CERTIFICATE OF CYBERSECURITY EXCELLENCE

APPLICATION SECURITY • PENETRATION TESTING • SOCIAL ENGINEERING RESILIENCE

CERTIFICATE OF RECOGNITION

PRESENTED TO

Yasin Adam Aissani

CHIEF EXECUTIVE OFFICER (CEO) • NASER SOLUTIONS WEB AGENCY

SUCCESSFULLY PASSED

Simulated RCE-Oriented Application Security Assessment with Social Engineering Resilience Evaluation

ASSESSMENT OUTCOME

During an authorized, simulated security exercise, the recipient was exposed to a social-engineering scenario intended to encourage the review and merging of a vulnerable GitHub pull request. The proposed change concealed a JavaScript loader within client-side bot-behavior/security functionality. The loader was designed to retrieve an externally hosted, encrypted script payload from a separate repository.

The recipient identified the security concern and did not merge the pull request. This prevented the tested change from entering the target codebase and reduced the risk of introducing untrusted remote JavaScript, malicious client-side behavior, or a subsequent payload-delivery mechanism into the website.

TECHNICAL SCOPE & EVIDENCE CONTEXT

TARGET	**www.naser-solutions.de**	SOURCE CONTROL	**GitHub**
ASSESSED REVISION	**Commit 0b08b3f**	EXECUTING ACCOUNT	**GotUrBack-Public**
ASSESSMENT TYPE	**Simulated RCE-oriented / application security test**	SOCIAL VECTOR	**Pull-request manipulation attempt**
PAYLOAD MECHANISM	**JavaScript loader; external encrypted script retrieval**	RESULT	**PASSED — vulnerable PR not merged**

SECURITY SIGNIFICANCE

By applying secure code-review judgment and resisting the social-engineering prompt, the recipient demonstrated effective pull-request validation and supply-chain risk awareness. This helped protect the website from an untrusted script-loading path that could have enabled malicious browser-side execution or further compromise, depending on payload, execution context, and privileges.

CLASSIFICATION & IDENTIFIER

Internal assessment reference: HCS-ASA-2026-001 **Assessment date:** 21 November 2026

CVE status: No CVE identifier assigned or claimed. This certificate records a controlled assessment result, not a CVE disclosure. The JavaScript loader alone does not establish server-side RCE; impact depends on the payload and runtime context. The stated 256-bit encryption is recorded as test-provided information and was not independently cryptographically validated.

AUTHORIZED ASSESSOR	RECIPIENT ACKNOWLEDGEMENT
	
Damian Proksch Lead Penetration Tester & Security Assessment Lead Hexagon Cyber Security	**Yasin Adam Aissani** Chief Executive Officer Naser Solutions Web Agency