

[Home](#)[Instructions](#)[Setup / Reset DB](#)[Brute Force](#)[Command Injection](#)[CSRF](#)[File Inclusion](#)[File Upload](#)[Insecure CAPTCHA](#)[SQL Injection](#)[SQL Injection \(Blind\)](#)[Weak Session IDs](#)[XSS \(DOM\)](#)[XSS \(Reflected\)](#)[XSS \(Stored\)](#)[CSP Bypass](#)[JavaScript](#)[Authorisation Bypass](#)[Open HTTP Redirect](#)[DVWA Security](#)[PHP Info](#)[About](#)[Logout](#)

DVWA Security

Security Level

Security level is currently: **low**.

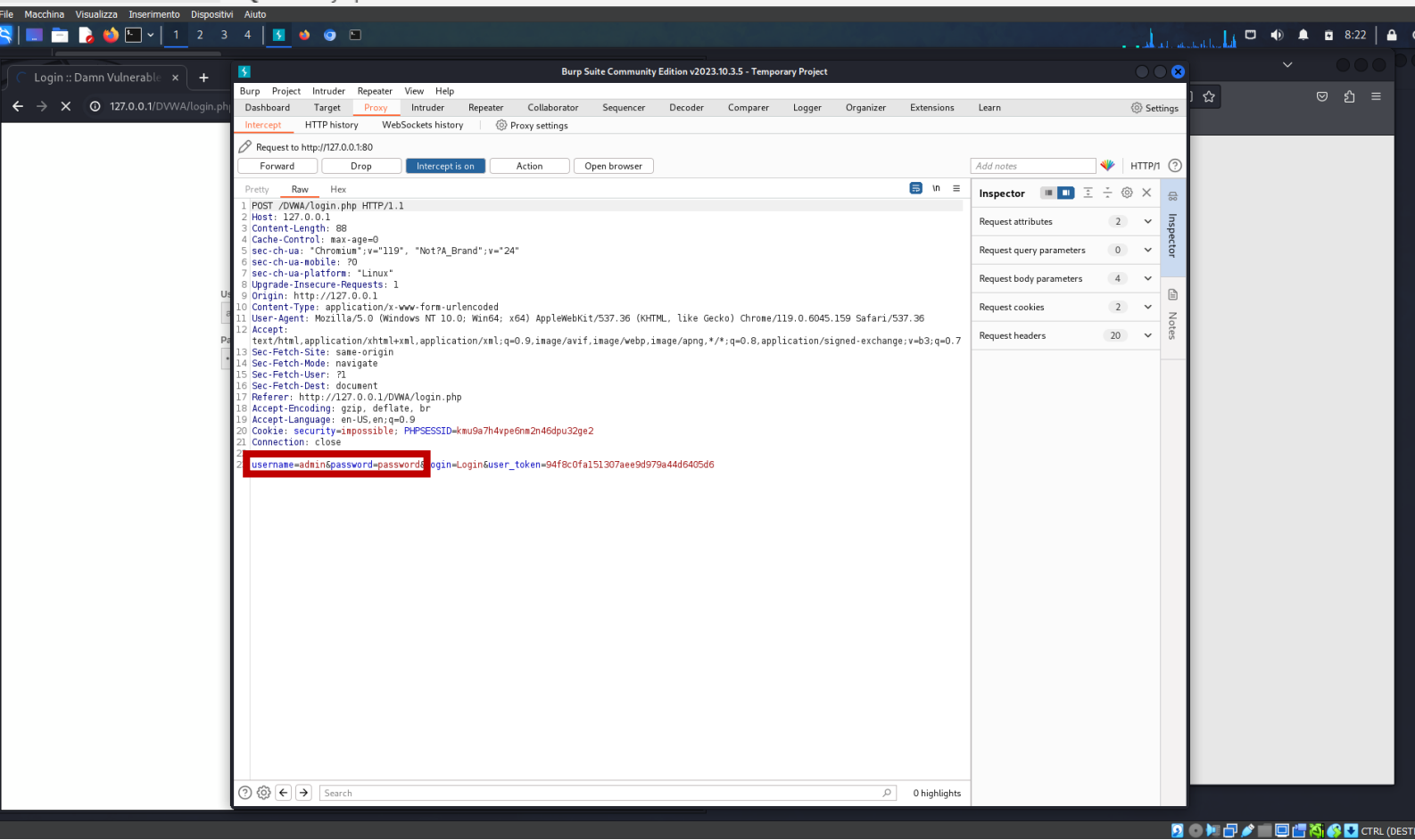
You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

1. Low - This security level is completely vulnerable and **has no security measures at all**. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of **bad security practices**, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of **harder or alternative bad practices** to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare the vulnerable source code to the secure source code.
Prior to DVWA v1.9, this level was known as 'high'.

Low  Submit

Security level set to low

Username: admin
Security Level: low
Locale: en
SQLi DB: mysql



The screenshot shows a web browser window with the URL `127.0.0.1/DVWA/login.php`. The browser's developer tools are open, showing the network tab with a request to `http://127.0.0.1:80`. The request is a POST to `/DVWA/login.php` with the following headers:

```
POST /DVWA/login.php HTTP/1.1
Host: 127.0.0.1
Content-Length: 88
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="119", "Not?A_Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
Origin: http://127.0.0.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://127.0.0.1/DVWA/login.php
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: security-impossible; PHPSESSID=kmu9a7h4pe6m2n46dpu32qe2
Connection: close
```

The request body is `username=admin&password=password`. The Burp Suite interface is visible in the background, showing the request details and the 'Intercept' tab.

1 x +

Send

Cancel

< >

Target: http://127.0.0.1

HTTP/1

Request

PrettyRawHex

1 GET /DVWA/index.php HTTP/1.1

2 Host: 127.0.0.1

3 Cache-Control: max-age=0

4 sec-ch-ua: "Chromium";v="119", "Not?A_Brand";v="24"

5 sec-ch-ua-mobile: ?0

6 sec-ch-ua-platform: "Linux"

7 Upgrade-Insecure-Requests: 1

8 Origin: http://127.0.0.1

9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)

10 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159 Safari/537.36

11 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

12 Sec-Fetch-Site: same-origin

13 Sec-Fetch-Mode: navigate

14 Sec-Fetch-User: ?1

15 Sec-Fetch-Dest: document

16 Referer: http://127.0.0.1/DVWA/login.php

17 Accept-Encoding: gzip, deflate, br

18 Accept-Language: en-US,en;q=0.9

19 Cookie: security=impossible; PHPSESSID=kmu9a7h4vpe6nm2n46dpu32ge2

20 Connection: close

21

Response

PrettyRawHexRender

1 HTTP/1.1 200 OK

2 Date: Wed, 06 Dec 2023 13:22:55 GMT

3 Server: Apache/2.4.58 (Debian)

4 Expires: Tue, 23 Jun 2009 12:00:00 GMT

5 Cache-Control: no-cache, must-revalidate

6 Pragma: no-cache

7 Vary: Accept-Encoding

8 Content-Length: 6103

9 Connection: close

10 Content-Type: text/html; charset=utf-8

11

12 <!DOCTYPE html>

13

14 <html lang="en-GB">

15

16 <head>

17 <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />

18

19 <title>

20 Welcome :: Damn Vulnerable Web Application (DVWA)

21 </title>

22

23 <link rel="stylesheet" type="text/css" href="dvwa/css/main.css" />

24

25 <link rel="icon" type="image/ico" href="favicon.ico" />

26

27 <script type="text/javascript" src="dvwa/js/dvwaPage.js">

28 </script>

29

30 </head>

31

32 <body class="home">

33 <div id="container">

34

35 <div id="header">

36

37

38

39 </div>

40

41 <div id="main_menu">

42 <div id="main_menu_padded">

43 <ul class="menuBlocks">

44 <li class="selected">

45

46

47

48

49

50

51

52

53

54

55

56

57

58

59

60

61

62

63

64

65

66

67

68

69

70

71

72

73

74

75 </div>

76 <!--div id="content"-->

77

78 <div id="footer">

79

80 </div>

81

82 </body>

83 </html>

Inspector

Request attributes2

Request query parameters0

Request body parameters0

Request cookies2

Request headers18

Response headers9

0 highlights

0 highlights

2 x +

Send

Cancel

< >

Target: http://127.0.0.1

HTTP/1

Request

PrettyRawHex

1 GET /DVWA/login.php HTTP/1.1

2 Host: 127.0.0.1

3 Cache-Control: max-age=0

4 sec-ch-ua: "Chromium";v="119", "Not?A_Brand";v="24"

5 sec-ch-ua-mobile: ?0

6 sec-ch-ua-platform: "Linux"

7 Upgrade-Insecure-Requests: 1

8 Origin: http://127.0.0.1

9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)

10 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159 Safari/537.36

11 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

12 Sec-Fetch-Site: same-origin

13 Sec-Fetch-Mode: navigate

14 Sec-Fetch-User: ?1

15 Sec-Fetch-Dest: document

16 Referer: http://127.0.0.1/DVWA/login.php

17 Accept-Encoding: gzip, deflate, br

18 Accept-Language: en-US,en;q=0.9

19 Cookie: security=impossible; PHPSESSID=kmu9a7h4vpe6nm2n46dpu32ge2

20 Connection: close

21

Response

PrettyRawHexRender

47 Username

48 <label>

49 <input type="text" class="loginInput" size="20" name="username">

50

51

52 <label for="pass">

53 Password

54 </label>

55 <input type="password" class="loginInput" AUTOCOMPLETE="off" size="20" name="password">

56

57

58 <p class="submit">

59 <input type="submit" value="Login" name="Login">

60 </p>

61

62 </fieldset>

63

64 <input type="hidden" name="user_token" value="8002c16dale4eef2eacc338203cc010e" />

65

66 </form>

67

68

69

70 <div class="message">

71 Login failed

72

73

74

75

76

77

78

79

80

81 </div>

82 <!--div id="content"-->

83

84 <div id="footer">

85

86 </div>

87

Inspector

Request attributes2

Request query parameters0

Request body parameters0

Request cookies2

Request headers18

Response headers9

0 highlights

0 highlights