

Why Software Still Stinks

...and what you can do about it!



About Ed Adams

- CEO, Security Innovation Inc.
- Host of Ed TALKS: www.edtalks.io
- Director, Cyversity
- Research Fellow, Ponemon Institute
- Privacy by Design Ambassador, Canada
- Mechanical Engineer, Software Engineer
- In younger days, built non-lethal weapons systems for government & law enforcement



www.edtalks.io






About Security Innovation

- Securing software *and* its ecosystem for two decades



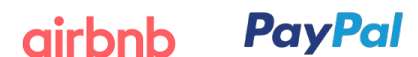
- Helping clients get smarter about software security

-  **Assessments:** understand gaps
-  **Standards:** establish repeatable practices
-  **Training:** enable good decisions

Over
3.5 Million
Users

Authored
18
Books

Gartner MQ
6x
Security Training





Attack Example #1: *SQL Injection*

- Apps are dumb; they do as they're told
- A login field sends a message to the database

```
SELECT * FROM USERS WHERE  
Username = 'Ed' AND Password = 'Adams';
```

- But... humans know logic
 - What if you give it something it can't argue with?
 - Maybe something that's always true?
 - Will the dumb app be fooled?

DEMO TIME!

LOG IN

TO SHADOW BANK

LOG IN

[Forgot password?](#)



Example #2: *Cross-site Scripting*

- Apps execute code commands
- JavaScript has many such commands

- Some humans are not nice
 - They might feed apps harmful commands
 - Can the dumb app be fooled again?

DEMO TIME!

LOG IN TO SHADOW BANK

LOG IN

[Forgot password?](#)





Example #3: *Escalation of Privilege*

- Get into an easy to open door
- Explore and exploit once inside
- Do damage and extract goods

- Did I mention some humans are not nice?
 - They will mess with “safe” areas

DEMO TIME!

Example #3: *Escalation of Privilege*



I want in here



I can get in here

What's in a house?

- TV
- Computers
- Electronics
- Money



What's in a shed?

- Ladders
- Bolt cutters
- Spare keys
- Drills & Saws





Start Here



Go Here



Examples #4, 5, and 6

- Time permitting, we'll also look at:
- Parameter Tampering
- Fuzzing Inputs
- Cloud Service Misconfiguration

DEMO TIME!



- BANKING
- BROKERAGE
- EXCHANGE
- COMMUNITY
- ABOUT

LOG OUT

Account

- Account Summary
- Transfer Money
- View All Transfers
- Request A Loan

Account Summary for The Shadow

Account Number: 83247638

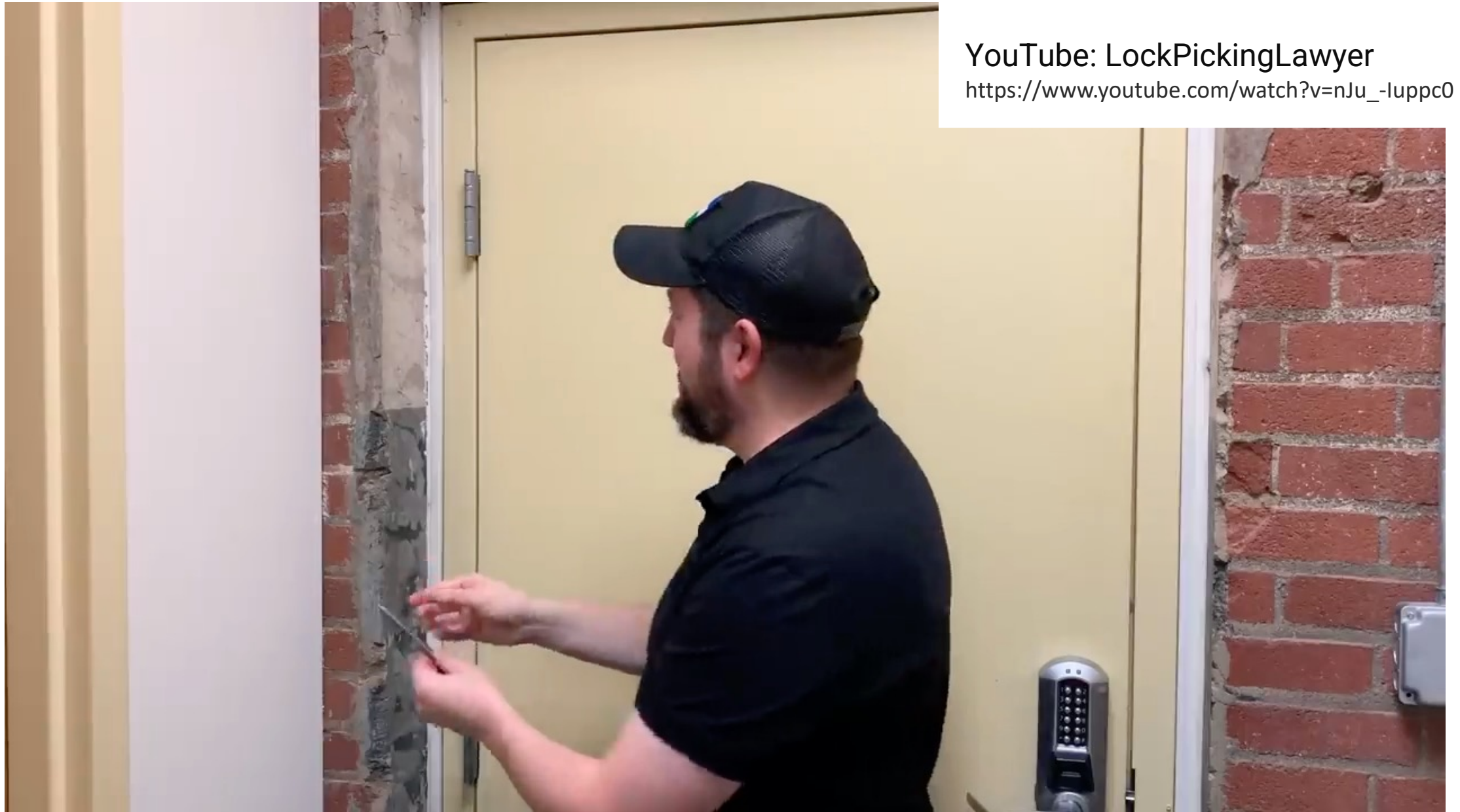
Balance: \$1873.32

Recent Transactions (View All)

Date	Details	Amount
7/6/21	Transfer to Dark Trader	(400.00)
7/6/21	Transfer from Arnold T'Poodle	300.00



YouTube: LockPickingLawyer
https://www.youtube.com/watch?v=nJu_-luppc0



Thank You



eadams@securityinnovation.com

www.edtalks.io

Security Training Benchmarks

getsec.in/PonemonReport

