Application Security Testing

Capability Snapshot

- Performed more than 700 application security assessments for customers across Financial Services, Manufacturing, Retail, Software Services and Healthcare domains.
- Hybrid Methodology - Automated and Manual Web Application Security Testing for target applications
- we45's Security Testing tools:
  - Commercial
  - Open Source
  - Custom Developed – In House (Python and Java based)
- Best Practices Assessed for:
  - SANS CWE Top 25
  - OWASP Top 10
  - Attacks derived from Threat Modeling

Assessment Objectives

- Engage with business and technical stakeholders of the client and identify possible application risk and threat profiles
- Identify all possible Vulnerabilities – In Design (Architecture), Development and Deployment
- Prioritize Vulnerabilities and Exploits by business risk and benchmarked against globally accepted standards
- Provide clear, actionable intelligence to clients after the security test.
- Enhance knowledge of the product team on secure application development practices

The we45 Approach

Security Profiles and Threat Modeling	• Application Overview - Understanding the functionality of the Application • Identifying Key Security Risks to the Application and prioritizing said risks. • Application Security Threat Modeling with STRIDE and other world-class Methodologies
Application Vulnerability Assessment	• Performing Reconnaissance and Mapping against the application • Identifying Vulnerabilities in the Application and related system components
Application Penetration and Post Exploitation	• Penetration Selected Vulnerabilities in Application • Maintaining Persistent Access to exploited application for deeper analysis
Analysis, Reporting and Skill Enhancement	• Delivering presentation to key management stakeholders • Preparing and delivering Comprehensive Web Security Testing Reports • Designed Action Plan for Management Review • Secure Application Development Bootcamp for Developers

Security Profiles & Threat Modeling

- Overview – we45's Security Analysts would perform an walkthrough the application's functionality. This is meant to identify key data security risks for information stored, processed and transmitted by the application. These risks are meant to unlock the highest business value for the client.
- Security Profiles – we45's Security Analysts will create security profiles for the key risks identified in the Overview process. For instance, Theft of Payment Card Data would be a key risk for an eCommerce Application. They would also assign a score to the risk severity.
- Threat Models – Based on the Security Profiles, we45's Security Analysts would identify various attack scenarios that could be used to recreate the security profile. This is done based on the STRIDE and DREAD Methodologies by Microsoft.
- SCRUM – The Threat Models would be used as an attack plan. we45 uses a SCRUM Model to prioritize and test the application for maximum efficiency and effectiveness.

Examples – Security Profiles

"Critical Security Threat – If one broker gains access to the account of another brokerage"

"Critical Security Threat – If an external attacker can gain access to HealthCare Information stored in the SQL DB or the Analytics DB"

"Major Security Threat – If a user can tamper with pricing information during the checkout process "

"Critical Security Threat – Unauthorized user can access sensitive application data on device (Stolen/Lost Device)"

Security Profiles & Threat Modeling

- Overview – we45's Security Analysts would perform an walkthrough the application's functionality. This is meant to identify key data security risks for information stored, processed and transmitted by the application. These risks are meant to unlock the highest business value for the client.
- Security Profiles – we45's Security Analysts will create security profiles for the key risks identified in the Overview process. For instance, Theft of Payment Card Data would be a key risk for an eCommerce Application. They would also assign a score to the risk severity.
- Threat Models – Based on the Security Profiles, we45's Security Analysts would identify various attack scenarios that could be used to recreate the security profile. This is done based on the STRIDE and DREAD Methodologies by Microsoft.
- SCRUM – The Threat Models would be used as an attack plan. we45 uses a SCRUM Model to prioritize and test the application for maximum efficiency and effectiveness.

Security Profiles & Threat Modeling

- Overview – we45's Security Analysts would perform an walkthrough the application's functionality. This is meant to identify key data security risks for information stored, processed and transmitted by the application. These risks are meant to unlock the highest business value for the client.
- Security Profiles – we45's Security Analysts will create security profiles for the key risks identified in the Overview process. For instance, Theft of Payment Card Data would be a key risk for an eCommerce Application. They would also assign a score to the risk severity.
- Threat Models – Based on the Security Profiles, we45's Security Analysts would identify various attack scenarios that could be used to recreate the security profile. This is done based on the STRIDE and DREAD Methodologies by Microsoft.
- SCRUM – The Threat Models would be used as an attack plan. we45 uses a SCRUM Model to prioritize and test the application for maximum efficiency and effectiveness.

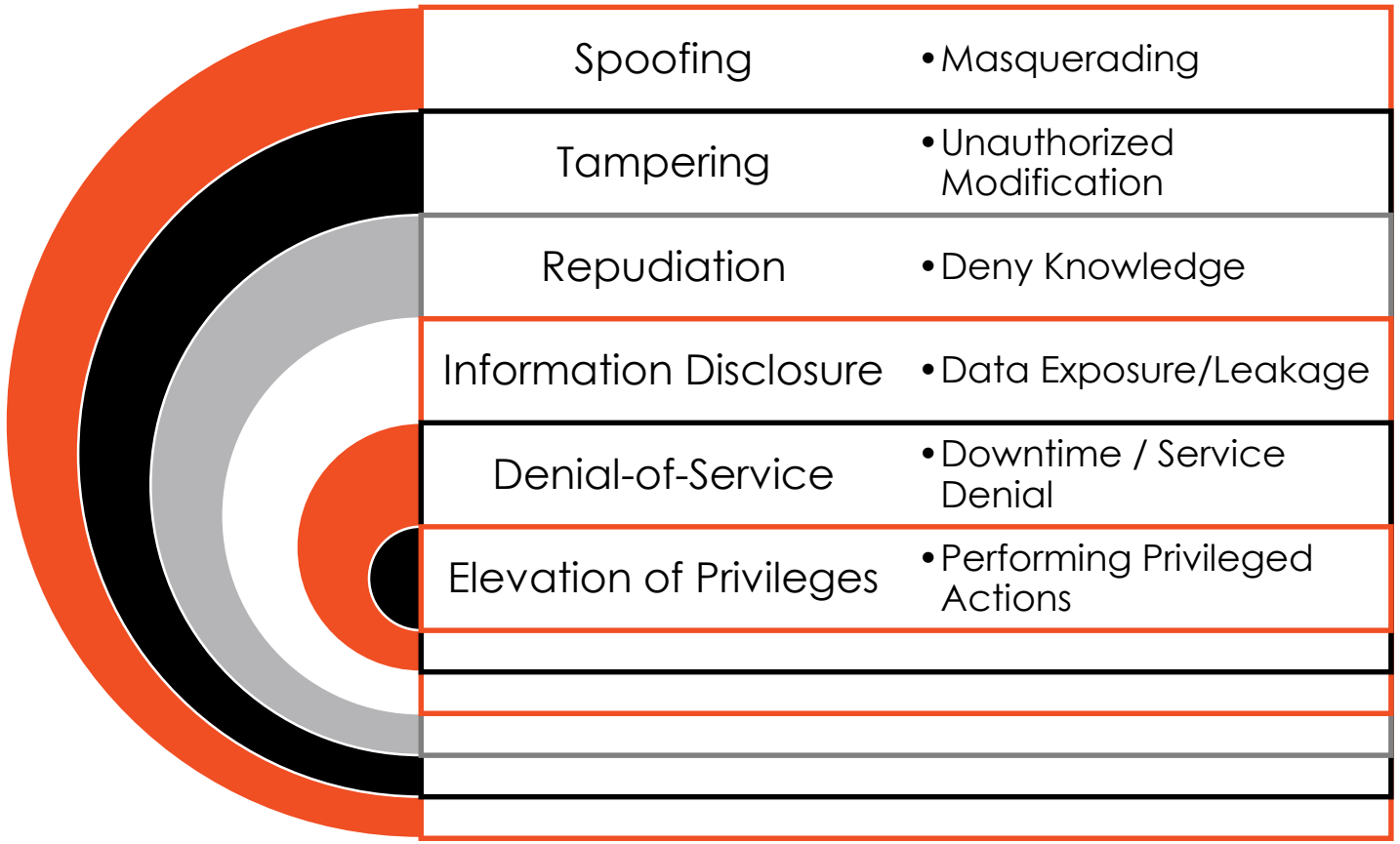
Security Profiles & Threat Modeling

- Overview – we45's Security Analysts would perform an walkthrough the application's functionality. This is meant to identify key data security risks for information stored, processed and transmitted by the application. These risks are meant to unlock the highest business value for the client.
- Security Profiles – we45's Security Analysts will create security profiles for the key risks identified in the Overview process. For instance, Theft of Payment Card Data would be a key risk for an eCommerce Application. They would also assign a score to the risk severity.
- Threat Models – Based on the Security Profiles, we45's Security Analysts would identify various attack scenarios that could be used to recreate the security profile. This is done based on the STRIDE and DREAD Methodologies by Microsoft.
- SCRUM – The Threat Models would be used as an attack plan. we45 uses a SCRUM Model to prioritize and test the application for maximum efficiency and effectiveness.

Security Profiles & Threat Modeling

- Overview – we45's Security Analysts would perform an walkthrough the application's functionality. This is meant to identify key data security risks for information stored, processed and transmitted by the application. These risks are meant to unlock the highest business value for the client.
- Security Profiles – we45's Security Analysts will create security profiles for the key risks identified in the Overview process. For instance, Theft of Payment Card Data would be a key risk for an eCommerce Application. They would also assign a score to the risk severity.
- Threat Models – Based on the Security Profiles, we45's Security Analysts would identify various attack scenarios that could be used to recreate the security profile. This is done based on the STRIDE and DREAD Methodologies by Microsoft.
- SCRUM – The Threat Models would be used as an attack plan. we45 uses a SCRUM Model to prioritize and test the application for maximum efficiency and effectiveness.

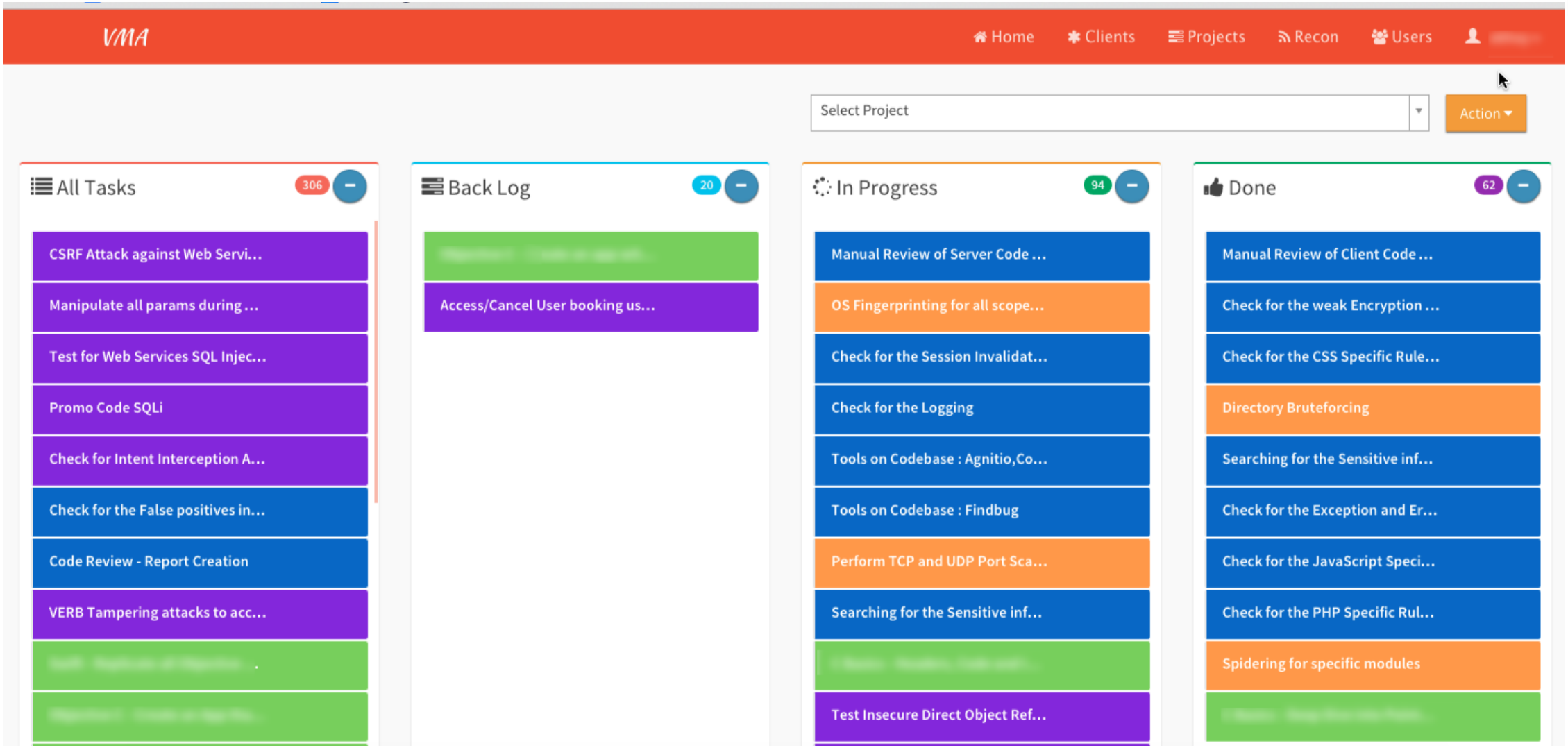
Threat Modeling Using STRIDE



Security Profiles & Threat Modeling

- Overview – we45's Security Analysts would perform an walkthrough the application's functionality. This is meant to identify key data security risks for information stored, processed and transmitted by the application. These risks are meant to unlock the highest business value for the client.
- Security Profiles – we45's Security Analysts will create security profiles for the key risks identified in the Overview process. For instance, Theft of Payment Card Data would be a key risk for an eCommerce Application. They would also assign a score to the risk severity.
- Threat Models – Based on the Security Profiles, we45's Security Analysts would identify various attack scenarios that could be used to recreate the security profile. This is done based on the STRIDE and DREAD Methodologies by Microsoft.
- SCRUM – The Threat Models would be used as an attack plan. we45 uses a SCRUM Model to prioritize and test the application for maximum efficiency and effectiveness.

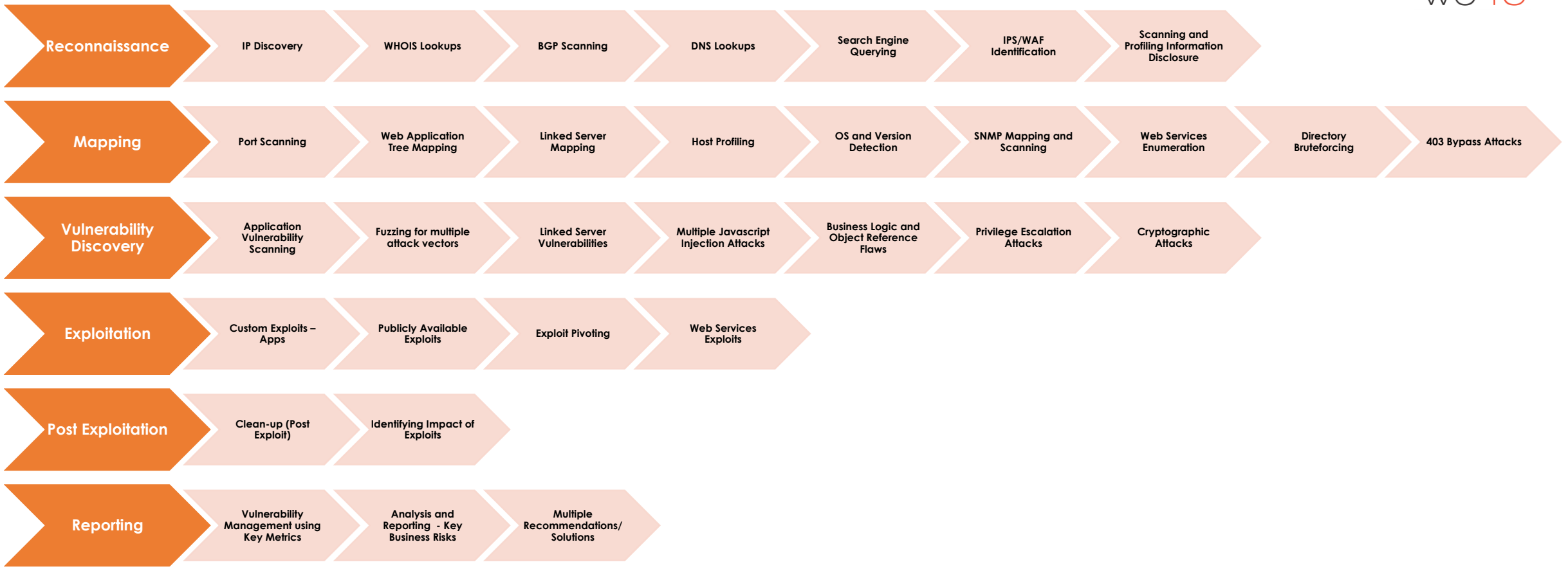
we45 – Penetration Testing SCRUM Board



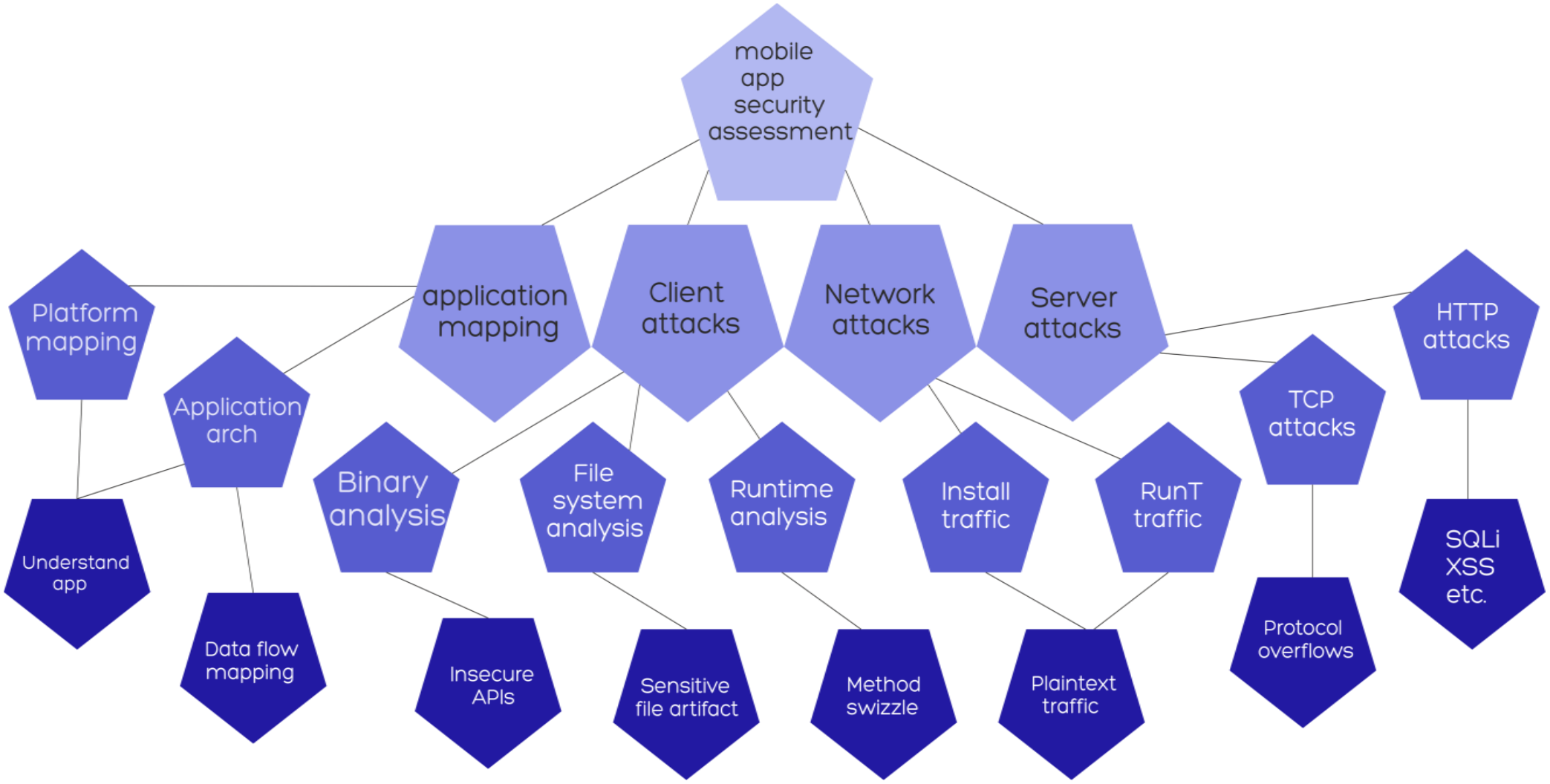
Security Profiles & Threat Modeling

- Overview – we45's Security Analysts would perform an walkthrough the application's functionality. This is meant to identify key data security risks for information stored, processed and transmitted by the application. These risks are meant to unlock the highest business value for the client.
- Security Profiles – we45's Security Analysts will create security profiles for the key risks identified in the Overview process. For instance, Theft of Payment Card Data would be a key risk for an eCommerce Application. They would also assign a score to the risk severity.
- Threat Models – Based on the Security Profiles, we45's Security Analysts would identify various attack scenarios that could be used to recreate the security profile. This is done based on the STRIDE and DREAD Methodologies by Microsoft.
- SCRUM – The Threat Models would be used as an attack plan. we45 uses a SCRUM Model to prioritize and test the application for maximum efficiency and effectiveness.

security testing methodology – high level snapshot

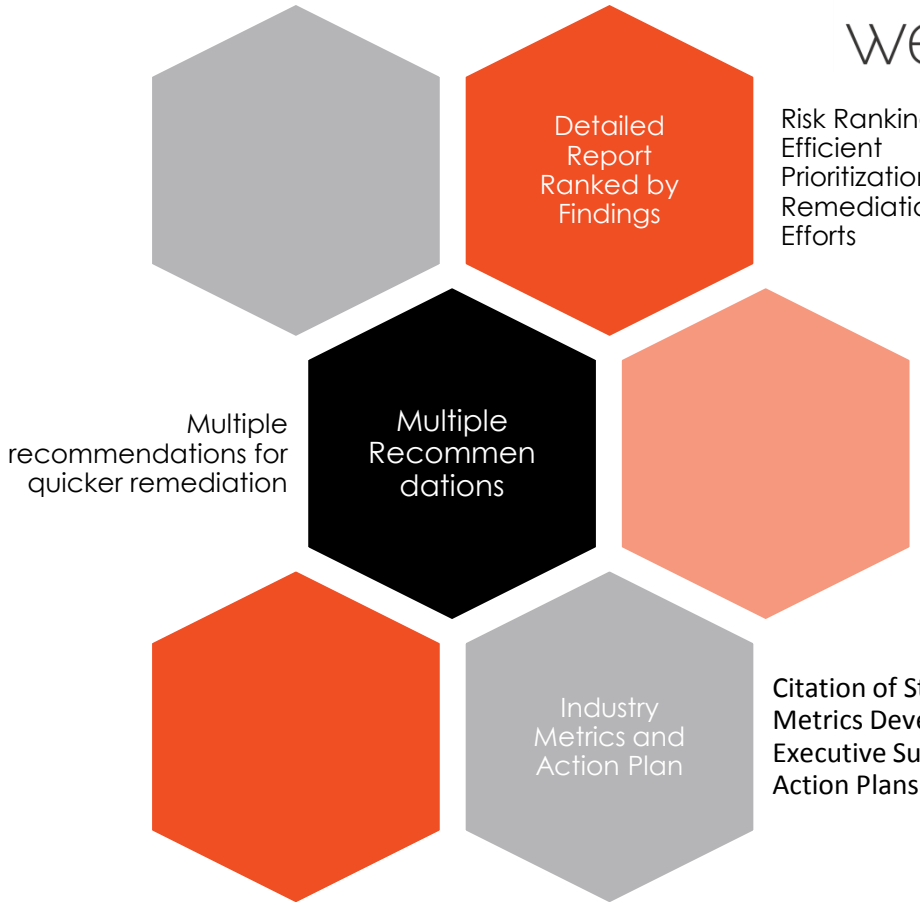


Mobile application security – exploit channel



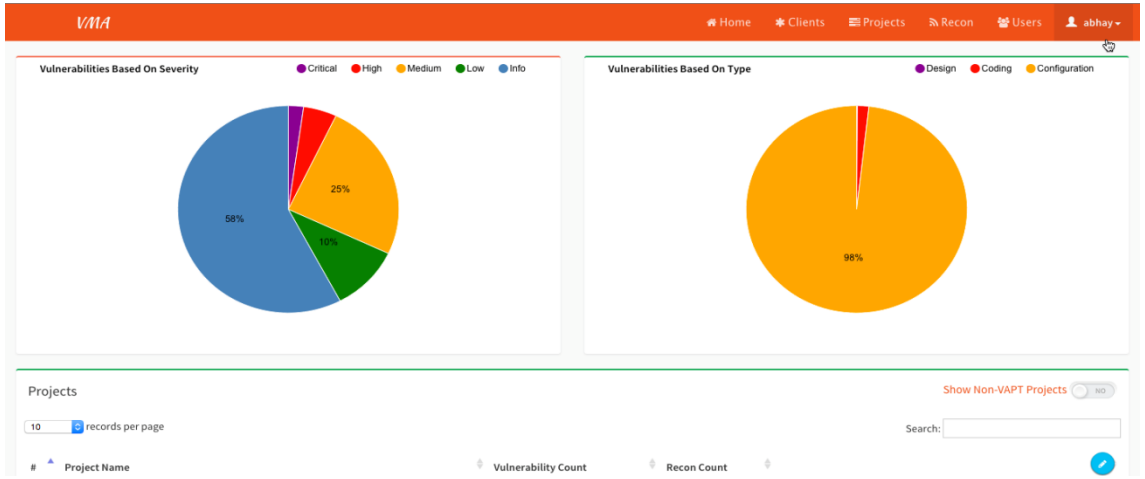
analysis & reporting

- Vulnerabilities ranked as per priority, exploit vector and business impact
- Findings - referenced with Industry metrics like CWE and CVE.
- Multiple recommendations and remediation strategies provided along with exploit vectors
- Remediation examples provided as code-snippets
- Executive Summary and Action Plan prepared for Management Action



vulnerability management engine

- we45's in – house security assessment analysis and reporting dashboard
- Integrates Vulnerability Assessment Results across multiple tools and applications
- Provides powerful analytics and integrated dashboards
- Recommendations, Metrics and Remediation Information
- Custom export of results



our application security solutions

- Application (Web/ Mobile/ Client-Server) Vulnerability Assessment and Penetration Testing
- Secure Application Development - Advisory and Consulting
- Application Security Code Review
- New Product Development / Revamp Architecture Review
- Application Security Risk Assessment
- Application Security (Web/ Mobile) Workshops

Thank You

www.we45.com