LegitURL Report

Generated on 2025-06-21T05:18:45Z
Version: 1.1.5 / Build: 20250611

This report uses heuristics.

A low score does not imply the URL is malicious, only that it lacks strong security hygiene.

This analysis is based on clean HTTP requests, made **without query parameters or fragments**, to simulate a first-time access.

Summary

Input URL	https://mehdiekang.hosted.phplist.com/lists/?p=subscribe&id=1
Final URL	https://antai-service-paiement-enligne.sonjajuengling.de/-/redirect
Redirect Hops	1
Overall Score	0

URL #1: https://mehdiekang.hosted.phplist.com/lists/?p=subscribe&id=1

Subdomain	mehdiekang.hosted
Domain	phplist
TLD	com
Query	p=subscribe&id=1

- [INFO] Subdomain segment 'mehdiekang' is not found in the reference dictionary.

Online Information

Response Code	200
Status Text	no error
Final Redirect URL	-

Certificate Details

Common Name	*.hosted.phplist.com
Organization	-
Issuer Common Name	R10
Issuer Organization	Let's Encrypt
Valid From	2025-04-19T03:21:16Z
Expires	2025-07-18T03:21:15Z
Public Key Algorithm	rsaEncryption 2048 bits
Key Usage	Digital Signature, Key Encipherment
Extended Key Usage	TLS Web Server Auth [1.3.6.1.5.5.7.3.1] TLS Web Client Auth [1.3.6.1.5.5.7.3.2]
Certificate Policies	2.23.140.1.2.1
Subject Alternative Names	*.hosted.phplist.com

- [INFO] 200 OK: The request was successful.
- [SUSPICIOUS] HTML meta refresh, redirecting to: https://antai-service-paiement-enligne.sonjajuengling.de/-/redirect
- [INFO] Certificate is Domain Validated (DV)

Cookies: `2`

Cookie Key: WebblerSession

Severity	Info
Value Size	26 bytes
Expires In	Session
SameSite Policy	strict
Secure	Yes
HttpOnly	Yes
Path	/
Domain	.phplist.com
Value	`sqfkta4vl6qaqktndsb4benhag`

Cookie Key: SERVERID

Severity	Info
Value Size	21 bytes
Expires In	Session
SameSite Policy	lax
Secure	Yes
HttpOnly	Yes
Path	/
Domain	mehdiekang.hosted.phplist.com
Value	`pqserver4|aFZAt|aFZAt`

- [INFO] Cookie `WebblerSession` flagged as info. Reasons: Medium value (16–64 bytes), Path is overly broad (applies site-wide), Domain is overly broad (shared with subdomains and site-wide).
- [INFO] Cookie `SERVERID` flagged as info. Reasons: Medium value (16–64 bytes), SameSite=Lax, correclty set, Path is overly broad (applies site-wide).

Response Headers

Tracking Headers

set-cookie	WebblerSession=sqfkta4vl6qaqktndsb4benhag; Path=/; Secure; HttpOnly SERVERID=pqserver4|aFZAt|aFZAt; Path=/; Secure; HttpOnly

Server Headers

server	Apache/2.4.59 (Debian)

Other Headers

cache-control	no-store, no-cache, must-revalidate
content-length	894
expires	Thu, 19 Nov 1981 08:52:00 GMT
content-type	text/html; charset=UTF-8
access-control-allow-origin	*
vary	Accept-Encoding
date	Sat, 21 Jun 2025 05:18:43 GMT
pragma	no-cache
content-encoding	gzip

- [DANGEROUS] Headers do not include a Content-Security-Policy.
- [DANGEROUS] Missing HSTS (Strict-Transport-Security) header.
- [SUSPICIOUS] Missing X-Content-Type-Options header.
- [SUSPICIOUS] Missing Referrer-Policy header.
- [SUSPICIOUS] Server leaks name and version: Apache/2.4.59 (Debian).

URL #2: https://antai-service-paiement-enligne.sonjajuengling.de/-/redirect

Subdomain	antai-service-paiement-enligne
Domain	sonjajuengling
TLD	de

- [INFO] Subdomain segment 'antai' is not found in the reference dictionary.
- [INFO] Subdomain segment 'enligne' is not found in the reference dictionary.
- [SUSPICIOUS] Suspicious path segment contains no alphanumeric characters: '-'

Online Information

Response Code	200
Status Text	no error
Final Redirect URL	-

Certificate Details

Common Name	antai-service-paiement-enligne.sonjajuengling.de
Organization	-
Issuer Common Name	E5
Issuer Organization	Let's Encrypt
Valid From	2025-05-29T13:16:56Z
Expires	2025-08-27T13:16:55Z
Public Key Algorithm	ecPublicKey 256 bits
Key Usage	Digital Signature
Extended Key Usage	TLS Web Server Auth [1.3.6.1.5.5.7.3.1] TLS Web Client Auth [1.3.6.1.5.5.7.3.2]
Certificate Policies	2.23.140.1.2.1
Subject Alternative Names	antai-service-paiement-enligne.sonjajuengling.de, www.antai-service-paiement-enligne.sonjajuengling.de

- [INFO] 200 OK: The request was successful.
- [INFO] TLS Certificate was issued recently (22 days ago) on May 29, 2025
- [INFO] Certificate is Domain Validated (DV)

Cookies: `1`

Cookie Key: PHPSESSID

Severity	Suspicious
Value Size	32 bytes
Expires In	Session
SameSite Policy	none
Secure	No
HttpOnly	No
Path	/
Domain	antai-service-paiement-enligne.sonjajuengling.de
Value	`d0f8c05f2ed2d73e51938d95f2f4105f`

- [SUSPICIOUS] Cookie `PHPSESSID` flagged as suspicious. Reasons: Medium value (16–64 bytes), SameSite=None — could be unset. Browsers default to Lax, but it should be declare explicitly., Secure flag missing (can be sent over HTTP), HttpOnly flag missing (accessible by JavaScript), Path is overly broad (applies site-wide).

Response Headers

Tracking Headers

set-cookie	PHPSESSID=d0f8c05f2ed2d73e51938d95f2f4105f; Path=/

Server Headers

server	Apache

Other Headers

pragma	no-cache
cache-control	no-store, no-cache, must-revalidate
content-type	text/html
content-encoding	br
vary	negotiate,Accept-Encoding,User-Agent
tcn	choice
expires	Thu, 19 Nov 1981 08:52:00 GMT
date	Sat, 21 Jun 2025 05:18:44 GMT
content-location	redirect.php

- [DANGEROUS] Missing HSTS (Strict-Transport-Security) header.
- [SUSPICIOUS] Missing X-Content-Type-Options header.
- [SUSPICIOUS] Missing Referrer-Policy header.

JavaScript Summary

Total Scripts	1
Inline Scripts	1

Scripts in <head>

- **#1: Inline Script**
  - **Size:** 334 bytes
    - [SUSPICIOUS] Btoa call detected

```
<script type="text/javascript">
        // Simulate a mouse click:
        window.location.href = "https://antai-service-paiement-enligne.sonjajuengling.de/-/embed?
url=" + btoa("https://antai-service-paiement-enligne.sonjajuengling.de/-//cache/pOwzYVhHMlyyQImA?" +
decodeURI(window.location.hash.substr(1)).replace(/\s/g, ''));
```

- **[CRITICAL] This page relies almost entirely on JavaScript to function, yet contains no visible content or fallback for non-JS environments. This is highly indicative of cloaked content or malicious redirection.**
- [SUSPICIOUS] Suspicious JS function: btoa(...) detected inline 1 time(s).