“The most frequent vulnerabilities that I have come across in the financial services sector tend to be misconfigurations and vulnerabilities common in legacy software. This is likely due to the complexity of financial systems, large amounts of sensitive data handled, and the pressure to launch new products in the market. Financial services organizations have significant security challenges, ranging from protecting sensitive data to regulatory compliance. However, this also offers them the opportunity to improve cybersecurity, foster collaboration, and develop innovations that strengthen security and trust.”

Richard Alviarez, @Rhack
Security Researcher Specializing in Financial Services Organizations

“Having hacked on a variety of financial service targets, I've noticed that these organizations often have a wider and more complex attack surface due to their company structures, which often include numerous acquisitions and subsidiaries. As a result, I’ve found vulnerabilities on obscure hosts—sometimes on newly launched or less commonly known domains. Due to the need to obtain an account for deeper testing, which is difficult and sometimes even impossible due to geographical restrictions (applying for a loan/credit card), a significant portion of the attack surface remains untouched."

Iustin Ladunca, @youstin
Security Researcher Specializing in Financial Services Organizations

Recommendations

- [x] Implement a strong authorization framework that relies on user policies and hierarchy, and validate authorization for every request that involves accessing sensitive objects or resources.
- [x] Avoid using functions that automatically bind a client's input into variables, internal objects, or object properties.
- [x] Use indirect, random, and unique identifiers instead of exposing direct references to internal objects and resources. Map these identifiers to the actual objects on the server side while validating and authorizing user-supplied input.