Welcome

To the world of security Nullify Network

A team of information security experts. Since 2022, we have been protecting businesses from digital threats, turning risks into opportunities for growth.
Our foundation is hands-on experience and up-to-date manual testing methods.

Building your security step by step

Contact us on Telegram

Contact us via email

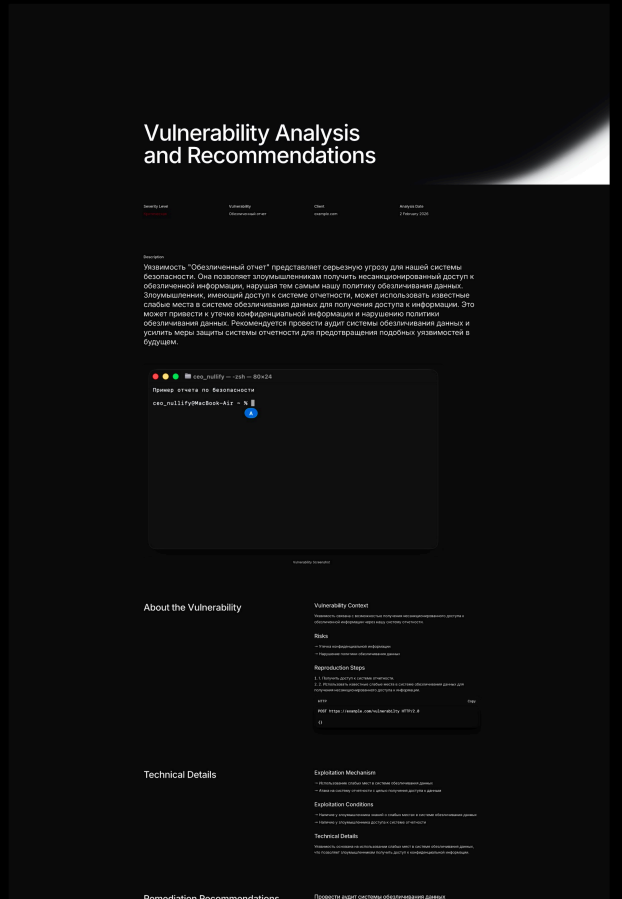
Contact us on LinkedIn

Vulnerability reports in a user-friendly format

HTTP:

```
POST /api/v1/users/info HTTP/2
Host: your-website.com
Content-Length: 18
Accept-Language: ru-RU,ru;q=0.9
Sec-Ch-Ua: "Chromium";v="143", "Not A(Brand";v="24"
X-Token: **********
Content-Type: application/json
User-Agent: Nullify
Accept: */*
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{"__proto__":{"vuln_param":"bnVsbGlmeQ=="}}
```



WhiteBox testing

Source Code Analysis

We review the architecture and implementation for vulnerabilities, errors, and violations of security standards.

Automated Vulnerability Detection (SAST + AI)

We identify critical risks such as SQL injection, XSS, data handling errors, and other common vulnerabilities.

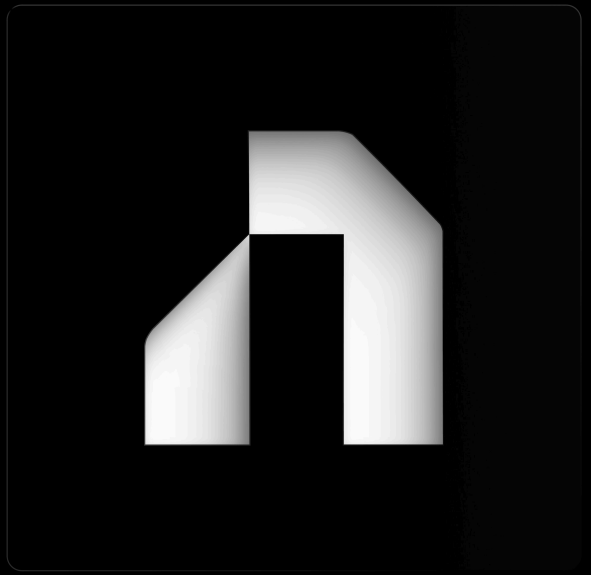
AI-enhanced analysis:
Detection of complex and non-standard vulnerabilities
Reduction of false positives
Prioritization based on business risk
Context-aware remediation recommendations

System Logic Review

We analyze execution scenarios and system behavior in edge cases and non-standard situations.

What is White Box testing?

A testing method in which the internal structure, source code, and architecture of the system are fully known and analyzed. It focuses on verifying how the system works internally, identifying hidden vulnerabilities, logic flaws, and security issues at the code level, and ensuring compliance with secure development practices.



Black Box Testing

Simulating Attacker Behavior

Security assessment performed without access to source code or internal documentation — from the perspective of an external or low-privileged user. Testing is conducted as if the attacker has no insider knowledge.

External Interface Testing

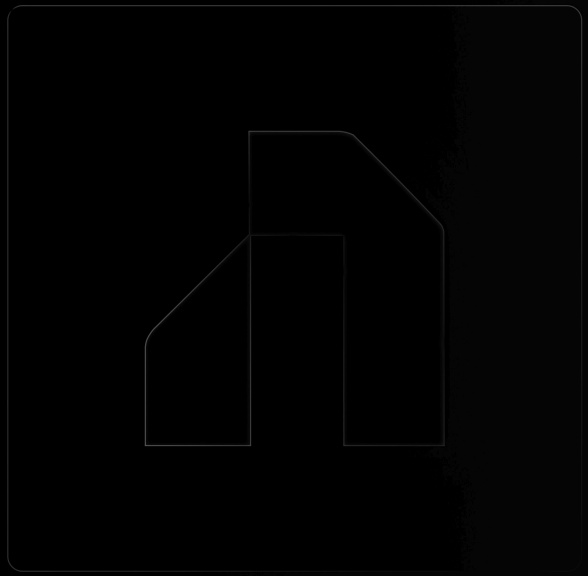
Analysis of web applications, APIs, client-side components, and entry points for vulnerabilities such as SQL injection, XSS, SSRF, IDOR, authentication and authorization flaws, improper data handling, and other common and advanced attack vectors.

Business Logic & Attack Scenario Analysis

Evaluation of application logic, user workflows, and edge cases. Identification of logical flaws that may allow bypassing restrictions, gaining unauthorized access, or compromising data integrity.

What is Black Box testing?

A penetration testing method in which a system is analyzed without any knowledge of its internal structure. The main focus is on real-world attack scenarios accessible to a potential attacker, and on evaluating the actual level of security of the service under real operating conditions.



Priority of Manual Testing Supported by Automation

Automated scanners are effective at detecting common issues, but they are significantly less capable of identifying complex logic and context-based vulnerabilities that require manual analysis.

Manual testing allows for a deeper understanding of system architecture, business logic, and real user scenarios. This makes it possible to uncover non-trivial attack vectors, chained vulnerabilities, and abuse scenarios that are not detectable through automation.

The most accurate assessment of real-world risk and product security is achieved through a combination of expert human analysis, practical experience of security specialists, and selective use of automated tools.

AI also plays a supporting role in this process: it assists manual testers by highlighting potential weak points, suggesting deeper areas for investigation, reducing noise from false positives, and helping prioritize testing efforts based on potential business impact.

Together, this hybrid approach significantly improves both the depth and efficiency of security assessment.

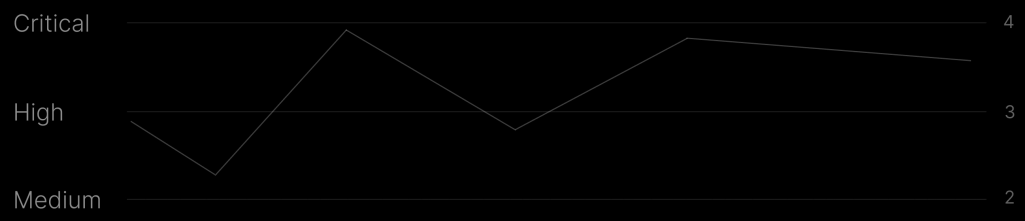
AI Tool — Nullify Network

Our internal AI tool not only identifies vulnerabilities, but also automatically suggests and implements ways to fix them.

Unlike traditional scanners that are limited to surface-level analysis, our solution performs a comprehensive system review, including application logic, business processes, and hidden interaction scenarios.

This enables the detection of more complex and non-trivial vulnerabilities that often remain unnoticed by standard tools.

AI Tool Analysis Results



Advantages

Automatic vulnerability remediation
It not only detects issues but also helps resolve them.

Deep system analysis
Examines code, business logic, and hidden dependencies.

Detection of complex vulnerabilities
Identifies non-trivial and chained security flaws.

Fewer false positives
Higher accuracy compared to traditional scanning tools.

Development lifecycle integration
Supports early detection of issues (shift-left approach).

Results of AI Tool Implementation (NDA Clients)

Operational Processes

- Reduced execution time for key tasks through automation of routine operations
- Increased speed of processing requests, documents, and analytics
- Lower workload on teams due to AI-assisted support
- More consistent output quality (reduced human variability)

Business Impact

- Faster decision-making cycles
- Increased process productivity without expanding headcount
- Reduced operational costs for task execution
- Improved scalability of processes (AI easily adapts to new use cases)

Nullify Network

We ensure information security at the highest level.

Focus on growing your business — security will be handled by the best specialists in the industry!

Telegram Manager: @nullifysupport
Email: nullify.group@gmail.com

Nullify Network