hackerearth

Penetration Testing Report

For

“Take Last 2”

S.NO.	Title	#
1.	Challenge Category	Web Application
2.	Challenge Related Files	N/A
3.	File Link / Target IP	N/A

PROCEDURE

1. Check there are 2 box one for name and other for token
2. Only if we enter the correct name our token is checked and we get a message ther our token is checked.
3. Exploit script https://pastebin.com/StPUqKDB
4. You can't read the flag on the website as it's not reflected so either you can make a payload to make a http request to your server or you can get a reverse shell with the script above.

   BONUS :   (CVE-2017-5941)
   https://www.exploit-db.com/docs/english/41289-exploiting-node.js-deserialization-bug-for-remote-code-execution.pdf

Flags:

S.No.	Flag - No.	Flag
1.	Flag 1	HE{deserialization_is_not_just_for_PHP_u_know}