CodePath

Week 1

CS 4760 F18
Christopher Raley

Topics

Week 1

Readings available on CodePath Course website

- Fundamental Security Principles
- HTTP Requests
- URL Manipulation
- Insecure Direct Object Reference (IDOR)

Fundamental Security Principles

1. Never trust users
2. Least privilege
3. Simple is more secure
4. Expect the unexpected
5. Defense in depth
6. Security through obscurity
7. Prefer whitelisting over blacklisting
8. Map data movement and exposure

HTTP Requests

HTTP (HyperText Transfer Protocol) - Used to send requests to web servers

Request Types: ***GET***, ***POST***, *HEAD*, *PUT*, *DELETE*, *CONNECT*, *OPTIONS*

HTTP GET/POST Requests

GET

- Used when data data does *not* change
- View, search, sort, or filter data
- Sent when URL is entered in the browser and links are clicked on

POST

- Used when data does change
- Create, update, or delete data
- Sent when web forms are submitted

Attack: URL Manipulation

- URL's act not only as identifiers for other websites, but as requesters as well
  - Recall GET/POST Requests
- Nothing stops an attacker from entering other possible "commands" in the address bar
  - Websites that do not take account into this fact can be vulnerable

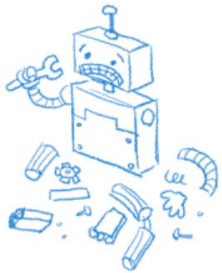
URL Manipulation Prevention

- Just because the user can’t see a link to a specific URL, doesn’t mean that it is not there
  - Don’t consider URLs to be private
- Error handling
- Expect the unexpected

Google

404. That’s an error.

The requested URL /admin was not found on this server.
That’s all we know.



Attack: IDOR

- Insecure Direct Object Reference
- When a direct reference to an object is available without proper authentication
- Usually concerned with databases, files, directories, etc.

What’s the vulnerability?

http://foo.com/receipt?invoice=TPX-10457

IDOR Prevention

- Validate the user's credentials (most effective)
- Reject all input, except for acceptable ones
- Direct Object References -> Indirect Object References
    - Make it meaningful to only the actual user

Lab 1

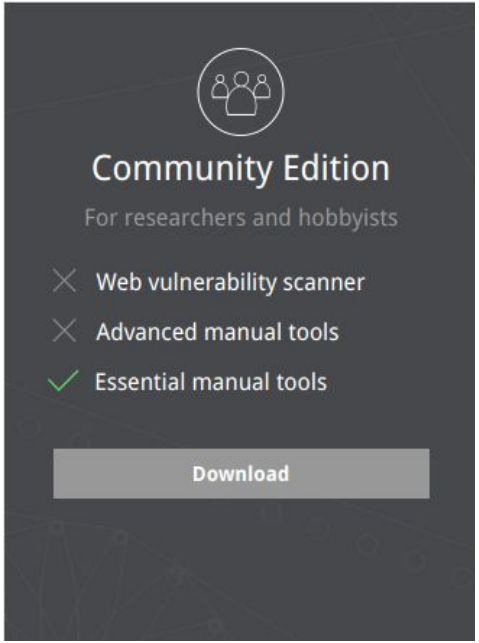
Introduction to Burp and Security Shepherd

Installing Burp Proxy

https://portswigger.net/burp

Download and install the

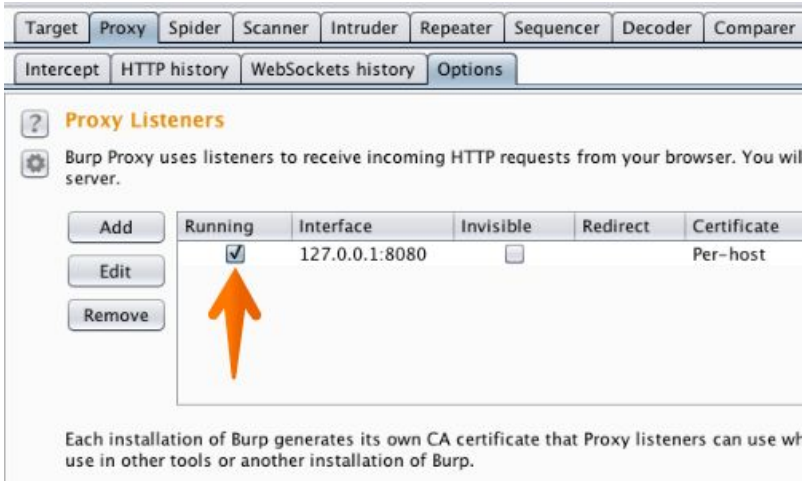
Community Edition



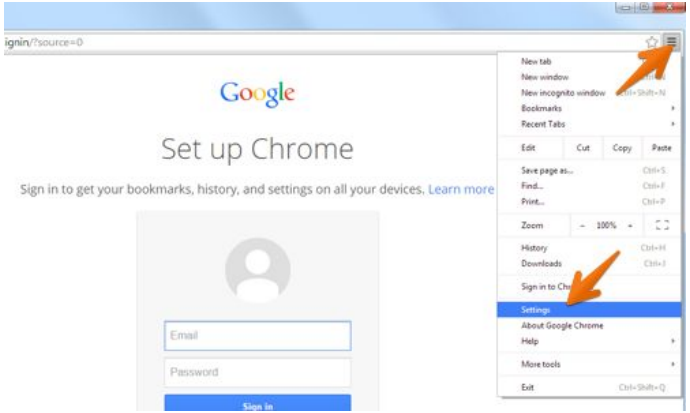
Run Burp and click “Next”, then “Start Burp”

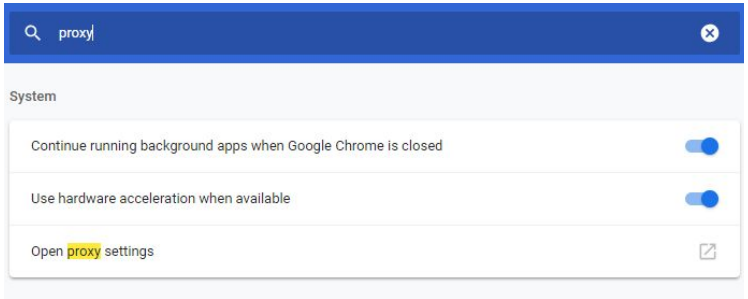
Go to the “Proxy” tab then “Options”

Make sure that the “Interface” matches the image on the right

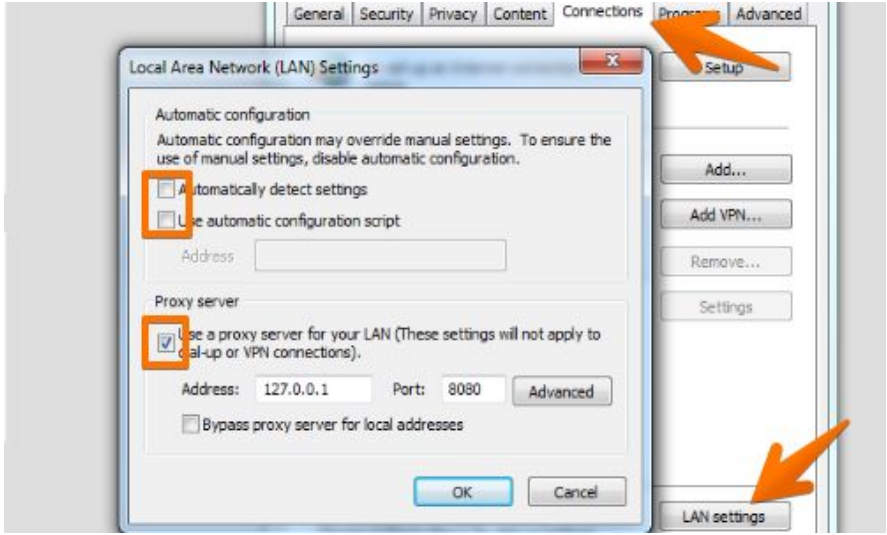


1) Go to Chrome Menu (Top-right)
2) Go to Settings
3) Search for “proxy”
4) Select “Open proxy settings”
5) Go to the Connections tab, and click on the "LAN settings" button
6) Make sure only “Use a proxy server…” is checked
7) Enter “127.0.0.1” in “Address” field and “8080” in “Port” field
8) Then click on the "Advanced" button.
9) Make sure the "Use the same proxy server for all protocols" box is checked.
10) Delete anything that appears in the "Exceptions" field.
11) Then click "OK" to close all of the options dialogs.

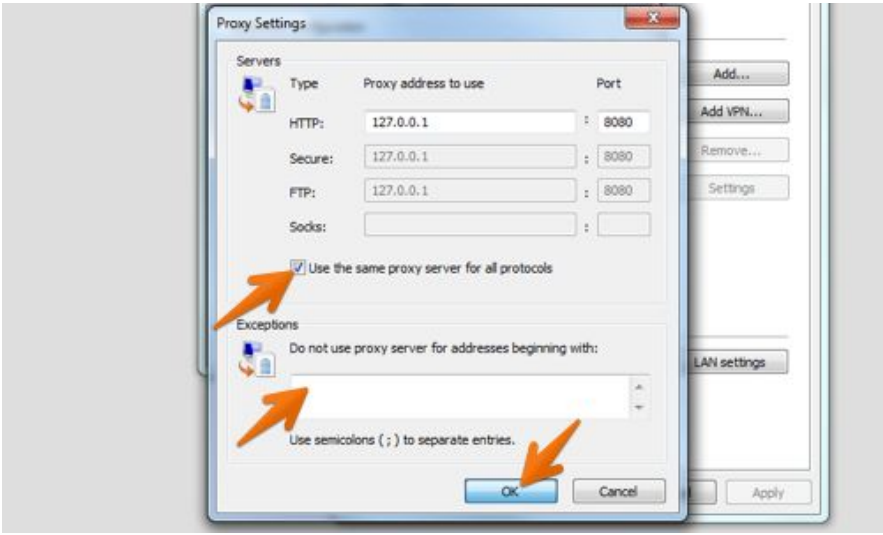




1) Go to Chrome Menu (Top-right)
2) Go to Settings
3) Search for “proxy”
4) Select “Open proxy settings”
5) Go to the Connections tab, and click on the "LAN settings" button
6) Make sure only “Use a proxy server…” is checked
7) Enter “127.0.0.1” in “Address” field and “8080” in “Port” field
8) Then click on the "Advanced" button.
9) Make sure the "Use the same proxy server for all protocols" box is checked.
10) Delete anything that appears in the "Exceptions" field.
11) Then click "OK" to close all of the options dialogs.



1) Go to Chrome Menu (Top-right)
2) Go to Settings
3) Search for “proxy”
4) Select “Open proxy settings”
5) Go to the Connections tab, and click on the "LAN settings" button
6) Make sure only “Use a proxy server...” is checked
7) Enter “127.0.0.1” in “Address” field and “8080” in “Port” field
8) Then click on the "Advanced" button.
9) Make sure the "Use the same proxy server for all protocols" box is checked.
10) Delete anything that appears in the "Exceptions" field.
11) Then click "OK" to close all of the options dialogs.



Proxy is done... but we can’t access websites that use HTTPS...

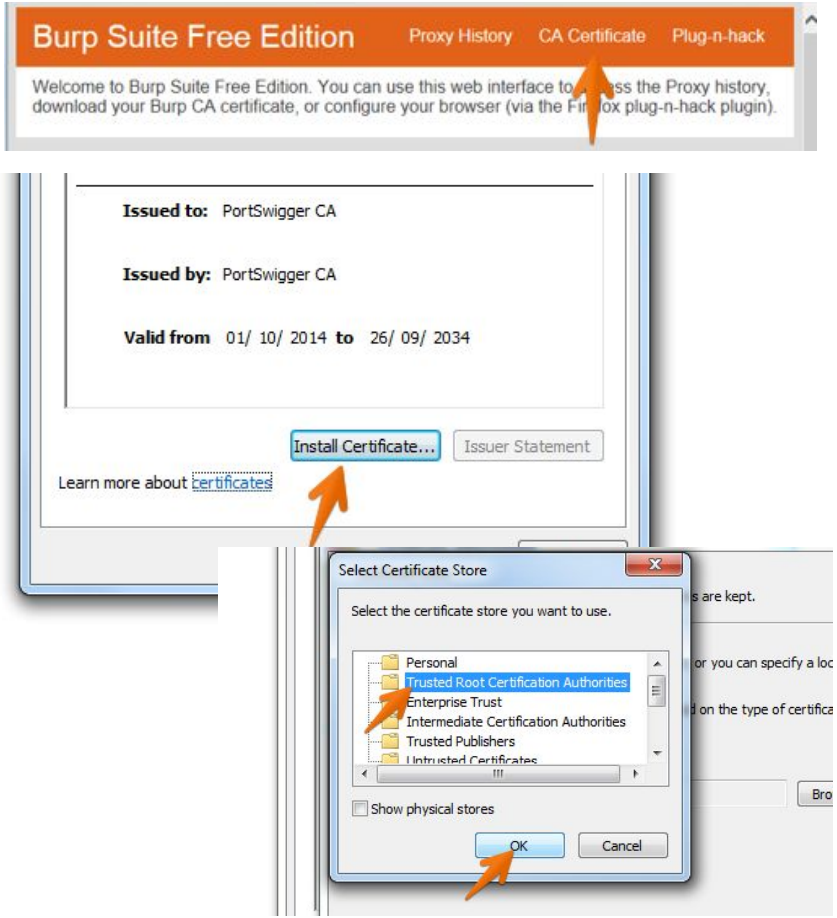
More on why later in the course!

Launch Google Chrome

With Burp running, visit http://burp in the address bar and click the “CA Certificate” bar at the top right to download and save your Burp CA certificate

Open the downloaded certificate

- Click “Install Certificate”.
- In the “Certificate Import Wizard” dialog box click “Next”.
- In the Certificate Import Wizard, select "Place all certificates in the following store" and click “Browse”.
- In the “Select Certificate Store” window select "Trusted Root Certification Authorities" and click “OK”.
- Complete the wizard by clicking “Next” followed by “Finish”.
- Click "Yes" on the security warning.
- Restart Chrome



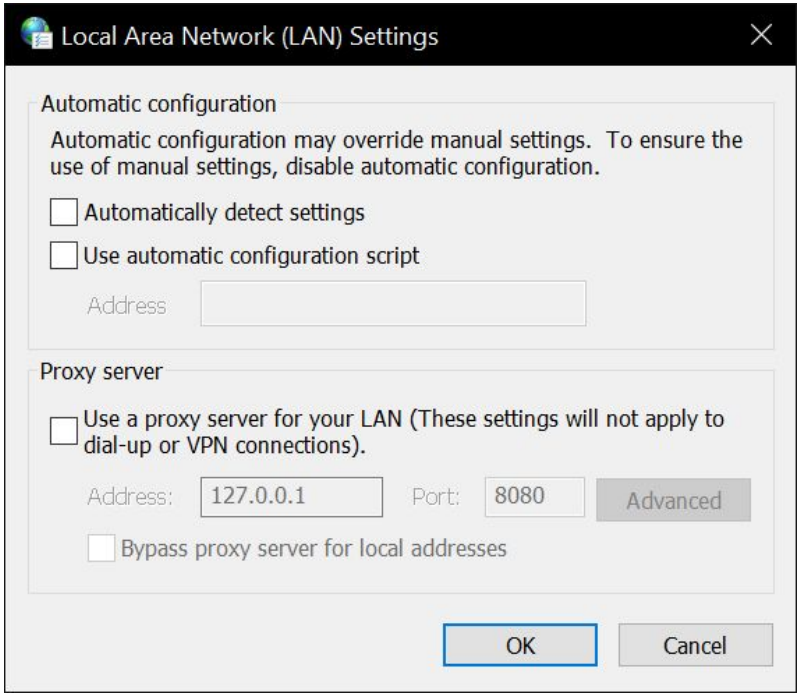
Go to Proxy -> HTTP history and try browsing the web

Make sure that you can access websites that use HTTPS

You should be able to see GET/POST requests

You can only browse when the Burp Proxy is **active**.

Uncheck “Use a proxy server for your LAN...” to use Chrome normally.



https://security.codepath.com/login.jsp

* Go to Proxy -> Intercept and click on the “Intercept is on” so that it says “Intercept is off”

Introduction to CTF's

“A cyber security CTF is a competition between security professionals and/or students learning about cyber security”

We will be focusing on a Jeopardy style CTF

https://ctf.codepath.com

* If you haven’t registered yet, do so now at the link

Office Hours

Monday / Thursday : 5 - 7 PM @ Rice 226