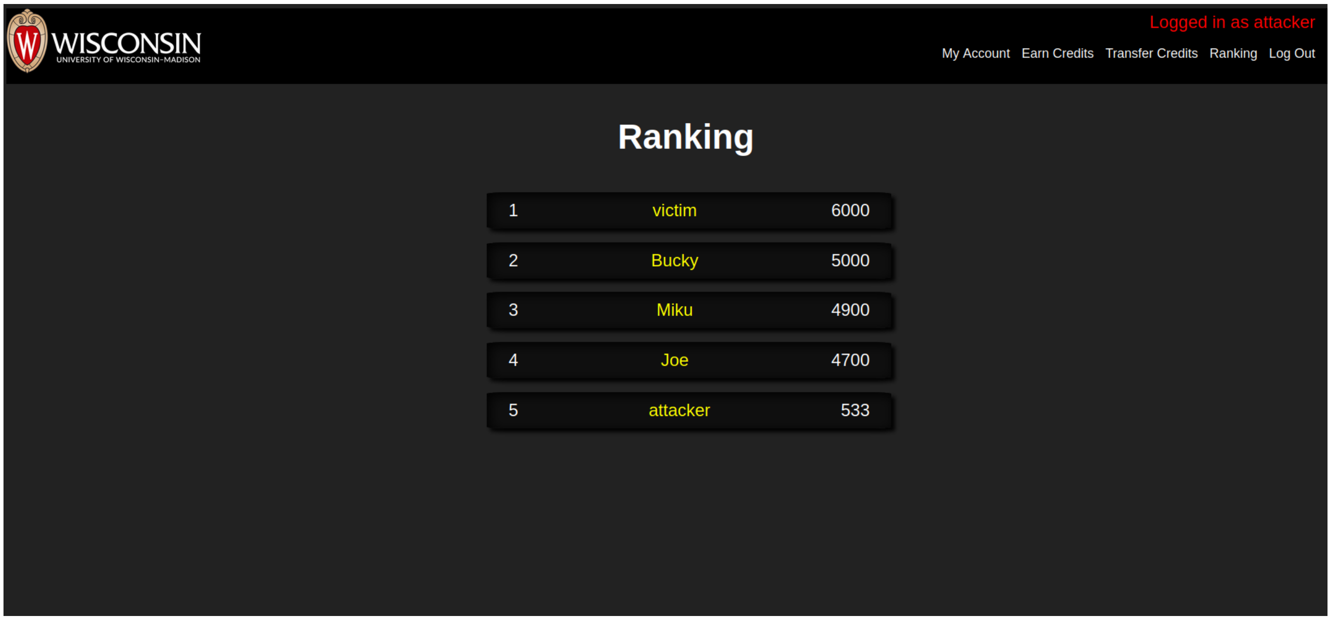
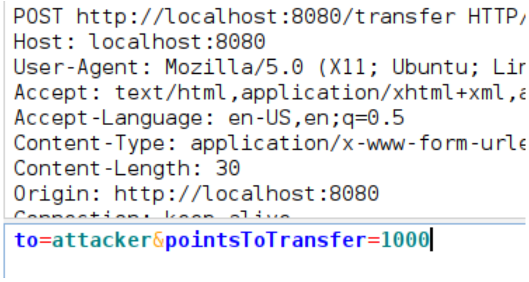


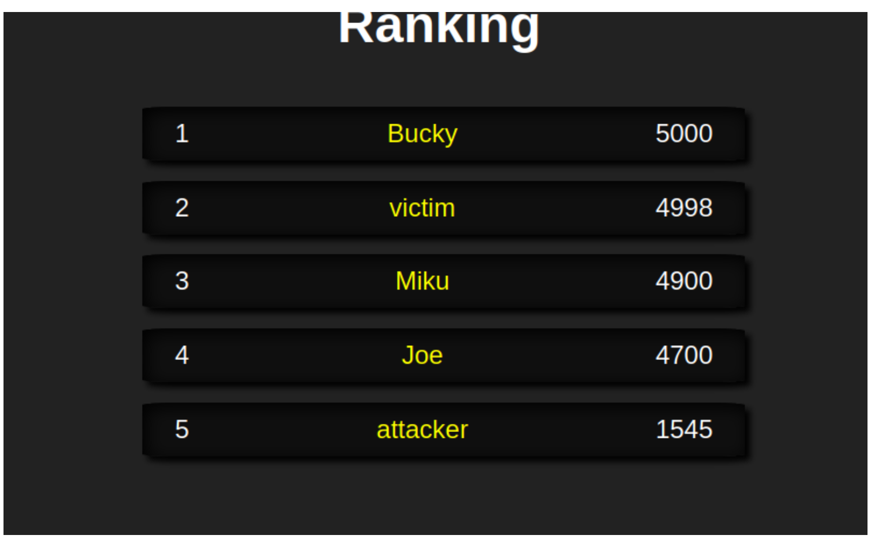
Ranking

1	victim	6000
2	Bucky	5000
3	Miku	4900
4	Joe	4700
5	attacker	533



```
POST http://localhost:8080/transfer HTTP/
Host: localhost:8080
User-Agent: Mozilla/5.0 (X11; Ubuntu; Lir
Accept: text/html,application/xhtml+xml,a
Accept-Language: en-US,en;q=0.5
Content-Type: application/x-www-form-urle
Content-Length: 30
Origin: http://localhost:8080
Connection: keep-alive
```

```
to=attacker&pointsToTransfer=1000
```



Ranking

1	Bucky	5000
2	victim	4998
3	Miku	4900
4	Joe	4700
5	attacker	1545

I interrupted the transfer of credits process through ZAP via a breakpoint whenever the request body contained the string “pointsToTransfer” and then modified it to be 1000 points instead of 1. This would only be possible for the attacker if they had access to ZAP for the running server and a knowledge of what the pattern of transfer requests looks like.