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: "2AvVhdsgUs0FSA3SDFAdag=="));
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]

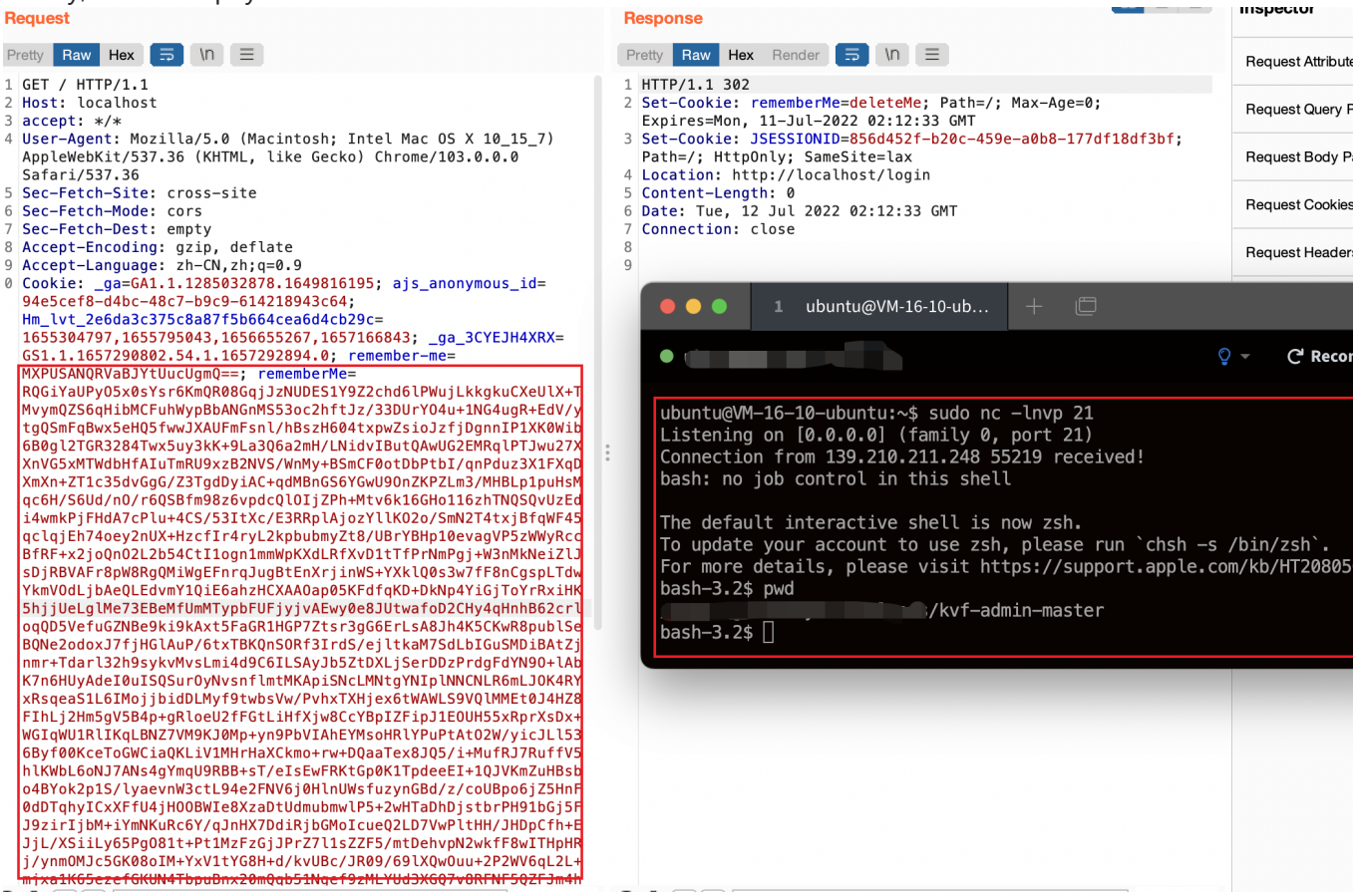
Forward | Drop | Intercept is on | Action | Open Browser

Pretty Raw Hex \n

```
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_3CYEJH4XRX=
   GS1.1.1657290802.54.1.1657292894.0; remember-me=MXPUSANQRVaBJYtUucUgmQ==; JSESSIONID=b45fa52f-4c55-43e6-8cb7-9c02d6447748;
   rememberMe=
   1twtHQ4xolEl4r3ffH6NSKt3sjexDQ9YBCvUNCiuR8jT0O1NK9vgvp1p/p0mkBrexEsHNcd+VepVx59PjRlM3ODHszv8vclUP9UL095bTXqhURcY8bkwbRls6nWsgtJxyaL
   t4NfNbLN52dfCct0EV38LaUJJquTx+ma0w4r0iPkm1aq/JZqdFuu1WtlK6hfLC2zC+PZHsFZSkbbX+TFPiUKSxbcqZmPipZk6ERQOIHTUUSzFyAAGRmTiM42E5GPAEG6SMl
   l3NZpstCFpURUkNvLBIZCeI5EMRWq2K/YyMgi17LXL8FnBVFDM7ATWJkGAmEbKHZXF/+DXLSnXlFJnmbkAHNOLJv2c3QcGg1dXwK0x4w4egiAeg2nxV3ork5HjcuC717FgH
   N6oIUgmobg45C0X2mOq+voZ5Ta5tYCSWiTwPfR4rO78lg1N9hcHbqlLcOBLmXBW7LN9R1o94PbPsK7JL5w0JhVL0xXHsK5tdR/98ysfxL4EQElUgQ29TG0ZjYsfSSPT5NA8
   8Ki7VdUlcZAfPLoVJQ070gUnzqSG4SYbl1OXBQ+NeCEpGTzp6VRVnJ7OARZZBsSCRW7vTN2TZ4iejPC/a/ZLFKM8FH5HKCkksY10j6jWz1j/Z0XVL+DjOgcgfDFUxB3bmBi
   pwz4RrHQsM6h+Yn7RuQvyyV5vgGYJvp5fMKpUQe8y5Ab3zjPiYkguSF2gRMcDAruTMgirkGRxPgVTNzDX0hthiGX44/h1phoePLb5S/i1vdrs3VkAKqg4vbSY8PHIAymzzB
   wuUkIBLniHi7ZJh9SVfqXJqJKLjtdlhj48gPlY50a/iWBV32DI2GTuw6y+S2edXu7tdvnDDJqwrLhUAMYkKkKQlt1QsuQm4bVSwfafOB3NrCsDDEkecS+/JoeaxAhuprMVT
   JuzBk0BEtAgvLk6yPybIVbCZAj4uyEO5ytMbKgCPtWPqHjs1MIlo63Cq2AQxwV0iD9N3gtUtuqf4Hbw/bNyfrF7dwYngaMp7wfJSrBRQjzOpkqvysxskjyKx0bdIIm09/c9
   Ad8UYqLyrXpAyY6DECkUqVa81chdvJDstMhxjkfkL4GYjXnwJMiHf4EF4V0bwKV0d5IrsjVeFz6iCadvm7GLeJY5g7j200flN9s11+l6VClehETBl0vzVayabXDl26vUTOs
   RTHSkRvWuZ4cAjx0GnQNinkqqvQEB+EB7bbL8Ec43TogFQ0ger762VtQQGbr8Akxxwb GIe0Ykchj+PEgnku89XBG3aMiLH2ptPVPYXd/krVb09UtnnnsGLsLw5p91QhHkEF
   n7MJOQCOl11uD36ngpUY3TY4GOcwOqTK1SmNWA6eg5zsz5D+oxlmYj+lu6rLfcbdCc1u7FAnhrqG1c4vNyFphzdrc76+b+mI91s6leummELtq4oYHZKeIf5G4/VXoDjisOK
   lm/dZaHCTIN0h1Imlu51SXUaPp4Y5jzKNec42Ecy3nPLDG+/1tx7qgDm/cmUmIrffbGmhbjw1MbSrTstQxnUfeaVaxgobjEQek3Yvb1ePU7jU6UPah7U3L5PcHg0TePO2Pj
   JF+TwPI90KCGQAPfzzGNA0zkbxAOImrP
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




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**