SoftwareSecured

# FaceBroke Lab

Born on a faraway planet, Mork Zickerbarg is an alien without a normal understanding of human behaviour and emotions.

Recently, he crash landed on Earth somewhere in the area of Boston and was immediately offered a full ride to Harvard (yes, it's just that easy). Today, he wants you to test his new social network, FaceBroke (cooked up over a night of green tea in his dorm room). As the fledgling company's new Chief Security Officer (you were mostly chosen since your dorm is across the hall), it's your task to look for the most common security vulnerabilities in web apps that can accidentally be introduced by tired alien beings (i.e. the average software developer).

To get you started, here are some goals for finding commonly broken pieces of Web-apps:

Your tasks:

- Create a popup on the page, without using the console, that says "I understand XSS!" that will dump out the current Session ID
- Create another pop up, without using the console, that shows up whenever browsing to a particular user's page, saying "I understand stored XSS!"
- Post to another User's wall, but have it appear as someone else
- Change the profile picture of Andrew Price (Mork seems like he's pretty important)
- Get a list of every user, including hashed passwords, on one page
- Upload an image that allows arbitrary JavaScript execution (hint: https://en.wikipedia.org/wiki/Scalable_Vector_Graphics)

**Getting Started**

Make sure you've got a recent version of FireFox installed!

Take note of your Team Number! You'll be navigating to 35.182.192.19:180{TEAM NUMBER}.
For example, team **01** would go to 35.182.192.19:180**01**

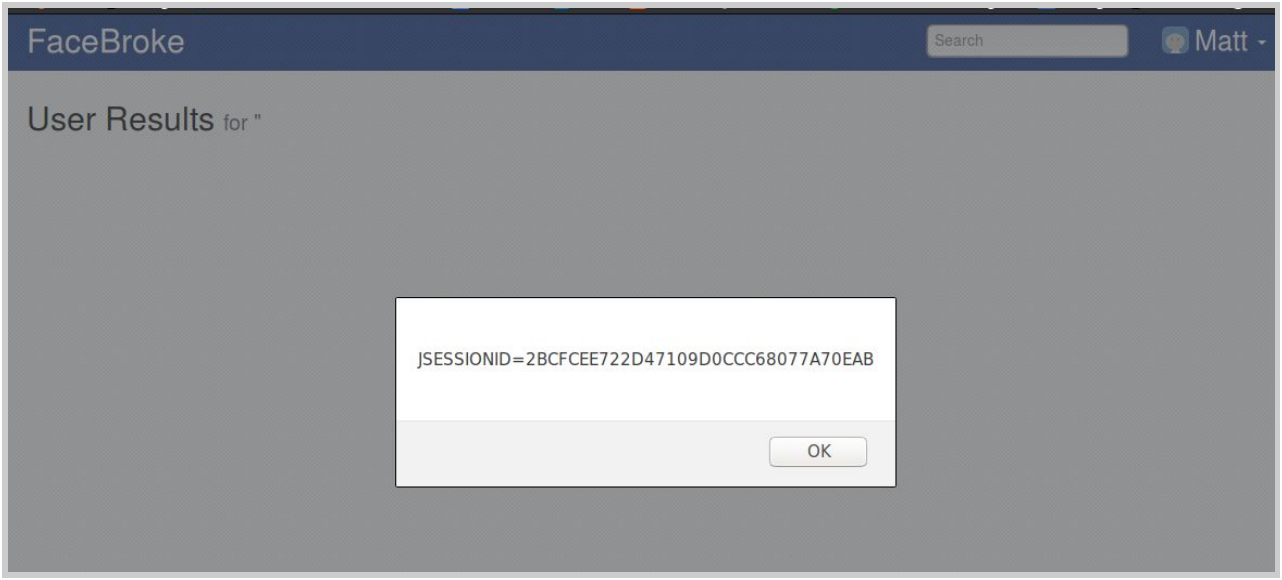
**For your report, make sure to record the following:**

- Description of vulnerability (i.e. how you exploited, why it's dangerous)
- Screenshot of results
- Any code snippet you needed to exploit the vulnerability
- How could this type of vulnerability be prevented?

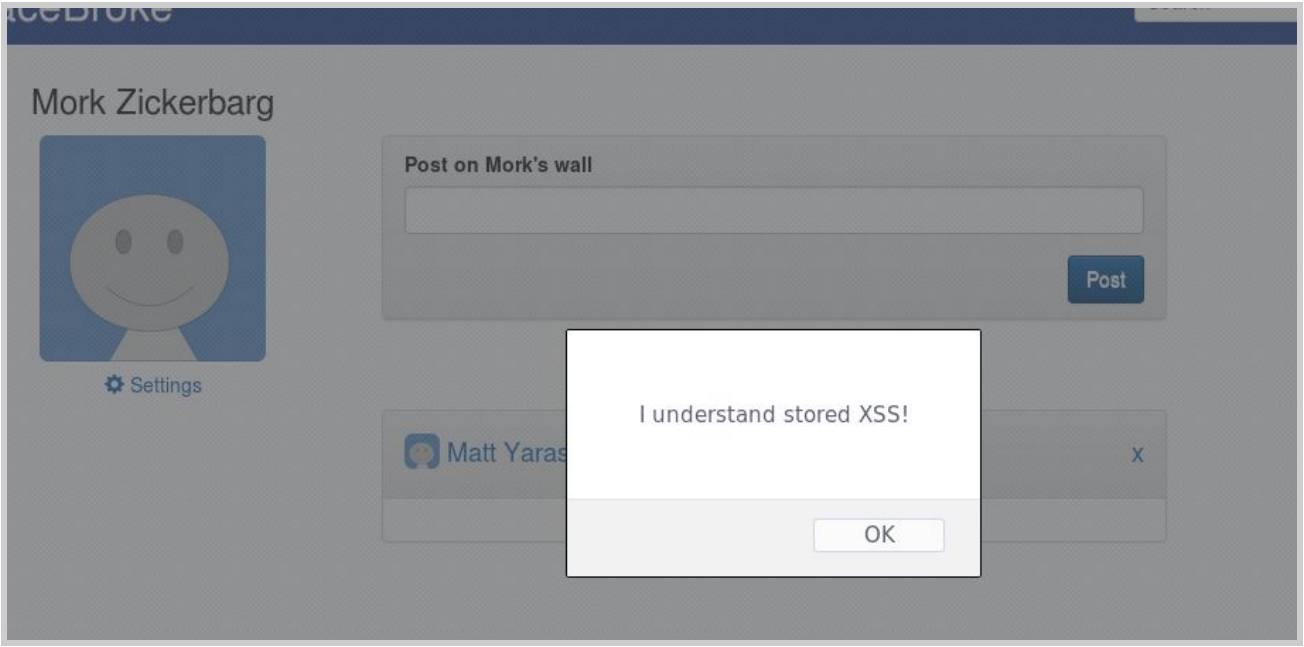
**Extra / Bonus**

As is the case with a lot most startups, everyone has a hand in everything at FaceBroke. You're asked to develop a new extension / functionality piece and submit it as a Pull Request on GitHub. For more info, take a look at https://github.com/softwaresecured/FaceBroke and follow the guidelines in CONTRIBUTING.md.

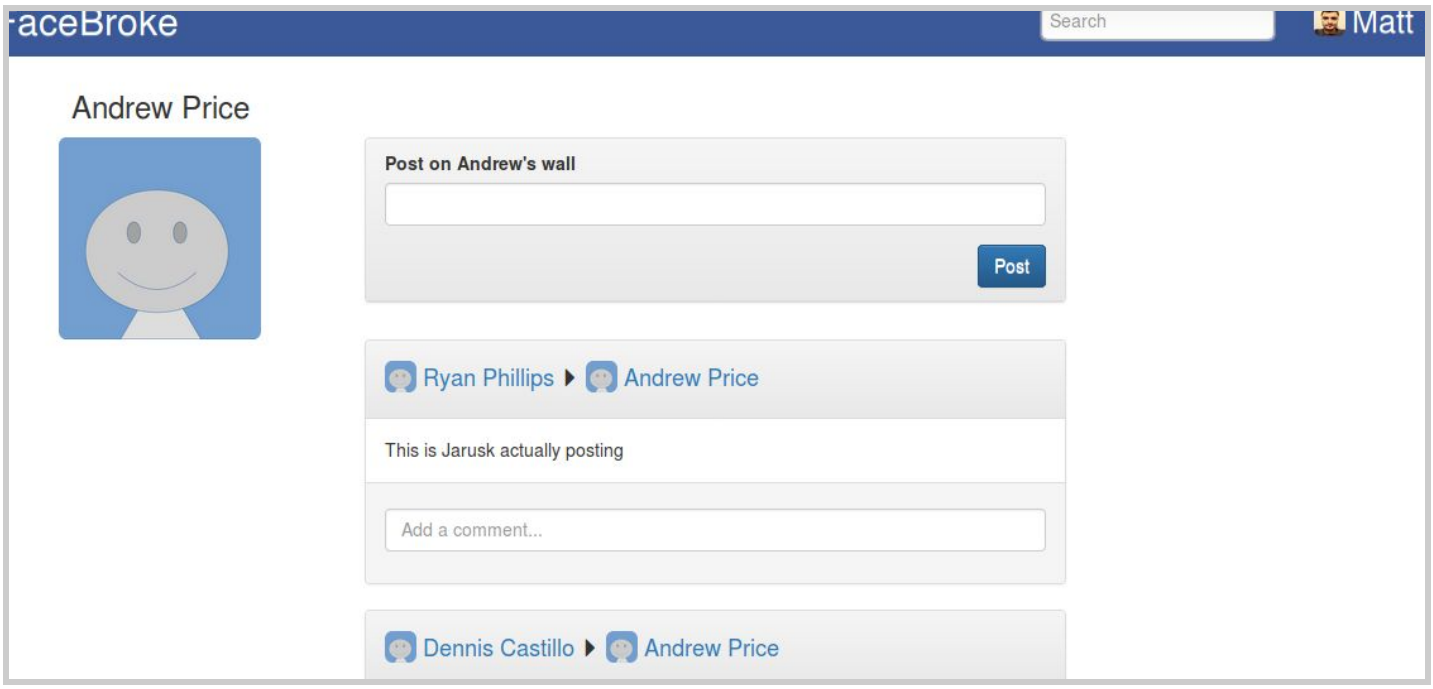
# Goal 1



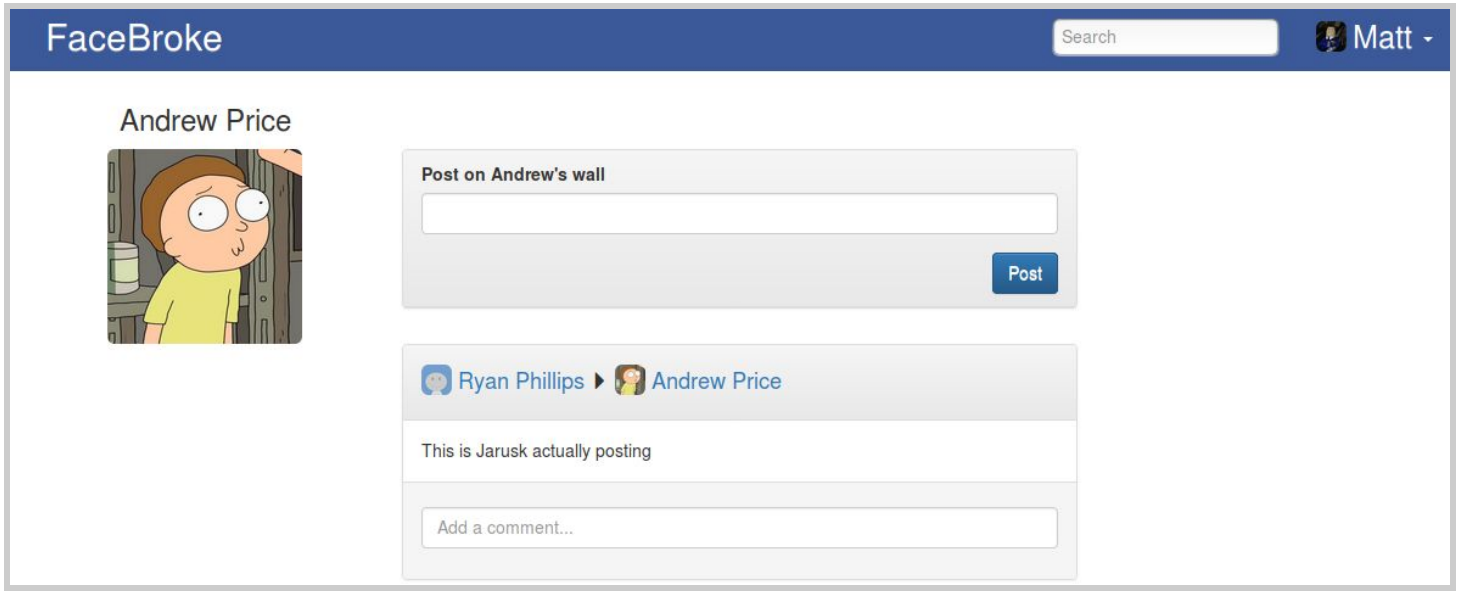

# Goal 2



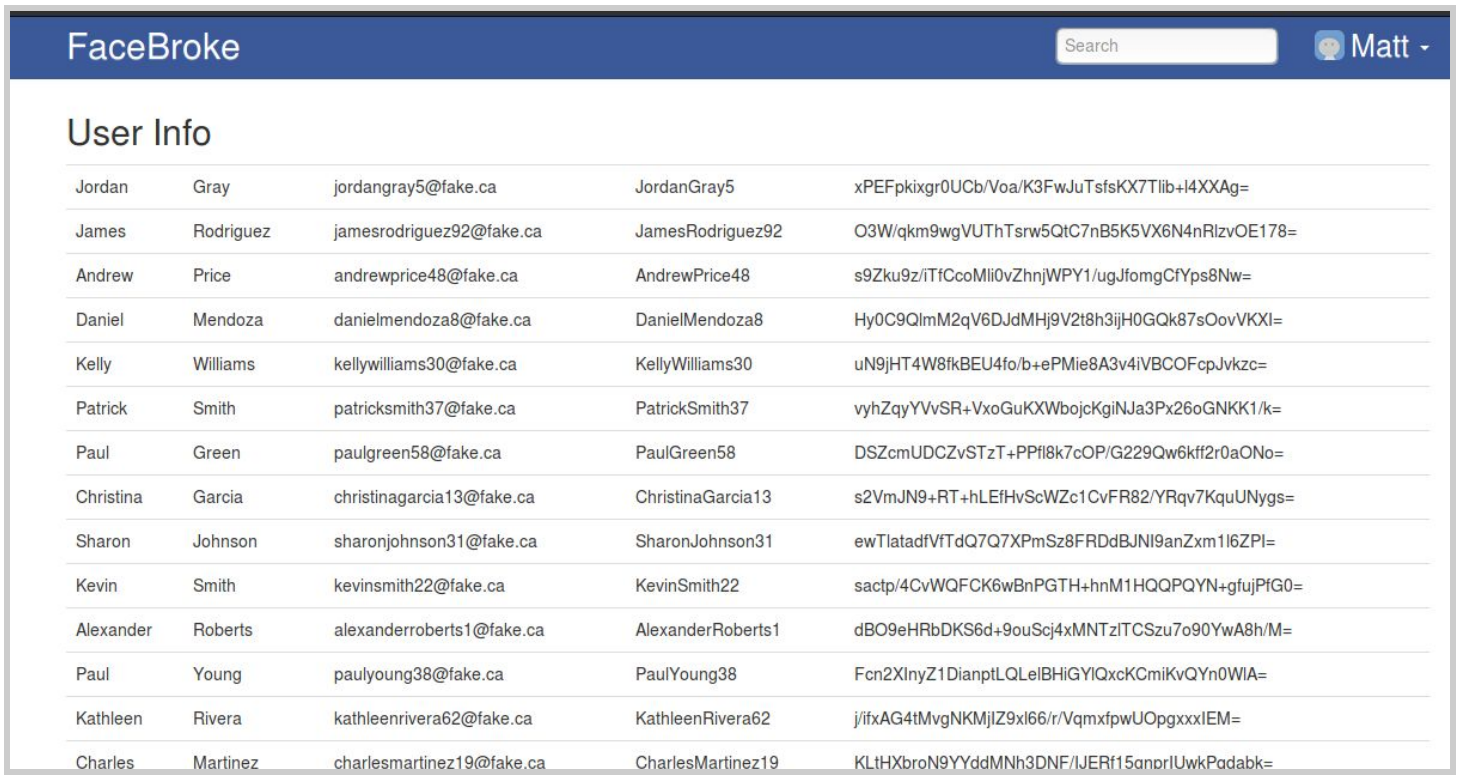
## Goal 3




## Goal 4



## Goal 5




## Goal 6