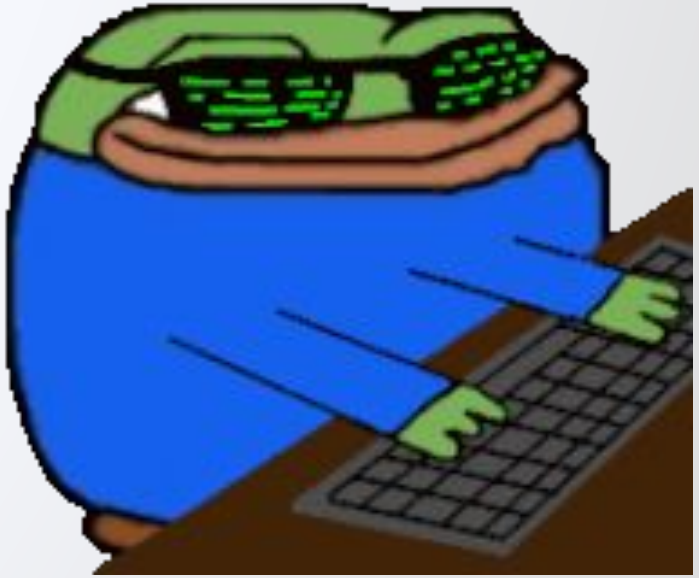
Exploiting Business Logic Flaws:

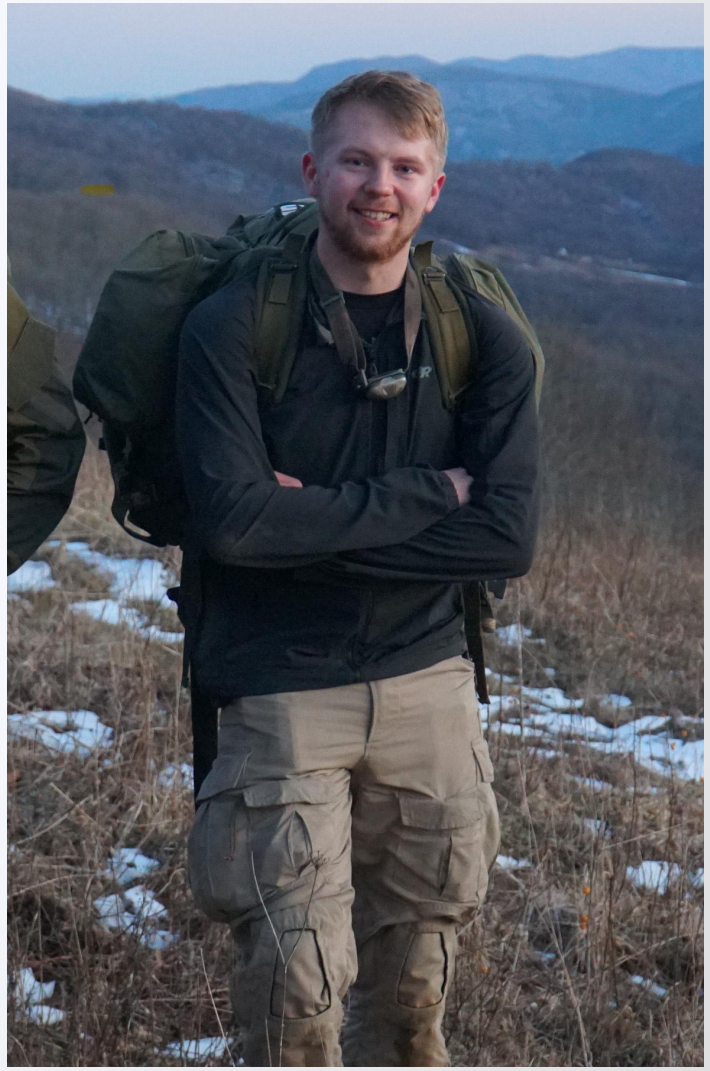
The Hidden Weaknesses That Hackers Love



Presentation by Chandler Johnson

whoami

- Chandler Johnson
- OWASP Knoxville Chapter Leader
- Ethical Hacking Consultant at Zelvin Security
- Veteran
- Outdoors Enjoyer
- Just Another Nerd…



Agenda

- What is Business Logic?
- Causes of Business Logic Flaws
- Exploiting Business Logic Flaws
- Modern Security Tooling Ineffective
- Preventing Vulnerabilities
- Questions

What is Business Logic?

The term “business logic” simply refers to the **set of rules that define how the application operates**.

As these rules aren’t always directly related to a business, the associated vulnerabilities are also known as “application logic vulnerabilities” or simple “logic flaws”.

OWASP Definition:

OWASP: “business logic vulnerabilities are ways of using the legitimate processing flow of an application in a way that results in a negative consequence to the organization.”

NVD Categorization: CWE-840: Business Logic Errors

Causes of Business Logic Flaws

Primary Causes

- Client-Side Validation *Reliance*
- Improper Workflow Validation
- Improper Data Validation
- Flawed User Behavior Assumptions

https://portswigger.net/web-security/logic-flaws

Exploitation Research - Bug Bounty Reports

- HackerOne: https://hackerone.com/hacktivity/overview
- Real world reports.
- POC (Proof-of-Concept) often supplied on disclosed vulnerabilities.
- Sophisticated techniques frequently presented.




cwe:("Business Logic Errors") AND disclosed:true

Search for reports

cwe:("Business Logic Errors") AND disclosed:true

Filter Sort

Disclosed Undisclosed

Double Payout via PayPal

Coinbase — Critical — $10,000 — Resolved

295

Double Payout via PayPal

Disclosed 6 years ago by dawgyg Business Logic Errors

Valve — Critical — $7,500 — Resolved

Modify in-flight data to payment provider Smart2Pay

410

Disclosed 3 years ago by drbrix Business Logic Errors

A vulnerability was discovered
changing the email associated
amount they desired. This cou

Modify in-flight data to payment provider Smart2Pay

Stripe — Medium — $5,000 — Resolved

Fee discounts can be redeemed many times, resulting in unlimited fee-free transactions

233

Disclosed 2 years ago by ian Business Logic Errors

A fee discount offer on Stripe transactions could be redeemed multiple times, resulting in unlimited fee-free transactions. The vulnerability allowed the attacker to call the `/ajax/accept_fee_discount_offer` endpoint multiple times, applying the discount each time. The impact was unlimited fee-free discounts, costing Stripe about 3% of each discount. This summary was automatically generated.

Reddit — High — $5,000 — Resolved

Able to approve admin approval and change effective status without adding payment details .

163

Disclosed 2 years ago by bisesh Business Logic Errors

The vulnerability allowed an attacker to bypass the review process and change the status of an ad campaign to approved and active without adding payment details. This was

Modern Security Tooling Ineffective

Preventing Business Logic Flaws

OWASP

TM