

From Secure-by-Design to Abuse-by-Design: Why Modern Systems Fail in Ways We Don’t Model

2026 CORNCON CYBERSECURITY CONFERENCE

Meet Your Corn-speakers



Arjun Katneni



Lead Security Engineer

Swati Babbar



Application Security Engineer

This Photo by Unknown Author is licensed under CC BY-SA-NC

2026 CORNCON CYBERSECURITY CONFERENCE

Agenda



1. What Traditional Threat Modeling Does Well?
2. Let's STRIDE
3. The Missing Layer: Modeling Abuse
4. The Abuse Lens?
5. Demo
6. Why This Matters More Today?
7. Abuse Trees
8. Five Questions For Every Critical Workflow
9. The Abuse Review Framework
10. What's Next?

JPMorgan Chase sues more customers who allegedly stole cash in ‘infinite money glitch’

PUBLISHED WED, APR 16 2025·8:07 AM EDT | UPDATED WED, APR 16 2025·10:31 AM EDT

Retrospective: Recent Coinbase Bug Bounty Award

By Feb 18, 2022 • 3min read

At Coinbase, our number one priority is ensuring that we uphold our security commitments to our customers.

On February 11, 2022, we received a report from a third-party researcher indicating that they had uncovered a flaw in Coinbase’s trading interface. We promptly mobilized our security incident response team to identify and patch the bug, and resolved the underlying system issue without any impact to customer funds.



2026 CORNCON CYBERSECURITY CONFERENCE

What happened?

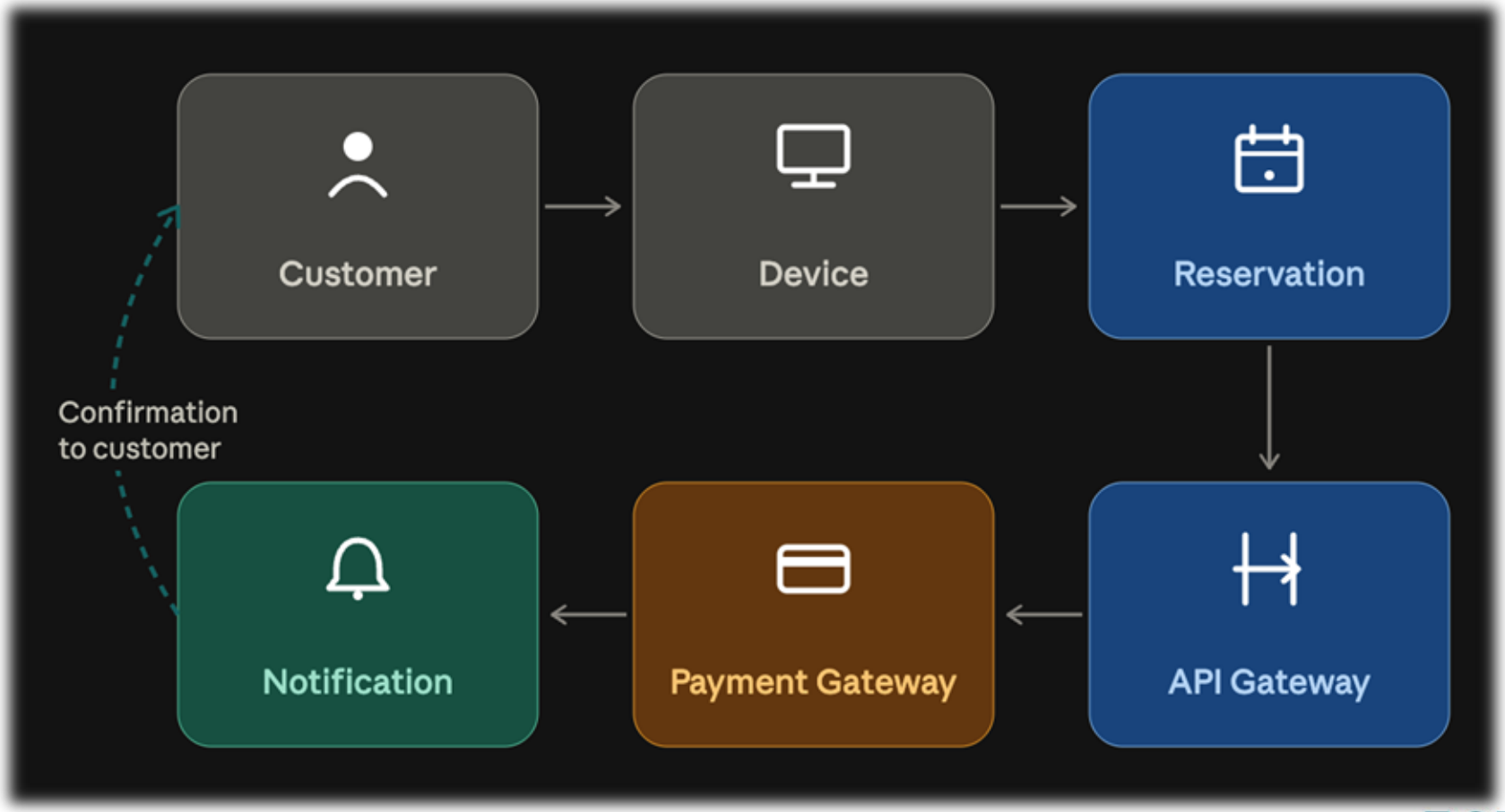


Was any control bypassed?

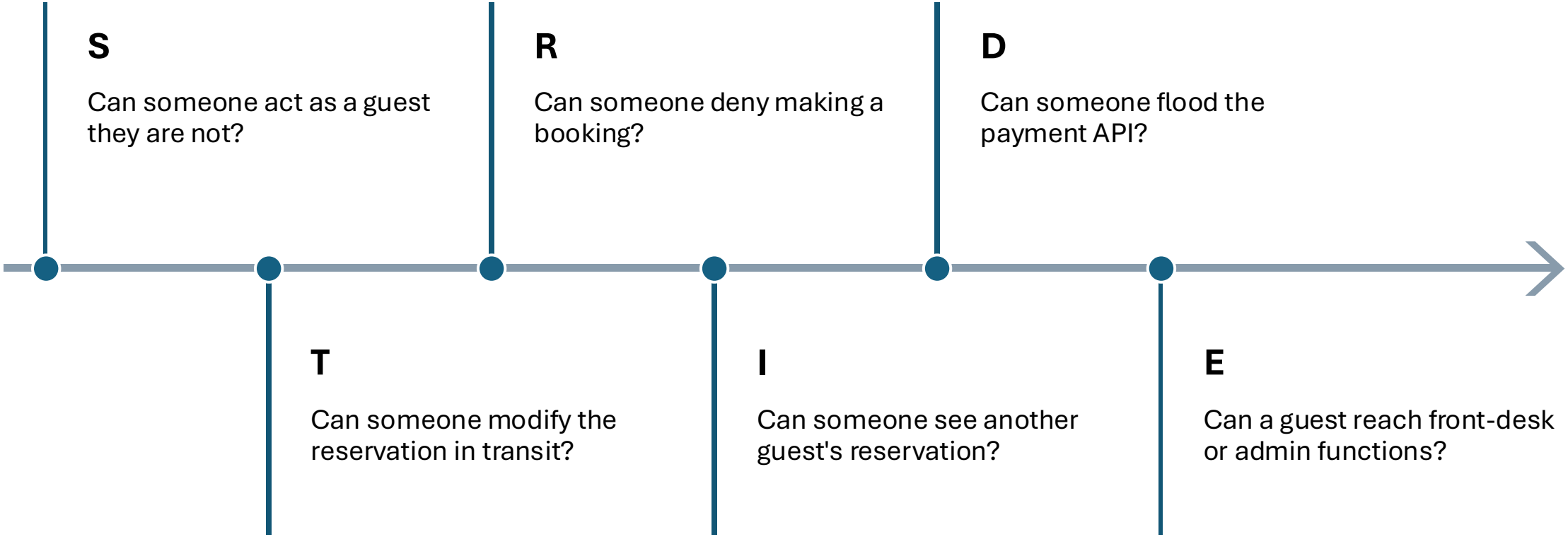
Did authentication fail?

Did authorization fail?

What Traditional Threat Modeling Does Well?



Let’s STRIDE


S
Can someone act as a guest they are not?
T
Can someone modify the reservation in transit?
R
Can someone deny making a booking?
I
Can someone see another guest's reservation?
D
Can someone flood the payment API?
E
Can a guest reach front-desk or admin functions?

The Missing Layer: Modeling Abuse

STRIDE is very good at asking whether a system can be **broken**. It is not built to ask whether a system can be **used, correctly**, in a way we never intended.

Traditional Question

"Can someone bypass authentication?"

Abuse Lens

"What can an authenticated, authorized user legitimately do that we never intended?"

The Abuse Lens?

Repeat

A valid action is submitted more times than intended

Reorder

Step 3 happens before step 1

Race

Parallel requests each pass on their own

Combine

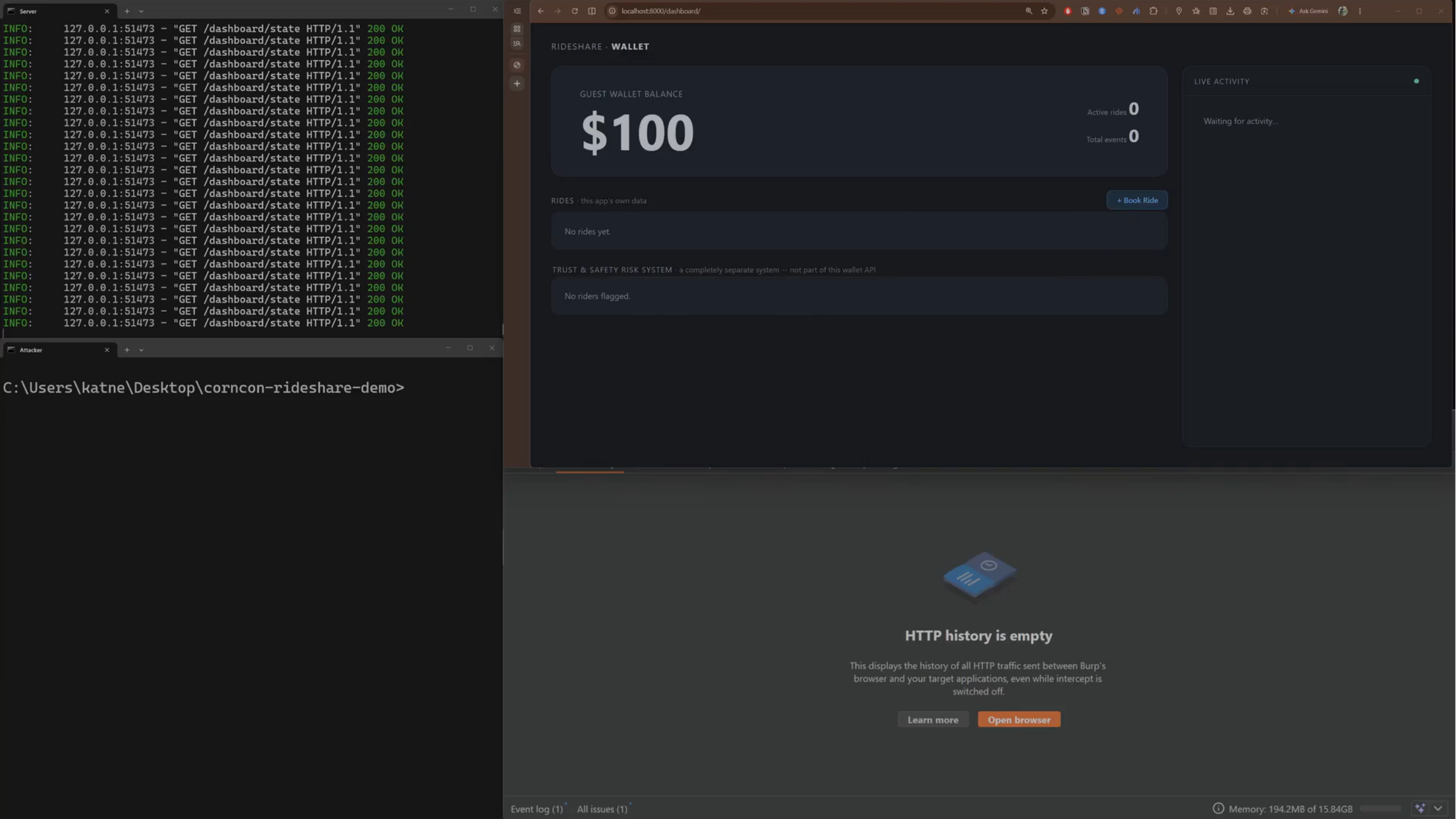
Two valid actions interacting in a way nobody planned

Exhaust

A shared resource is consumed faster than intended



CornCon 12


Server
INFO: 127.0.0.1:51473 - "GET /dashboard/state HTTP/1.1" 200 OK
Attacker
C:\Users\katne\Desktop\corncon-rideshare-demo>
localhost:8000/dashboard/
RIDESHARE · WALLET
GUEST WALLET BALANCE
$100
Active rides 0
Total events 0
LIVE ACTIVITY
Waiting for activity...
RIDES · this app's own data
+ Book Ride
No rides yet.
TRUST & SAFETY RISK SYSTEM · a completely separate system -- not part of this wallet API
No riders flagged.
HTTP history is empty
This displays the history of all HTTP traffic sent between Burp's browser and your target applications, even while intercept is switched off.
Learn more
Open browser
Event log (1)
All issues (1)
Memory: 194.2MB of 15.84GB

Pull Back The Curtain

Semantic web Racer: Dynamic security testing of the web application against race condition in the business layer

Article | Recommended articles | Cited by (6) | Metrics

Smashing the state machine: the true potential of web race conditions



James Kettle
Director of Research
@albinowax

Published: Wednesday, 9 August 2023 at 18:00 UTC

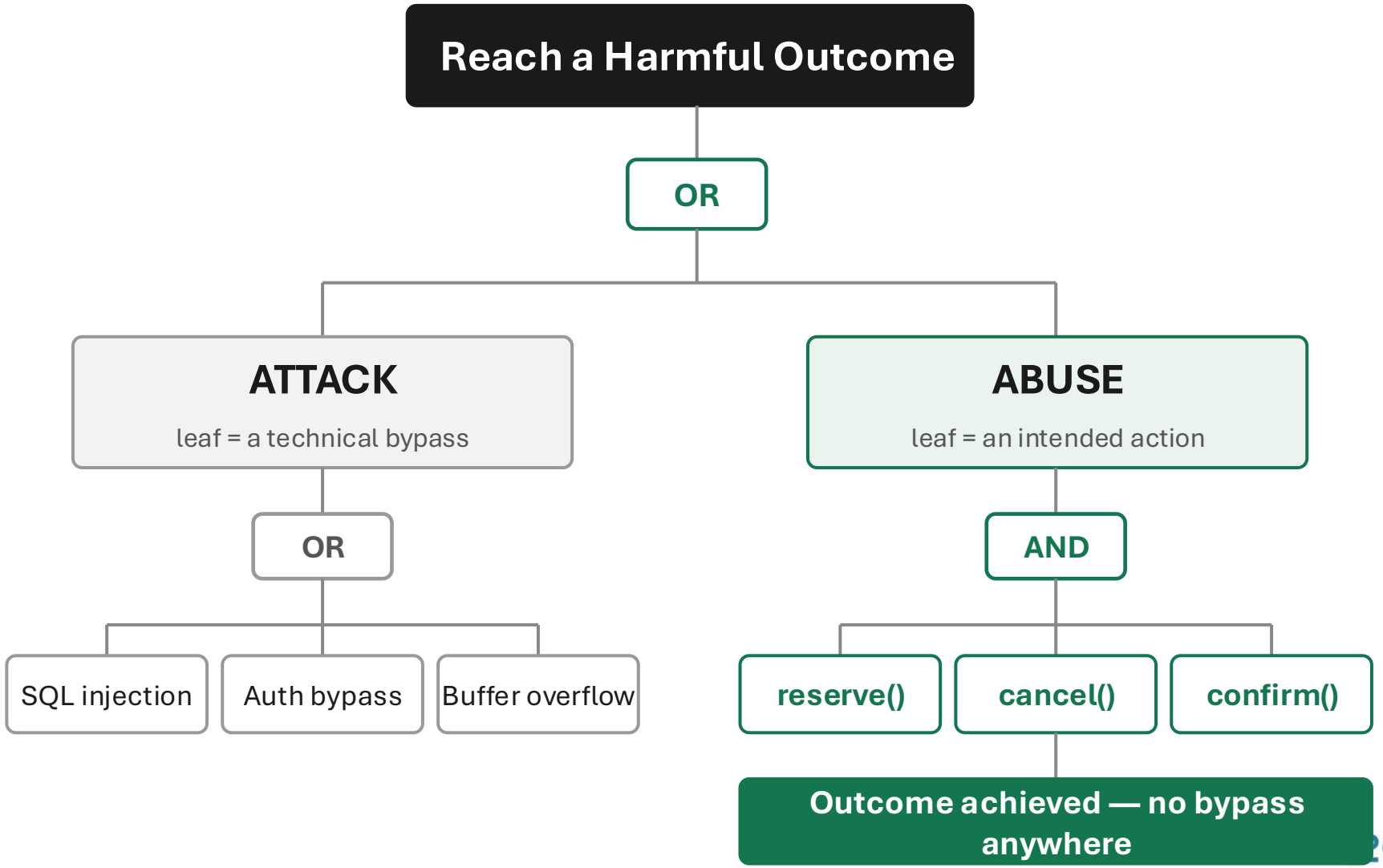
Updated: Monday, 18 September 2023 at 14:17 UTC

2026 CORNCON CYBERSECURITY CONFERENCE

Why this matters more today?



Abuse Trees



2026 CORNCON CYBERSECURITY CONFERENCE

Five Questions for Every Critical Workflow



1

Unenforced Assumptions

What assumptions are we making that are not enforced in code?

2

Repeat Actions

What actions can be repeated that we assumed happen once?

3

State Skipping

What states can be skipped or revisited?

4

Dangerous Combinations

What combinations of individually valid actions become risky together?

5

Incentive

What incentive exists for someone to try?

2026 CORNCON CYBERSECURITY CONFERENCE

The Abuse Review Framework

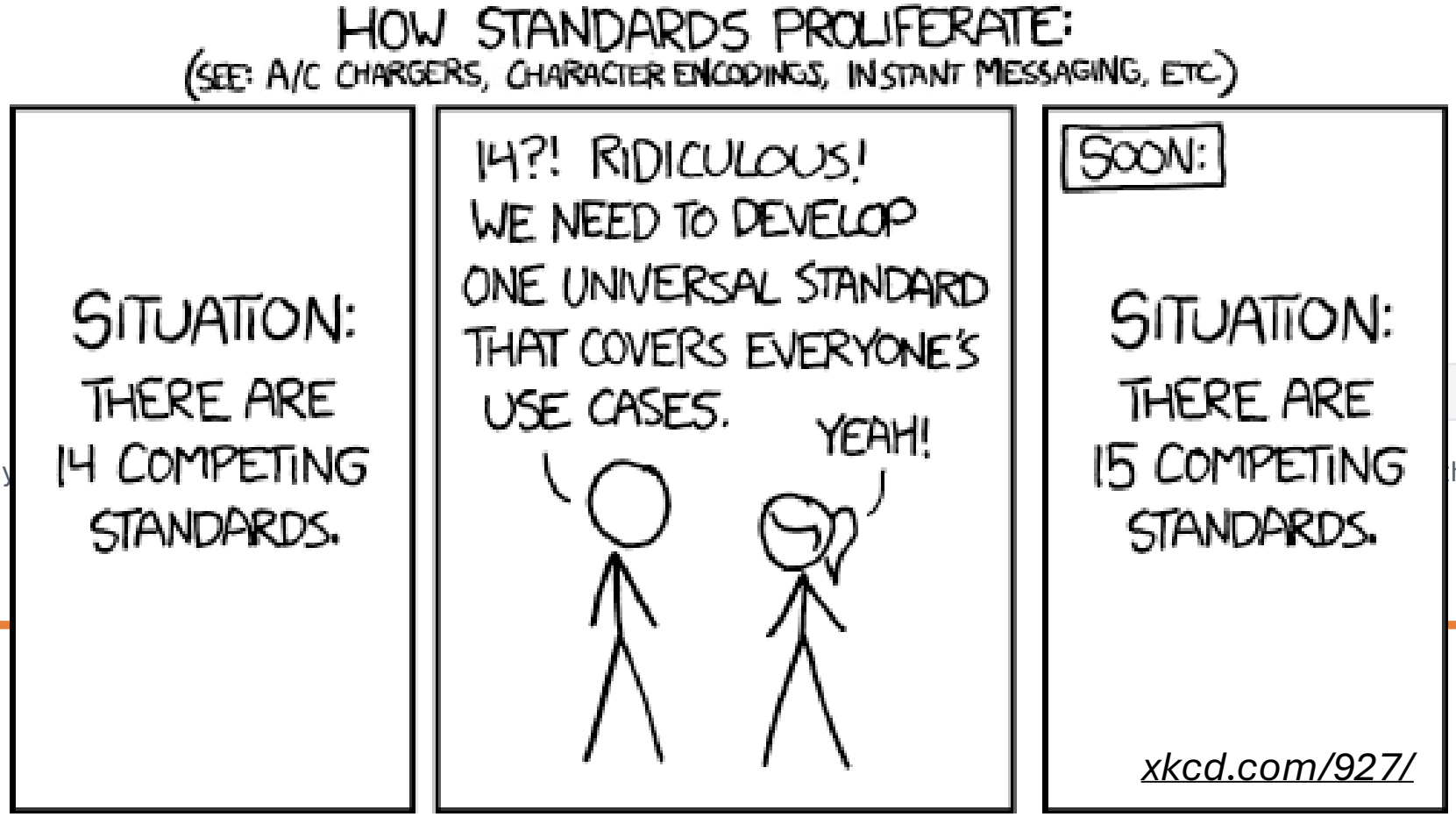
STEP 1

Scope

STRIDE

Reuse the boundary y
drew.

he data lives.



What's Next?

Here is how you use this on Monday.





1

Keep doing threat modeling

Nothing here replaces it.

2

Add an Abuse Review

Top five revenue- or access-critical workflows. Run the four steps on them.

3

Write assumptions down, explicitly

Enforce them at the data layer. Look hard at any workflow where an AI agent now holds permissions a person used to.

Thank you!



2026 CORNCON
CYBERSECURITY
CONFERENCE