

Website Vulnerability Scanner Report

✓ <https://replenish-your-space.webnode.ec/>

Target added due to a redirect from <https://replenish-your-space.webnode.ec/>

! The Light Website Scanner didn't check for critical issues like SQLi, XSS, Command Injection, XXE, etc. [Upgrade to run Deep scans](#) with 40+ tests and detect more vulnerabilities.

Summary

Overall risk level:

Medium

Risk ratings:



Scan information:

Start time: Sep 09, 2024 / 18:33:26 UTC-05
Finish time: Sep 09, 2024 / 18:37:29 UTC-05
Scan duration: 4 min, 3 sec
Tests performed: 39/39
Scan status: Finished

Findings

🚩 Insecure cookie setting: domain too loose

CONFIRMED

URL	Cookie Name	Evidence
https://replenish-your-space.webnode.ec/	PHPSESSID	Set-Cookie: .replenish-your-space.webnode.ec Request / Response

▼ Details

Risk description:

The risk is that a cookie set for example.com may be sent along with the requests sent to dev.example.com, calendar.example.com, hostedsite.example.com. Potentially risky websites under your main domain may access those cookies and use the victim session from the main site.

Recommendation:

The **Domain** attribute should be set to the origin host to limit the scope to that particular server. For example if the application resides on server app.mysite.com, then it should be set to **Domain=app.mysite.com**

Classification:

CWE : [CWE-614](#)

OWASP Top 10 - 2017 : [A6 - Security Misconfiguration](#)

OWASP Top 10 - 2021 : [A5 - Security Misconfiguration](#)

🚩 Missing security header: Content-Security-Policy

CONFIRMED

URL	Evidence
https://replenish-your-space.webnode.ec/	Response does not include the HTTP Content-Security-Policy security header or meta tag Request / Response

▼ Details

Risk description:

The risk is that if the target application is vulnerable to XSS, lack of this header makes it easily exploitable by attackers.

Recommendation:

Configure the Content-Security-Header to be sent with each HTTP response in order to apply the specific policies needed by the

application.

References:

https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy>

Classification:

CWE : [CWE-693](#)
OWASP Top 10 - 2017 : [A6 - Security Misconfiguration](#)
OWASP Top 10 - 2021 : [A5 - Security Misconfiguration](#)

Missing security header: Referrer-Policy

CONFIRMED

URL	Evidence
https://replenish-your-space.webnode.ec/	Response headers do not include the Referrer-Policy HTTP security header as well as the <meta> tag with name 'referrer' is not present in the response. Request / Response

▼ Details

Risk description:

The risk is that if a user visits a web page (e.g. "http://example.com/pricing/") and clicks on a link from that page going to e.g. "https://www.google.com", the browser will send to Google the full originating URL in the **Referer** header, assuming the Referrer-Policy header is not set. The originating URL could be considered sensitive information and it could be used for user tracking.

Recommendation:

The Referrer-Policy header should be configured on the server side to avoid user tracking and inadvertent information leakage. The value **no-referrer** of this header instructs the browser to omit the Referer header entirely.

References:

https://developer.mozilla.org/en-US/docs/Web/Security/Referer_header:_privacy_and_security_concerns

Classification:

CWE : [CWE-693](#)
OWASP Top 10 - 2017 : [A6 - Security Misconfiguration](#)
OWASP Top 10 - 2021 : [A5 - Security Misconfiguration](#)

Missing security header: Strict-Transport-Security

CONFIRMED

URL	Evidence
https://replenish-your-space.webnode.ec/	Response headers do not include the HTTP Strict-Transport-Security header Request / Response

▼ Details

Risk description:

The risk is that lack of this header permits an attacker to force a victim user to initiate a clear-text HTTP connection to the server, thus opening the possibility to eavesdrop on the network traffic and extract sensitive information (e.g. session cookies).

Recommendation:

The Strict-Transport-Security HTTP header should be sent with each HTTPS response. The syntax is as follows:

Strict-Transport-Security: max-age=<seconds>[; includeSubDomains]

The parameter **max-age** gives the time frame for requirement of HTTPS in seconds and should be chosen quite high, e.g. several months. A value below 7776000 is considered as too low by this scanner check.
The flag **includeSubDomains** defines that the policy applies also for sub domains of the sender of the response.

Classification:

CWE : [CWE-693](#)
OWASP Top 10 - 2017 : [A6 - Security Misconfiguration](#)
OWASP Top 10 - 2021 : [A5 - Security Misconfiguration](#)

Missing security header: X-Content-Type-Options

CONFIRMED

URL	Evidence
-----	----------

<https://replenish-your-space.webnode.ec/>

Response headers do not include the X-Content-Type-Options HTTP security header
[Request / Response](#)

▼ Details

Risk description:

The risk is that lack of this header could make possible attacks such as Cross-Site Scripting or phishing in Internet Explorer browsers.

Recommendation:

We recommend setting the X-Content-Type-Options header such as `X-Content-Type-Options: nosniff`.

References:

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options>

Classification:

CWE : [CWE-693](#)

OWASP Top 10 - 2017 : [A6 - Security Misconfiguration](#)

OWASP Top 10 - 2021 : [A5 - Security Misconfiguration](#)

🚩 Robots.txt file found

CONFIRMED

URL

<https://replenish-your-space.webnode.ec/robots.txt>

▼ Details

Risk description:

There is no particular security risk in having a robots.txt file. However, it's important to note that adding endpoints in it should not be considered a security measure, as this file can be directly accessed and read by anyone.

Recommendation:

We recommend you to manually review the entries from robots.txt and remove the ones which lead to sensitive locations in the website (ex. administration panels, configuration files, etc).

References:

<https://www.theregister.co.uk/2015/05/19/robotstxt/>

Classification:

OWASP Top 10 - 2017 : [A6 - Security Misconfiguration](#)

OWASP Top 10 - 2021 : [A5 - Security Misconfiguration](#)










Screenshot:

```
User-agent: robot
Disallow: /
User-agent: *
Disallow: /servers/frontend/
Crawl-delay: 10
Sitemap: http://replenish-your-space.webnode.ec/sitemap.xml
```

Figure 1. robots.txt

🚩 Server software and technology found

UNCONFIRMED ⓘ

Software / Version	Category
 Google Font API	Font scripts
 Nginx	Web servers, Reverse proxies
 OpenResty	Web servers
 PHP	Programming languages
 Hammer.js 2.0.8	JavaScript libraries
 jQuery 3.7.0	JavaScript libraries
 Open Graph	Miscellaneous
 Cart Functionality	Ecommerce
 WebNode 2	CMS, Page builders

▼ Details

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.

References:

https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server.html

Classification:

OWASP Top 10 - 2017 : [A6 - Security Misconfiguration](#)

OWASP Top 10 - 2021 : [A5 - Security Misconfiguration](#)

Screenshot:



Figure 2. Website Screenshot

🚩 Interesting files found

UNCONFIRMED ⓘ

URL	Page Title	Page Size	Summary
https://replenish-your-space.webnode.ec/server/	ToCupboard	49.76 KB	Possibly Macromedia JRun or CRX WebDAV upload

▼ Details

Risk description:

The risk is that these files/folders usually contain sensitive information which may help attackers to mount further attacks against the

server. Manual validation is required.

Recommendation:

We recommend you to analyze if the mentioned files/folders contain any sensitive information and restrict their access according to the business purposes of the application.

Classification:

CWE : [CWE-200](#)

OWASP Top 10 - 2017 : [A6 - Security Misconfiguration](#)

OWASP Top 10 - 2021 : [A5 - Security Misconfiguration](#)

🚩 Login Interface Found

CONFIRMED

URL	Evidence
https://replenish-your-space.webnode.ec/user-login	<pre><input id="field-wnd_EmailField_678302290" maxLength="255" name="wnd_EmailField_678302290" required="" type="email" value="@"/> <input id="field-wnd_PasswordField_677472068" minLength="6" name="wnd_PasswordField_677472068" required="" type="password" value="" /> <button class="b-btn-l" name="send" type="submit" value="wnd_UserLoginFormBlock_731490140"> Entrar </button></pre> <p>Request / Response</p>
https://replenish-your-space.webnode.ec/user-registration/	<pre><input id="field-wnd_EmailField_125190680" maxLength="255" name="wnd_EmailField_125190680" required="" type="email" value="@"/> <input id="field-wnd_PasswordField_122910904" minLength="6" name="wnd_PasswordField_122910904" required="" type="password" value="" /> <button class="b-btn-l" name="send" type="submit" value="wnd_UserRegistrationFormBlock_945784491"> Regístrate </button></pre> <p>Request / Response</p>

▼ Details

Risk description:

The risk is that an attacker could use this interface to mount brute force attacks against known passwords and usernames combinations leaked throughout the web.

Recommendation:

Ensure each interface is not bypassable using common knowledge of the application or leaked credentials using occasional password audits.

References:

<https://pentest-tools.com/network-vulnerability-scanning/password-auditor>

<http://capec.mitre.org/data/definitions/16.html>

Screenshot:

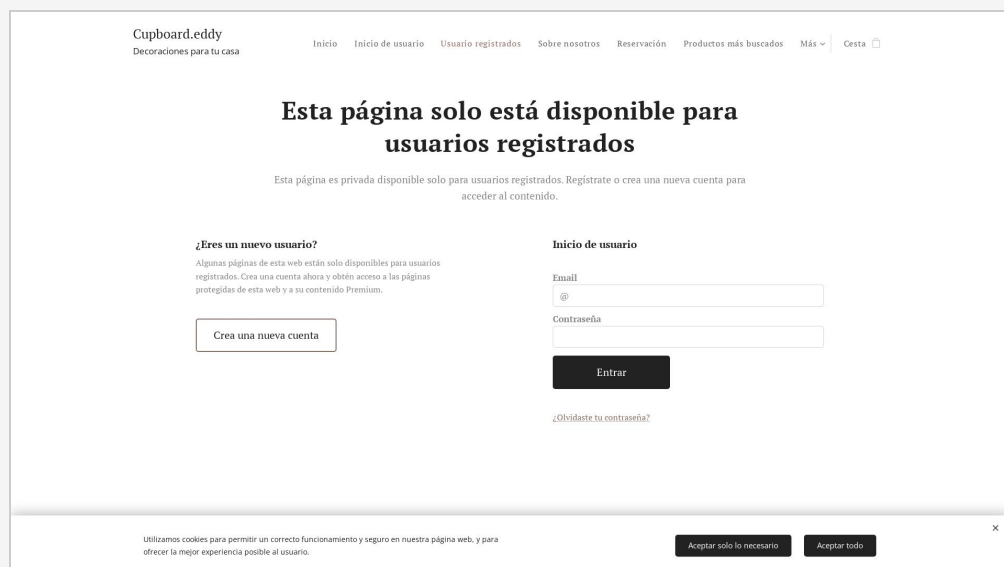


Figure 3. Login Interface

Security.txt file is missing

CONFIRMED

URL

Missing: <https://replenish-your-space.webnode.ec/.well-known/security.txt>

Details

Risk description:

There is no particular risk in not having a security.txt file for your server. However, this file is important because it offers a designated channel for reporting vulnerabilities and security issues.

Recommendation:

We recommend you to implement the security.txt file according to the standard, in order to allow researchers or users report any security issues they find, improving the defensive mechanisms of your server.

References:

<https://securitytxt.org/>

Classification:

OWASP Top 10 - 2017 : [A6 - Security Misconfiguration](#)

OWASP Top 10 - 2021 : [A5 - Security Misconfiguration](#)

Spider results

URL	Method	Parameters	Page Title	Page Size	Status Code
https://replenish-your-space.webnode.ec/	GET		ToCupboard	49.75 KB	200
https://replenish-your-space.webnode.ec/cart	GET		Cesta de la compra :: ToCupboard	43.58 KB	200
https://replenish-your-space.webnode.ec/p/	GET		404 - Página no encontrada :: ToCupboard	41.78 KB	404
https://replenish-your-space.webnode.ec/p/kit-cocina-4p	GET		Kit cocina 4p :: ToCupboard	59.8 KB	200
https://replenish-your-space.webnode.ec/p/kit-cocina-4p/	POST	Body: id=200000030	Kit cocina 4p :: ToCupboard	59.8 KB	200
https://replenish-your-space.webnode.ec/p/kit-concina	GET		Kit concina :: ToCupboard	60.43 KB	200
https://replenish-your-space.webnode.ec/p/kit-concina/	POST	Body: id=200000025	Kit concina :: ToCupboard	60.43 KB	200
https://replenish-your-space.webnode.ec/p/mesa-lateral	GET		Mesa lateral :: ToCupboard	60.47 KB	200
https://replenish-your-space.webnode.ec/p/mesa-lateral/	POST	Body: id=200000026	Mesa lateral :: ToCupboard	60.48 KB	200
https://replenish-your-space.webnode.ec/politica-de-privacidad	GET		Política de privacidad :: ToCupboard	48.55 KB	200
https://replenish-your-space.webnode.ec/reservacion	GET		Reservación :: ToCupboard	49.44 KB	200
https://replenish-your-space.webnode.ec/reservacion/	POST	Body: wnd_DateField_108237514= wnd_EmailField_311805246=@ wnd_RadioGroupField_786734198=wnd_Ra dioGroupOption_368912947 wnd_ShortTextField_958699366=	Reservación :: ToCupboard	49.46 KB	200

https://replenish-your-space.webnode.ec/sobre-nosotros	GET		Sobre nosotros :: ToCupboard	61.57 KB	200
https://replenish-your-space.webnode.ec/terminos-y-condiciones	GET		Términos y Condiciones :: ToCupboard	43.83 KB	200
https://replenish-your-space.webnode.ec/tienda-online	GET		Productos más buscados :: ToCupboard	61.01 KB	200
https://replenish-your-space.webnode.ec/user-login	GET		Usuario registrados :: ToCupboard	45 KB	200
https://replenish-your-space.webnode.ec/user-login/	POST	Body: wnd_EmailField_678302290=@ wnd_PasswordField_677472068=	Usuario registrados :: ToCupboard	45 KB	200
https://replenish-your-space.webnode.ec/user-recovery/	GET		Recuperación de contraseña :: ToCupboard	43.15 KB	200
https://replenish-your-space.webnode.ec/user-recovery/	POST	Body: wnd_EmailField_519868731=@	Recuperación de contraseña :: ToCupboard	43.15 KB	200
https://replenish-your-space.webnode.ec/user-registration/	GET		Inicio de usuario :: ToCupboard	43.75 KB	200
https://replenish-your-space.webnode.ec/user-registration/	POST	Body: wnd_EmailField_125190680=@ wnd_PasswordField_122910904= wnd_ShortTextField_266783542=	Inicio de usuario :: ToCupboard	43.75 KB	200
https://replenish-your-space.webnode.ec/cart/	GET		Cesta de la compra :: ToCupboard	43.58 KB	200
https://replenish-your-space.webnode.ec/checkout	GET		Cesta de la compra :: ToCupboard	43.58 KB	200
https://replenish-your-space.webnode.ec/checkout/	GET		Cesta de la compra :: ToCupboard	43.58 KB	200
https://replenish-your-space.webnode.ec/home	GET		ToCupboard	49.75 KB	200
https://replenish-your-space.webnode.ec/home/	GET		ToCupboard	49.75 KB	200
https://replenish-your-space.webnode.ec/p	GET		404 - Página no encontrada :: ToCupboard	41.78 KB	404
https://replenish-your-space.webnode.ec/p/armario-de-vidrio	GET		Armario de vidrio :: ToCupboard	59.84 KB	200
https://replenish-your-space.webnode.ec/p/armario-de-vidrio/	GET		Armario de vidrio :: ToCupboard	59.84 KB	200
https://replenish-your-space.webnode.ec/p/armario-organizador	GET		Armario organizador :: ToCupboard	59.87 KB	200
https://replenish-your-space.webnode.ec/p/armario-organizador/	GET		Armario organizador :: ToCupboard	59.87 KB	200
https://replenish-your-space.webnode.ec/p/kit-cocina-4p/	GET		Kit cocina 4p :: ToCupboard	59.8 KB	200
https://replenish-your-space.webnode.ec/p/kit-concina/	GET		Kit concina :: ToCupboard	60.43 KB	200
https://replenish-your-space.webnode.ec/p/mesa-lateral/	GET		Mesa lateral :: ToCupboard	60.47 KB	200
https://replenish-your-space.webnode.ec/p/modular-3-repisas	GET		Modular 3 repisas :: ToCupboard	59.81 KB	200

https://replenish-your-space.webnode.ec/p/modular-3-repisas/	GET		Modular 3 repisas :: ToCupboard	59.81 KB	200
https://replenish-your-space.webnode.ec/page-not-found-404	GET		404 - Página no encontrada :: ToCupboard	42.12 KB	404
https://replenish-your-space.webnode.ec/page-not-found-404/	GET		404 - Página no encontrada :: ToCupboard	42.12 KB	404
https://replenish-your-space.webnode.ec/politica-de-privacidad/	GET		Política de privacidad :: ToCupboard	48.55 KB	200
https://replenish-your-space.webnode.ec/reservacion/	GET		Reservación :: ToCupboard	49.44 KB	200
https://replenish-your-space.webnode.ec/server/	GET		ToCupboard	49.73 KB	200
https://replenish-your-space.webnode.ec/servers	GET		404 - Página no encontrada :: ToCupboard	41.78 KB	404
https://replenish-your-space.webnode.ec/servers/	GET		404 - Página no encontrada :: ToCupboard	41.78 KB	404
https://replenish-your-space.webnode.ec/servers/frontend	GET		404 - Página no encontrada :: ToCupboard	41.78 KB	404
https://replenish-your-space.webnode.ec/sobre-nosotros/	GET		Sobre nosotros :: ToCupboard	61.57 KB	200
https://replenish-your-space.webnode.ec/terminos-y-condiciones/	GET		Términos y Condiciones :: ToCupboard	43.83 KB	200
https://replenish-your-space.webnode.ec/tienda-online/	GET		Productos más buscados :: ToCupboard	61.01 KB	200
https://replenish-your-space.webnode.ec/user-login/	GET		Usuario registrados :: ToCupboard	45 KB	200
https://replenish-your-space.webnode.ec/user-recovery	GET		Recuperación de contraseña :: ToCupboard	43.15 KB	200
https://replenish-your-space.webnode.ec/user-registration	GET		Inicio de usuario :: ToCupboard	43.75 KB	200

▼ Details

Risk description:

The table contains all the unique pages the scanner found. The duplicated URLs are not available here as scanning those is considered unnecessary

Recommendation:

We recommend to advanced users to make sure the scan properly detected most of the URLs in the application.

References:

[All the URLs the scanner found, including duplicates](#) (available for 90 days after the scan date)

Cloud Hosted URLs

URL	Cloud Provider	Found at URL
https://d9a107cd26.cbaul-cdnwnd.com/c77e579aaa525e5bd27b7212e458fe27/200000042-e4734e4736	AWS	https://replenish-your-space.webnode.ec/

https://duyn491kcolsw.cloudfront.net/files/34/34m/	AWS	https://replenish-your-space.webnode.ec/
https://replenish-your-space.webnode.ec/tienda-online	AWS	https://replenish-your-space.webnode.ec/
https://www.webnode.com/es/	AWS	https://replenish-your-space.webnode.ec/
https://www.webnode.ec/?utm_campaign=free2&utm_content=wnd2&utm_medium=footer&utm_source=text	AWS	https://replenish-your-space.webnode.ec/terminos-y-condiciones

▼ Details

Risk description:

The risk is that publicly accessible web addresses hosted in the cloud can expose sensitive information. If access to these resources is not carefully configured, it makes it easier for attackers to gain unauthorized access and cause data breaches.

Recommendation:

We recommend you to implement strong access controls and conduct regular security checks to protect these URLs. Ensure compliance with best practices to protect sensitive data.

- 🚩 website is accessible.
- 🚩 Nothing was found for vulnerabilities of server-side software.
- 🚩 Nothing was found for client access policies.
- 🚩 Outdated JavaScript libraries were merged into server-side software vulnerabilities.
- 🚩 Nothing was found for use of untrusted certificates.
- 🚩 Nothing was found for enabled HTTP debug methods.
- 🚩 Nothing was found for sensitive files.
- 🚩 Nothing was found for administration consoles.
- 🚩 Nothing was found for information disclosure.
- 🚩 Nothing was found for software identification.
- 🚩 Nothing was found for enabled HTTP OPTIONS method.
- 🚩 Nothing was found for secure communication.
- 🚩 Nothing was found for directory listing.
- 🚩 Nothing was found for error messages.

🚩 Nothing was found for debug messages.

🚩 Nothing was found for code comments.

🚩 Nothing was found for Insecure Direct Object Reference.

🚩 Nothing was found for mixed content between HTTP and HTTPS.

🚩 Nothing was found for internal error code.

🚩 Nothing was found for HttpOnly flag of cookie.

🚩 Nothing was found for Secure flag of cookie.

🚩 Nothing was found for Server Side Request Forgery.

🚩 Nothing was found for Open Redirect.

🚩 Nothing was found for Exposed Backup Files.

🚩 Nothing was found for unsafe HTTP header Content Security Policy.

🚩 Nothing was found for OpenAPI files.

🚩 Nothing was found for file upload.

Scan coverage information

List of tests performed (39/39)

- ✓ Starting the scan...
- ✓ Checking for missing HTTP header - Content Security Policy...
- ✓ Checking for missing HTTP header - Referrer...
- ✓ Checking for missing HTTP header - Strict-Transport-Security...
- ✓ Checking for missing HTTP header - X-Content-Type-Options...
- ✓ Checking for domain too loose set for cookies...
- ✓ Spidering target...
- ✓ Scanning for cloud URLs on target...
- ✓ Checking for login interfaces...
- ✓ Checking for website technologies...
- ✓ Checking for vulnerabilities of server-side software...
- ✓ Checking for client access policies...
- ✓ Checking for robots.txt file...
- ✓ Checking for absence of the security.txt file...
- ✓ Checking for outdated JavaScript libraries...
- ✓ Checking for use of untrusted certificates...
- ✓ Checking for enabled HTTP debug methods...

- ✓ Checking for sensitive files...
- ✓ Checking for administration consoles...
- ✓ Checking for interesting files... (this might take a few hours)
- ✓ Checking for information disclosure... (this might take a few hours)
- ✓ Checking for software identification...
- ✓ Checking for enabled HTTP OPTIONS method...
- ✓ Checking for secure communication...
- ✓ Checking for directory listing...
- ✓ Checking for error messages...
- ✓ Checking for debug messages...
- ✓ Checking for code comments...
- ✓ Checking for Insecure Direct Object Reference...
- ✓ Checking for mixed content between HTTP and HTTPS...
- ✓ Checking for internal error code...
- ✓ Checking for HttpOnly flag of cookie...
- ✓ Checking for Secure flag of cookie...
- ✓ Checking for Server Side Request Forgery...
- ✓ Checking for Open Redirect...
- ✓ Checking for Exposed Backup Files...
- ✓ Checking for unsafe HTTP header Content Security Policy...
- ✓ Checking for OpenAPI files...
- ✓ Checking for file upload...

Scan parameters

Target: https://replenish-your-space.webnode.ec/
Scan type: Light
Authentication: False

Scan stats

Unique Injection Points Detected:	31
URLs spidered:	76
Total number of HTTP requests:	15442
Average time until a response was received:	6ms
Total number of HTTP request errors:	42