Web Application Penetration Testing

Hackers Love Web Applications

Web Applications are attractive targets for hackers. Just as you are reading this, a hacker could be probing and prodding relentlessly at your external-facing web application in order to uncover weaknesses to exploit your application. With Web Application Penetration Testing, you can discover loopholes in your web application and evaluate its current security posture, allowing you to take action before the hacker does.

At LGMS, we work closely with our clients in a proactive manner to understand their application workflow and ensure that their web applications are thoroughly tested to minimize the risk of a security breach.

To date, our Web Application Penetration Testing has become an integral part of the Software Development Life Cycle (SDLC) for many of our regional clients — providing guidance for our clients in building more secure web applications while accommodating complex business requirements.

At LGMS, we are committed to a highly-disciplined and methodical penetration testing practice—utilizing a combination of a wide range of commercial and open-source tools as well as manual penetration tests. Our methodology not only adheres to worldwide industry standards such as Open Source Web Application Security Project (OWASP), we also conduct customized tests based on the application's business logic.

All vulnerabilities identified will be manually verified to weed out false positives. A comprehensive penetration test report will then be produced with guidelines for remediation for each discovered vulnerability.

LGMS' Web Application Penetration Testing deliverables are accepted as a baseline for TÜV TRUST IT's "Trusted Application" certification.

Our Coverage

LGMS adheres to worldwide industry standards and customizes tests leveraged from our vast penetration testing experience in various industries. The tests include but are not limited to:

- Bypassing Business Process Workflow
- Bypassing File Upload Restrictions and Extension Filters
- Bypassing Function Level Access Control
- Bypassing Weak Data Validation
- Data Exfiltration
- Privilege Escalation
- Post Exploitation for Server Takeover
- Session Hijacking

RECONNAISSANCE & MAPPING

- Crawl and analyze the target
- Map the application by identifying its components and functions.

AUTOMATED & MANUAL TESTING

- Static analysis to identify common application weaknesses
- Customise test cases for different business nature

VERIFICATION & ANALYSIS

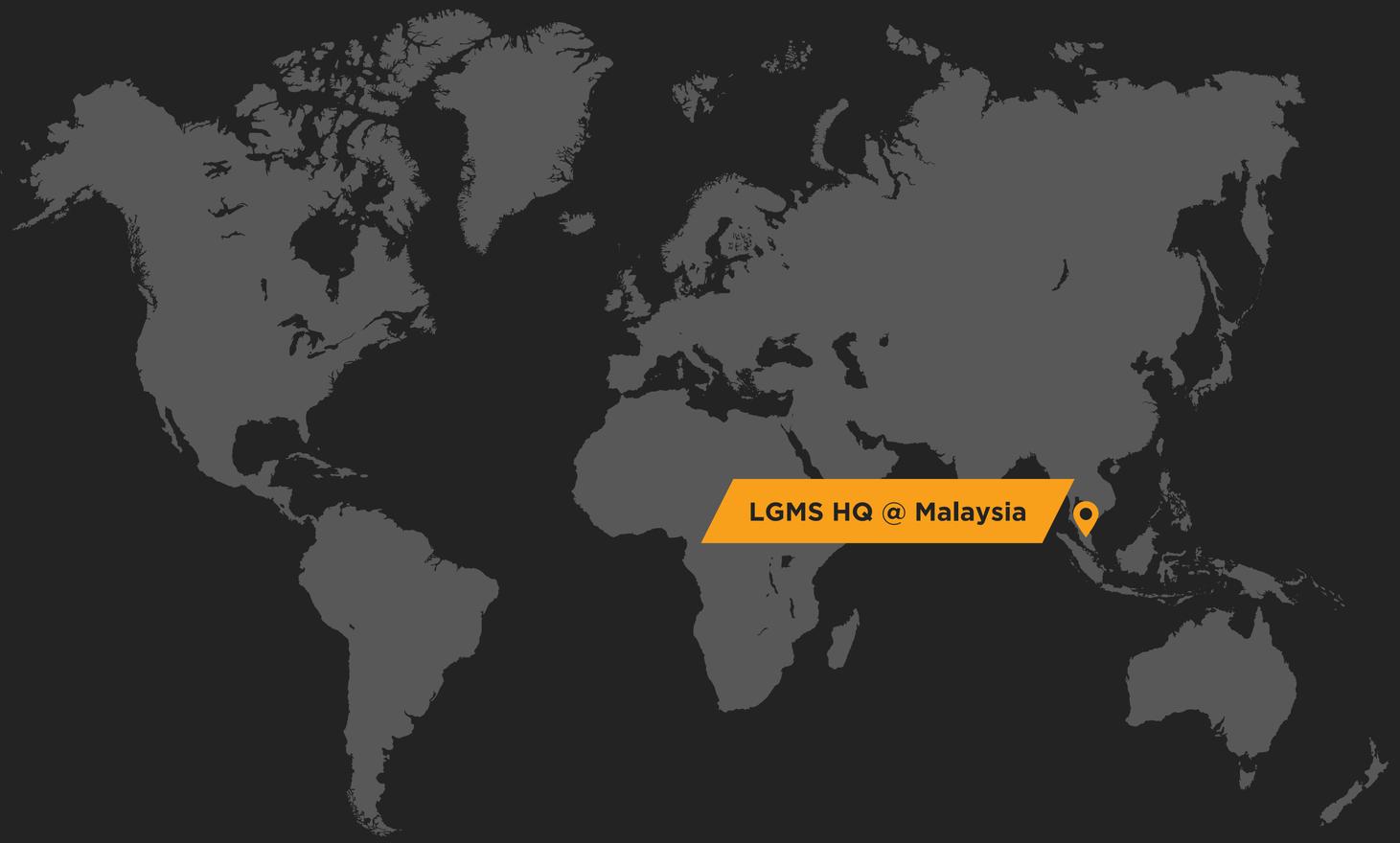
- In-depth analysis to eliminate false positives and provide proof-of-concept screenshots
- Determine severity rating based on likelihood, technical impact, and business impact

Deliverables

LGMS will present a penetration test report with the following:

- Executive Summary
- In-depth Application Vulnerability Technical Details
- Security Risk Rating (OWASP Risk Rating) and Prioritization of Findings
- Comprehensive Remediation Guidance
- Recommendation for Future Improvements

LGMS BERHAD
202001039091 (1395412-W)
LE GLOBAL SERVICES SDN. BHD.
200501018357 (700472-M)



Contact Us

LGMS Berhad

A-11-01, Empire Office Tower,
Jalan SS 16/1, 47500 Subang Jaya,
Selangor, Malaysia.

+603-8605 0155

info@lgms.global

www.lgms.global