

Section 6

# Interactive Exploit & Hijack Simulator

Investigated by: Agent Carla

Interactive Exploit & Hijack Simulator

## Interactive Exploit & Hijack Simulator

### Context & source limits

A reconstruction of the path from the phishing message to the server-side key registration and the trade swap. Before 2023, a Web API key registered on an account could read its inventory, cancel a pending trade offer and create a new one, and no trade-confirmation screen was shown to the account holder for any of those actions. That is the absence of least privilege (OWASP A01:2021). The timings in this simulation are illustrative and are not live measurements of the current platform.

Step through the reconstructed hijack. Each phase shows what the account holder sees and, beside it, the call Steam receives at the same moment. **Every one of those calls is correctly authenticated.** Nothing in the sequence needs Steam's authentication to fail — it needs the key it issues to carry no scope (OWASP A01:2021).

### What the player sees. What changes behind it. WALKTHROUGH SIMULATOR

01 / THE CHAT LURE **A friend asks to vote** Victim receives a message with a link.

02 / THE LOGIN **A lookalike portal** Victim enters sign-in credentials.

03 / THE ACCESS **Silent Web API creation** Attacker registers a developer key.

04 / THE SWITCH **Legitimate trade swapped** Clone bot duplicates target recipient.

05 / CONFIRMATION **Counterfeit approved** Wrong offer approved on mobile.

**The Exploit Completed.** Expecting a mobile prompt for their original trade, the victim approves the replacement trade. This is an integrated forensic walkthrough showing how the absence of Least Privilege (OWASP A01:2021) enables automated, sub-second asset hijacking.

The same step, seen from the network Reconstruction of the pre-2023 pattern · illustrative call shapes

**Victim** Approves the mobile prompt that was expected for the original trade.

**Attacker** Receives the items at the clone account.

**Steam sees** A transfer confirmed by the account holder on a registered device.

**Confirmation** genuine — made by the account holder

**Recipient** the clone bot, not the intended counterparty

*The confirmation is authentic. The offer it confirms is not the one the user initiated.*

**The record left behind:** a trade the user approved. That is the record Steam Support reads when the complaint arrives, and the reason the archived complaints were closed as user error. The complaints are in [the enforcement archive](#).

[Download PDF](#)

[Download JSON](#)

[Download PGP signature](#)

PhishDestroy · file integrity signature for this fact

[Material record ↗](#)