



DAST TEST

ZURI 9

Versão 2024Q4.10



1. Informações gerais

Este documento contém as evidências do teste DAST (OWASP ZAP) realizado no pacote de atualização do Zuri. Teste DAST (Dynamic Application Security Testing) é uma técnica de teste de segurança de aplicações que simula um ataque de um invasor externo em um aplicativo em execução. Nesse tipo de teste, a ferramenta de teste realiza uma série de solicitações para a aplicação em teste, fornecendo diferentes entradas e observando as respostas do sistema. O objetivo do teste DAST é identificar vulnerabilidades de segurança que possam ser exploradas por atacantes externos. OWASP ZAP (Zed Attack Proxy) é uma ferramenta de segurança de código aberto, utilizada para testar a segurança de aplicações web. Desenvolvida pela comunidade OWASP (Open Web Application Security Project), o ZAP é uma ferramenta amplamente utilizada e confiável, capaz de identificar vulnerabilidades em aplicações web, incluindo as mais complexas. O teste DAST foi implementado no pipeline de geração de pacotes do Zuri, ficando assim documentado com os registros de geração do pacote. Em caso de dúvidas, entre em contato com o nosso suporte para acompanhamento, através do e-mail suporte@gozuri.com.

2. Resultado do teste

22/maio/2025 10:40

Total of 2 URLs

PASS: Vulnerable JS Library (Powered by Retire.js) [10003]
PASS: In Page Banner Information Leak [10009]
PASS: Cookie No HttpOnly Flag [10010]
PASS: Cookie Without Secure Flag [10011]
PASS: Re-examine Cache-control Directives [10015]
PASS: Cross-Domain JavaScript Source File Inclusion [10017]
PASS: Content-Type Header Missing [10019]
PASS: Anti-clickjacking Header [10020]
PASS: X-Content-Type-Options Header Missing [10021]
PASS: Information Disclosure - Debug Error Messages [10023]
PASS: Information Disclosure - Sensitive Information in URL [10024]
PASS: Information Disclosure - Sensitive Information in HTTP Referrer Header [10025]
PASS: HTTP Parameter Override [10026]
PASS: Information Disclosure - Suspicious Comments [10027]
PASS: Open Redirect [10028]
PASS: Cookie Poisoning [10029]
PASS: User Controllable Charset [10030]
PASS: User Controllable HTML Element Attribute (Potential XSS) [10031]
PASS: Viewstate [10032]

PASS: Directory Browsing [10033]
PASS: Heartbleed OpenSSL Vulnerability (Indicative) [10034]
PASS: Strict-Transport-Security Header [10035]
PASS: HTTP Server Response Header [10036]
PASS: Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) [10037]
PASS: Content Security Policy (CSP) Header Not Set [10038]
PASS: X-Backend-Server Header Information Leak [10039]
PASS: Secure Pages Include Mixed Content [10040]
PASS: HTTP to HTTPS Insecure Transition in Form Post [10041]
PASS: HTTPS to HTTP Insecure Transition in Form Post [10042]
PASS: User Controllable JavaScript Event (XSS) [10043]
PASS: Big Redirect Detected (Potential Sensitive Information Leak) [10044]
PASS: Content Cacheability [10049]
PASS: Retrieved from Cache [10050]
PASS: X-ChromeLogger-Data (XCOLD) Header Information Leak [10052]
PASS: Cookie without SameSite Attribute [10054]
PASS: CSP [10055]
PASS: X-Debug-Token Information Leak [10056]
PASS: Username Hash Found [10057]
PASS: X-AspNet-Version Response Header [10061]
PASS: PII Disclosure [10062]
PASS: Permissions Policy Header Not Set [10063]
PASS: Timestamp Disclosure [10096]
PASS: Hash Disclosure [10097]
PASS: Cross-Domain Misconfiguration [10098]
PASS: Source Code Disclosure [10099]
PASS: Weak Authentication Method [10105]
PASS: Reverse Tabnabbing [10108]
PASS: Modern Web Application [10109]
PASS: Dangerous JS Functions [10110]
PASS: Authentication Request Identified [10111]
PASS: Session Management Response Identified [10112]
PASS: Verification Request Identified [10113]
PASS: Script Served From Malicious Domain (polyfill) [10115]
PASS: Absence of Anti-CSRF Tokens [10202]
PASS: Private IP Disclosure [2]
PASS: Session ID in URL Rewrite [3]
PASS: Script Passive Scan Rules [50001]
PASS: Insecure JSF ViewState [90001]
PASS: Java Serialization Object [90002]
PASS: Sub Resource Integrity Attribute Missing [90003]
PASS: Insufficient Site Isolation Against Spectre Vulnerability [90004]
PASS: Charset Mismatch [90011]
PASS: Application Error Disclosure [90022]
PASS: WSDL File Detection [90030]
PASS: Loosely Scoped Cookie [90033]
FAIL-NEW: 0 FAIL-INPROG: 0 WARN-NEW: 0 WARN-INPROG: 0 INFO: 0
IGNORE: 0 PASS: 65



Em caso de dúvidas, entre em contato:

suporte@gozuri.com