# Website Penetration Testing Lab

## People Against Security

Ryan Robeson

### Tools needed:

* Kali Linux VM
* pas.zip (obtained from instructor)
* hashcat

### Goals:

Penetrate the "People Against Security" Social Network and steal all of its users' passwords.

### Kali Setup (from terminal):

* Update Kali
  + aptitude update && aptitude safe-upgrade
* Install development libraries (required to build ruby 2)
  + aptitude install libssl-dev ruby1.9.1-dev libsqlite3-dev
* Install Ruby 2
  + git clone https://github.com/sstephenson/rbenv.git ~/.rbenv
  + echo 'export PATH="$HOME/.rbenv/bin:$PATH"' >> ~/.bash\_profile
  + echo 'eval "$(rbenv init -)"' >> ~/.bash\_profile
  + Close and reopen terminal
  + git clone https://github.com/sstephenson/ruby-build.git ~/.rbenv/plugins/ruby-build
  + rbenv install 2.1.0
* Configure Ruby 2 as the default
  + For the current shell only if you're worried about it
    - rbenv shell 2.1.0
  + Or globally (within Kali) for convenience and the latest features
    - rbenv global 2.1.0
* Copy in pas.zip to Kali (the Home folder will work fine)
  + ls
    - Should show pas.zip
  + unzip pas.zip -d pas
  + cd pas
  + Double check ruby version(need to be 2.1)
    - ruby -v
  + Install bundler ("Ruby Dependency Manager")
    - gem install bundler
  + bundle install --without development test
  + RACK\_ENV=production bundle exec rackup
* PAS is now running on Kali. The port is displayed in the terminal.

Intro: You are a Black Hat hacker hired by Dr. Lehrfeld to exploit a popular social network (PAS). They are constantly accusing him of being crazy for wasting time improving security and have banned him from their website. He is tired of being insulted and ignored. Your goal is to steal the passwords of its users from its database. This attack will take several steps to be successful. These exploits are all contained within the web application. Take screenshots after each step as proof of work.

After setting up Kali, the site will be accessible inside your virtual machine. Open up a browser to http://localhost:PORT where PORT is the port displayed in the terminal.

The first step in many attacks is information gathering. Take a look around. Consider creating an account. Look for anything that may give you a better understanding of PAS' implementation. View the page’s source. In some web applications, there are scripts for downloading files that take the filename as a parameter. Without proper validation, these scripts could be used to download files that hackers really don’t need to see, like the server side code behind a web page. Perhaps PAS has a similar vulnerability? See if you can gain access to PAS's source. Take a screenshot.

Obtaining access to the application’s source code is not enough. You still need to retrieve those passwords. Elevating privileges from a regular user to an admin can be very beneficial in an attack like this. Generally, different roles have different navigation items available to them. These are hidden on the server side so that normal users can’t find them. But, you have the source code. Maybe there is a hidden management url that could be used to create an administrator account. Take a screenshot once you have gained administrator access.

You’ve figured out how to gain admin access. Now you need to gain access to the database. Conveniently, PAS' administrators have created a simple solution for backing up their database. You can take advantage of this.

Now that you have a copy of the database, you need to get those passwords. As you are exploring the database, you notice that PAS was smart enough to hash their passwords. However, they did not salt them. This will make cracking them much easier. You just need to find out what hashing algorithm LehrBook is using on its passwords. You also need to write a SQL statement to extract all of the email addresses and passwords to a text file in a format suitable for hashcat. "username:hash" tends to work well.

Now you just need to run hashcat with the appropriate options to specify your cleverly crafted wordlist which will speed up the attack, which hash PAS is using, and the file containing the email addresses and passwords. When it finishes, you will have successfully stolen all of the user account details from PAS. Take a screenshot of hashcat running.

Congratulations! You just hacked a popular social network and made Dr. Lehrfeld very happy.