Web vulnerability in 2021: large scale inspection, findings, analysis and remedies

Prof.Borka Jerman Blažič

International postgraduate school Jožef Stefan and Institute Jožef Stefan

Ljubljana, Slovenia

IJS

IARIA

MEDNARODNA PODIPLOMSKA ŠOLA JOŽEFA STEFANA
SLOVENIJA
LJUBLJANA
2004

The web site presence and content design

- Since its appearance in the early 1990s, the World Wide Web has evolved from a platform to access text and other media to a framework for running complex web applications.
- These applications appear in many forms, from small home made to large scale commercial services (Google Docs, Twitter, Facebook)
- The system that enable and manage the web site content is known as Web Content Management System
- WordPress is a free open-source content management system based on PHP scripting language and MySQL database.
- Word Press is easy to be learnt and used. It allows users to create websites. even without knowing the HTML or PHP language, which means tha also suitable for the beginners.

Word Press is the most popular WCMS system on the Internet

1. WordPress (WP) appeared on the web in 2003, when it was introduced to the public as a simple blogging platform where users could write text, post images and link to other websites.

2. WP is due to its ease of use is one of the most widespread WCMS.

3. The popularity of WP lays in the easiness in setting web pages for particular website, the low cost of use and maintenance.

4. The abundance of plug-ins for developing very different type of services and scenarios, like blogs, social network applications, webmail service, banking, e-commerce, educational services contribute to its popularity.

5. WordPress is applied for the creation of websites of companies like NBC, CNN, TED, New York Times, Forbes, eBay, Best Buy, Sonny, UPS, CBS Radio, TechCrunch and others

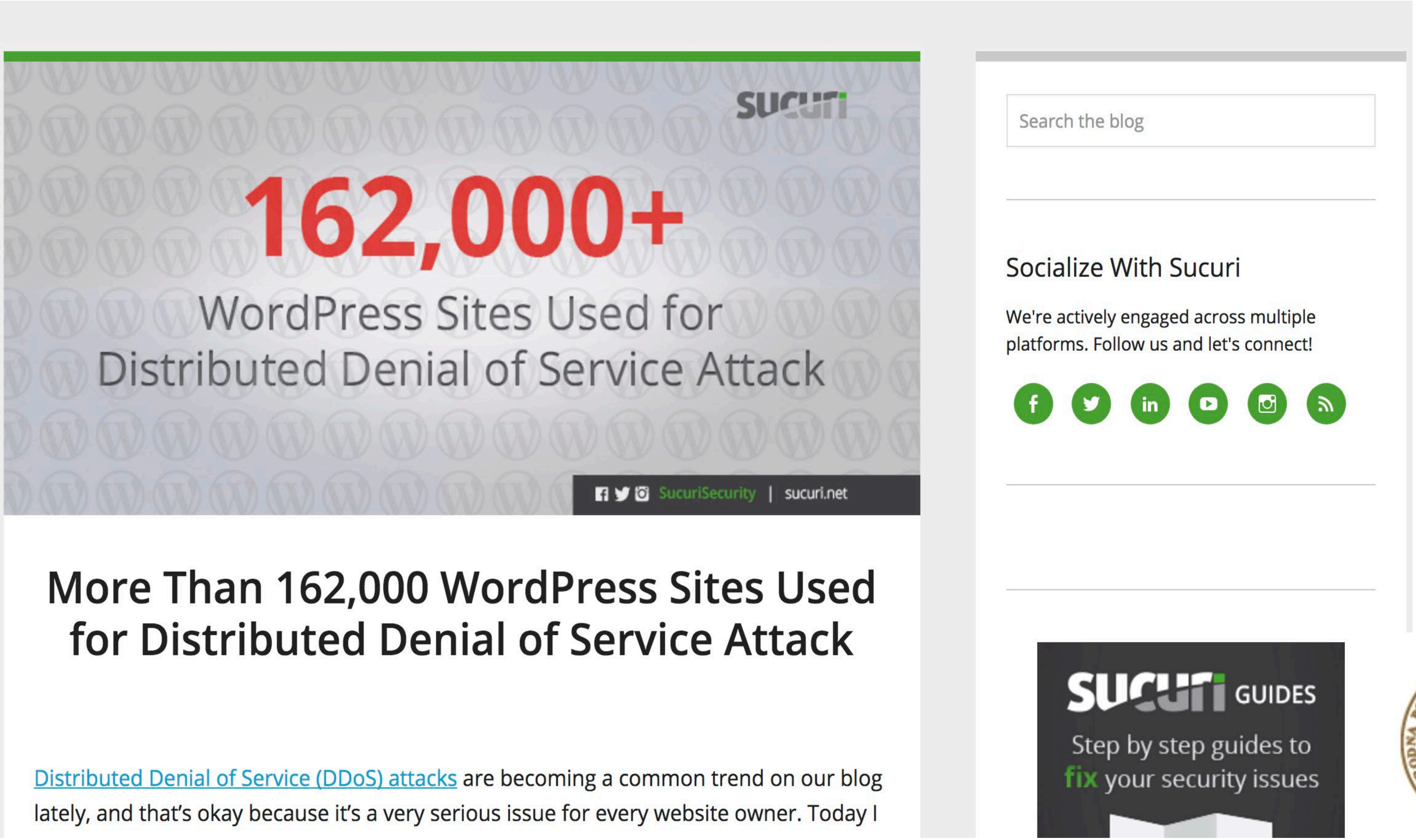
Some differences regarding Possibilities of an attack among the applications provided on the client side (the browser) and the server side of the Web service

The attacks and the vulnerabilities are happening mainly on the server side.

The server, the WCMS and associated plug-ins are the focus of the web attacs

Basis of Comparison	Client-side scripting	Server-side scripting
Use	Works on the frontend and is visible among users	It works in the backend, which cannot be seen at the end of the client
Processing	Does not need interaction with the server	Requires server interaction
Supported Languages	HTML, CSS, JavaScript, etc.	PHP, Python, etc.
Running	It runs on user’s computer	It runs on web server
Execution	The scripting process for the server side is done on remote computer and hence the response is comparatively slower than the client side one	The scripting process of client server is executed on a local computer and thus the response is comparatively quicker when compared to server-side scripting
Database Connection	Does not connect to the databases	Connects to the databases that are already present in the server
Access to Files	No access to all the files on the server	Access to all the files on the server
Source Code	Source code is visible to user	Source code is not visible to user
Security	Less secure as the scripts are usually not hidden from the client end	Relatively secure, but more secure than client-side scripting as the server-side scripts are usually hidden from the client end

Table 1: Client-side and server-side comparison.


sucuri
162,000+
WordPress Sites Used for
Distributed Denial of Service Attack
SucuriSecurity | sucuri.net

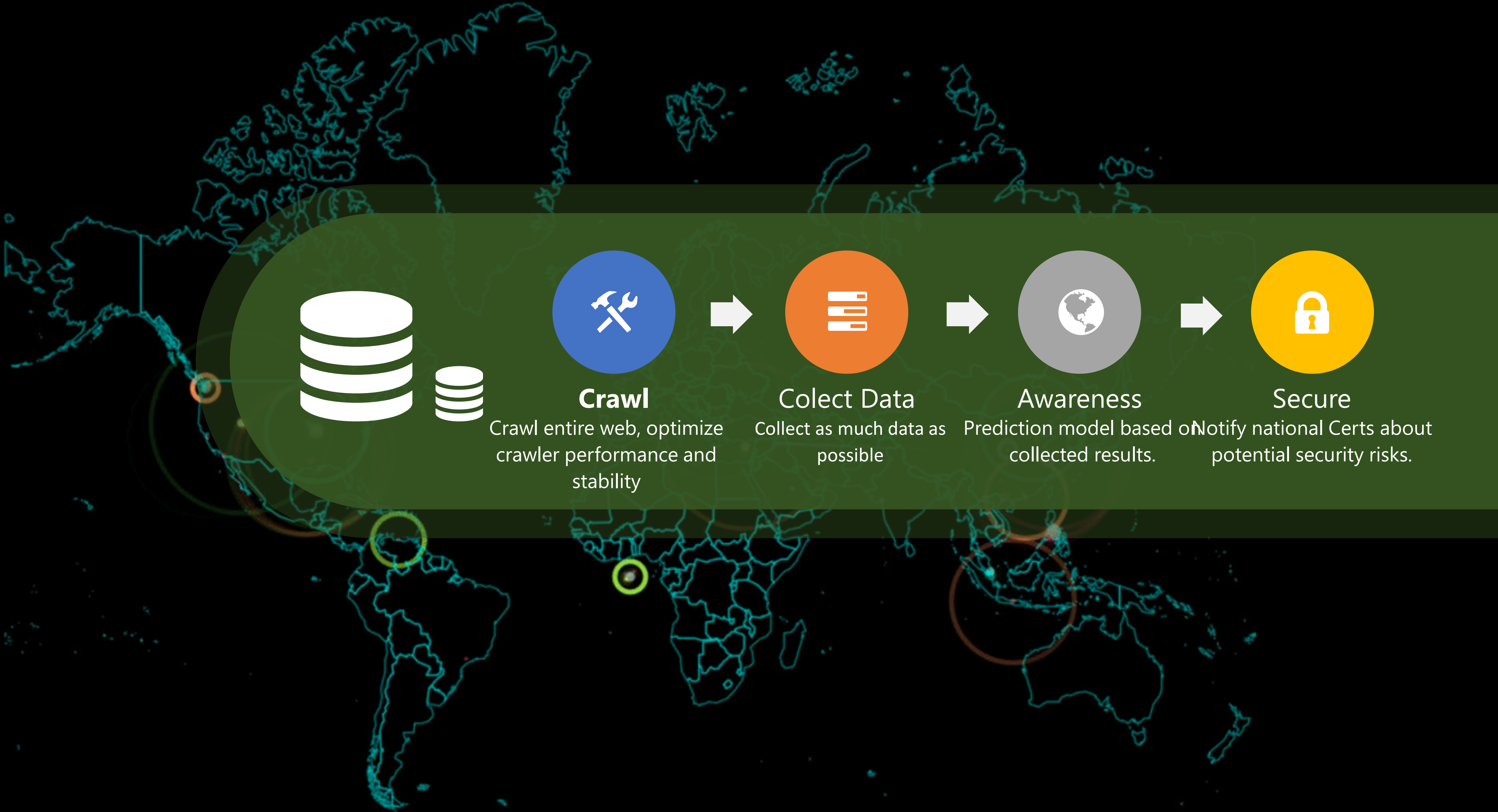
More Than 162,000 WordPress Sites Used for Distributed Denial of Service Attack

Distributed Denial of Service (DDoS) attacks are becoming a common trend on our blog lately, and that's okay because it's a very serious issue for every website owner. Today I

Search the blog

Socialize With Sucuri

We're actively engaged across multiple platforms. Follow us and let's connect!



Crawl

Crawl entire web, optimize crawler performance and stability

Colect Data

Collect as much data as possible

Awareness

Prediction model based on collected results.

Secure

Notify national Certs about potential security risks.

WEB site vulnerabilities enabling the attacks to be successful

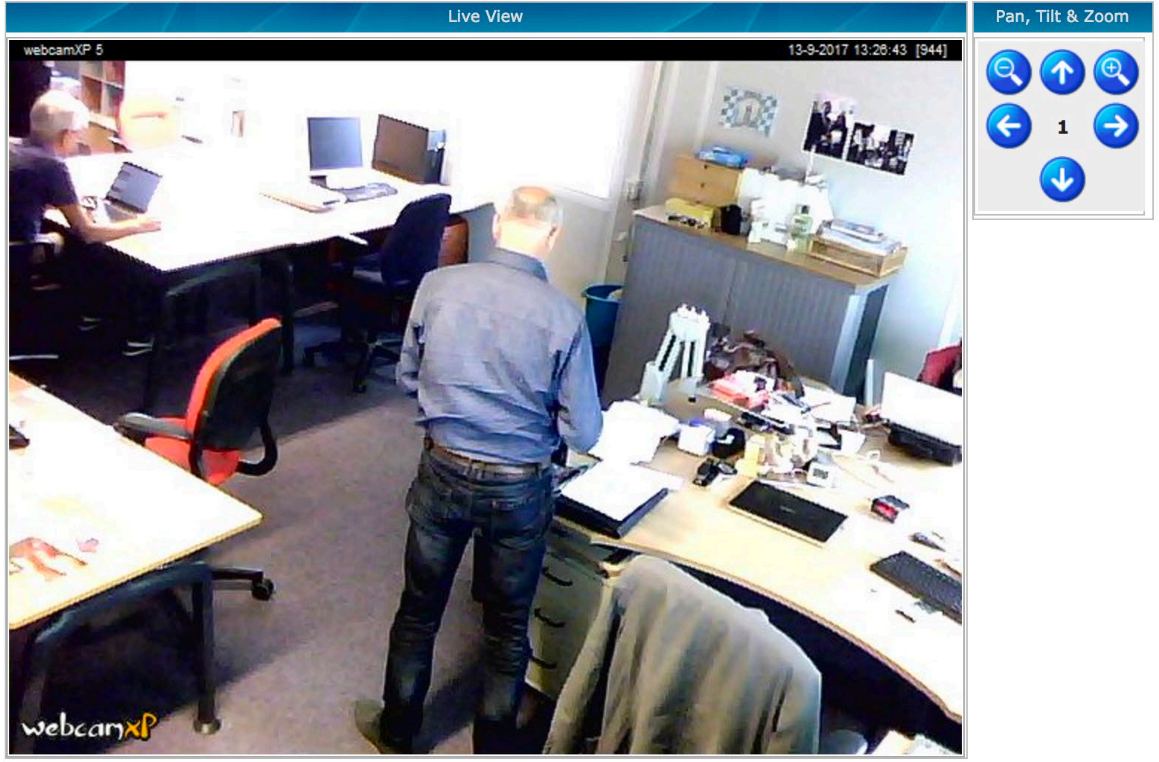
Web site security can be inspected on two different ways:
Open source and Close source

Other types of inspection are dynamic (on going with crawlers) and static where source code is required to be provided by the owner

Top vulnerabilities of a web site according to Open Web Application Security Project

A1	Injection
A2	Broken Authentication and Session Management
A3	Sensitive Data Exposure
A4	XML External Entities (XXE)
A5	Broken Access Control
A6	Security Misconfiguration
A7	Cross-Site Scripting XSS
A8	Insecure Deserialization
A9	Using Components with Known Vulnerabilities
A10	Insufficient Logging & Monitoring

Crawlers on the Internet



- Use of crawling tools is very popular, but they are not always welcomed
- They are accepted but as well denied to access to web site by the owners

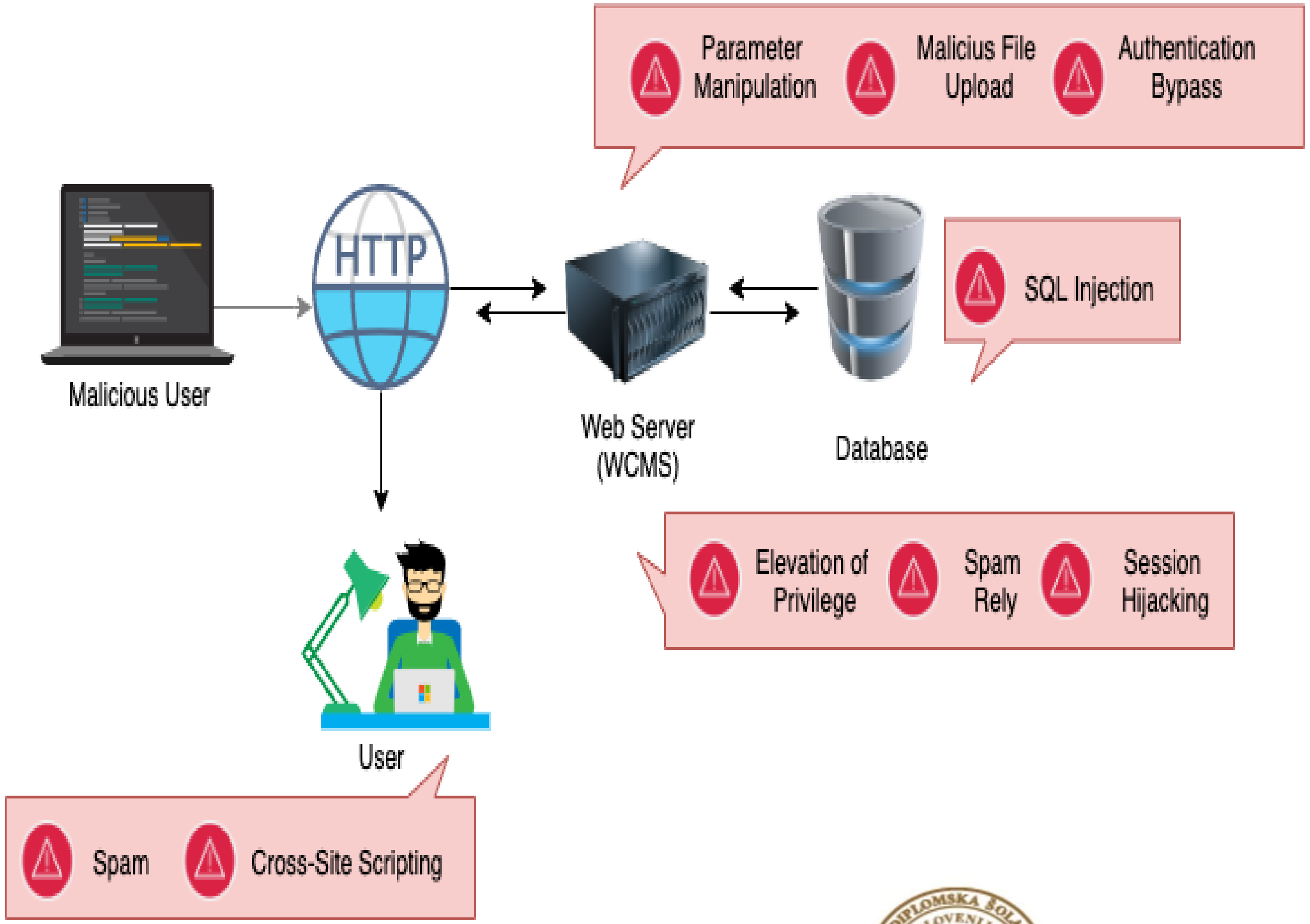
Some owners is hiding the version of the used SW release, with an idea that this protect the web site from an attack

Services for crawling the internet 24/7 in order to provide the latest Internet Intelligence, are located all over the world.

Services for crawling are used around the world by researchers, securit professionals, large enterprises, CERTs and everybody in between.

They are used mainly in inspecting servers instead of the content they like WMCS and the applied data

How hacked web sites are compromised



Parameter Manipulation

Malicius File Upload

Authentication Bypass

Malicious User

HTTP

Web Server (WCMS)

Database

SQL Injection

Elevation of Privilege

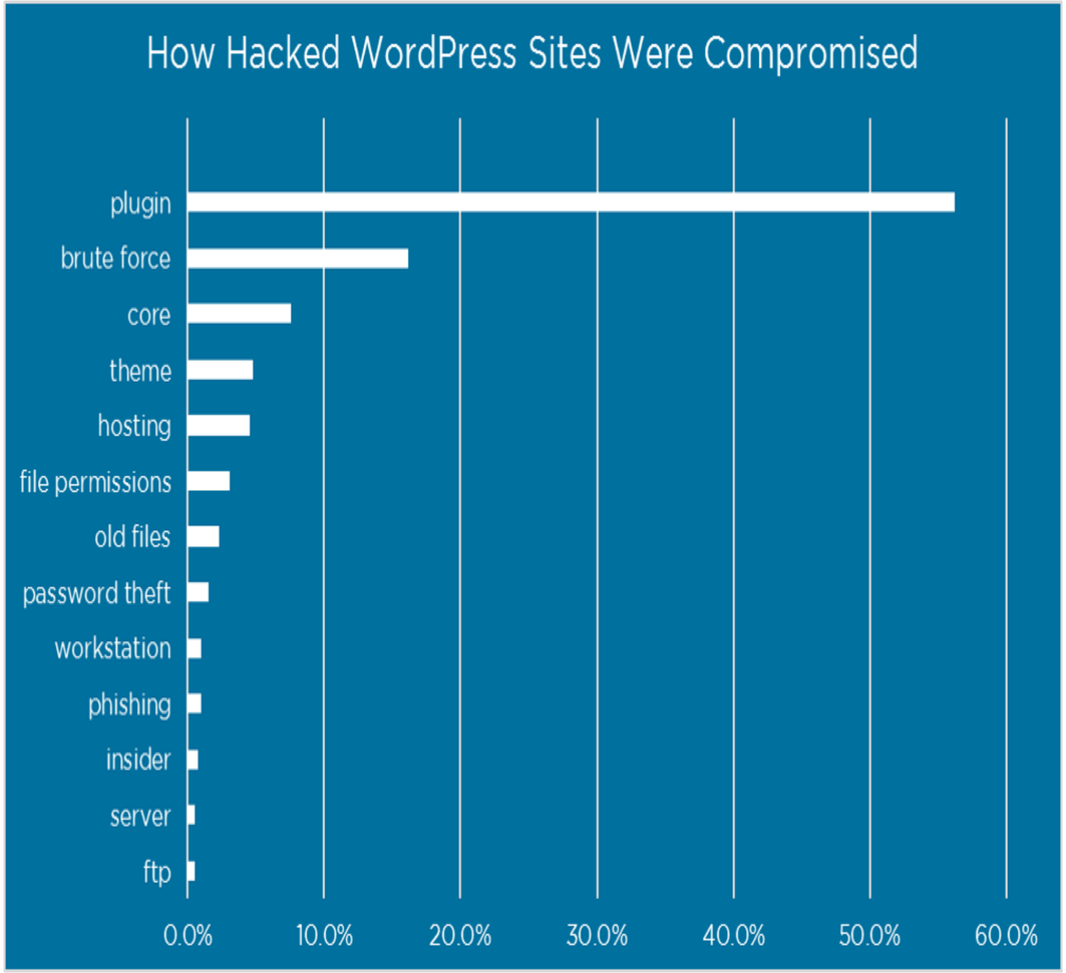
Spam Rely

Session Hijacking

User

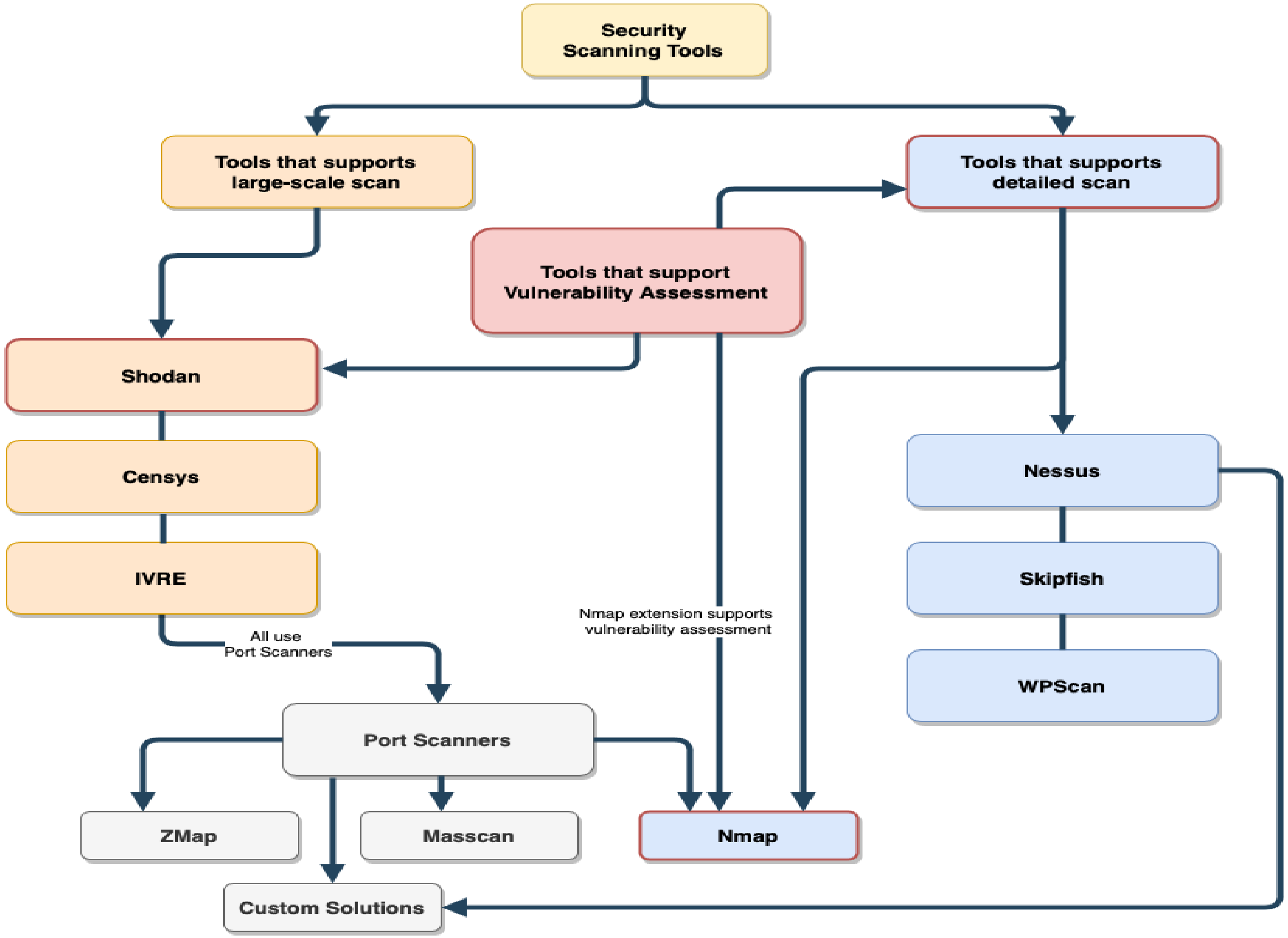
Spam

Cross-Site Scripting



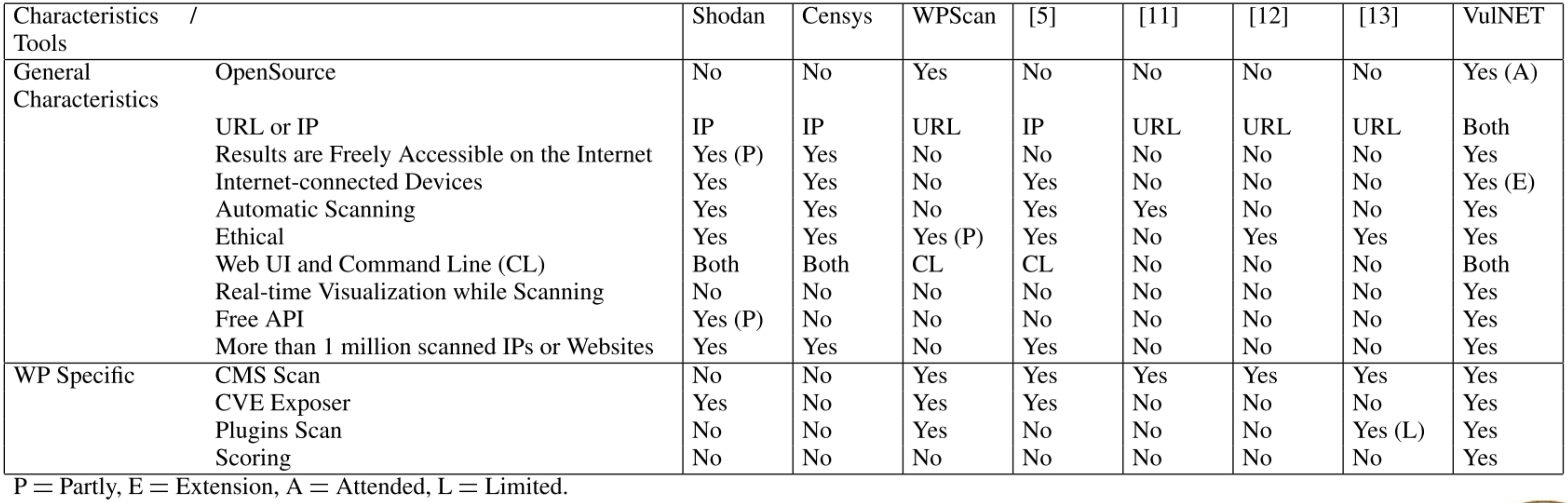
How Hacked WordPress Sites Were Compromised

Security scanning tools and their functionality



Security Scanning Tools
Tools that supports large-scale scan
Tools that supports detailed scan
Tools that support Vulnerability Assessment
Shodan
Censys
IVRE
All use Port Scanners
Nessus
Skipfish
WPScan
Nmap extension supports vulnerability assessment
Port Scanners
ZMap
Masscan
Nmap
Custom Solutions

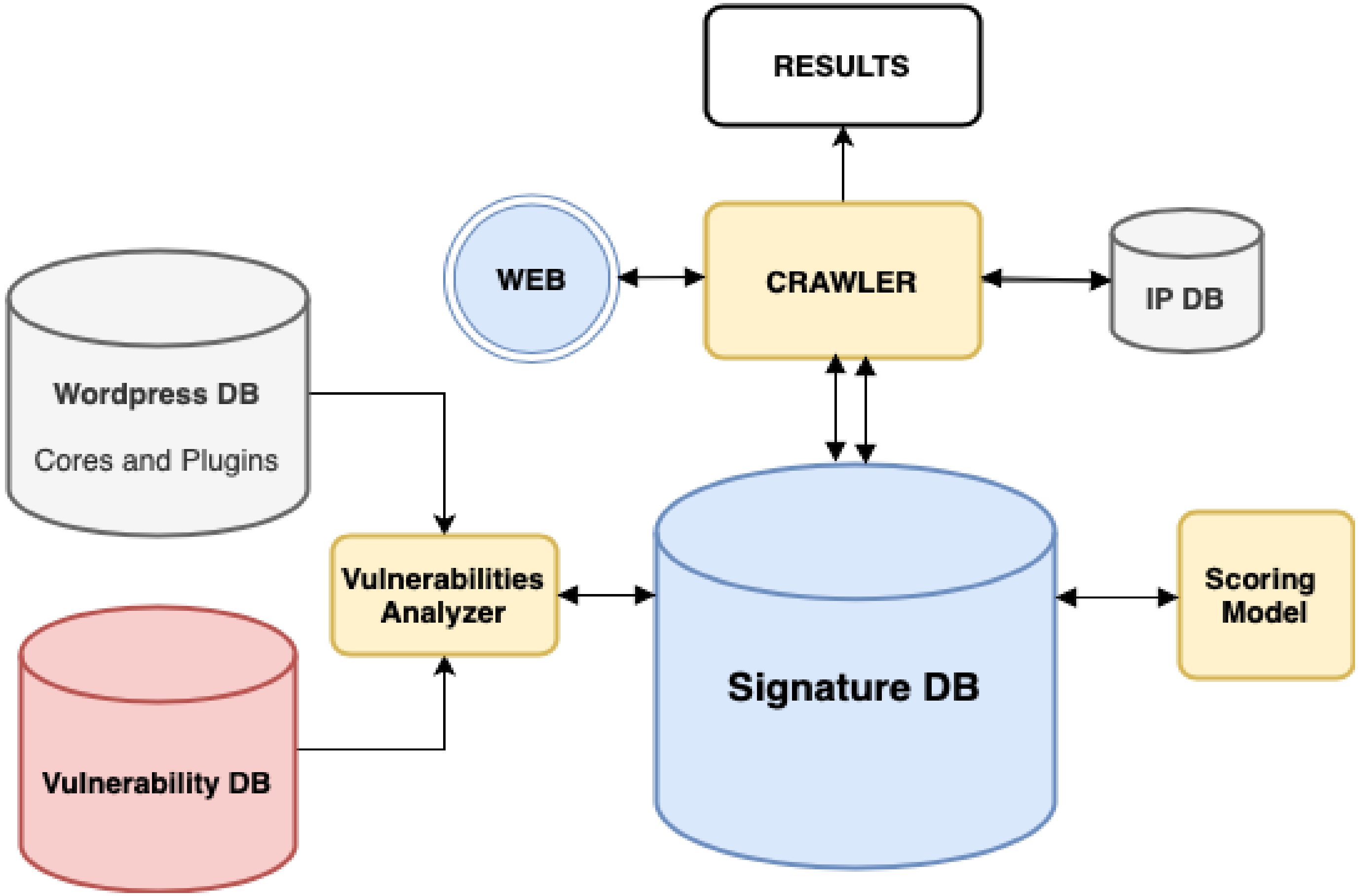
Comparison of the most known vulnerability scanning tools with crawlers



Characteristics / Tools		Shodan	Censys	WPScan	[5]	[11]	[12]	[13]	VulNET
General Characteristics	OpenSource	No	No	Yes	No	No	No	No	Yes (A)
	URL or IP	IP	IP	URL	IP	URL	URL	URL	Both
	Results are Freely Accessible on the Internet	Yes (P)	Yes	No	No	No	No	No	Yes
	Internet-connected Devices	Yes	Yes	No	Yes	No	No	No	Yes (E)
	Automatic Scanning	Yes	Yes	No	Yes	Yes	No	No	Yes
	Ethical	Yes	Yes	Yes (P)	Yes	No	Yes	Yes	Yes
	Web UI and Command Line (CL)	Both	Both	CL	CL	No	No	No	Both
	Real-time Visualization while Scanning	No	No	No	No	No	No	No	Yes
	Free API	Yes (P)	No	No	No	No	No	No	Yes
	More than 1 million scanned IPs or Websites	Yes	Yes	No	Yes	No	No	No	Yes
WP Specific	CMS Scan	No	No	Yes	Yes	Yes	Yes	Yes	Yes
	CVE Exposer	Yes	No	Yes	Yes	No	No	No	Yes
	Plugins Scan	No	No	Yes	No	No	No	Yes (L)	Yes
	Scoring	No	No	No	No	No	No	No	Yes

P = Partly, E = Extension, A = Attended, L = Limited.

The system and component scheme of the new developed tool at IJS for large scanning WP web sites over the Internet – VULNET enables fast and ethical scanning at large



WEB site presence on the internet in Numbers found by VULNET in the first large scan of the Internet

126
Million+

There were over 126 millions scanned websites (194 countries)

16
MILLION

WordPress Websites

5
MILLION

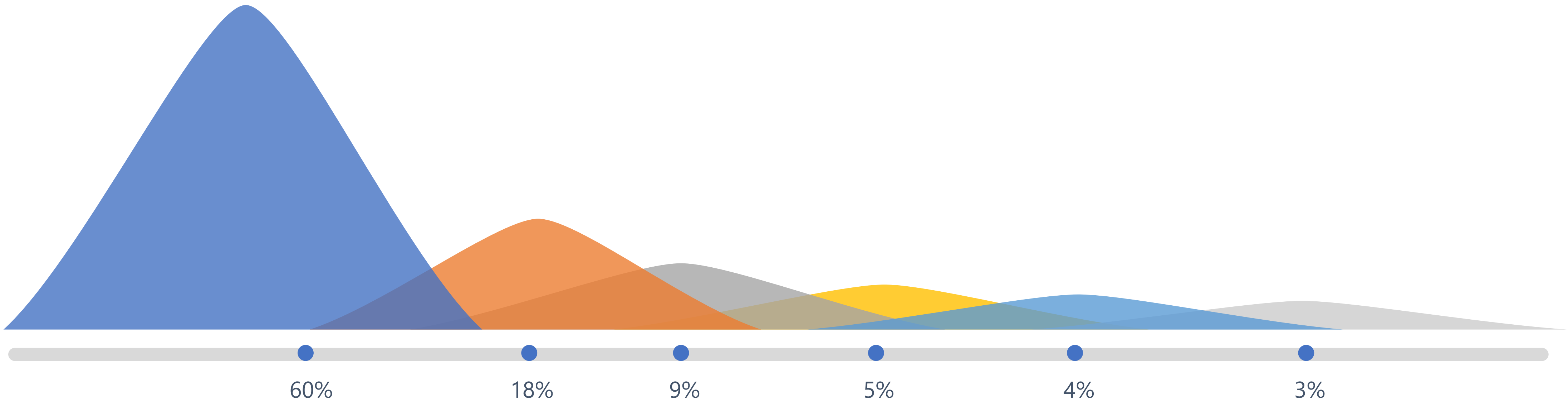
More than 5 millionion web sites had vulnerability, with a score of 5 or more

MEDNARODNA PODIPLOMSKA ŠOLA JOŽEFA STEFANA
SLOVENIJA
LJUBLJANA
2004

Owners and the hacked compromised WP web sites

From the **1,032** survey respondents who answered to the submitted questions about their own web site vulnerability awareness after the successful attack

61,5% didn’t know how the attacker compromised their website!



● **Plugins**

Plugins are the biggest risk. There are cca 50 000 plugins available.

● **Theme**

● **Brute Force Attacks**

A brute force attack is a password guessing attack.

● **File permissions**

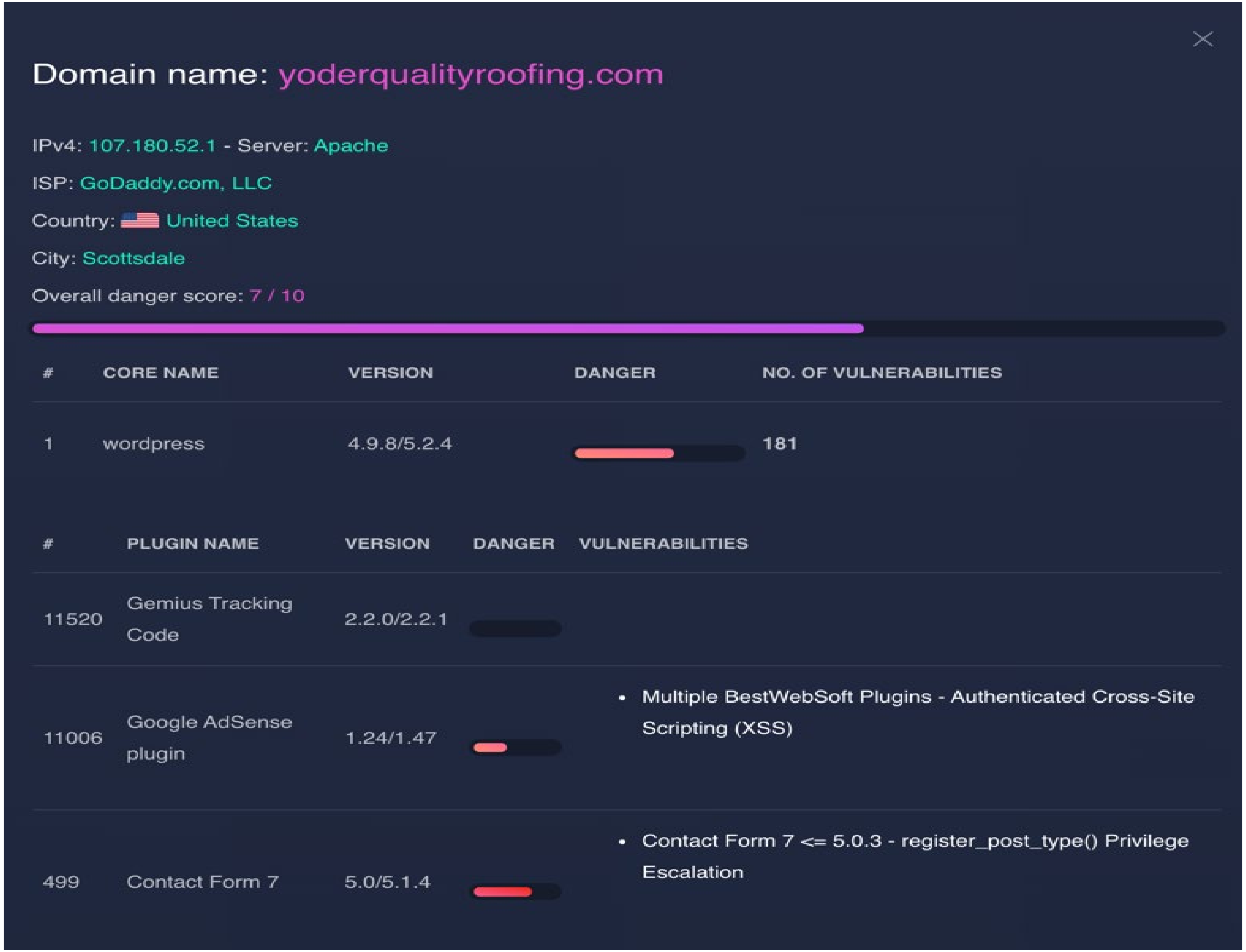
● **Core**

●

The measured vulnerability

of one affected domain

with VULNET tool



Domain name: yoderqualityroofing.com

IPv4: 107.180.52.1 - Server: Apache

ISP: GoDaddy.com, LLC

Country: United States

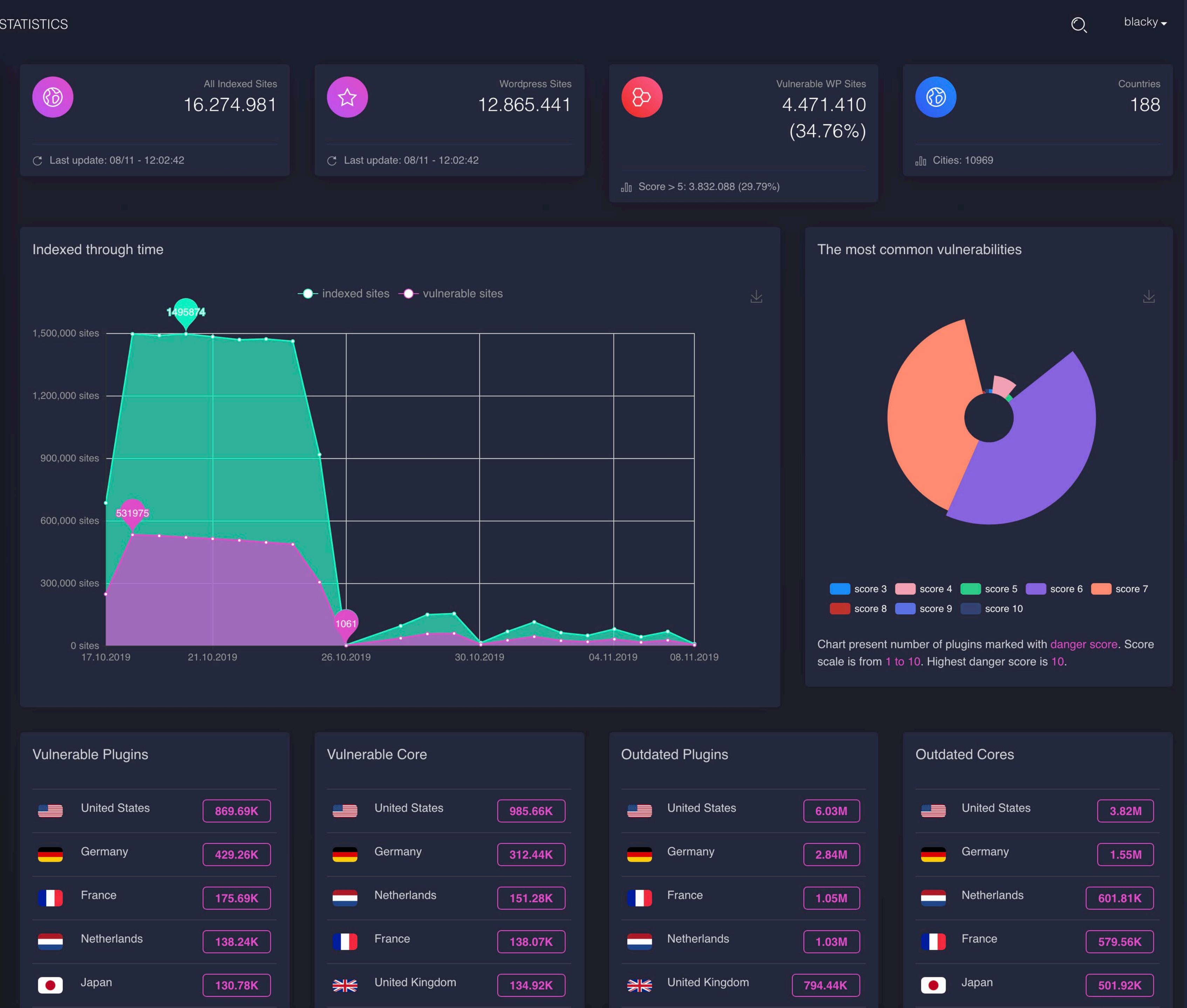
City: Scottsdale

Overall danger score: 7 / 10

#	CORE NAME	VERSION	DANGER	NO. OF VULNERABILITIES
1	wordpress	4.9.8/5.2.4		181

#	PLUGIN NAME	VERSION	DANGER	VULNERABILITIES
11520	Gemius Tracking Code	2.2.0/2.2.1		
11006	Google AdSense plugin	1.24/1.47		• Multiple BestWebSoft Plugins - Authenticated Cross-Site Scripting (XSS)
499	Contact Form 7	5.0/5.1.4		• Contact Form 7 <= 5.0.3 - register_post_type() Privilege Escalation

MEDNARODNA PODIPLOMSKA ŠOLA JOŽEFA STEFANA
SLOVENIJA
LJUBLJANA
2004



All Indexed Sites	Wordpress Sites	Vulnerable WP Sites	Countries
16.274.981	12.865.441	4.471.410 (34.76%)	188
Last update: 08/11 - 12:02:42	Last update: 08/11 - 12:02:42	Score > 5: 3.832.088 (29.79%)	Cities: 10969

Indexed through time

The most common vulnerabilities

Chart present number of plugins marked with danger score. Score scale is from 1 to 10. Highest danger score is 10.

Vulnerable Plugins

United States	869.69K
Germany	429.26K
France	175.69K
Netherlands	138.24K
Japan	130.78K

Vulnerable Core

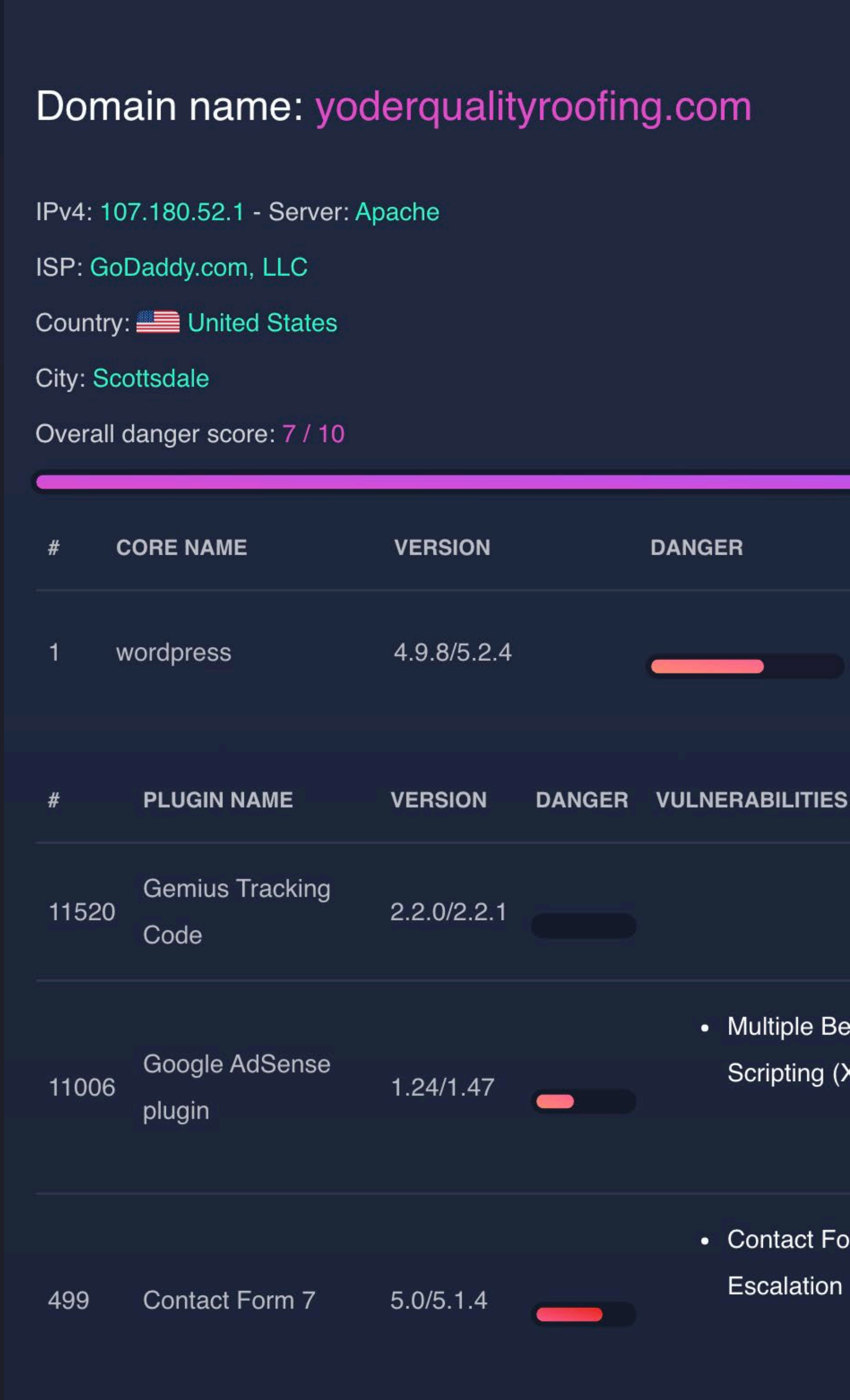
United States	985.66K
Germany	312.44K
Netherlands	151.28K
France	138.07K
United Kingdom	134.92K

Outdated Plugins

United States	6.03M
Germany	2.84M
France	1.05M
Netherlands	1.03M
United Kingdom	794.44K

Outdated Cores

United States	3.82M
Germany	1.55M
Netherlands	601.81K
France	579.56K
Japan	501.92K



Domain name: yoderqualityroofing.com

IPv4: 107.180.52.1 - Server: Apache

ISP: GoDaddy.com, LLC

Country: United States

City: Scottsdale

Overall danger score: 7 / 10

#	CORE NAME	VERSION	DANGER
1	wordpress	4.9.8/5.2.4	

#	PLUGIN NAME	VERSION	DANGER	VULNERABILITIES
11520	Gemius Tracking Code	2.2.0/2.2.1		
11006	Google AdSense plugin	1.24/1.47		- Multiple Be Scripting (X
499	Contact Form 7	5.0/5.1.4		- Contact Fo Escalation

Comparison of known scanning tools and VULNET according to properties

The table legend:
'•••' is used to denote a strong support, '••'
to denote a moderate support,
 and '•' for a weak support
(i.e., unavailable) of a
specific feature.
CPE, Common Platform
Enumeration, CVE,
Common Vulnerability and
Exposure.

Tool	Aggressive assessment	Passive assessment	Automated CPE / CVE	Vuln. score	Port scan cover	Vuln. Notifications	Recognized web app.	Ethical	Scan Speed	Large-Scale
Nmap	•••	•	••	•	•••	•	•	•	•	•
ZMap	•••	•	•	•	•••	•	•	•	•••	••
Masscan	•••	•	•	•	•••	•	•	•	•••	••
Shodan	•	•••	••	•	•••	•	•	•	•	••
Censys	•	•••	•	•	••	•	•	•	•••	••
IVRE	•	•••	•	•	•••	•	•	•	•••	••
Nessus	•••	•	••	•	•••	•	••	•	•	•
Skipfish	•••	•	•	•	•	•	•••	•	•	•
WPScan	•••	••	••	•	•	•	••	••	•	•
(Goethem, Chen, Nikiforkais, Desmet, & Joosen)	•	••	••	••	•	•	••	••	•	•
(Stock, Pellegrino, Li, Backes, & Rossow, 2018)	•	••	•	•	•	••	•	•••	•	•
(Vasek, Wadleigh, & Moore, 2015)	•	•••	••	•	•	•	••	•••	•	•
(Schagen, Koning, Bos, & Giuffrida, 2018)	••	•	•	•	•••	•	•	•	•••	••
VulNet	•	•••	•••	•••	•	•••	•••	•••	•••	•••

'•••' is used to denote a strong support, '••' to denote a moderate support, and '•' for a weak support (i.e., unavailable) of a specific feature. CPE, Common Platform Enumeration, CVE, Common Vulnerability and Exposure.

What was studied and what was found

- The aim of the analysis was to find out the **percentage of insecure WP websites among the WP websites** found.

- **The level of Digital skills to be compared with the appearnce of** web insecurity

- The cost of fixed access normalized with GNI was the second parameter studied as impact factor that affect the appearance of insecure web sites.

- The subset of studied countries was composed from: Germany (DE), Netherlands (NL), France (FR), Great Britain (GB), Italy (IT), Denmark (DK), Poland (PL), Spain (ES), Sweden (SE), Switzerland (CH), Czech Republic (CZ), Ireland (IE), Finland (FI), Austria (AT), Romania (RO), Belgium (BE), Hungary (HU), Bulgaria (BG), Norway (NO), Slovakia (SK), Estonia (EE), Slovenia (SI), Portugal (PT), Croatia (HR), Lithuania (LV), Luxembourg (LU), Greece (GR), Iceland (IS), Latvia (LT), Cyprus (CY), and Malta (MT)

Security state in the EU WP web space

The web space with domains representing 28 members states and three other (Switzerland, Norway) was inspected for discovering the presence of insecure and secure web sites with WP core and added plug-ins.
Web sites that did not provided information of WP core version were classified as unknown, the others with score higher than 5 from a scale of 10 were classified as critically insecure and the other with identified vulnerability but having lower insecure score were classified as insecure.

The top five ranked countries with highest numbers of vulnerabilityy and out-dated plug-ins were found in the general internet at large scan to be: USA, France, Germany, Netherlands and Japan (this is related also to the highest numbers of present web sites.

		unknown [%]	secure [%]	insecure [%]	critical [%]	DS
Count	30	30	30	30	30	30
Mean	124621.8	34.02	27.6	38.38	30.98	59.13
Std	183737.33	3.56	4.66	4.52	4.57	15.14
Min	864	27.38	21.22	30.31	22.1	29
25%	14924.75	31.38	24.19	35.32	27.29	48.5
50%	53261	34.21	26.05	39.44	31.97	58
75%	140195	36.98	30.98	41.57	34.76	71
Max	805279	40.15	37.85	47.37	41.31	85

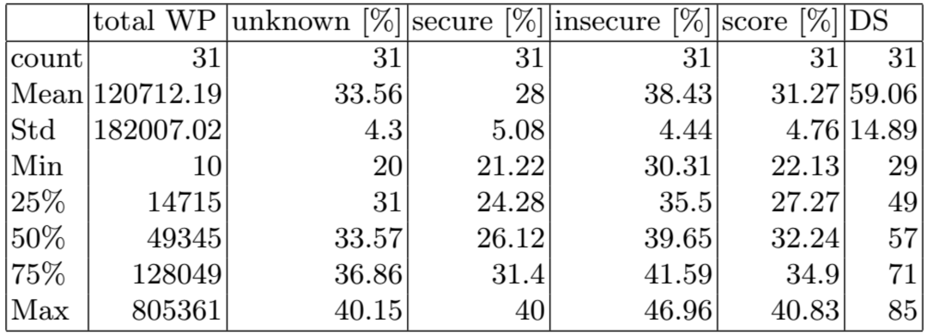
Analysis of the EU web space

Results and the analysis

- On average, we could not determine the vulnerability status in the first scan for a third of the sites in a domain, due to unknown (hiden) core or plug-in versions. Then the second scan with 31 countries gave more significant result.

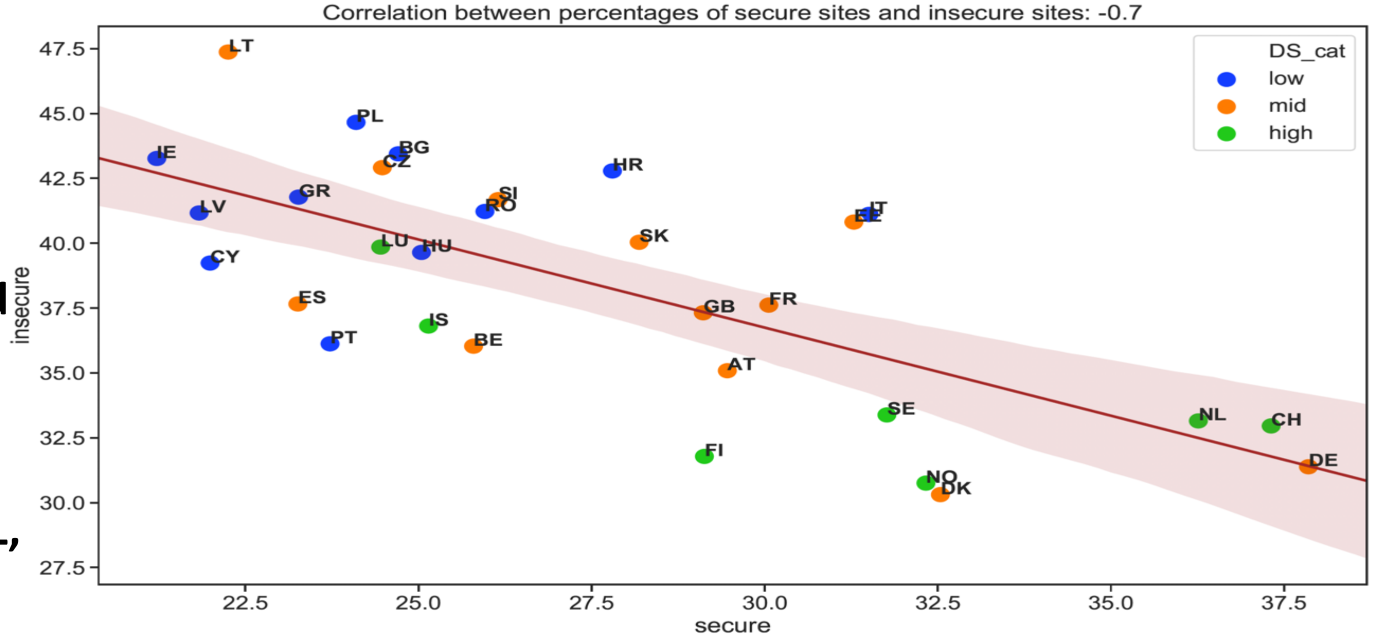
- The percentages of **secure sites were between 21% and 40%, with an average of 28%.** The percentage of **insecure sites is in the range of 30% and 47%, with a mean of 38%, a median of 40%,** and a standard deviation of 4.4%. There were no univariate outliers in either variable.

Table 1. Summary statistics of all the WP sites found, the vulnerability percentages, and the digital-skills (DS) index.

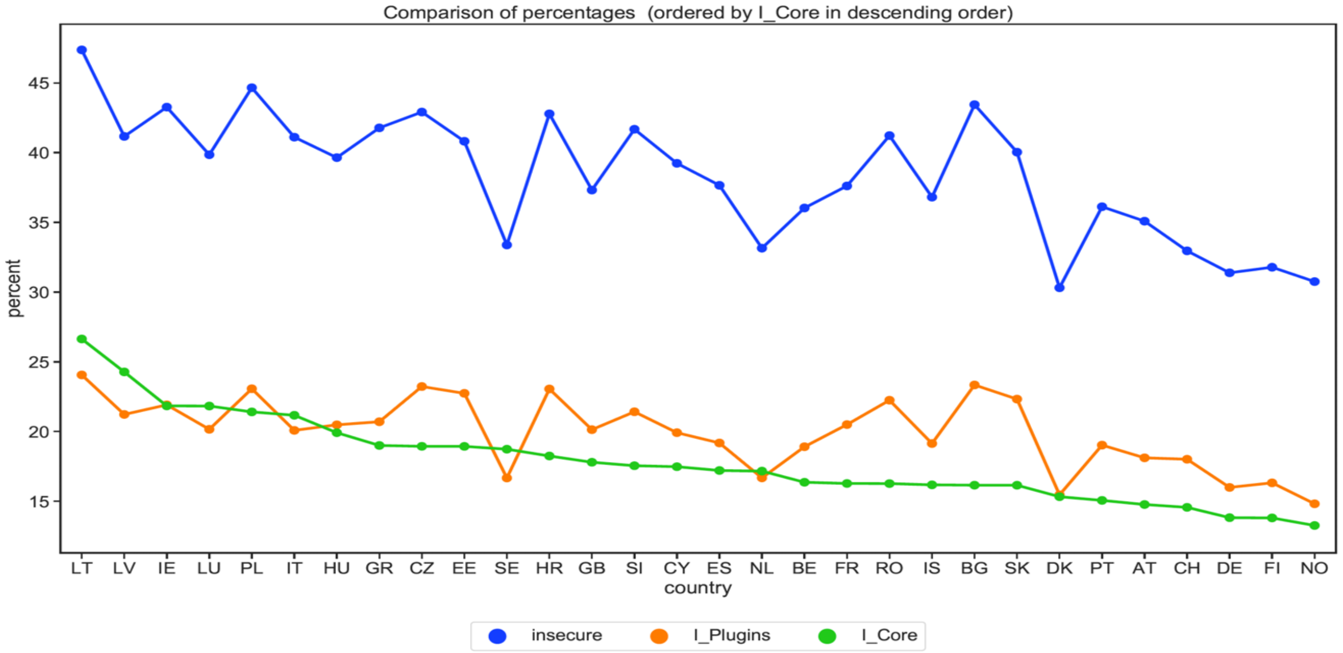


	total WP	unknown [%]	secure [%]	insecure [%]	score [%]	DS
count	31	31	31	31	31	31
Mean	120712.19	33.56	28	38.43	31.27	59.06
Std	182007.02	4.3	5.08	4.44	4.76	14.89
Min	10	20	21.22	30.31	22.13	29
25%	14715	31	24.28	35.5	27.27	49
50%	49345	33.57	26.12	39.65	32.24	57
75%	128049	36.86	31.4	41.59	34.9	71
Max	805361	40.15	40	46.96	40.83	85

The correlation between insecure and secure sites in a country shows that the countries with well developed digital skills (high percentage of DS) among the population have low percentage of insecure sites.
The group is consisted from SE, CH, NL, DE,NO,DK, FI.

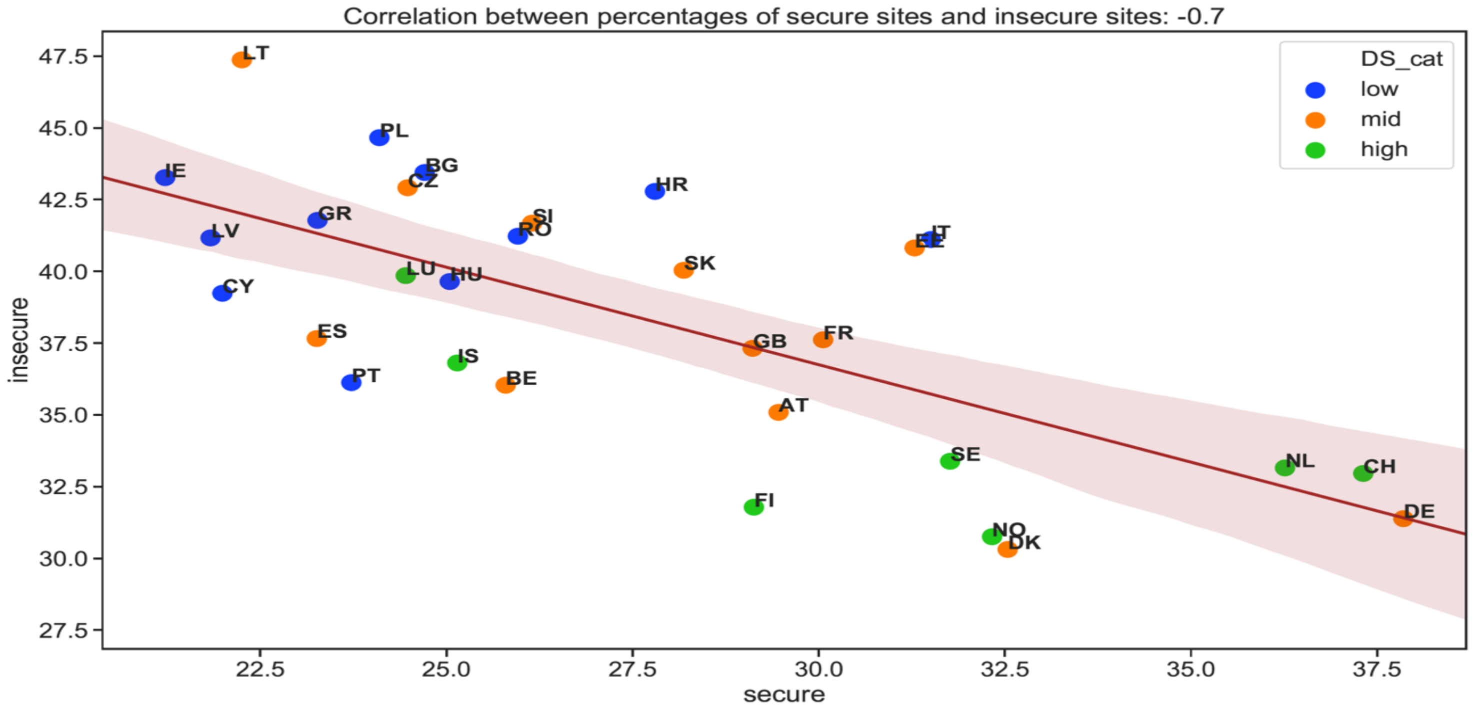

Correlation between percentages of secure sites and insecure sites: -0.7

The insecurity among plug-ins was found to be the
factor that has most influence on the site to be insecure.

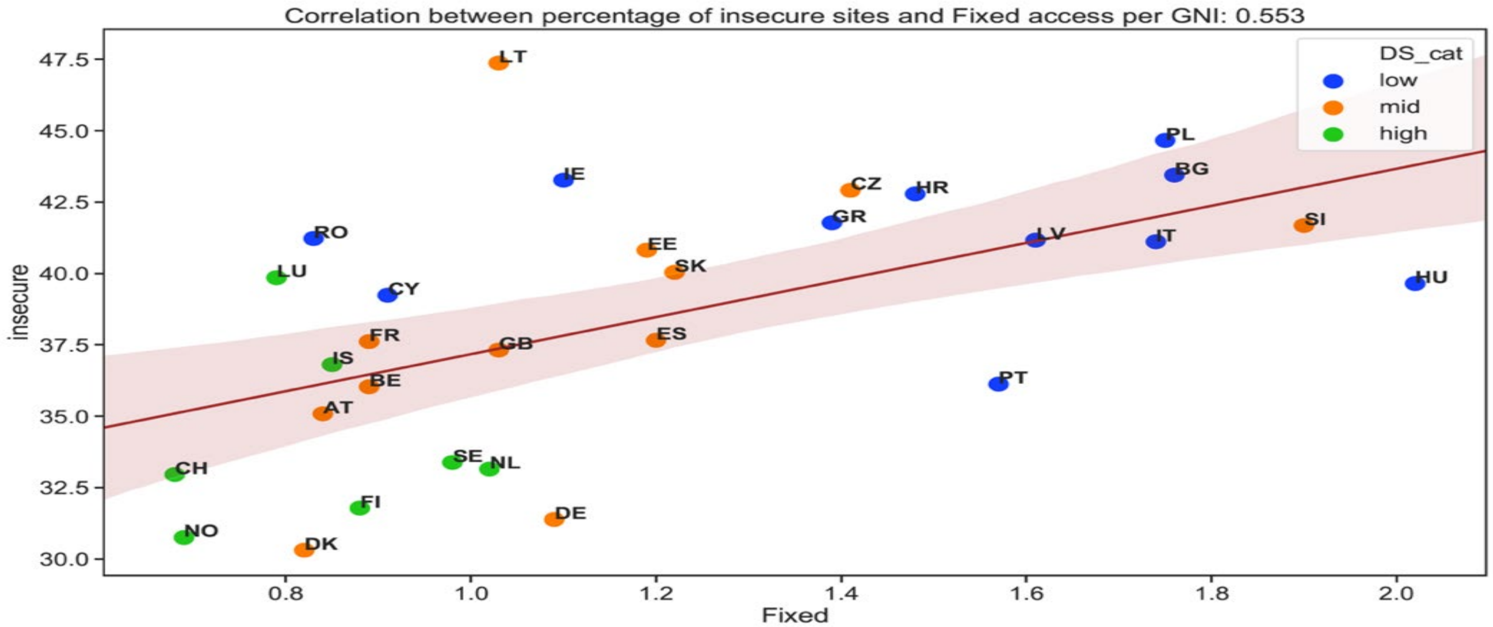

Comparison of percentages (ordered by I_Core in descending order)

MEDNARODNA PODIPLOMSKA ŠOLA JOŽEFA STEFANA
SLOVENIJA
LJUBLJANA
2004

The study about appearance of insecure sites and the Digital skills among the country population has shown that those countries that have high percentage of population with digital skills have the lowest percentage of Insecure web sites. This group is consisted from the countries SE, CH, NL,DE,NO,DK, FI.



The study as well has shown that countries with low cost of fixed internet access have also low percentage of insecure web sites

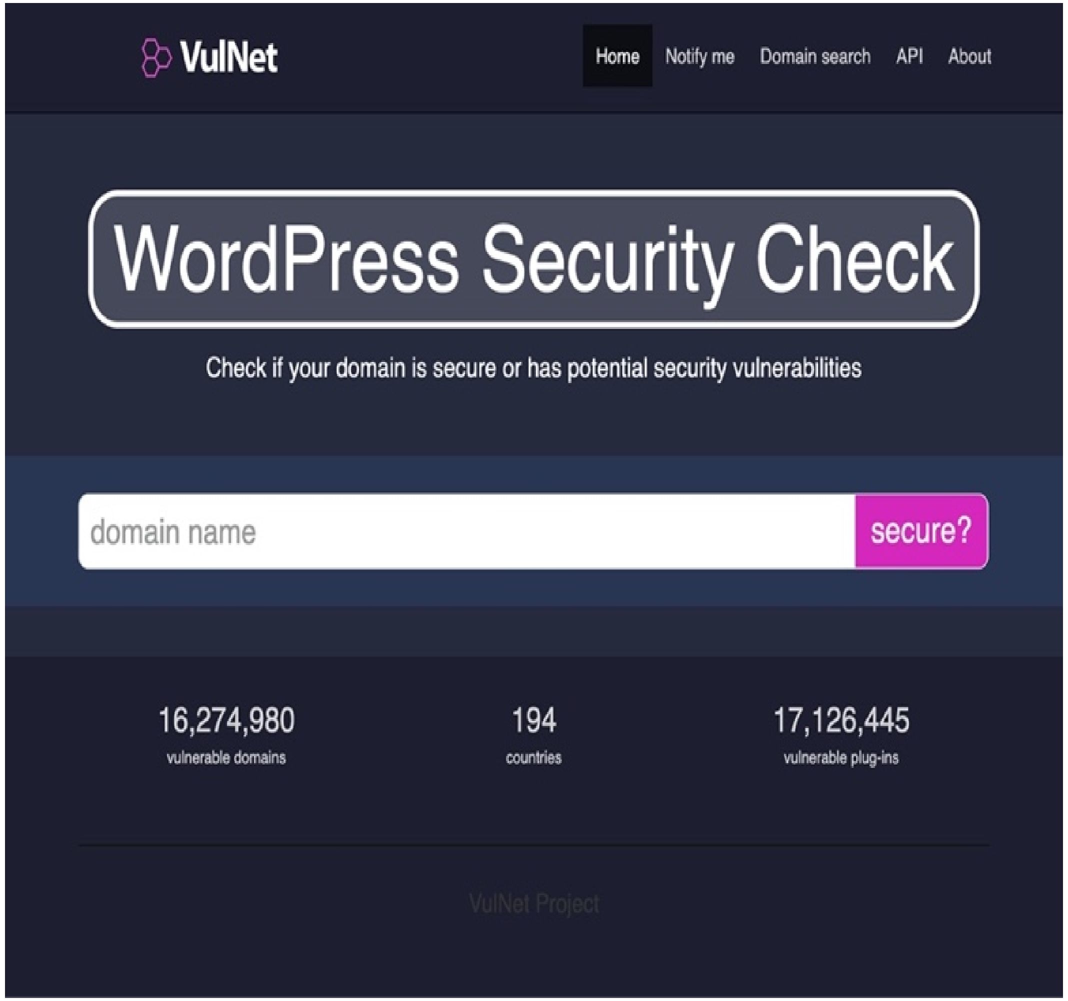


VulNet service offered

to the public a service for checking

the website vulnerability

in safe and privacy protected manner



WordPress Security Check

Check if your domain is secure or has potential security vulnerabilities

16,274,980
vulnerable domains

194
countries

17,126,445
vulnerable plug-ins

VulNet Project

CONCLUSION

- **Vulnerability presence is still a risk issue for the security of the web space**
- **Improvement were noticed with the third large VULNET scan that happened 6 months later due to the replacement of old WP versions with the new releases of the web core system**
- **The best remedy was found to be continuous checking of the insecurity presence in the web sites by the maintainers and owners with a public service that guarantee the owner privacy**