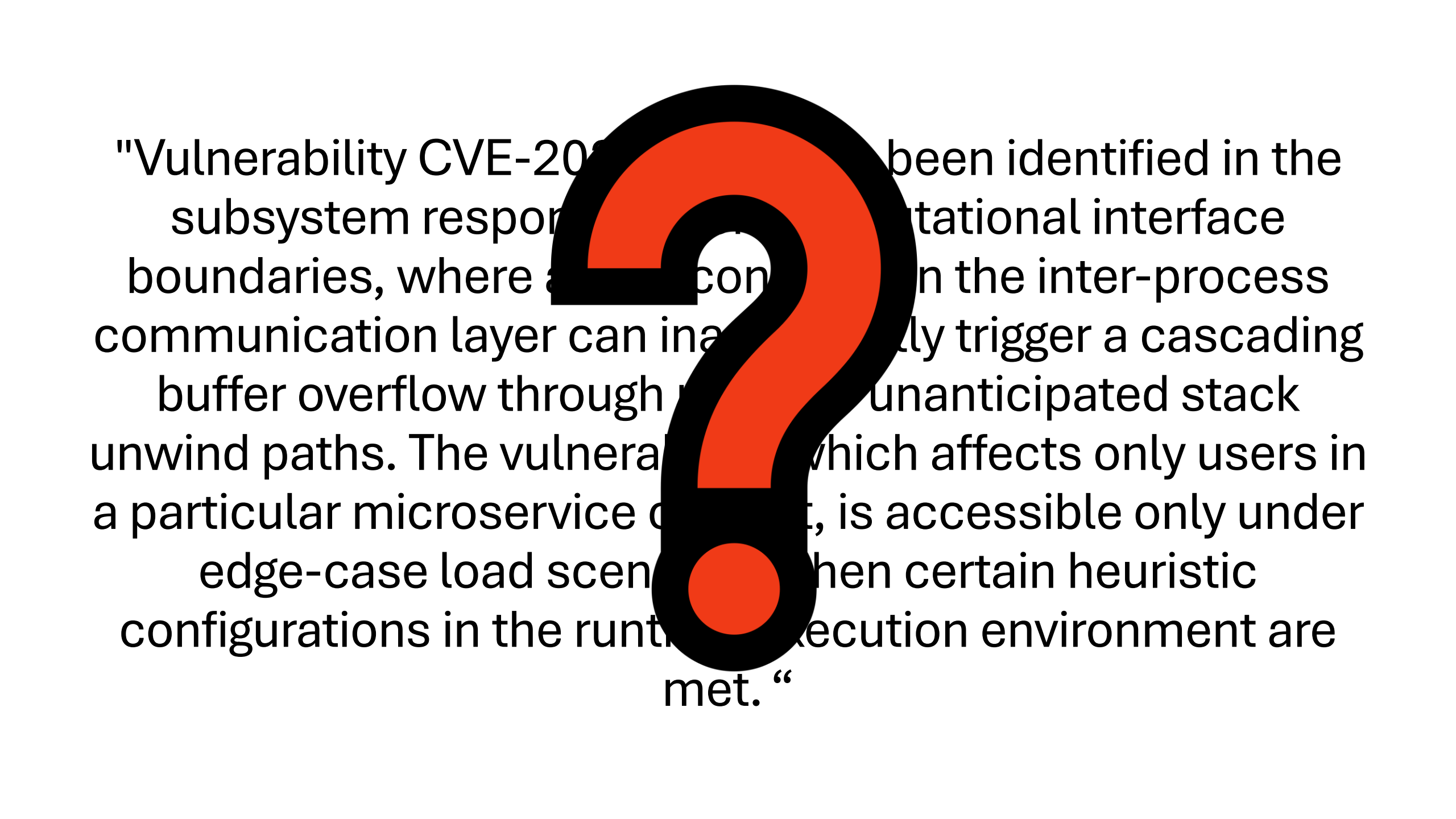
CHESS Brokerage Event at JIC


# Usability of Penetration Testing Reports

Katarína Galanská

"Vulnerability CVE-2023-XXXX has been identified in the subsystem responsible for computational interface boundaries, where a race condition in the inter-process communication layer can inadvertently trigger a cascading buffer overflow through multiple unanticipated stack unwind paths. The vulnerability, which affects only users in a particular microservice context, is accessible only under edge-case load scenarios when certain heuristic configurations in the runtime execution environment are met. “


"Vulnerability CVE-20
been identified in the
subsystem respon
tational interface
boundaries, where a
con
n the inter-process
communication layer can ina
ly trigger a cascading
buffer overflow through
unanticipated stack
unwind paths. The vulnera
which affects only users in
a particular microservice c
t, is accessible only under
edge-case load scen
hen certain heuristic
configurations in the runti
ecution environment are
met. “

- 🧐 **Confused Security**
- 💬 ***"What does this report even mean?"***
- 📄 **Dense text, unclear formatting**

- 🧐 **Confused Security**
- 💬 ***"What does this report even mean?"***
- 📄 **Dense text, unclear formatting**
- ⏳ **Time Passing...**
- 🔥 **Vulnerability Still Open!**
- ❌ **Risk Level Increasing**

| 🔍 Report Type | ❌ Confusing & Unclear |
| --- | --- |
| **Finding** | SQL Injection exists due to improper input validation. |
| **Technical Details** | |
| **Remediation** | |
| **Actionable Steps?** | |

| 🔍 Report Type | ❌ Confusing & Unclear | ✅ Clear & Actionable |
| --- | --- | --- |
| **Finding** | SQL Injection exists due to improper input validation. | **SQL Injection detected in /login.php (HIGH RISK). Attackers can bypass authentication.** |
| **Technical Details** | | |
| **Remediation** | | |
| **Actionable Steps?** | | |

| 🔍 Report Type | ❌ Confusing & Unclear | ✅ Clear & Actionable |
| --- | --- | --- |
| **Finding** | SQL Injection exists due to improper input validation. | **SQL Injection detected in /login.php (HIGH RISK). Attackers can bypass authentication.** |
| **Technical Details** | Affected Endpoint: /login.php, Payload Used: admin' -- | **Attack Scenario:** Hacker can inject admin' -- to log in as admin. |
| **Remediation** | Implement proper security controls. | **Fix:** Use prepared statements. **Example Code:** SELECT * FROM users WHERE username = ? AND password = ? |
| **Actionable Steps?** | ❌ No clear urgency or timeline. | ✅ Fix within **24 hours**, assigned to **Development Team**. |

# Goal

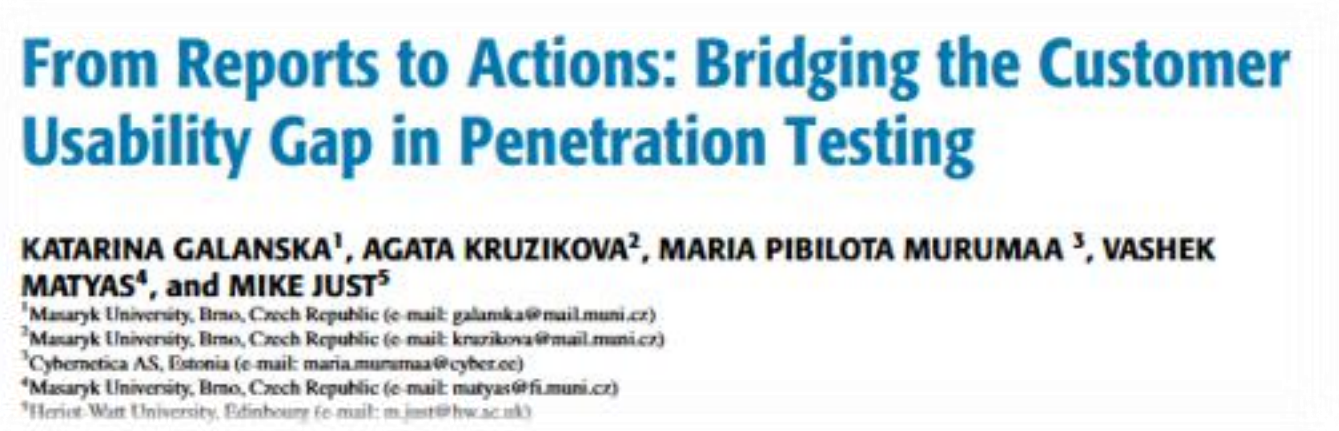
- Focus on making penetration testing reports more **usable, clear, and actionable** to help security teams **respond faster and fix vulnerabilities effectively.**

# Goal

- Focus on making penetration testing reports more **usable, clear, and actionable** to help security teams **respond faster and fix vulnerabilities effectively.**

If security reports are confusing, security doesn’t improve!

# Now and Next



From Reports to Actions: Bridging the Customer Usability Gap in Penetration Testing

KATARINA GALANSKA[1], AGATA KRUZIKOVA[2], MARIA PIBILOTA MURUMAA [3], VASHEK MATYAS[4], and MIKE JUST[5]

[1]Masaryk University, Brno, Czech Republic (e-mail: galanska@mail.muni.cz)
[2]Masaryk University, Brno, Czech Republic (e-mail: kruzikova@mail.muni.cz)
[3]Cybernetica AS, Estonia (e-mail: maria.murumaa@cyber.ee)
[4]Masaryk University, Brno, Czech Republic (e-mail: matyas@fi.muni.cz)
[5]Heriot-Watt University, Edinburgh (e-mail: m.just@hw.ac.uk)

🔍 Seeking Collaboration: Partnering with companies to conduct experiments involving professionals who work with penetration testing reports.

**E-mail**: galanska@mail.muni.cz