

# Web Exercises

## Part 1: XSS

**Barton P. Miller**

Computer Sciences Department  
University of Wisconsin

[bart@cs.wisc.edu](mailto:bart@cs.wisc.edu)

**Elisa Heymann**

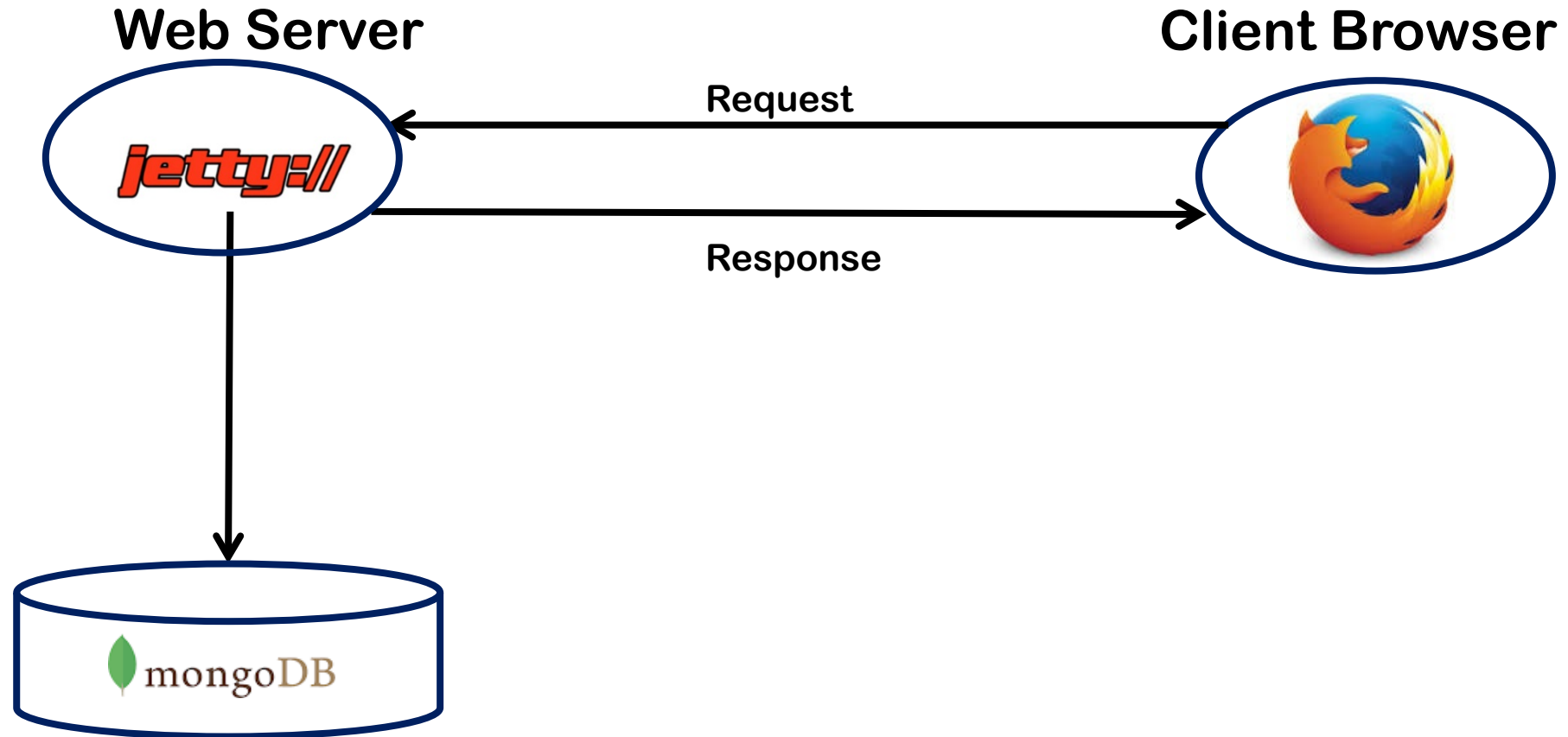
Computer Sciences Department  
University of Wisconsin  
Universitat Autònoma de Barcelona

[elisa@cs.wisc.edu](mailto:elisa@cs.wisc.edu)

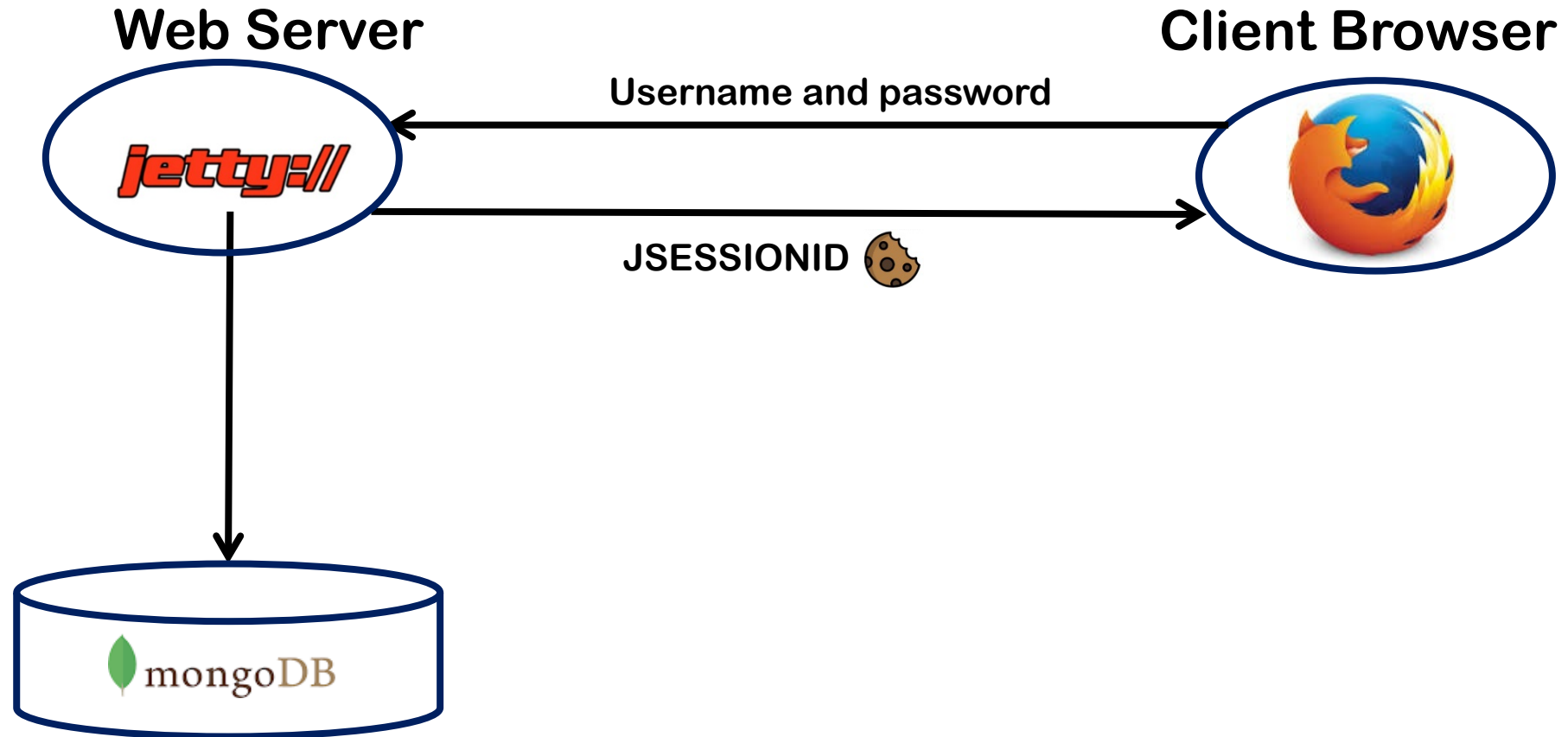
# WisClick. Our Web Application

- **A simple game.**
  - Players click on a button to earn credits.
  - Users can manage their profiles.
  - Users can transfer (some of) their credits to others.
  - There is a top five ranking.
  - Users can view other users' page through the top five ranking.
- **Vulnerable to web attacks.**
- **Exploit those vulnerabilities.**

# WisClick



# WisClick



# WisClick. Our web application

You will use two accounts:

username: **attacker**

password: **theattacker**

username: **victim**

password: **thevictim**

To reset the database at anytime run:

```
cd ~/Web_Attack/src  
mongo ResetMongo.js
```

# Run WisClick

**On a console run the web server:**

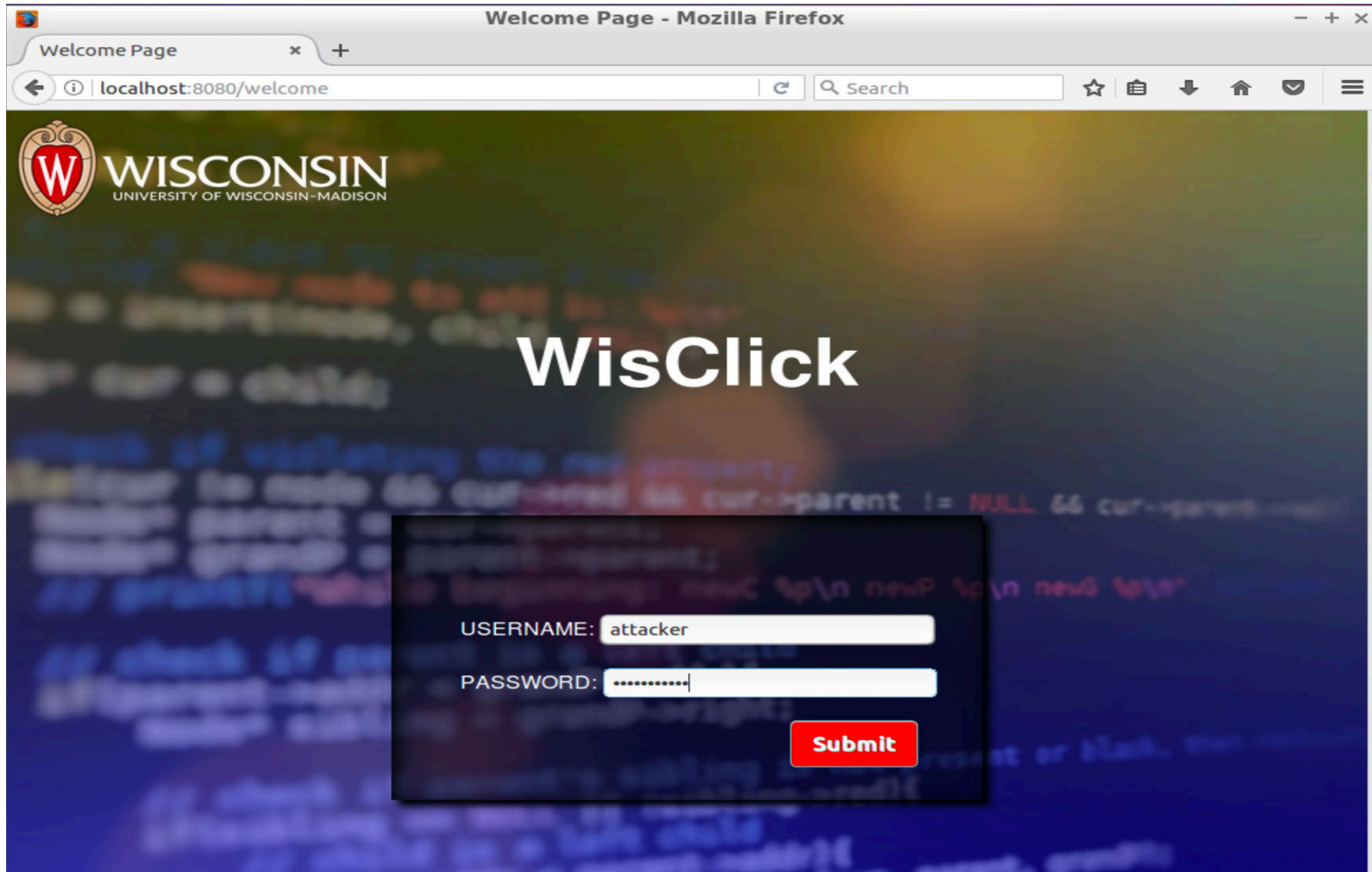
```
cd Web_Attack  
ant  
cd build/classes  
./run.sh
```

**On your web browser go to:**

```
http://localhost:8080/welcome
```

**Get familiar with the application:**

# Run WisClick

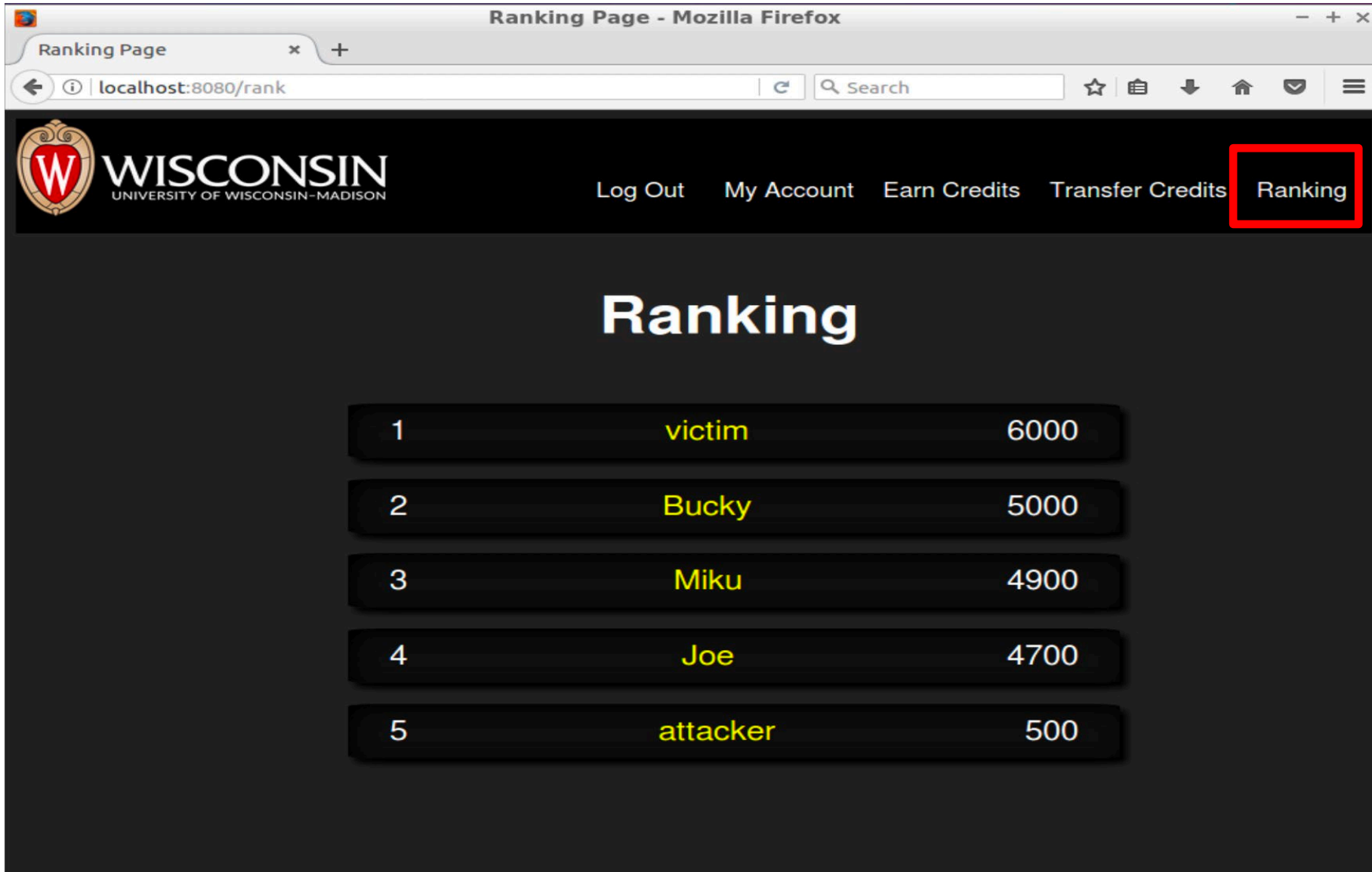


# Run WisClick

The screenshot shows a Mozilla Firefox browser window titled "Account Page - Mozilla Firefox". The address bar displays "localhost:8080/account". The page header features the University of Wisconsin-Madison logo and navigation links: "Log Out", "My Account", "Earn Credits", "Transfer Credits", and "Ranking". The main content area has a dark background with the text "Welcome to attacker 's Page!" in large white font. Below this, there are two dark rectangular boxes. The first box is titled "My Credits" and shows "500 Credits" in red text. The second box is titled "My Profile" and has an "Edit" button in the bottom right corner.



# Run WisClick



Ranking Page - Mozilla Firefox

Ranking Page

localhost:8080/rank

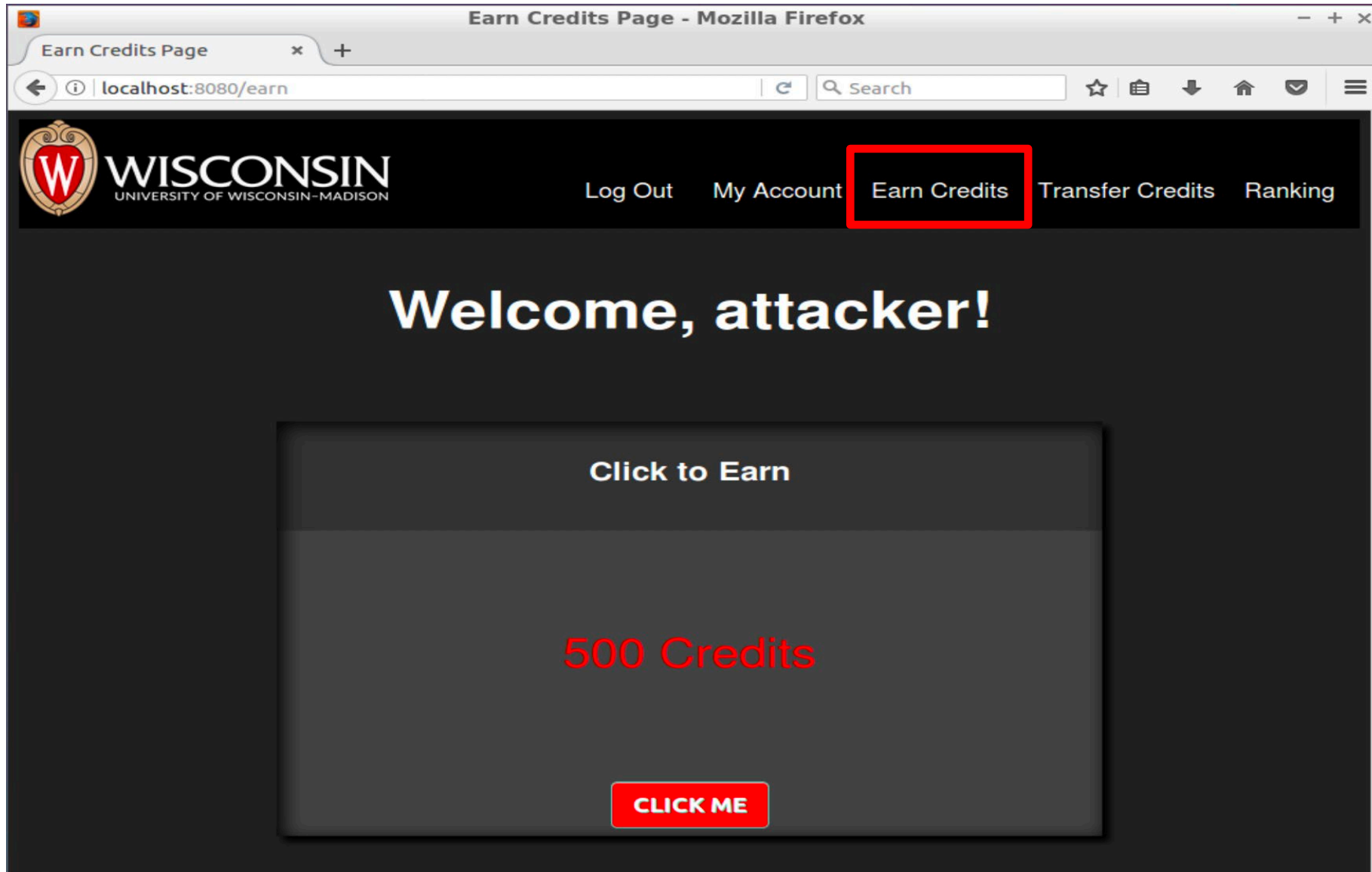
WISCONSIN UNIVERSITY OF WISCONSIN-MADISON

Log Out My Account Earn Credits Transfer Credits **Ranking**

## Ranking

1	victim	6000
2	Bucky	5000
3	Miku	4900
4	Joe	4700
5	attacker	500

# Run WisClick



# Run WisClick

The screenshot shows a web browser window titled "Transfer Page - Mozilla Firefox" with the address bar displaying "localhost:8080/transfer". The page header features the University of Wisconsin-Madison logo and navigation links: "Log Out", "My Account", "Earn Credits", "Transfer Credits" (highlighted with a red box), and "Ranking". The main content area is titled "Transfer Your Credits" and contains a form with the following elements:

- A message: "Your Credits: 500" in red text.
- A "To:" label followed by a white input field.
- A "Points:" label followed by a white input field.
- A red "Submit" button.

# WisClick Vulnerabilities

1. **Cross-Site Scripting (XSS).**
2. **Cross-Site Request Forgery (CSRF).**
3. **Extracting Credentials and using them.**

# 1. Cross-Site Scripting (XSS)

## A. Check if WisClick is vulnerable to XSS.

- Try to pop up an alert window for the victim.
- Find the attack surface for that.
- Open a **New Private Window** and log in as the victim to verify the attack.

# 1. Cross-Site Scripting (XSS)

Sessions are handled with session ids stored in cookies.

## **B. Use XSS to get the victim's session id cookie.**

- Same attack surface as before.
- Note that for that it's the victim viewing their own session id.

# Web Exercises

## Part 1: XSS

**Barton P. Miller**

Computer Sciences Department  
University of Wisconsin

[bart@cs.wisc.edu](mailto:bart@cs.wisc.edu)

**Elisa Heymann**

Computer Sciences Department  
University of Wisconsin  
Universitat Autònoma de Barcelona

[elisa@cs.wisc.edu](mailto:elisa@cs.wisc.edu)