Route	Parameter	XSS Successful?
http://127.0.0.1:8081/	Password	Yes
http://127.0.0.1:8081/register	Password	Yes
http://127.0.0.1:8081/register	Password2	Yes
http://127.0.0.1:8081/register	Name	No
http://127.0.0.1:8081/login	Password	Yes
http://127.0.0.1:8081/	type	No
http://127.0.0.1:8081/	name	No
http://127.0.0.1:8081/register	type	No
http://127.0.0.1:8081/register	name	No
http://127.0.0.1:8081/login	type	No
http://127.0.0.1:8081/login	name	No
http://127.0.0.1:8081/updateuser	type	No
http://127.0.0.1:8081/updateuser	type	No
http://127.0.0.1:8081/updateuser	type	No
http://127.0.0.1:8081/updateuser	name	No
http://127.0.0.1:8081/createproduct	type	No
http://127.0.0.1:8081/createproduct	type	No
http://127.0.0.1:8081/createproduct	type	No
http://127.0.0.1:8081/createproduct	name	No
http://127.0.0.1:8081/updateproduct	name	Yes
http://127.0.0.1:8081/updateproduct	type	Yes
http://127.0.0.1:8081/updateproduct	type	No
http://127.0.0.1:8081/updateproduct	type	No
http://127.0.0.1:8081/updateproduct	type	No

1. The results are different because the session ID allows the attacker to log into the website and access more vulnerabilities within web pages that require a logged in account. The session ID allows an attacker to access content using a logged in user's account thus bypassing the need to log in using the user's account's password.

2. Yes, it was able to cover all the access points once the session ID was provided. However, PwnXSS was not able to access /updateproduct unless a product was already created, which was a page that was susceptible to multiple XSS attacks with its product_name and last_date values.