

# Assignment 4 Using and Understanding burp suite

Target



Username

Password

Login

Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project

Hint: default username is 'admin' with password 'password'

IP 192.168.1.231

2. Intruder attack of http://192.168.1.231 - Temporary attack - Not saved to project file

AttackSaveColumns

ResultsPositionsPayloadsResource poolSettings

Filter: Showing all items

Request	Position	Payload	Status code	Error	Timeout	Length	Comment
8	1	spring2013	302	<input type="checkbox"/>	<input type="checkbox"/>	392	
9	1	spring2014	302	<input type="checkbox"/>	<input type="checkbox"/>	392	
10	1	spring2013	302	<input type="checkbox"/>	<input type="checkbox"/>	392	
11	1	Summer2017	302	<input type="checkbox"/>	<input type="checkbox"/>	391	
12	1	Summer2016	302	<input type="checkbox"/>	<input type="checkbox"/>	391	
13	1	Summer2015	302	<input type="checkbox"/>	<input type="checkbox"/>	392	
14	1	Summer2014	302	<input type="checkbox"/>	<input type="checkbox"/>	392	
15	1	Summer2013	302	<input type="checkbox"/>	<input type="checkbox"/>	391	
16	1	summer2017	302	<input type="checkbox"/>	<input type="checkbox"/>	391	
17	1	summer2016	302	<input type="checkbox"/>	<input type="checkbox"/>	391	
18	1	summer2015	302	<input type="checkbox"/>	<input type="checkbox"/>	391	
19	1	summer2014	302	<input type="checkbox"/>	<input type="checkbox"/>	391	
20	1	summer2013	302	<input type="checkbox"/>	<input type="checkbox"/>	391	

RequestResponse

PrettyRawHex

1 POST /dvwa/login.php HTTP/1.1

2 Host: 192.168.1.231

3 User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:109.0) Gecko/20100101 Firefox/115.0

4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8

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

6 Accept-Encoding: gzip, deflate

7 Content-Type: application/x-www-form-urlencoded

8 Content-Length: 35

9 Origin: http://192.168.1.231

10 Connection: keep-alive

11 Referer: http://192.168.1.231/dvwa/login.php

12 Cookie: security=high; PHPSESSID=050b104ae3bc48abbaa21a7be877062c

?

⚙

⬅

➡

Search...

0 highlights

28 of 444

6. Intruder attack of http://192.168.1.231 - Temporary attack - Not saved to project file

Attack Save Columns

Results Positions Payloads Resource pool Settings

Filter: Showing all items

Request ^	Payload 1	Payload 2	Status code	Error	Timeout	Length	Comment
0			302	<input type="checkbox"/>	<input type="checkbox"/>	392	
1	admin	admin	302	<input type="checkbox"/>	<input type="checkbox"/>	392	
2	password	admin	302	<input type="checkbox"/>	<input type="checkbox"/>	392	
3	admin	password	302	<input type="checkbox"/>	<input type="checkbox"/>	392	
4	password	password	302	<input type="checkbox"/>	<input type="checkbox"/>	392	

Request Response

Pretty Raw Hex

```

1 POST /dvwa/login.php HTTP/1.1
2 Host: 192.168.1.231
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 44
9 Origin: http://192.168.1.231
10 Connection: keep-alive
11 Referer: http://192.168.1.231/dvwa/login.php
12 Cookie: security=high; PHPSESSID=050b104ae3bc48abbbaa21a7be877062c
13 Upgrade-Insecure-Requests: 1
14

```

Finished

1. Open Burp Suite and start the proxy.
2. Open your web browser and navigate to the web application you want to test.
3. Click on the Intercept button in the Burp Suite toolbar.
4. Enter your credentials to log in to the web application.
5. Click on the Forward button to send the request to the web server.
6. In the Burp Suite Request tab, modify the request as needed.
7. Click on the Forward button to send the modified request to the web server.
8. In the Burp Suite Response tab, view the response from the web server.

[Home](#)[Instructions](#)[Setup](#)[Brute Force](#)[Command Execution](#)[CSRF](#)[File Inclusion](#)[SQL Injection](#)[SQL Injection \(Blind\)](#)[Upload](#)[XSS reflected](#)[XSS stored](#)[DVWA Security](#)[PHP Info](#)[About](#)[Logout](#)

## Welcome to Damn Vulnerable Web App!

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

### WARNING!

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing [XAMPP](#) onto a local machine inside your LAN which is used solely for testing.

### Disclaimer

We do not take responsibility for the way in which any one uses this application. We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

### General Instructions

The help button allows you to view hits/tips for each vulnerability and for each security level on their respective page.

Successfully logged in!!!!!!