Nestor Angulo de Ugarte

Round 1! FIGHT! – Or how to survive against a malicious hacker

A lot is said about security, fences, plugins … But what does all this REALLY mean? Let's imagine that you are a "Street Fighter" or a "Mortal Kombat" character from those 80's video games and you have to face your particular fight against a bad guy.

ROUND 1

FIGHT

Or how to survive an attack by a malicious hacker

Nestor Angulo de Ugarte (@pharar)

#WCCH

PUSH START
INSERT COIN

Nestor Angulo

- **CISSP** (ISC2.org - 2022)
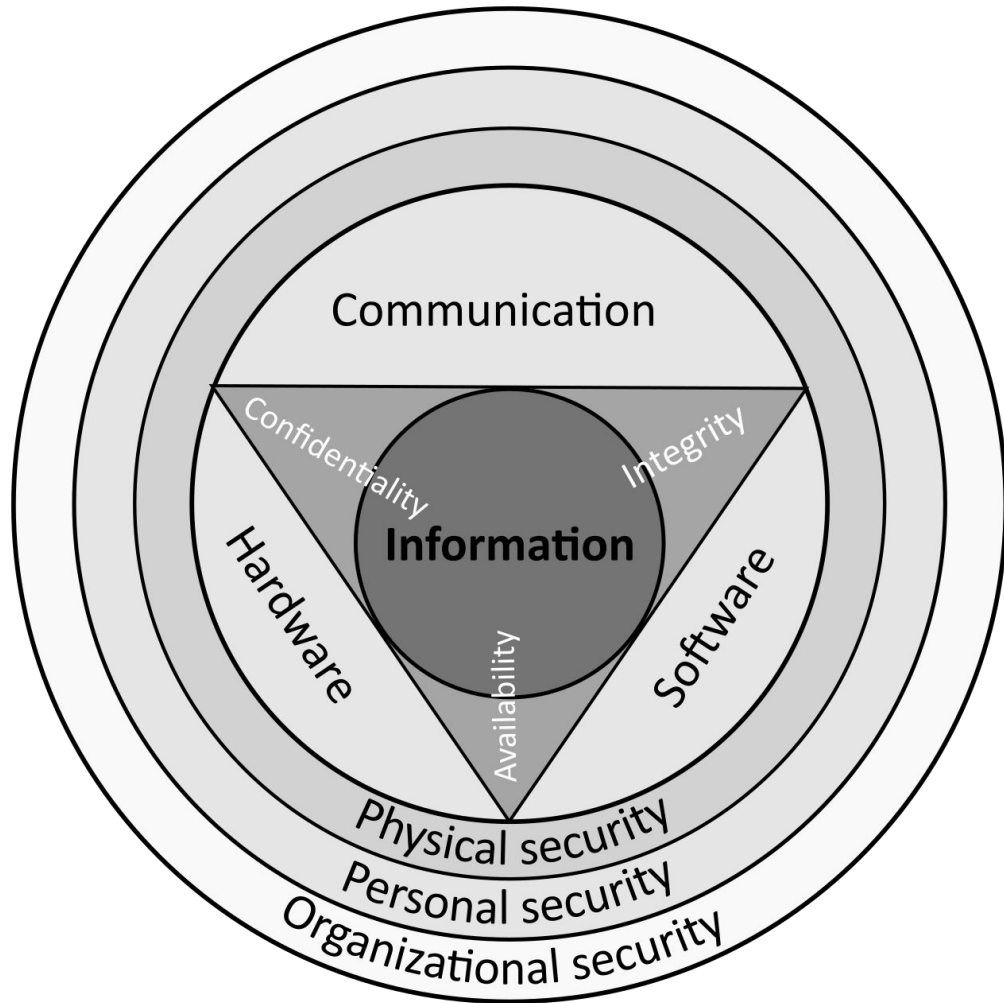- **Web Security Analyst** (2015-2023)
  - @GoDaddy WebSecurity
  - @sucuri.net

- New beginning: **nestorangulo.pro**

- Brand Ambassador: **Patchstack**

  patchstack

- @pharar

What is Information Security

The Game

POSSIBLE OBJECTIVES

Users	Database	Content
Infrastructure	**Bot Net**	**Reputation**

The Life bar

It represents the **protection capacity** of your website.
More bar, more **probability** of winning.

Factors Affecting the Life Bar

- **Each defense category** that you add **sums points**, max of 100 pts.

- **Not updating** your site -> Lowers your bar by **5% / month.**

- **Additional admin/ disabled plugin** -> Lowers by an additional **2% / month**.

- 0 pts. means that even a script kiddie can hack your site.

Characters

Hacker:

Curious person who loves to go beyond limits or convetionalisms.

Cyberterrorist / Cracker:

Computer Hacker, whom intentions are always aligned to enrich himself in a zero-sum game situation.

The bad guy

- **Lise Meitner** (1878-1968): Nuclear fission.

- **Alan Turing** (1912-1954): Turing machine

- **Hedy Lamarr** (1914-2000): Wi-Fi

- **Leonardo da Vinci** (1452-1519)

- **Hypatia of Alexandria** (c. 350-415): Astrolabe

- **Archimedes** (c. 287-212 BC): Water displacement

- **Ada Lovelace** (1815-1852): First programmer

- **Grace Hopper** (1906-1992): COBOL

- **Michael Faraday** (1791-1867): Electricity

Good guys

- White Hat Hackers
- blue / red / purple team
- Security Analysts
- Technical Support
- Security Plugins
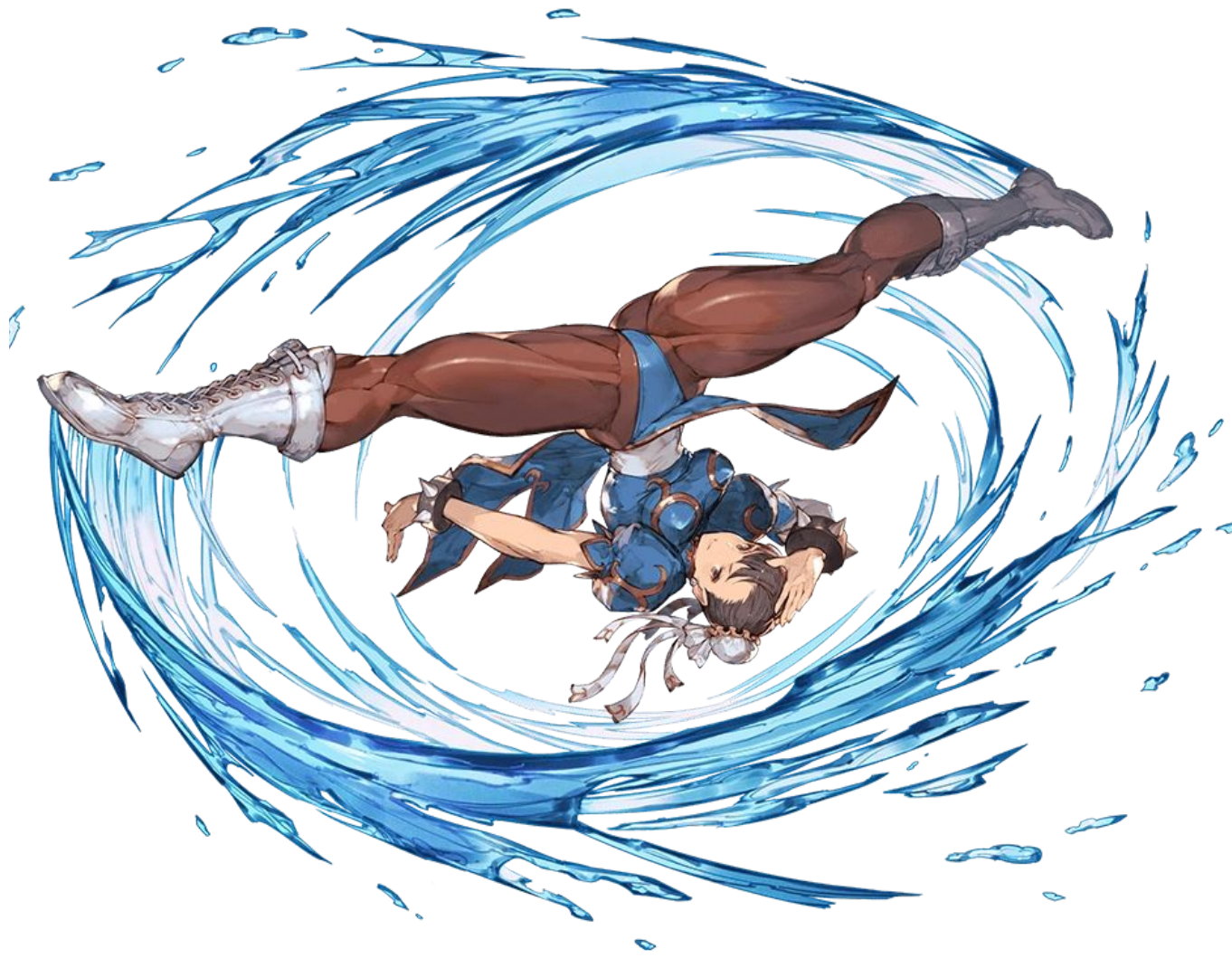
Luca

Our good guy hacker

Hackers
"On their own"

- Gray Hat Hackers
- Hacktivists

Anika

Our freelance hacker.

Fill in the fighting ___ word of your choice.

Bad guys

- Black Hat Hacker
- Cyberterrorist / Criminals
- Script Kiddies
- Lone wolf
- Organized Teams

Cammy

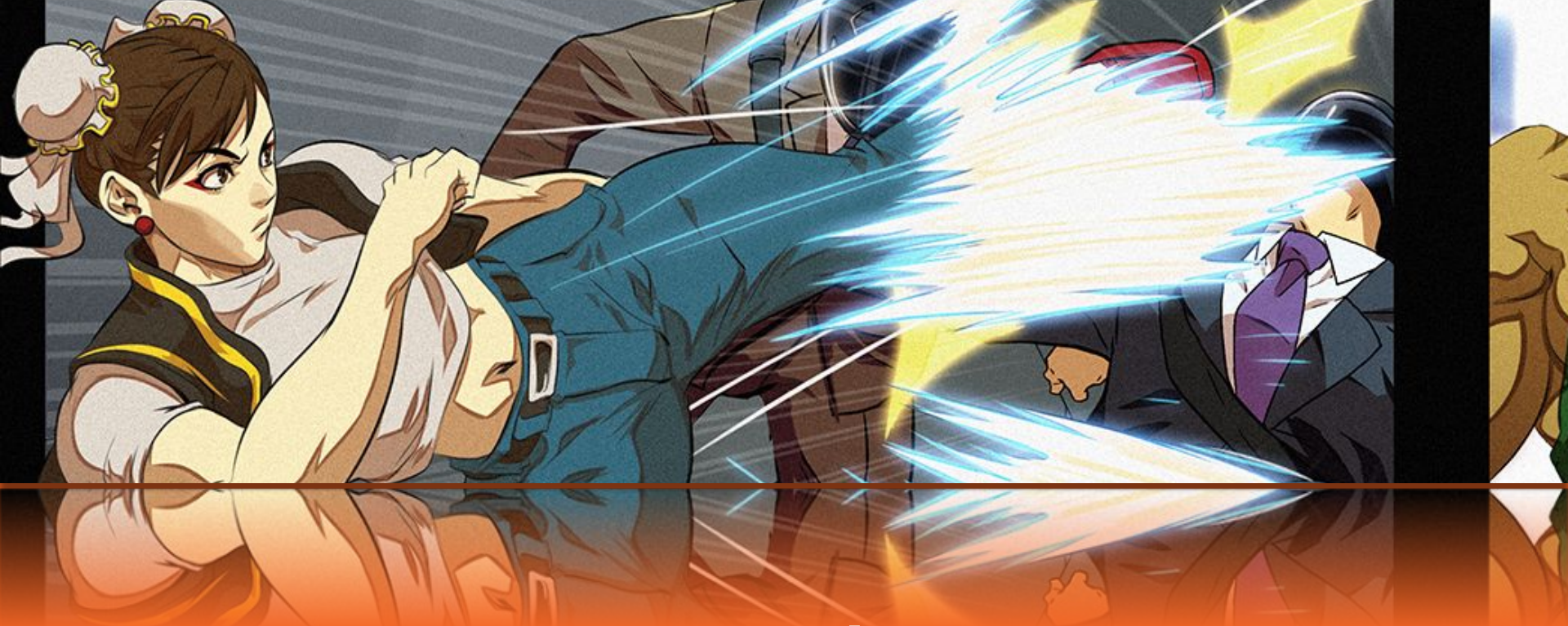Our Script Kiddie.
Life bar: 20-30pts.

Bruce

Our professional Black Hat Hacker.
Life bar: 50-70pts.

The General

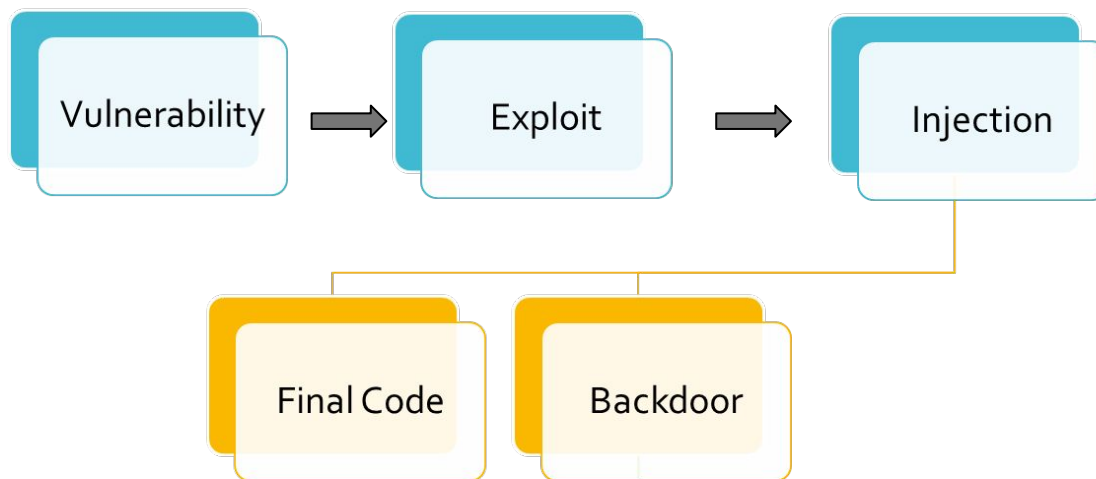Our organized team of black hat hackers. The bad boss. The Boss. Life bar: 100pts.
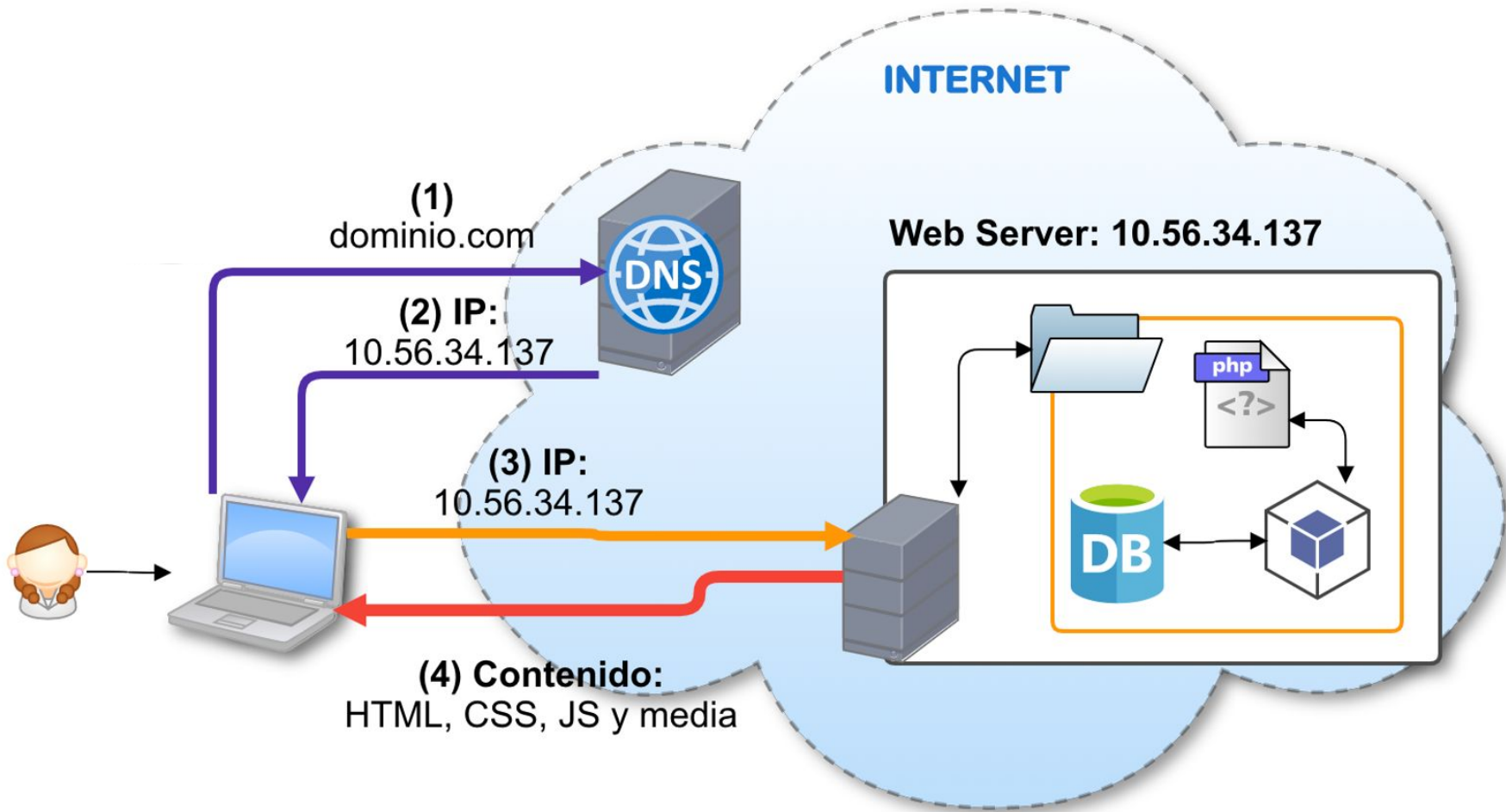
Attacks

How do you hack a WordPress site?

Vulnerability → Exploit → Injection

Injection
├── Final Code
└── Backdoor

INTERNET

(1) dominio.com

(2) IP: 10.56.34.137

(3) IP: 10.56.34.137

Web Server: 10.56.34.137

(4) Contenido: HTML, CSS, JS y media

DNS

DB

php
<?>

Attack	Description	Categorie	Level
Phishing / Spam	Injection or use of, to capture information.	Reputation, Login	

Remote site: /public_html/wp-content/plugins/joom|

Filename	Fi
..	
_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	

Remote site: /public_html/wp-content/plugins

Filename ⌃	Filesize
..	
Login-wall-KiLxb	
Login-wall-NUJIF	
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

Examples of fake Plugins/Themes

wp-content/plugins
wp-content/themes

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

Attack	Description	Categorie	Level
Phishing / Spam	Injection or use of, to capture information.	Reputation, Login	
Brute Force / Dictionary	Try username/password combinations, informed or not. 💡 *Wikipedia*: 10,000_most_common_passwords 💡 haveibeenpwned.com	Login	

Attack	Description	Categorie	Level
Phishing / Spam	Injection or use of, to capture information.	Reputation, Login	
Brute Force / Dictionary	Try username/password combinations, informed or not. 💡 *Wikipedia*: 10,000_most_common_passwords 💡 haveibeenpwned.com	Login	
XSS	Redirection (JS)	Reputation	

Google

Google Membership Rewards

G **Congratulations**
January 26 at 12:03am

Google Gift!

Every Tuesday we select 10 lucky Apple us[...]d!) from [redacted]
our sponsors. This free gift is **exclusively** [...] s 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 [redacted] 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

Attack	Description	Categorie	Level
Phishing / Spam	Injection or use of, to capture information.	Reputation, Login	
Brute Force / Dictionary	Try username/password combinations, informed or not. 💡 *Wikipedia*: 10,000_most_common_passwords 💡 haveibeenpwned.com	Login	
XSS	Redirection (JS)	Reputation	
New vulnerabilities	Discover new vulnerabilities	Investigation	

Attack	Description	Categorie	Level
Phishing / Spam	Injection or use of, to capture information.	Reputation, Login	
Brute Force / Dictionary	Try username/password combinations, informed or not. 💡 *Wikipedia*: 10,000_most_common_passwords 💡 haveibeenpwned.com	Login	
XSS	Redirection (JS)	Reputation	
New vulnerabilities	Discover new vulnerabilities	Investigation	
Man in the Middle	Intervene communications	Communications	

Original Connection

User

Web Application

New Connection

Man in the Middle

Attacker

1
Injects fake
DNS entry

Client

2
Issues request
to real website

DNS

3
Request resolves
to fake website

www
Fake website

www
Real website

Attack	Description	Categorie	Level
Phishing / Spam	Injection or use of, to capture information.	Reputation, Login	
Brute Force / Dictionary	Try username/password combinations, informed or not. 💡 *Wikipedia*: 10,000_most_common_passwords 💡 haveibeenpwned.com	Login	
XSS	Redirection (JS)	Reputation	
New vulnerabilities	Discover new vulnerabilities	Investigation	
Man in the Middle	Intervene communications	Communications	
DoS / DDoS	Disable a service	Communications, resources	

Attack	Description	Categorie	Level
Phishing / Spam	Injection or use of, to capture information.	Reputation, Login	
Brute Force / Dictionary	Try username/password combinations, informed or not. 💡 *Wikipedia*: 10,000_most_common_passwords 💡 haveibeenpwned.com	Login	
XSS	Redirection (JS)	Reputation	
New vulnerabilities	Discover new vulnerabilities	Investigation	
Man in the Middle	Intervene communications	Communications	
DoS / DDoS	Disable a service	Communications, resources	
SQL Injection	Database attack	Database	

Attack	Description	Categorie	Level
Phishing / Spam	Injection or use of, to capture information.	Reputation, Login	
Brute Force / Dictionary	Try username/password combinations, informed or not. 💡 *Wikipedia*: 10,000_most_common_passwords 💡 haveibeenpwned.com	Login	
XSS	Redirection (JS)	Reputation	
New vulnerabilities	Discover new vulnerabilities	Investigation	
Man in the Middle	Intervene communications	Communications	
DoS / DDoS	Disable a service	Communications, resources	
SQL Injection	Database attack	Database	
Ransomware	Sequestration of data/files	Files	

Attack	Description	Categorie	Level
Cryptomining	Use of third-party infrastructure to mine crypto	Resources	

Attack	Description	Categorie	Level
Cryptomining	Use of third-party infrastructure to mine crypto	Resources	
BotNode	Use of the infected site (zombie) as an attack platform.	Communications, Files	

Attack	Description	Categorie	Level
Cryptomining	Use of third-party infrastructure to mine crypto	Resources	
BotNode	Use of the infected site (zombie) as an attack platform.	Communications, Files	
Cross-site Contamination	From a hacked site or a backup, infect other sites	Files, database	

Attack	Description	Categorie	Level
Phishing / Spam	Injection or use of, to capture information.	Reputation, Login	
Brute Force / Dictionary	Try username/password combinations, informed or not. 💡 *Wikipedia*: 10,000_most_common_passwords 💡 haveibeenpwned.com	Login	
XSS	Redirection (JS)	Reputation	
New vulnerabilities	Discover new vulnerabilities	Investigation	
Man in the Middle	Intervene communications	Communications	
DoS / DDoS	Disable a service	Communications, resources	
SQL Injection	Database attack	Database	
Ransomware	Sequestration of data/files	Files	
Cryptomining	Use of third-party infrastructure to mine crypto	Resources	

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.

2017		2021
A01:2017-Injection		A01:2021-Broken Access Control
A02:2017-Broken Authentication		A02:2021-Cryptographic Failures
A03:2017-Sensitive Data Exposure		A03:2021-Injection
A04:2017-XML External Entities (XXE)	(New)	A04:2021-Insecure Design
A05:2017-Broken Access Control		A05:2021-Security Misconfiguration
A06:2017-Security Misconfiguration		A06:2021-Vulnerable and Outdated Components
A07:2017-Cross-Site Scripting (XSS)		A07:2021-Identification and Authentication Failures
A08:2017-Insecure Deserialization	(New)	A08:2021-Software and Data Integrity Failures
A09:2017-Using Components with Known Vulnerabilities		A09:2021-Security Logging and Monitoring Failures*
A10:2017-Insufficient Logging & Monitoring	(New)	A10:2021-Server-Side Request Forgery (SSRF)*

* From the Survey

And what about the AI?

AI Conundrum

Defenses

Attack	Defense(s)	Category

Attack	Defense(s)	Category
Phishing / Spam	Habilidad, Frontend monitor	Reputation, Login

Attack	Defense(s)	Category
Phishing / Spam	Habilidad, Frontend monitor	Reputation, Login
Brute Force / Dictionary	WAF, Limit login plugin	Login

Website Application Firewall (WAF)

Protect and Speed Up Your Website

Visitor · Website host · WAF · WordPress Website

Attack	Defense(s)	Category
Phishing / Spam	Habilidad, Frontend monitor	Reputation, Login
Brute Force / Dictionary	WAF, Limit login plugin	Login
XSS	WAF, Files integrity scanner	Reputation

Attack	Defense(s)	Category
Phishing / Spam	Habilidad, Frontend monitor	Reputation, Login
Brute Force / Dictionary	WAF, Limit login plugin	Login
XSS	WAF, Files integrity scanner	Reputation
New vulnerabilities	WAF, maintenance	Research

Attack	Defense(s)	Category
Phishing / Spam	Habilidad, Frontend monitor	Reputation, Login
Brute Force / Dictionary	WAF, Limit login plugin	Login
XSS	WAF, Files integrity scanner	Reputation
New vulnerabilities	WAF, maintenance	Research
Man in the Middle	SSL	Communications

SSL
Secure Sockets Layer

Data Theft

Eavesdropping

Internet

SSL

User

Encrypted Connection

Website

Internet Service Providers

Hackers

Governments

🔒 Encrypted tunnel

VPN

Using your computer abroad

Internet

Attack	Defense(s)	Category
Phishing / Spam	Habilidad, Frontend monitor	Reputation, Login
Brute Force / Dictionary	WAF, Limit login plugin	Login
XSS	WAF, Files integrity scanner	Reputation
New vulnerabilities	WAF, maintenance	Research
Man in the Middle	SSL	Communications
DoS / DDoS	WAF	Communications, Resources

Attack	Defense(s)	Category
Phishing / Spam	Habilidad, Frontend monitor	Reputation, Login
Brute Force / Dictionary	WAF, Limit login plugin	Login
XSS	WAF, Files integrity scanner	Reputation
New vulnerabilities	WAF, maintenance	Research
Man in the Middle	SSL	Communications
DoS / DDoS	WAF	Communications, Resources
SQL Injection	WAF, Logs	Database

Attack	Defense(s)	Category
Phishing / Spam	Habilidad, Frontend monitor	Reputation, Login
Brute Force / Dictionary	WAF, Limit login plugin	Login
XSS	WAF, Files integrity scanner	Reputation
New vulnerabilities	WAF, maintenance	Research
Man in the Middle	SSL	Communications
DoS / DDoS	WAF	Communications, Resources
SQL Injection	WAF, Logs	Database
Ransomware	Backups	Files

Attack	Defense(s)	Category
Phishing / Spam	Habilidad, Frontend monitor	Reputation, Login
Brute Force / Dictionary	WAF, Limit login plugin	Login
XSS	WAF, Files integrity scanner	Reputation
New vulnerabilities	WAF, maintenance	Research
Man in the Middle	SSL	Communications
DoS / DDoS	WAF	Communications, Resources
SQL Injection	WAF, Logs	Database
Ransomware	Backups	Files
Cryptomining	Logs, users	Resources, Reputation

Attack	Defense(s)	Category
Phishing / Spam	Habilidad, Frontend monitor	Reputation, Login
Brute Force / Dictionary	WAF, Limit login plugin	Login
XSS	WAF, Files integrity scanner	Reputation
New vulnerabilities	WAF, maintenance	Research
Man in the Middle	SSL	Communications
DoS / DDoS	WAF	Communications, Resources
SQL Injection	WAF, Logs	Database
Ransomware	Backups	Files
Cryptomining	Logs, users	Resources, Reputation
BotNode	WAF, Logs	Communications, Files

Attack	Defense(s)	Category
Phishing / Spam	Habilidad, Frontend monitor	Reputation, Login
Brute Force / Dictionary	WAF, Limit login plugin	Login
XSS	WAF, Files integrity scanner	Reputation
New vulnerabilities	WAF, maintenance	Research
Man in the Middle	SSL	Communications
DoS / DDoS	WAF	Communications, Resources
SQL Injection	WAF, Logs	Database
Ransomware	Backups	Files
Cryptomining	Logs, users	Resources, Reputation
BotNode	WAF, Logs	Communications, Files
Cross-Site Contamination	Files integrity scanner	Files

Attack	Defense(s)	Category
Phishing / Spam	Habilidad, Frontend monitor	Reputation, Login
Brute Force / Dictionary	WAF, Limit login plugin	Login
XSS	WAF, Files integrity scanner	Reputation
New vulnerabilities	WAF, maintenance	Research
Man in the Middle	SSL	Communications
DoS / DDoS	WAF	Communications, Resources
SQL Injection	WAF, Logs	Database
Ransomware	Backups	Files
Cryptomining	Logs, users	Resources, Reputation
BotNode	WAF, Logs	Communications, Files
Cross-Site Contamination	Integridad de Files	Files

Summarizing the Defenses list

Type	Description	Pts
WAF	Web Application Firewall.	40

Summarizing the Defenses list

Type	Description	Pts
WAF	Web Application Firewall.	40
Monitoring	Logs, scanners and triggers.	10

Summarizing the Defenses list

Type	Description	Pts
WAF	Web Application Firewall.	40
Monitoring	Logs, scanners and triggers.	10
Backups	Good strategy of backups	10

Summarizing the Defenses list

Type	Description	Pts
WAF	Web Application Firewall.	40
Monitoring	Logs, scanners and triggers.	10
Backups	Good strategy of backups	10
SSL	Secured transmissions with / from a site	10

Summarizing the Defenses list

Type	Description	Pts
WAF	Web Application Firewall.	40
Monitoring	Logs, scanners and triggers.	10
Backups	Good strategy of backups	10
SSL	Secured transmissions with / from a site	10
Maintenance / hardening	Updates, obfuscation, reduce attack surface	20

Summarizing the Defenses list

Type	Description	Pts
WAF	Web Application Firewall.	40
Monitoring	Logs, scanners and triggers.	10
Backups	Good strategy of backups	10
SSL	Secured transmissions with / from a site	10
Maintenance / hardening	Updates, obfuscation, constant minimization of attack surface	20
Expertise	Human expert taking care	10

Combos

The power of his Hurricane Punch and Dragon Punch are renowned since ancient times.

Sure Killing Technique
(While facing right)

Hurricane Punch
↓↘→ and **punch** ⊙ simultaneously

Dragon Punch
→↘↓ and **punch** ⊙ simultaneously

Cyclone Kick
↓↙← and **kick** ⊙ simultaneously

Ken has moved to America in order to train against a greater variety of opponents.

Sure Killing Technique
(While facing right)

Hurricane Punch
↓↘→ and **punch** ⊙ simultaneously

Dragon Punch
→↘↓ and **punch** ⊙ simultaneously

Cyclone Kick
↓↙← and **kick** ⊙ simultaneously

He has joined the competition to prove the superiority of the Japanese Sumo Wrestler.

Sure Killing Technique
(While facing right)

Hundred-Hand Slap
press **punch** ⊙ many times rapidly

Killer Head Ram
hold ← then →
and **punch** ⊙ simultaneously

Possessing incredible speed, she often makes her opponents look like slow-moving tree slugs.

Sure Killing Technique
(While facing right)

Hundred-Foot Kick
press **kick** ⊙ many times rapidly

Spinning Bird Kick
hold ↓ then ↑
and **kick** ⊙ simultaneously

His past is clouded in mystery. Looks quite different from any ordinary man. Possesses inhuman speed.

Sure Killing Technique
(While facing right)

Thunder Storm
press **punch** ⊙ many times rapidly

Rolling Attack
hold ← then →
and **punch** ⊙ simultaneously

A pile-driver or brain-buster from his mountainous body is nearly unwithstandable.

Sure Killing Technique
(While facing right)

Double Lariatt
⊙ + ⊙ + ⊙
press softly, medium, then hard

Screw Pile Driver
While near the opponent,
spin the lever once and **punch** ⊙

GUILE
U.S.A.

With icy cool, he assaults his opponents without restraint. His somersault kick is devastating.

Sure Killing Technique
(While facing right)

Sonic Boom
hold ← then →
and **punch** ⊙ simultaneously

Somersault Kick
hold ↓ then ↑
and **kick**

SHALSIM
INDIA

A master of yoga, he is capable of manipulating his body in ways that are unbelievable to ordinary humans.

Sure Killing Technique
(While facing right)

Yoga Fire
↓↙→ and **punch** ⊙ simultaneously

Yoga Blast
↙↓↘ and **punch** ⊙ simultaneously

BALROG
U.S.A.

He has defeated all challengers in the boxing ring.

Sure Killing Technique
(While facing right)

Turning Punch
punch + **punch** + **punch**
light   middle   heavy
Momentarily press all 3 punch buttons and release at the same time.

Dashing Straight Punch
hold ← then →
and **punch** ⊙ simultaneously

VEGA
SPAIN

Nick named "The Spanish Ninja," he is the quickest contestant in the round up.

Sure Killing Technique
(While facing right)

Rolling Crystal Flash
hold ← then →
and **punch** ⊙ simultaneously

Barcelona Attack
hold ↓ then ↑
and **kick** ⊙ simultaneously

Izna Drop

SAGAT
THAILAND

Though he was once defeated by Rhu's Dragon Punch, this former champion came back to regain his former status.

Sure Killing Technique
(While facing right)

Tiger Shot
↓↘→ and **punch** ⊙ simultaneously

Grand Tiger Shot
↓↙← and **kick** ⊙ simultaneously

BISON
SECRET SOCIETY
OF SHADLUE

He manipulates auras to his own questionable ends. His veracity as a fighter is nearly super human.

Sure Killing Technique
(While facing right)

Pyscho-crusher
hold ← then →
and **punch** ⊙ simultaneously

Double knee press
hold ← then →
and **kick** ⊙ simultaneously

Remember!

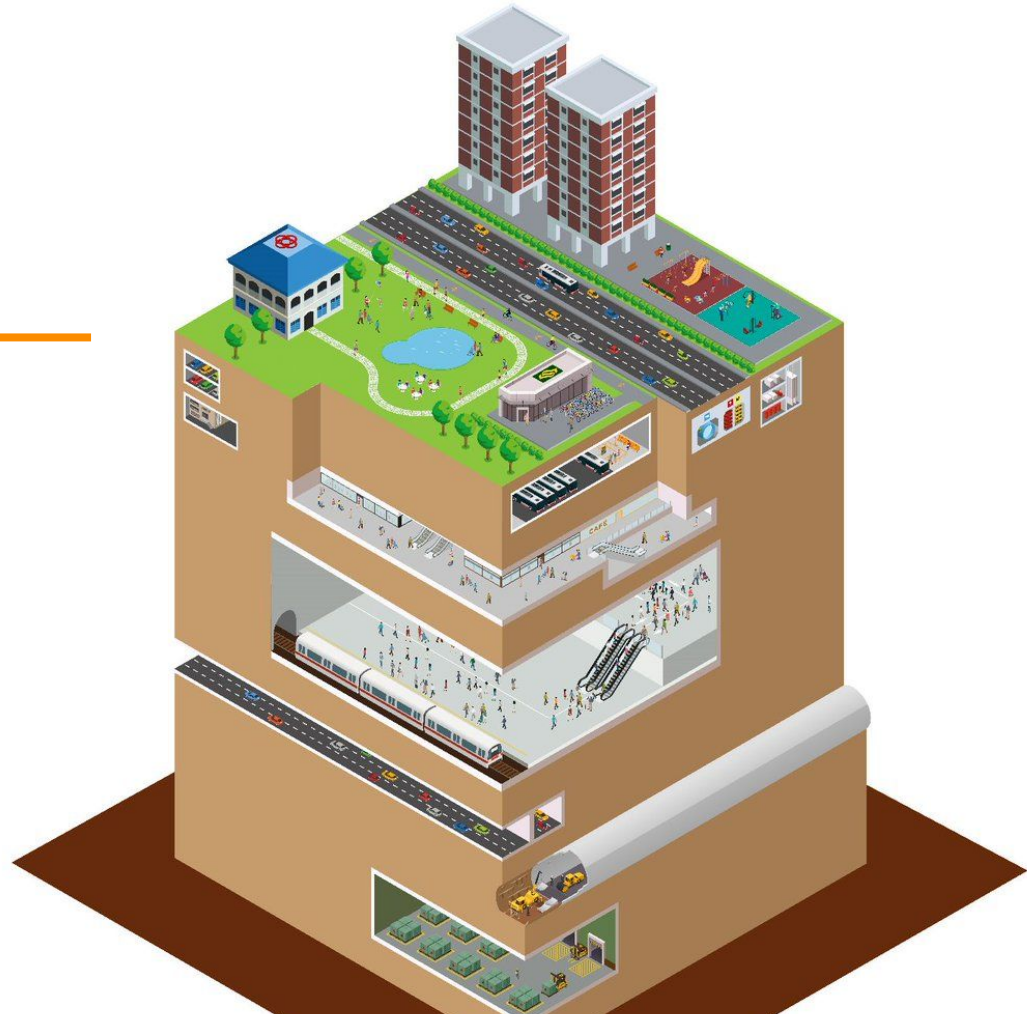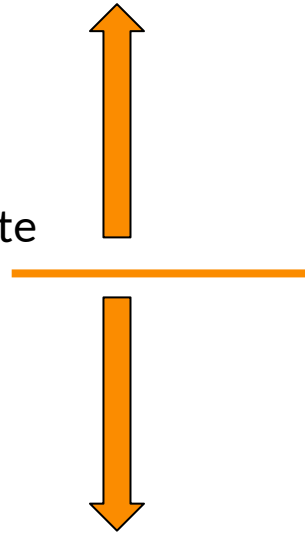∀ **COST** Web down

<

∀ **COST** Web hacked

Site Owner

- App
- Data
- Security of the site

Hosting provider

- Networks
- Hardware
- SO
- Virtualization
- Security

Security Liability

# WordPress Security

https://es.wordpress.org/about/security/

MY Combo

❖ **Cloud WAF + CDN**
➢ Sucuri (or CloudFlare)

❖ **Security plugins + 2FA**
➢ WordFence Free (no WAF)
  o iThemes Security
➢ Fail2Ban
  o Limit Login Attempts
  Reloaded
➢ CAPTCHA 4WP

❖ **Monitoring vulnerabilities + internal WAF**
➢ Patchstack

❖ **Hosting**
➢ SSL
➢ Support + BackUps
➢ Managed plans

❖ **Backups**
➢ VaultPress (Jetpack)
  o BlogVault
  o UpDraft

The importance of UPDATING
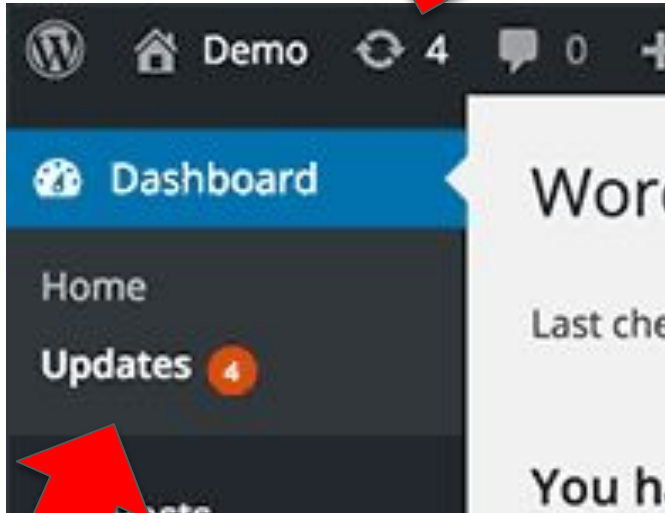
- **Security patches**

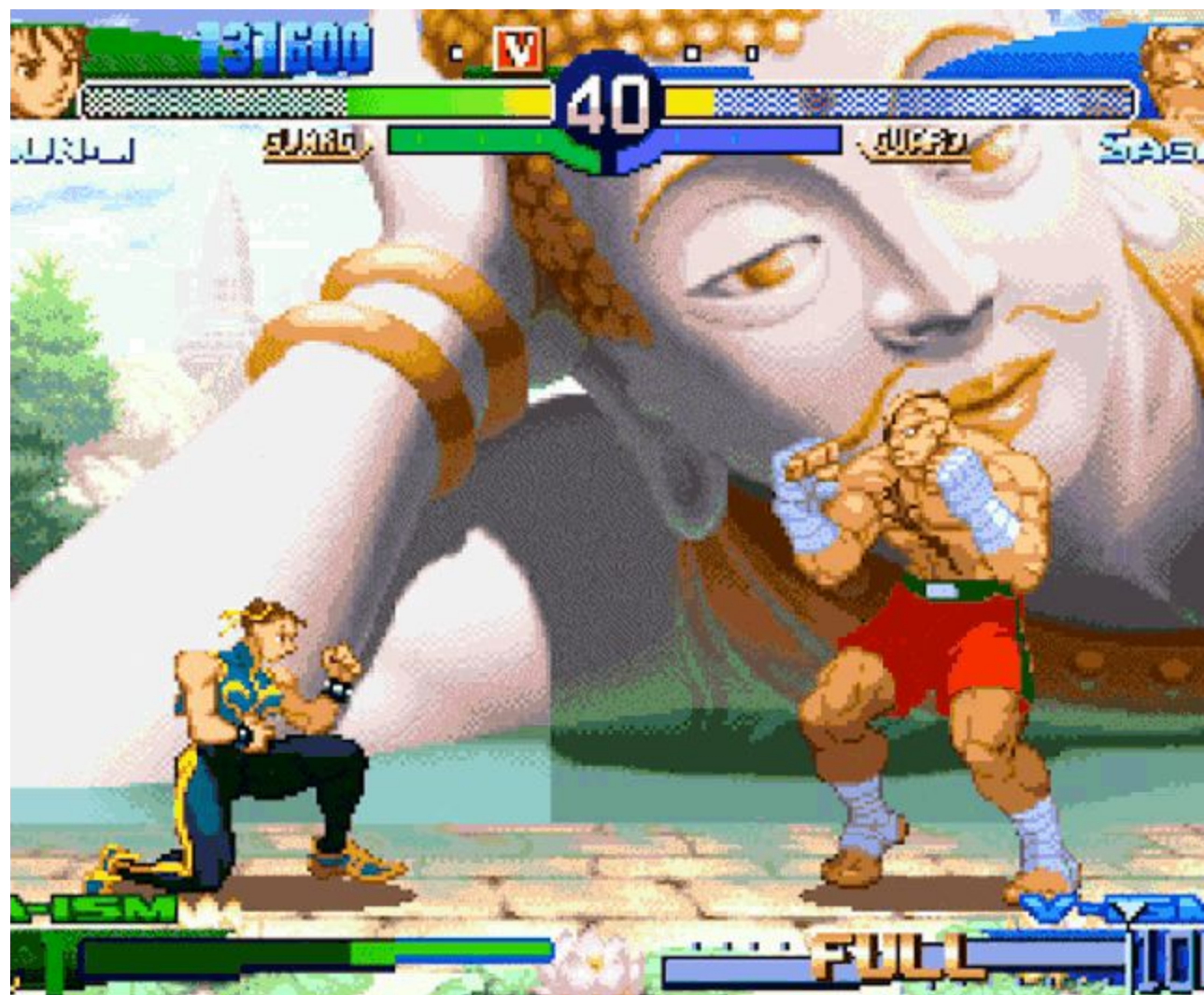- Keep in mind: Security patches appears **AFTER** exploits.

- Overwrite your site code with **trustworthy code.**

- >70% of succeed hacking attempts uses **outdated plugins/themes**.

The importance of PASSWORDS & 2FA

Factors of **AUTH**:

- Something you **are** (fingerprint, facial id,…).

- Something you **have** (cell phone, yubikey, …)

- Something you **know** (password, PIN, …).

+factors, +secure, +complex

GAME OVER

Any questions?

Des questions?

Fragen?

Nestor Angulo de Ugarte

Round 1! FIGHT! – Or how to survive against a malicious hacker

A lot is said about security, fences, plugins … But what does all this REALLY mean? Let's imagine that you are a "Street Fighter" or a "Mortal Kombat" character from those 80's video games and you have to face your particular fight against a bad guy.