BLIND XSS

@adam_baldwin

^lift

Adam Baldwin

- Chief Security Officer at &yet
- Security Lead for ^Lift Security
- Also @liftsecurity & @nodesecurity

LET'S TALK BLIND XSS

- What is it?
- Using it in penetration tests
- Challenges
- xss.io

WTF IS BLIND XSS

XSS IS:

- Reflected
- Persistent (stored)
- DOM

BLIND XSS IS:

- Reflected
- **Persistent (stored)**
- DOM

IT'S A DIFFERENT CHALLENGE.

IT'S NOT LIKE BLIND SQLI WHERE YOU GET IMMEDIATE FEEDBACK.

YOU HAVE NO IDEA **WHERE** YOUR PAYLOAD'S GOING TO END UP.

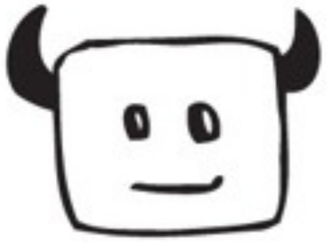
YOU DON'T EVEN KNOW WHETHER YOUR PAYLOAD WILL EXECUTE (OR WHEN!)

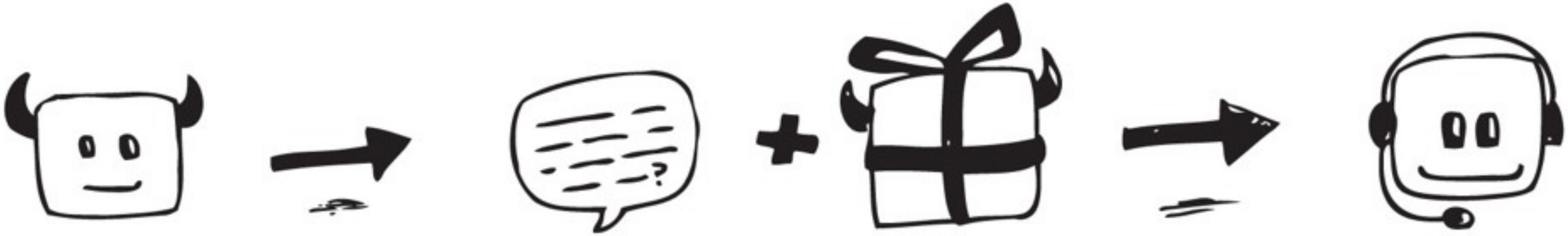
YOU MUST **THINK AHEAD** ABOUT WHAT YOU WANT TO ACCOMPLISH.

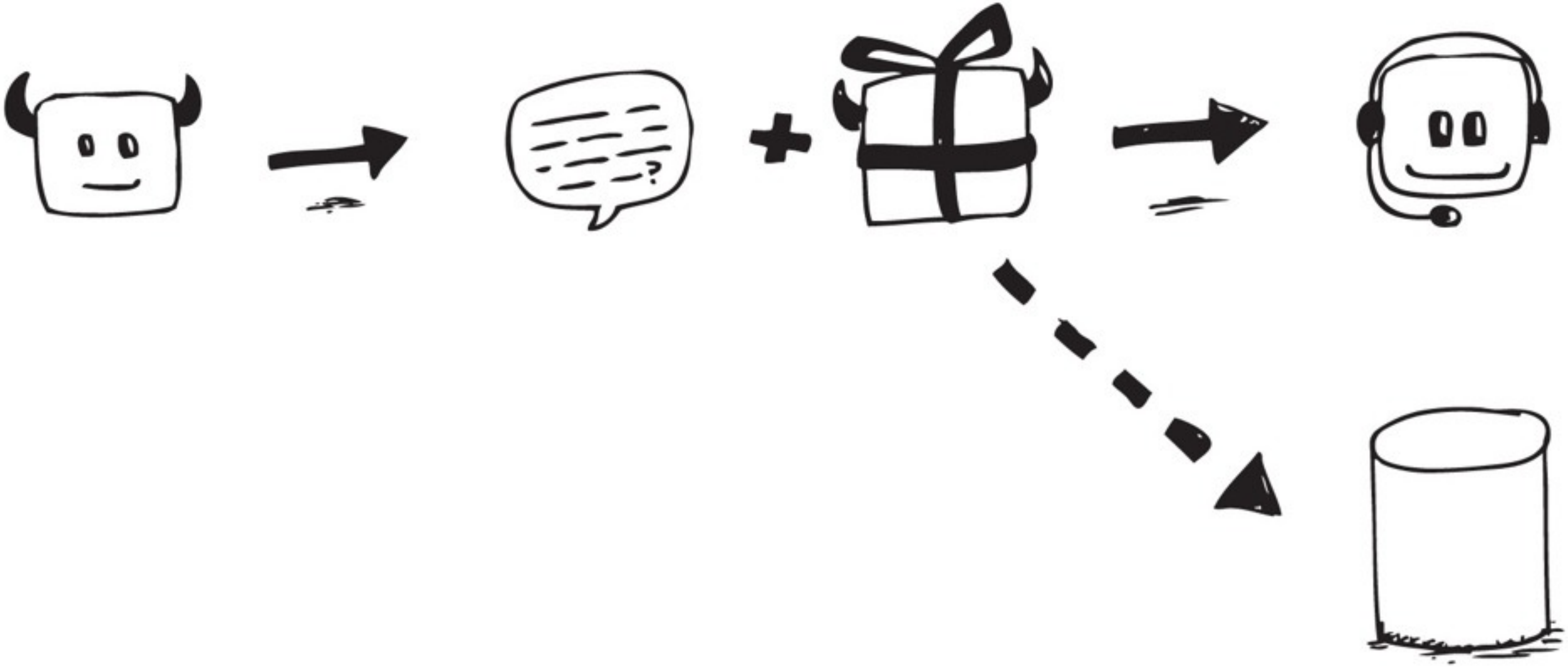
... AND YOU HAVE TO BE LISTENING.

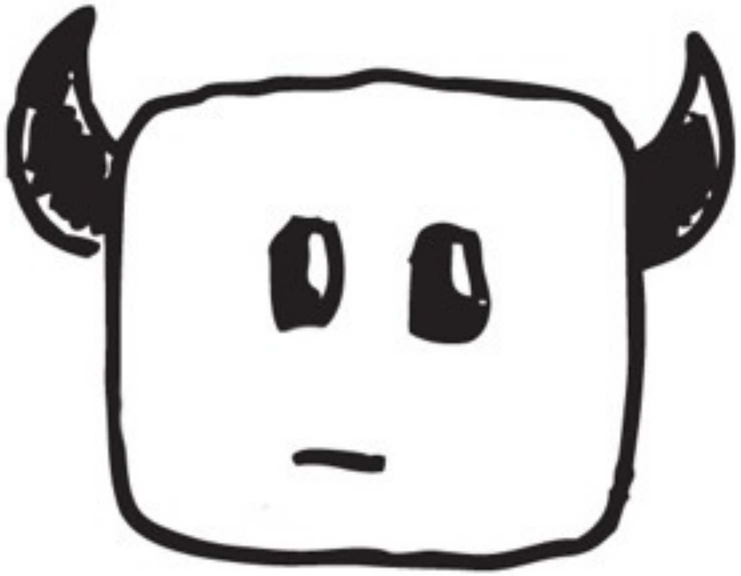
FOR EXAMPLE...

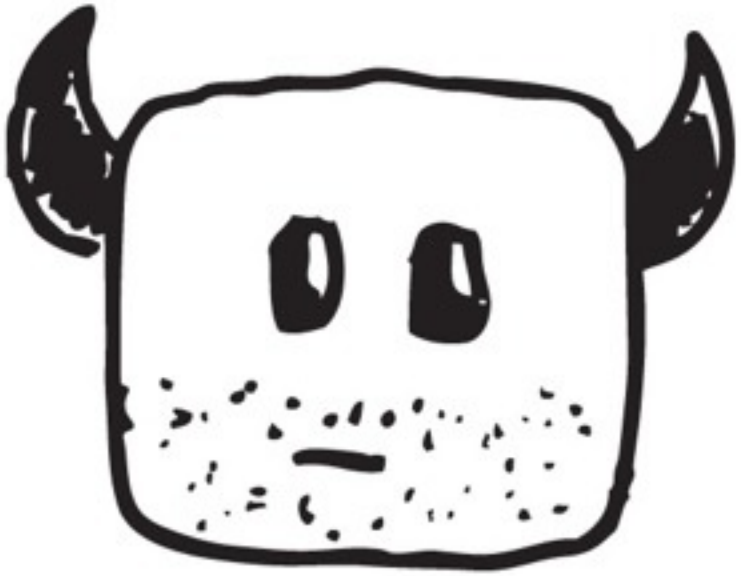
From a penetration test

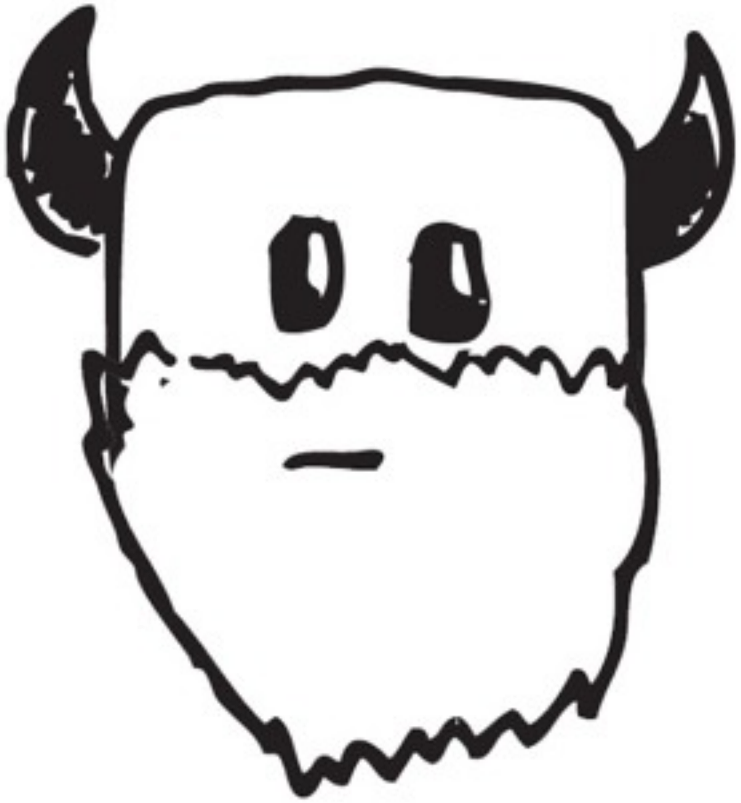




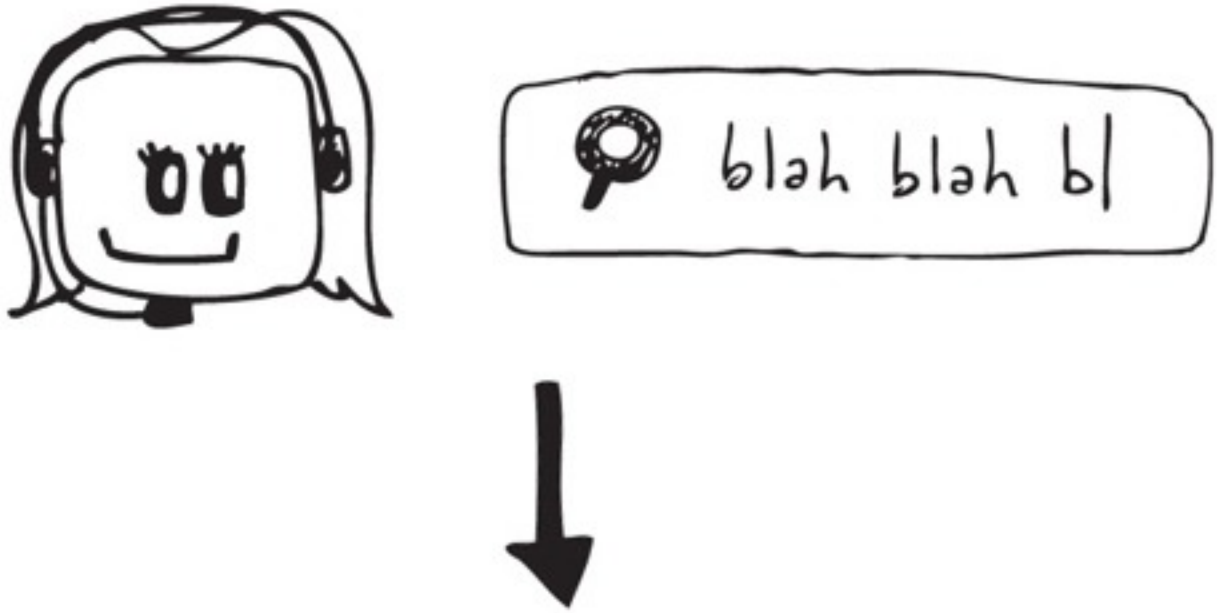


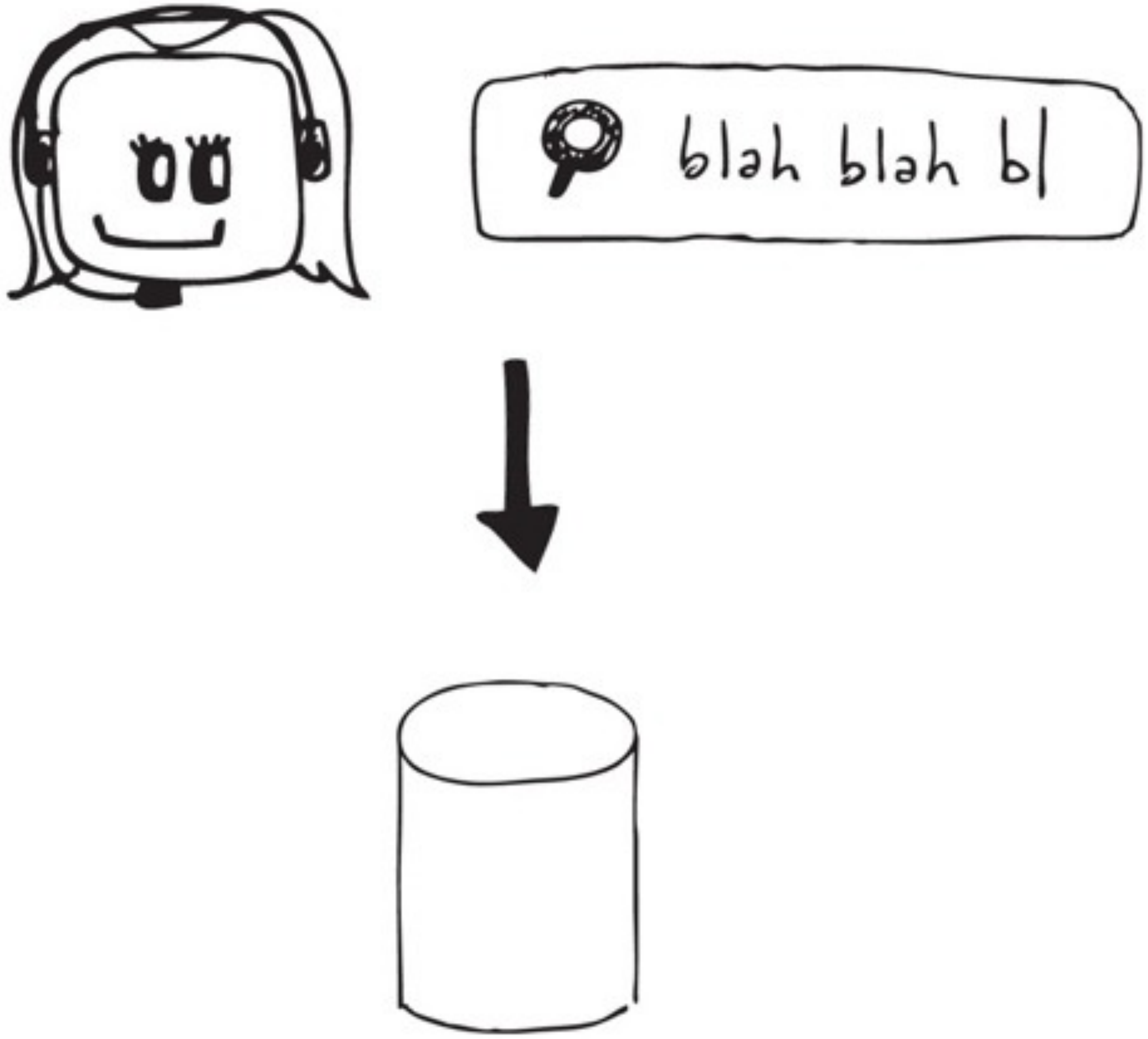


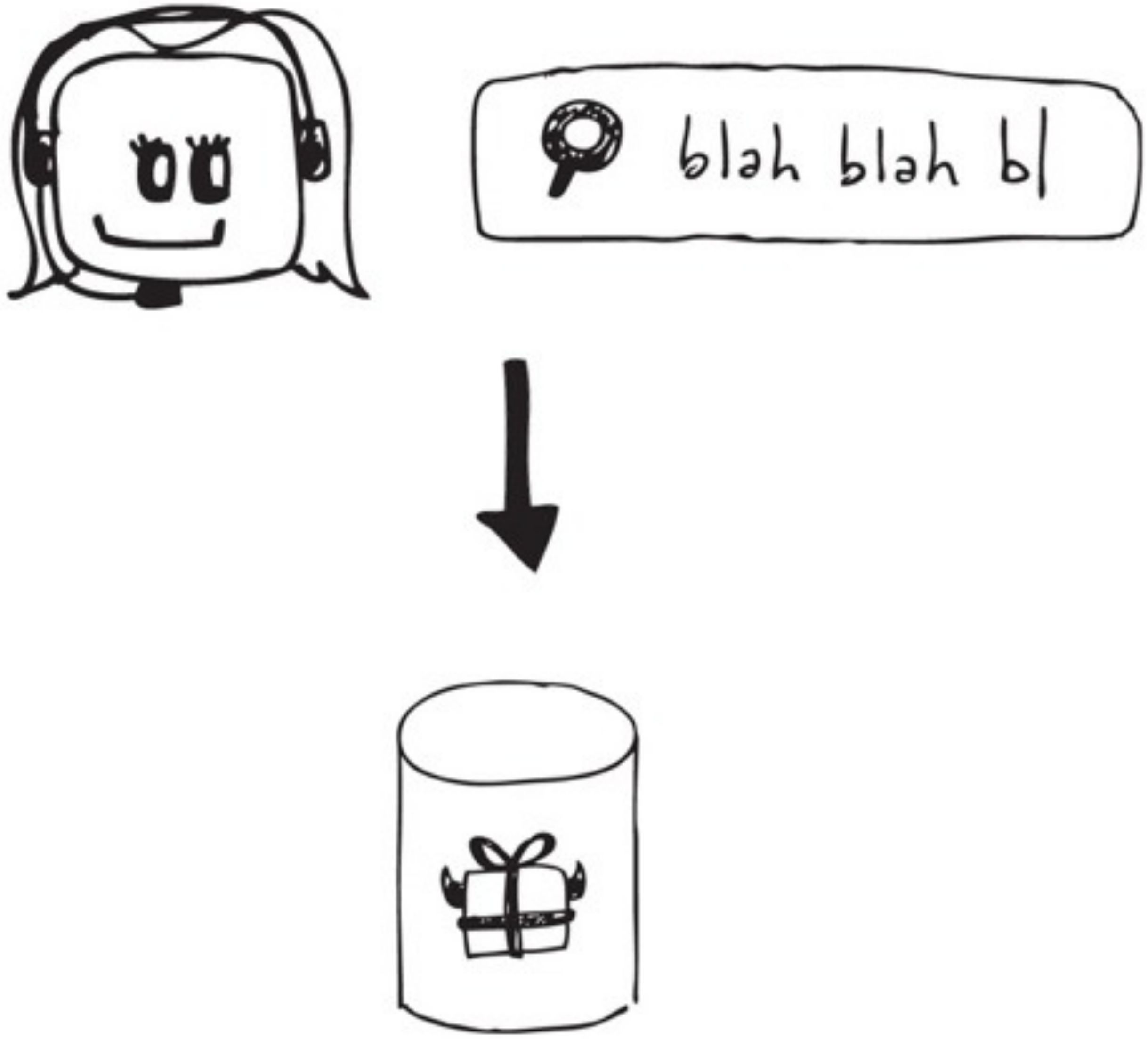


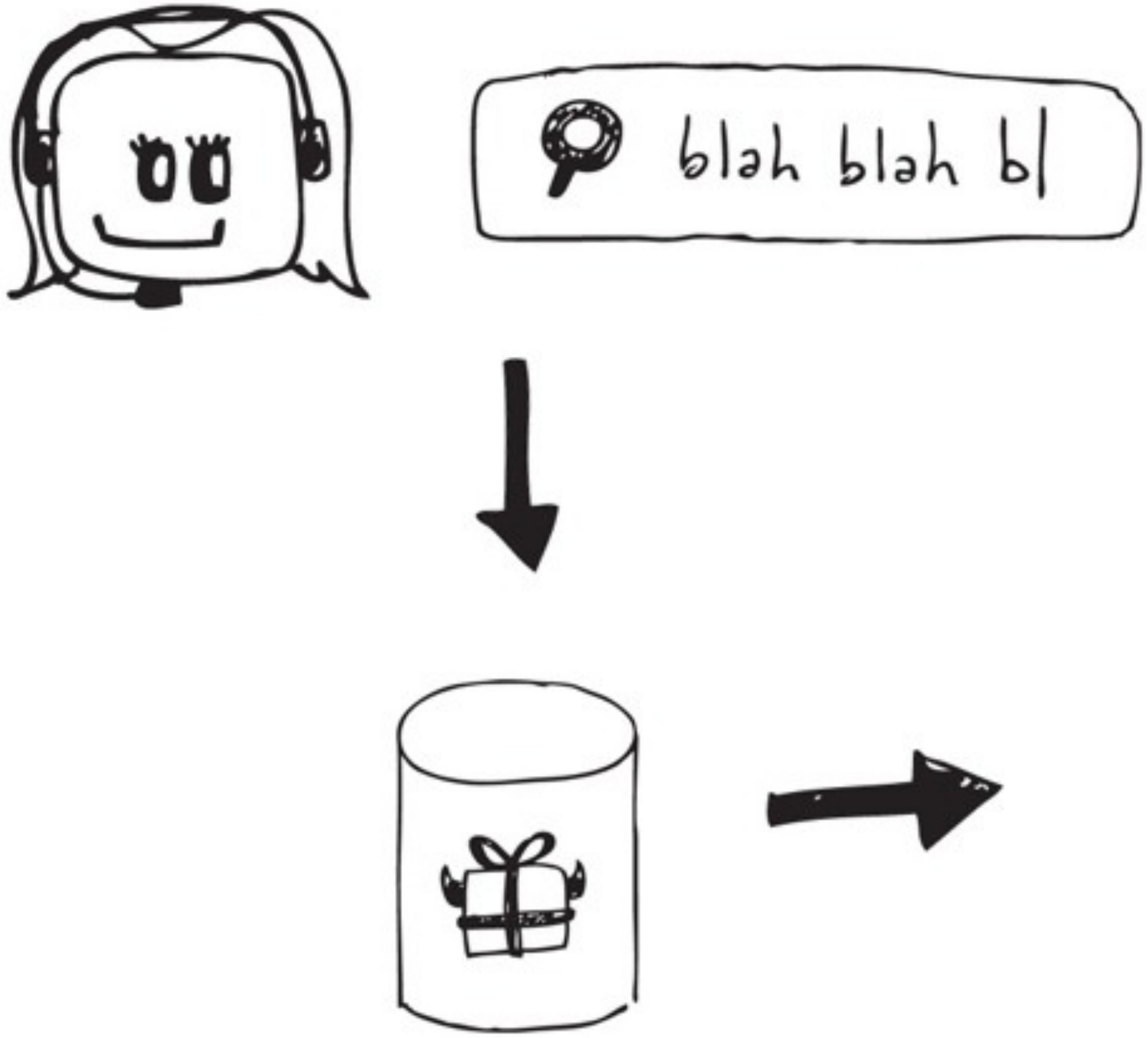


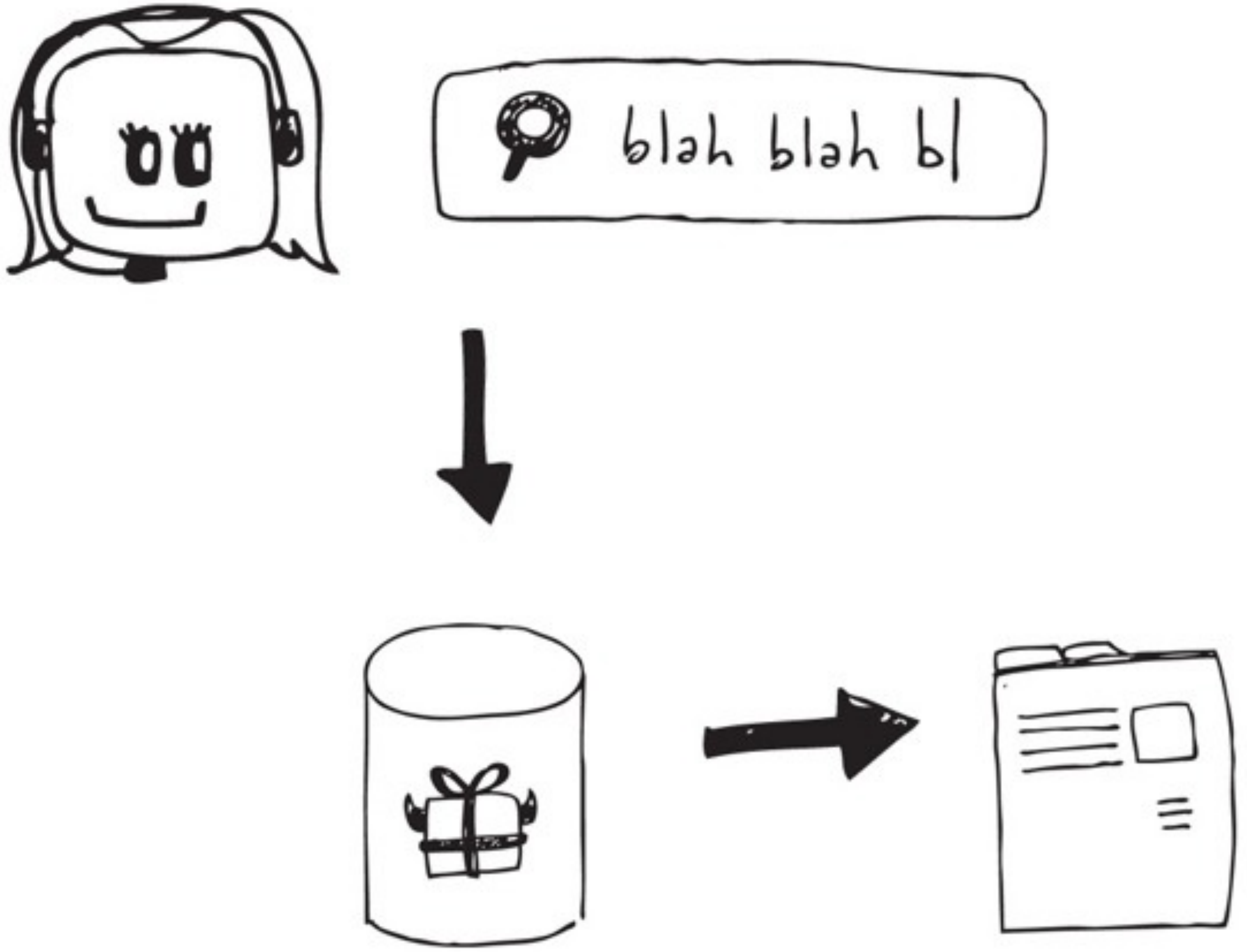
blah blah bl

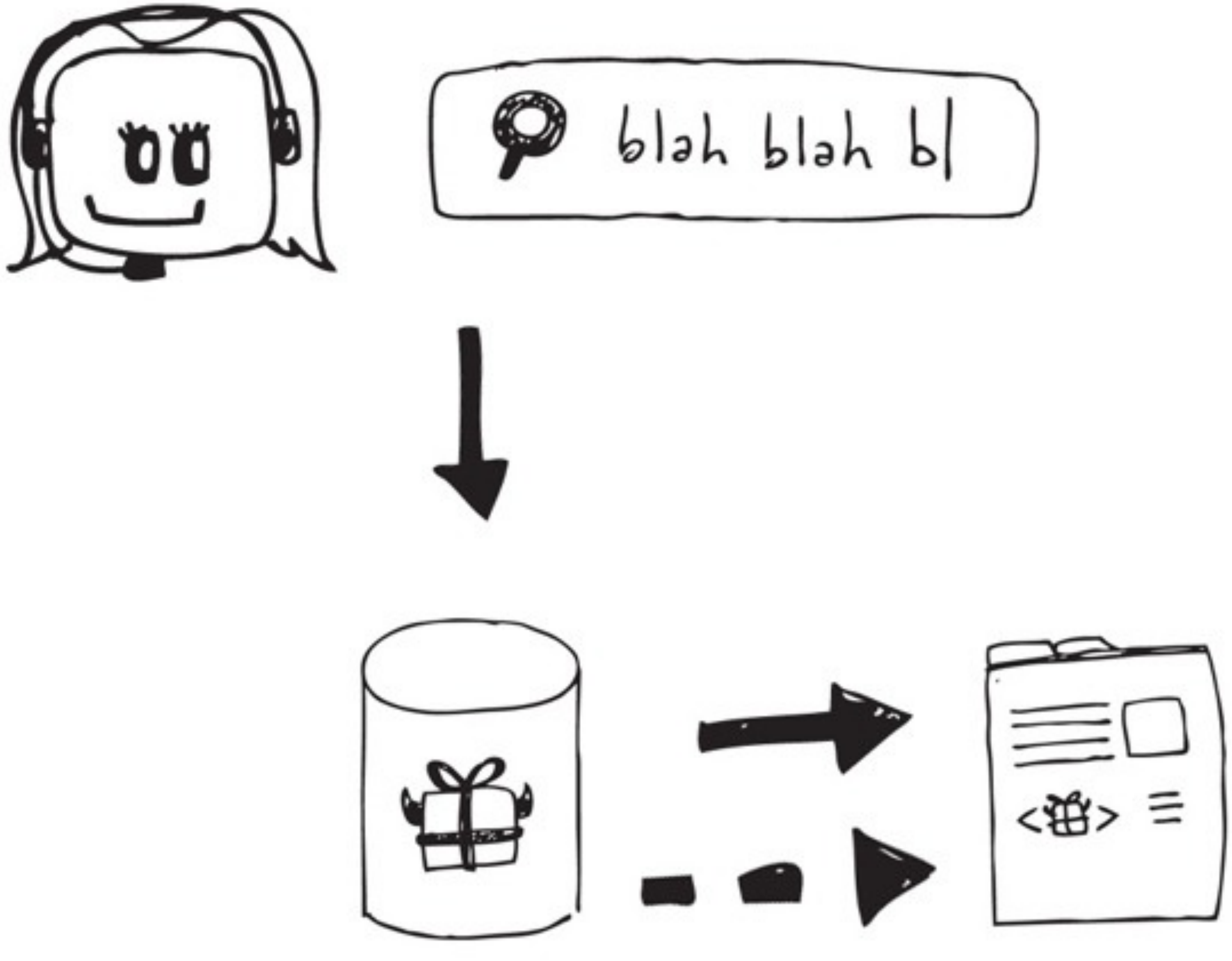

blah blah bl

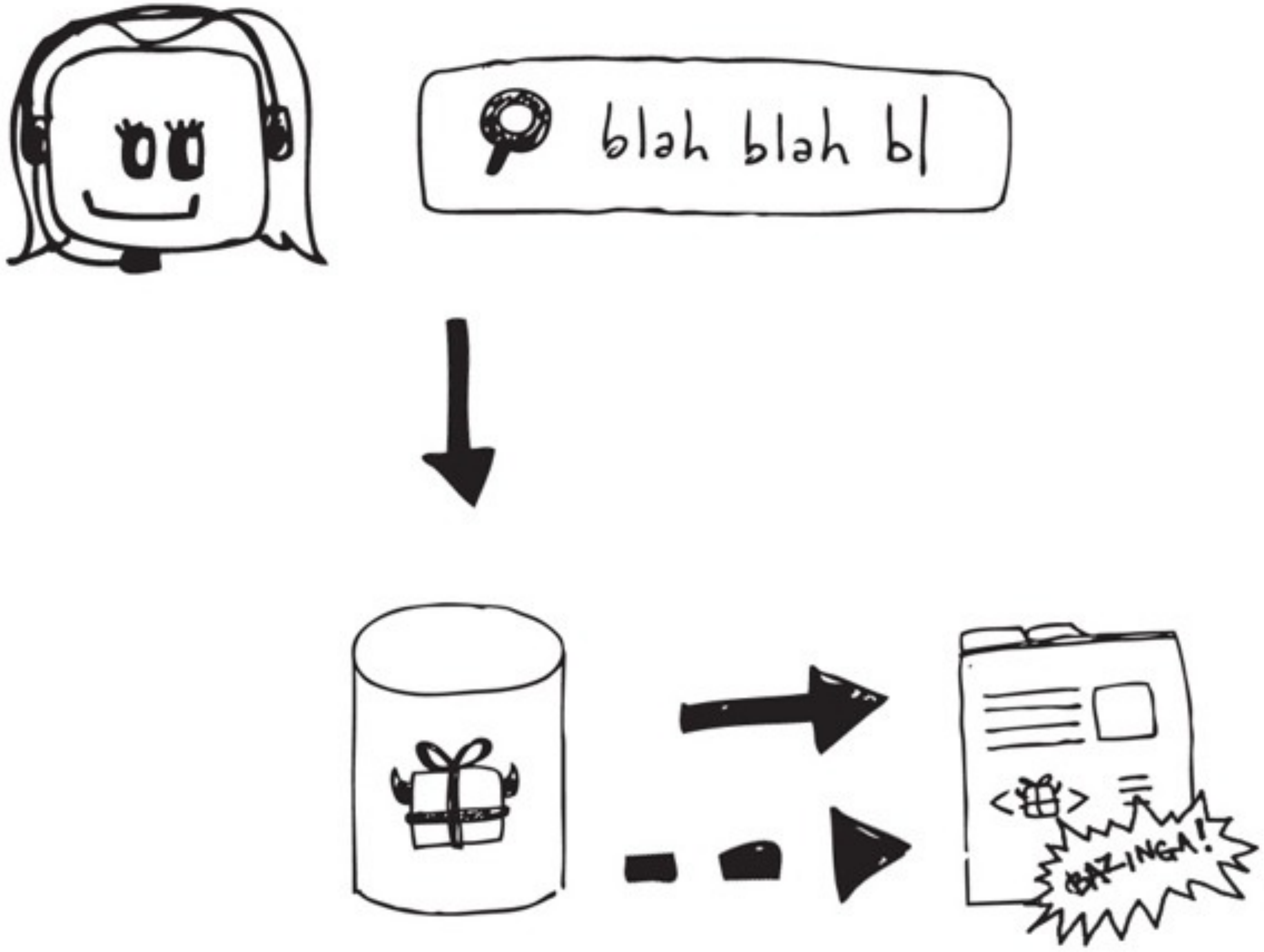

blah blah bl

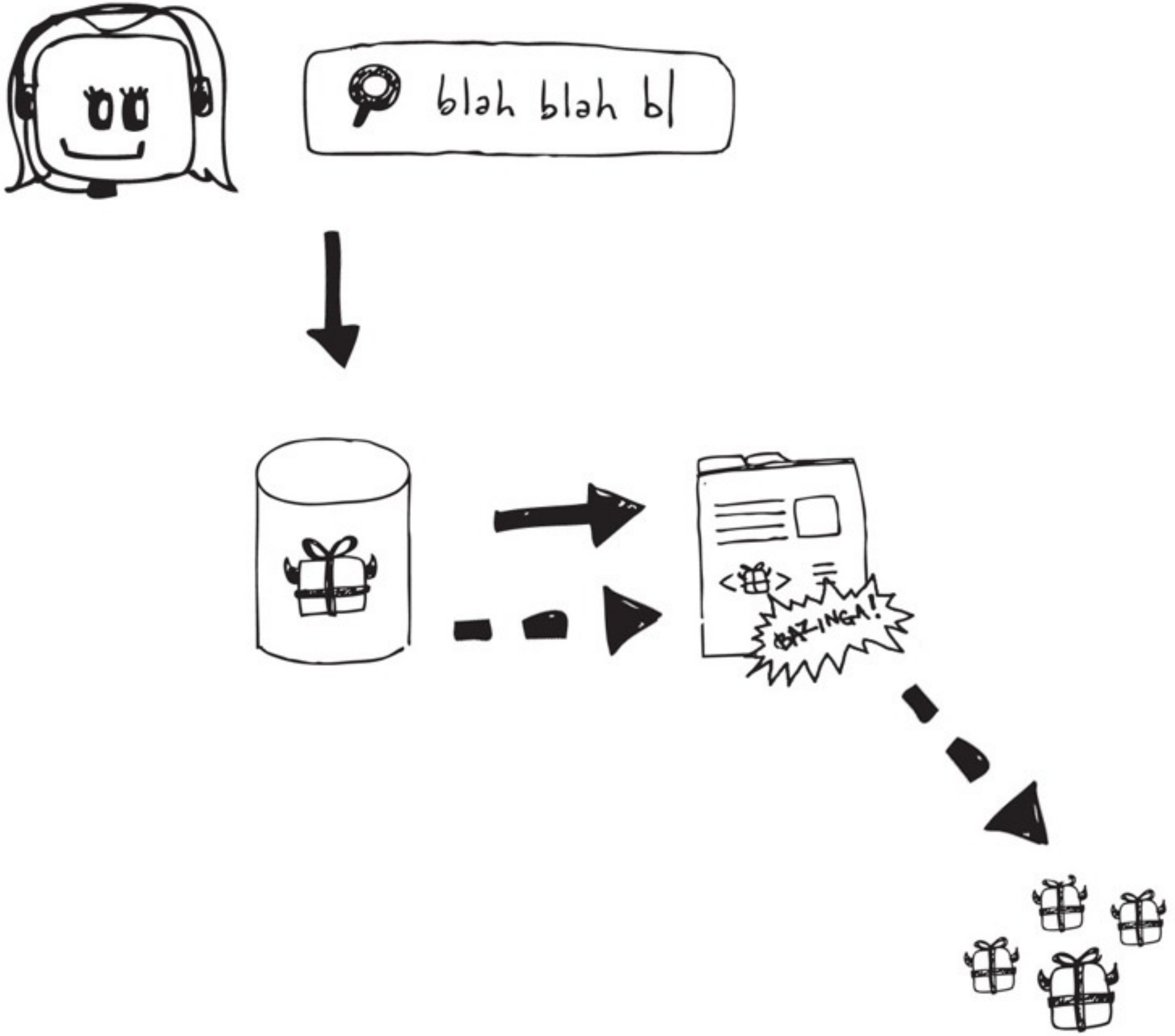

blah blah bl

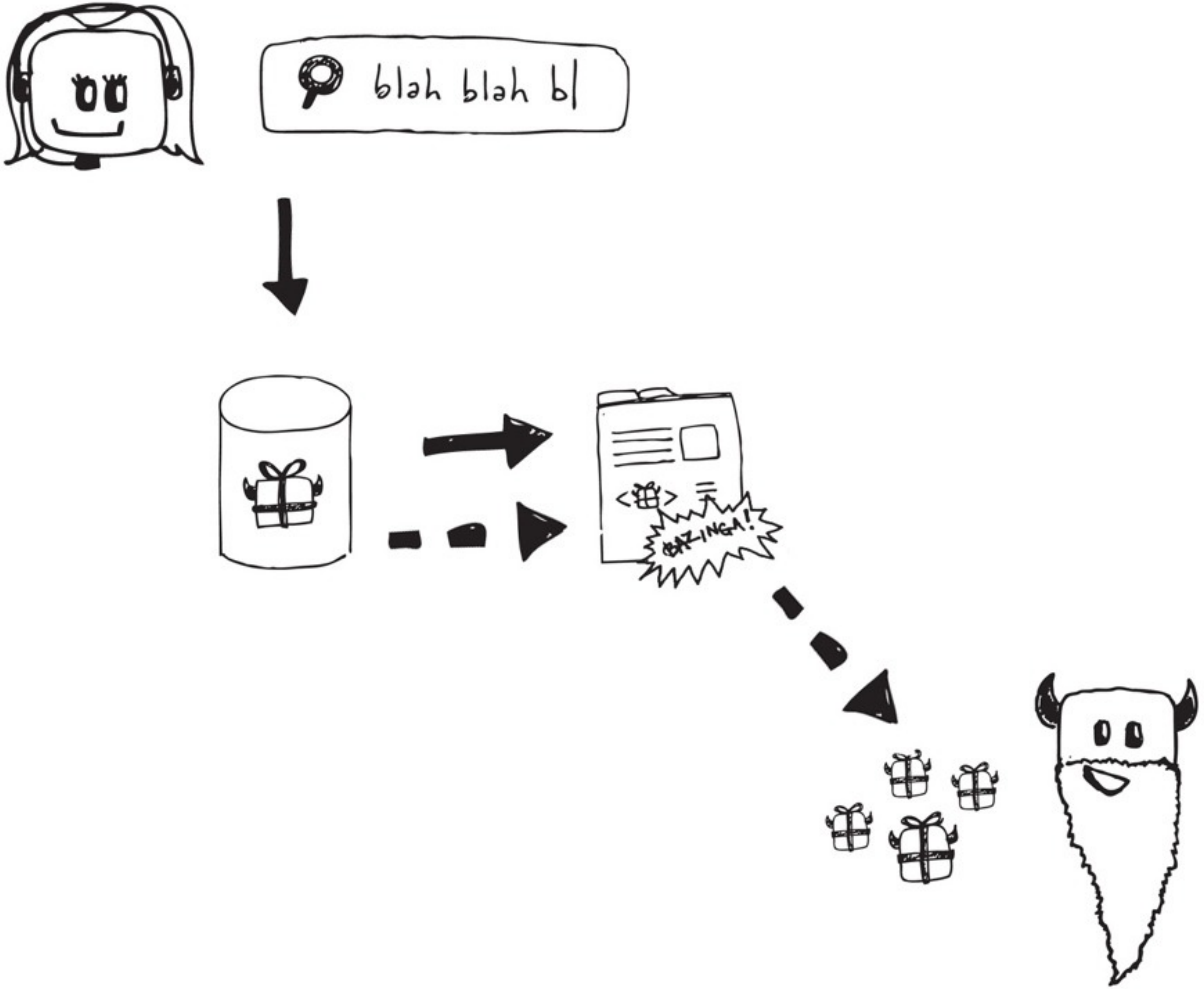

blah blah bl


blah blah bl


blah blah bl


blah blah bl
BAZINGA!


blah blah bl
BAZINGA!


blah blah bl
BAZINGA!

STEPS TO A SUCCESSFUL BLIND XSS EXPLOIT:

1. Carefully choose the right payload for the right situation.

STEPS TO A SUCCESSFUL BLIND XSS EXPLOIT:

1. Carefully choose the right payload for the right situation.
2. Get lucky!

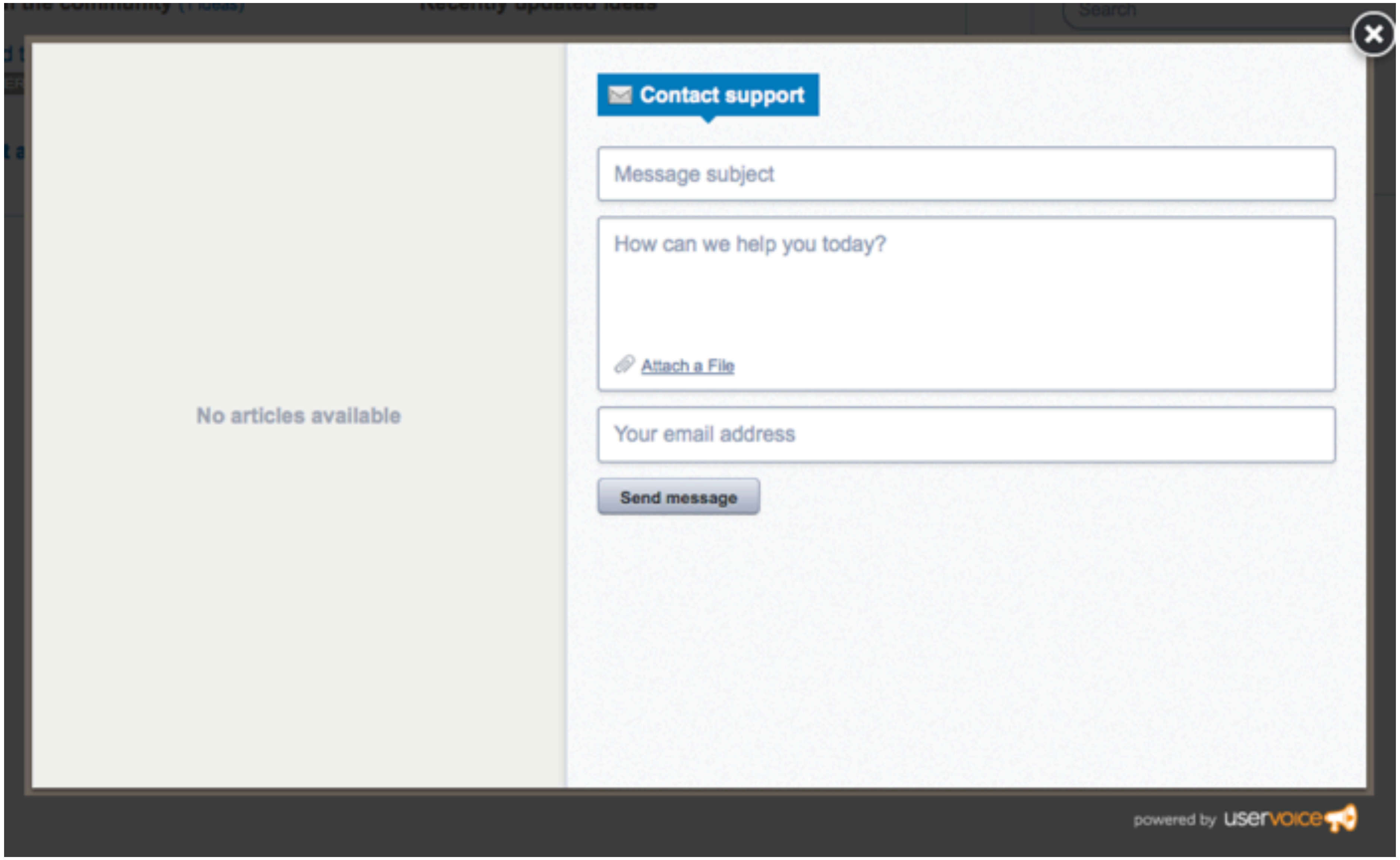
HTML5SEC.ORG

- Lots of payloads for various situations.
- ...but doing everything would be overkill.

PLAN YOUR PAYLOAD. HOW WILL THE APP USE YOUR DATA?

NICE TARGETS:

- log viewers
- exception handlers
- customer service apps (chats, tickets, forums, etc)
- anything moderated



No articles available

BLIND XSS MANAGEMENT

XSS.IO CAN HELP!

SIZE MATTERS... RIGHT?

- Sometimes you need all the character space you can get.
- No short-url GUID
- xss.io uses custom referrer-based redirects instead

EXPLOIT CREATOR

- Snippets for common tasks
- Quickly create and reference dynamic payloads

DEAD DROP BLIND XSS API AND MANAGER

(XSS.IO DEMO)

</PRESENTATION>

@adam_baldwin | @LiftSecurity

^lift