


kali-linux-2022.3-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Auto

1 2 3 4

Login - Damn Vulnerable x +

127.0.0.1/DVWA/login.php



Username
admin

Password

Login

You have logged out

Damn Vulnerable Web Application (DVWA)

Burp Suite Community Edition v2022.7.1 - Temporary Project

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

Request to http://127.0.0.1:80

Forward Drop Microsoft icon Action Open Browser

Request Headers

1 POST /DVWA/login.php HTTP/1.1
2 Host: 127.0.0.1
3 Content-Length: 88
4 Cache-Control: max-age=0
5 sec-ch-ua: "Chromium";v="103", ".Not/A)Brand";v="99"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Linux"
8 Upgrade-Insecure-Requests: 1
9 Origin: http://127.0.0.1
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.134 Safari/537.36
12 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=0.9
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Referer: http://127.0.0.1/DVWA/login.php
18 Accept-Encoding: gzip, deflate
19 Accept-Language: en-US,en;q=0.9
20 Cookie: PHPSESSID=7abae0b0d0ff1cadgn1f0ff; security=impossible
21 Connection: close
22
23 username=admin&password=password&Login=Login&user_token=2519581ba425c5f9611069f105a0ac94

Inspector

Request Attributes
Request Query Parameters
Request Body Parameters
Request Cookies
Request Headers
Response Headers

Burp Suite Community Edition v2022.7.1 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

1 x +

Send Cancel < >

Target: http://127.0.0.1

Request

Pretty Raw Hex

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="103", ".Not/A)Brand";v="99"
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) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.134 Safari/537.36
10 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=0.9
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: http://127.0.0.1/DVWA/login.php
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18 Cookie: PHPSESSID=6eqkqmt5k7Vqois147dm9890; security=impossible
19 Connection: close
20
21

Response

Pretty Raw Hex Render

52
53 <p class="submit">
54 <input type="submit" value="Login" name="Login">
55 </p>
56
57 </fieldset>
58
59 <input type="hidden" name="user_token" value='
60 9d15d5c0c704e732a277b27d9c9be124' />
61 </form>
62
63

64
65 <div class="message">
66 Login failed
67 </div>
68
69

70
71

72

73
74 <!-- -->
75 </div>
76 <!--<div id="content">-->
77
78 <div id="footer">
79
80
81 _blank
82 Damn Vulnerable Web Application (DVWA)
83 </p>
84 </div>
85 <!--<div id="footer">-->
86
87 </div>
88 <!--<div id="wrapper">-->
89

Inspector

Request Attributes 2
Request Query Parameters 0
Request Body Parameters 0
Request Cookies 2
Request Headers 18
Response Headers 9

0 matches

0 matches

1,745 byte

1 x +

SendCancel<>

T

Request

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="103", ".Not/A)Brand";v="99"

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) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.134 Safari/537.36

10 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=0.9

11 Sec-Fetch-Site: same-origin

12 Sec-Fetch-Mode: navigate

13 Sec-Fetch-User: ?1

14 Sec-Fetch-Dest: document

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

16 Accept-Encoding: gzip, deflate

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

18 Cookie: PHPSESSID=fvabpkm679d8fflcmdgonlf85v; security=impossible

19 Connection: close

20

21

Response

1 HTTP/1.1 200 OK

2 Date: Wed, 09 Nov 2022 13:56:24 GMT

3 Server: Apache/2.4.54 (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: 6416

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) v1.10

21 *Development*

22 </title>

23

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

25

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

27

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

29 </script>

30

31 </head>

32

33 <body class="home">

34 <div id="container">

35

36 <div id="header">

37

38

39

40 </div>

41

42 <div id="main_menu">

43

44

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

76

77

78

79

80

81

82

83

84

85

86

87

88

89

90

91

92

93

94

95

96

97

98

99

100

0 matches

0 matches

Done