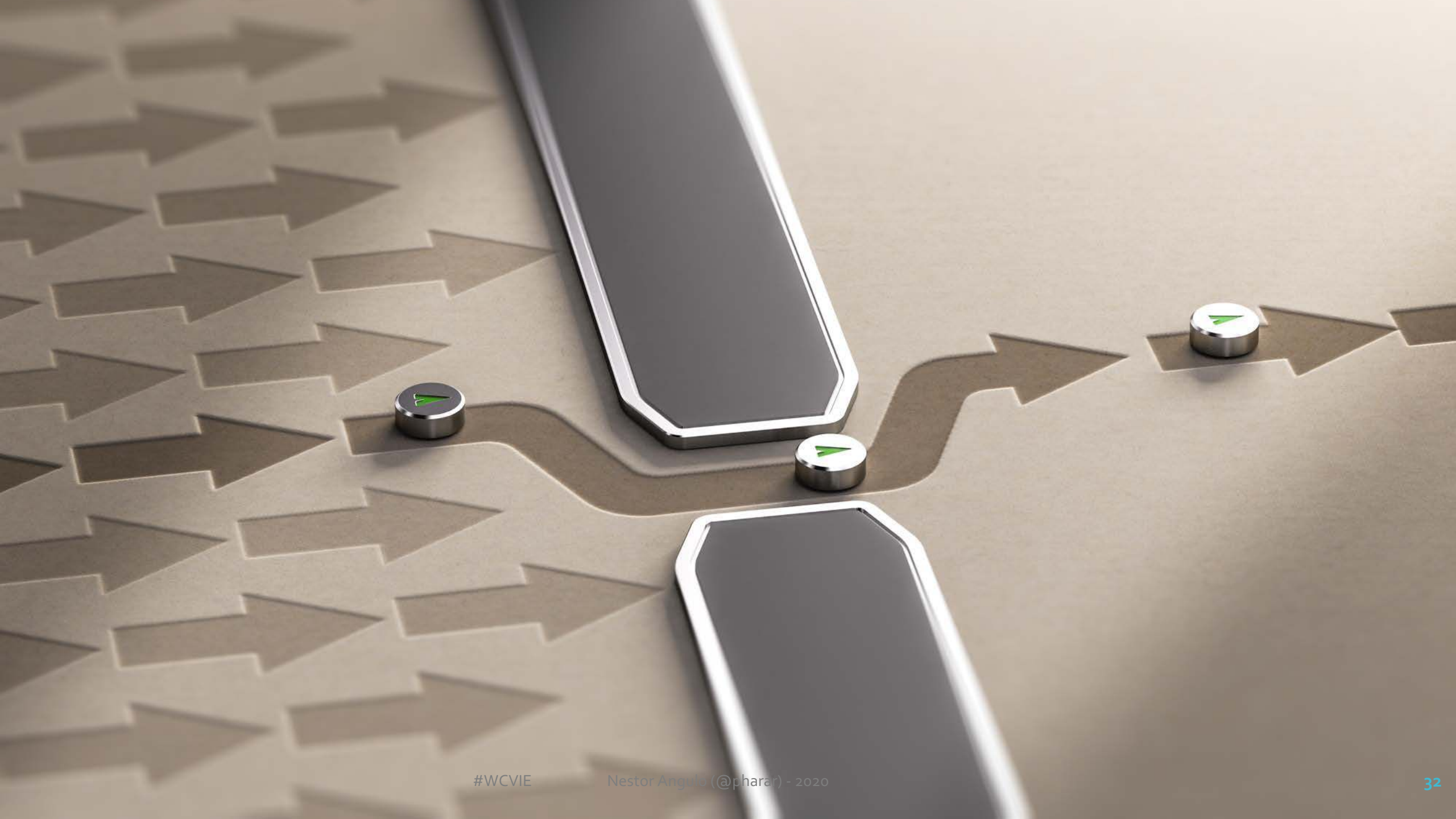
The problem is that...
... is **extremely easy** to create
an **insecure site** with **WordPress**



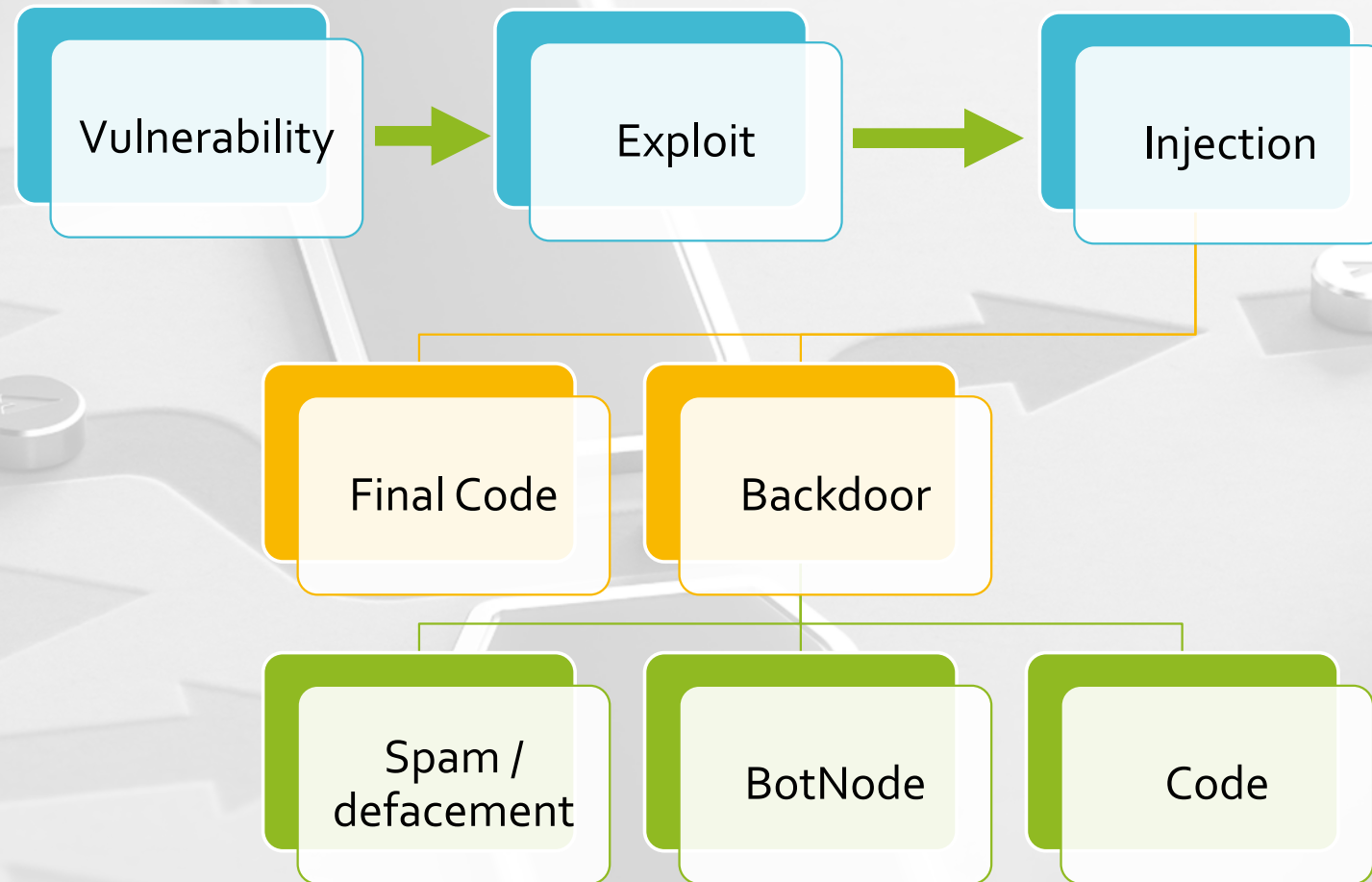
```
button.Constructor=t,e.fn.button.noConflict=function(){return e.fn.button=n,this},e(document).on("click.button.data-ap
"[data-toggle^=button]",function(t){var n=e(t.target);n.hasClass("btn")||(n=n.closest(".btn")),n.button("toggle")})(w
,!function(e){"use strict";var t=function(t,n){this.$element=e(t),this.$indicators=this.$element.find(".carousel-indica
.options=n,this.options.pause=="hover"&&this.$element.on("mouseenter",e.proxy(this.pause,this)).on("mouseleave",e.proxy
this))};t.prototype={cycle:function(t){return t||(this.paused=!1),this.interval&&clearInterval(this.interval),this.opti
.interval&&!this.paused&&(this.interval=setInterval(e.proxy(this.next,this),this.options.interval)),this},getActiveInd
{return this.$active=this.$element.find(".item.active"),this.$items=this.$active.parent().children(),this.$items.index
.$active)},to:function(t){var n=this.getActiveIndex(),r=this;if(t>this.$items.length-1||t<0)return;return this.sliding
.$element.one("slid",function(){r.to(t)}):n==t?this.pause().cycle():this.slide(t>n?"next":"prev",e(this.$items[t])),pa
(t){return t||(this.paused=!0),this.$element.find(".next, .prev").length&&e.support.transition.end&&(this.$element.trig
.support.transition.end),this.cycle(!0)),clearInterval(this.interval),this.interval=null,this},next:function(){if(this
return;return this.slide("next")},prev:function(){if(this.sliding)return;return this.slide("prev")},slide:function(t,n
r=this.$element.find(".item.active"),i=n||r[t](),s=this.interval,o=t=="next"?"left":"right",u=t=="next"?"first":"last",
this.sliding=!0,s&&this.pause(),i=i.length?i:this.$element.find(".item")[u](),f=e.Event("slide",{relatedTarget:i[0],di
if(i.hasClass("active"))return;this.$indicators.length&&(this.$indicators.find(".active").removeClass("active"),this.$
("slid",function(){var t=e(a.$indicators.children()[a.getActiveIndex()]);t&&t.addClass("active")}));if(e.support.trans
.$element.hasClass("slide")){this.$element.trigger(f);if(f.isDefaultPrevented())return;i.addClass(t),i[0].offsetWidth,
i.addClass(o),this.$element.one(e.support.transition.end,function(){i.removeClass([t,o].join(" ")).addClass("active")
.removeClass(["active",o].join(" ")),a.sliding=!1,setTimeout(function(){a.$element.trigger("slid")},0)}})else{this.$ele
(f);if(f.isDefaultPrevented())return;r.removeClass("active"),i.addClass("active"),this.sliding=!1,this.$element.trigger
}return s&&this.$element.trigger(f)},e.fn.carousel=function(n){return this.each(function(){var r=e(this)
("carousel"),r=e.extend({},e.fn.carousel.defaults,typeof n=="object"&&n),o=typeof n=="string"?n:s.slide;i||r.data("caro
t(this,s)),typeof n=="number"?i.to(n):o?i[o]():s.interval&&i.pause().cycle()}}),e.fn.carousel.defaults={interval:5e3,
pause:"hover"},e.fn.carousel.Constructor=t,e.fn.carousel.noConflict=function(){return e.fn.carousel=n,this},e(document)
.carousel.data("carousel"),[data-slide], [data-slide-to]",function(t){var n=e(this),r,i=e(n.attr("data-target"))||(r=n.attr("
.replace(/.*(?=#[^\s]+)$/,""),s=e.extend({},i.data(),n.data()),o;i.carousel(s),(o=n.attr("data-slide-to"))&&i.data("ca
.pause().to(o).cycle(),t.preventDefault()}})(window.jQuery),!function(e){"use strict";var t=function(t,n){this.$element
.options=e.extend({},e.fn.collapse.defaults,n),this.options.parent&&(this.$parent=e(this.options.parent)),this.options
.toggle()};t.prototype={constructor:t,dimension:function(){var e=this.$element.hasClass("width");return e?"width":"heig
show:function(){var t,n,r,i;if(this.transitioning||this.$element.hasClass("in"))return;t=this.dimension(),n=e.camelCase
t].join("-")),r=this.$parent&&this.$parent.find("> .accordion-group > .in");if(r&&r.length){i=r.data("collapse");if(i&
.transitioning)return;r.collapse("hide"),i||r.data("collapse",null)}this.$element[t](0),this.transition("addClass",e.Ev
"shown"),e.support.transition&&this.$element[t](this.$element[0][n])},hide:function(){var t;if(this.transitioning||!th
.hasClass("in"))return;t=this.dimension(),this.reset(this.$element[t]()),this.transition("removeClass",e.Event("hide"),
this.$element[t](0)),reset:function(e){var t=this.dimension();return this.$element.removeClass("collapse")[t](e)||"auto"
this.$element[t](0)},reset:function(e){var t=this.dimension();return this.$element.removeClass("collapse")[t](e)||"auto"
this.$element[t](0)}
```

The Hacking

How it happens.



The Process





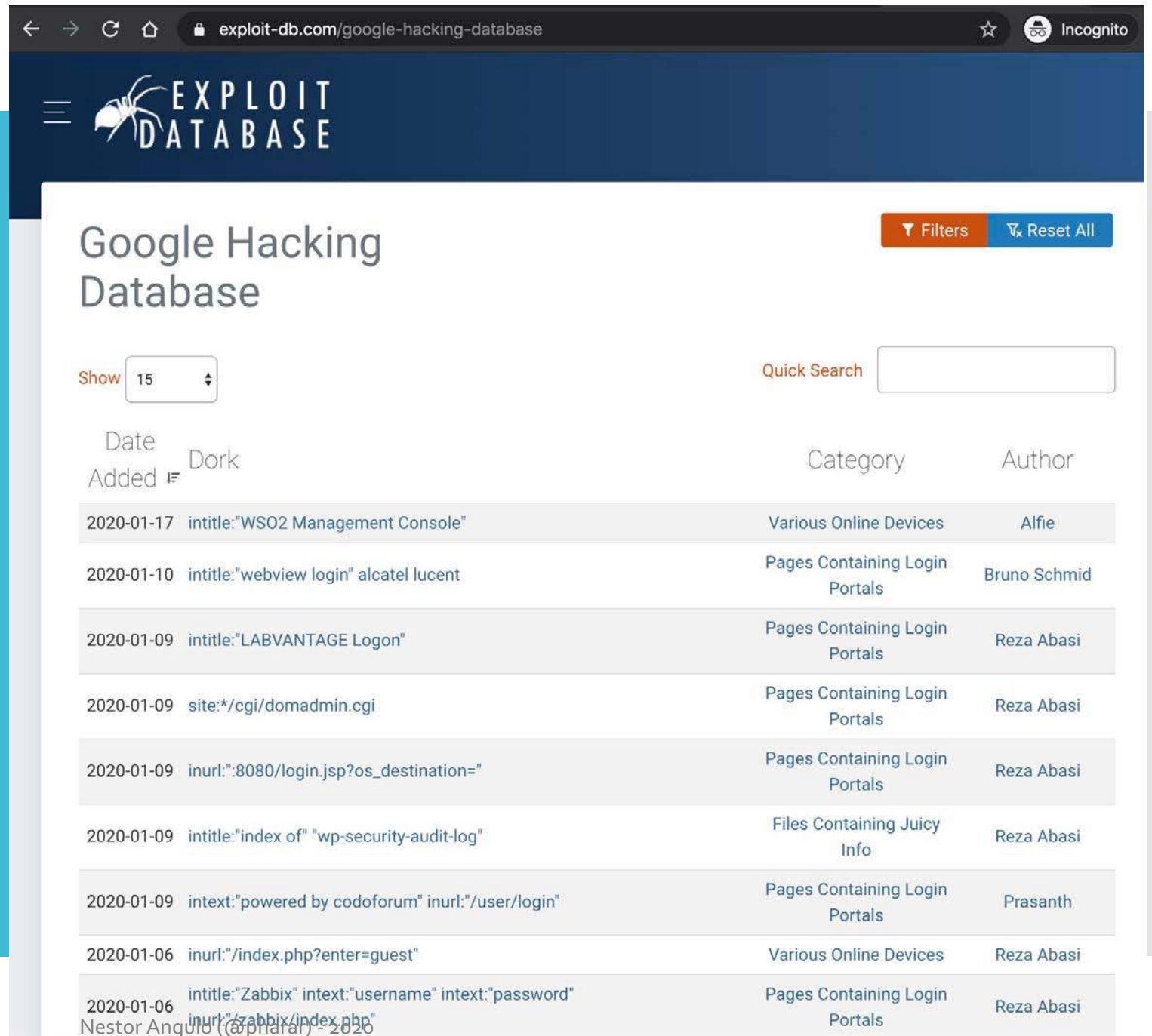


Searching the vulnerability

Google Hacking Database

[exploit-db.com/
google-hacking-
database](https://exploit-db.com/google-hacking-database)

#WCVIE



The screenshot shows the Exploit Database website interface. At the top, there is a navigation bar with the site logo and a search bar. Below the navigation bar, the main content area displays a list of search results. The results are organized into a table with columns for Date Added, Dork, Category, and Author. The table contains several entries, each with a date, a search query (dork), a category, and an author name.

Date Added	Dork	Category	Author
2020-01-17	intitle:"WSO2 Management Console"	Various Online Devices	Alfie
2020-01-10	intitle:"webview login" alcatel lucent	Pages Containing Login Portals	Bruno Schmid
2020-01-09	intitle:"LABVANTAGE Logon"	Pages Containing Login Portals	Reza Abasi
2020-01-09	site:*/cgi/domadmin.cgi	Pages Containing Login Portals	Reza Abasi
2020-01-09	inurl:":8080/login.jsp?os_destination="	Pages Containing Login Portals	Reza Abasi
2020-01-09	intitle:"index of" "wp-security-audit-log"	Files Containing Juicy Info	Reza Abasi
2020-01-09	intext:"powered by codoforum" inurl:"/user/login"	Pages Containing Login Portals	Prasanth
2020-01-06	inurl:"/index.php?enter=guest"	Various Online Devices	Reza Abasi
2020-01-06	intitle:"Zabbix" intext:"username" intext:"password" inurl:"zabbix/index.php"	Pages Containing Login Portals	Reza Abasi



WPSecurity Vulnerability Database wpvulndb.com

WPSecurity Vulnerability Database

Cataloging **16867** WordPress Core, Plugin and Theme vulnerabilities

Free Email Alerts

Submit a Vulnerability

Try our API

Latest WordPress Vulnerabilities

- 2019-10-14 [WordPress <= 5.2.3 - Admin Referrer Validation](#)
- 2019-10-14 [WordPress <= 5.2.3 - JSON Request Cache Poisoning](#)
- 2019-10-14 [WordPress <= 5.2.3 - Server-Side Request Forgery \(SSRF\) in URL Validation](#)
- 2019-10-14 [WordPress <= 5.2.3 - Stored XSS in Customizer](#)
- 2019-10-14 [WordPress <= 5.2.3 - Stored XSS in Style Tags](#)
- 2019-10-14 [WordPress <= 5.2.3 - Unauthenticated View Private/Draft Posts](#)
- 2019-09-05 [WordPress <= 5.2.2 - Cross-Site Scripting \(XSS\) in URL Sanitisation](#)

Latest Plugin Vulnerabilities

- 2019-11-26 [WP Spell Check <= 7.1.9 - Cross-Site Request Forgery \(CSRF\)](#)
- 2019-11-19 [Jetpack 5.1-7.9 - Vulnerability in Shortcode Embed Code](#)
- 2019-11-19 [WP Maintenance <= 5.0.5 - Cross-Site Request Forgery to Stored Cross-Site Scr...](#)
- 2019-11-17 [Sassy Social Share <= 3.3.3 - Cross-Site Scripting \(XSS\)](#)
- 2019-11-16 [WP Social < 5.9.0 - Cross-Site Scripting Issue](#)
- 2019-11-16 [Email Subscribers & Newsletter v1.0.0 - Multiple Issues](#)



Ex1: Using Google Hacking DB

github.com › WOWHoneyPot › blob › master › art ▼ Traducir esta página

WOWHoneyPot/wp-config.txt at master · morihisa ... - GitHub

<?php. /**. * **The** base configuration for **WordPress**. *. * **The** wp-config.php creation script uses this file during **the**. * installation. You don't have to use **the** web ...

www. [redacted] › wp-content › uploads › 2018/07 › wp-config-... ▼

wp-config-backup

You don't have to use **the** web site, you can just copy this file * to "wp-config.php" and fill in **the** values. * * @package **WordPress** */ // ** Ajustes solicitado ...

[redacted] › dup-wp-config-arc__3266a... ▼ Traducir esta página

<?php /** Enable W3 Total Cache */ define('WP_CACHE ...

This file has **the** following configurations: MySQL settings, Table Prefix, * Secret Keys, **WordPress** Language, and ABSPATH. You can find more information * by ...

[redacted] › wp-config ▼ Traducir esta página

<?php /** Enable W3 Total Cache */ define('WP_CACHE', true ...

This file has **the** following configurations: MySQL settings, Table Prefix, * Secret Keys, **WordPress** Language, and ABSPATH. You can find more information by ...

www. [redacted] › cms › wordpress › wp-c... ▼ Traducir esta página

<?php /** * wp-config.php - the James Canonical Version ...

Ex1: Using Google Hacking DB

```
<?php
/**
 * Configuración básica de WordPress.
 *
 * Este archivo contiene las siguientes configuraciones: ajustes de MySQL, prefijo de tablas,
 * claves secretas, idioma de WordPress y ABSPATH. Para obtener más información,
 * visita la página del Codex{@link http://codex.wordpress.org/Editing_wp-config.php Editing
 * wp-config.php} . Los ajustes de MySQL te los proporcionará tu proveedor de alojamiento web.
 *
 * This file is used by the wp-config.php creation script during the
 * installation. You don't have to use the web site, you can just copy this file
 * to "wp-config.php" and fill in the values.
 *
 * @package WordPress
 */

// ** Ajustes solicitado 20180626 ** //

// ** Ajustes de MySQL. Solicita estos datos a tu proveedor de alojamiento web. ** //
/** El nombre de tu base de datos de WordPress */
define('DB_NAME', 'E');

/** Tu nombre de usuario de MySQL */
define('DB_USER', 'E');

/** Tu contraseña de MySQL */
define('DB_PASSWORD', 'E');

/** Host de MySQL (es muy probable que no necesites cambiarlo) */
define('DB_HOST', 'localhost');

/** Codificación de caracteres para la base de datos. */
define('DB_CHARSET', 'utf8mb4');

/** Cotejamiento de la base de datos. No lo modifiques si tienes dudas. */
define('DB_COLLATE', '');

/**#@+
 * Claves únicas de autenticación
```

WordPress Vulnerabilities

Ex2: Using WPVULNDB

| 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 |

I in version 4.7.16

I in version 4.7.16

I in version 4.7.16

I in version 4.7.16

I in version 4.7.15

I in version 4.7.15

I in version 4.7.15

I in version 4.7.15

I in version 4.7.15

I in version 4.7.15

I in version 4.7.15

I in version 4.7.15

I in version 4.7.15

I in version 4.7.14

I in version 4.7.13

I in version 5.0.1

I in version 4.7.12

I in version 4.7.12

I in version 4.7.12

I in version 4.7.12

Ex
W

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.



The screenshot shows a vulnerability report from SUCURI. At the top, the SUCURI logo is displayed in a stylized font, followed by the text 'VULNERABILITY DETAILS' and the WordPress logo. The main title of the report is 'Content Injection Vulnerability in WordPress'. Below the title, the date 'FEBRUARY 1, 2017' and the author 'MARC-ALEXANDRE MONTPAS' are listed, accompanied by small flags of Italy and Brazil. A summary box contains the following details: Security Risk: Severe; Exploitation Level: Easy/Remote; DREAD Score: 9/10; Vulnerability: Privilege Escalation / Content Injection; Patched Version: 4.7.2.

SUCURI
VULNERABILITY DETAILS



Content Injection Vulnerability in WordPress

FEBRUARY 1, 2017   [MARC-ALEXANDRE MONTPAS](#)

Security Risk: Severe
Exploitation Level: Easy/Remote
DREAD Score: 9/10
Vulnerability: Privilege Escalation / Content Injection
Patched Version: 4.7.2

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
`

`Kurdish Hacker Here
`

`If you want Fix Problem Website … !
`

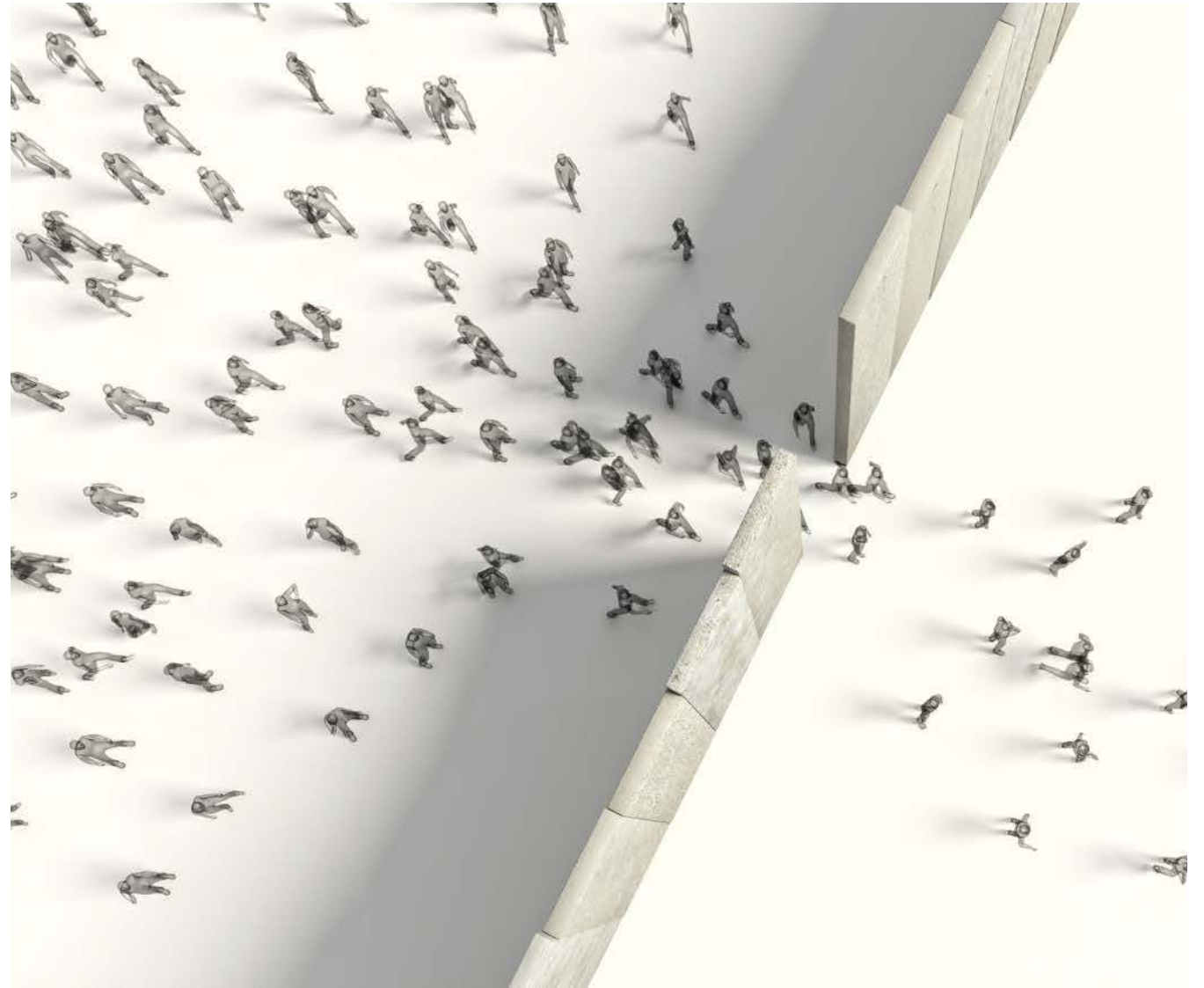
`Contact Me via Gmail : darinsniper007@ gmail.com
`

`Contact Me Via Facebook : https://www.facebook.com
/balasniper007 </p>`

```
<title>~!Hacked By GeNErAL alias Mathis!~</title>
<h2>Hacked By GeNErAL</h2>&nbsp;&nbsp;&nbsp;</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>\!/</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
4.7.15
4.7.15
4.7.15
4.7.15
4.7.15
4.7.15
4.7.13
5.0.1
4.7.12
4.7.12
4.7.12
4.7.12

What
happens
if...



Defacements



Example: Photographer Gallery

St. Louis Weddings - Photography



Engagements



Portraits



Newborns & Maternity



Seniors



Headshots & Executive Portraits



Galleries - ALL

St. Louis Wedding
Photography



Hacked By Dik4h4nZ

Headshots &
Executive portraits



Security Attack !!!

Contact

Hacked by El Moujahidin



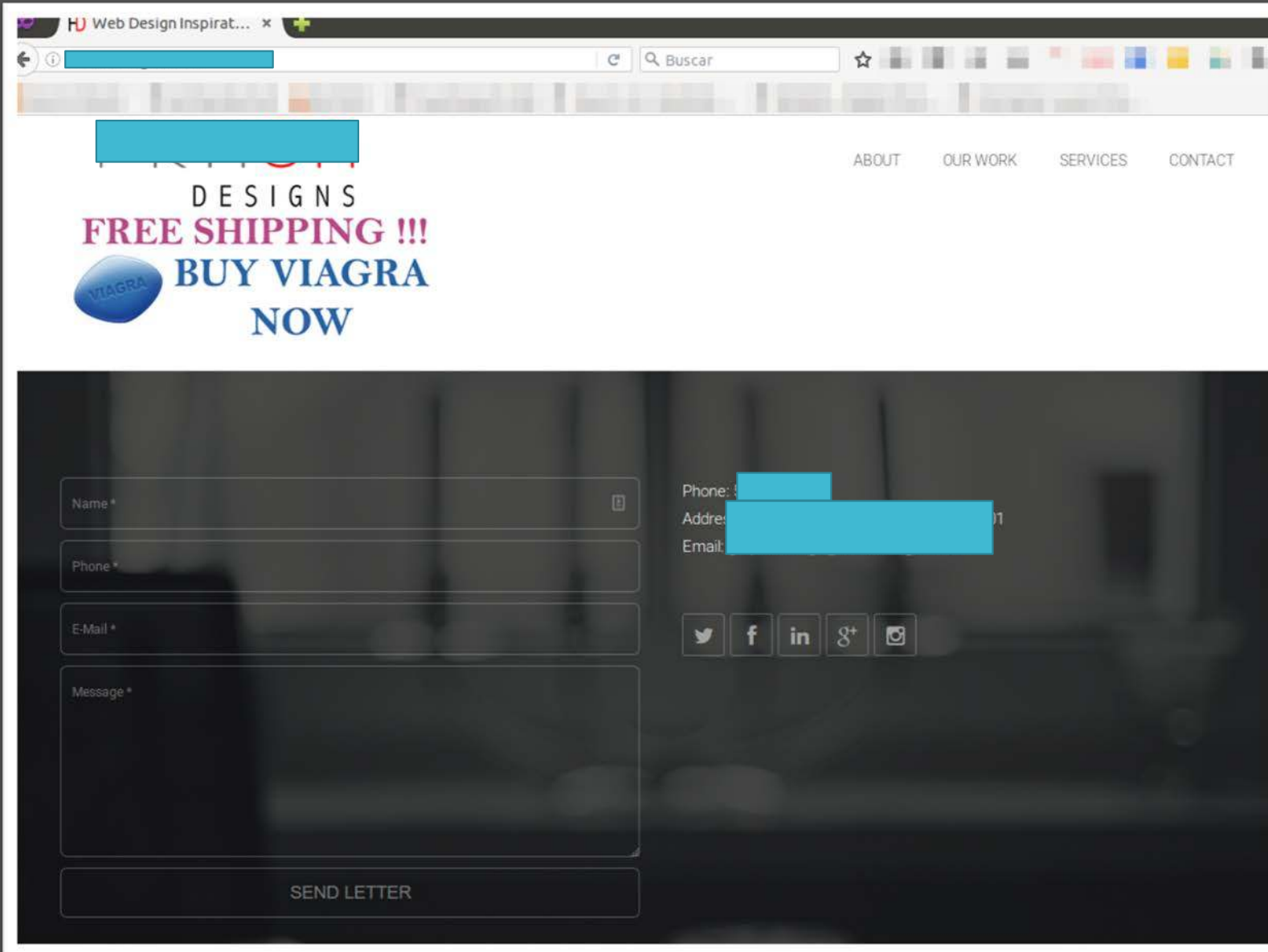
#Free Syria
#Free Palestine

Tell Your Gov , To Know About Palestine
We Will Countinue Hacking The Sites , To Send The Message Of Our Palestine And All Arabs
We Dont Accept Killing Medicine From Whom Stop Killing US



Black Hat SEO





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 smartphones 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 smartphones at Droidepot.

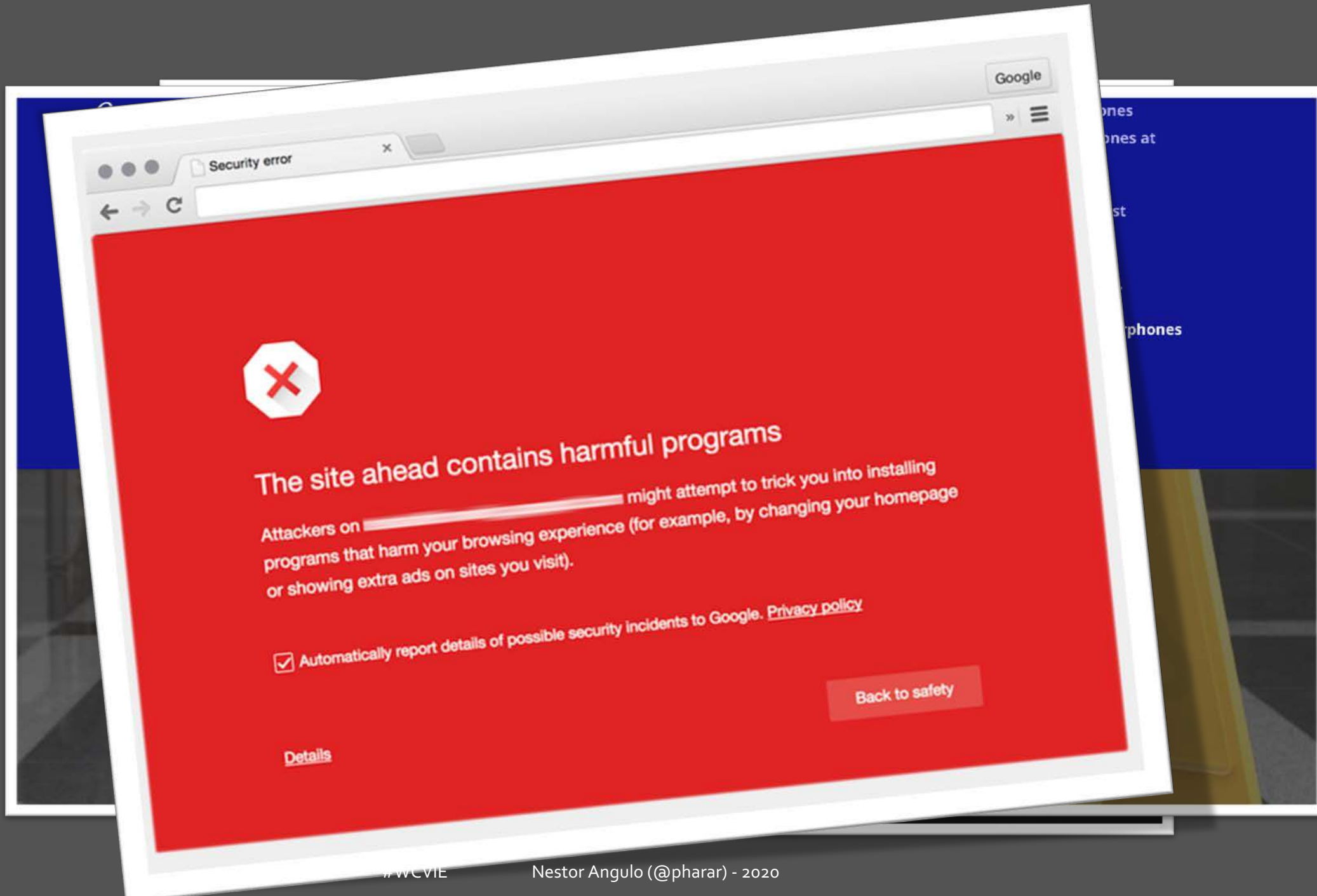
Construction. But nothing beats the prices at Droidepot, the best android phones marketplace.

Professional Janitorial Services

Consistency. Simplicity. Value.

Trusted by Corpus Christi businesses





[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 possible security issues to Google

[Back to safety](#)

[Details](#)



DDoS Attacks / BotNets

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 |

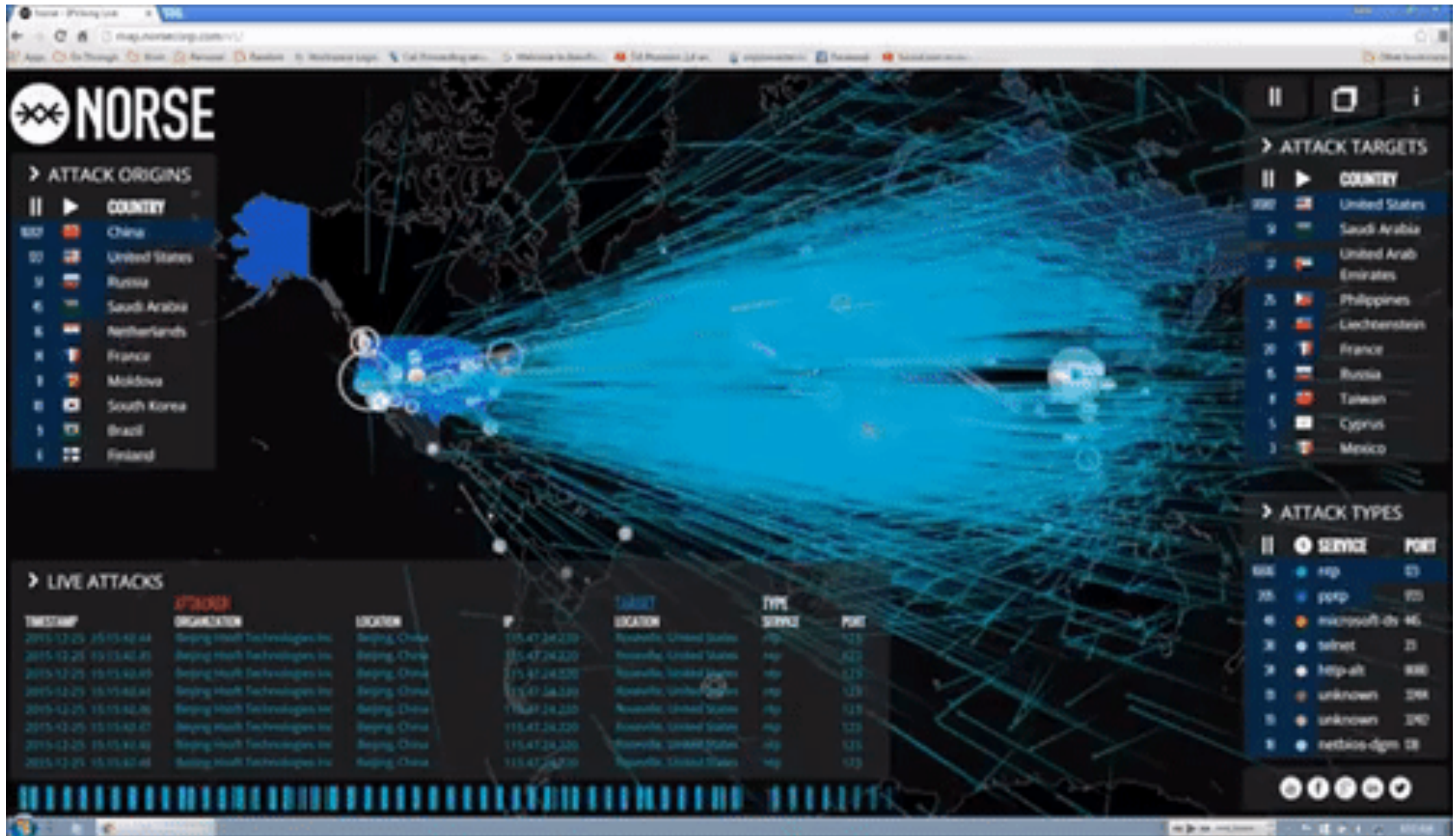
ATTACKS

| Timestamp | Organization | Attacker Location | IP | Target Location | 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 |

ATTACK TYPES

| # | Service |
|---|-------------|
| 2 | discard |
| 1 | ssh |
| 1 | unknown |
| 1 | netbios-dgm |
| 1 | db-lsp-disc |
| 1 | ms-sql-s |
| 1 | isakmp |
| 1 | unknown |

Normal, tending to calm





#WCVIE

Néstor Angulo (@pharar) - 2020

A large, white, cylindrical countermeasure device is mounted on the turret of a tank. The device has a flared, funnel-like shape at the front. The tank is in a factory or workshop setting, with other military vehicles visible in the background. The scene is dimly lit, with a focus on the countermeasure device.

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

Users [Add New](#)

66

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 Change role to...

6 items

| <input type="checkbox"/> | Username | Name | Email | Role | Posts |
|-------------------------------------|-------------------------------|----------------------------------|--------------------------|---------------|-------|
| <input type="checkbox"/> | admin | [redacted] | [redacted] | Administrator | 78 |
| <input checked="" type="checkbox"/> | akmin | | no@email.com | Administrator | 1 |
| <input type="checkbox"/> | janel | [redacted] | [redacted] | Contributor | 0 |
| <input type="checkbox"/> | levy | [redacted] | [redacted] | Contributor | 33 |
| <input checked="" type="checkbox"/> | managed-wp-migration-465790ae | Managed WordPress Migration User | noreply@secureserver.net | Administrator | 0 |
| <input checked="" type="checkbox"/> | wp.service.controller.lHmp6 | | | None | 0 |
| <input type="checkbox"/> | Username | Name | Email | Role | Posts |

Bulk Actions Change role to...

6 items

- Dashboard
- All in One SEO
- Jetpack
- Unyson
- Blog Posts
- Media
- Pages
- Comments
- Forms
- FooGallery
- Portfolio
- Feedback
- Forms
- Appearance
- Plugins 3
- Users**

All Users [Add New](#)

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

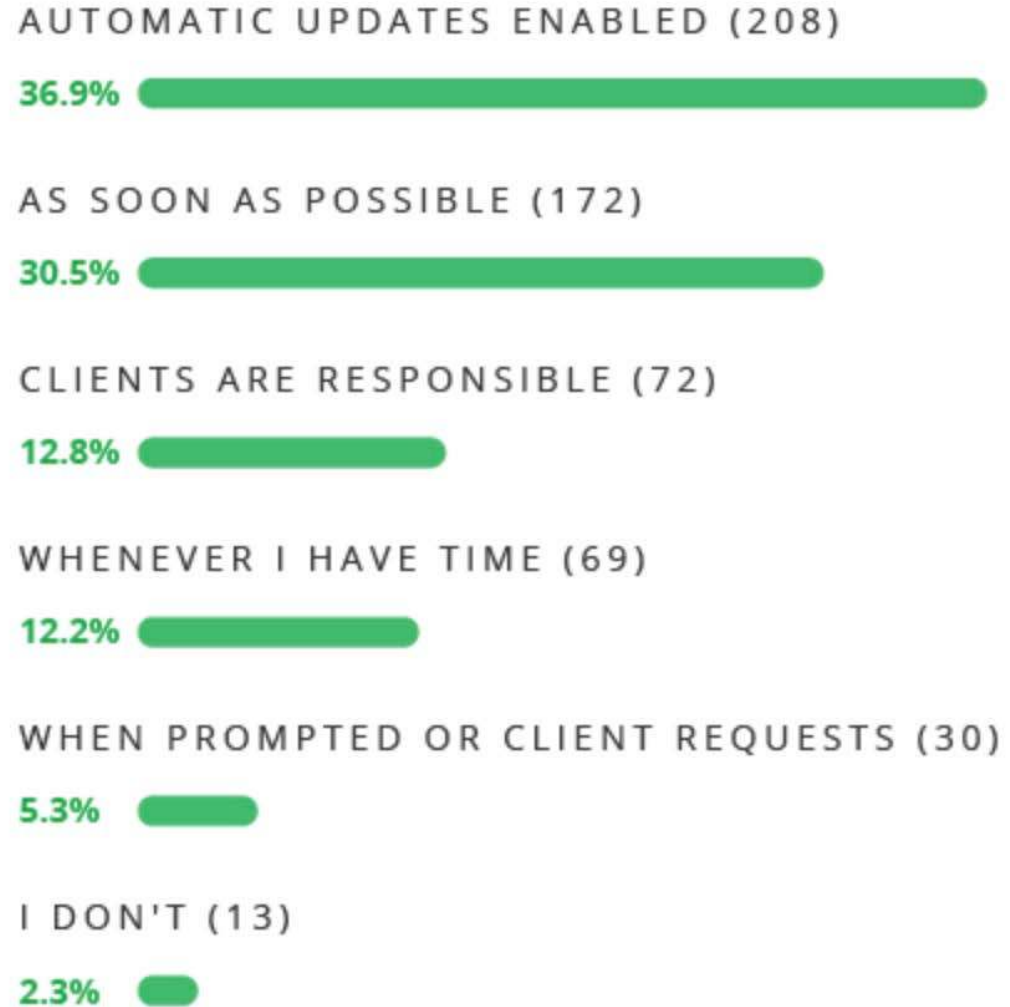
- PLUGINS
- THEMES
- CORE
- PHP
- APACHE / NGINX
- SERVER
- CPANEL / PLESK
- ...



Updates

Source:
Web Professional
Security Survey 2019
sucuri.net

How Frequently do you Install Security Patches for your clients'?



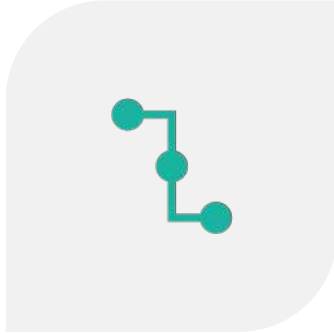
Remember to
invest in...



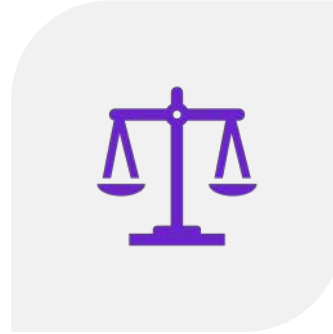
SECURITY



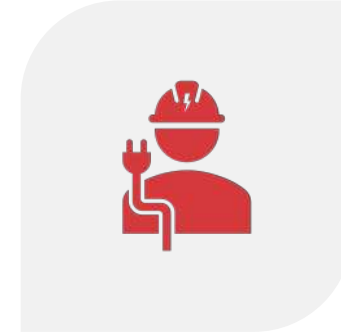
HOSTING



**FIRST LAYER OF
YOUR SITE'S DEFENSE**



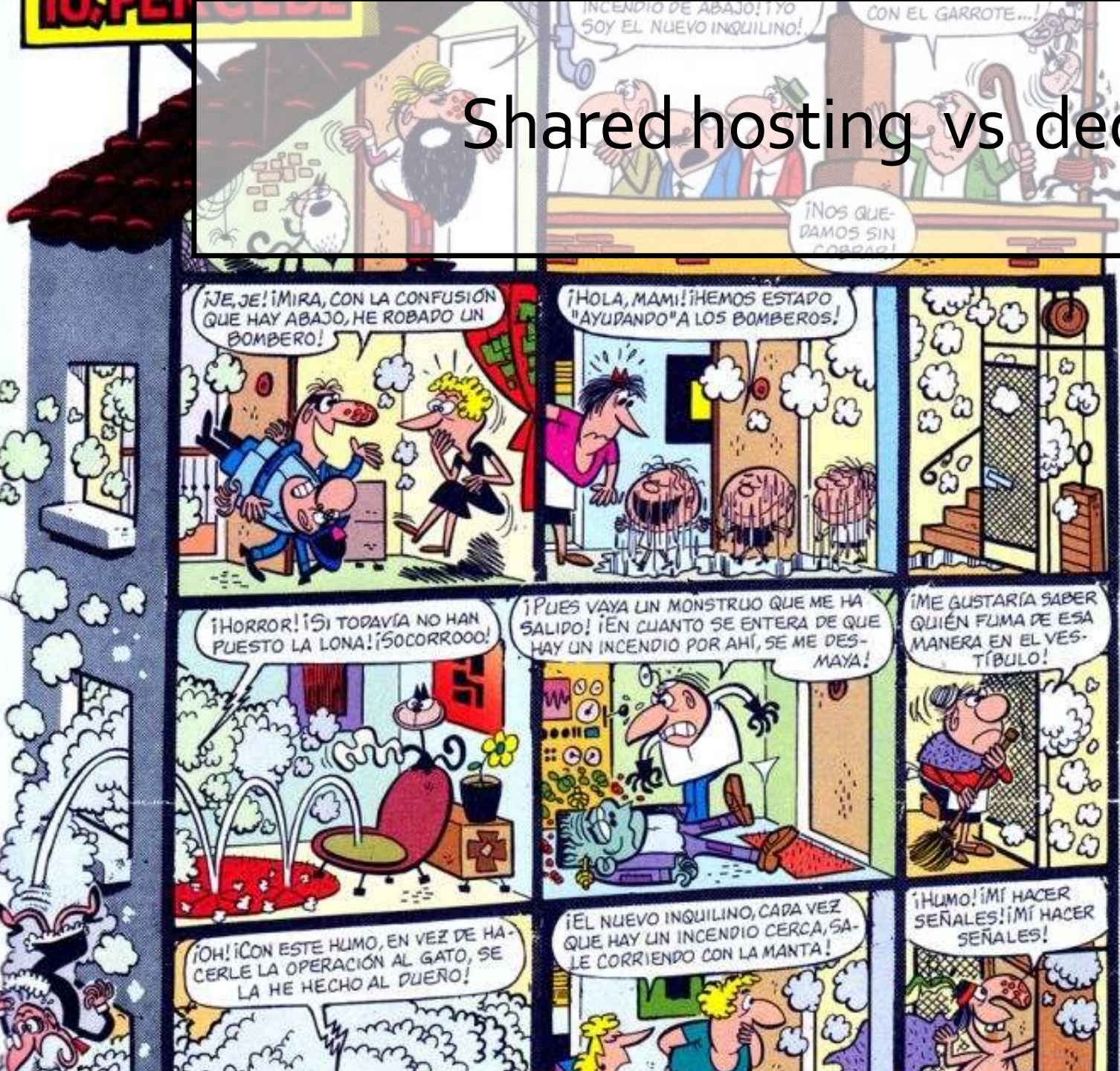
**BALANCE BETWEEN
PRICE AND FEATURES**



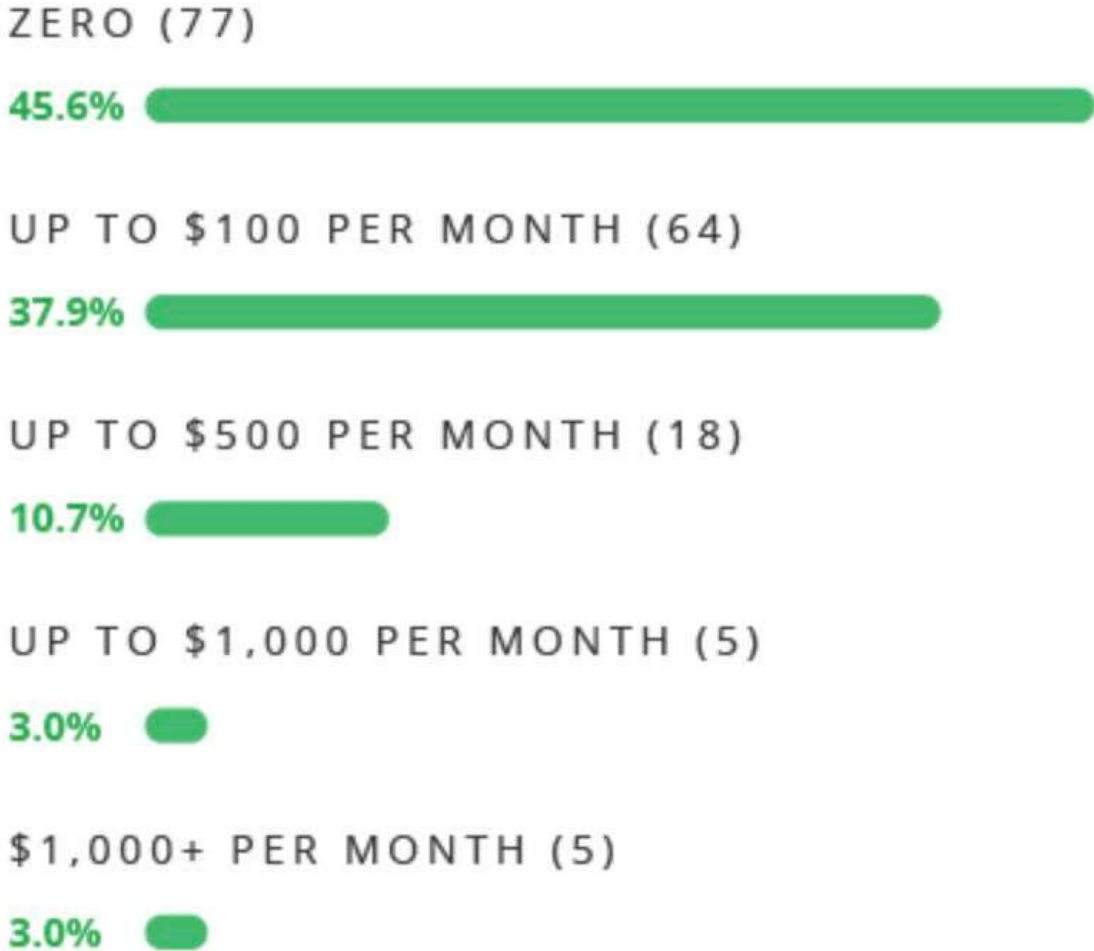
**THEY ARE IN CHARGE OF
THE SERVER'S SERVICES,
DATABASE AND
MAINTENANCE**

Hosting

Shared hosting vs dedicated



How much budget do you have to invest in website security?



Source:
2019 Sucuri
survey to
ecommerce
owners.

WAF

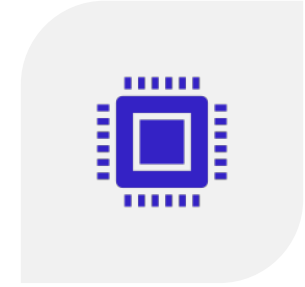
Your guard dog



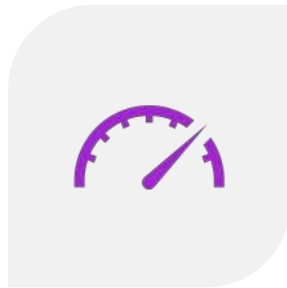
**FILTERS ALL YOUR
WEB TRAFFIC**



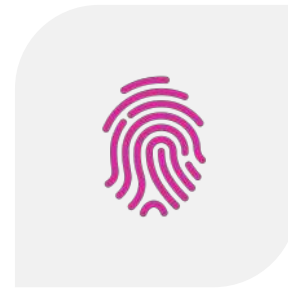
**PROTECTS AGAINST
XSS, DDOS, ...**



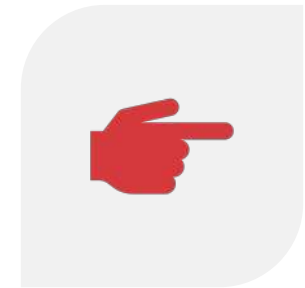
**PATCHS VIRTUALLY WIDELY
KNOWN SOFTWARE
VULNERABILITIES**



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



**FORENSIC ANALISYS
TOOL**



**ALLOWS MANUAL
BLOCKING**

WAF

Your guard

WAF!



LY WIDELY
TWARE
LITIES

ANUAL
NG

Sucuri Network



Good
HTTP / HTTPS Traffic



Bad
HTTP / HTTPS Traffic



Everybody needs a hacker



@pharar

Nestor Angulo de Ugarte

Danke schön!
Fragen?