Website Vulnerability Scanner Report

✔ **http://theme6.com.au/**

Target added due to a redirect from http://theme6.com.au

Summary

Overall risk level:

Medium

Risk ratings:

Critical:	0
High:	0
Medium:	1
Low:	4
Info:	2

Scan information:

Start time:	Mar 30, 2026 / 08:21:34 UTC+03
Finish time:	Mar 30, 2026 / 08:48:23 UTC+03
Scan duration:	26 min, 49 sec
Tests performed:	74
Scan status:	Finished

Findings

Communication is not secure

port 80/tcp

CONFIRMED

URL	Response URL	Evidence
http://theme6.com.au/	http://theme6.com.au/	Communication is made over unsecure, unencrypted HTTP.

Details

Risk description:

The risk is that an attacker who manages to intercept the communication at the network level can read and modify the data transmitted (including passwords, secret tokens, credit card information and other sensitive data).

Recommendation:

We recommend you to reconfigure the web server to use HTTPS - which encrypts the communication between the web browser and the server.

Classification:

CWE : CWE-319
OWASP Top 10 - 2017 : A3 - Sensitive Data Exposure
OWASP Top 10 - 2021 : A4 - Insecure Design
OWASP Top 10 - 2025 : A04 - Cryptographic Failures

Missing security header: X-Content-Type-Options

port 80/tcp

CONFIRMED

URL	Evidence
http://theme6.com.au/	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
OWASP Top 10 - 2025 : A02 - Security Misconfiguration

Missing security header: Content-Security-Policy

CONFIRMED

port 80/tcp

URL	Evidence
http://theme6.com.au/	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-1021
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration
OWASP Top 10 - 2025 : A02 - Security Misconfiguration

Missing security header: Referrer-Policy

CONFIRMED

port 80/tcp

URL	Evidence
http://theme6.com.au/	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
OWASP Top 10 - 2025 : A02 - Security Misconfiguration

Server software and technology found

UNCONFIRMED

port 80/tcp

Software / Version	Category
Nginx	Web servers, Reverse proxies

OpenResty 1.27.1.1	Web servers

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:
CWE : CWE-200
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration
OWASP Top 10 - 2025 : A02 - Security Misconfiguration

Screenshot:

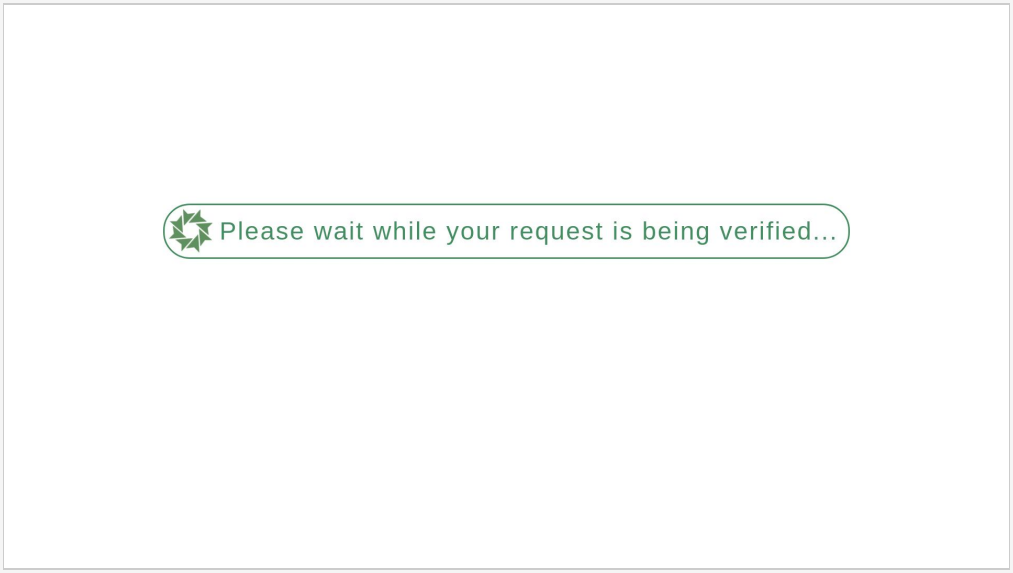

Figure 1. Website Screenshot

Input Reflected in Response

port 80/tcp

CONFIRMED

URL	Method	Vulnerable Parameter	Evidence	Replay Attack
http://theme6.com.au/	GET	pttdcebc3ec (Query Parameter)	Injected the string `pttad60bacb` in the **pttdcebc3ec query parameter** and it was found reflected in the response. Request / Response	

Details

Risk description:
The risk is that the reflection of input without proper sanitization or encoding can potentially be leveraged by attackers to inject malicious scripts or content in the client browser context.

Recommendation:
It is recommended that a tester inspects this issue manually to find out if it can be escalated to higher-risk vulnerabilities.

References:
https://owasp.org/www-community/attacks/xss
https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html

Classification:
CWE : CWE-20
OWASP Top 10 - 2021 : A3 - Injection

OWASP Top 10 - 2025 : A05 - Injection

Spider Results

UNCONFIRMED

URL	Method	Page Title	Page Size	Status Code
http://theme6.com.au/	GET	One moment, please...	11.67 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)

Scan coverage information

List of tests performed (74)

Port 80

- ✔ Scanned for secure communication
- ✔ Scanned for missing HTTP header - Content Security Policy
- ✔ Scanned for missing HTTP header - Referrer
- ✔ Scanned for missing HTTP header - X-Content-Type-Options
- ✔ Scanned for website technologies
- ✔ Scanned for Input Reflected in response body
- ✔ Performed web-crawling on target
- ✔ Scanned for version-based vulnerabilities of server-side software
- ✔ Scanned for client access policies
- ✔ Scanned for robots.txt file
- ✔ Scanned for absence of the security.txt file
- ✔ Scanned for CORS misconfiguration
- ✔ Scanned for use of untrusted certificates
- ✔ Scanned for enabled HTTP debug methods
- ✔ Scanned for administration consoles
- ✔ Scanned for information disclosure
- ✔ Scanned for software identification
- ✔ Scanned for sensitive files
- ✔ Scanned for interesting files
- ✔ Performed URL search in Wayback Machine
- ✔ Scanned for enabled HTTP OPTIONS method
- ✔ Scanned for GraphQL endpoints
- ✔ Performed fuzzing for OpenAPI files
- ✔ Scanned for misconfigurations
- ✔ Scanned for directory listing
- ✔ Scanned for passwords submitted unencrypted
- ✔ Scanned for Cross-Site Scripting
- ✔ Scanned for SQL Injection
- ✔ Scanned for Local File Inclusion
- ✔ Scanned for OS Command Injection
- ✔ Scanned for error messages
- ✔ Scanned for debug messages
- ✔ Scanned for code comments
- ✔ Scanned for missing HTTP header - Strict-Transport-Security
- ✔ Scanned for XML External Entity Injection
- ✔ Scanned for Insecure Direct Object Reference

- ✔ Scanned for passwords submitted in URLs
- ✔ Scanned for domain too loose set for cookies
- ✔ Scanned for mixed content between HTTP and HTTPS
- ✔ Scanned for cross domain file inclusion
- ✔ Scanned for internal error code
- ✔ Scanned for HttpOnly flag of cookie
- ✔ Scanned for Secure flag of cookie
- ✔ Scanned for login interfaces
- ✔ Scanned for secure password submission
- ✔ Scanned for sensitive data
- ✔ Scanned for Server Side Request Forgery
- ✔ Scanned for Open Redirect
- ✔ Scanned for PHP Code Injection
- ✔ Scanned for JavaScript Code Injection
- ✔ Scanned for Ruby Code Injection
- ✔ Scanned for Python Code Injection
- ✔ Scanned for Perl Code Injection
- ✔ Scanned for Remote Code Execution through Log4j
- ✔ Scanned for Server Side Template Injection
- ✔ Scanned for Remote Code Execution through VIEWSTATE
- ✔ Scanned for Prototype Pollution
- ✔ Scanned for Exposed Backup Files
- ✔ Scanned for Request URL Override
- ✔ Scanned for HTTP/1.1 Request Smuggling
- ✔ Scanned for CSRF
- ✔ Scanned for NoSQL Injection
- ✔ Scanned for Insecure Deserialization
- ✔ Scanned for unsafe HTTP header Content Security Policy
- ✔ Scanned for OpenAPI files
- ✔ Scanned for file upload
- ✔ Scanned for SQL statement in request parameter
- ✔ Scanned for password returned in later response
- ✔ Scanned for Path Disclosure
- ✔ Scanned for Session Token in URL
- ✔ Scanned for API endpoints
- ✔ Scanned for Response Header Injection
- ✔ Scanned for emails
- ✔ Scanned for missing HTTP header - Rate Limit

Scan parameters

Target:	http://theme6.com.au/
Scan type:	Deep_scan_default
Authentication:	False
fingerprint:	True
software_vulnerabilities:	True
check_robots:	True
outdated_js:	True
untrusted_certificates:	True
client_access_policies:	True
http_debug_methods:	True
security_txt:	True
cors_misconfiguration:	True
resource_discovery:	True
sensitive_files:	True
admin_consoles:	True
interesting_files:	True
server_info_disc:	True
server_software:	True
misconfigurations:	True
graphql_endpoint:	True
fuzz_openapi_locations:	True
ai_endpoint_discovery:	True
approach:	Auto
depth:	10
max_time:	3600
requests_per_second:	100
xss:	True

sqli:	True
lfi:	True
oscmdi:	True
ssrf:	True
open_redirect:	True
broken_authentication:	True
php_code_injection:	True
js_code_injection:	True
ruby_code_injection:	True
python_code_injection:	True
perl_code_injection:	True
log4j_rce:	True
ssti:	True
xxe:	True
viewstate_rce:	True
prototype_pollution:	True
backup_files:	True
request_url_override:	True
http_request_smuggling:	True
csrf:	True
insecure_deserialization:	True
nosqli:	True
session_fixation:	True
idor:	True
jwt:	True
response_header_injection:	True
security_headers:	True
cookie_security:	True
directory_listing:	True
secure_communication:	True
weak_password_submission:	True
error_debug_messages:	True
password_cleartext:	True
cross_domain_source:	True
mixed_content:	True
sensitive_data:	True
login_interfaces:	True
file_upload:	True
openapi_documents:	True
path_disclosure:	True
sql_statement_in_request:	True
password_in_response:	True
session_token_in_url:	True
api_endpoint:	True

Scan stats

Unique Injection Points Detected:	1
URLs spidered:	1
Total number of HTTP requests:	12626
Average time until a response was received:	14ms
Total number of HTTP request errors:	264