Adjusted attack strategy per tartget

BY UNCLE RAT

Agenda

- Why it matters
- Attacks per target
- What to avoid in a target
- What to look for in a target

Why it matters

Why it matters

- Same strategy on all targets = guaranteed fail
- We need to overcome and adept
- Every target is different
- More precise testing is less time waste

Attacks per target

Attacks per target – Newspaper

- Very little functionality to test
- Login functionality
  - Including forgot password
  - Including XXE for account pictures and possibly IDOR
- Paywall bypass

Attacks per target – Webshop

- Somewhat more functionality but requires investment
  - Buying an item
  - Returning an item
- Login functionality
  - Including forgot password
  - Including XXE for account pictures
  - Including IDOR
- XSS is no use here, it's almost always self XSS
  - Maybe you can chain it? CSRF > XSS?

Attacks per target – Blog or similar

- XSS but keep your testing to private objects where possibe
- Login functionality
  - Including forgot password
  - Including XXE for account pictures
  - Including IDOR

Attacks per target – B2B invoicing app

- You get or can create different access level users
  - Broken access control
- IDOR within 1 company
- IDOR between company
- Login functionality
  - Including forgot password
  - Including XXE for account pictures
- All the available functionality testing for business logic flaws

Attacks per target – Bank

- Very hardened
- Focus on the business logic flaws
  - Money transfers
  - Fraud checks
  - Getting a loan you should not get
  - …
- IDORs
- XSS is almost always useless here, almost always self XSS

Attacks per target – And many more...

- Casino websites
  - Business logic, focus on getting free plays or free money
- Wide scope targets
  - See wide scope methodology
- IoT
  - Focus on the api interaction and IDORs
- Booking websites
  - Focus on finding bookings with personal info of other people
- E-health platforms
  - Focus on personal information of other people

What to avoid in a target

What to avoid in a target

What to avoid in a target

- High payouts
- Static websites
- Websites with little functionality like newspapers
- Very hardened targets such as banks
- Harder technologies like websockets
  - Learn the basics first
- Booking websites, they are usually more advanced
- Targets that don't give you credentials and don't let you make them

What to look for in a target

What to avoid in a target

What to avoid in a target

- Medior to VDP payouts
- very dynamic websites
- Websites with lots of functionality like B2B programs
- Look for the less secure tech like php
- Simple websites with simple tech like sequential id's
- Targets that do give you credentials or let you make them