Powered by GLESEC

CYBERSECURITY NEWS CUSTOM REPORT

Generated on 03/28/2025 by

Earn $1000: Account Takeover by This Methodology

03/28/2025 03:10

Member-only story

Abhijeet Kumawat

.

Follow

3 min read·Just now

--

Share

Free Article Link

Imagine earning **$1000** just by finding a vulnerability in a website's authentication system. Account Takeover (**ATO**) vulnerabilities are among the most critical security flaws, and bounty programs reward researchers handsomely for reporting them. This write-up will guide you **step by step** through a practical methodology to exploit and report an **ATO vulnerability**. □♂

Created by Copilot

How I Made $300 in 5 Minutes□

□Free Article Link

infosecwriteups.com

Account Takeover occurs when an attacker gains **unauthorized access** to a user's account by exploiting weaknesses in authentication or session management. The impact can be severe, including **financial fraud**, **identity theft**, and **data breaches**. □

Many platforms, including **Bugcrowd, HackerOne**, and private programs, pay **up to $1000 or more** for valid ATO reports. This guide will walk you through a methodology that has led to **real-world payouts**. □

Deep Recon Methodology for Bug Bounty Hunters | Part-1

Hello, everyone!

cybersecuritywriteups.com

1 Choose a **target** with a login and account recovery feature. 2 Identify authentication mechanisms: **Email, phone number, OAuth, or SSO**. 3 Analyze **password reset and account recovery** flows.

Most ATO exploits target **weak recovery mechanisms**. Common issues include:

- **IDOR (Insecure Direct Object References)** in password reset.
- **Email or phone number enumeration**…

FutureProof 2.0 | Episode #6: Cybersecurity in an AI-Powered World

03/28/2025 03:34

Member-only story

Bayo Adebogun

.

Follow

4 min read·Just now

--

Share

FutureProofing Cybersecurity

AI Is Evolving — So Are the Threats

AI is no longer just accelerating innovation — it’s transforming the threat landscape itself.

From deepfakes and real-time phishing to autonomous cyberattacks, we’re entering a world where machine-speed crime is the new norm. According to **Cybersecurity Ventures**, the global cost of cybercrime is projected to hit **$10.5 trillion** by 2025. Meanwhile, cybersecurity spending is set to top **$2 trillion**, driven largely by the explosion of AI-enabled threats.

In a world where malware writes itself and fake voices pass as real, defense must move faster than offense. **Proactive protection is no longer optional — it's existential.**

The Rise of AI-Generated Threats
Deepfakes & Synthetic Media

AI-generated audio and video are now indistinguishable from real people. In a high-profile incident, scammers used **deepfake voice cloning** to impersonate a CEO and trick a bank into wiring **$35 million**. The tools are widely accessible — and frighteningly effective.

Autonomous Cyberattacks

Tools like **WormGPT** and **FraudGPT** — black-hat offshoots of language models — are being used to craft malware, phishing emails, and ransomware at scale, all without human guidance. AI can now scan for vulnerabilities and exploit them autonomously in real time.

AI-Powered Phishing & Social Engineering

LLMs like ChatGPT (or malicious clones) are enabling hyper-personalized, convincing scams across email, voice, and even video calls.

Red Teaming: The New Frontier

In March 2025, **MITRE and the U.S. Department of Homeland Security** released guidelines for **AI red teaming** — testing AI systems by simulating adversarial use. Top firms like **Anthropic** and **Microsoft** now include adversarial AI teams focused on stress-testing their models before deployment.

Why It Matters:

 Threats now operate at machine speed.
 Criminals don't need skills — just access to the right…