Session, Cookie, and Web Security - Demo Resources

Building Modern Web Applications - CPEN322

Karthik Pattabiraman
Kumseok Jung

Part 1 - Using a Cookie

CPEN322 Bank App is at: http://3.96.141.132:5000

Your username: `YOUR_GITHUB_USERNAME`

Your password: `YOUR_STUDENT_NUMBER`

Vicky's Session Cookie: `db7068de02ff8861c1a1432b651ef0c2`

Part 2 - Non-persistent XSS Attack

CPEN322 Online Shop is at: http://3.96.141.132:3000

Your personal storage is at: http://3.96.141.132:8080/USERNAME

To push data to your storage, use:

http://3.96.141.132:8080/USERNAME/push?access=StudentNumber&text=DATA

To access your storage, include your student number in the query string:

http://3.96.141.132:8080/USERNAME?access=StudentNumber

* *You'll need to URL-escape the ampersand (&) character to %26 when you embed it as part of the attack string.*

Part 2 - Persistent XSS Attack

CPEN322 Instant Messenger App is at: http://3.96.141.132:4000

Your username: `YOUR_GITHUB_USERNAME`

Your password: `YOUR_STUDENT_NUMBER`

Your personal storage is at: http://3.96.141.132:8080/USERNAME

To push data to your storage, use:

http://3.96.141.132:8080/USERNAME/push?access=StudentNumber&text=DATA

To access your storage, include your student number in the query string:

http://3.96.141.132:8080/USERNAME?access=StudentNumber

Part 3 - XSRF Attack

CPEN322 Bank App is at: http://3.96.141.132:5000

CPEN322 Instant Messenger App is at: http://3.96.141.132:4000

Your username: `YOUR_GITHUB_USERNAME`

Your password: `YOUR_STUDENT_NUMBER`

To create your malicious form, go to: http://3.96.141.132:8080/USERNAME/form/edit

To view your malicious form, go to: http://3.96.141.132:8080/USERNAME/form