Network Vulnerability Scanner Report (Light)

Unlock the full capabilities of this scanner

See what the DEEP scanner can do

Perform in-depth scanning and detect a wider range of vulnerabilities.

Scanner capabilities	Light scan	Deep scan
Open ports detection	✓	✓
Version based vulnerability detection	✓	✓
Active vulnerability detection (57000+ plugins)	✗	✓
Find service misconfigurations	✗	✓
Detect missing security patches	✗	✓

✓ assureworld.us

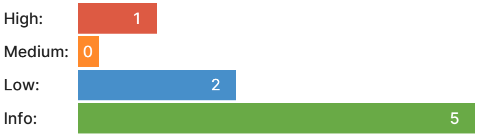
! The Light Network Scanner only ran limited, version-based detection. Upgrade to run Deep scansthat check for 20,000+ additional vulnerabilities - with fewer False Positives

Summary

Overall risk level:

High

Risk ratings:



Scan information:

Start time:	Oct 17, 2024 / 10:41:01 UTC+03
Finish time:	Oct 17, 2024 / 10:41:37 UTC+03
Scan duration:	36 sec
Tests performed:	8/8
Scan status:	Finished

Findings

Vulnerabilities found for PHP 8.2.19

port 443/tcp

UNCONFIRMED

Risk level	CVSS	CVE	Summary	Exploit
●	9.8	CVE-2024-4577	In PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, when using Apache and PHP-CGI on Windows, if the system is set up to use certain code pages, Windows may use "Best-Fit" behavior to replace characters in command line given to Win32 API functions. PHP CGI module may misinterpret those characters as PHP options, which may allow a malicious user to pass options to PHP binary being run, and thus reveal the source code of scripts, run arbitrary PHP code on the server, etc.	N/A
●	8.8	CVE-2024-5585	In PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, the fix for CVE-2024-1874 does not work if the command name includes trailing spaces. Original issue: when using proc_open() command with array syntax, due to insufficient escaping, if the arguments of the executed command are controlled by a malicious user, the user can supply arguments that would execute arbitrary commands in Windows shell.	N/A

●	5.9	CVE-2024-2408	The openssl_private_decrypt function in PHP, when using PKCS1 padding (OPENSSL_PKCS1_PADDING, which is the default), is vulnerable to the Marvin Attack unless it is used with an OpenSSL version that includes the changes from this pull request: https://github.com/openssl/openssl/pull/13817 (rsa_pkcs1_implicit_rejection). These changes are part of OpenSSL 3.2 and have also been backported to stable versions of various Linux distributions, as well as to the PHP builds provided for Windows since the previous release. All distributors and builders should ensure that this version is used to prevent PHP from being vulnerable. PHP Windows builds for the versions 8.1.29, 8.2.20 and 8.3.8 and above include OpenSSL patches that fix the vulnerability.	N/A
●	5.3	CVE-2024-5458	In PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, due to a code logic error, filtering functions such as filter_var when validating URLs (FILTER_VALIDATE_URL) for certain types of URLs the function will result in invalid user information (username + password part of URLs) being treated as valid user information. This may lead to the downstream code accepting invalid URLs as valid and parsing them incorrectly.	N/A

Details

Risk description:

These vulnerabilities expose the affected applications to the risk of unauthorized access to confidential data and possibly to denial of service attacks. An attacker could search for an appropriate exploit (or create one) for any of these vulnerabilities and use it to attack the system.

Notes:

- The vulnerabilities are identified based on the server's version.
- Only the first 30 vulnerabilities with the highest risk are shown for each port.

Recommendation:

We recommend you to upgrade the affected software to the latest version in order to eliminate the risks imposed by these vulnerabilities.

SPF record: Soft-fail ~all configuration

CONFIRMED

DNS Record Type	Description	Value
SPF	Sender Policy Framework	"v=spf1 include:_spf.mail.hostinger.com ~all"

Details

Vulnerability description:

We found that the Sender Policy Framework (SPF) record for the domain is configured with ~all (soft fail), which indicates that emails from unauthorized IP addresses are not explicitly denied. Instead, the recipient mail server is instructed to treat these messages with suspicion but may still accept them. This configuration may not provide enough protection against email spoofing and unauthorized email delivery, leaving the domain more vulnerable to impersonation attempts.

Risk description:

The ~all directive in an SPF record allows unauthorized emails to pass through some email servers, even though they fail SPF verification. While such emails may be marked as suspicious or placed into a spam folder, not all mail servers handle soft fail conditions consistently. This creates a risk that malicious actors can spoof the domain to send phishing emails or other fraudulent communications, potentially causing damage to the organization's reputation and leading to successful social engineering attacks.

Recommendation:

We recommend changing the SPF record's ~all (soft fail) directive to -all (hard fail). The -all setting tells recipient mail servers to reject emails from any IP addresses not listed in the SPF record, providing stronger protection against email spoofing. Ensure that all legitimate IP addresses and services that send emails on behalf of your domain are properly included in the SPF record before implementing this change.

Missing DMARC policy

CONFIRMED

We didn't find any TXT records associated with the target.

Details

Vulnerability description:

We found that the target server has no DMARC policy configured. A missing DMARC (Domain-based Message Authentication, Reporting, and Conformance) policy means that the domain is not enforcing any DMARC policies to protect against email spoofing and phishing attacks. Without DMARC, even if SPF (Sender Policy Framework) or DKIM (DomainKeys Identified Mail) are configured, there is no mechanism to tell receiving email servers how to handle messages that fail authentication. This leaves the domain vulnerable to abuse, such as email spoofing and impersonation.

Risk description:
Without a DMARC policy, your domain is highly vulnerable to email spoofing, allowing attackers to impersonate your brand and send fraudulent emails that appear legitimate. This can lead to phishing attacks targeting your customers, employees, or partners, potentially resulting in stolen credentials, financial loss, or unauthorized access to sensitive systems. Additionally, repeated spoofing attempts can severely damage your brand's reputation, as recipients may lose trust in communications from your domain, associating your brand with malicious activity. The absence of DMARC also prevents you from monitoring and mitigating email-based attacks, leaving your domain exposed to ongoing abuse.

Recommendation:
We recommend implementing a DMARC policy for your domain. Start by configuring a DMARC record with a policy of p=none, which will allow you to monitor email flows without impacting legitimate emails. This initial setup helps identify how emails from your domain are being processed by recipient servers. Once you've verified that legitimate emails are passing SPF and DKIM checks, you can gradually enforce stricter policies like p=quarantine or p=reject to protect against spoofing and phishing attacks. Additionally, include rua and ruf email addresses in the DMARC record to receive aggregate and forensic reports. These reports will provide valuable insights into authentication failures and help you detect any spoofing attempts.

IP Information

CONFIRMED

IP Address	Hostname	Location	Autonomous system (AS) Information	Organization (Name & Type)
91.108.103.145	assureworld.us	Manchester, England, United Kingdom	-	Ripe Network Coordination Centre (business)

Details

Risk description:
If an attacker knows the physical location of an organization's IP address and its Autonomous System (AS) number, they could launch targeted physical or cyber attacks, exploiting regional vulnerabilities or disrupting critical infrastructure.

Recommendation:
We recommend reviewing physical security measures and monitoring network traffic for unusual activity, indicating potential cyber threats. Additionally, implementing robust network segmentation and adopting encryption protocols for data in transit can help protect sensitive information, even if attackers are aware of the IP addresses and the Autonomous System (AS) number.

DNS Records

CONFIRMED

DNS Record Type	Description	Value
A	IPv4 address	84.32.84.82
NS	Name server	ns1.dns-parking.com
NS	Name server	ns2.dns-parking.com
MX	Mail server	10 mx2.hostinger.in
MX	Mail server	5 mx1.hostinger.in
SOA	Start of Authority	ns1.dns-parking.com. dns.hostinger.com. 2024101701 10000 2400 604800 600
AAAA	IPv6 address	2a02:4780:35:5b20:afc7:84fc:fc:bc64
SPF	Sender Policy Framework	"v=spf1 include:_spf.mail.hostinger.com ~all"
CAA	Certificate Authority Authorization	0 issue "globalsign.com"
CAA	Certificate Authority Authorization	0 issue "pki.goog"
CAA	Certificate Authority Authorization	0 issue "digicert.com"
CAA	Certificate Authority Authorization	0 issuewild "globalsign.com"
CAA	Certificate Authority Authorization	0 issuewild "letsencrypt.org"
CAA	Certificate Authority Authorization	0 issue "letsencrypt.org"
CAA	Certificate Authority Authorization	0 issuewild "digicert.com"
CAA	Certificate Authority Authorization	0 issuewild "pki.goog"
CAA	Certificate Authority Authorization	0 issue "comodoca.com"

CAA	Certificate Authority Authorization	0 issuewild "comodoca.com"
CAA	Certificate Authority Authorization	0 issuewild "sectigo.com"
CAA	Certificate Authority Authorization	0 issue "sectigo.com"

Details

Risk description:
An initial step for an attacker aiming to learn about an organization involves conducting searches on its domain names to uncover DNS records associated with the organization. This strategy aims to amass comprehensive insights into the target domain, enabling the attacker to outline the organization's external digital landscape. This gathered intelligence may subsequently serve as a foundation for launching attacks, including those based on social engineering techniques. DNS records pointing to services or servers that are no longer in use can provide an attacker with an easy entry point into the network.

Recommendation:
We recommend reviewing all DNS records associated with the domain and identifying and removing unused or obsolete records.

Web redirect detected on port 80

CONFIRMED

Port 80 redirects to 443

Details

Recommendation:
Vulnerability checks are skipped for ports that redirect to another port. We recommend scanning the redirected port directly.

Open ports discovery

CONFIRMED

Port	State	Service	Product	Product Version
80	open	http	hcdn	
443	open	https	hcdn	

Details

Risk description:
This is the list of ports that have been found on the target host. Having unnecessary open ports may expose the target to more risks because those network services and applications may contain vulnerabilities.

Recommendation:
We recommend reviewing the list of open ports and closing the ones which are not necessary for business purposes.

Server software and technologies

port 443/tcp

UNCONFIRMED

Software / Version	Category
PHP 8.2.19	Programming languages
Laravel	Web frameworks
Bootstrap 5.0.2	UI frameworks
Alpine.js	JavaScript frameworks
Lightbox	JavaScript libraries
Font Awesome	Font scripts
Hostinger	Hosting
Livewire	Web frameworks, Miscellaneous
HTTP/3	Miscellaneous

Details

Vulnerability description:
We noticed that server software and technology details are exposed, potentially aiding attackers in tailoring specific exploits against identified systems and versions.

Risk description:
The risk is that an attacker could use this information to mount specific attacks against the identified software type and version.

Recommendation:
We recommend you to eliminate the information which permits the identification of software platform, technology, server and operating system: HTTP server headers, HTML meta information, etc.

Scan coverage information

List of tests performed (8/8)

- ✓ Running IP information lookup phase...
- ✓ DNS enumeration
- ✓ Web redirect detected on port 80
- ✓ Port discovery
- ✓ Checking for soft-fail ~all configuration in SPF record
- ✓ Checking for missing DMARC policy
- ✓ Fingerprinting website for technologies on port 443
- ✓ Scanning for vulnerabilities of PHP on port 443

Scan parameters

Target:	assureworld.us
Preset:	Custom
Scanning engines:	Version_based
Check alive:	False
Extensive modules:	-
Protocol type:	TCP
Ports to scan:	Top 100 ports
CVEs:	
Requests per second:	-