

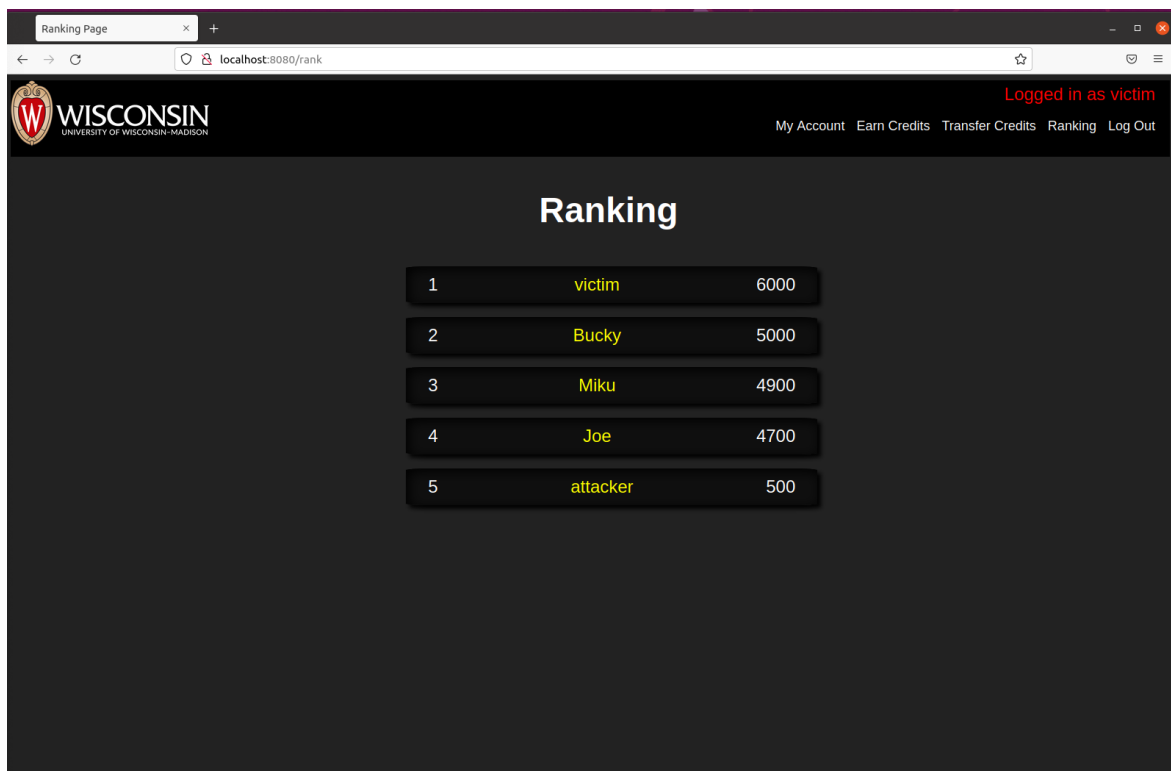
CS 542 – Introduction to Software Security

Exercise on Tampering with ZAP

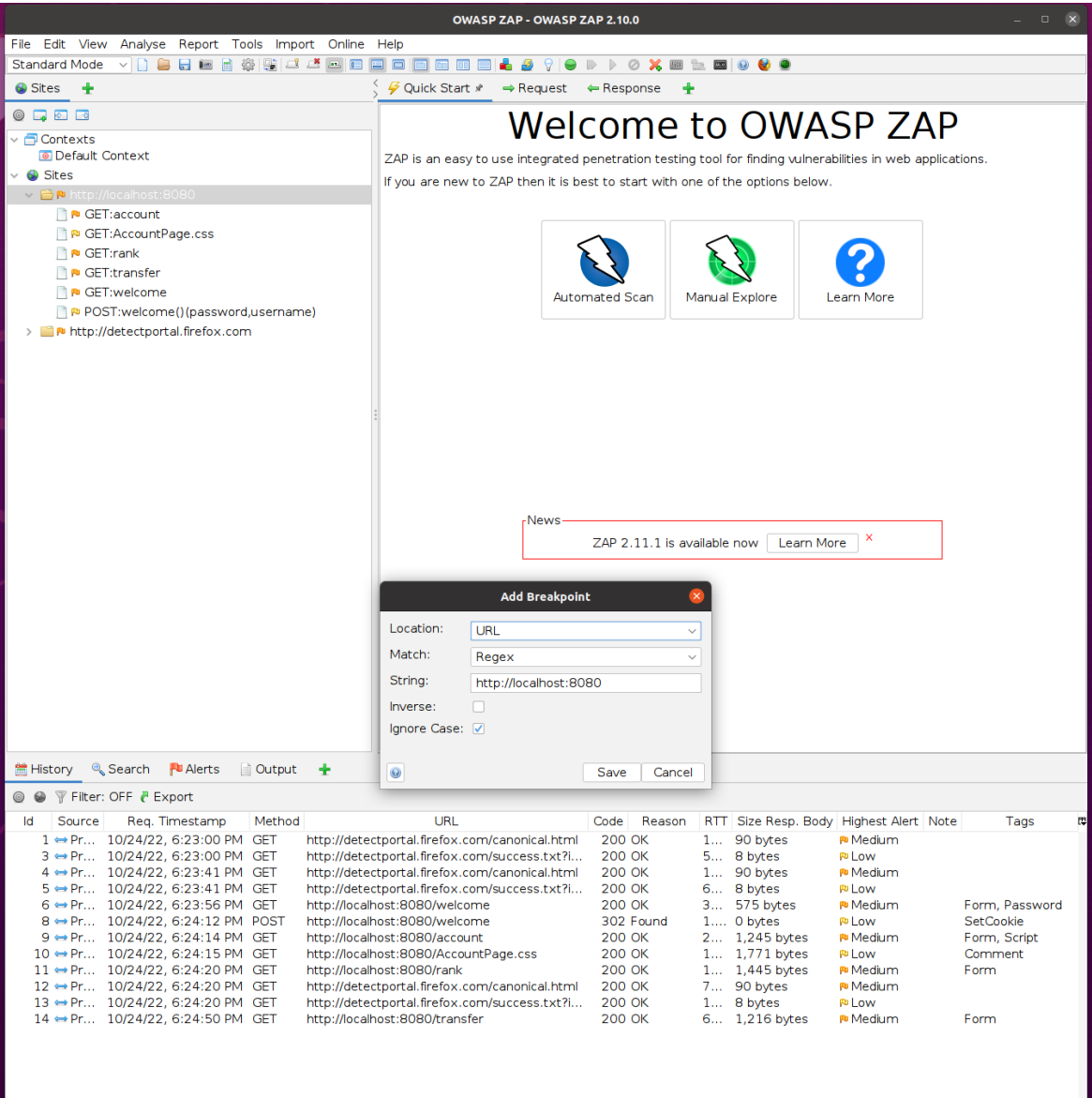
Binhao Chen (bchen276@wisc.edu), Steven Yang (yang558@wisc.edu)

Due: October 25 at 2:30pm.

- 1 A screenshot showing the attackers and victim's credits, on the ranking page, before the attack.



2 A screenshot showing the modified request for the attack.



OWASP ZAP - OWASP ZAP 2.10.0

File Edit View Analyse Report Tools Import Online Help

Standard Mode

Sites

- Contexts
 - Default Context
- Sites
 - http://detectportal.firefox.com
 - http://localhost:8080
 - GET:account
 - GET:rank
 - GET:transfer
 - POST:transfer()(pointsToTransfer,to)**
 - GET:welcome
 - POST:welcome()(password,username)

Method: POST Header: Text Body: Text

POST http://localhost:8080/transfer HTTP/1.1

Host: localhost:8080

User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:98.0) Gecko/20100101 Firefox/98.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

Accept-Language: en-US,en;q=0.5

Content-Type: application/x-www-form-urlencoded

Content-Length: 30

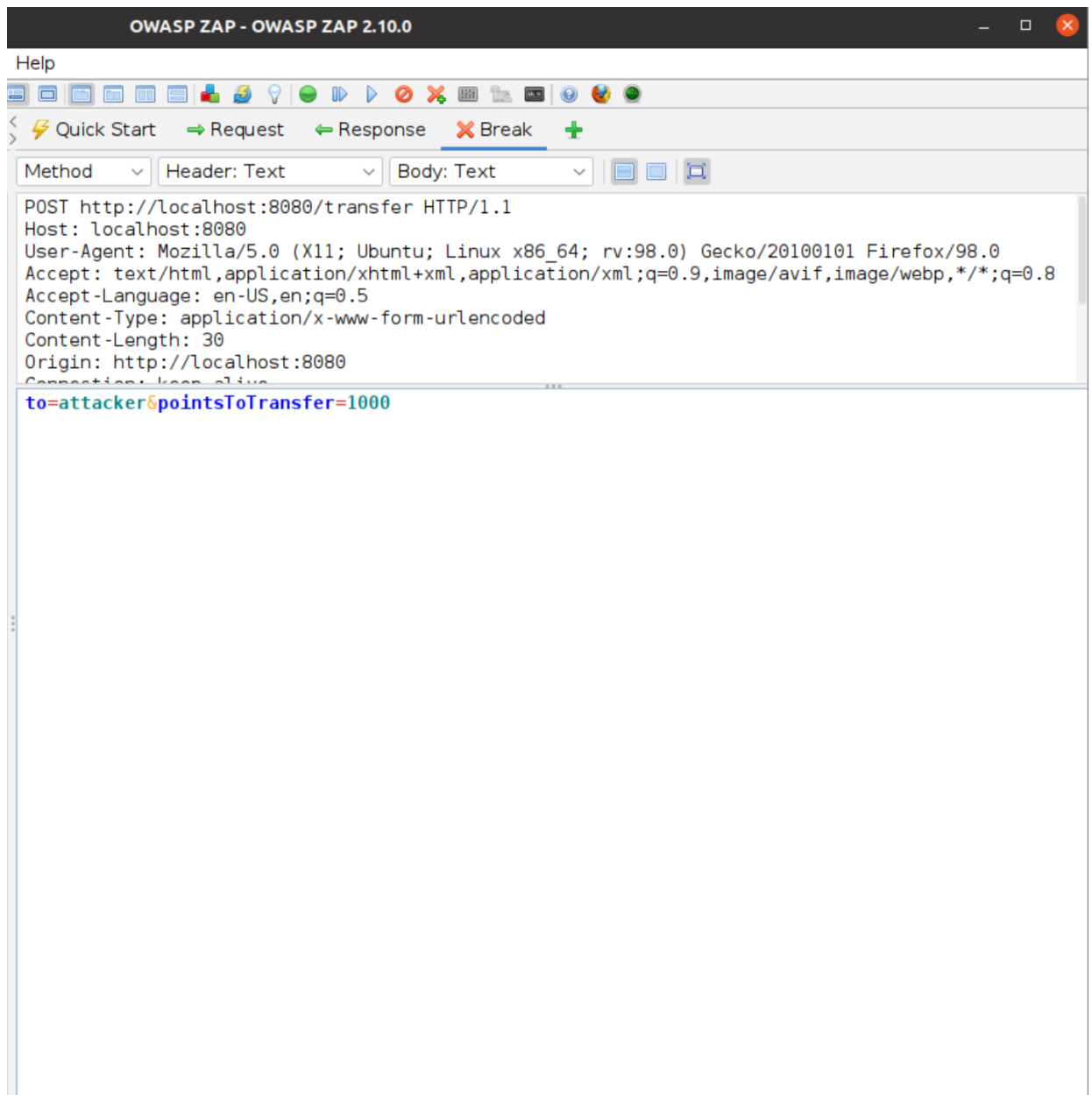
Origin: http://localhost:8080

Cookie: keep-alive

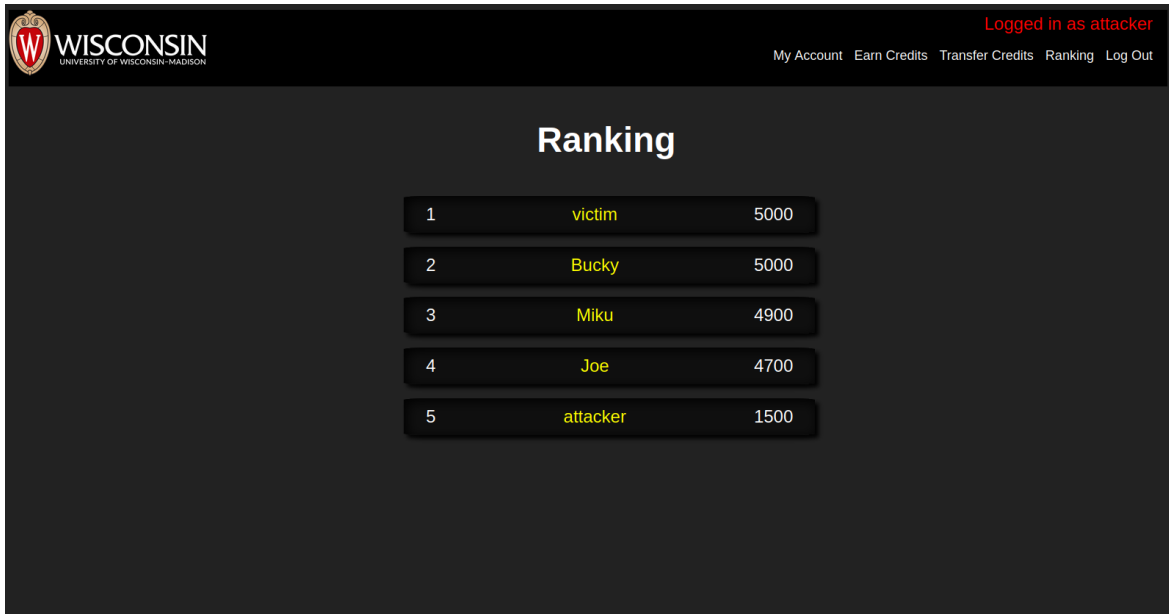
to=attacker&pointsToTransfer=1

History Search Alerts Output Breakpoints

Enabled	Type	Condition
<input checked="" type="checkbox"/>	HTTP	URL: Regex: Ignore Case:http://localhost:8080/transfer



- 3 A screenshot showing the attackers and victim's credits, on the ranking page, after the attack.



The screenshot shows the University of Wisconsin-Madison logo in the top left corner. In the top right corner, it says "Logged in as attacker" in red text. Below this, there are links for "My Account", "Earn Credits", "Transfer Credits", "Ranking", and "Log Out". The main heading is "Ranking". Below the heading is a table with 5 rows, each representing a user's rank and credits.

Rank	User	Credits
1	victim	5000
2	Bucky	5000
3	Miku	4900
4	Joe	4700
5	attacker	1500

4 Include a description of the attack, specifically:

4.1 What was the attack and how did you execute it?

This is a web attack by modifying the web request through the intercepting proxy. The intercepting proxy will then send the modified malicious request to the server, instead of the original one. We execute it by simply changing the user input 1 to 1000 in the intercepting proxy.

4.2 What resources were required by the attacker to execute this attack?

The attacker needs an Intercepting Proxy that can send/receive the request/response between the Web Server and the user/client. The Intercepting Proxy manipulates the data/request sent by the client before passing it to the Web Server, and then to the database.