## **🧠 INDUSTRY: Medical / BioTech**

### **💉 Smart Syringe / IV Bag**

* **Exploit:** Micro-print barcode on medical packaging that encodes a malformed patient ID.
* **Trigger:** Barcode scanner misreads → injects dosage meant for a different patient or logs it under the wrong name.
* **Goal:** Data poisoning, medical sabotage, insurance fraud.

### **🧬 Genetic Sequencing Machines**

* **Exploit:** DNA strand contains malware (already POC’d in academia).
* **Trigger:** Sequencer reads malicious base pair pattern, buffer overflow hits backend.
* **Goal:** Backdoor into research labs, tamper with biotech analysis.

## **🧾 INDUSTRY: Retail / Logistics**

### **📦 Barcode Overlays**

* **Exploit:** Transparent overlay with alternate barcode reads different SKU.
* **Trigger:** Scanner pulls a payload that looks like a valid product but triggers logic exploits in POS software.
* **Goal:** Free items, logic corruption, inventory fraud.

### **📦 Return Label Exploits**

* **Exploit:** Return label QR or RFID tag contains malformed return data.
* **Trigger:** Return systems log unauthorized refund or generate phantom tracking logs.
* **Goal:** Fraud, delivery rerouting, laundering schemes.

## **🚗 INDUSTRY: Automotive / Transit**

### **⛽ Fuel Composition Exploit**

* **Exploit:** Modify fuel mixture with trace contaminants.
* **Trigger:** Vehicle sensors misread levels → detuning, ECU logic faults.
* **Goal:** Silent disablement, GPS spoof, fleet disruption.

### **🎫 Smart Toll Tag Hacks**

* **Exploit:** Place tuned metallic film over RFID.
* **Trigger:** Sends modified vehicle class signal (e.g., "motorcycle" not "truck").
* **Goal:** Route manipulation, toll fraud, network poisoning.

## **🎓 INDUSTRY: Education / Certification**

### **📚 Exam Sheet Exploit**

* **Exploit:** Hidden UV-inked QR code on a test paper that, when scanned for grading, auto-uploads backdoor payloads.
* **Trigger:** Grade scanner system receives malformed file disguised as scanned answer sheet.
* **Goal:** System compromise via scan-based logic injection.

## **🏢 INDUSTRY: Office / Access Control**

### **🖨 Printer Paper Payload**

* **Exploit:** Print malformed PCL/PS code on innocent-looking document.
* **Trigger:** Printer parses paper and executes code during print.
* **Goal:** Printer compromise → network access.

### **🧾 Badge Access with RFID Echo**

* **Exploit:** Fake access badge with passive RFID echo that delays actual UID packet slightly.
* **Trigger:** Reader accepts false credential during a timing window.
* **Goal:** Ghost entry, anti-forensics access.

## **🧱 INDUSTRY: Construction / Architecture**

### **🔌 Smart Tool Injection**

* **Exploit:** Deliver firmware-based payload via fake battery pack in smart drills.
* **Trigger:** When tool syncs with site server for diagnostics.
* **Goal:** Blueprint theft, worker tracking, remote site access.

### **🪟 Thermal Pane Reflection Mapping**

* **Exploit:** Install reflective coating on external glass.
* **Trigger:** Causes LiDAR/optical scanning drones to misread geometry.
* **Goal:** Map spoofing, perimeter blindness.

## **🪙 INDUSTRY: Finance**

### **💳 Smart Coin**

* **Exploit:** Coin alloy engineered to mimic magnetic stripe voltage of a specific card.
* **Trigger:** Insert into older hybrid swipe/NFC systems.
* **Goal:** Local brute auth, trigger fallback logic, or logic desync.

### **📄 Check with Invisible Ink Field**

* **Exploit:** Includes ghost endorsement lines only visible under IR.
* **Trigger:** Scanner reads altered line signatures.
* **Goal:** Check redirection, silent endorsement swapping.