Your plug & play cyber security suite.
Resilient and Reliable Security solution for your application

- 27,000+ Vulnerabilities Uncovered Every Month
- 8000+ Hours Saved of Developers & CXOs
- 75% Vulnerability Fixing Rate

Security Testing Methodology
Table of Contents

1. Introduction
   1.1 About Astra Security
   1.2 Objective of Security Testing
   1.3 Astra Security's VAPT Framework

2. Security Audit Scope of Work (SOW)

3. Testing Methodologies
   3.1 For Websites / Web Applications
   3.2 For Mobile Applications (Android)
   3.3 For Mobile Applications (iOS)
   3.4 For API Security
   3.5 For AWS Cloud Infrastructure
   3.6 For Azure Cloud Infrastructure
   3.7 For Network Devices - Firewall/Routers/Printers

4. Security Testing Report & Video POCs

5. Methodology for Patching Vulnerabilities

6. Our Security Suite

7. Our VAPT Customers

8. Awards & Recognition

9. List of Top Security Issues Tested

10. Contact

Vulnerabilities in App Code

API Testing

Cloud Security Diagnostics

Business Logic Testing

Network VAPT
1. Introduction

Vulnerability Assessment & Penetration Testing that comes without a 100 emails, 250 Google searches & painstaking PDFs. Saves hundreds of hours of your & developer’s time.

1.1 About Astra Security

Astra Security makes cyber security super simple for online businesses. The company offers a security suite that comprises of security audit, firewall & malware scanner.

Every solution within our suite takes under five minutes to setup & offers a 10x better experience than their contemporaries. The suite is beautifully knit, offering a homogenous experience that makes security delightful. Astra Security is a Techstars backed company, awarded by President of France & PM of India for its innovation in cyber security.

1.2 Objective of Security Testing

The security testing focuses on evaluating the security of the web, mobile, networks, API, SaaS, blockchain & cloud applications by methodically validating & verifying the effectiveness of security controls. The process involves an active analysis of any application for any available weaknesses, technical flaws, or vulnerabilities.

Every vulnerability that is found will be present with an assessment of the impact, a proposal for a technical solution using our collaborative cloud dashboard.
1.3 Astra Security’s VAPT Framework

Every VAPT (Vulnerability Assessment & Penetration Test) is tailored to application being tested. Apart from the standard security tests, massive stress is put on designing security tests tailored to your application’s work flow.
2. Security Audit Scope of Work (SOW)

Astra’s Security Testing is based on the OWASP (Open Web Application Security Project) Testing Methodologies and the OWASP Testing Framework. During the audit we perform over 1250+ ‘active’ tests that have been classified on the basis of type of vulnerabilities found. Each active test is followed by hundreds of sub-tests.

A detailed security audit’s scope will be a tailored approach basis on the individual requirements such as a number applications to be audited, types of application, desired type of security testing, our predefined number of tests for each type of application, security assessment tools, and more.

The security audit scope of work will include:

- **Vulnerability Assessment and Penetration Testing (VAPT)**
- **Static & dynamic code analysis**
- **Technical assistance in patching found security vulnerabilities**
- **Collaborative cloud dashboard for vulnerability reporting & management**
- **Access to our security tools/APIs**
- **Consultation on the best security practices for your application**

Hacker style testing, powered by our powerful vulnerability management & collaboration dashboard.
Qualified & Friendly Security Team

The security audit is the high-level description of the many ways organizations can test and assess their overall security posture.

Astra’s team of security auditors maintain the ethical and professional approach for the testing and assessing your organization’s security posture. Our professional auditors combine the wisdom, qualifications and skills acquired over the years doing thousands of security audits. You get nothing but the best experience throughout the engagement.

In addition, the auditors have both technical & communication skills to uncover all vulnerabilities on your platform and collaborate with your development team to help them patch discovered vulnerabilities in your application/network. Our team take prides in being developer friendly.

Our security auditors have wide education backgrounds & hold industry specific certifications (not limited to the list below):

- Bachelors in Information Security from Northumbria University, Singapore
- CEH - Certified Ethical Hacker
- Advanced Diploma in Information Security, MDI, Singapore
- Cyber Security Fundamentals from Kaspersky
- Policy Compliance Certification, Qualys
Vulnerability Management Areas

Websites / Web Applications
- Blackbox Testing
- Whitebox Testing
- Greybox Testing

Mobile Apps (iOS/Android)
- Mobile app assessment
- PDA security assessment
- Network & source code testing

API Security
- API analysis
- API enumeration
- Scope & roles testing
- iDOR (Insecure Direct Object Reference)

Cloud Infra. (AWS/Azure)
- Cloud configuration review of environment
- Network and perimeter assessments (Internal/External)
- Cloud security diagnostics
- Server and network penetration testing

Network Devices
- Network vulnerability assessment with a data review
- Reviewing network strengths against common attacks
- Network devices penetration testing
- Security assessment of network devices
3. Testing Methodologies

Our security testing approach and methodology is based on industry leading practices such as OWASP, OSSTMM, WASC, NIST etc.

### 3.1 For Websites/Web Applications

<table>
<thead>
<tr>
<th>Phase</th>
<th>Phase I</th>
<th>Phase II</th>
<th>Phase III</th>
<th>Phase IV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phase name</td>
<td>Initiation</td>
<td>Evaluation</td>
<td>Discovery</td>
<td>Reporting</td>
</tr>
<tr>
<td>Description</td>
<td>Define scope of testing for an application</td>
<td>Perform static code analysis of an application</td>
<td>Perform dynamic analysis &amp; penetration tests</td>
<td>Determine ease of vulnerability exploitation</td>
</tr>
<tr>
<td></td>
<td>Document initial testing requirements</td>
<td>Server Infrastructure Testing &amp; DevOps</td>
<td>Payment manipulation testing</td>
<td>Provide app vulnerabilities details on your Astra VAPT Dashboard</td>
</tr>
<tr>
<td></td>
<td>Develop testing &amp; scanning schedule</td>
<td>Identify the loopholes in the business logic</td>
<td>Test for known CVEs</td>
<td>Provide technical solution or recommendations for fixes</td>
</tr>
<tr>
<td></td>
<td>Understand implemented functionalities in an application</td>
<td>Do authorization checks for user access (UAC)</td>
<td>Technology specific attack vectors and payloads</td>
<td>Independent quality review and Final Report submissions</td>
</tr>
<tr>
<td></td>
<td>Sampling of browser-server traffic flow</td>
<td>Schedule manual &amp; automated application scanning using own tools</td>
<td>Verify findings and remove false positives</td>
<td>Provide VAPT Certificate for security audit</td>
</tr>
<tr>
<td></td>
<td>Finalize testing deliverables format</td>
<td>List commercial and open source tools for security testing</td>
<td>Catalogue all the exposed vulnerabilities</td>
<td></td>
</tr>
</tbody>
</table>

**Outcome**

Testing results are periodically updated in Astra VAPT Dashboard

*For more information, visit: [https://www.getastra.com/website-vapt](https://www.getastra.com/website-vapt)*

Hybrid of Human & Automated Vulnerability Testing.
# 3.2 For Mobile Applications (Android)

<table>
<thead>
<tr>
<th>Phase</th>
<th>Phase I</th>
<th>Phase II</th>
<th>Phase III</th>
<th>Phase IV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phase name</td>
<td>Initiation</td>
<td>Evaluation</td>
<td>Discovery</td>
<td>Reporting</td>
</tr>
</tbody>
</table>
| Description | • Installation of apk file in Android security testing devices  
• Reconnaissance & threat modeling  
• All app components are identified and known to be documented  
• Define overall scope of testing  
• Document initial testing requirements  
• Develop testing schedule  
• Sampling of test data | • Intercept the proxy to analyze the incoming & outgoing packets of the app  
• Perform source code analysis  
• Understand the basic business functionality of the app to identify possible entry and exit points of information  
• Identify application’s data store (at rest, in transit or on display) and sensitivity | • Based on the observations, formulate test cases and carry out the security testing for  
  o Data storage and privacy  
  o Cryptography  
  o Authenticaton & session management  
  o Encrypted network communications  
  o Platform interaction  
  o Code quality and build settings | • Determine ease of vulnerability exploitation  
• Provide app vulnerabilities details on your Astra VAPT Dashboard  
• Provide technical solution or recommendatio ns for fixes  
• Independent quality review and Final Report submissions  
• Provide VAPT Certificate for security audit |

**Outcome**

Testing results are periodically updated in Astra VAPT Dashboard

**Tools used for Android security testing:** Network Proxy, MitmProxy, Quark, APKTool, Android Debug Bridge, MobSF, ZAP & more.

For more information, visit: [https://www.getastra.com/mobile-app-vapt](https://www.getastra.com/mobile-app-vapt)
# 3.3 For Mobile Applications (iOS)

<table>
<thead>
<tr>
<th>Phase</th>
<th>Phase I</th>
<th>Phase II</th>
<th>Phase III</th>
<th>Phase IV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phase name</td>
<td>Initiation</td>
<td>Evaluation</td>
<td>Discovery</td>
<td>Reporting</td>
</tr>
</tbody>
</table>
| Description | - Installation of ipa file in iOS security testing devices  
- Re却naissance & threat modeling  
- All app components are identified and known to be documented  
- Define overall scope of testing  
- Document initial testing requirements  
- Develop testing schedule  
- Sampling of test data  

- Intercept the proxy to analyze the packets coming in and going out of the app  
- Perform source code analysis  
- Understand the basic business functionality of the app to identify possible entry and exit points of information  
- Identify application’s data store (at rest, in transit or on display) and sensitivity  

- Based on the observations, formulate test cases and carry out the security testing for:  
  - Data storage and privacy  
  - Cryptography  
  - Authenticatio & session management  
  - Encrypted network communications  
  - Platform interaction  
  - Code quality and build settings  

- Determine ease of vulnerability exploitation  
- Provide app vulnerabilities details on your Astra VAPT Dashboard  
- Provide technical solution or recommendatio ns for fixes  
- Independent quality review and Final Report submissions  
- Provide VAPT Certificate for security audit |
| Outcome | Testing results are periodically updated in Astra VAPT Dashboard |

Tools used for iOS security testing: Network Proxy, MitmProxy, Quark, MobSF, ZAP, IMAS & more.

For more information, visit: [https://www.getasta.com/mobile-app-vapt](https://www.getasta.com/mobile-app-vapt)
### 3.4 For API Security

<table>
<thead>
<tr>
<th>Phase</th>
<th>Phase I</th>
<th>Phase II</th>
<th>Phase III</th>
<th>Phase IV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phase name</td>
<td>Initiation</td>
<td>Evaluation</td>
<td>Discovery</td>
<td>Reporting</td>
</tr>
</tbody>
</table>
| Description | • Analyze the API endpoints  
• Checking type of Authentication implemented:  
  ○ Basic HTTP authentication  
  ○ User Input validation checks  
  ○ Access token  
  ○ Cookies  
• Document initial testing requirements  
• Develop testing schedule  
• Setup testing environment and prepare testing tools | • Check if all the endpoints are protected behind authentication to avoid broken authentication process  
• Test for API Input Fuzzing  
• Test for Unhandled HTTP Methods  
• Analyzing API request and response  
• Testing Integration endpoints | • Test for following vulnerabilities:  
  ○ Unauthorized Access  
  ○ Data leakage  
  ○ Sanctioning Fuzzy input  
  ○ Injection Vulnerabilities  
  ○ Parameter Tampering, etc.  
• Data validation testing  
• Access permissions  
• IDOR (Insecure Direct Object Reference) | • Determine ease of vulnerability exploitation  
• Provide vulnerabilities details on your Astra VAPT Dashboard  
• Provide technical solution or recommendations for fixes  
• Independent quality review and final report submissions  
• Provide VAPT Certificate for security audit |
| Outcome | Testing results are periodically updated in Astra VAPT Dashboard |

**Tools used for API security testing:** Burp Suite, Proxy, SQLmap, Acunetix, DirBuster, Fuzzapi, Commix, REST API Clients & more.

For more information, visit: [https://getastra.com/blog/knowledge-base/api-security-testing](https://getastra.com/blog/knowledge-base/api-security-testing)
### 3.5 For AWS Cloud Infrastructure

<table>
<thead>
<tr>
<th>Phase name</th>
<th>Initiation</th>
<th>Evaluation</th>
<th>Discovery</th>
<th>Reporting</th>
</tr>
</thead>
</table>
| Description | - Define scope of testing for your AWS integration  
- Obtain root access keys  
- Network and perimeter assessments (Internal/External)  
- Finalize testing deliverables format  
- Configuration review of the environment  
- Reviewing Identity and Access Management (IAM) users, groups and roles  
- Managing the access control on the cloud  
- Reviewing EC2, SNS, RDS Security configuration review  
- Reviewing other AWS policies for:  
  - S3 Bucket  
  - SQS queue  
  - KMS keys | - Based on evaluation start finding open vulnerabilities & security loopholes  
- Running vulnerability scanning with tools such as CloudSploit  
- Perform server and network penetration testing  
- Perform 50+ security tests  
- Run cloud security diagnostics | - Provide details of vulnerabilities & misconfigurations on your Astra VAPT Dashboard  
- Provide technical solution or recommendations for fixes  
- Independent quality review and final report submissions  
- Provide VAPT Certificate for security audit |

| Outcome | Testing results are periodically updated in Astra VAPT Dashboard |

Tools used for Cloud infrastructure testing for AWS: Prowler, CloudSploit, Cloudplaining, ScoutSuite CloudJack, & more.

For more information, visit: [https://getastra.com/blog/security-audit/aws-security-audit](https://getastra.com/blog/security-audit/aws-security-audit)
## 3.6 For Azure Cloud Infrastructure

<table>
<thead>
<tr>
<th>Phase name</th>
<th>Description</th>
<th>Outcome</th>
</tr>
</thead>
</table>
| Initiation | • Define scope of testing for your Azure integration  
• Obtain root access keys  
• Network and perimeter assessments (Internal/External)  
• Finalize testing deliverables format | Testing results are periodically updated in Astra VAPT Dashboard |
| Evaluation | • Configuration review of the environment  
• Reviewing Identity and Access Management (IAM) users, groups and roles  
• Managing the access control on the cloud  
• Storage, VMs, SQL Database, Keyvault, & App service environment Security configuration review  
• Reviewing data protection & encryption | |
| Discovery | • Based on evaluation start finding open vulnerabilities & security loopholes  
• Running vulnerability scanning with tools  
• Perform server and network penetration testing  
• Perform 50+ security tests  
• Run cloud security diagnostics | |
| Reporting | • Provide details of vulnerabilities & misconfigurations on your Astra VAPT Dashboard  
• Provide technical solution or recommendations for fixes  
• Independent quality review and final report submissions  
• Provide VAPT Certificate for security audit | |

**Tools used for Cloud infrastructure testing for Azure:** Azucar, CloudSploit, ScoutSuite, MicroBurst, cs-suite, & more.
### 3.7 For Network Devices - Firewall/Routers/Printers

<table>
<thead>
<tr>
<th>Phase</th>
<th>Phase I</th>
<th>Phase II</th>
<th>Phase III</th>
<th>Phase IV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phase name</td>
<td>Initiation</td>
<td>Evaluation</td>
<td>Discovery</td>
<td>Reporting</td>
</tr>
</tbody>
</table>
| Description | • Define scope of testing for network devices  
• Develop testing schedule  
• Identify any deficiencies that put the customer at risk of a security breach  
• Understand integration of the device and topology  
• Sampling of network traffic  
• Finalize testing deliverables format | • Check if all the endpoints of devices are protected with authentication  
• Security policies & architecture review  
• Do authorization checks for user access (UAC)  
• Network data review  
• Evaluate the policies for remote access, etc.  
• Reviewing network strengths against common attacks | • Perform risk assessment to identify threats, and analyze the control environment to determine what risks are and their potential impact.  
• Vulnerability assessment for device process, application & function  
• Perform penetration testing to find flaws in the vulnerable devices | • Provide details of vulnerabilities & misconfigured/unpatched network devices on your Astra VAPT Dashboard  
• Provide technical solution or recommendations for fixes  
• Independent quality review and final report submissions  
• Provide VAPT Certificate for security audit |

**Outcome**

Testing results are periodically updated in Astra VAPT Dashboard

**Tools used for Network devices testing:** Nmap, Wireshark, Nessus, Metasploit, burp, Sublist3r & more.

For more information, visit: [https://getastra.com/blog/security-audit/it-security-audit](https://getastra.com/blog/security-audit/it-security-audit)

Astra Security's proprietary vulnerability management platform is unlike anything you must have ever seen. A birds eye view for CISOs helps ensure you're always on top of the status of the security audit. A detailed vulnerability report with video proof of concepts, selenium scripts & ability to collaborate with our security engineers within dashboard ensures vulnerabilities are fixed in a record time.

- Details of vulnerability
- Screenshots & video PoCs
- Selenium scripts for your developers to help reproduce vulnerabilities
- Threat criticality with CVSS score
- Business impact & consequences
- Steps to re-create the issue
- Tailored steps to fix the vulnerability (Patching)
- Best Practices for future

Astra Security's vulnerability management dashboard comes with a birds eye view for management keeping you always on the top of security assessment status.

Video PoCs, selenium scripts & collaboration with security team enables your developers to fix the vulnerabilities in record time. With Astra Security, VAPT takes 40% less time than other solutions.
Build trust among your customers & partners with a security certificate

A secure application calls for some bragging. After our engineers verify you’ve fixed the uncovered vulnerabilities, we issue a safe-to-host certificate. This helps inspire confidence among your customers and partners.
5. **Methodology for patching vulnerabilities**

We have a strong emphasis on security patching post the audit. It is important to close the loop and make the application bulletproof from hackers.

**We achieve this by providing:**

- Detailed steps for patching
- Best practices while development
- Round-the-clock technical assistance
- Video POCs of discovered vulnerabilities and security loopholes
- Re-audit to ensure the issue has been fixed

After the security vulnerabilities have been satisfactorily resolved, a **full re-scan** is conducted to ensure that there are no gaps. A certificate will be then issued to confirm the same.

**Additional Security Mechanisms**

To ensure utmost security we believe in ‘Proactive Security’ measures where we anticipate the infiltration techniques used by hackers and recommend additional security countermeasures.

We take security in our own hands and fortify the application:

- Application specific security mechanisms
- Countermeasures for known attack techniques
- Framework to monitor user actions on application
- Mechanisms to tackle hackers
6. Our Security Suite

- Intelligent web application firewall & malware scanner
- Protects against 100+ types of attacks
- Daily automatic malware scans
- Community-driven
- No DNS changes required
- No routing of traffic through our servers
- We never become a single point of failure
- Protection tailored to technology stack

**A Rock Solid Firewall** that detects, stops & neutralizes 100+ threats neutralizes 100+ threats including bad bots, SQLi, LFI, RFI etc. Automatic decision making & dozens of security features like country blocking, GDPR cookie consent, rate limiting, fake search engine bots detection & more.
Create your own community security (Bug Bounty) program

Your business is vulnerable. There’s always a new malware or hack floating around that you are not protected against.

With community security, ethical hackers guard your website, report vulnerabilities and earn rewards. You allow people to report any security weaknesses they find through a dedicated channel and strengthen your website before it’s attacked—at no cost to your business.

- Launch in 4 minutes
- Leverage the security community
- Managed by our security experts
- Self serves dashboard
- Reward hackers
- Be known as a security conscious company

For more information, visit here: https://www.getastra.com/community-security
8. Our VAPT Customers

Trusted by The Ones You Trust

Astra carried out a security audit on our digital application which is a solution that allows companies to manage their whistleblower system. Due to the sensitive nature of the information that is processed in the application, we wanted to identify all possible security loopholes. I am very satisfied with the result and the recommendations of the audit report. It was an eye opener. We were able to optimize the security of the app to meet the expectations of our customers.

- Olivier Trupiano, CEO, Signalement (a whistleblowing platform in Europe)
8. Awards & Recognition

Astra Security was awarded a grant from the French Government under their French Tech Ticket program. We were awarded by the French president Mr. François Hollande himself.

Astra Security was awarded ‘Best Cyber Security Startup’ by the PM of India Mr. Narendra Modi at Global Conference on Cyber Security.

Astra Security is recognized by NASSCOM as top 50 emerging cyber security companies & has been awarded with the Emerge50 award.
### 9. List of Top Security Issues Tested

The following table captures the top security issues found. The list is illustrative of the security issues tested for. During actual security audit, under head below thousands of tests are performed including tailored tests for your application.

<table>
<thead>
<tr>
<th>Vulnerabilities Tested</th>
<th>Exploitability</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration and Deployment Misconfiguration</td>
<td>Easy</td>
<td>Moderate</td>
</tr>
<tr>
<td>Application or Framework Specific Vulnerabilities</td>
<td>Difficult</td>
<td>Severe</td>
</tr>
<tr>
<td>Business Logic Flaws</td>
<td>Average</td>
<td>High</td>
</tr>
<tr>
<td>Shopping Cart &amp; Payment Gateway Manipulation</td>
<td>Difficult</td>
<td>Severe</td>
</tr>
<tr>
<td>Known Security Issues (CVEs)</td>
<td>Average</td>
<td>Moderate</td>
</tr>
<tr>
<td>Weak Identity Management</td>
<td>Average</td>
<td>High</td>
</tr>
<tr>
<td>Broken Authentication</td>
<td>Average</td>
<td>Severe</td>
</tr>
<tr>
<td>Improper Authorization</td>
<td>Average</td>
<td>Severe</td>
</tr>
<tr>
<td>Broken Session Management</td>
<td>Average</td>
<td>High</td>
</tr>
<tr>
<td>Weak Input Validation</td>
<td>Easy</td>
<td>Moderate</td>
</tr>
<tr>
<td>Error Handling</td>
<td>Difficult</td>
<td>Moderate</td>
</tr>
<tr>
<td>SQL Injection</td>
<td>Easy</td>
<td>Severe</td>
</tr>
<tr>
<td>Weak or Broken Cryptography</td>
<td>Difficult</td>
<td>High</td>
</tr>
<tr>
<td>Client Side Script Security</td>
<td>Easy</td>
<td>Moderate</td>
</tr>
<tr>
<td>Cross-Site Request Forgery (CSRF)</td>
<td>Average</td>
<td>Moderate</td>
</tr>
<tr>
<td>Cross-Site Scripting (XSS)</td>
<td>Average</td>
<td>Moderate</td>
</tr>
<tr>
<td>Clickjacking</td>
<td>Easy</td>
<td>Moderate</td>
</tr>
<tr>
<td>Unrestricted File Upload</td>
<td>Difficult</td>
<td>Severe</td>
</tr>
<tr>
<td>Sensitive Data Exposure</td>
<td>Difficult</td>
<td>Severe</td>
</tr>
<tr>
<td>Insufficient Attack Protection</td>
<td>Easy</td>
<td>Moderate</td>
</tr>
<tr>
<td>Under-protected APIs</td>
<td>Average</td>
<td>Moderate</td>
</tr>
<tr>
<td>HTTP Security Header Information</td>
<td>Average</td>
<td>Moderate</td>
</tr>
</tbody>
</table>
Secure your business from cyber threats using Astra Security Suite.

How can we help you? Let’s talk.

hello@getastra.com

www.getastra.com

fb.com/getAstra

@getastra

linkedin.com/company/getastra

Schedule a Call

Making Security Simple for thousands of online businesses