INTRO TO ETHICAL HACKING

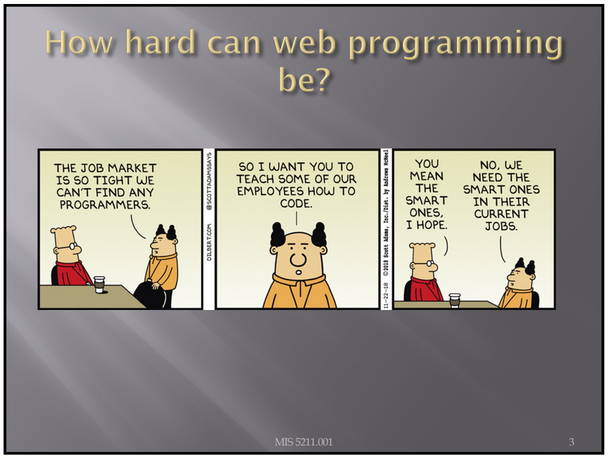
MIS 5211.001
Week 9

1

Tonight's Plan

- Web Application Security

2



How hard can web programming be?

THE JOB MARKET IS SO TIGHT WE CAN'T FIND ANY PROGRAMMERS.
SO I WANT YOU TO TEACH SOME OF OUR EMPLOYEES HOW TO CODE.
YOU MEAN THE SMART ONES, I HOPE.
NO, WE NEED THE SMART ONES IN THEIR CURRENT JOBS.
DILBERT.COM @SCOTTADAMSSAYS
11-22-18 ©2018 Scott Adams, Inc./Dist. by Andrews McMeel

3

Web Application Security

- First (and nearly only) Rule

Never Trust User Input

MIS 5211.001 4

4

Where Do We Start

- For web application security and web application penetration testing

Owasp.org

MIS 5211.001 5

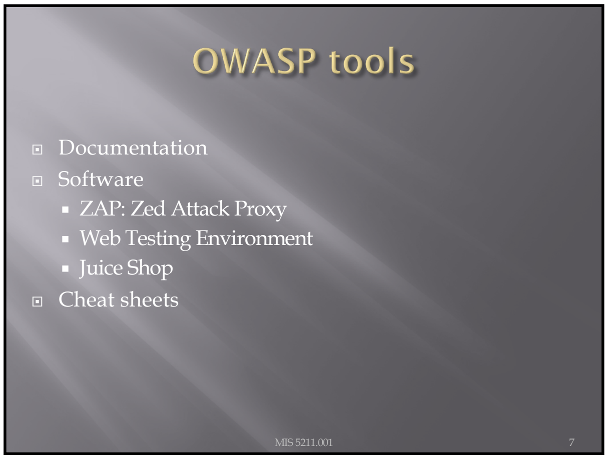
5

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

MIS 5211.001 6

6

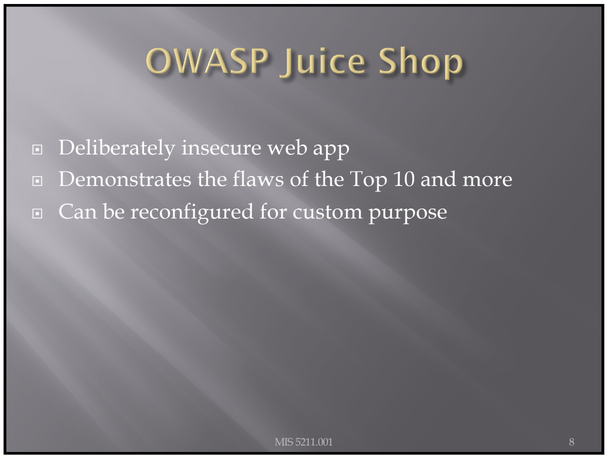


OWASP tools

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

MIS 5211.001 7

7

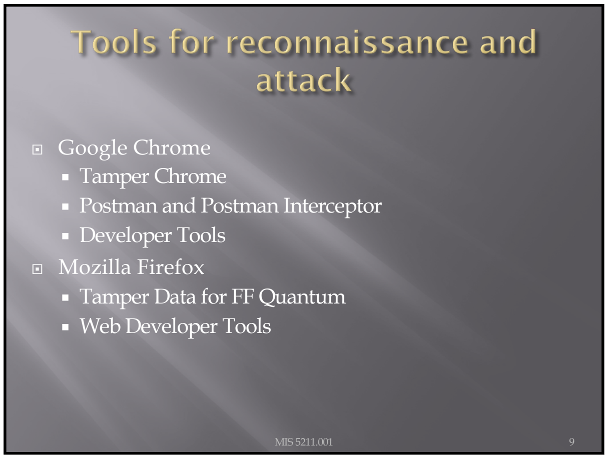


OWASP Juice Shop

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

MIS 5211.001 8

8



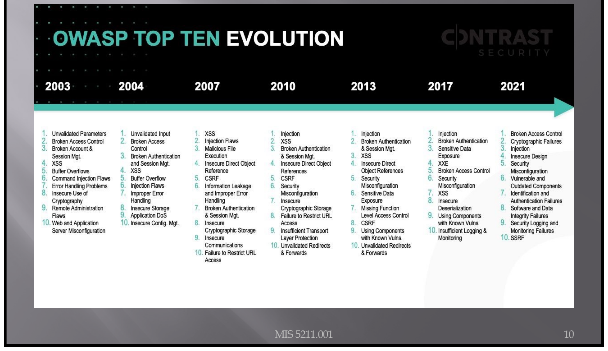
Tools for reconnaissance and attack

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

MIS 5211.001 9

9

History of OWASP Top 10



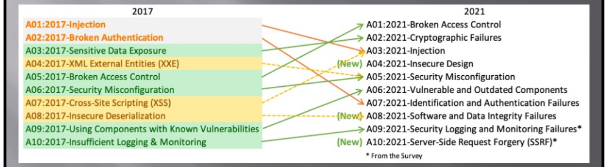
OWASP TOP TEN EVOLUTION

CONTRAST SECURITY

	2003	2004	2007	2010	2013	2017	2021
1.	Unvalidated Parameters	Unvalidated Input	XSS	Injection	Injection	Injection	Broken Access Control
2.	Broken Access Control	Broken Access Control	Injection Flaws	XSS	Broken Authentication & Session Mgt.	Broken Authentication	Cryptographic Failures
3.	Broken Account & Session Mgt.	Broken Authentication and Session Mgt.	Malicious File Execution	Broken Authentication & Session Mgt.	XSS	Sensitive Data Exposure	Injection
4.	XSS	XSS	Insecure Direct Object Reference	Insecure Direct Object References	Insecure Direct Object References	XXE	Insecure Design
5.	Buffer Overflows	Buffer Overflow	CSRF	CSRF	Security Misconfiguration	Broken Access Control	Security Misconfiguration
6.	Command Injection Flaws	Injection Flaws	Information Leakage and Improper Error Handling	Security Misconfiguration	Sensitive Data Exposure	Security Misconfiguration	Vulnerable and Outdated Components
7.	Error Handling Problems	Improper Error Handling	Broken Authentication & Session Mgt.	Insecure Cryptographic Storage	Missing Function Level Access Control	XSS	Identification and Authentication Failures
8.	Insecure Use of Cryptography	Insecure Storage	Insecure Cryptographic Storage	Failure to Restrict URL Access	CSRF	Insecure Deserialization	Software and Data Integrity Failures
9.	Remote Administration Flaws	Application DoS	Insecure Communications	Insufficient Transport Layer Protection	Using Components with Known Vulns.	Using Components with Known Vulns.	Security Logging and Monitoring Failures
10.	Web and Application Server Misconfiguration	Insecure Config. Mgt.	Failure to Restrict URL Access	Unvalidated Redirects & Forwards	Unvalidated Redirects & Forwards	Insufficient Logging & Monitoring	SSRF

10

Changes from 2017 - 2021



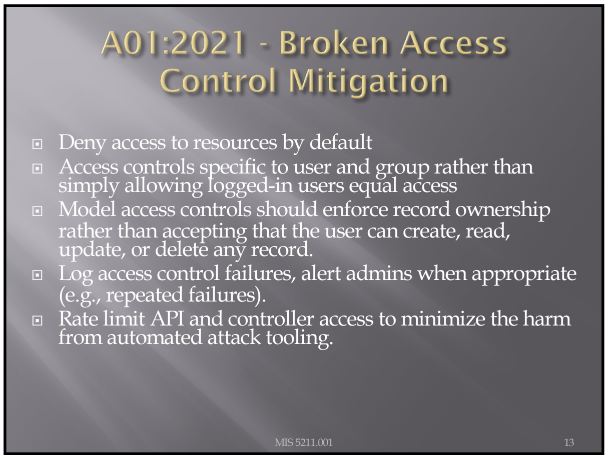
2017
A01:2017-Injection
A02:2017-Broken Authentication
A03:2017-Sensitive Data Exposure
A04:2017-XML External Entities (XXE)
A05:2017-Broken Access Control
A06:2017-Security Misconfiguration
A07:2017-Cross-Site Scripting (XSS)
A08:2017-Insecure Deserialization
A09:2017-Using Components with Known Vulnerabilities
A10:2017-Insufficient Logging & Monitoring
2021
A01:2021-Broken Access Control
A02:2021-Cryptographic Failures
A03:2021-Injection
(New) A04:2021-Insecure Design
A05:2021-Security Misconfiguration
A06:2021-Vulnerable and Outdated Components
A07:2021-Identification and Authentication Failures
(New) A08:2021-Software and Data Integrity Failures
A09:2021-Security Logging and Monitoring Failures*
(New) A10:2021-Server-Side Request Forgery (SSRF)*
* From the Survey

11

A01:2021 - Broken Access Control

Access control enforces policy such that users cannot act outside of their intended permissions. Failures typically lead to unauthorized information disclosure, modification, or destruction of all data or performing a business function outside the user's limits.

12

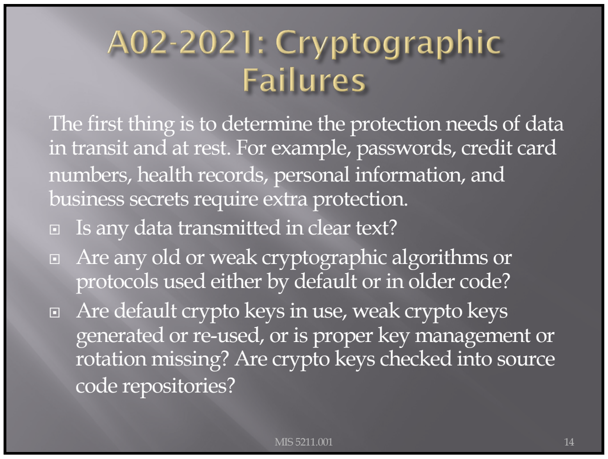


A01:2021 - Broken Access Control Mitigation

- Deny access to resources by default
- Access controls specific to user and group rather than simply allowing logged-in users equal access
- Model access controls should enforce record ownership rather than accepting that the user can create, read, update, or delete any record.
- Log access control failures, alert admins when appropriate (e.g., repeated failures).
- Rate limit API and controller access to minimize the harm from automated attack tooling.

MIS 5211.001 13

13



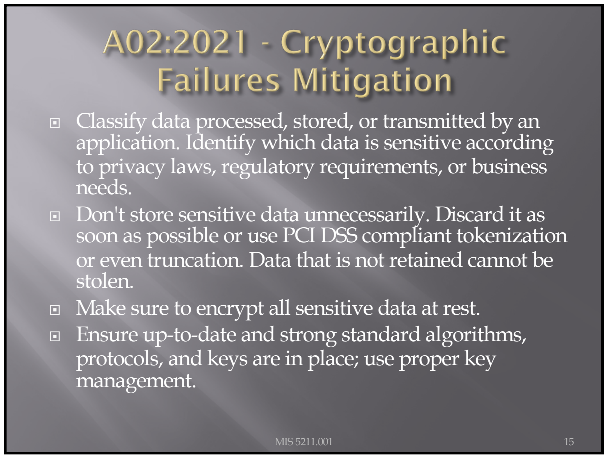
A02-2021: Cryptographic Failures

The first thing is to determine the protection needs of data in transit and at rest. For example, passwords, credit card numbers, health records, personal information, and business secrets require extra protection.

- Is any data transmitted in clear text?
- Are any old or weak cryptographic algorithms or protocols used either by default or in older code?
- Are default crypto keys in use, weak crypto keys generated or re-used, or is proper key management or rotation missing? Are crypto keys checked into source code repositories?

MIS 5211.001 14

14

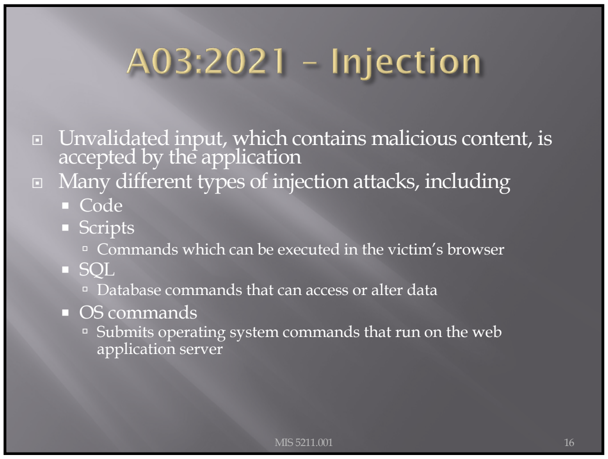


A02:2021 - Cryptographic Failures Mitigation

- Classify data processed, stored, or transmitted by an application. Identify which data is sensitive according to privacy laws, regulatory requirements, or business needs.
- Don't store sensitive data unnecessarily. Discard it as soon as possible or use PCI DSS compliant tokenization or even truncation. Data that is not retained cannot be stolen.
- Make sure to encrypt all sensitive data at rest.
- Ensure up-to-date and strong standard algorithms, protocols, and keys are in place; use proper key management.

MIS 5211.001 15

15

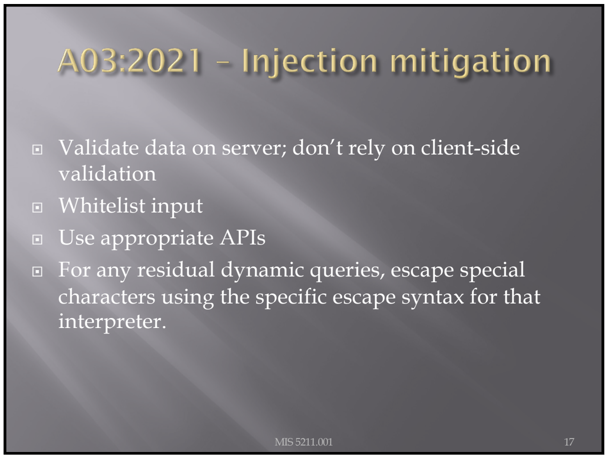


A03:2021 – Injection

- 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

MIS 5211.001 16

16

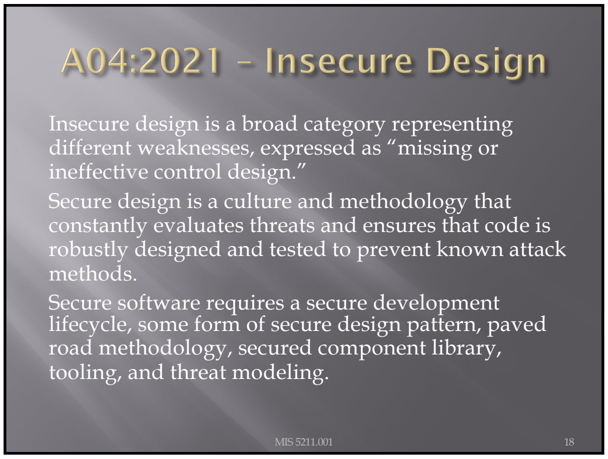


A03:2021 – Injection mitigation

- Validate data on server; don't rely on client-side validation
- Whitelist input
- Use appropriate APIs
- For any residual dynamic queries, escape special characters using the specific escape syntax for that interpreter.

MIS 5211.001 17

17



A04:2021 – Insecure Design

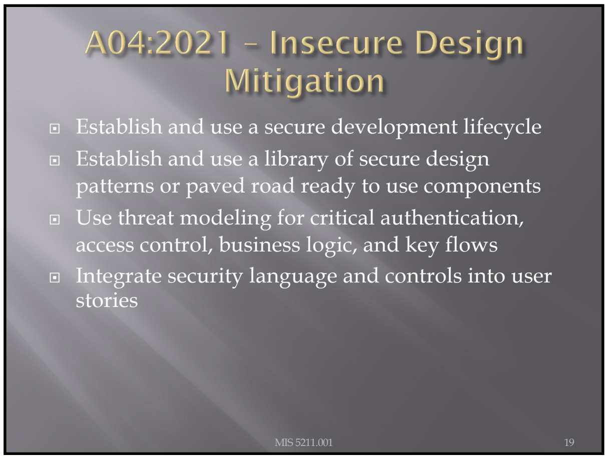
Insecure design is a broad category representing different weaknesses, expressed as "missing or ineffective control design."

Secure design is a culture and methodology that constantly evaluates threats and ensures that code is robustly designed and tested to prevent known attack methods.

Secure software requires a secure development lifecycle, some form of secure design pattern, paved road methodology, secured component library, tooling, and threat modeling.

MIS 5211.001 18

18

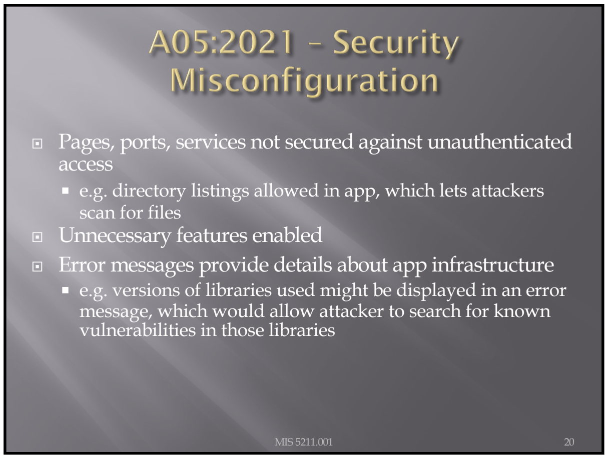


A04:2021 – Insecure Design Mitigation

- Establish and use a secure development lifecycle
- Establish and use a library of secure design patterns or paved road ready to use components
- Use threat modeling for critical authentication, access control, business logic, and key flows
- Integrate security language and controls into user stories

MIS 5211.001 19

19

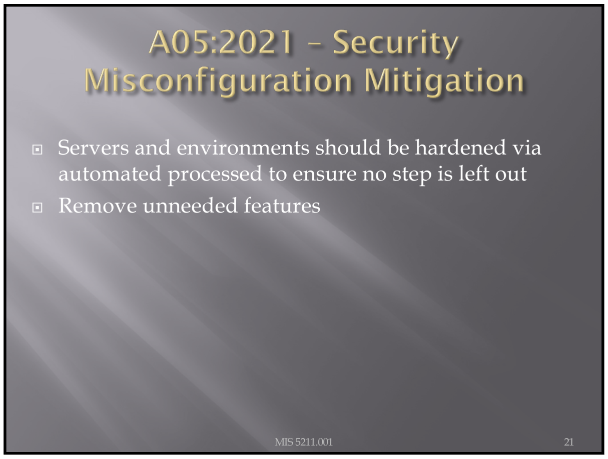


A05:2021 – Security Misconfiguration

- 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

MIS 5211.001 20

20

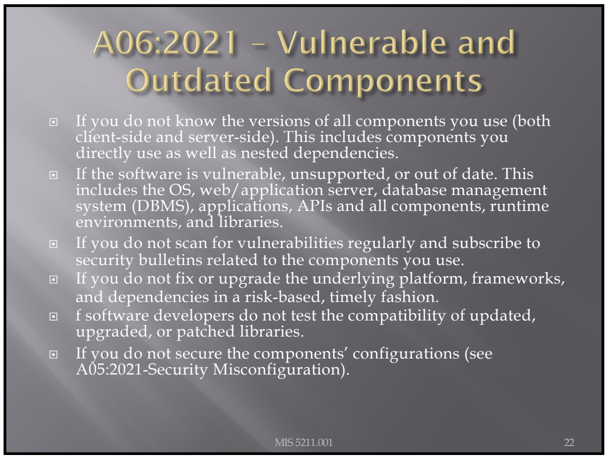


A05:2021 – Security Misconfiguration Mitigation

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

MIS 5211.001 21

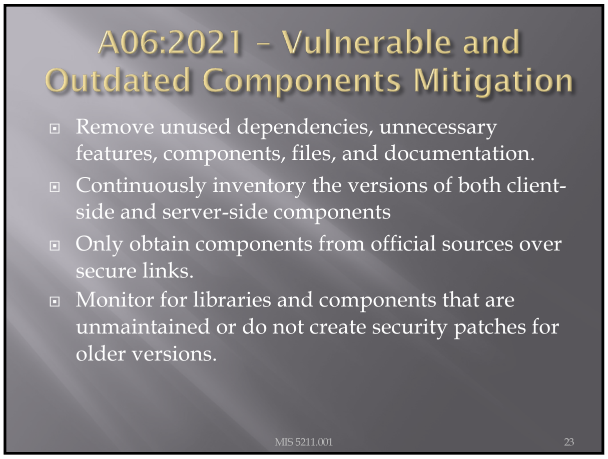
21



A06:2021 – Vulnerable and Outdated Components

- If you do not know the versions of all components you use (both client-side and server-side). This includes components you directly use as well as nested dependencies.
- If the software is vulnerable, unsupported, or out of date. This includes the OS, web/application server, database management system (DBMS), applications, APIs and all components, runtime environments, and libraries.
- If you do not scan for vulnerabilities regularly and subscribe to security bulletins related to the components you use.
- If you do not fix or upgrade the underlying platform, frameworks, and dependencies in a risk-based, timely fashion.
- f software developers do not test the compatibility of updated, upgraded, or patched libraries.
- If you do not secure the components' configurations (see A05:2021-Security Misconfiguration).

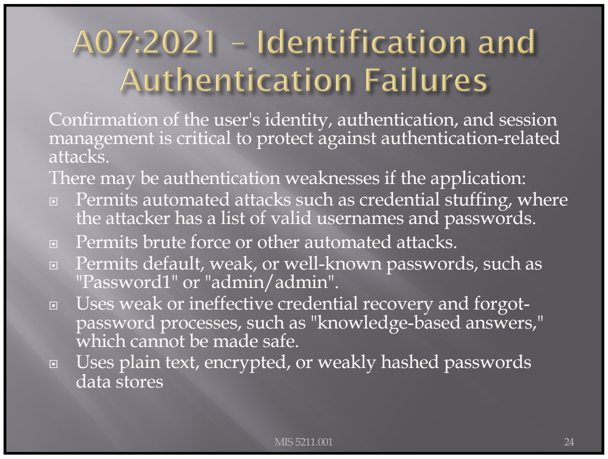
22



A06:2021 – Vulnerable and Outdated Components Mitigation

- Remove unused dependencies, unnecessary features, components, files, and documentation.
- Continuously inventory the versions of both client-side and server-side components
- Only obtain components from official sources over secure links.
- Monitor for libraries and components that are unmaintained or do not create security patches for older versions.

23



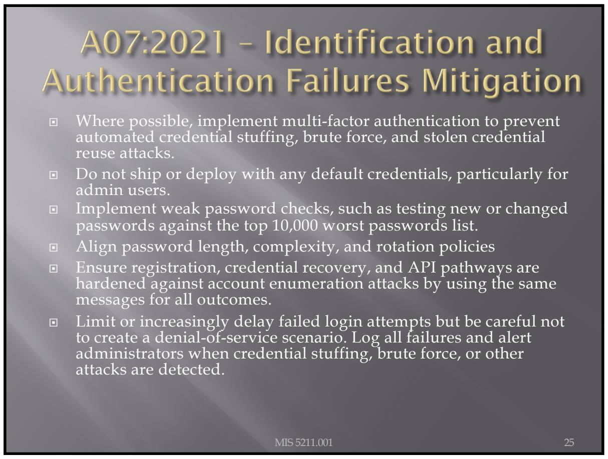
A07:2021 – Identification and Authentication Failures

Confirmation of the user's identity, authentication, and session management is critical to protect against authentication-related attacks.

There may be authentication weaknesses if the application:

- Permits automated attacks such as credential stuffing, where the attacker has a list of valid usernames and passwords.
- Permits brute force or other automated attacks.
- Permits default, weak, or well-known passwords, such as "Password1" or "admin/admin".
- Uses weak or ineffective credential recovery and forgot-password processes, such as "knowledge-based answers," which cannot be made safe.
- Uses plain text, encrypted, or weakly hashed passwords data stores

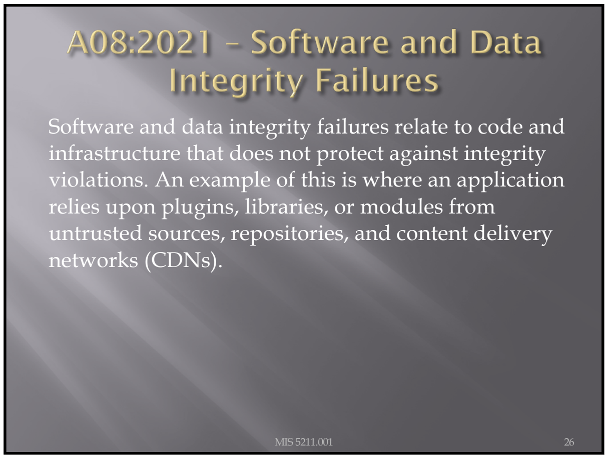
24



A07:2021 – Identification and Authentication Failures Mitigation

- Where possible, implement multi-factor authentication to prevent automated credential stuffing, brute force, and stolen credential reuse attacks.
- Do not ship or deploy with any default credentials, particularly for admin users.
- Implement weak password checks, such as testing new or changed passwords against the top 10,000 worst passwords list.
- Align password length, complexity, and rotation policies
- Ensure registration, credential recovery, and API pathways are hardened against account enumeration attacks by using the same messages for all outcomes.
- Limit or increasingly delay failed login attempts but be careful not to create a denial-of-service scenario. Log all failures and alert administrators when credential stuffing, brute force, or other attacks are detected.

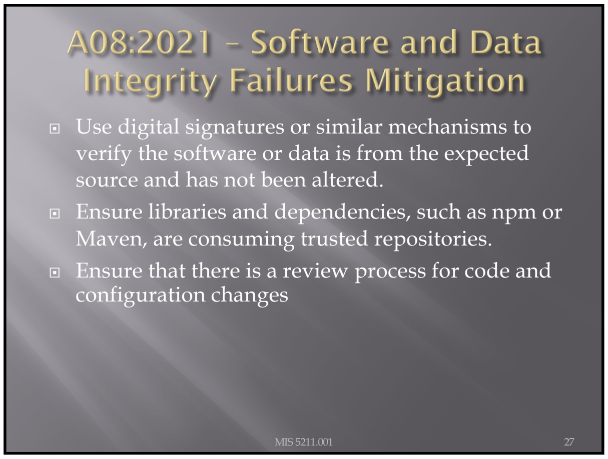
25



A08:2021 – Software and Data Integrity Failures

Software and data integrity failures relate to code and infrastructure that does not protect against integrity violations. An example of this is where an application relies upon plugins, libraries, or modules from untrusted sources, repositories, and content delivery networks (CDNs).

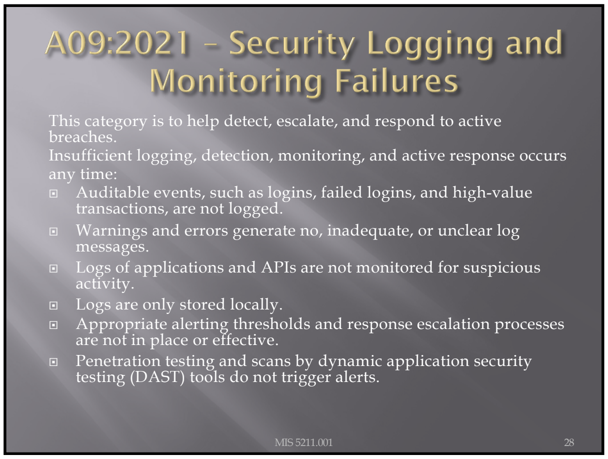
26



A08:2021 – Software and Data Integrity Failures Mitigation

- Use digital signatures or similar mechanisms to verify the software or data is from the expected source and has not been altered.
- Ensure libraries and dependencies, such as npm or Maven, are consuming trusted repositories.
- Ensure that there is a review process for code and configuration changes

27



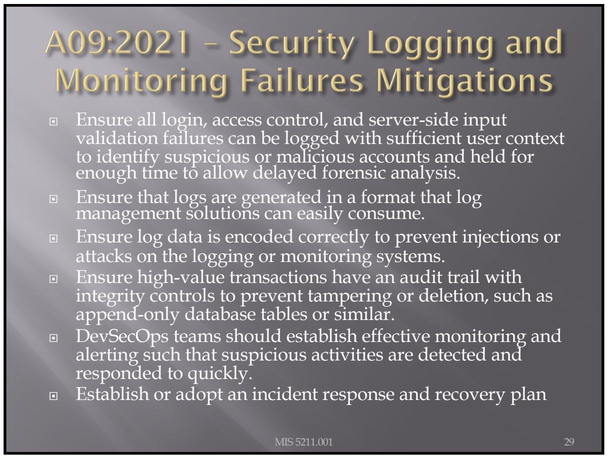
A09:2021 – Security Logging and Monitoring Failures

This category is to help detect, escalate, and respond to active breaches.

Insufficient logging, detection, monitoring, and active response occurs any time:

- Auditable events, such as logins, failed logins, and high-value transactions, are not logged.
- Warnings and errors generate no, inadequate, or unclear log messages.
- Logs of applications and APIs are not monitored for suspicious activity.
- Logs are only stored locally.
- Appropriate alerting thresholds and response escalation processes are not in place or effective.
- Penetration testing and scans by dynamic application security testing (DAST) tools do not trigger alerts.

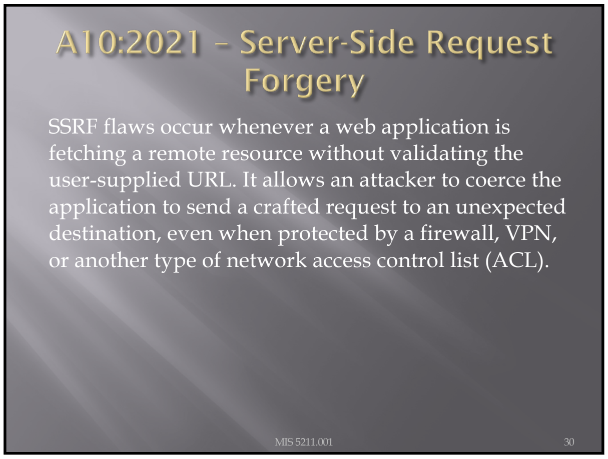
28



A09:2021 – Security Logging and Monitoring Failures Mitigations

- Ensure all login, access control, and server-side input validation failures can be logged with sufficient user context to identify suspicious or malicious accounts and held for enough time to allow delayed forensic analysis.
- Ensure that logs are generated in a format that log management solutions can easily consume.
- Ensure log data is encoded correctly to prevent injections or attacks on the logging or monitoring systems.
- Ensure high-value transactions have an audit trail with integrity controls to prevent tampering or deletion, such as append-only database tables or similar.
- DevSecOps teams should establish effective monitoring and alerting such that suspicious activities are detected and responded to quickly.
- Establish or adopt an incident response and recovery plan

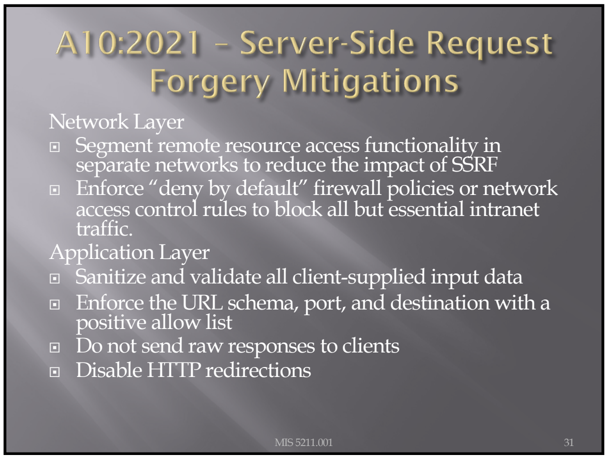
29



A10:2021 – Server-Side Request Forgery

SSRF flaws occur whenever a web application is fetching a remote resource without validating the user-supplied URL. It allows an attacker to coerce the application to send a crafted request to an unexpected destination, even when protected by a firewall, VPN, or another type of network access control list (ACL).

30



A10:2021 – Server-Side Request Forgery Mitigations

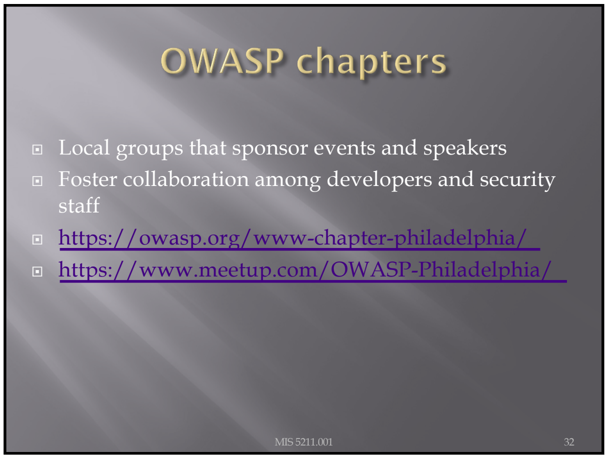
Network Layer

- Segment remote resource access functionality in separate networks to reduce the impact of SSRF
- Enforce “deny by default” firewall policies or network access control rules to block all but essential intranet traffic.

Application Layer

- Sanitize and validate all client-supplied input data
- Enforce the URL schema, port, and destination with a positive allow list
- Do not send raw responses to clients
- Disable HTTP redirections

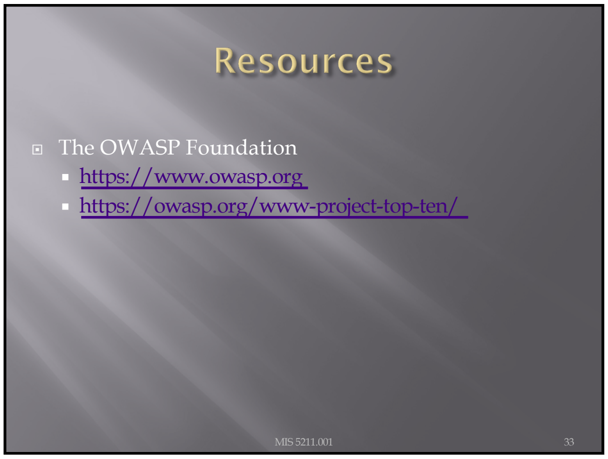
31



OWASP chapters

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

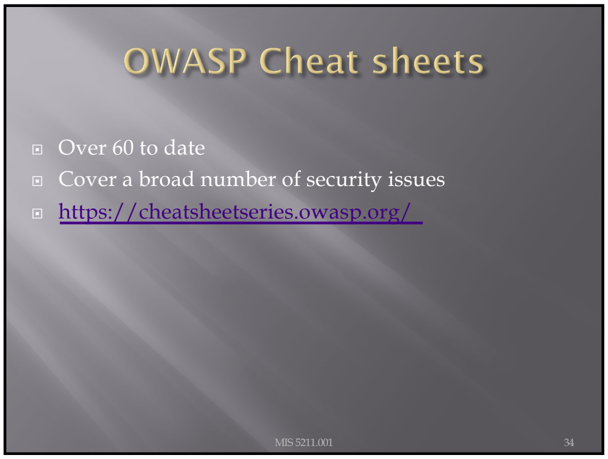
32



Resources

- The OWASP Foundation
  - https://www.owasp.org
  - https://owasp.org/www-project-top-ten/

33

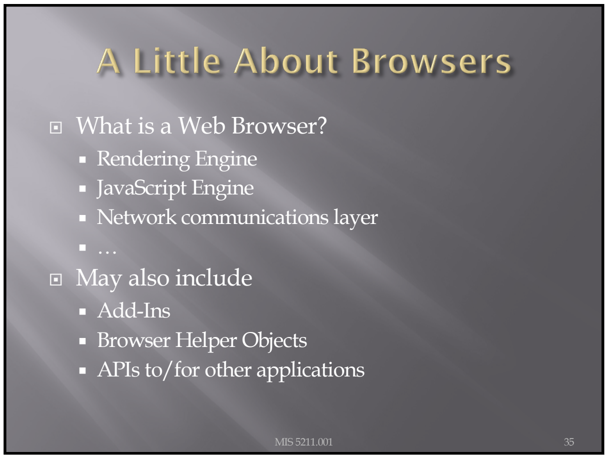


OWASP Cheat sheets

- Over 60 to date
- Cover a broad number of security issues
- https://cheatsheetseries.owasp.org/

MIS 5211.001 34

34

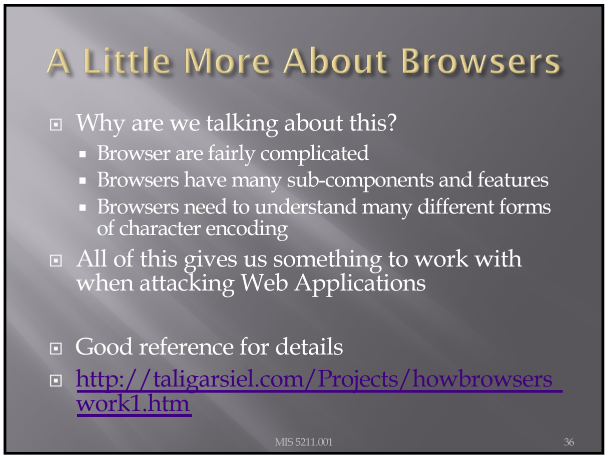


A Little About Browsers

- 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

MIS 5211.001 35

35



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

MIS 5211.001 36

36

Now What

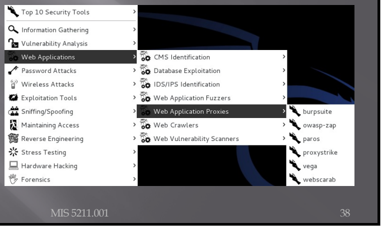
- So, all of this is interesting, but does that have to do with penetration testing
- Or, to put it another way. How de we exploit these issues?
- First step:

Intercepting Proxies

37

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



38

Some Rules for Our Use of Intercepting Proxies

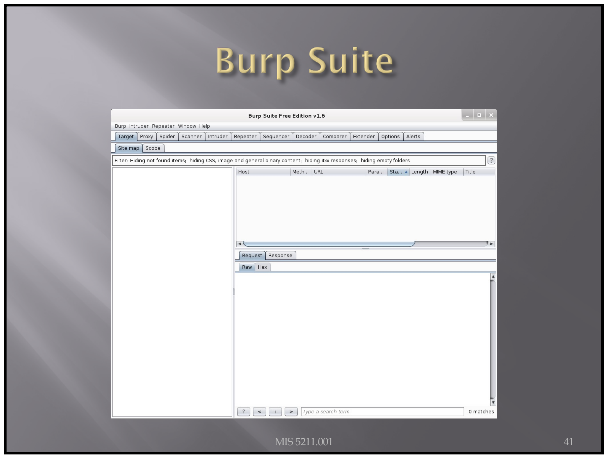
- For this course
- Monitor and record ONLY UNLESS YOU ARE ON A TEST SITE YOU OWN
- Do not inject or alter any traffic unless you personally own the web site.
- We'll save changing traffic in the next course

39

Burp Suite

- Start Burp Suite by logging in to Kali and selecting Burp Suite from:
- Kali Linux>Web Applications>Web Application Proxies>burpsuite
- For those interested in a video, here is a link to a YouTube video I found useful:
- https://www.youtube.com/watch?v=G3hpAeoZ4ek
- There are many others

40

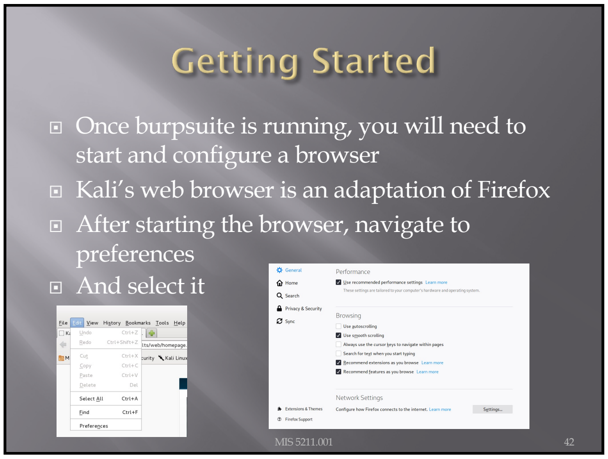


Burp Suite

Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Site map Scope
Host Meth... URL Para... Sta... Length MIME type Title
Request Response
Raw Hex
Type a search term
0 matches

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

41



Getting Started

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

Performance

☑ Use recommended performance settings Learn more

These settings are tailored to your computer's hardware and operating system.

Browsing

□ Use autoscrolling
☑ Use smooth scrolling
□ Always use the cursor keys to navigate within pages
□ Search for text when you start typing
☑ Recommend extensions as you browse Learn more
☑ Recommend features as you browse Learn more

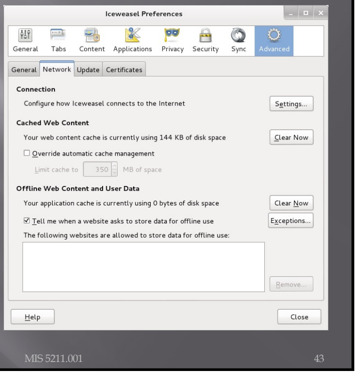
Network Settings

Configure how Firefox connects to the internet. Learn more

42

Configuring the Network Proxy

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



Connection

Configure how Iceweasel connects to the Internet

Cached Web Content

Your web content cache is currently using 144 KB of disk space

□ Override automatic cache management

Limit cache to 350 MB of space

Offline Web Content and User Data

Your application cache is currently using 0 bytes of disk space

☑ Tell me when a website asks to store data for offline use

The following websites are allowed to store data for offline use:

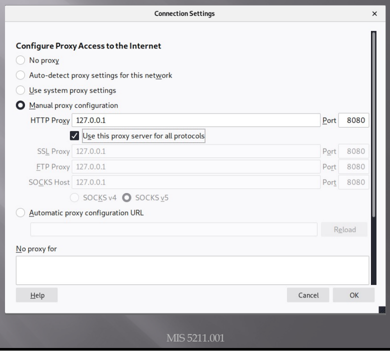
43

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

44

Configuring the Network Proxy



Configure Proxy Access to the Internet

○ No proxy

○ Auto-detect proxy settings for this network

○ Use system proxy settings

● Manual proxy configuration

HTTP Proxy 127.0.0.1 Port 8080

☑ Use this proxy server for all protocols

SSL Proxy 127.0.0.1 Port 8080

FTP Proxy 127.0.0.1 Port 8080

SOCKS Host 127.0.0.1 Port 8080

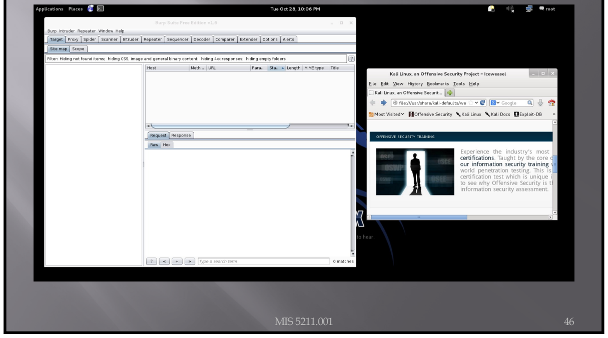
○ SOCKS v4 ● SOCKS v5

○ Automatic proxy configuration URL

No proxy for

45

Should Look Like This


Applications
Places
Tue Oct 28, 10:06 PM
root
Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Site map Scope
Host Meth... URL Para... Sta... Length MIME type Title
Request Response
Raw Hex
Type a search term
0 matches
Kali Linux, an Offensive Security Project – Iceweasel
File Edit View History Bookmarks Tools Help
Kali Linux, an Offensive Securit...
file:///usr/share/kali-defaults/we
Google
Most Visited Offensive Security Kali Linux Kali Docs Exploit-DB
OFFENSIVE SECURITY TRAINING

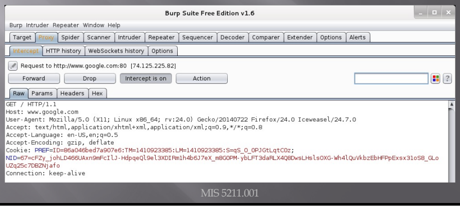
Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Experience the industry's most certifications. Taught by the core o our information security training world penetration testing. This is certification test which is unique i to see why Offensive Security is t information security assessment.

46

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


Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Raw Params Headers Hex

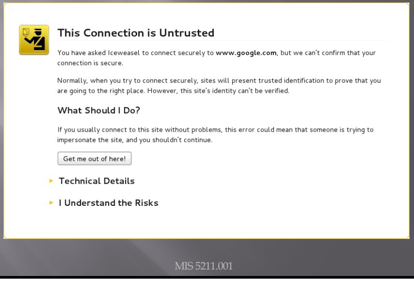
Request to http://www.google.com:80 [74.125.225.82]

```
GET / HTTP/1.1
Host: www.google.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:24.0) Gecko/20140722 Firefox/24.0 Iceweasel/24.7.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: PREF=ID=86a046bed7a907e6:TM=1410923385:LM=1410923385:S=qS_0_0PJGtLqtC0z;
NID=67=cFZy_johLD466UAxn9mFcIlJ-HdpqeQl9el3XDIRm1h4b6J7eX_m8G0PM-ybLFT3daRLX4Q8DwsLHslsOXG-Wh4lQuVkbzEbHFPpExsx31oS8_GLo
UZq25c7DBZNjafo
Connection: keep-alive
```

47

Browser Knows Something is Up

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



This Connection is Untrusted

You have asked Iceweasel to connect securely to **www.google.com**, but we can't confirm that your connection is secure.

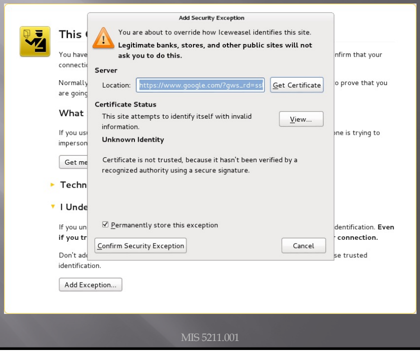
Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

48

Browser Knows Something is Up



Add Security Exception

You are about to override how Iceweasel identifies this site.

Legitimate banks, stores, and other public sites will not ask you to do this.

Server

Location: https://www.google.com/?gws_rd=ss [Get Certificate]

Certificate Status

This site attempts to identify itself with invalid information. [View...]

Unknown Identity

Certificate is not trusted, because it hasn't been verified by a recognized authority using a secure signature.

☑ Permanently store this exception

[Confirm Security Exception] [Cancel]

49

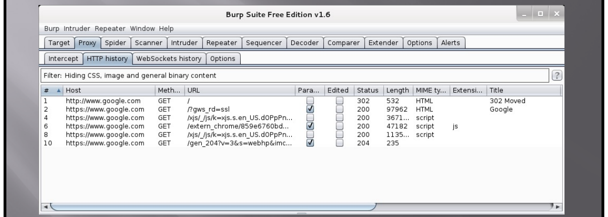
Continuing

- 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

50

Results

- Your traffic

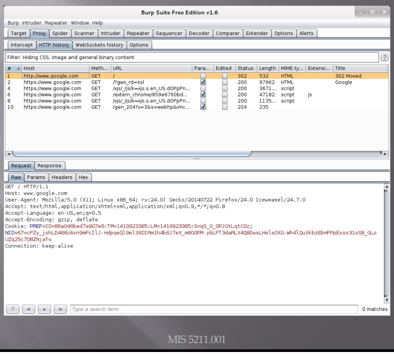

Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options

Filter: Hiding CSS, image and general binary content

#	Host	Meth...	URL	Para...	Edited	Status	Length	MIME ty...	Extensi...	Title
1	http://www.google.com	GET	/	☐	☐	302	532	HTML		302 Moved
2	https://www.google.com	GET	/?gws_rd=ssl	☑	☐	200	97962	HTML		Google
4	https://www.google.com	GET	/xjs/_/js/k=xjs.s.en_US.dOPpPn...	☐	☐	200	3671...	script		
6	https://www.google.com	GET	/extern_chrome/859e6760bd...	☑	☐	200	47182	script	js	
8	https://www.google.com	GET	/xjs/_/js/k=xjs.s.en_US.dOPpPn...	☐	☐	200	1135...	script		
10	https://www.google.com	GET	/gen_204?v=3&s=webhp&imc...	☑	☐	204	235			

51

More Results


Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Request Response
Raw Params Headers Hex
? < + > Type a search term 0 matches

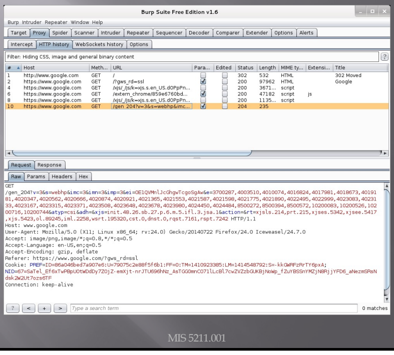
Filter: Hiding CSS, image and general binary content

#	Host	Meth...	URL	Para...	Edited	Status	Length	MIME ty...	Extensi...	Title
1	http://www.google.com	GET	/	☐	☐	302	532	HTML		302 Moved
2	https://www.google.com	GET	/?gws_rd=ssl	☑	☐	200	97962	HTML		Google
4	https://www.google.com	GET	/xjs/_/js/k=xjs.s.en_US.dOPpPn...	☐	☐	200	3671...	script		
6	https://www.google.com	GET	/extern_chrome/859e6760bd...	☑	☐	200	47182	script	js	
8	https://www.google.com	GET	/xjs/_/js/k=xjs.s.en_US.dOPpPn...	☐	☐	200	1135...	script		
10	https://www.google.com	GET	/gen_204?v=3&s=webhp&imc...	☑	☐	204	235			

```
GET / HTTP/1.1
Host: www.google.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:24.0) Gecko/20140722 Firefox/24.0 Iceweasel/24.7.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: PREF=ID=86a046bed7a907e6:TM=1410923385:LM=1410923385:S=qS_0_0PJGtLqtC0z;
NID=67=cFZy_johLD466UAxn9mFcIlJ-HdpqeQl9el3XDIRm1h4b6J7eX_m8G0PM-ybLFT3daRLX4Q8DwsLHsls0XG-Wh4lQuVkbzEbHFPpExsx31oS8_GLo
UZq25c7DBZNjafo
Connection: keep-alive
```

52

More Results


Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Request Response
Raw Params Headers Hex
? < + > Type a search term 0 matches

Filter: Hiding CSS, image and general binary content

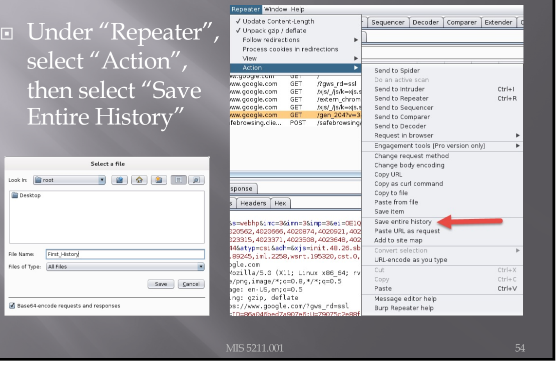
#	Host	Meth...	URL	Para...	Edited	Status	Length	MIME ty...	Extensi...	Title
1	http://www.google.com	GET	/	☐	☐	302	532	HTML		302 Moved
2	https://www.google.com	GET	/?gws_rd=ssl	☑	☐	200	97962	HTML		Google
4	https://www.google.com	GET	/xjs/_/js/k=xjs.s.en_US.dOPpPn...	☐	☐	200	3671...	script		
6	https://www.google.com	GET	/extern_chrome/859e6760bd...	☑	☐	200	47182	script	js	
8	https://www.google.com	GET	/xjs/_/js/k=xjs.s.en_US.dOPpPn...	☐	☐	200	1135...	script		
10	https://www.google.com	GET	/gen_204?v=3&s=webhp&imc...	☑	☐	204	235			

```
GET
/gen_204?v=3&s=webhp&imc=3&imn=3&imp=3&ei=0E1QVMnlJcGhgwTcgoSgAw&e=3700287,4003510,4010074,4016824,4017981,4018673,40191
81,4020347,4020562,4020666,4020874,4020921,4021365,4021553,4021587,4021598,4021775,4021890,4022495,4022999,4023083,40231
33,4023167,4023315,4023371,4023508,4023648,4023678,4023980,4024450,4024484,8500272,8500394,8500572,10200083,10200526,102
00716,10200744&atyp=csi&adh=&xjs=init.48.26.sb.27.p.6.m.5.ifl.3.jsa.1&action=&rt=xjsls.214,prt.215,xjses.5342,xjsee.5417
,xjs.5423,ol.89245,iml.2258,wsrt.195320,cst.0,dnst.0,rqst.7161,rspt.7242 HTTP/1.1
Host: www.google.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:24.0) Gecko/20140722 Firefox/24.0 Iceweasel/24.7.0
Accept: image/png,image/*;q=0.8,*/*;q=0.5
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.google.com/?gws_rd=ssl
Cookie: PREF=ID=86a046bed7a907e6:U=79075c2e88f5f6b1:FF=0:TM=1410923385:LM=1414548792:S=-kkGWRFzRrTY6pxA;
NID=67=SaTel_Ef6xTwPBpUOtWDdDy7ZOjZ-emXjt-nrJTU696hNz_AsTGG0mnC071lLcBl7cwZVZzbGUKBjNoWp_fZuYBSSnYMZjN8RjjYFD6_aNezmSRsN
dsk2W2Ut7ozs6TF
Connection: keep-alive
```

53

Saving Our Results

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

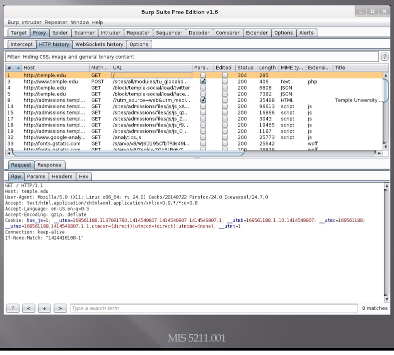


54

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

Temple.edu


Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Request Response
Raw Params Headers Hex
?
<
+
>
Type a search term
0 matches

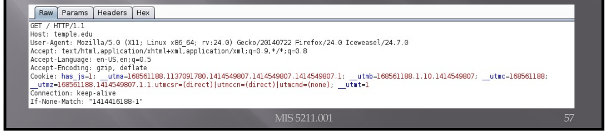
Filter: Hiding CSS, image and general binary content

# ▲	Host	Meth...	URL	Para...	Edited	Status	Length	MIME ty...	Extensi...	Title
1	http://temple.edu	GET	/	☐	☐	304	285			
3	http://www.temple.edu	POST	/sites/all/modules/tu_global/d...	☑	☐	200	406	text	php	
4	http://temple.edu	GET	/block/temple-social/load/twitter	☐	☐	200	6808	JSON		
5	http://temple.edu	GET	/block/temple-social/load/face...	☐	☐	200	7382	JSON		
8	http://admissions.templ...	GET	/?utm_source=web&utm_medi...	☑	☐	200	35498	HTML		Temple University ...
14	http://admissions.templ...	GET	/sites/admissions/files/js/js_xA...	☐	☐	200	96613	script	js	
15	http://admissions.templ...	GET	/sites/admissions/files/js/js_qz...	☐	☐	200	16866	script	js	
17	http://admissions.templ...	GET	/sites/admissions/files/js/js_Z...	☐	☐	200	3043	script	js	
18	http://admissions.templ...	GET	/sites/admissions/files/js/js_f9...	☐	☐	200	19465	script	js	
19	http://admissions.templ...	GET	/sites/admissions/files/js/js_Cl...	☐	☐	200	1187	script	js	
32	http://www.google-analy...	GET	/analytics.js	☐	☐	200	25773	script	js	
33	http://fonts.gstatic.com	GET	/s/arvo/v8/WJ6D195CfbTRlls49l...	☐	☐	200	25642		woff	
39	http://fonts.gstatic.com	GET	/s/arvo/v8/7solcx-ZOo6LBqlyZ	☐	☐	200	26879		woff	

```
GET / HTTP/1.1
Host: temple.edu
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:24.0) Gecko/20140722 Firefox/24.0 Iceweasel/24.7.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: has_js=1; __utma=168561188.1137091780.1414549807.1414549807.1414549807.1; __utmb=168561188.1.10.1414549807; __utmc=168561188;
__utmz=168561188.1414549807.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none); __utmt=1
Connection: keep-alive
If-None-Match: "1414416188-1"
```

Some Basics

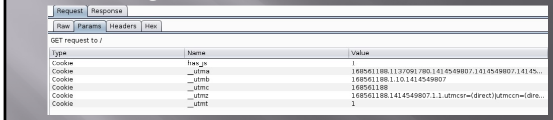
- What can we tell from this?
- First we can see what we are telling temple about us
  - Web Browser is Iceweasel, a derivative of Firefox
  - What versions we are running
  - Cookies
  - What exactly is If-None-Match: “1414416188-1”?



```
GET / HTTP/1.1
Host: temple.edu
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:24.0) Gecko/20140722 Firefox/24.0 Iceweasel/24.7.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: has_js=1; __utma=168561188.1137091780.1414549807.1414549807.1414549807.1; __utmb=168561188.1.10.1414549807; __utmc=168561188;
__utmz=168561188.1414549807.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none); __utmt=1
Connection: keep-alive
If-None-Match: "1414416188-1"
```

But Wait, There's More

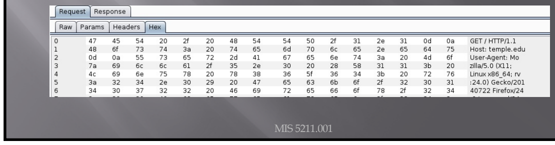
- As Darth Vader says "Come to the Dark Side, We've got Cookies"



GET request to /

Type	Name	Value
Cookie	has_js	1
Cookie	__utma	168561188.1137091780.1414549807.1414549807.14145...
Cookie	__utmb	168561188.1.10.1414549807
Cookie	__utmc	168561188
Cookie	__utmz	168561188.1414549807.1.1.utmcsr=(direct)|utmccn=(dire...
Cookie	__utmt	1

- Or worse "Hex"

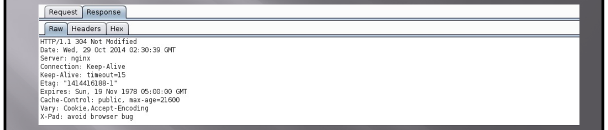


```
0    47  45  54  20  2f  20  48  54    54  50  2f  31  2e  31  0d  0a   GET / HTTP/1.1
1    48  6f  73  74  3a  20  74  65    6d  70  6c  65  2e  65  64  75   Host: temple.edu
2    0d  0a  55  73  65  72  2d  41    67  65  6e  74  3a  20  4d  6f   User-Agent: Mo
3    7a  69  6c  6c  61  2f  35  2e    30  20  28  58  31  31  3b  20   zilla/5.0 (X11;
4    4c  69  6e  75  78  20  78  38    36  5f  36  34  3b  20  72  76   Linux x86_64; rv
5    3a  32  34  2e  30  29  20  47    65  63  6b  6f  2f  32  30  31   :24.0) Gecko/201
6    34  30  37  32  32  20  46  69    72  65  66  6f  78  2f  32  34   40722 Firefox/24
```

58

We've Got Both Sides

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

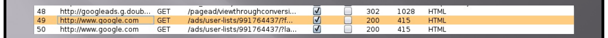


```
HTTP/1.1 304 Not Modified
Date: Wed, 29 Oct 2014 02:30:39 GMT
Server: nginx
Connection: Keep-Alive
Keep-Alive: timeout=15
Etag: "1414416188-1"
Expires: Sun, 19 Nov 1978 05:00:00 GMT
Cache-Control: public, max-age=21600
Vary: Cookie,Accept-Encoding
X-Pad: avoid browser bug
```

59

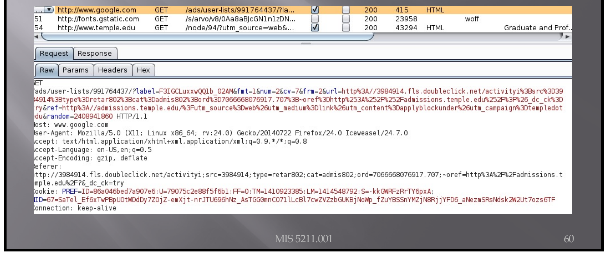
A Few Interesting Things

- Google Adds



48	http://googleads.g.doub...	GET	/pagead/viewthroughconversi...	☑	☐	302	1028	HTML
49	http://www.google.com	GET	/ads/user-lists/991764437/?f...	☑	☐	200	415	HTML
50	http://www.google.com	GET	/ads/user-lists/991764437/?la...	☑	☐	200	415	HTML

- Other outside references



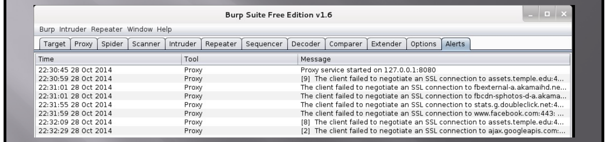
...	http://www.google.com	GET	/ads/user-lists/991764437/?la...	☑	☐	200	415	HTML		
51	http://fonts.gstatic.com	GET	/s/arvo/v8/0Aa8aBJcGN1n1zDN...	☐	☐	200	23958		woff	
54	http://www.temple.edu	GET	/node/94/?utm_source=web&...	☑	☐	200	43294	HTML		Graduate and Prof...

```
ET
ads/user-lists/991764437/?label=F3IGCLuxxwQQ1b_02AM&fmt=1&num=2&cv=7&frm=2&url=http%3A//3984914.fls.doubleclick.net/activityi%3Bsrc%3D39
4914%3Btype%3Dretar802%3Bcat%3Dadmis802%3Bord%3D7066668076917.707%3B~oref%3Dhttp%253A%252F%252Fadmissions.temple.edu%252F%3F%26_dc_ck%3D
ry&ref=http%3A//admissions.temple.edu/%3Futm_source%3Dweb%26utm_medium%3Dlink%26utm_content%3Dapplyblockunder%26utm_campaign%3Dtempledot
du&random=2408941860 HTTP/1.1
ost: www.google.com
ser-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:24.0) Gecko/20140722 Firefox/24.0 Iceweasel/24.7.0
ccept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
ccept-Language: en-US,en;q=0.5
ccept-Encoding: gzip, deflate
eferer:
ttp://3984914.fls.doubleclick.net/activityi;src=3984914;type=retar802;cat=admis802;ord=7066668076917.707;~oref=http%3A%2F%2Fadmissions.t
mple.edu%2F?&_dc_ck=try
ookie: PREF=ID=86a046bed7a907e6:U=79075c2e88f5f6b1:FF=0:TM=1410923385:LM=1414548792:S=-kkGWRFzRrTY6pxA;
ID=67=SaTel_Ef6xTwPBpUOtWDdDy7ZOjZ-emXjt-nrJTU696hNz_AsTGG0mnC071lLcBl7cwZVZzbGUKBjNoWp_fZuYBSSnYMZjN8RjjYFD6_aNezmSRsNdsk2W2Ut7ozs6TF
onnection: keep-alive
```

60

Check The Alerts

- A few things to look at



Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts

```
Time                    Tool      Message
22:30:45 28 Oct 2014    Proxy     Proxy service started on 127.0.0.1:8080
22:30:59 28 Oct 2014    Proxy     [9]  The client failed to negotiate an SSL connection to assets.temple.edu:4...
22:31:01 28 Oct 2014    Proxy     The client failed to negotiate an SSL connection to fbexternal-a.akamaihd.ne...
22:31:01 28 Oct 2014    Proxy     The client failed to negotiate an SSL connection to fbcdn-sphotos-d-a.akama...
22:31:55 28 Oct 2014    Proxy     The client failed to negotiate an SSL connection to stats.g.doubleclick.net:4...
22:31:59 28 Oct 2014    Proxy     The client failed to negotiate an SSL connection to www.facebook.com:443: ...
22:32:09 28 Oct 2014    Proxy     [8]  The client failed to negotiate an SSL connection to assets.temple.edu:4...
22:32:29 28 Oct 2014    Proxy     [2]  The client failed to negotiate an SSL connection to ajax.googleapis.com:...
```

61

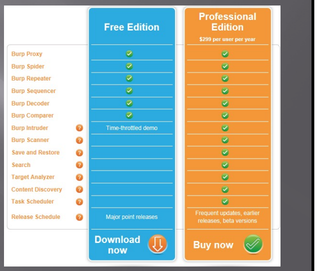
What Now

- 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)

62

A Few More Things

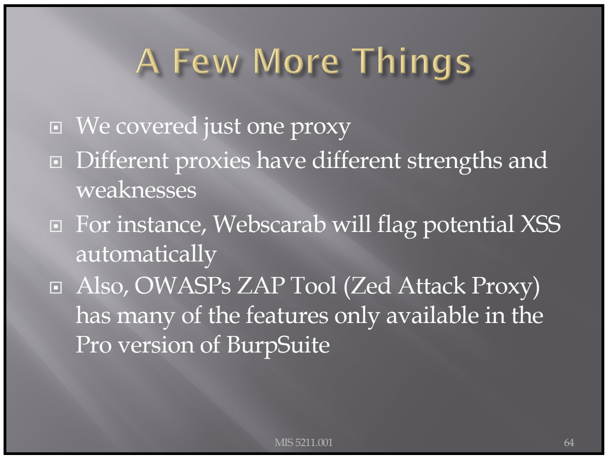
- This is the "Free" version of burpsuite
- Some of the more interesting features are turned off or limited
  - Scanner
  - Intruder



	Free Edition	Professional Edition $299 per user per year
Burp Proxy	✓	✓
Burp Spider	✓	✓
Burp Repeater	✓	✓
Burp Sequencer	✓	✓
Burp Decoder	✓	✓
Burp Comparer	✓	✓
Burp Intruder ?	Time-throttled demo	✓
Burp Scanner ?		✓
Save and Restore ?		✓
Search ?		✓
Target Analyzer ?		✓
Content Discovery ?		✓
Task Scheduler ?		✓
Release Schedule ?	Major point releases	Frequent updates, earlier releases, beta versions
	Download now	Buy now

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

63

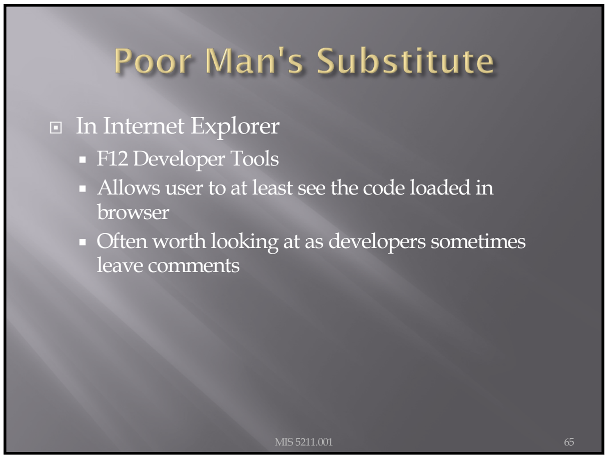


A Few More Things

- 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

MIS 5211.001 64

64

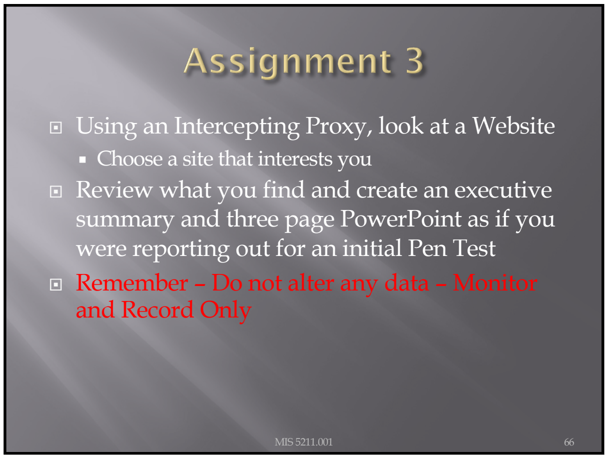


Poor Man's Substitute

- 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

MIS 5211.001 65

65

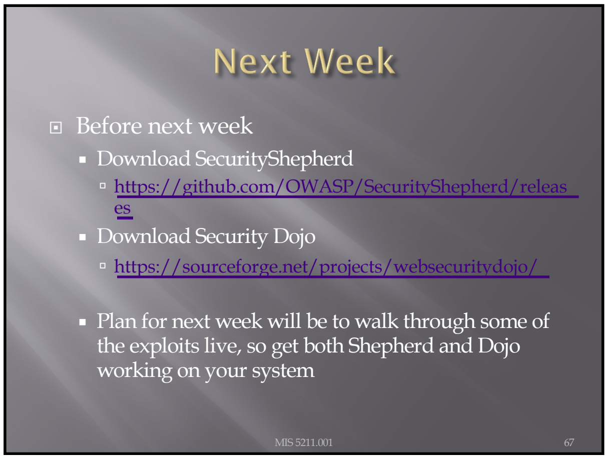


Assignment 3

- 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

MIS 5211.001 66

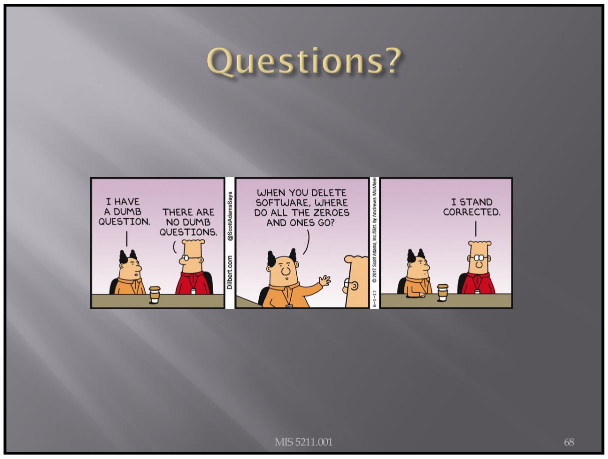
66



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

67



Questions?

I HAVE A DUMB QUESTION.
THERE ARE NO DUMB QUESTIONS.
@ScottAdamsSays
Dilbert.com
WHEN YOU DELETE SOFTWARE, WHERE DO ALL THE ZEROES AND ONES GO?
I STAND CORRECTED.

68