



WordCamp Switzerland 2023
#WCCH

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.





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

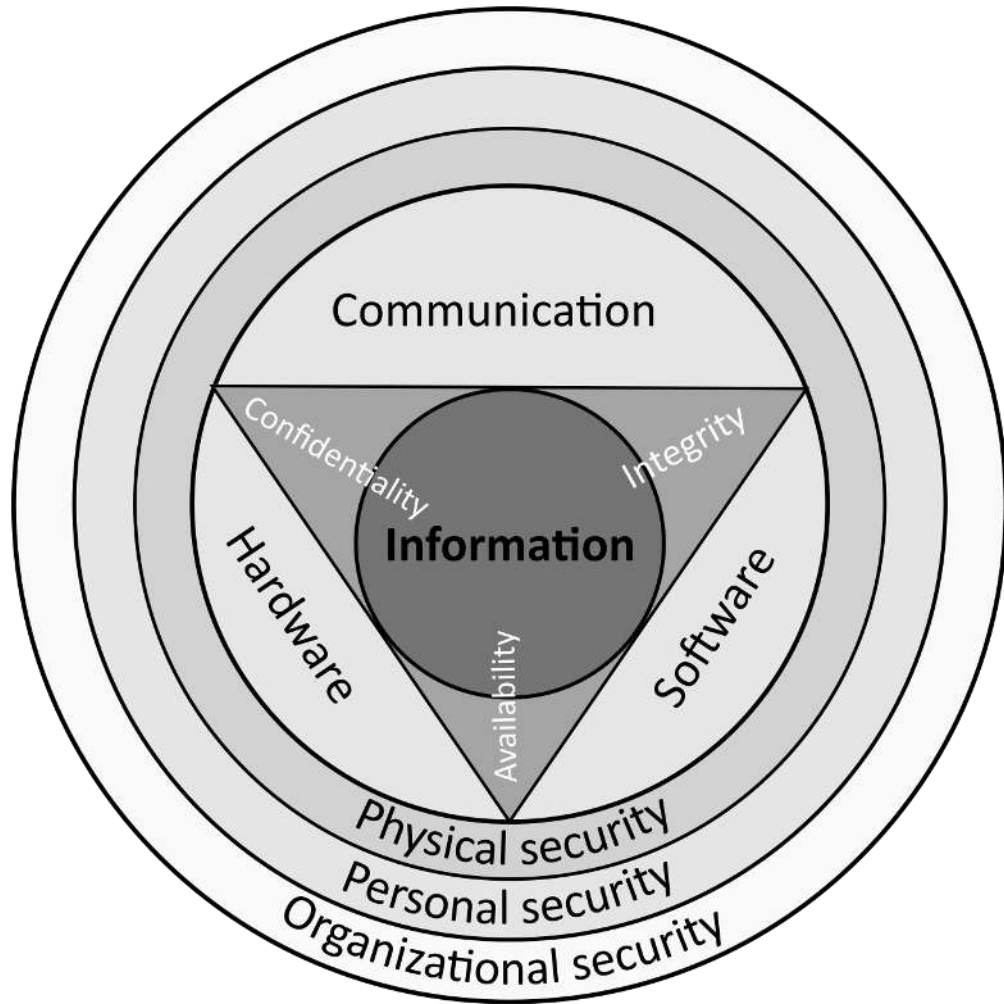
- Brand Ambassador: Patchstack



-  @pharar



What is Information Security





The Game

Your Fort



It represents your
WordPress Site

KO

ROUND 1
FIGHT!





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.

IP 300 NIN 50000

KO

78

DHALSIM



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 conventionalisms.



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





powerdrain

Hackers

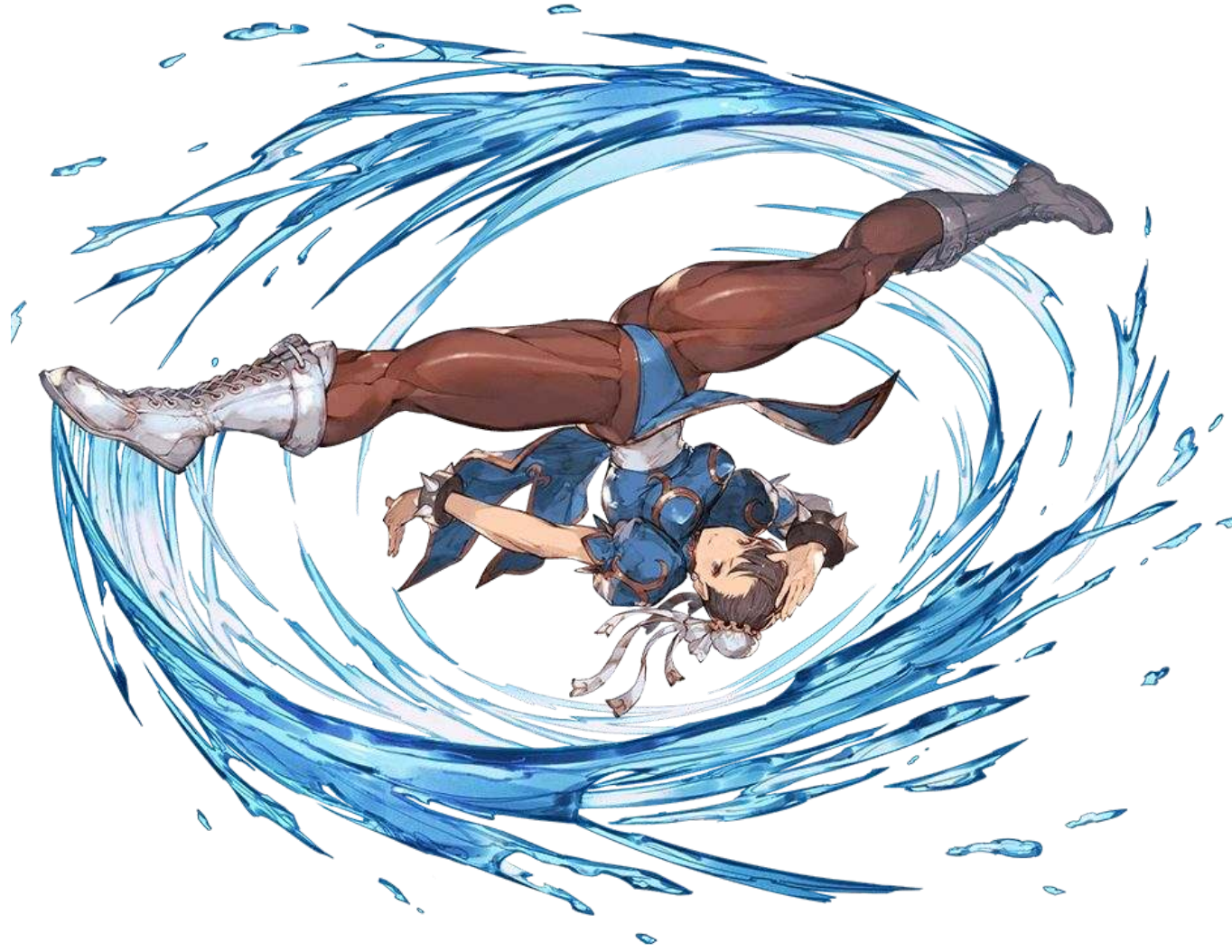
"On their own"

- Gray Hat Hackers
- Hacktivists



Anika

Our freelance
hacker.







Bad guys

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

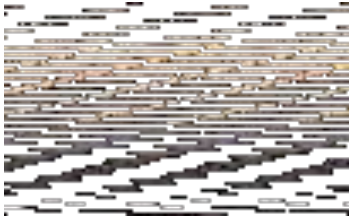
Cammy

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



Bruce

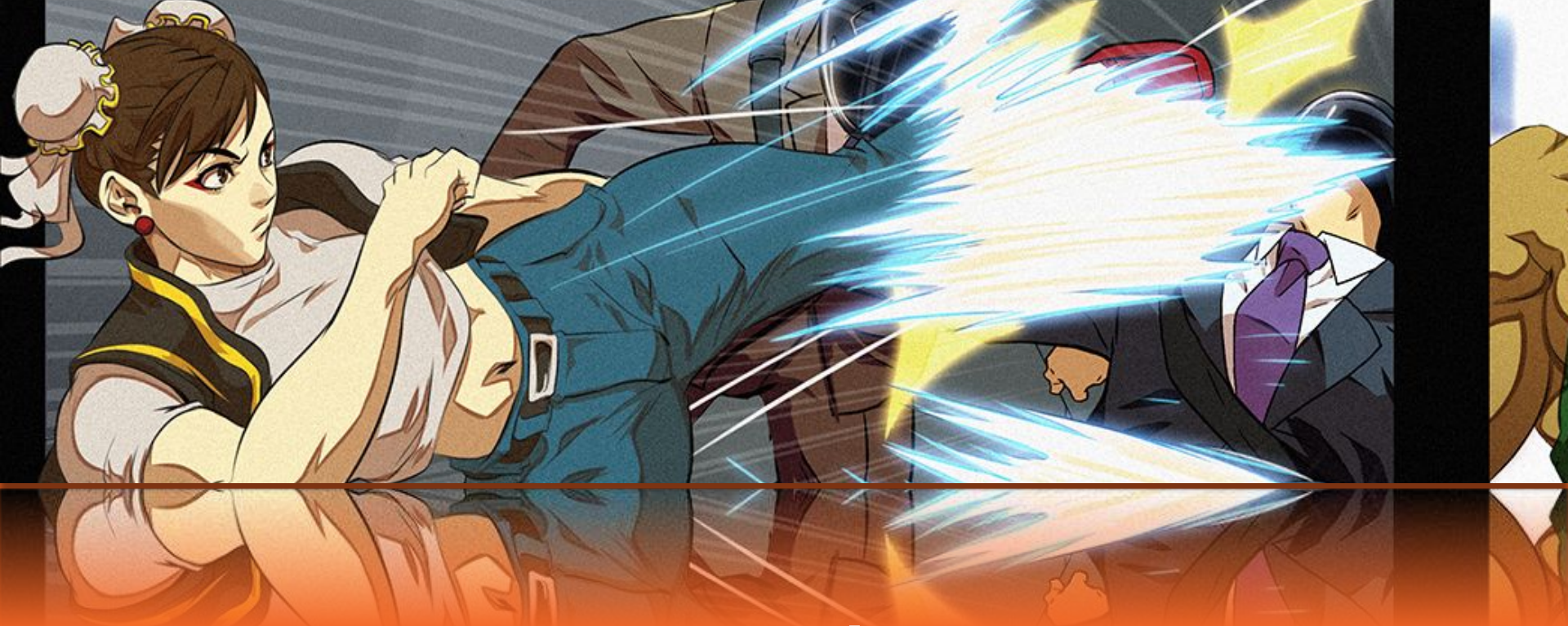
Our professional Black Hat Hacker.
Life bar: 50-70pts.



The General

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

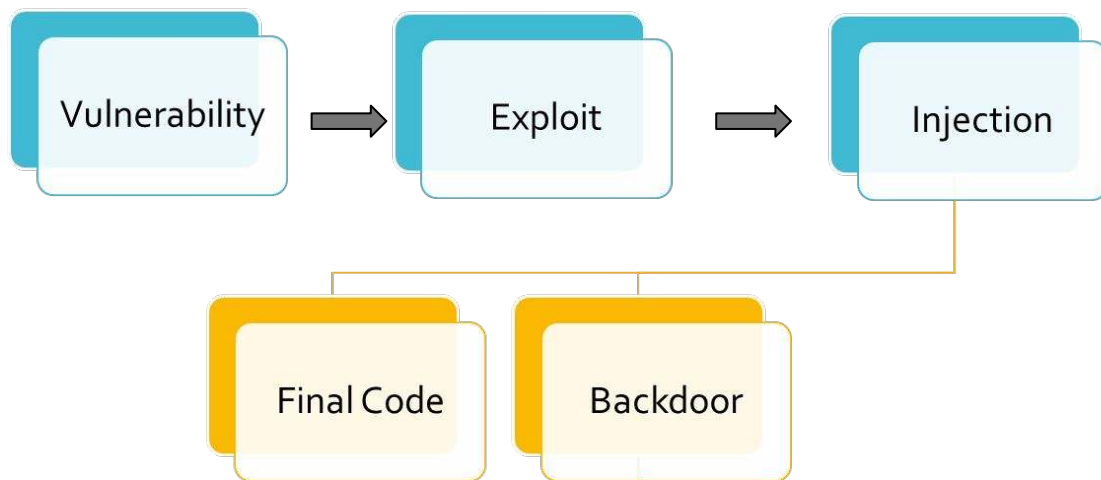


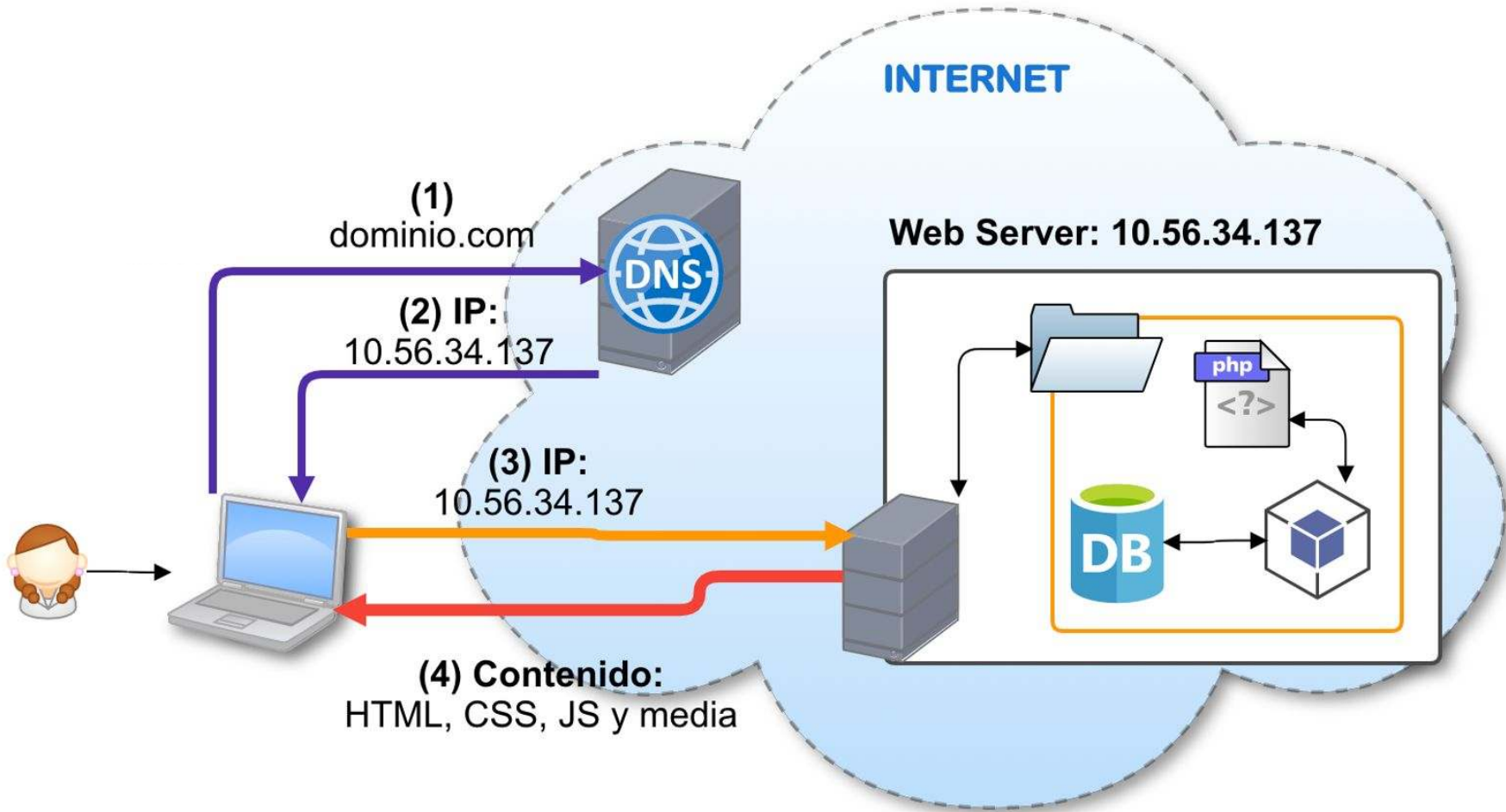



Attacks



How do you hack a WordPress site?





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

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

Remote site: /public_html/wp-content/plugins

Filename | Fi

Filename ^ | Filesize

- ..
- _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



- ..
- Login-wall-KiLxb
- Login-wall-NUJIF
- advanced-custom-fields
- all-in-one-wp-security-and-firewall
- alltimeusdfloatingin
- 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. 💡 <i>Wikipedia</i> : 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	<p>Try username/password combinations, informed or not.</p> <p>💡 <i>Wikipedia</i>: 10,000_most_common_passwords</p> <p>💡 haveibeenpwned.com</p>	Login	
XSS	Redirection (JS)	Reputation	



Google Membership Rewards



Congratulations

January 26 at 12:03am

Every Tuesday we select 10 lucky Apple users from our sponsors. This free gift is **exclusively** for our loyal members. It's our way of saying thank you for your continuous support for our product and service.

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!

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

Google Gift!

[redacted] (d!) from [redacted]
is just our way to thank you for your

Question 1 of 4: Who founded Google?

Bill Gates

Mark Zuckerberg

Larry Page

newsfile.club wants to





Show notifications






Block Allow

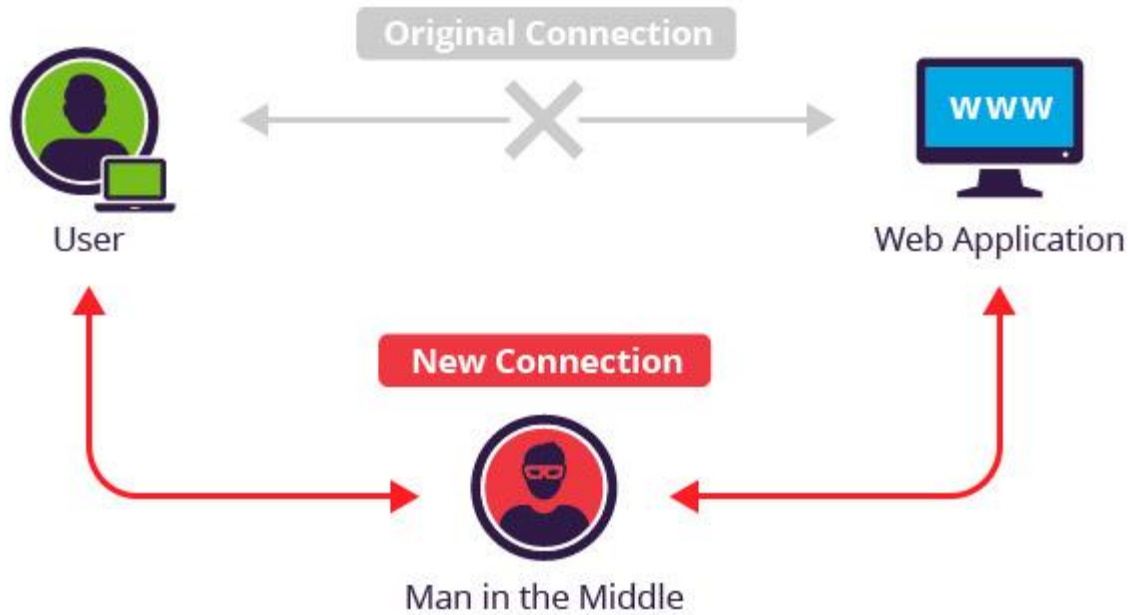


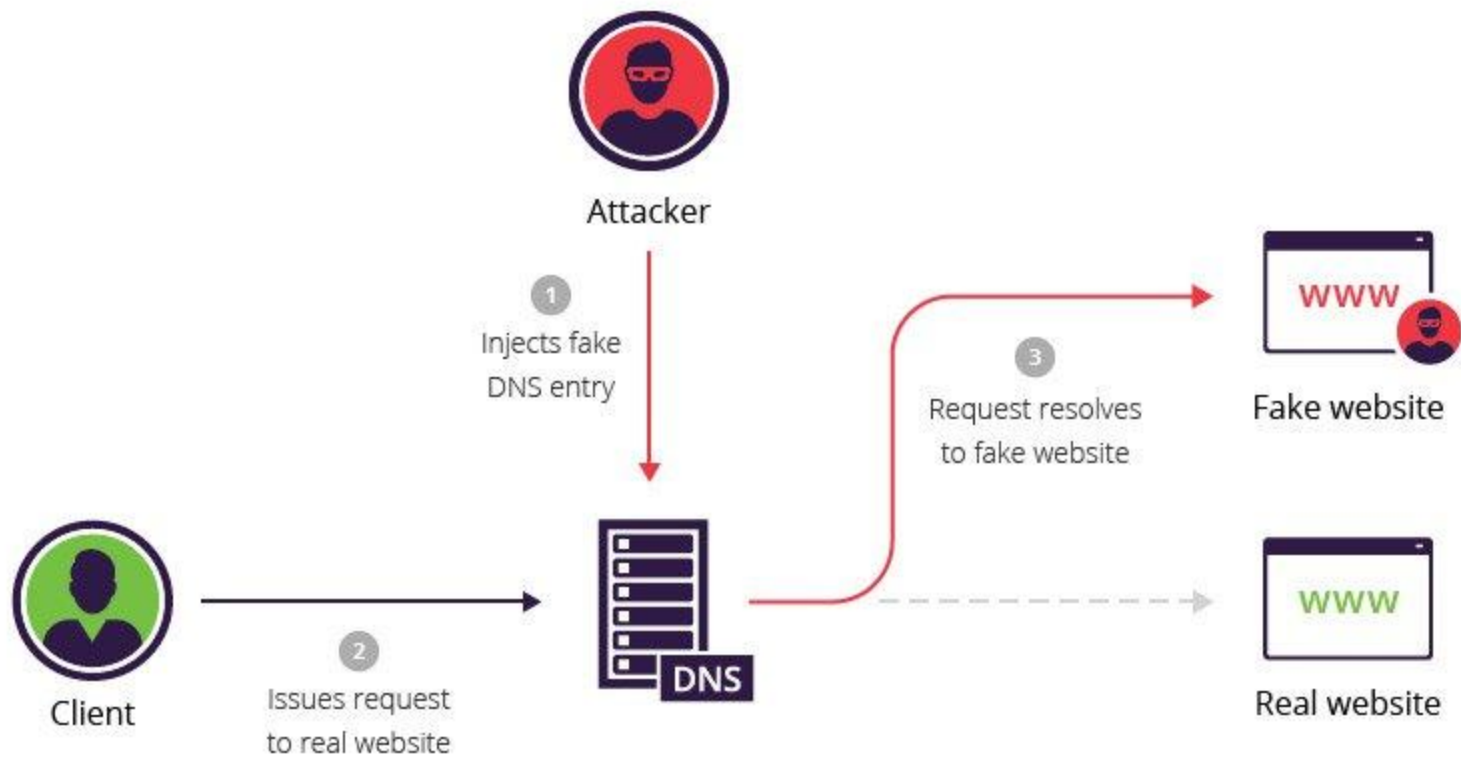
Haga clic en "Permitir" para confirmar que no es un robot









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. 💡 <i>Wikipedia</i> : 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. 💡 <i>Wikipedia</i> : 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	





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. 💡 <i>Wikipedia</i> : 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	

NORSE

ATTACK ORIGINS

COUNTRY
China
United States
Russia
Saudi Arabia
Netherlands
France
Moldova
South Korea
Brazil
Iceland

LIVE ATTACKS

TIMESTAMP	ORGANIZATION	LOCATION	IP	TARGET LOCATION	TYPE	PORT
2015-12-25 15:15:40.99	Beijing Huasheng Technologies Inc	Beijing, China	115.47.24.229	Russville, United States	http	80
2015-12-25 15:15:40.99	Beijing Huasheng Technologies Inc	Beijing, China	115.47.24.229	Russville, United States	http	80
2015-12-25 15:15:40.99	Beijing Huasheng Technologies Inc	Beijing, China	115.47.24.229	Russville, United States	http	80
2015-12-25 15:15:40.99	Beijing Huasheng Technologies Inc	Beijing, China	115.47.24.229	Russville, United States	http	80
2015-12-25 15:15:40.99	Beijing Huasheng Technologies Inc	Beijing, China	115.47.24.229	Russville, United States	http	80
2015-12-25 15:15:40.99	Beijing Huasheng Technologies Inc	Beijing, China	115.47.24.229	Russville, United States	http	80
2015-12-25 15:15:40.99	Beijing Huasheng Technologies Inc	Beijing, China	115.47.24.229	Russville, United States	http	80
2015-12-25 15:15:40.99	Beijing Huasheng Technologies Inc	Beijing, China	115.47.24.229	Russville, United States	http	80
2015-12-25 15:15:40.99	Beijing Huasheng Technologies Inc	Beijing, China	115.47.24.229	Russville, United States	http	80
2015-12-25 15:15:40.99	Beijing Huasheng Technologies Inc	Beijing, China	115.47.24.229	Russville, United States	http	80








ATTACK TARGETS









COUNTRY
United States
Saudi Arabia
United Arab Emirates
Philippines
Liechtenstein
France
Russia
Taiwan
Cyprus
Mexico

ATTACK TYPES



SERVICE	PORT
http	80
https	443
microsoft-ds	445
telnet	23
http-alt	8080
unknown	2048
unknown	2049
netbios-dgm	138

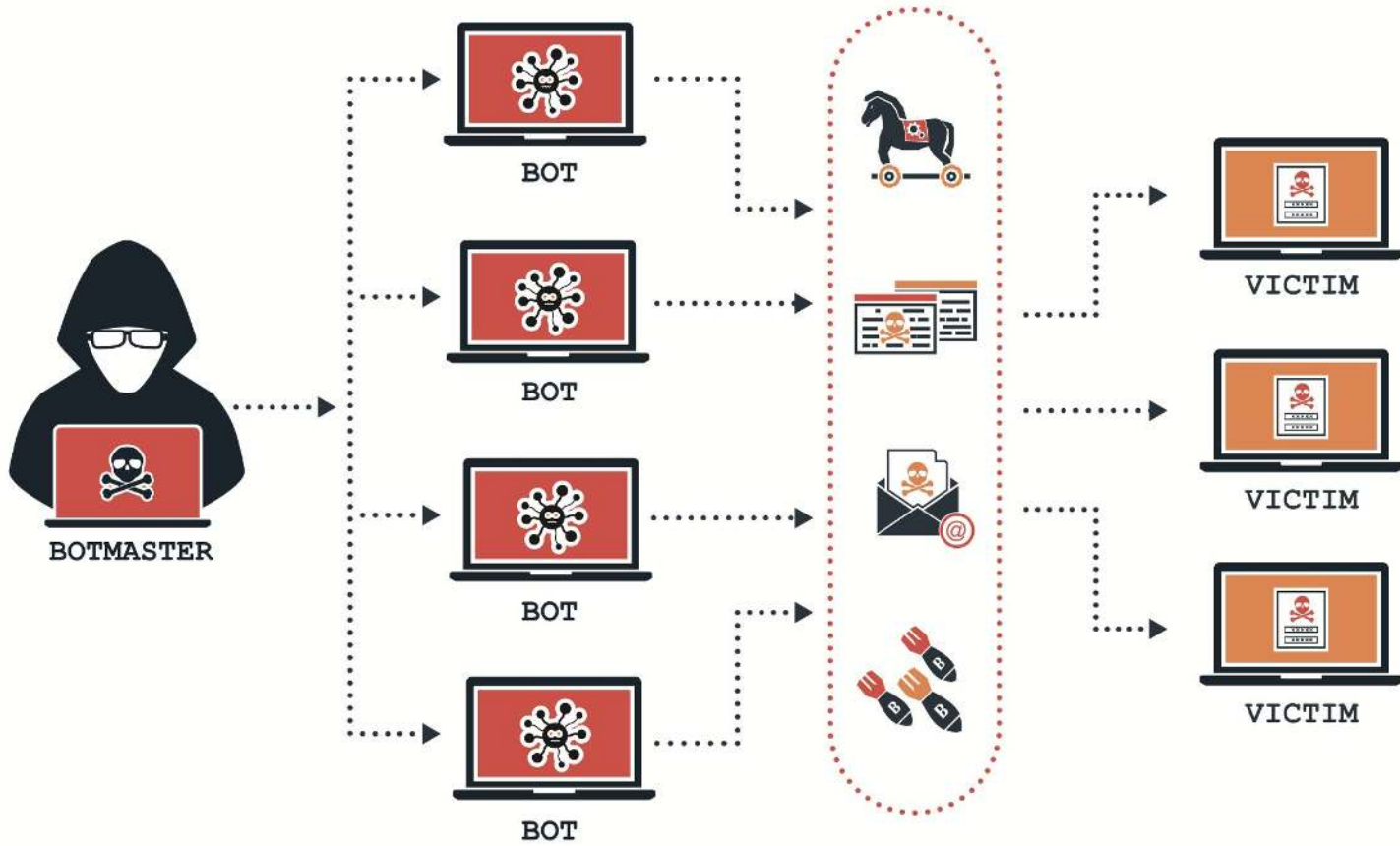





Attack	Description	Categorie	Level
Phishing / Spam	Injection or use of, to capture information.	Reputation, Login	
Brute Force / Dictionary	Try username/password combinations, informed or not. 💡 <i>Wikipedia</i> : 10,000_most_common_passwords 💡 haveibeenpwned.com	Login	
XSS	Redirection (JS)	Reputation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

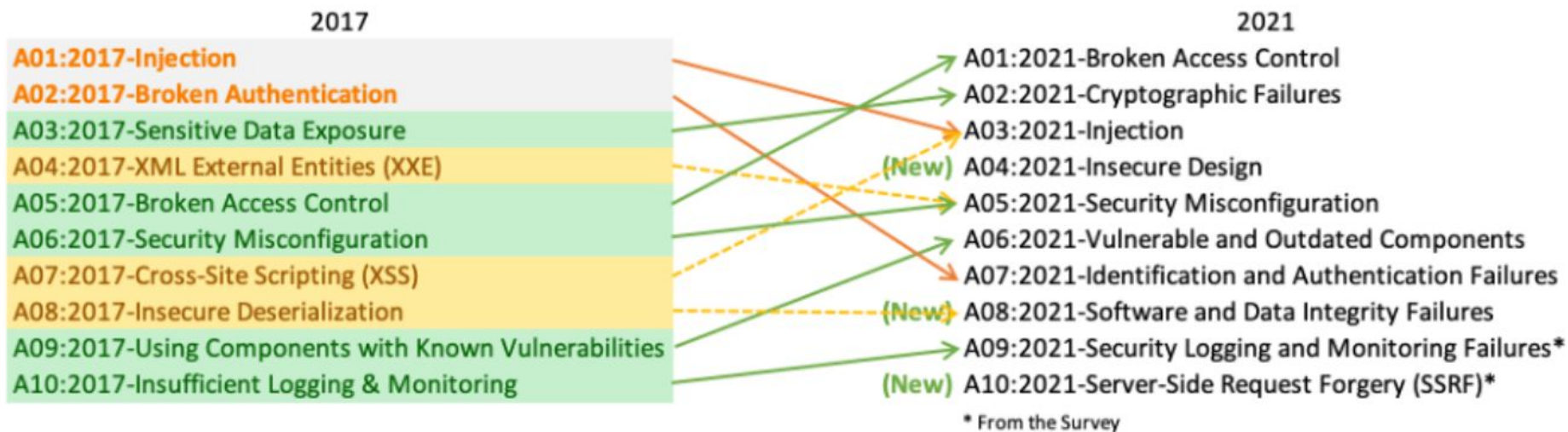


Attack	Description	Categorie	Level
Cryptomining	Use of third-party infrastructure to mine crypto	Resources	
BotNode	Use of the infected site (zombie) as an attack platform.	Communications, Files	
Cross-site Contamination	From a hacked site or a backup, infect other sites	Files, database	

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. 💡 <i>Wikipedia</i> : 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.



Two futuristic humanoid robots are shown from the waist up. The robot on the left is primarily red and white, with glowing blue lights on its chest and joints. The robot on the right is primarily white and black, also with glowing blue lights. Both robots have a human-like face with visible internal components and are posed in a similar, slightly forward-leaning stance. The background is a light blue gradient.

And what about the AI?

AI Conundrum



Defenses



Attack	Defense(s)	Category
--------	------------	----------

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



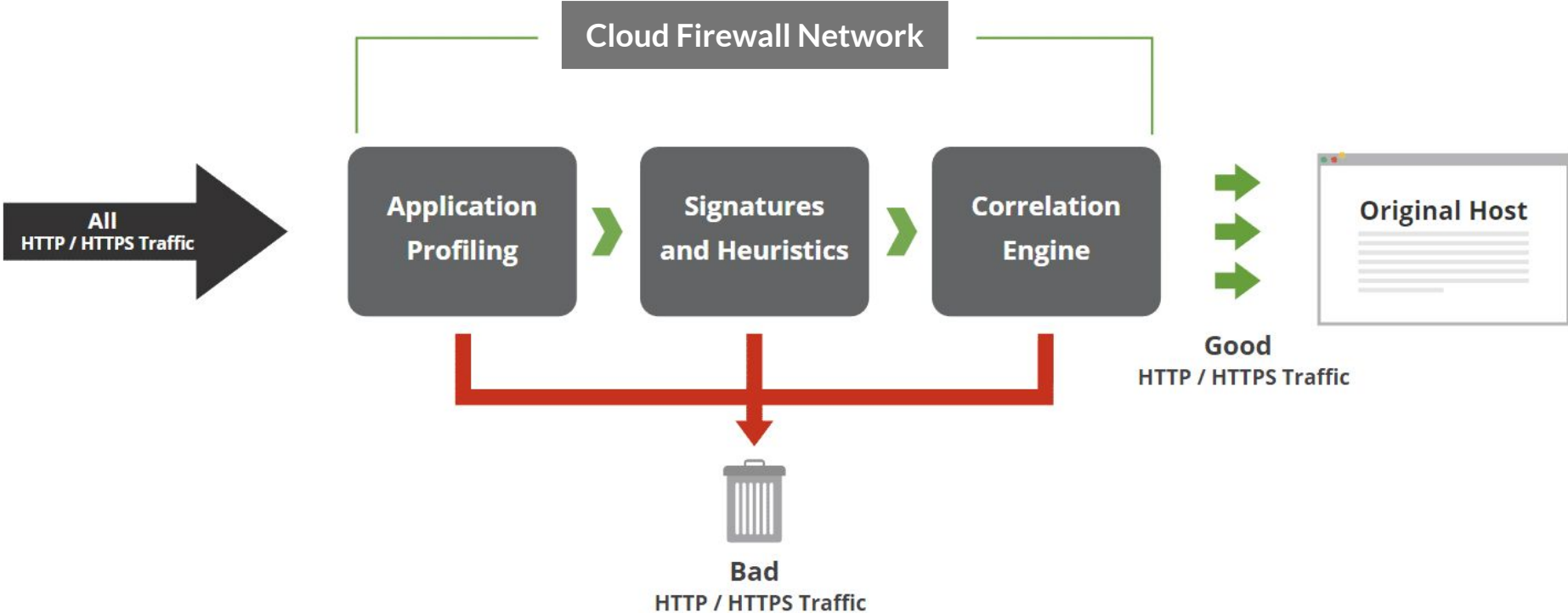
Attack	Defense(s)	Category
Phishing / Spam	Habilidad, Frontend monitor	Reputation, Login
Brute Force / Dictionary	WAF, Limit login plugin	Login

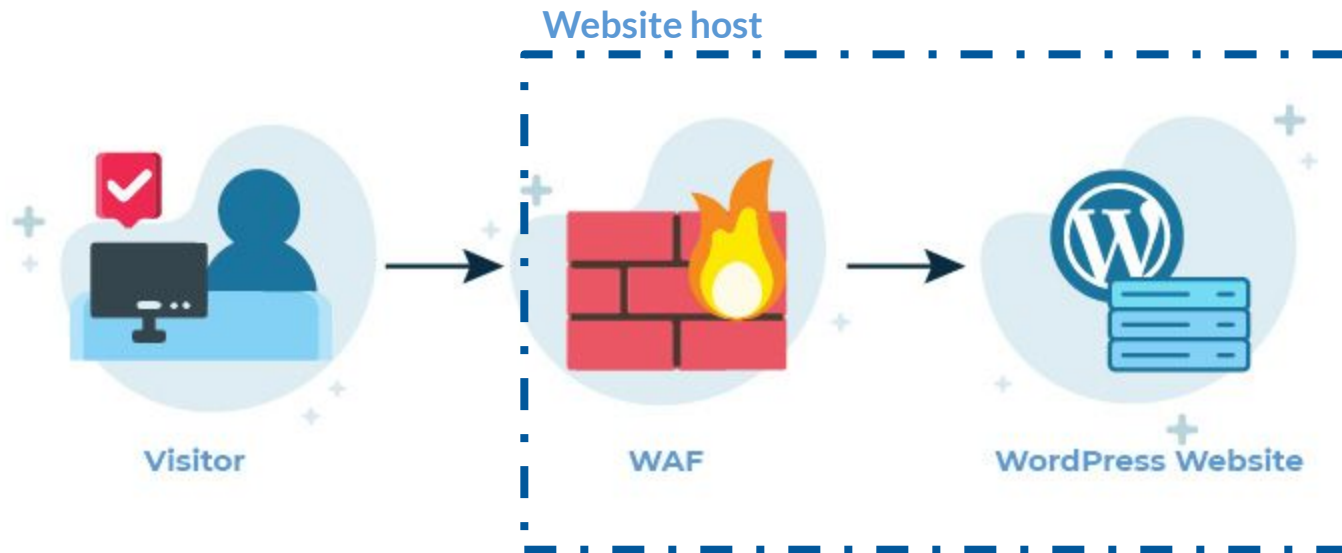




Website Application Firewall (WAF)

Protect and Speed Up Your Website





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

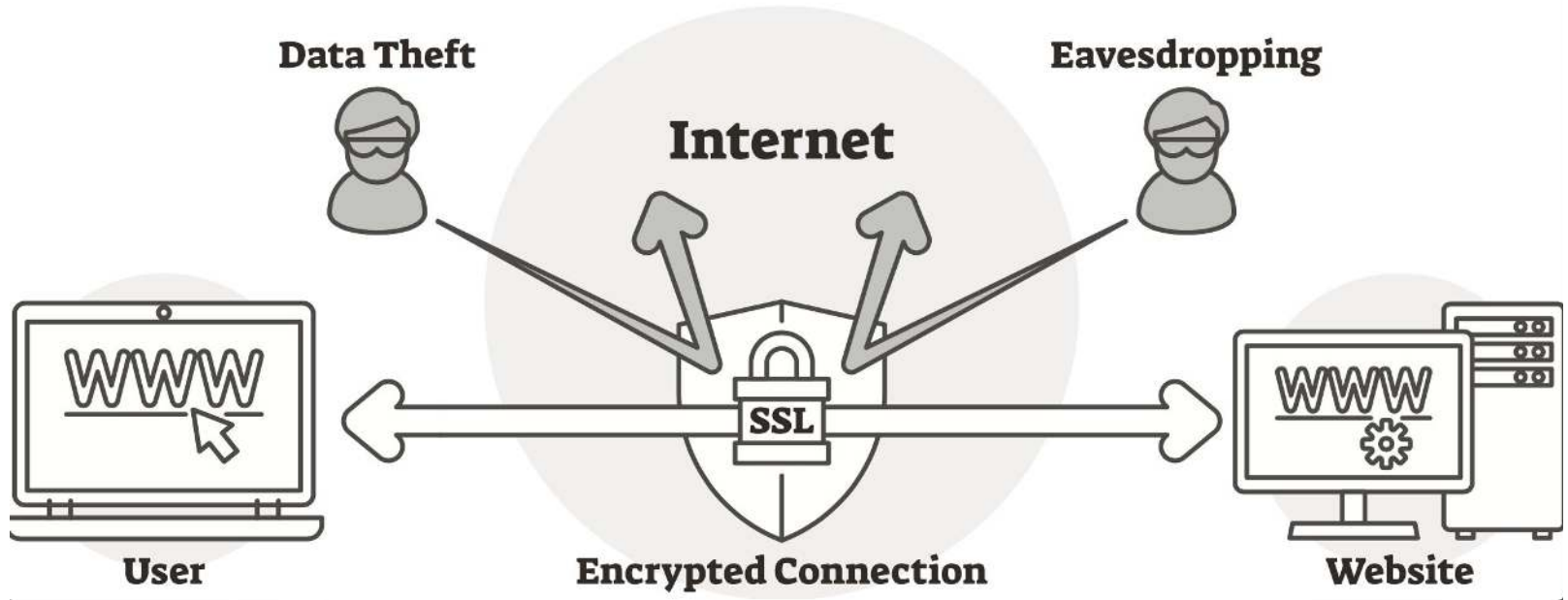


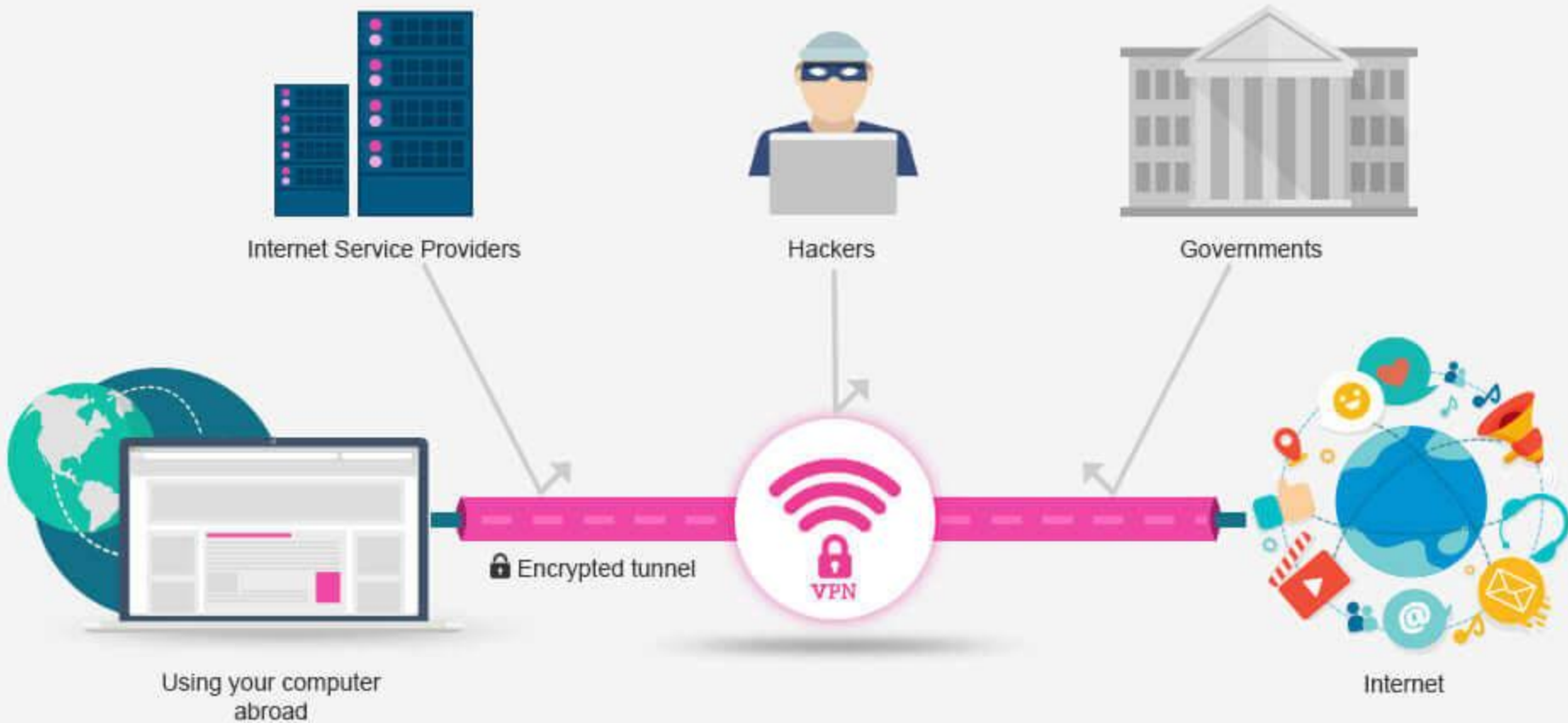
Attack	Defense(s)	Category
Phishing / Spam	Habilidad, Frontend monitor	Reputation, Login
Brute Force / Dictionary	WAF, Limit login plugin	Login
XSS	WAF, Files integrity scanner	Reputation
New vulnerabilities	WAF, maintenance	Research
Man in the Middle	SSL/TLS	Communications



SSL

Secure Sockets Layer





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/TLS	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/TLS	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/TLS	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/TLS	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/TLS	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/TLS	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/TLS	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/TLS	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/TLS	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/TLS	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 ○ simultaneously

Dragon Punch
→↘ and ○ simultaneously

Cyclone Kick
↓↙ and ○ 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 ○ simultaneously

Dragon Punch
→↘ and ○ simultaneously

Cyclone Kick
↓↙ and ○ 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 ○ many times rapidly

Killer Head Ram
hold ← then → and ○ 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 ○ many times rapidly

Spinning Bird Kick
hold ↓ then ↑ and ○ 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 ○ many times rapidly

Rolling Attack
hold ← then → and ○ simultaneously

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

Sure Killing Technique

(While facing right)

Double Lariat
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 ○ simultaneously

Somersault Kick
hold ↓ then ↑ and ○ simultaneously



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 ○ simultaneously

Yoga Blast
←↘ and ○ simultaneously



BALROG
U.S.A.

He has defeated all challengers in the boxing ring.

Sure Killing Technique

(While facing right)

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

Dashing Straight Punch
hold ← then → and ○ 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 ○ simultaneously

Barcelona Attack
hold ↓ then ↑ and ○ simultaneously



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 ○ simultaneously

Grand Tiger Shot
↓↘ and ○ 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)

Psycho-crusher
hold ← then → and ○ simultaneously

Double knee press
hold ← then → and ○ simultaneously

Remember!

 **COST** Web down



 **COST** Web hacked

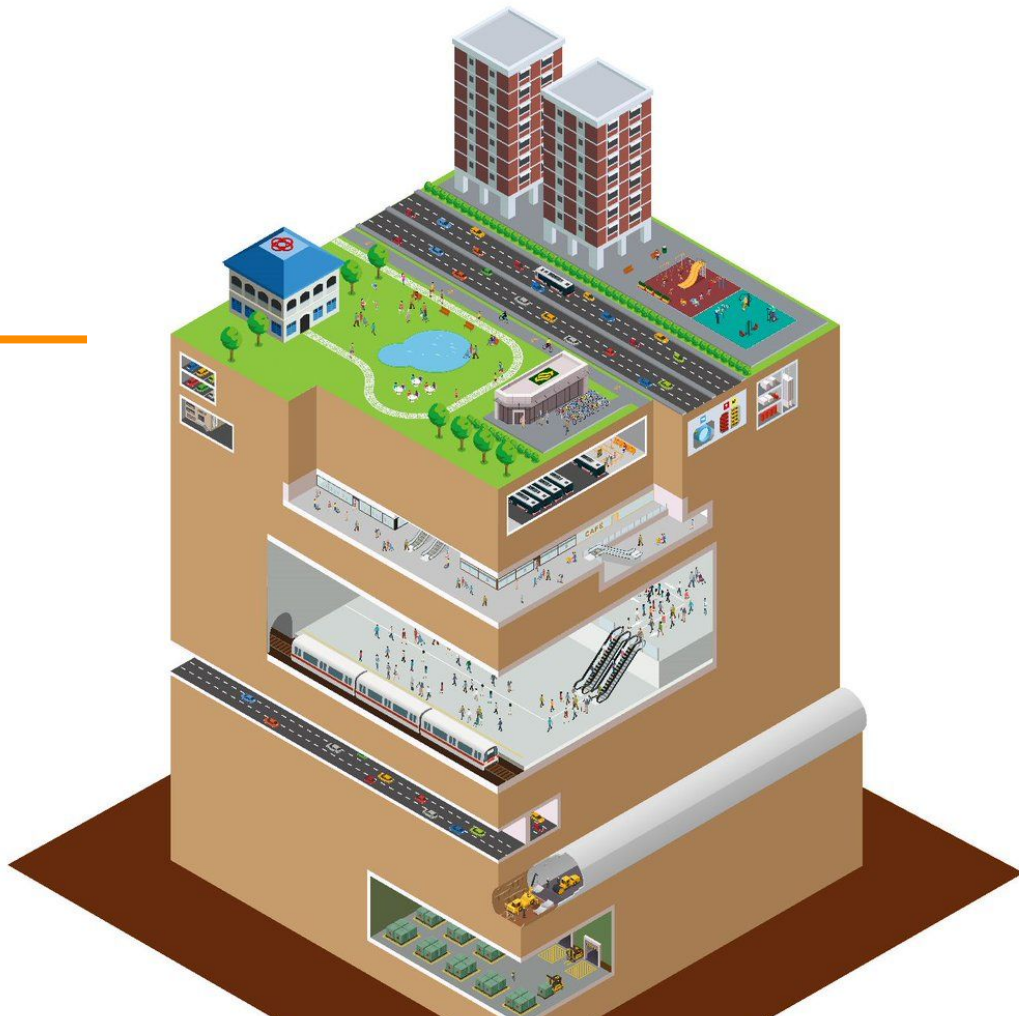
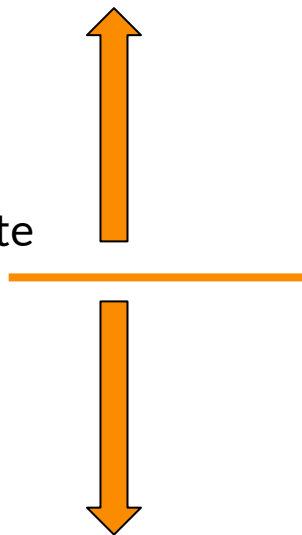
Site Owner

- App
- Data
- Security of the site

Hosting provider

- Networks
- Hardware
- SO
- Virtualization
- Security

Security Liability



WordPress Security

[https://wordpress.org/
about/security/](https://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



❖ **Vulnerabilities scanner + internal WAF**

- Patchstack

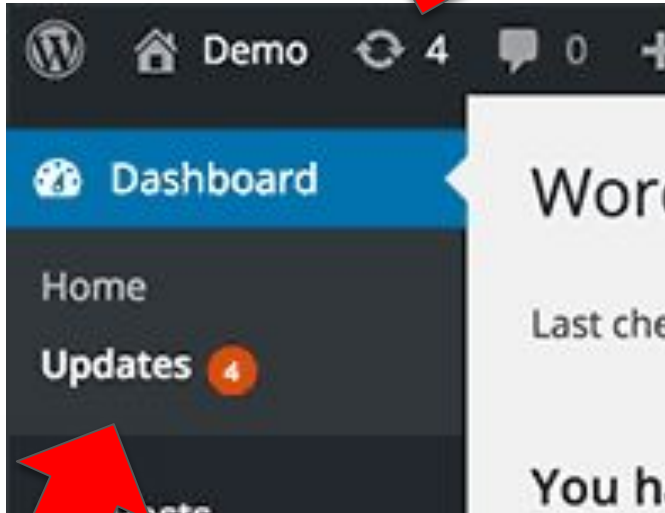
❖ **Hosting**

- SSL/TLS
- Support + BackUps
- Managed plans

❖ **Backups**

- VaultPress (Jetpack)
 - o BlogVault
 - o UpDraft

The importance of UPDATING



- **Security patches**



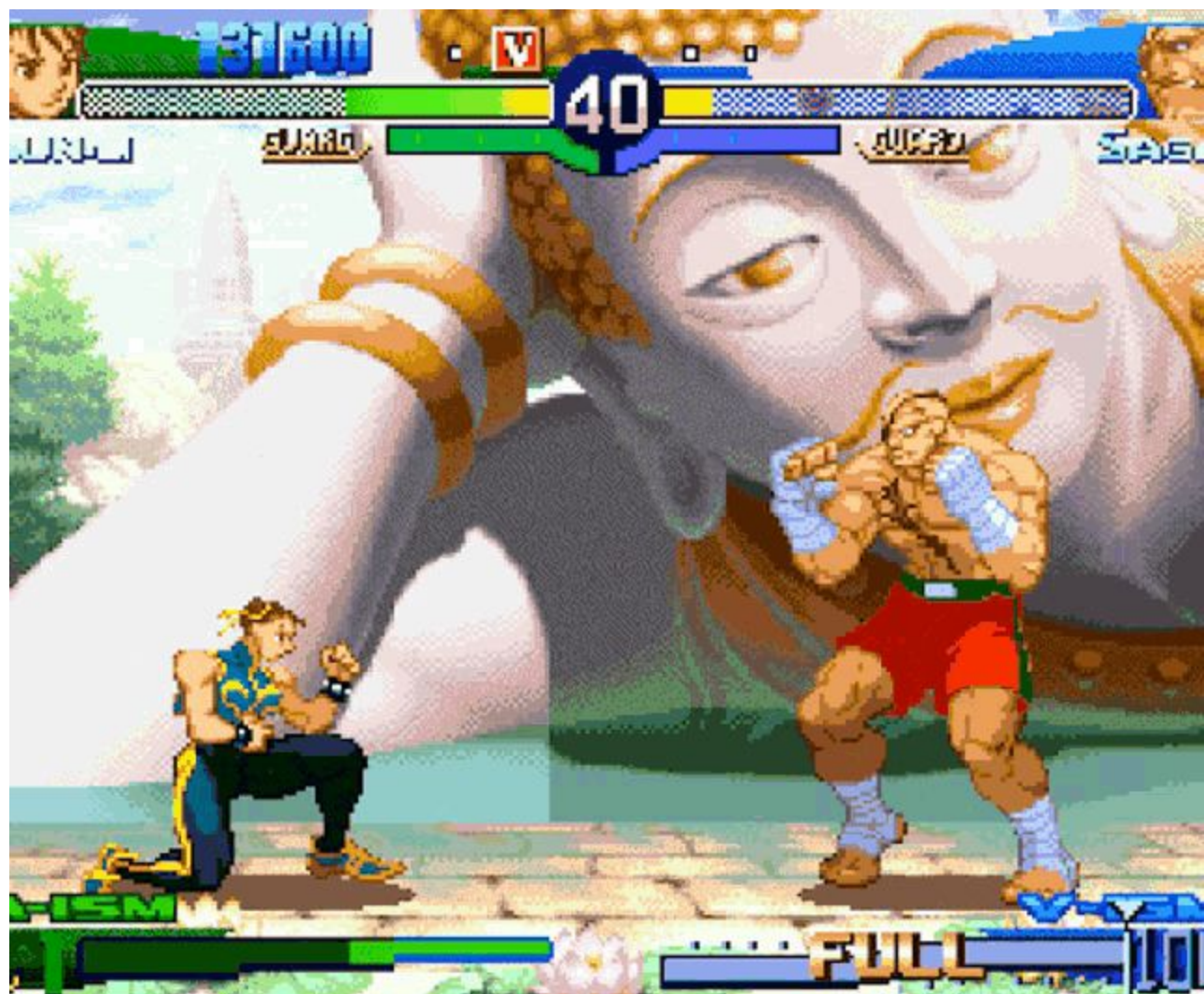
- Keep in mind: Security patches appears **AFTER** exploits.
- Overwrite your site code with **trustworthy code**.
- >70% of succeed hacking attempts uses **outdated plugins/themes**.

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, ...).







GAME OVER



A black and white photograph showing the back of a person wearing a dark t-shirt. The t-shirt has the text "Everybody needs a hacker" printed on it in a white, sans-serif font. The person's hair is visible at the top of the frame. The background is out of focus, showing some light sources. The entire image is framed by a thin white border and set against a solid orange background.

Everybody needs a hacker



WordCamp Switzerland 2023
#WCCH

Any questions?

Des questions?

Fragen?





WordCamp Switzerland 2023
#WCCH

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.

