

Informe de pentesting

BadStore

Alejandro Parrado Di Doménico

alejoparrado@icloud.com

Tabla de contenido

1.	Introducción	2
	a. scope	
	b. datos iniciales	
	c. problemas encontrados	
	d. horario y fechas de ejecución	
2.	Conclusiones	3
3.	Recomendaciones	4
	a. corto plazo	
	b. medio y largo plazo	
4.	Vulnerabilidades (tabla resumen)	6
	a. descripción	
	b. explotación	



Introducción

Se ha solicitado realizar un pentesting a la aplicación web BadStore, que se encuentra alojada en la dirección IP 192.168.0.24, se tenía alcance a todas las páginas, funcionalidades y apartados de la aplicación. Se encontraron múltiples vulnerabilidades, que permitieron, entre otras cosas, ejecutar código JavaScript, acceder a páginas no indexadas, obtener credenciales de usuarios, obtener permisos de administrador, obtener información sensible, cambiar contraseñas de otros usuarios, hacer peticiones a la base de datos e interceptar comunicaciones no cifradas. Posteriormente se explicará cada vulnerabilidad a detalle y su proceso de explotación.

Fecha: 8 de Octubre del 2022

Conclusiones

Se encontraron vulnerabilidades en la aplicación web BadStore, que permitieron acceso a información sensible, se pudo hacer un ataque XSS para robar las cookies de la sesión del usuario, se hizo un SQL Injection, cracking de contraseñas hasheadas, ingreso sin autenticación y obtención de privilegios de administrador.

A continuación se presentan las vulnerabilidades y su nivel de criticidad según la calculadora CVSS v3.0

Versión 2 y 3 de SSL	9.8
Apache versión < 2.4.49	9.8
Escalada de privilegios (Administrador)	9.8
SQL Injection	9.7
Acceso a directorios con información sensible	8.6
XSS (Cross Site Scripting)	7.5

Recomendaciones

Soluciones a corto plazo

Versión 2 y 3 de SSL - Deshabilitar la conexión por SSL 2 o 3, en vez de eso, utilizar TLS 1.2 o superior para mayor seguridad.

Apache versión 2.4.49 - Actualizar el servicio de Apache a la versión 2.4.49 o posteriores.

Escalada de privilegios (Administrador) - Debido a que se puede hacer esta escalada de privilegios de diferentes formas, hay diferentes procedimientos para llevar a cabo:

- No realizar la asignación de rol de un usuario que se está registrando mediante la petición HTTP, ya que esta se puede interceptar y cambiar su valor.
- Filtrar los inputs en el Login para no permitir SQL Injection (se especificará en el siguiente punto), ya que mediante cambiar una consulta SQL es que fue posible acceder como Administrador a la aplicación.
- Cambiar el proceso de reinicio de contraseña, ya que por defecto se cambia por “Welcome” sin hacer ninguna validación, lo cual permite cambiar la contraseña de cualquier usuario sin tener su correo ni saber la anterior.

SQL Injection - Prevenir SQLi hoy día es posible sólo usando las últimas tecnologías, las cuales ya vienen con sistemas de prevención y tratamiento de inputs para lidiar con esta vulnerabilidad. En todo caso es importante tener en cuenta los siguientes puntos:

- Todo el equipo de desarrollo debe estar entrenado en las diferentes formas de prevenir esta vulnerabilidad acorde al lenguaje de programación y al servicio de base de datos que se utilice.
- No se debe confiar en los inputs de los usuarios.
- Utilice filtros con white y blacklists, estas listas permiten establecer qué caracteres o cadenas son permitidos en un input y cuáles no.
- Utilice las últimas tecnologías (y las mejor verificadas).
- Haga escaneos regularmente.

Para más información:

- [SQL Injection Prevention Cheat Sheet - OWASP](#)
- [SQL Injection and How to Prevent It - Acunetix](#)

Acceso a Directorios con Información Sensible - Implementar servicios de autenticación y autorización en las diferentes páginas de la aplicación, y de ser información como cuentas de usuario, estas no deben estar indexadas en ninguna página, sino alojadas en la base de datos en el servidor web.

XSS - Prevenir los ataques de XSS puede variar en dificultad dependiendo de la complejidad de la aplicación. Sin embargo esto es posible siguiendo las siguientes medidas:

- Filtrar los inputs. Utilice parámetros estrictos, teniendo en cuenta el input esperado o válido y el que no lo es.
- Encodear la información en el output. Al momento de la respuesta HTTP, es importante que el output esté encodeado para evitar que sea interpretado y en el caso de JavaScript, que se llegue a ejecutar alguna función.
- Utilice headers apropiados en las respuestas HTTP. Por ejemplo, si una respuesta no debería poseer contenido HTML o JavaScript, se pueden usar los headers Content-Type y X-Content-Type-Options.

Para más información:

- [Cross-site scripting prevention - Port Swigger](#)

Recomendaciones a medio y largo plazo

1. Mantener actualizadas las tecnologías, servicios y protocolos. Para estar al día con los parches de seguridad.
2. Desconfiar de cualquier input y aplicar todos los filtros necesarios, para que sólo se genere interacción con aquella información válida.
3. Desarrollar y/o implementar sistemas de autenticación.
4. No indexar información sensible en el contenido de la aplicación.
5. Utilizar algoritmos de Hashing más modernos para las contraseñas, como el SHA-256.

Vulnerabilidades

Primeramente se realizó un escaneo con Nessus a la dirección IP donde se alojaba la aplicación (192.168.0.24), y luego manualmente, se fueron revisando los diferentes apartados y probando explotar distintas vulnerabilidades, a continuación el procedimiento mediante el cual se consiguieron explotar.

Cross-site Scripting

Explotación:

En la dirección <http://192.168.0.24/cgi-bin/badstore.cgi?action=guestbook> es posible encontrar una página con un formulario para escribir comentarios sobre la BadStore. Esta es vulnerable a XSS y se consiguió explotar de la siguiente forma.

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:

Se ingresó el anterior código JavaScript, el cual imprime por pantalla las cookies de la sesión del usuario actual, esto solo con el fin de demostrar la vulnerabilidad.

🌐 192.168.0.24

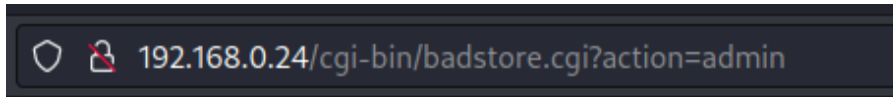
SSOid=dGVzdEB0ZXN0LmNvbTo4MWRjOWJkYjUyZDA0ZGM5MDAzNmRiZDgzMTNiZDA1NTp0ZXN0OUIU%3D%0A

OK

Acceso a Directorios con Información Sensible

Explotación:

Haciendo pruebas con el parámetro “action” de la URL, se encontró la siguiente página al ingresar el parámetro igual a “admin”.



Secret Administration Menu

Where do you want to be taken today?

Sin embargo, al hacer alguna petición se nos retorna el siguiente error por no estar logueados como administrador. Esto se intentará de nuevo más adelante.

Secret Administration Portal

Error - test is not an Admin!

Something weird happened - you tried to access the Administrative Portal, but you are not an Administrative User.

You must login as an Admin to access this resource.

Use your browser's Back button and go to Login.

(If you're trying to hack - I know who you are: 192.168.0.26)

Buscando en el archivo robots.txt de la página web, se han encontrado las siguientes direcciones.


```
# /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
```

Al probar las direcciones se halla lo siguiente.

BS Index of /backup BS 192.168.0.24/robots.txt +

← → ↻ 🏠 🔒 192.168.0.24/backup/

Index of /backup

Name	Last modified	Size	Description
Parent Directory	07-Oct-2022 23:59	-	

Apache/1.3.28 Server at 192.168.0.24 Port 80

Index of /supplier

Name	Last modified	Size	Description
Parent Directory	07-Oct-2022 23:59	-	
[] accounts	29-Nov-2004 20:51	1k	

Apache/1.3.28 Server at 192.168.0.24 Port 80

Especialmente en /supplier, hay un archivo con algunas cuentas de usuario del sistema, que están encodeadas en Base64.

```
1001:am9ldXNlci9wYXNzd29yZC9wbGF0bnVtLzE5Mi4xNjguMTAwLjU2DQo=  
1002:a3JvZWlci9zM0NyM3QvZ29sZC8xMC4xMDAuMTAwLjE=  
1003:amFuZXVzZXIvd2FpdGluZzRGcmkYXkvMTcyLjIyLjEyLjE5  
1004:a2Jvb2tvdXQvc2VuZGllYXBvLzEwLjEwMC4xMDAuMjA=
```

Utilizando la herramienta online [Cyber Chef](#), se han parseado estas cuentas de usuarios para poder verlas en texto claro.

```
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
```

Escalada de Privilegios (Administrador)

Explotación:

Primero se intercepta la petición enviada al registrarse como nuevo usuario, con la herramienta Burp Suite.

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.)

Es aquí donde se reconoce que el rol del usuario se envía en la misma petición HTTP que el email y la contraseña.

Original request ▾

Pretty **Raw** Hex

```
1 POST /cgi-bin/badstore.cgi?action=register HTTP/1.1
2 Host: 192.168.0.24
3 Content-Length: 89
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.0.24
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8;
10 Referer: http://192.168.0.24/cgi-bin/badstore.cgi?action=loginregister
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Connection: close
14
15 fullname=new_user&email=random%40email&passwd=1234&pwdhint=green&role=U&Register=Register
```

Suponiendo que role=U se refiere a “User”, role=A se referiría a “Admin”, así que se cambia la petición y se envía de esta forma.

`&role=A&`

Para verificar que efectivamente el usuario new_user (que se ha acabado de crear), posee permisos de Administrador, se hizo una petición en la página de ?action=admin.

Welcome new_user - Cart contains 0 items at \$0.00

 [View Cart](#)

Secret Administration Portal

BadStore.net Sales Report

Saturday, October 8, 2022 at 11:02:21

Date	Time	Cost	Count	Items	Account	IP	Paid	Credit_Card_Used	ExpDate
2022-09-03	00:00:11	\$360.00	1	1002	fred@newuser.com	172.22.15.47	Y	2014-0000-0000-009	0705
2022-09-19	00:00:11	\$1137.90	3	1008,1009,1011	sue@spender.com	10.10.10.350	Y	6011-0000-0000-0004	1006
2022-09-19	00:00:11	\$137.90	3	1008,1009,1011	mary@spender.com	192.168.10.70	Y	3000-0000-0000-04	0506
2022-09-25	-02:03:58	\$22.95	1	1008	joe@supplier.com	10.10.10.50	Y	3400-0000-0000-009	1008
2022-10-01	00:00:11	\$46.95	3	1000,1003,1008	joe@supplier.com	10.10.10.150	Y	5500-0000-0000-0004	0905
2022-10-02	-07:01:57	\$46.95	3	1000,1003,1008	joe@supplier.com	10.10.10.50	Y	4111-1111-1111-1111	0705
2022-10-04	-03:05:51	\$137.90	3	1008,1009,1011	sue@spender.com	10.10.10.350	Y	6011-0000-0000-0004	1006
2022-10-05	00:00:11	\$137.90	3	1008,1009,1011	mary@spender.com	192.168.10.70	Y	3000-0000-0000-04	0506
2022-10-05	00:00:11	\$22.95	1	1008	joe@supplier.com	10.10.10.50	Y	3400-0000-0000-009	1008
2022-10-05	00:00:11	\$46.95	3	1000,1003,1008	joe@supplier.com	10.10.10.50	Y	4111-1111-1111-1111	0705
2022-10-05	00:00:11	\$46.95	3	1000,1003,1008	joe@supplier.com	10.10.10.150	Y	5500-0000-0000-0004	0905
2022-10-06	-08:08:53	\$22.95	1	1008	joe@supplier.com	10.10.10.50	Y	3400-0000-0000-009	1008

Logrando esta vez obtener la información sin problema.

Aquí la tabla completa:

Secret Administration Portal

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	9726255eec083aa56dc0449a21b33190	blue	Big Spender	U
ray@supplier.com	99b0e8da24e29e4ccb5d7d76e677c2ac	red	Ray Supplier	S
robert@spender.net	e40b34e3380d6d2b238762f0330fbd84	orange	Robert Spender	U
bill@gander.org	5f4dcc3b5aa765d61d8327deb882cf99	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	0DF3DBF0EF9B6F1D49E88194D26AE243	green	Curt Wilson	U
paul@supplier.com	EB7D34C06CD6B561557D7EF389CDDA3C	red	Paul Rice	S
kevin@spender.com			Kevin Richards	U
ryan@badstore.net	40C0BBD4AEEAA39166825F8B477EDB4	purple	Ryan Shorter	A
stefan@supplier.com	8E0FAA8363D8EE4D377574AEE8DD992E	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	EEE86E9B0FE29B2D63C714B51CE54980	green	John Stiber	U
heinrich@supplier.de	5f4dcc3b5aa765d61d8327deb882cf99	red	Heinrich Hä'sÄ°ber	S
tommy@customer.net	7f43c1e438dc11a93d19616549d4b701	orange	Tom O'Kelley	U
test@test.com	81dc9bdb52d04dc20036dbd8313ed055	green	test	U
valid@email.com	81dc9bdb52d04dc20036dbd8313ed055	green	abcabc	U
random@email	81dc9bdb52d04dc20036dbd8313ed055	green	new_user	A

Se utiliza la herramienta hash-identifier para saber si el hash con el que se almacenan las contraseñas está roto.

```
HASH: 81dc9bdb52d04dc20036dbd8313ed055
```


```
Possible Hashs:  
[+] MD5
```

Viendo que es un hash MD5, se sabe que es posible crackear las contraseñas. En la siguiente tabla, se evidencia los usuarios, los hashes y las contraseñas en claro.

User	Hash	Password
AAA_Test_User	098F6BCD4621D373CADE4E832627B4F6	test
admin	83218ac34c1834c26781fe4bde918ee4	Welcome
joe@supplier.com	62072d95acb588c7ee9d6fa0c6c85155	iforgot
big@spender.com	9726255eec083aa56dc0449a21b33190	money
ray@supplier.com	99b0e8da24e29e4ccb5d7d76e677c2ac	supplier
robert@spender.net	e40b34e3380d6d2b238762f0330fbd84	cheap
bill@gander.org	5f4dcc3b5aa765d61d8327deb882cf99	password
steve@badstore.net	8cb554127837a4002338c10a299289fb	profit
fred@whole.biz	356c9ee60e9da05301adc3bd96f6b383	whole
debbie@supplier.com	2fbd38e6c6c4a64ef43fac3f0be7860e	helpme
mary@spender.com	7f43c1e438dc11a93d19616549d4b701	luv2buy
sue@spender.com	ea0520bf4d3bd7b9d6ac40c3d63dd500	got2buy
curt@customer.com	0DF3DBF0EF9B6F1D49E88194D26AE243	carbondale
paul@supplier.com	EB7D34C06CD6B561557D7EF389CDDA3C	BMWMotorcycle
kevin@spender.com		
ryan@badstore.net	40C0BBDC4AEEAA39166825F8B477EDB4	Shavelick
stefan@supplier.com	8E0FAA8363D8EE4D377574AEE8DD992E	badstore
landon@whole.biz	29A4F8BFA56D3F970952AFC893355ABC	TEXAN
sam@customer.net	5EBE2294ECD0E0F08EAB7690D2A6EE69	secret
david@customer.org	356779A9A1696714480F57FA3FB66D4C	California
john@customer.org	EEE86E9B0FE29B2D63C714B51CE54980	Disneyland
heinrich@supplier.de	5f4dcc3b5aa765d61d8327deb882cf99	password
tommy@customer.net	7f43c1e438dc11a93d19616549d4b701	luv2buy
test@test.com	81dc9bdb52d04dc20036dbd8313ed055	1234
valid@email.com	81dc9bdb52d04dc20036dbd8313ed055	1234
random@email	81dc9bdb52d04dc20036dbd8313ed055	1234

En la página <http://192.168.0.24/cgi-bin/badstore.cgi?action=myaccount> hay un apartado que permite la recuperación de contraseña, aunque tiene una vulnerabilidad, y es que siempre se cambia por la misma ("Welcome") sin pedir la anterior, ni enviar un correo de verificación. Por lo cual, únicamente es

necesario ingresar el usuario, y responder la pregunta de seguridad, que tiene 6 posibles respuestas, así que es posible probar una por una hasta que permita cambiarla.

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

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...)

The password for user: admin

...has been reset to: Welcome

Ya tendríamos acceso a la cuenta de Administrador.

SQL Injection

La página de Login, ubicada en la dirección <http://192.168.0.24/cgi-bin/badstore.cgi?action=loginregister> tiene una vulnerabilidad a SQL Injection, identificada con SQLMap, así que ingresamos el siguiente query, el cual nos va permitir el acceso a la cuenta admin, ya que generalmente es la que posee el id=1.

Login to Your Account

Email Address:

Password:

Ni siquiera solicita que se ingrese la contraseña, simplemente permite el Login como Administrador.

Welcome **Master System Administrator** -
en oo