# Red Team Assessment by Seqrite Services yielded significant results for a leading financial institution

## About Client

This Seqrite Services client is a major private sector bank who, not just offers a wide range of financial services, but also includes personal, business, and wealth management services.

## Why Red Team is Necessary

The challenges in the path of a well-known financial institution are diverse. Every single piece of information, available physically or digitally, are of utmost confidentiality. Many responsibilities, actions and decisions are executed within the organization with the mentioned types of data and its security. Red Team assessment gives the practical understanding that how an attacker can gain unauthorized access to sensitive information that leads up to data breaches and other loss.

## Our Strategy

Red Team Assessment is our flagship and most comprehensive offering. It is not a one-estimate-fits-all approach, we customize our strategy as one of its kind by taking into consideration the business needs and plans of the organization. In kick-off meeting we collaboratively decided the scope, objectives and success matrix parameters and explained the Game Masters our activities, methodologies, timelines and team roles for the assessment.

## Multiple Attack Vectors

Red-Team reveals real-world opportunities which leverage the loopholes and compromise all aspects of an organization. Seqrite Services utilized a variety of techniques for gaining access to their sensitive data. Building on the reconnaissance efforts and the attack paths, our Red Team successfully executed each attack, which yielded valuable pieces of information. Following activities were performed in this multi-faceted attack to measure how well network, applications, physical security controls and people of the bank can withstand against a real-time attack.

1. **Open source intelligence (OSINT) and Darknet Monitoring Techniques**
   - Examined exposure of the bank and its employees' information by OSINT and Darknet Monitoring.
   - Leveraged this information to direct access employees, gain highly sensitive information such as PAN Cards of 4 CxOs
2. **Web and Mobile Application Penetration Testing**
   - Performed automated and manual web application testing that stimulated current threats along with pivoting and post exploitation.
   - Compromised main website of the organisation by writing a custom build exploit.
   - Successfully got remote access of their web server by exploiting the vulnerabilities like SQL Injection and Cross site scripting (XSS)
   - Performed dynamic and static analysis of mobile application testing for all platforms
   - Performed proxy bypass testing and validate internal and external security controls.
   - Assessed the security posture in terms of both technical vulnerabilities and business logic flaws.
   - Reality check to their incident response and detection capabilities.

3. **Internal and External Network Penetration Testing**
    - Recon-misconfigured web-servers, leaked credentials apart from conventional details
    - Got shell access of business-critical servers by compromising the internal/external Wi-Fi points.
    - Conducted PT on public facing network as well as internal network
    - Assessed the security posture of routers, firewalls, IDS and other security appliances.
    - Checked possible misconfigurations and correlated vulnerabilities with applications on the network.
4. **Social Engineering Attacks**
    - Compromised five (5) user email id / password and other details like employee ID, department etc. through various social engineering techniques like:
        - Phishing / Spear Phishing
        - Vishing / Direct Calling
        - SmiShing / Evil Twin
        - USB Baiting
        - Eavesdropping/ Offsite meeting
5. **Physical Security Breach**
    - Performed Physical PT for Data Centre, Corporate Office and Branch Office
    - Analysed vulnerable transit points
    - Tailgating / Access control bypass and gained access to internal devices and networks
    - Enumerated physical security countermeasures
    - Awareness assessment from Security Guard to C-Suite.

## Red Team Assessment Results and Conclusions

The Red Team assessment executed by Seqrite Services was highly successful and yielded a significant set of results. During the physical penetration testing, security awareness from security guards to C-suite was assessed and most of them didn't followed the basic security hygiene; as our team was successful to obtain the access of systems, unquestioned floorwalks, sensitive documents, USB baiting and a lot more. The incident response was slow and ineffectual, allowing our team to leave without reprimand.

The information gathered from open source intelligence and darknet monitoring revealed the lack of security awareness of many executive level employees who are unaware of safeguarding their digital footprints, in result we got PAN card of four CxOs, intranet portals of the bank and responses on personalized and fraudulent e-mails, and phone calls, all of which were performed by Seqrite Services.

The penetration testing revealed a number of vulnerabilities within its working applications, ranging from web applications to mobile applications which lead to one root cause- lack of adherence to security policies that leave the bank vulnerable to attack via any of the Seqrite Services team-member performing this activity.

Seqrite Services ensured that no detail was overlooked and has provided recommendations for all the issues to ensure that no doubt remain uncleared regarding proper practices to plug these security loopholes, and will continue to do so in the future as their right security partner.

> **“Red Team by Seqrite Services pulled out all the stops to ensure that the work was completed on time and to cost. The quality of the final product was in excess of the specification. We were particularly impressed by their professional approach to handling potentially sensitive issues in the study organizations, and their ability to engage with all stakeholders. They were very proactive & responsive in their communications of progress and issues throughout the work. As a result, we are looking forward to working with Red Team again in the future, and would not hesitate to recommend them for similar projects.”**
>
> - CISO, Bank