Hijacking via PDF

Executive Summary

This handout distills the key ideas behind the live Black Hat demonstration on using malformed PDFs to hijack user sessions. Rather than focusing on exploit delivery mechanics, the narrative centers on how misconfigurations, embedded JavaScript, and trust decisions intersect to create high-impact compromise opportunities.

Attack Surface Review

- Modern PDF readers support a broad feature set: forms, embedded media, document scripts, and network calls.
- Legacy enterprise workflows often require enabling privileged behaviors such as automatic form submission or file writes.
- Security teams routinely whitelist internal PDF generators, creating an implicit trust boundary attackers can abuse.

Weaponization Narrative

During the demo we walk through repurposing a legitimate procurement form. The malicious build starts with removing brittle XFA payloads and replacing them with reliable interactive elements. Crafted annotations trigger script execution the moment a reviewer opens the file, harvesting session cookies before proxying the victim to an innocuous decoy page. The same technique works against viewers that honor legacy JavaScript APIs or that permit silent network calls in trusted zones.

Defensive Countermeasures

- Disable high-risk PDF features—JavaScript, embedded file launches, and network submissions—unless business requirements demand them.
- Implement content disarm and reconstruction (CDR) on inbound PDFs to flatten dynamic features before delivery to end users.
- Pair viewer hardening with telemetry that captures document-originated network traffic and privilege escalations.

Key Takeaways

- PDF complexity creates fertile ground for stealthy session hijacking and credential theft.
- Operational trust in custom business forms grants attackers the pretext needed for reliable exploitation.
- Defensive teams must monitor reader capabilities, enforce least privilege, and routinely strip unnecessary features.

For a deeper dive, reference the companion research paper and tooling notes released alongside the session.