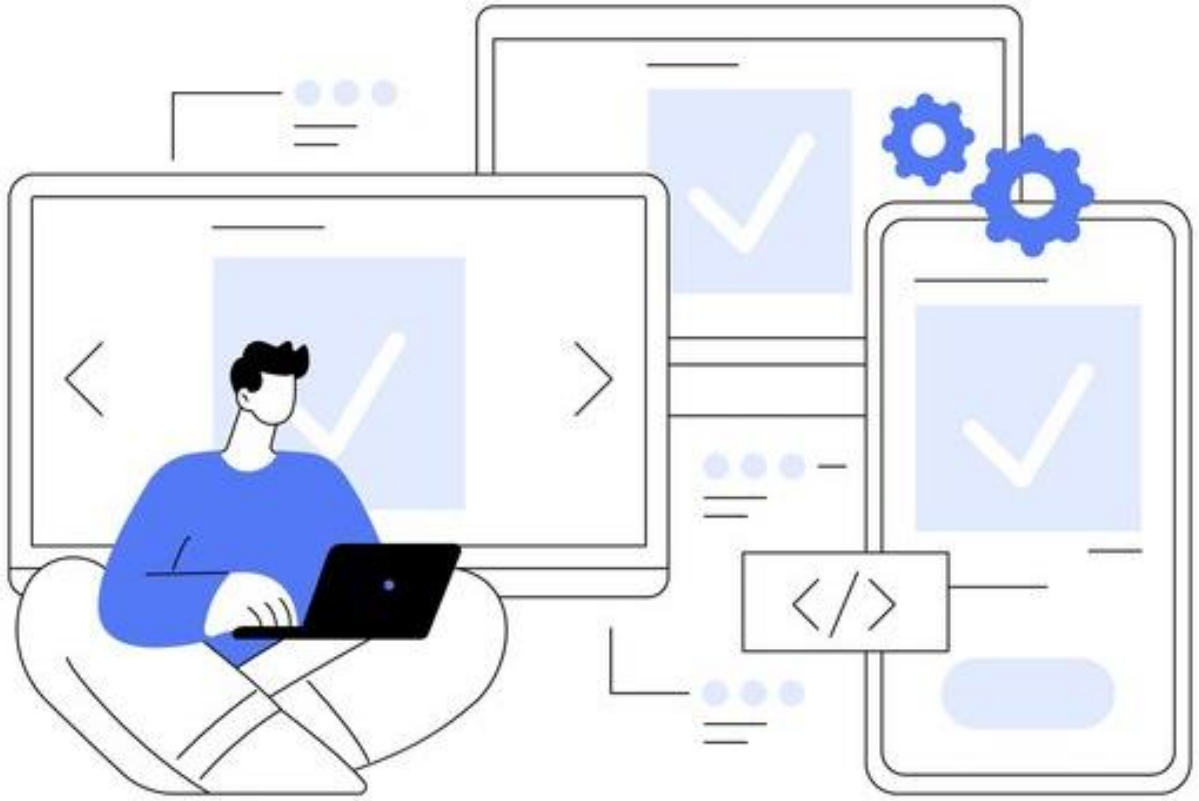
Technical -Approach

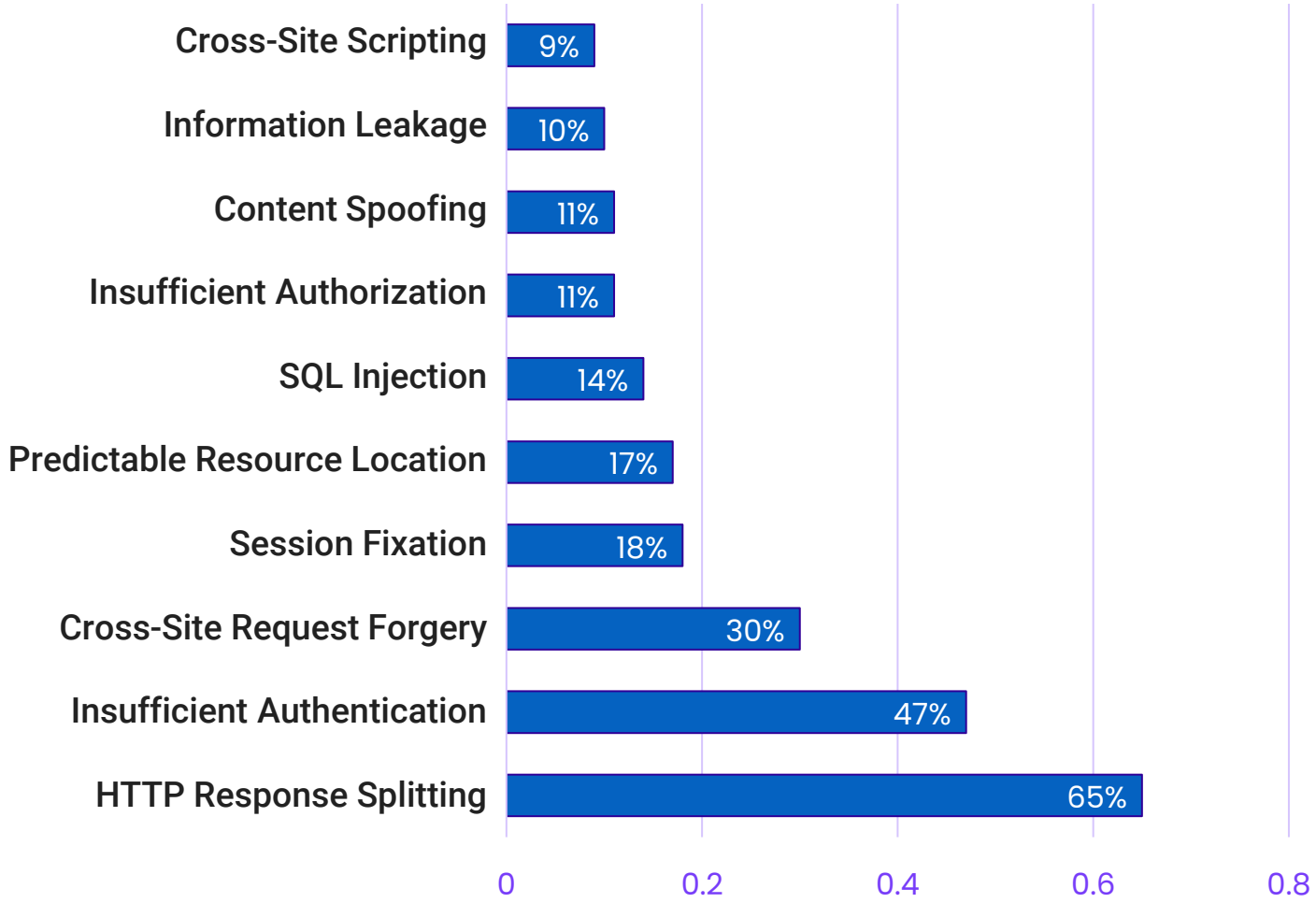
Web Application Security

Infopercept

INVINSENSE

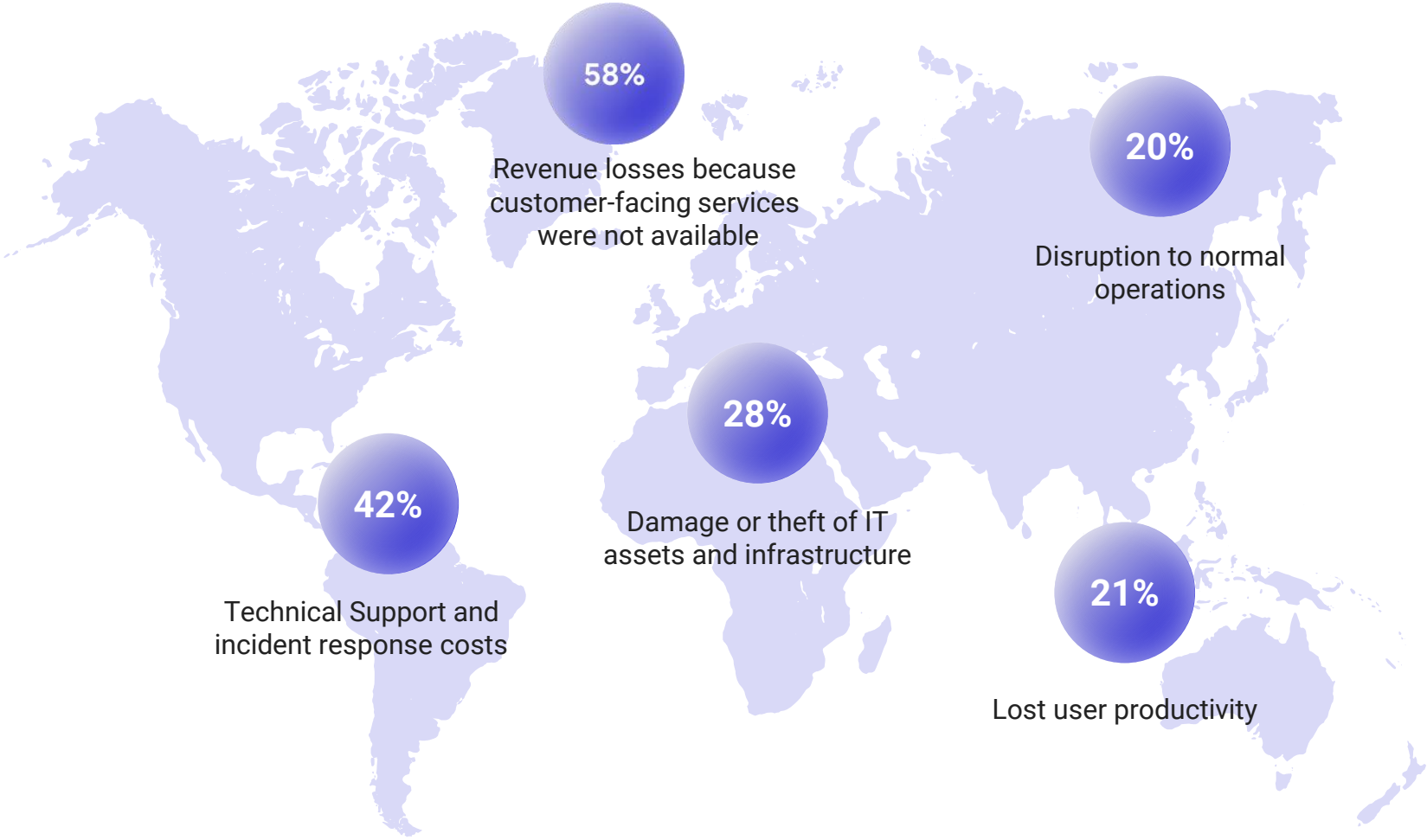


Highest Security Risk Approach



Web application attacks represent the greatest threat to an organization’s security.

Breakdown of the cost of web application attacks

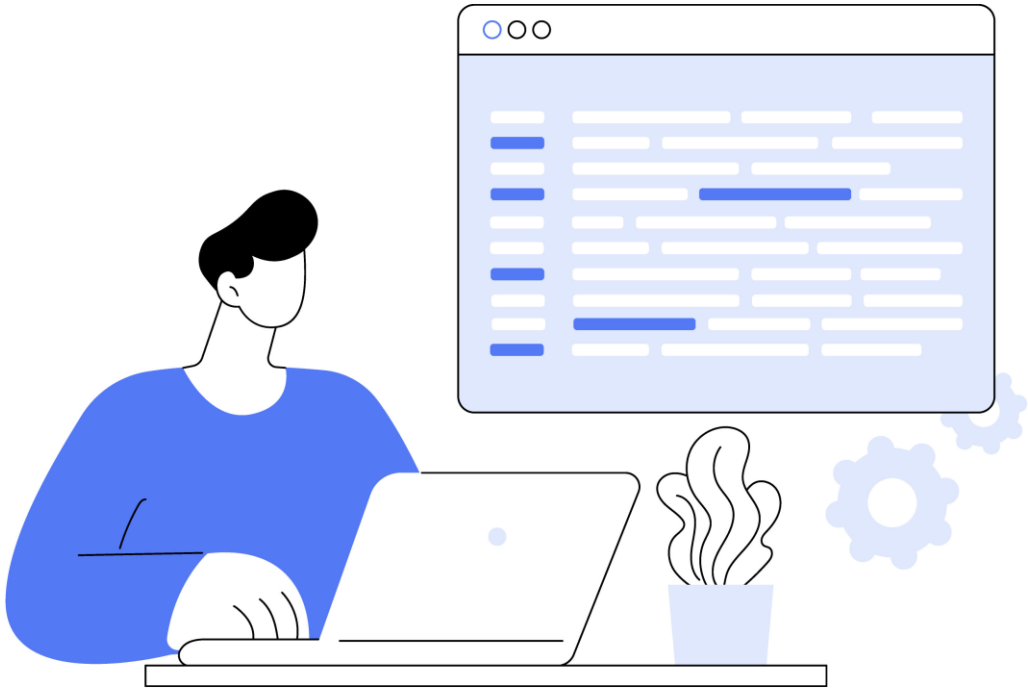


What Is Web Application Security?

In an Application Development Life Cycle, Application Security (AppSec) is one of the most important components. Much of the Application Security (AppSec) happens during the development phase, by utilizing tools and methods in order to ensure the protection of the applications once they are deployed. Application Security therefore needs a well-defined and adept approach throughout the Systems Development Life Cycle (SDLC). So as to ensure there are no security gaps and the application is stable to be rolled out in the market.

A form of stress testing, which exposes weaknesses or flaws in a Web Application,

Art of finding a ways to exploit Web Application.



Web API

With ease of API integrations comes the difficult part of ensuring proper AUTHN (authentication) and AUTHZ (authorization). In a multitenant environment, proper security controls need to be put in place to only allow access on "need to have access basis" based on proper AUTHN and AUTHZ. Appropriate AUTHN schemes enable producers (API's or services) to properly identify consumers (clients or calling programs) and to evaluate their access level (authz). In other words, can a consumer invoke a particular method (business logic) based on credentials presented?

Approach

Authentication Assessment (Grey Box Assessment)

- Dynamic Pages / Static Pages
- Login Page
- Provided with Login Credentials

Non-Authentication Assessment (Black Box Assessment)

- Dynamic Pages / Static Pages
- Publicly Available Pages
- Login Page / No login page
- Not Provided with Login Credentials

Methodology for Application Security

1. Scope/Goal Definition

- What type of Assessment to be conducted
  - Authenticated Assessment
  - Non-Authenticated Assessment
- Which Web Application the test will be conducted
- Duration of the test

2. Application Discovery

- Web application discovery is a process aimed at identifying web applications on a given infrastructure. The latter is usually specified as a set of IP addresses (maybe a net block), but may consist of a set of DNS symbolic names or a mix of the two.
- This information is handed out prior to the execution of an assessment an application-focused assessment.

3. Infrastructure Analysis

- Conducting Analysis to find the location of Web Application in the Infrastructure.
- Do the analysis of what is placed to protect Web Server & find out gaps of the placement.
- Check for the details for how is Web Server, Application Server and Database Server Located.

4. Threat Assessment

- Threat Assessment is conducted based on the findings of Step 2 and Step 3.
- All the possible Threat related to the Application and Infrastructure are Assessed in this phase.

5. Vulnerability Assessment

- Tool Based Scan is conducted based on the Scope defined in the step 1
  - Authentication Assessment (Grey Box Assessment)
    1. Dynamic Pages / Static Pages
    2. Login Page
    3. Provided with Login Credentials
- Our Expert team does analysis based on the manual intelligence
  - False Positive / False Negative
    1. Infopercept team conduct analysis to find False Positive and False Negative.
    2. Vulnerabilities are rated as Critical, High, Medium and Low after the analysis.

6. Exploitation Attempts

- Has Two Sub Stages
  - Has Two Sub Stages
    1. Known / available exploit selection – Tester acquires publicly available s/w for exploiting.
    2. Exploit customization – Customize exploits s/w program to work as desired.
    3. Exploit development – Develop own exploit if no exploit program available
    4. Exploit testing – Exploit must be tested before formal Test to avoid damage.
    5. Attack – Use of exploit to gain unauthorized access to target.
  - Privilege Escalation

    What can be done with acquired access / privileges
    1. Team of consuAlter
    2. Damage
    3. What not

Team of consultants at Isolations will be conducting POC to exploit the Critical and High Vulnerabilities.

ltants at Isolations will be conducting POC to exploit the Critical and High Vulnerabilities.

7. Deliverables

Organize Data/related results for Management Reporting

- Consolidation of Information gathered.
- Analysis and Extraction of General conclusions.
- Recommendations.

About Infopercept

Infopercept's vision and core values revolve around making organizations more secure through the core values of Honesty, Transparency and Knowledge, so as to enable them to make better informed decisions about their security practices & goals. With our synergistic vision to combine technical expertise and professional experience, we aim to further establish our place as a one stop shop for our clients and partners' cybersecurity and accreditation needs.

Our specialized core team comprises experienced veterans, technical experts & security enthusiasts having good practical experience & thorough knowledge in the Cybersecurity domain, latest trends, and security innovations; ensuring that you always get the best security approach & solution for your specific business needs exactly the way you want it to be.

Imprint
© Infopercept Consulting Pvt. Ltd.

Address
3rd floor, Optionz Complex
Opp. Hotel Regenta,
CG Road, Navrangpura,
Ahmedabad - 380 009,
Gujarat, India.

Contact Info
M: +91 9898857117
W: www.infopercept.com
E: sos@infopercept.com

Global Office

United State of America
+1 516 713 5040

United Kingdom
+44 2035002056

Sri Lanka
+94 702 958 909

Kuwait

India
+91 9898857117

Infopercept