

**IL WEBINAR INIZIA TRA QUALCHE MINUTO
GRAZIE PER AVER SCELTO DI PARTECIPARE**

MÜSA
FORMAZIONE E LAVORO



**MASSIMO
CHIRIVI**

IT SECURITY ETHICAL HACKING

**Webinar Gratuito IT Security | Web Application
Vulnerability Assessment Example**

 **aipsi**
ASSOCIAZIONE ITALIANA PROFESSIONISTI SICUREZZA INFORMATICA



4 Stages of a Vulnerability Assessment



Webinar Gratuito IT Security | Web Application Vulnerability Assessment Example

CWE

CWE™ is a community-developed list of software and hardware weakness types. It serves as a common language, a measuring stick for security tools, and as a baseline for weakness identification, mitigation, and prevention efforts.

<https://cwe.mitre.org/>

CVE

The Common Vulnerabilities and Exposures (CVE) system provides a reference-method for publicly known information-security vulnerabilities and exposures. The United States National Cybersecurity FFRDC, operated by The Mitre Corporation, maintains the system, with funding from the US National Cyber Security Division of the US Department of Homeland Security. The system was officially launched for the public in September 1999.

The Security Content Automation Protocol uses CVE, and CVE IDs are listed on Mitre's system as well as in the US National Vulnerability Database

<https://nvd.nist.gov/vuln/search>

OWASP

The OWASP Top 10 is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications.

<https://owasp.org/www-project-top-ten/>

WASC

The Web Application Security Consortium (WASC) is 501c3 non profit made up of an international group of experts, industry practitioners, and organizational representatives who produce open source and widely agreed upon best-practice security standards for the World Wide Web.

<http://www.webappsec.org/>

Webinar Gratuito IT Security | Web Application Vulnerability Assessment Example

CVSS

The Common Vulnerability Scoring System (CVSS) provides a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity. The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organizations properly assess and prioritize their vulnerability management processes. CVSS is a published standard used by organizations worldwide, and the SIG's mission is to continue to improve it.

<https://www.first.org/cvss/>

CVSS v2.0 Ratings		CVSS v3.0 Ratings	
Severity	Base Score Range	Severity	Base Score Range
		None	0.0
Low	0.0-3.9	Low	0.1-3.9
Medium	4.0-6.9	Medium	4.0-6.9
High	7.0-10.0	High	7.0-8.9
		Critical	9.0-10.0

Iniziamo a farci alcune domande:

- 1) FQDN
- 2) IP
- 3) DNS coinvolti
- 4) Registrar
- 5) Hosting

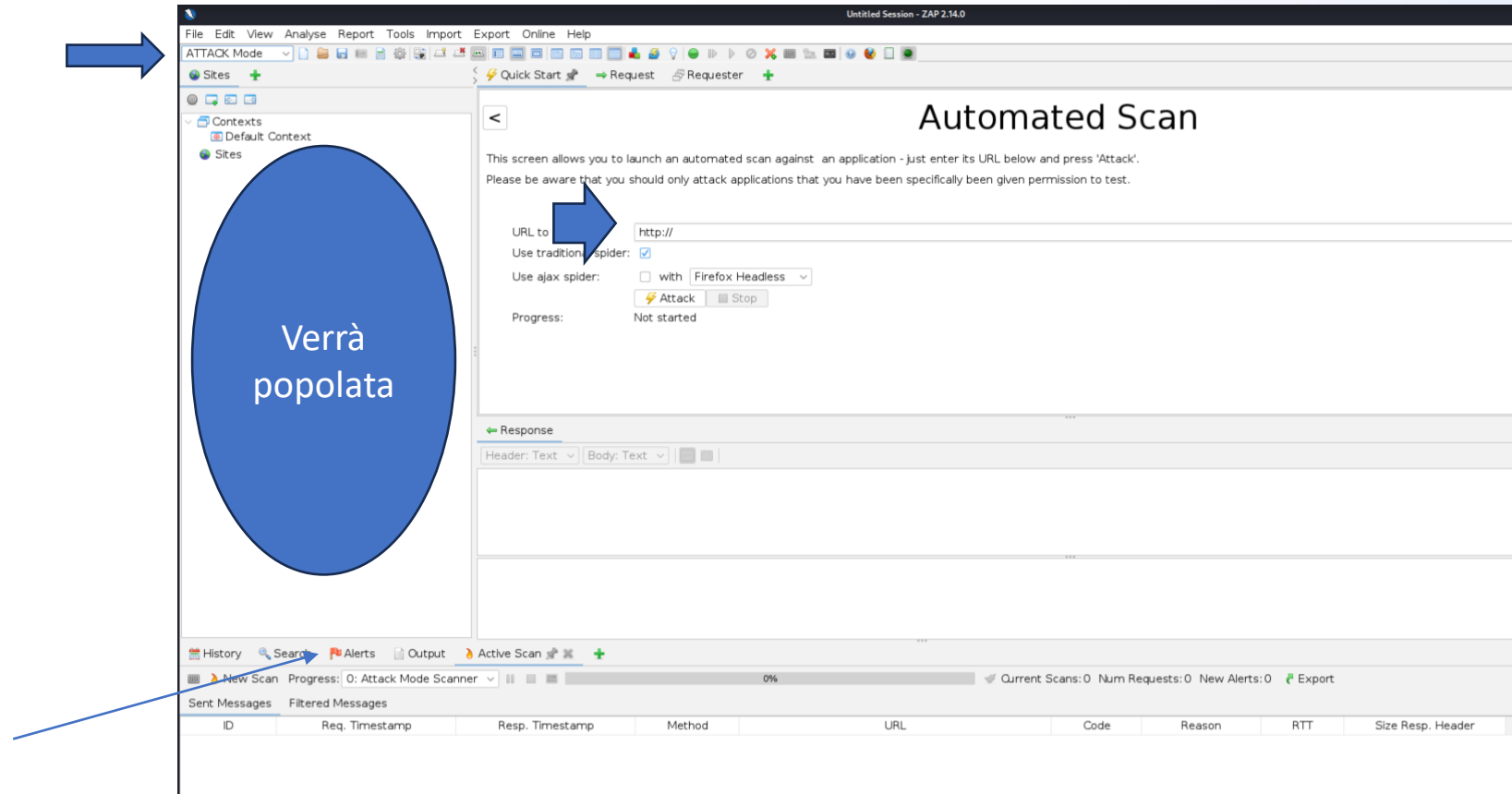
Open Source Vs Closed

Community?

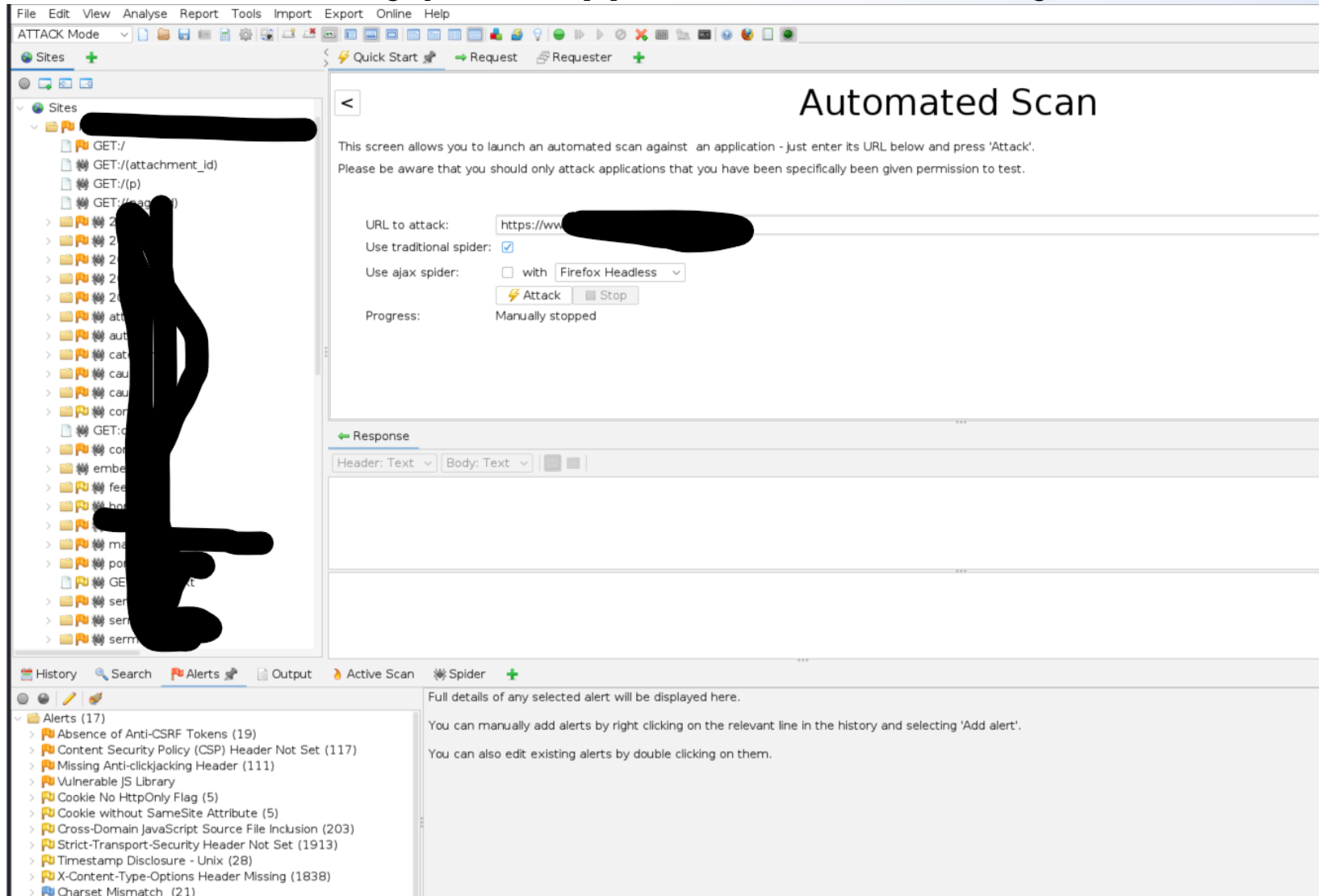
VA Tools/Plugin di riferimento

1. **GVM** (Progetto Open Source)
2. **Nikto** (Progetto Open Source)
3. **SonarQube** (Progetto Open Source)
4. **Nessus Teenable Expert** (Commercial Tool)
5. **WPSCAN** (Vertical VA tool)
6. **Zed Attack Proxy** (ZAP) (Progetto Open Source)
7. **Spiderfoot** (OSINT Tool)

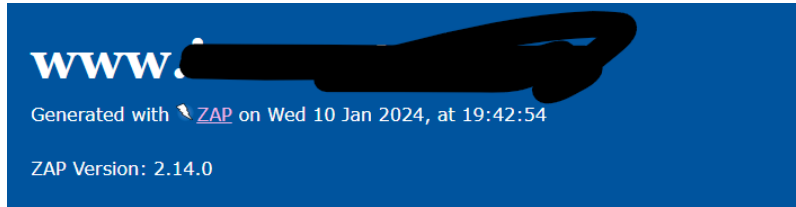
Webinar Gratuito IT Security | Web Application Vulnerability Assessment Example



Webinar Gratuito IT Security | Web Application Vulnerability Assessment Example



Webinar Gratuito IT Security | Web Application Vulnerability Assessment Example



Contents

- [About this report](#)
 - [Report parameters](#)
- [Summaries](#)
 - [Alert counts by risk and confidence](#)
 - [Alert counts by site and risk](#)
 - [Alert counts by alert type](#)
- [Alerts](#)
 - [Risk=High, Confidence=Medium \(2\)](#)
 - [Risk=High, Confidence=Low \(2\)](#)
 - [Risk=Medium, Confidence=High \(1\)](#)
 - [Risk=Medium, Confidence=Medium \(2\)](#)
 - [Risk=Medium, Confidence=Low \(2\)](#)
 - [Risk=Low, Confidence=High \(1\)](#)

Alert type	Risk	Count
Cloud Metadata Potentially Exposed	High	1 (4.2%)
Path Traversal	High	2 (8.3%)
SQL Injection - Oracle - Time Based	High	1 (4.2%)
SQL Injection - SQLite	High	3 (12.5%)
Absence of Anti-CSRF Tokens	Medium	110 (458.3%)
Content Security Policy (CSP) Header Not Set	Medium	213 (887.5%)
Directory Browsing	Medium	65 (270.8%)
Hidden File Found	Medium	4 (16.7%)
Missing Anti-clickjacking Header	Medium	201 (837.5%)
Cookie No HttpOnly Flag	Low	11 (45.8%)
Cookie without SameSite Attribute	Low	11 (45.8%)
Cross-Domain JavaScript Source File Inclusion	Low	126

Webinar Gratuito IT Security | Web Application Vulnerability Assessment Example

Path Traversal

Source	raised by an active scanner (plugin ID: 6)
CWE ID	22
WASC ID	33
Reference	<ul style="list-style-type: none">http://projects.webappsec.org/Path-Traversalhttp://cwe.mitre.org/data/definitions/22.html

SQL Injection - Oracle - Time Based

Source	raised by an active scanner (plugin ID: 40021)
CWE ID	89
WASC ID	19
Reference	<ul style="list-style-type: none">https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

SQL Injection - SQLite

Source	raised by an active scanner (plugin ID: 40024)
CWE ID	89
WASC ID	19
Reference	<ul style="list-style-type: none">https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

The screenshot shows the GitHub repository for `zap-proxies/zap-extensions`. The file `PathTraversalScanRule.java` is selected, showing its commit history and code. The code is a Java class that implements the `IScanRule` interface. It contains a `scan` method that checks for path traversal vulnerabilities by looking for `..` in the request path. The code is licensed under the Apache License, Version 2.0.

```
1  /*
2   * Zed Attack Proxy (ZAP) and its related class files.
3   *
4   * ZAP is an HTTP/HTTPS proxy for assessing web application security.
5   *
6   * Copyright 2011 The ZAP Development Team
7   *
8   * Licensed under the Apache License, Version 2.0 (the "License");
9   * you may not use this file except in compliance with the license.
10  * You may obtain a copy of the license at
11  *
12  * http://www.apache.org/licenses/LICENSE-2.0
13  *
14  * Unless required by applicable law or agreed to in writing, software
15  * distributed under the license is distributed on an "AS IS" BASIS,
16  * WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
17  * See the License for the specific language governing permissions and
18  * limitations under the license.
19  */
20 package org.zaproxy.zap.extension.ascanrules;
21
22 import static org.zaproxy.zap.extension.ascanrules.utils.Constants.NULL_BYTE_CHARACTER;
23
24 import java.io.IOException;
25 import java.net.SocketException;
26 import java.net.UnknownHostException;
27 import java.util.ArrayList;
28 import java.util.List;
29 import java.util.Map;
30 import java.util.regex.Matcher;
```

Webinar Gratuito IT Security | Web Application Vulnerability Assessment Example

Response	<p>▼ Status line and header section (411 bytes)</p> <pre>HTTP/1.1 200 OK Server: nginx Date: Wed, 18 Oct 2023 12:35:56 GMT Content-Type: text/html; charset=UTF-8 Connection: keep-alive Link: <https://www[REDACTED]wp-json/>; rel="https://api.w.org/" Link: <https://www[REDACTED]- [REDACTED]>; typ[REDACTED]; Link: <https://www[REDACTED]=1339>; rel=shortlink Vary: Accept-Encoding content-[REDACTED]</pre> <p>► Response body (64568 bytes)</p>
Parameter	<p>your-name</p>
Attack	<pre>field: [your-name], value [(SELECT UTL_INADDR.get_host_name('10.0.0.1') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.2') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.3') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.4') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.5') from dual)]</pre>
Solution	<p>Do not trust client side input, even if there is client side validation in place.</p> <p>In general, type check all data on the server side.</p> <p>If the application uses JDBC, use PreparedStatement or CallableStatement, with parameters passed by '?'</p>

Webinar Gratuito IT Security | Web Application Vulnerability Assessment Example



https://www.xxxco.com/

Thu, 28 Mar 2024 01:26:53 Pacific Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

- https://www.xxxco.com

Vulnerabilities by Plugin

- 98056 (6) - Missing HTTP Strict Transport Security Policy
- 98203 (1) - WordPress User Enumeration
- 98212 (1) - WordPress Directory Listing
- 98215 (1) - WordPress XML-RPC Interface Detected
- 98617 (1) - SSL/TLS Forward Secrecy Cipher Suites Not Supported
- 112496 (1) - TLS 1.0 Weak Protocol
- 112546 (1) - TLS 1.1 Weak Protocol
- 113449 (1) - WordPress Cron Enabled
- 98060 (6) - Missing 'X-Frame-Options' Header
- 98618 (6) - HTTP Header Information Disclosure
- 112553 (6) - Missing 'Cache-Control' Header
- 112529 (5) - Missing 'X-Content-Type-Options' Header
- 112551 (5) - Missing Content Security Policy
- 98063 (1) - Cookie Without HttpOnly Flag Detected
- 98064 (1) - Cookie Without Secure Flag Detected
- 98207 (1) - WordPress Administration Panel Login Form Detected
- 112539 (1) - SSL/TLS Weak Cipher Suites Supported
- 115540 (1) - Cookie Without SameSite Flag Detected
- 98050 (11) - Interesting Response
- 98526 (6) - Missing Permissions Policy
- 98527 (6) - Missing Referrer Policy

98212 (1) - WordPress Directory Listing

Synopsis

WordPress Directory Listing

Description

The scanner has detected publicly accessible WordPress directory listing on the target web application. This may expose information relating to the web server to an attacker which may allow for further exploitation techniques to be leveraged, possibly leading to a compromise of the target server

See Also

<https://codex.wordpress.org/htaccess>

Solution

Block requests to sensitive server information using .htaccess file or WAF for example.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

CVSS v2.0 Base Score

5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

References

XREF CWE:548 WASC:Directory Indexing HIPAA:164.312(a)(1) HIPAA:164.312(a)(2)(i) DISA_STIG:APSC-DV-002480 OWASP:2010-A6 OWASP:2013-A5 OWASP:2017-A6 OWASP:2021-A1 OWASP_API:2019-API7 OWASP_API:2023-API8 OWASP_ASVS:4.0.2-4.3.2 PCI_DSS:3.2-6.5.8 ISO:27001-A.13.1.1 ISO:27001-A.14.1.2 ISO:27001-A.14.1.3 ISO:27001-A.18.1.3 ISO:27001-A.6.2.2 ISO:27001-A.9.1.2 ISO:27001-A.9.4.1 ISO:27001-A.9.4.4 ISO:27001-A.9.4.5 NIST:sp800_53-AC-3

Plugin Information

Published: 2018/03/28, Modified: 2023/11/22

Instances

https://www.xxxco.com (tcp/443)
URL

https://www.xxxco.com/


OUTPUT

WAS Scanner has enumerated the following Directory Listings:

- https://www.xxxco.com/wp-content/uploads/
- https://www.xxxco.com/wp-includes/

Webinar Gratuito IT Security | Web Application Vulnerability Assessment Example

98203 (1) - WordPress User Enumeration	
Synopsis	
WordPress User Enumeration	
Description	
In default WordPress installation there are several methods to enumerate authors username. These WordPress users can then be used in brute-force attacks against WordPress login page to guess passwords.	
See Also	
https://wordpress.org/support/article/htaccess/ https://hackertarget.com/wordpress-user-enumeration/	
Solution	
Block requests to sensitive user information at the server using .htaccess file or WAF for example. You should block or redirect all requests made to '/wp-json/wp/v2/users/' and to 'author' parameter (via GET and POST requests).	
Risk Factor	
Medium	
CVSS v3.0 Base Score	
5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)	
CVSS v2.0 Base Score	
5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)	
References	
XREF	CWE:200 WASC:Information Leakage HIPAA:164.306(a)(1) HIPAA:164.306(a)(2) CAPEC:116 CAPEC:13 CAPEC:169 CAPEC:22 CAPEC:224 CAPEC:285 CAPEC:287 CAPEC:290 CAPEC:291 CAPEC:292 CAPEC:293 CAPEC:294 CAPEC:295 CAPEC:296 CAPEC:297 CAPEC:298 CAPEC:299 CAPEC:300 CAPEC:301 CAPEC:302 CAPEC:303 CAPEC:304 CAPEC:305 CAPEC:306 CAPEC:307 CAPEC:308 CAPEC:309 CAPEC:310 CAPEC:312 CAPEC:313 CAPEC:317 CAPEC:318 CAPEC:319 CAPEC:320 CAPEC:321 CAPEC:322 CAPEC:323 CAPEC:324 CAPEC:325 CAPEC:326 CAPEC:327 CAPEC:328 CAPEC:329 CAPEC:330 CAPEC:472 CAPEC:497 CAPEC:508 CAPEC:573 CAPEC:574 CAPEC:575 CAPEC:576 CAPEC:577 CAPEC:59 CAPEC:60 CAPEC:616 CAPEC:643 CAPEC:646 CAPEC:651 CAPEC:79 DISA_STIG:APSC-DV-000460 OWASP:2010-A6 OWASP:2013-A5 OWASP:2017-A6 OWASP:2021-A1 OWASP_API:2019-API7 OWASP_API:2023-API8 OWASP_ASVS:4.0.2-8.3.4 PCI_DSS:3.2-6.5.8 ISO:27001-A.14.2.5 NIST:sp800_53-SI-15
Plugin Information	
Published: 2020/09/09, Modified: 2023/12/06	
Instances	
https://www.xxxxco.com (tcp/443) URL	
https://www.xxxxco.com/?author=1	

Instances	
https://www.xxxxco.com (tcp/443) URL	
https://www.xxxxco.com/?author=1	
OUTPUT	
WAS Scanner has enumerated the following WordPress users: 	

Webinar Gratuito IT Security | Web Application Vulnerability Assessment Example

```
[!] 12 vulnerabilities identified:

[!] Title: WP <= 6.2 - Unauthenticated Blind SSRF via DNS Rebinding
References:
- https://wpscan.com/vulnerability/c8814e6e-78b3-4f63-a1d3-6906a84c1f11
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-3590
- https://blog.sonarsource.com/wordpress-core-unauthenticated-blind-ssrf/

[!] Title: WP < 6.2.1 - Directory Traversal via Translation Files
Fixed in: 6.1.2
References:
- https://wpscan.com/vulnerability/2999613a-b8c8-4ec0-9164-5dfe63adf6e6
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-2745
- https://wordpress.org/news/2023/05/wordpress-6-2-1-maintenance-security-release/

[!] Title: WP < 6.2.1 - Thumbnail Image Update via CSRF
Fixed in: 6.1.2
References:
- https://wpscan.com/vulnerability/a03d744a-9839-4167-a356-3e7da0f1d532
- https://wordpress.org/news/2023/05/wordpress-6-2-1-maintenance-security-release/

[!] Title: WP < 6.2.1 - Contributor+ Stored XSS via Open Embed Auto Discovery
Fixed in: 6.1.2
References:
- https://wpscan.com/vulnerability/3b574451-2852-4789-bc19-d5cc39948db5
- https://wordpress.org/news/2023/05/wordpress-6-2-1-maintenance-security-release/

[!] Title: WP < 6.2.2 - Shortcode Execution in User Generated Data
Fixed in: 6.1.3
References:
- https://wpscan.com/vulnerability/ef289d46-ea83-4fa5-b003-0352c690fd89
- https://wordpress.org/news/2023/05/wordpress-6-2-1-maintenance-security-release/
- https://wordpress.org/news/2023/05/wordpress-6-2-2-security-release/

[!] Title: WP < 6.2.1 - Contributor+ Content Injection
Fixed in: 6.1.2
References:
- https://wpscan.com/vulnerability/1527ebdb-18bc-4f9d-9c20-8d729a628670
- https://wordpress.org/news/2023/05/wordpress-6-2-1-maintenance-security-release/

[!] Title: WP 5.6-6.3.1 - Contributor+ Stored XSS via Navigation Block
Fixed in: 6.1.4
References:
- https://wpscan.com/vulnerability/cd130bb3-8d04-4375-a89a-883af131ed3a
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-38000
- https://wordpress.org/news/2023/10/wordpress-6-3-2-maintenance-and-security-release/
```

Webinar Gratuito IT Security | Web Application Vulnerability Assessment Example

```
[!] 12 vulnerabilities identified:

[!] Title: WP <= 6.2 - Unauthenticated Blind SSRF via DNS Rebinding
References:
- https://wpscan.com/vulnerability/c8814e6e-78b3-4f63-a1d3-6906a84c1f11
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-3590
- https://blog.sonarsource.com/wordpress-core-unauthenticated-blind-ssrf/

[!] Title: WP < 6.2.1 - Directory Traversal via Translation Files
Fixed in: 6.1.2
References:
- https://wpscan.com/vulnerability/2999613a-b8c8-4ec0-9164-5dfe63adf6e6
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-2745
- https://wordpress.org/news/2023/05/wordpress-6-2-1-maintenance-security-release/

[!] Title: WP < 6.2.1 - Thumbnail Image Update via CSRF
Fixed in: 6.1.2
References:
- https://wpscan.com/vulnerability/a03d744a-9839-4167-a356-3e7da0f1d532
- https://wordpress.org/news/2023/05/wordpress-6-2-1-maintenance-security-release/


[!] Title: WP < 6.2.1 - Contributor+ Stored XSS via Open Embed Auto Discovery
Fixed in: 6.1.2
References:
- https://wpscan.com/vulnerability/3b574451-2852-4789-bc19-d5cc39948db5
- https://wordpress.org/news/2023/05/wordpress-6-2-1-maintenance-security-release/

[!] Title: WP < 6.2.2 - Shortcode Execution in User Generated Data
Fixed in: 6.1.3
References:
- https://wpscan.com/vulnerability/ef289d46-ea83-4fa5-b003-0352c690fd89
- https://wordpress.org/news/2023/05/wordpress-6-2-1-maintenance-security-release/
- https://wordpress.org/news/2023/05/wordpress-6-2-2-security-release/

[!] Title: WP < 6.2.1 - Contributor+ Content Injection
Fixed in: 6.1.2
References:
- https://wpscan.com/vulnerability/1527ebdb-18bc-4f9d-9c20-8d729a628670
- https://wordpress.org/news/2023/05/wordpress-6-2-1-maintenance-security-release/

[!] Title: WP 5.6-6.3.1 - Contributor+ Stored XSS via Navigation Block
Fixed in: 6.1.4
References:
- https://wpscan.com/vulnerability/cd130bb3-8d04-4375-a89a-883af131ed3a
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-38000
- https://wordpress.org/news/2023/10/wordpress-6-3-2-maintenance-and-security-release/
```

Webinar Gratuito IT Security | Web Application Vulnerability Assessment Example

 **WPScan**

[Features](#) [Pricing](#) [Solutions](#) [Vulnerabilities](#) [Resources](#) [Login](#) [Talk to sales](#)

Be the first to know about new WordPress vulnerabilities

- ✓ All vulnerabilities are manually vetted in our database by seasoned WordPress security professionals.
- ✓ WPScan works with security researchers, vendors, and the WordPress community to triage vulnerabilities.
- ✓ The vulnerability database is updated constantly as we discover new threats.

[Get started](#)**621**
Vulnerabilities added in April**49.774**
Total vulnerabilities in our database

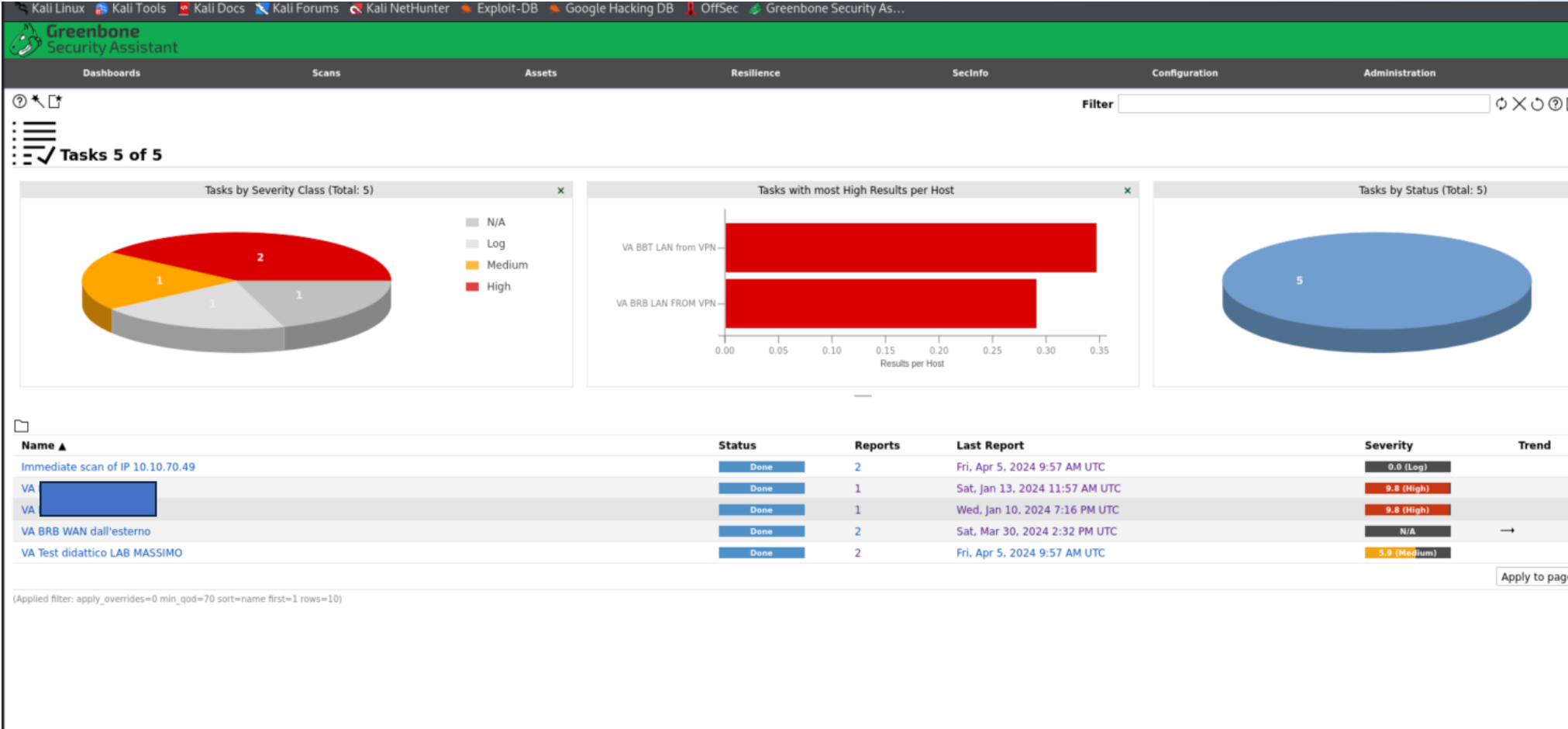
Webinar Gratuito IT Security | Web Application Vulnerability Assessment Example

```
- Nikto v2.5.0
-----
+ Multiple IPs found: [REDACTED]
+ Target IP: [REDACTED]
+ Target Hostname: [REDACTED]
+ Target Port: 80
+ Start Time: 2023-10-07 16:09:32 (GMT2)
-----
+ Server: openresty/1.13.6.1
+ /: IP address found in the 'server' header. The IP is "1.13.6.1". See:
https://portswigger.net/kb/issues/00600300\_private-ip-addresses-disclosed
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /6vlgPnHv.db: Uncommon header 'x-fail-reason' found, with contents: Bad Extension.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Scan terminated: 20 error(s) and 4 item(s) reported on remote host
+ End Time: 2023-10-07 16:49:11 (GMT2) (2379 seconds)
-----
+ 1 host(s) tested
```

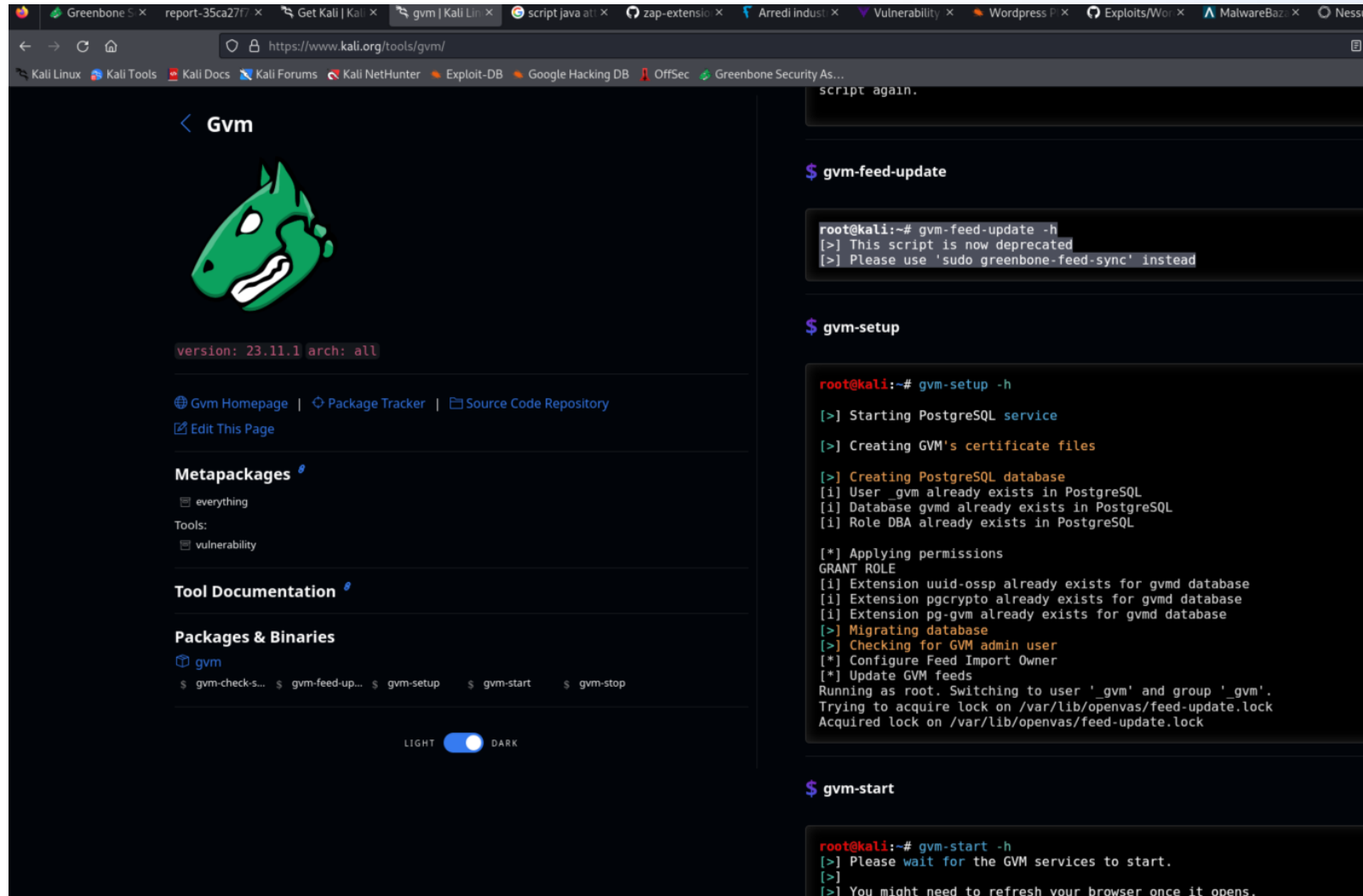
Webinar Gratuito IT Security | Web Application Vulnerability Assessment Example

```
- Nikto v2.5.0
-----
+ Multiple IPs found: [REDACTED]
+ Target IP: [REDACTED]
+ Target Hostname: [REDACTED]
+ Target Port: 80
+ Start Time: 2023-10-07 16:09:32 (GMT2)
-----
+ Server: openresty/1.13.6.1
+ /: IP address found in the 'server' header. The IP is "1.13.6.1". See:
https://portswigger.net/kb/issues/00600300\_private-ip-addresses-disclosed
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /6vlgPnHv.db: Uncommon header 'x-fail-reason' found, with contents: Bad Extension.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Scan terminated: 20 error(s) and 4 item(s) reported on remote host
+ End Time: 2023-10-07 16:49:11 (GMT2) (2379 seconds)
-----
+ 1 host(s) tested
```

Webinar Gratuito IT Security | Web Application Vulnerability Assessment Example



Webinar Gratuito IT Security | Web Application Vulnerability Assessment Example



The screenshot displays the Kali Linux web interface for GVM (Greenbone Vulnerability Manager). The browser address bar shows `https://www.kali.org/tools/gvm/`. The page features the GVM logo (a green dragon head) and the version `23.11.1` for `arch: all`. Navigation links include [Gvm Homepage](#), [Package Tracker](#), [Source Code Repository](#), and [Edit This Page](#). The **Metapackages** section lists `everything` and `vulnerability`. The **Tool Documentation** section is also visible. The **Packages & Binaries** section lists `gvm` and provides links to `gvm-check-s...`, `gvm-feed-up...`, `gvm-setup`, `gvm-start`, and `gvm-stop`. A dark mode toggle is at the bottom.

On the right, a terminal window shows the execution of several GVM commands:

```
script again.

$ gvm-feed-update

root@kali:~# gvm-feed-update -h
[>] This script is now deprecated
[>] Please use 'sudo greenbone-feed-sync' instead

$ gvm-setup

root@kali:~# gvm-setup -h

[>] Starting PostgreSQL service
[>] Creating GVM's certificate files

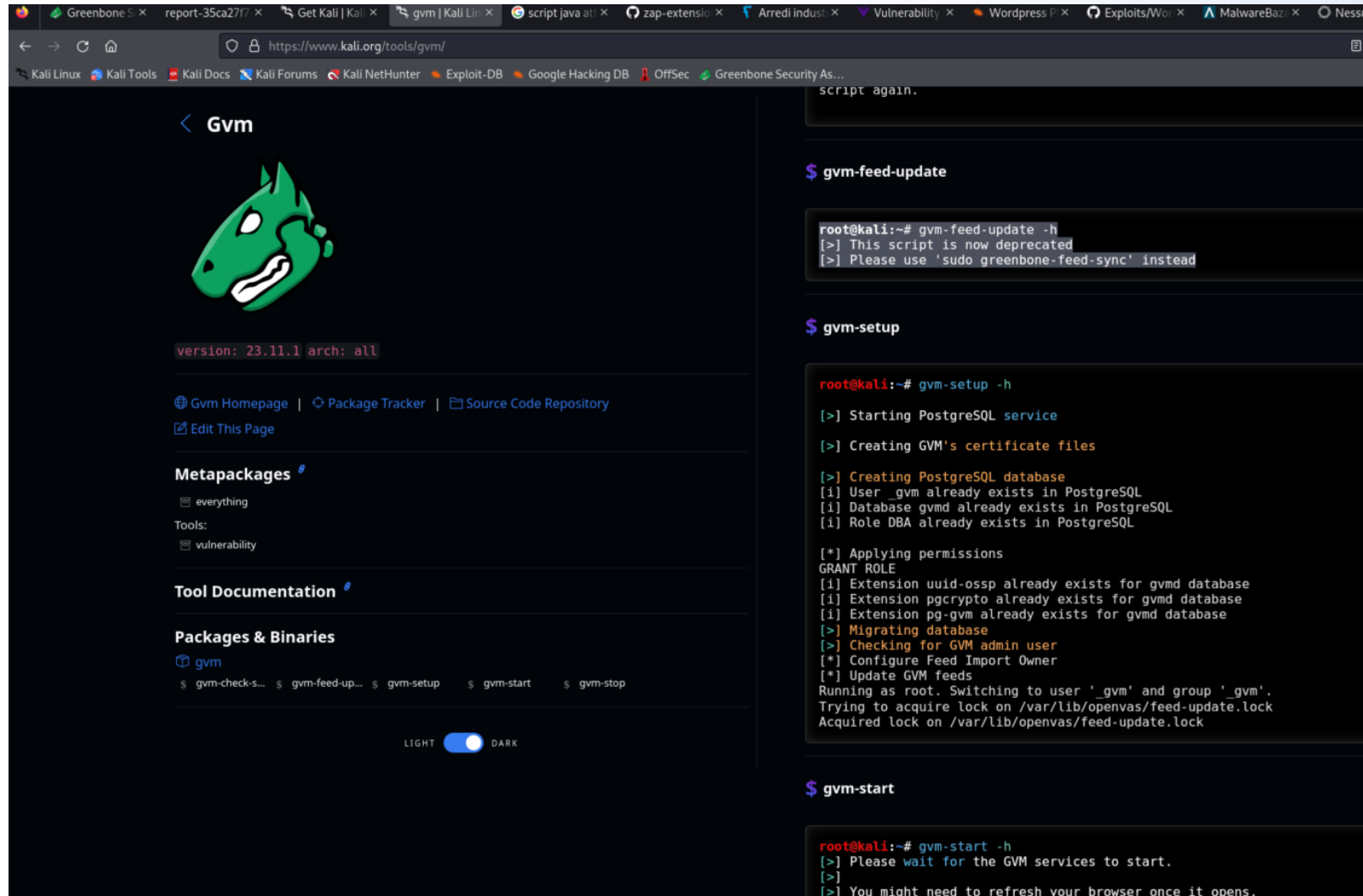
[>] Creating PostgreSQL database
[i] User _gvm already exists in PostgreSQL
[i] Database gvmd already exists in PostgreSQL
[i] Role DBA already exists in PostgreSQL

[*] Applying permissions
GRANT ROLE
[i] Extension uuid-ossf already exists for gvmd database
[i] Extension pgcrypto already exists for gvmd database
[i] Extension pg-gvm already exists for gvmd database
[>] Migrating database
[>] Checking for GVM admin user
[*] Configure Feed Import Owner
[*] Update GVM feeds
Running as root. Switching to user '_gvm' and group 'gvm'.
Trying to acquire lock on /var/lib/opensvas/feed-update.lock
Acquired lock on /var/lib/opensvas/feed-update.lock

$ gvm-start

root@kali:~# gvm-start -h
[>] Please wait for the GVM services to start.
[>]
[>] You might need to refresh your browser once it opens.
```

Webinar Gratuito IT Security | Web Application Vulnerability Assessment Example



The screenshot displays the Kali Linux web interface for GVM (Greenbone Vulnerability Manager). The browser address bar shows `https://www.kali.org/tools/gvm/`. The page features the GVM logo (a green dragon head) and the version `23.11.1` for `arch: all`. Navigation links include [Gvm Homepage](#), [Package Tracker](#), [Source Code Repository](#), and [Edit This Page](#). The **Metapackages** section lists `everything` and `vulnerability`. The **Tool Documentation** section is also visible. The **Packages & Binaries** section lists `gvm` and provides links to `gvm-check-s...`, `gvm-feed-up...`, `gvm-setup`, `gvm-start`, and `gvm-stop`. A dark mode toggle is at the bottom.

On the right, a terminal window shows the execution of several GVM commands:

```
script again.

$ gvm-feed-update

root@kali:~# gvm-feed-update -h
[>] This script is now deprecated
[>] Please use 'sudo greenbone-feed-sync' instead

$ gvm-setup

root@kali:~# gvm-setup -h

[>] Starting PostgreSQL service
[>] Creating GVM's certificate files

[>] Creating PostgreSQL database
[i] User _gvm already exists in PostgreSQL
[i] Database gvmd already exists in PostgreSQL
[i] Role DBA already exists in PostgreSQL

[*] Applying permissions
GRANT ROLE
[i] Extension uuid-ossf already exists for gvmd database
[i] Extension pgcrypto already exists for gvmd database
[i] Extension pg-gvm already exists for gvmd database
[>] Migrating database
[>] Checking for GVM admin user
[*] Configure Feed Import Owner
[*] Update GVM feeds
Running as root. Switching to user '_gvm' and group 'gvm'.
Trying to acquire lock on /var/lib/opensvas/feed-update.lock
Acquired lock on /var/lib/opensvas/feed-update.lock

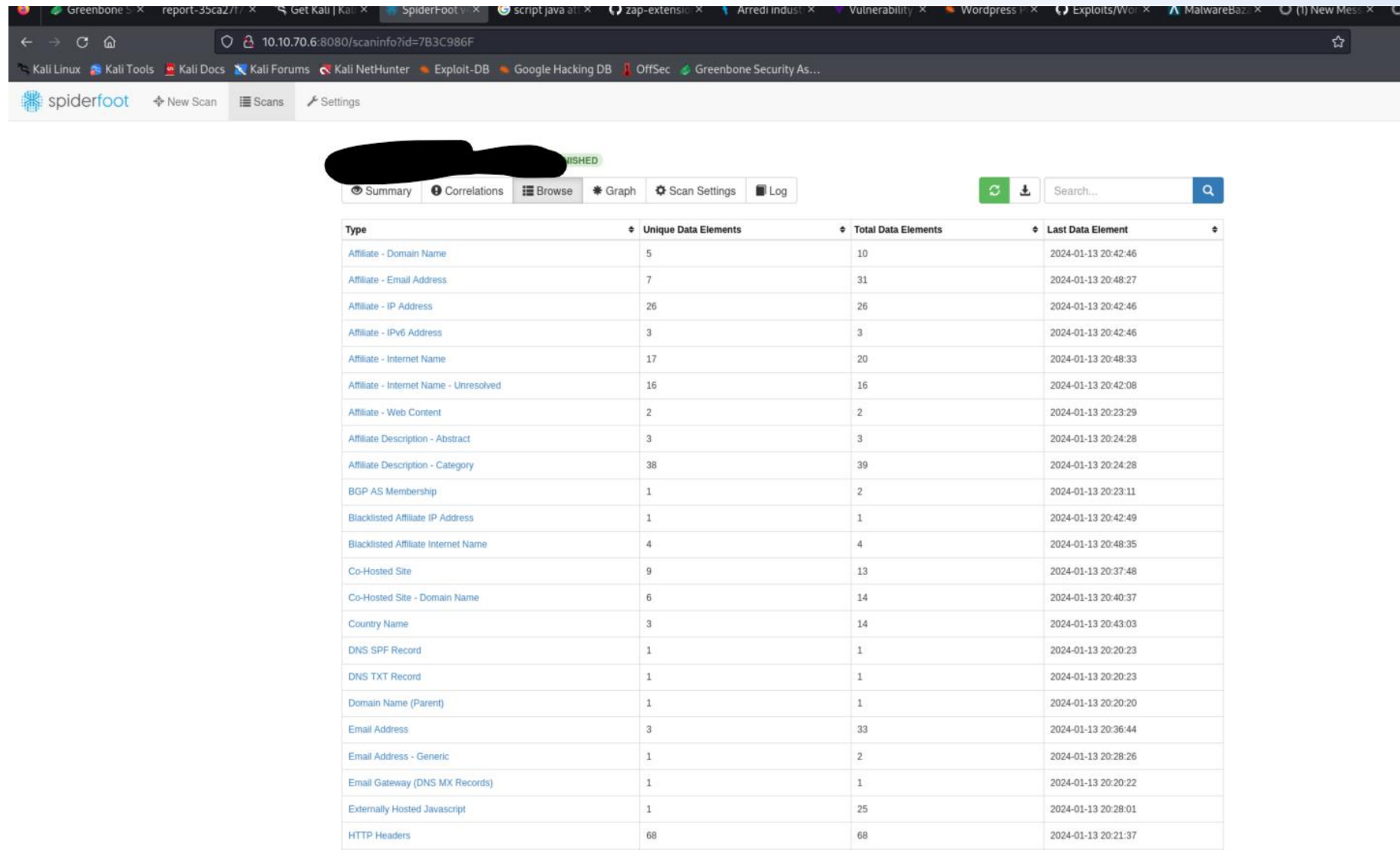
$ gvm-start

root@kali:~# gvm-start -h
[>] Please wait for the GVM services to start.
[>]
[>] You might need to refresh your browser once it opens.
```

Webinar Gratuito IT Security | Web Application Vulnerability Assessment Example

```
nouser@kali: ~  
File Actions Edit View Help  
(nouser@kali)~  
$ sudo spiderfoot -l 10.10.70.6:8080  
[sudo] password for nouser:  
  
*****  
Use SpiderFoot by starting your web browser of choice and  
browse to http://10.10.70.6:8080/  
*****  
  
2024-04-17 10:21:17,301 [INFO] sf : Starting web server at 10.10.70.6:8080 ...  
2024-04-17 10:21:17,315 [WARNING] sf :  
*****  
Warning: passwd file contains no passwords. Authentication disabled.  
Please consider adding authentication to protect this instance!  
Refer to https://www.spiderfoot.net/documentation/#security.  
*****  
  
Everything  
Tools  
Vulnerability  
  
Tool Documentation  
Packages & Binaries
```

Webinar Gratuito IT Security | Web Application Vulnerability Assessment Example



spiderfoot

Summary Correlations Browse Graph Scan Settings Log

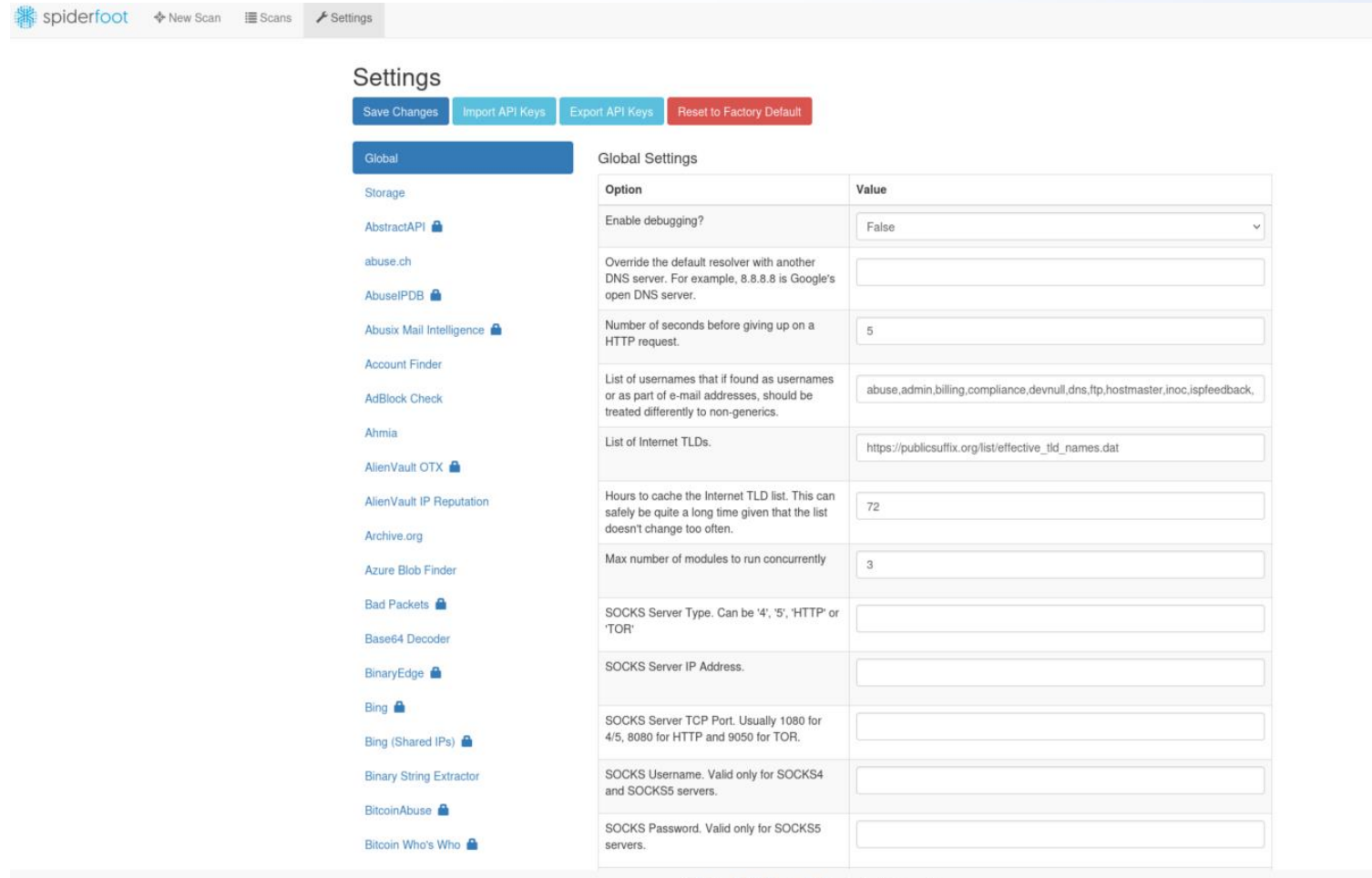
Type	Unique Data Elements	Total Data Elements	Last Data Element
Affiliate - Domain Name	5	10	2024-01-13 20:42:46
Affiliate - Email Address	7	31	2024-01-13 20:48:27
Affiliate - IP Address	26	26	2024-01-13 20:42:46
Affiliate - IPv6 Address	3	3	2024-01-13 20:42:46
Affiliate - Internet Name	17	20	2024-01-13 20:48:33
Affiliate - Internet Name - Unresolved	16	16	2024-01-13 20:42:08
Affiliate - Web Content	2	2	2024-01-13 20:23:29
Affiliate Description - Abstract	3	3	2024-01-13 20:24:28
Affiliate Description - Category	38	39	2024-01-13 20:24:28
BGP AS Membership	1	2	2024-01-13 20:23:11
Blacklisted Affiliate IP Address	1	1	2024-01-13 20:42:49
Blacklisted Affiliate Internet Name	4	4	2024-01-13 20:48:35
Co-Hosted Site	9	13	2024-01-13 20:37:48
Co-Hosted Site - Domain Name	6	14	2024-01-13 20:40:37
Country Name	3	14	2024-01-13 20:43:03
DNS SPF Record	1	1	2024-01-13 20:20:23
DNS TXT Record	1	1	2024-01-13 20:20:23
Domain Name (Parent)	1	1	2024-01-13 20:20:20
Email Address	3	33	2024-01-13 20:36:44
Email Address - Generic	1	2	2024-01-13 20:28:26
Email Gateway (DNS MX Records)	1	1	2024-01-13 20:20:22
Externally Hosted Javascript	1	25	2024-01-13 20:28:01
HTTP Headers	68	68	2024-01-13 20:21:37

CORSO: Ethical Hacker & Security Manager



SENIOR TRAINER: Massimo Chirivì

Webinar Gratuito IT Security | Web Application Vulnerability Assessment Example



The screenshot displays the Spiderfoot web application interface, specifically the 'Settings' page. The top navigation bar includes the Spiderfoot logo, a 'New Scan' button, a 'Scans' button, and a 'Settings' button. Below the navigation bar, the 'Settings' page is titled, and there are four buttons: 'Save Changes', 'Import API Keys', 'Export API Keys', and 'Reset to Factory Default'. A sidebar on the left lists various modules, with 'Global' selected. The main content area is titled 'Global Settings' and contains a table with two columns: 'Option' and 'Value'.

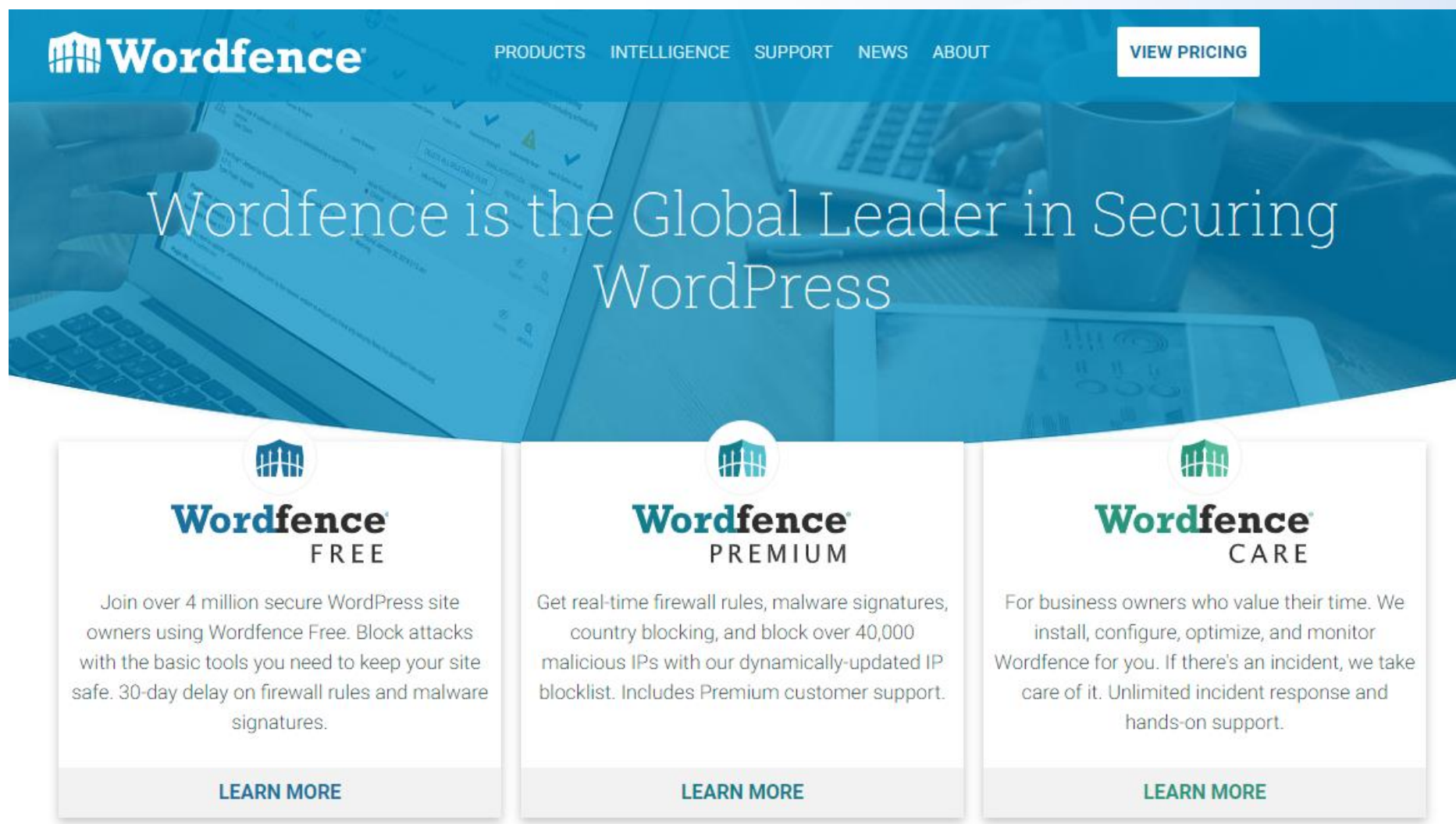
Option	Value
Enable debugging?	False
Override the default resolver with another DNS server. For example, 8.8.8.8 is Google's open DNS server.	
Number of seconds before giving up on a HTTP request.	5
List of usernames that if found as usernames or as part of e-mail addresses, should be treated differently to non-generics.	abuse,admin,billing,compliance,devnull,dns,ftp,hostmaster,inoc,ispfeedback,
List of Internet TLDs.	https://publicsuffix.org/list/effective_tld_names.dat
Hours to cache the Internet TLD list. This can safely be quite a long time given that the list doesn't change too often.	72
Max number of modules to run concurrently	3
SOCKS Server Type. Can be '4', '5', 'HTTP' or 'TOR'	
SOCKS Server IP Address.	
SOCKS Server TCP Port. Usually 1080 for 4/5, 8080 for HTTP and 9050 for TOR.	
SOCKS Username. Valid only for SOCKS4 and SOCKS5 servers.	
SOCKS Password. Valid only for SOCKS5 servers.	

CORSO: Ethical Hacker & Security Manager



SENIOR TRAINER: Massimo Chirivì

Webinar Gratuito IT Security | Web Application Vulnerability Assessment Example



The image shows a screenshot of the Wordfence website. The top navigation bar includes links for PRODUCTS, INTELLIGENCE, SUPPORT, NEWS, and ABOUT, along with a VIEW PRICING button. The main banner features the Wordfence logo and the text "Wordfence is the Global Leader in Securing WordPress". Below the banner, there are three pricing cards for Wordfence Free, Premium, and Care. Each card includes a description of the service and a "LEARN MORE" button.

Wordfence [®] FREE	Wordfence [®] PREMIUM	Wordfence [®] CARE
Join over 4 million secure WordPress site owners using Wordfence Free. Block attacks with the basic tools you need to keep your site safe. 30-day delay on firewall rules and malware signatures.	Get real-time firewall rules, malware signatures, country blocking, and block over 40,000 malicious IPs with our dynamically-updated IP blocklist. Includes Premium customer support.	For business owners who value their time. We install, configure, optimize, and monitor Wordfence for you. If there's an incident, we take care of it. Unlimited incident response and hands-on support.
LEARN MORE	LEARN MORE	LEARN MORE

CORSO: Ethical Hacker & Security Manager



SENIOR TRAINER: Massimo Chirivì

Webinar Gratuito IT Security | Web Application Vulnerability Assessment Example

[Wordfence Alert] Problems found on www[redacted] Esterni [News/AttackExample x]

WordPress [redacted]@aruba.it
a soc

Traduci in italiano

This email was sent from your website using the Wordfence plugin.
Wordfence found the following new issues on [redacted] (existing issues were also found again).
Alert generated at Tuesday 16th of April 2024 at 02:05:01 AM

See the details of these scan results on your site at: [https://www\[redacted\].min/admin.php?page=WordfenceScan](https://www[redacted].min/admin.php?page=WordfenceScan)

Critical Problems:

* The Plugin "Elementor" needs an upgrade (3.19.2 -> 3.21.0).

Update includes security-related fixes.
Vulnerability Severity: 6.4/10.0 (Medium) [Vulnerability Information](https://wordpress.org/plugins/elementor/#developers)
<https://wordpress.org/plugins/elementor/#developers>

16 existing issues were found again and are not shown.

NOTE: You are using the free version of Wordfence. Upgrade today:

- Receive real-time Firewall and Scan engine rule updates for protection as threats emerge
- Real-time IP Blocklist blocks the most malicious IPs from accessing your site
- Country blocking
- IP reputation monitoring
- Schedule scans to run more frequently and at optimal times
- Access to Premium Support
- Discounts for multi-year and multi-license purchases

Click here to upgrade to Wordfence Premium:
<https://www.wordfence.com/zz2/wordfence-signup/>

No longer an administrator for this site? [Click here](#) to stop receiving security alerts.

Rispondi Rispondi a tutti Inoltra

Recently Blocked Attacks

Time	IP / Action
March 4, 2024 10:04am	64.227.165.111 (India) Blocked for Known malicious User-Agents
March 4, 2024 1:03am	148.72.232.135 (Singapore) Blocked for Malicious File Upload (PHP)
March 4, 2024 1:03am	68.178.222.76 (United States) Blocked for Malicious File Upload (PHP)
March 4, 2024 1:03am	194.143.204.82 (Spain) Blocked for Malicious File Upload (PHP)
March 4, 2024 12:39am	91.92.240.125 (Bulgaria) Blocked for Known malicious User-Agents
March 3, 2024 3:58pm	172.233.143.221 (United States) Blocked for Known malicious User-Agents
March 3, 2024 3:58pm	172.233.143.221 (United States) Blocked for Known malicious User-Agents
March 3, 2024 3:58pm	172.233.143.221 (United States) Blocked for Known malicious User-Agents
March 3, 2024 3:58pm	172.233.143.221 (United States) Blocked for Known malicious User-Agents
March 3, 2024 3:58pm	172.233.143.221 (United States) Blocked for Known malicious User-Agents

and 133 additional attacks

[View Recent Traffic](#)

Recently Modified Files

Modified	File
March 2, 2024 6:48am	wp-content/uploads/wpforms/cache/addons.json
March 2, 2024 6:48am	wp-content/uploads/wpforms/cache/templates.json
March 2, 2024 6:48am	wp-content/uploads/wpforms/cache/docs.json
March 2, 2024 6:48am	wp-content/uploads/wpforms/cache/.htaccess
March 2, 2024 6:48am	wp-content/uploads/wpforms/cache/index.php
March 2, 2024 6:48am	wp-content/uploads/wpforms/.htaccess
March 1, 2024 12:42pm	wp-config.php
March 1, 2024 12:36pm	wp-content/languages/plugins/wpforms-lite-it_IT.po
March 1, 2024 12:36pm	wp-content/languages/plugins/wpforms-lite-it_IT.mo
March 1, 2024 12:36pm	wp-content/languages/plugins/wpforms-lite-it_IT.l10n.php

This list may include WordPress core/plugin/theme updates, error logs, cache files, and other normal changes.

AMPLIA LE TUE COMPETENZE

CON I CORSI DI ICT CONSULTANT

- Corso di Linux LPIC-1 Certificato
- Corso Windows Microsoft Livello Base
- Corso Ethical Hacker & Security manager
Certificato CompTIA Security+ e PenTest+
- Corso Sicurezza Informatica e Security Manager
Certificato CompTIA Security+
- Corso Penetration Test e Hacking Etico
Certificato CompTia PenTest+
- Laboratorio CompTIA Security+
- Laboratorio CompTIA PenTest+
- Corso di Informatica di Base
- Corso CompTIA Cloud Essentials+
- Corso IT Security Governance & Management
- Corso Windows Server Professional + Advanced Level
- Corso di Virtualizzazione di Base
- Corso di Networking Base - Avanzato
- Corso Trattamento dei Dati Personali Ambito Sanitario
- Corso Data Protection Officer a Scuola
- Corso Tutela della Privacy e Criminalità Informatica
- Corso GDPR Siti Internet Cookie e Informativa Privacy
- Corso Privacy Specialist DPO

MUSA
FORMAZIONE E LAVORO

VISITA

www.musaformazione.it

CONTATTACI SU WAPP
392 004 8820