

1. SSRF

```
72 public Object product_search_post(@RequestParam String program, @RequestParam String parameter, @RequestParam String value) {
73     Map<String, String> response_data = new HashMap<String, String>();
74     String msg = "";
75     try {
76         URL obj = new URL( spec: "http://localhost:8081/ssrf/product/" + program + "/" + parameter + "=" + value);
77         HttpURLConnection con = (HttpURLConnection) obj.openConnection();
78         con.setRequestMethod("POST");
79         con.setDoOutput(true);
80         OutputStream os = con.getOutputStream();
81         os.flush();
82         os.close();
```

```
72 public Object product_search_post(@RequestParam String parameter, @RequestParam String value) {
73     Map<String, String> response_data = new HashMap<String, String>();
74     String msg = "";
75     try {
76         URL obj = new URL( spec: "http://localhost:8081/ssrf/product/item" + "/" + parameter + "=" + value);
77         HttpURLConnection con = (HttpURLConnection) obj.openConnection();
78         con.setRequestMethod("POST");
79         con.setDoOutput(true);
80         OutputStream os = con.getOutputStream();
81         os.flush();
82         os.close();
```

```
1 $(document).ready(function () {
2     $("#product_search").submit(function (event) {
3         event.preventDefault();
4         document.getElementById("product_search_result").innerHTML = ''
5         var search = {}
6         //search['program'] = 'item';
7         search['parameter'] = 'id';
8         search['value'] = $("#value").val();
9         $("#product_search_submit").prop("disabled", true);
10        $.ajax({
```

```
POST http://localhost:8081/ssrf/ HTTP/1.1
Host: localhost:8081
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gecko/20100101 Firefox/83.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 22
Origin: https://localhost:8081
Connection: keep-alive
```

parameter=id&value=202

2. Info Disclosure:

idor.js

```

93     table_html = ''
94     var data_length = data.length;
95     if (data_length > 0) {
96         table_html += '<table>'
97         table_html += '<tr><th>Name</th><th>Email</th><th>Phone</th><th>Amount</th></tr>'
98         for (var i = 0; i < data_length; i++) {
99             item = data[i]
100             table_html += '<tr><td>' + item.name + '</td><td>' + item.email + '</td><td>' + item.phone + '</td><td>' + item.amount + '</td></tr>';
101         }
102
103         table_html += '</table>'
104         $('#alert-own-info').append(table_html);
105     }

```

```

93     table_html = ''
94     var data_length = data.length;
95
96     table_html += '<table>'
97     table_html += '<tr><th>Name</th><th>Email</th><th>Phone</th><th>Amount</th></tr>'
98
99     item = data[1]
100     table_html += '<tr><td>' + item.name + '</td><td>' + item.email + '</td><td>' + item.phone + '</td><td>' + item.amount + '</td></tr>';
101
102
103     table_html += '</table>'
104     $('#alert-own-info').append(table_html);
105 }
106

```

idorController.java

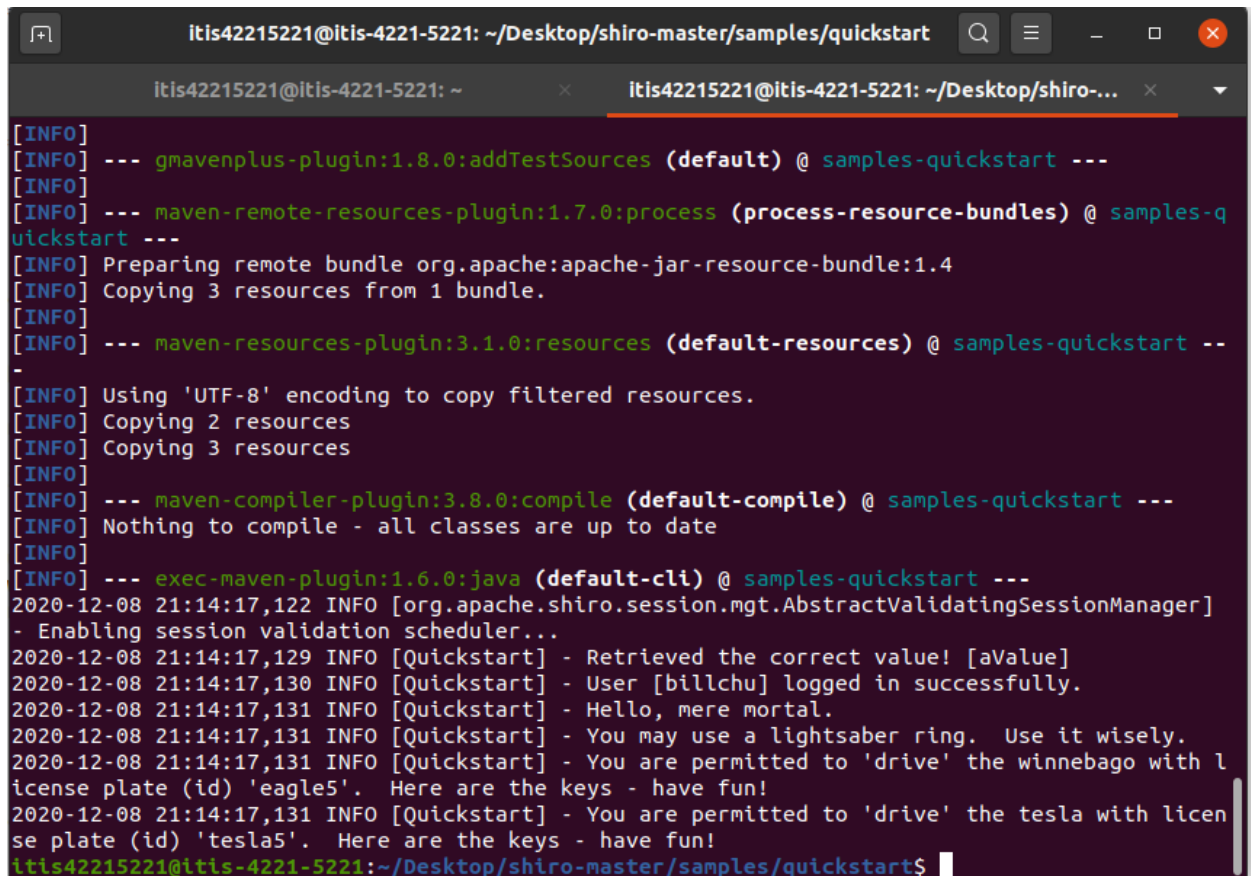
```

117
118     Map<String,String> list = new HashMap<>();
119     String json = "";
120     try {
121         for(Map.Entry<String, String> entry : session_customerInfo.entrySet()){
122             if(!entry.getKey().equals("id") && !entry.getKey().contentEquals(cs."password"))
123                 list.put(entry.getKey(),entry.getValue());
124         }
125         json = objectMapper.writeValueAsString(list);
126
127     } catch (JsonProcessingException e) {
128         json = "{\"status\":\"error\"}";
129         e.printStackTrace();
130     }
131     return json;
132 }

```

3. Apache Shiro

```
31 # -----
32 [users]
33 # user 'root' with password 'secret' and the 'admin' role
34 root = secret, admin
35 # user 'guest' with the password 'guest' and the 'guest' role
36 guest = guest, guest
37 # user 'presidentskroob' with password '12345' ("That's the same combination on
38 # my luggage!!!" ;)), and role 'president'
39 presidentskroob = 12345, president
40 # user 'darkhelmet' with password 'ludicrousspeed' and roles 'darklord' and 'schwartz'
41 darkhelmet = ludicrousspeed, darklord, schwartz
42 # user 'lonestarr' with password 'vespa' and roles 'goodguy' and 'schwartz'
43 lonestarr = vespa, goodguy, schwartz
44 billchu = chu, goodguy, 49er
45
46 # -----
47 # Roles with assigned permissions
48 #
49 # Each line conforms to the format defined in the
50 # org.apache.shiro.realm.text.TextConfigurationRealm#setRoleDefinitions JavaDoc
51 # -----
52 [roles]
53 # 'admin' role has all permissions, indicated by the wildcard '*'
54 admin = *
55 # The 'schwartz' role can do anything (*) with any lightsaber:
56 schwartz = lightsaber:*
57 goodguy = winnebago:drive:eagle5, tesla:drive:tesla1
58 49er = lightsaber:* , tesla:drive:*
```



```
itis42215221@itis-4221-5221: ~/Desktop/shiro-master/samples/quickstart
itis42215221@itis-4221-5221: ~
itis42215221@itis-4221-5221: ~/Desktop/shiro-...

[INFO] --- gmavenplus-plugin:1.8.0:addTestSources (default) @ samples-quickstart ---
[INFO] --- maven-remote-resources-plugin:1.7.0:process (process-resource-bundles) @ samples-q
[INFO] Preparing remote bundle org.apache:apache-jar-resource-bundle:1.4
[INFO] Copying 3 resources from 1 bundle.
[INFO] --- maven-resources-plugin:3.1.0:resources (default-resources) @ samples-quickstart --
[INFO] Using 'UTF-8' encoding to copy filtered resources.
[INFO] Copying 2 resources
[INFO] Copying 3 resources
[INFO] --- maven-compiler-plugin:3.8.0:compile (default-compile) @ samples-quickstart ---
[INFO] Nothing to compile - all classes are up to date
[INFO] --- exec-maven-plugin:1.6.0:java (default-cli) @ samples-quickstart ---
2020-12-08 21:14:17,122 INFO [org.apache.shiro.session.mgt.AbstractValidatingSessionManager]
- Enabling session validation scheduler...
2020-12-08 21:14:17,129 INFO [Quickstart] - Retrieved the correct value! [aValue]
2020-12-08 21:14:17,130 INFO [Quickstart] - User [billchu] logged in successfully.
2020-12-08 21:14:17,131 INFO [Quickstart] - Hello, mere mortal.
2020-12-08 21:14:17,131 INFO [Quickstart] - You may use a lightsaber ring. Use it wisely.
2020-12-08 21:14:17,131 INFO [Quickstart] - You are permitted to 'drive' the winnebago with l
license plate (id) 'eagle5'. Here are the keys - have fun!
2020-12-08 21:14:17,131 INFO [Quickstart] - You are permitted to 'drive' the tesla with licen
se plate (id) 'tesla5'. Here are the keys - have fun!
itis42215221@itis-4221-5221:~/Desktop/shiro-master/samples/quickstart$
```