BLIND XSS

@adam_baldwin
HI, I’M ADAM BALDWIN
NOT THAT ADAM BALDWIN
THIS ADAM BALDWIN

- Chief Security Officer at &yet
- Security Lead for ^Lift Security
- @adam_baldwin + @liftsecurity
LET’S TALK BLIND XSS

- What is it?
- Using it in penetration tests
- Challenges
- xss.io
WTF IS BLIND XSS
WTF IS 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.
BLIND XSS IS
BLIND XSS IS CALL ME MAYBE?
FOR EXAMPLE...
From a recent penetration test
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!
• 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
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
BUT WAIT, THERE’S MORE
Unrelated but equally awesome
CSRF.IO
</PRESENTATION>

@adam_baldwin | @LiftSecurity