Today’s Topics

- Sessions
  - Why do we need them?
  - What weaknesses can attacker’s take advantage of?
- Cross-site Scripting
  - Conceptually, what is it?
  - What can an attacker do with it?
A World w/o Sessions

get /control_panel

Please login
A World w/o Sessions

send
/login

data from form:
user name = john
password = money$

Welcome John!
A World w/o Sessions

get
/control_panel

Please login
Example with Sessions

get
/control_panel

session id: TH2S234S

Please login
Example with Sessions

To send:

/session

Data from form:

user name = john
password = money$
Example with Sessions

Hi John.

Here’s your control panel session id: TH2S234S
Sessions Shouldn’t Be

• Predictable
• Settable (session fixation)
Sessions Shouldn’t Be

- Predictable
- Settable (session fixation)
Predictable Sessions

Session ID is one digit

send /login

data from form:
user name = john
password = money$

Welcome John!

session id: 3

Victim
Predictable Sessions

session id: 3

Victim
Predictable Sessions

session id: 3
Victim

get /control_panel

session id: 1
Attacker

Please login
Predictable Sessions

session id: 3
Victim

session id: 2
get /control_panel
Attacker

Please login
Victim

session id: 3

get /control_panel

Attacker

Hi John.

Hi John.

Here’s your control panel
Sessions Shouldn’t Be

- Predictable
- Settable (session fixation)
Session Fixation
Session Fixation

/go here
/login?SID=I_KNOW
Session Fixation

/go here
/login?SID=I_KNOW

get
/login?SID=I_KNOW
Session Fixation

/go here
/login?SID=I_KNOW

get
/login?SID=I_KNOW

session id: I_KNOW
Please login
Session Fixation

session id: I_KNOW
Session Fixation

Send /login

Data from form:
user name = john
password = money$

Session id: I_KNOW
Session Fixation

send /login

data from form:
user name = john
password = money$

Welcome John!

session id: I_KNOW
Session Fixation

session id: I_KNOW
Session Fixation

session id: I_KNOW

get /control_panel

session id: I_KNOW

Hi John.
Here’s your control panel
Cross Site Scripting (XSS)

• What is it?
  • Attacker is able to place his own code on a website

• Why does it happen?
  • Website fails to sanitize data that attacker sends to it
Cross Site Scripting (XSS)

- XSS Attack
  - Attacker places JavaScript on a website
  - Website visitors unknowingly run the JavaScript
  - Attacker has control of website visitor
    - he can force the visitor to perform an action on the website
    - he can steal Session IDs (and thus become the visitor)
XSS Example: A Blog

/submit_comment is vulnerable to XSS
XSS Example: A Blog

/submit_comment is vulnerable to XSS

submit

/submit_comment

XSS Payload

submit

Payload

XSS

Payload
XSS Example: A Blog

/submit_comment is vulnerable to XSS

submit

/XSS Payload

Thank you for your comment
XSS Example: A Blog

/view_comments contains XSS Payload
XSS Example: A Blog

/view_comments contains XSS Payload

session id: TH2S234S
XSS Example: A Blog

/view_comments contains XSS Payload

get /view_comments

session id: TH2S234S
XSS Example: A Blog

/view_comments contains XSS Payload

get /view_comments

session id: TH2S234S

Here are the comments
XSS Example: A Blog

/view_comments contains XSS Payload

session id: TH2S234S

session id: TH2S234S
XSS Example: A Blog

attacker knows victim’s session id

get /control_panel

session id: TH2S234S
XSS Example: A Blog

attacker knows victim’s session id

Hi John.

Here’s your control panel

session id: TH2S234S