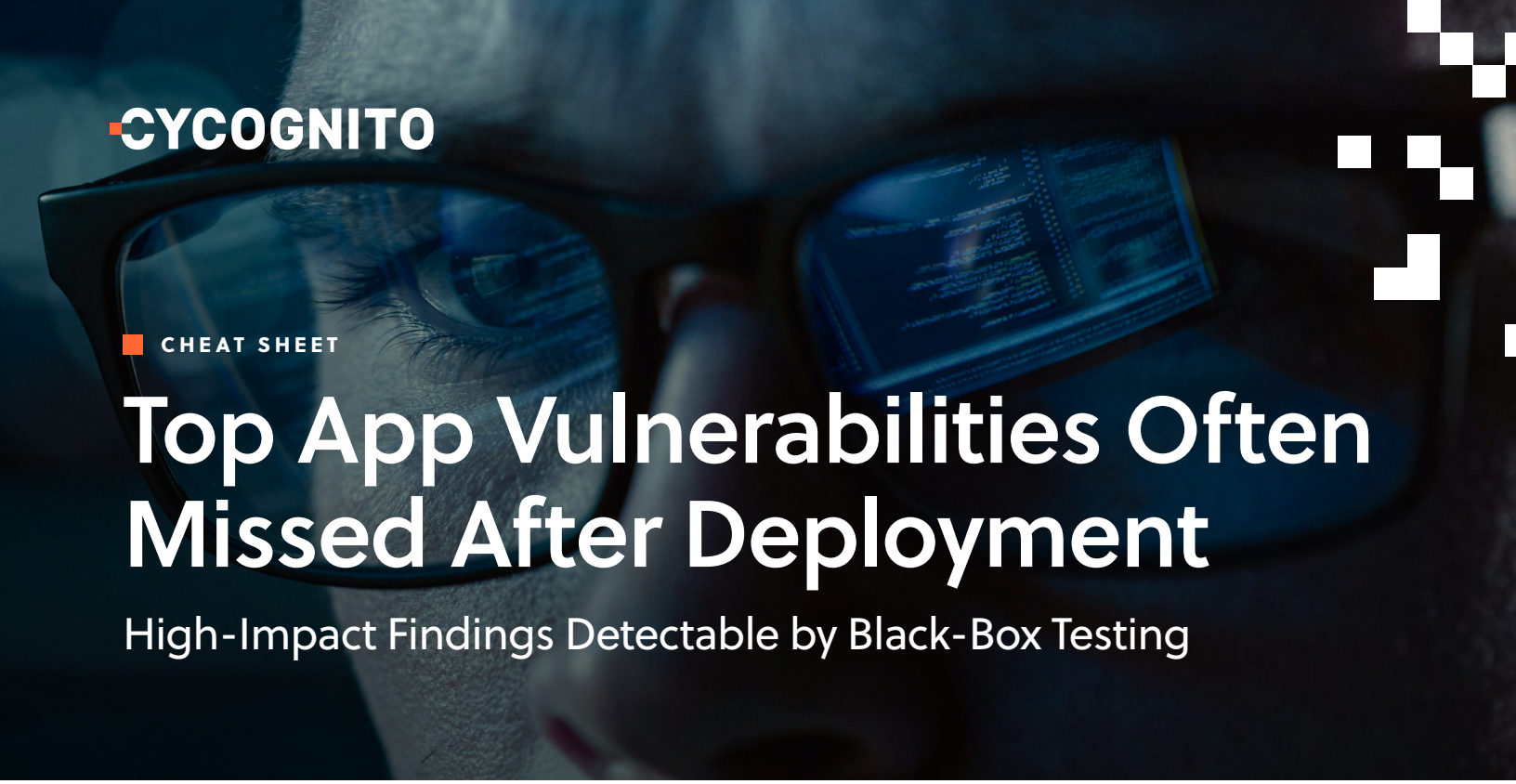

CYCOGNITO

CHEAT SHEET

Top App Vulnerabilities Often Missed After Deployment

High-Impact Findings Detectable by Black-Box Testing

Even with strong SDLC practices, some vulnerabilities slip into production due to misconfigurations or real-world drift. Black-box autonomous DAST tools help catch these issues without credentials, internal access, or chaining.

This list covers ten high-value vulnerabilities that are often missed post-deployment but may be detected through external automated testing, offering fast, practical wins for improving runtime security.impact coverage gaps and offers practical, actionable guidance to help security teams close them effectively.

VULNERABILITY 1

Excessively Verbose Error Messages

What it is: Stack traces, database errors, or debug info shown in HTTP responses due to unhandled exceptions or misconfigured error handling.

How DAST helps: Sends malformed or edge-case input to provoke errors and detects verbose output in responses (e.g., stack traces, SQL errors, file paths).

How to solve: Implement generic error responses in production; log detailed errors server-side only.

VULNERABILITY 2

Missing or Misconfigured Security Headers

What it is: Lack of headers like Content-Security-Policy, Strict-Transport-Security, incorrect set cookie, or X-Frame-Options weakens client-side security protections.

How DAST helps: Analyzes HTTP responses for missing or improperly set headers and flags those that reduce browser-level defenses.

How to solve: Apply recommended headers consistently across all responses through server or framework settings.

VULNERABILITY 3

Insecure Redirects / Open Redirects

What it is: Redirect endpoints that reflect user-supplied URLs without validation can be abused for phishing or redirect chaining.

How DAST helps: Identifies endpoints that accept arbitrary redirect targets and confirms if redirection behavior can be manipulated externally.

How to solve: Use a fixed allowlist of redirect targets; avoid reflecting user input in redirect logic.

VULNERABILITY 4

Sensitive Data Exposure via URLs

What it is: Query strings may include API tokens, credentials, or PII, which can leak via logs, browser history, or referer headers.

How DAST helps: Scans request and response patterns to identify sensitive data reflected in URLs or visible in response bodies.

How to solve: Avoid transmitting sensitive data in URLs; use secure headers or POST requests for confidential information.

VULNERABILITY 5

Outdated JS Libraries with Known Vulnerabilities

What it is: Client-side libraries (e.g., jQuery, Angular, Bootstrap) may include known CVEs if not regularly updated.

How DAST helps: Parses frontend code, inspects JavaScript libraries, and maps them to known vulnerable versions.

How to solve: Update all frontend libraries; use automated tools to track JS dependency versions and CVE impact.

VULNERABILITY 6

Reflected Cross-Site Scripting (XSS)

What it is: Unsanitized user input is reflected in the page's response without proper encoding, enabling script injection.

How DAST helps: Injects known XSS payloads and analyzes responses for successful reflection or script execution indicators.

How to solve: Use proper output encoding, sanitize inputs, and leverage secure templating engines or frameworks.

VULNERABILITY 7

Clickjacking

What it is: A user interface redressing attack where a page is embedded in an invisible iframe to trick users into clicking unintended elements.

How DAST helps: Checks whether pages can be rendered inside iframes by inspecting header configurations.

How to solve: Use headers like X-Frame-Options: DENY or Content-Security-Policy: frame-ancestors 'none'.

How Can CyCognito Help Your Organization?

The CyCognito platform extends your AppSec defenses beyond the SDLC by continuously discovering exposed applications, APIs, and cloud assets and identifying critical vulnerabilities that surface after deployment. Using advanced black-box testing, CyCognito uncovers gaps missed by traditional tools and helps security teams prioritize real-world risks.

Take a self-guided, interactive product tour to explore the platform, or request a customized demo to see how CyCognito can strengthen your external application security posture.