[Registro 2](#_Toc448829985)

[Servidores 2](#_Toc448829986)

[DNS 2](#_Toc448829987)

[Uso de xss 2](#_Toc448829988)

[Uso de etiqueta html 4](#_Toc448829989)

[Datos de login 5](#_Toc448829990)

[https://negocios2.buzonfiscal.com/login.jsp 5](#_Toc448829991)

[https://www4.oxxo.com/facturacion/fc.login 5](#_Toc448829992)

[http://www2.oxxo.com/AccessControl/login\_form.jsp 6](#_Toc448829993)

[ESCANEO DE PUERTOS 7](#_Toc448829994)

[Exploit para nginx 7](#_Toc448829995)

[Error url 7](#_Toc448829996)

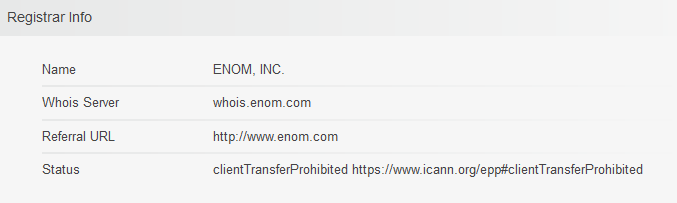
[PHPMYADMIN 8](#_Toc448829997)

[Metaesploit para phpmyadmin 9](#_Toc448829998)

El escaneo de puertos corresponde a la etapa de la enumeración, la estructura del reporte debe ser secuencial a las etapas del Pentesting, implementar primero OSSTMM y a lo ultimo cuando se llega a la infraestructura WEB se usa OWASP

# 

# Registro

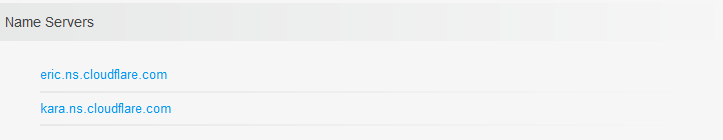


No veo las etapas de :  
OSINT  
FOOTPRINTIG  
ENUMERACION  
  
Debes incluír correos electrónicos asociados,url de documentos públicos en caso de existir etc etc.

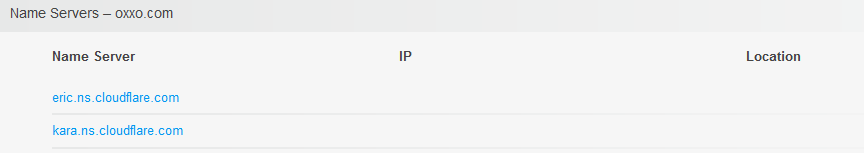
De igual modo esos servidores son de Cloudflare no nos sirve tener esa informacion

Cuando un servicio tiene cloudflrare, es decir está protegiendo la verdadera dirección IP, se debe aplicar metodologías de investigación OSINT para obtener DNS e implementar Google Hacking. Y justamente en este apartado se debe poner todos los dns

# Servidores



# DNS



Cuando se va a mostrar una vulnerabilidad existente debe tener la estructura que muestra ACUNETIX , no veo cabecera enviada ni cabecera recibida.

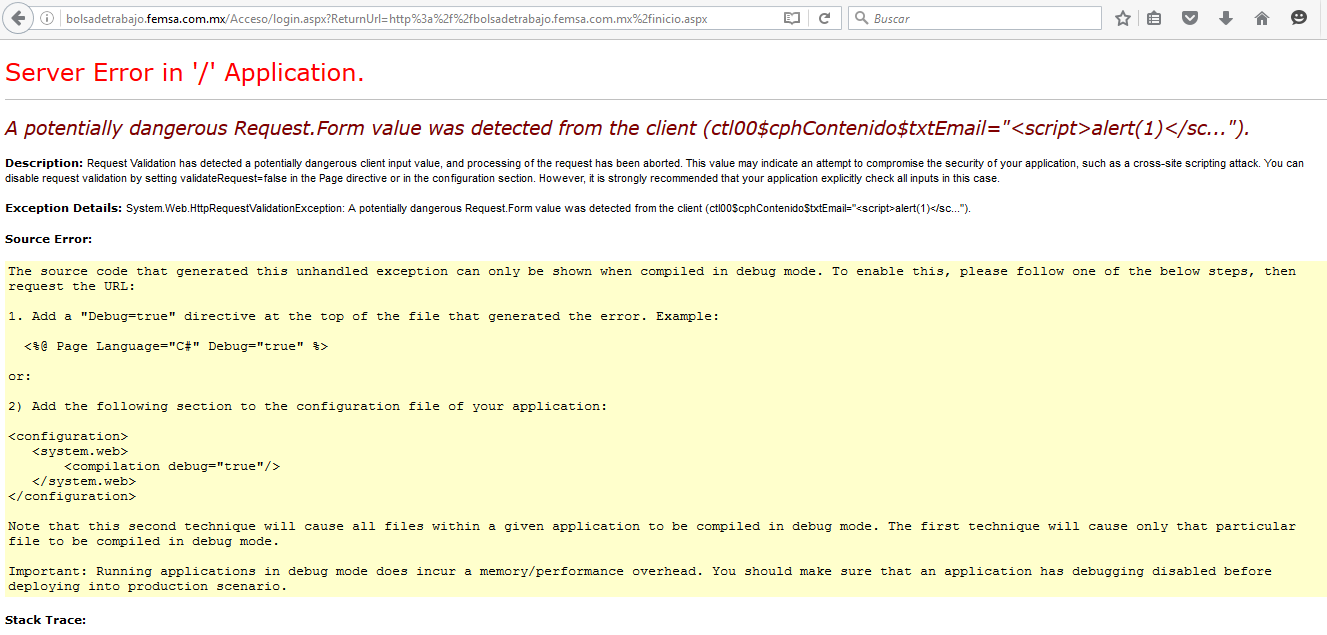
Ese DNS usado no corresponde al target principal, es de femsa el dueño de oxxo, esta bien pero hasta este momento primero se explican las vulnerabilidades de oxxo y después de los dominios o targets relacionados con el principal objetivo

# Uso de xss

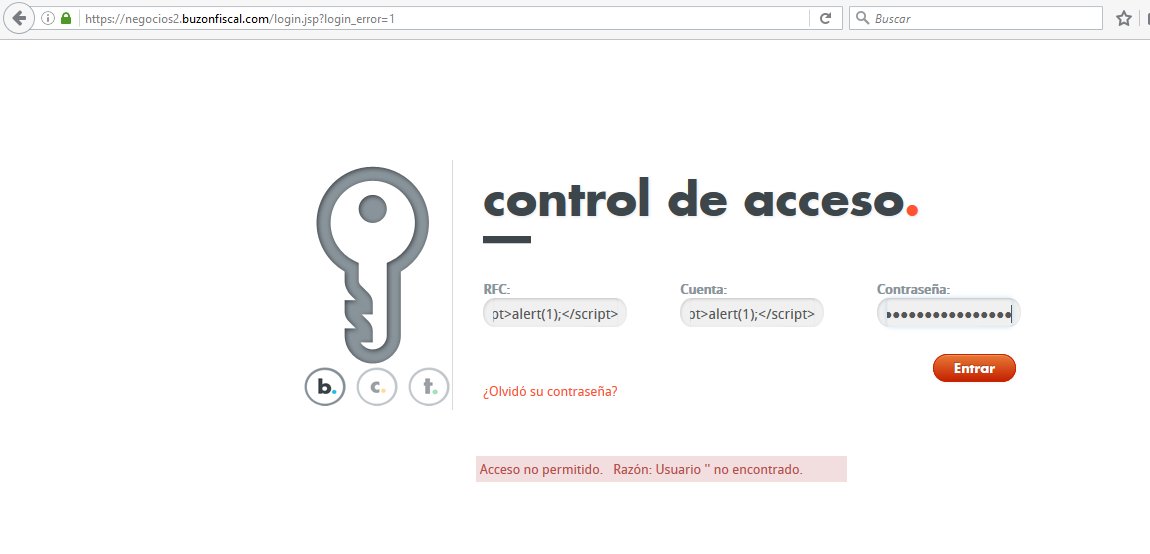
En el formulario de logeo se coloca <script>alert(1)</script> tanto en usuario como en contraseña y se presiona continuar.

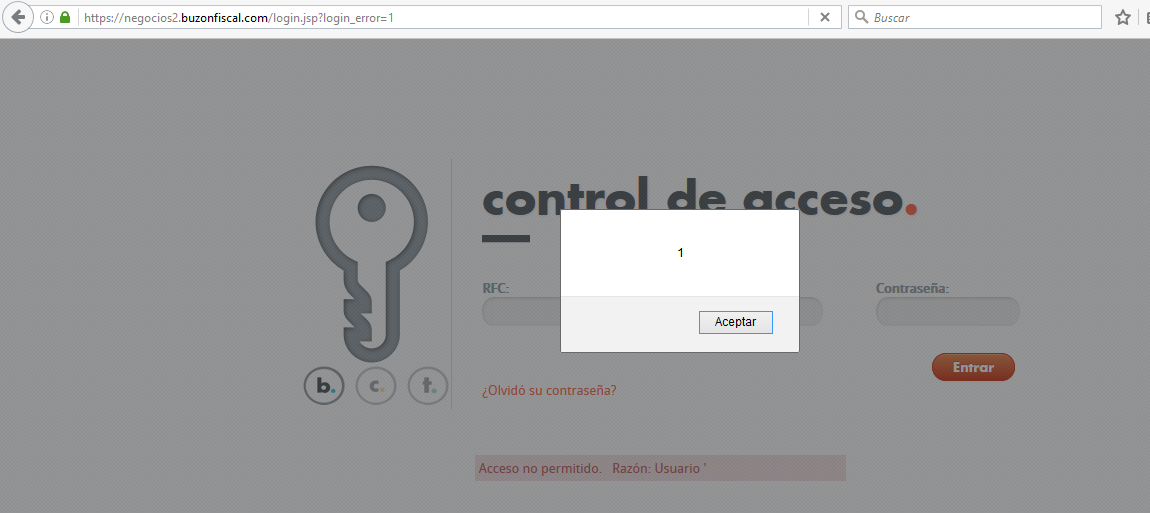


Una vez que se presiona continuar el portal muestra el siguiente error.



Se coloca <script>alert(1);</script> en todos los campos





La vulnerabilidad esta bien aplicada pero no corresponde al target, y de cualquier modo si perteneciera no se debe poner tantas imágenes, solo con mostrar cabecera vulnerable y en que variable se inyecta y la imagen donde arroja el resultado, (básate en los reportes que usa acuneteix y no estoy diciendo que lo pongas tal cual lo arroja, si no solo fijate en la estructura y tu mismo crea tu reporte)

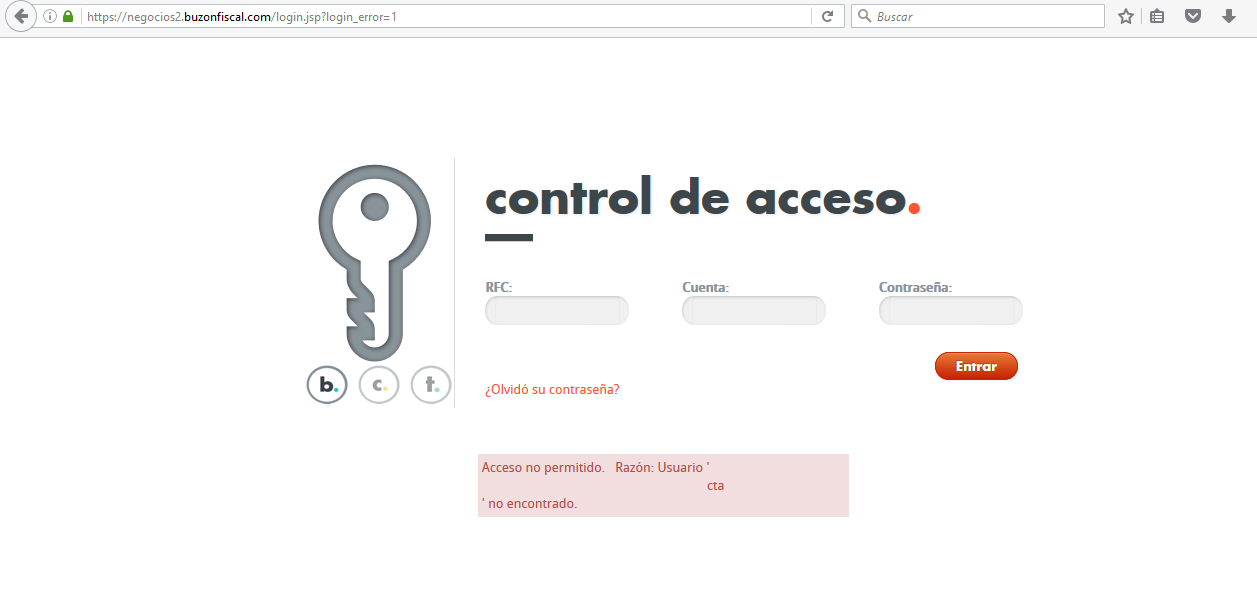
# Uso de etiqueta html

Se coloca

<marquee>rfc</marquee> en el campo rfc

<marquee>cta</marquee> en el campo cta

<marquee>hola</marquee> en el campo contraseña



# Datos de login

## <https://negocios2.buzonfiscal.com/login.jsp>

De igual manera no hace falta explicar los distintos exploits que se pueden usar, ahora después de explicar una vulnerabilidad se debe poner a manera de anotación y desde tu punto de vista como los desarrolladores deben corregir ese fallo, (puedes sugerir líneas de código y soft adicional)

**RFC:** msnm498490kd1

**USUARIO:**<script>alert(1)</script>

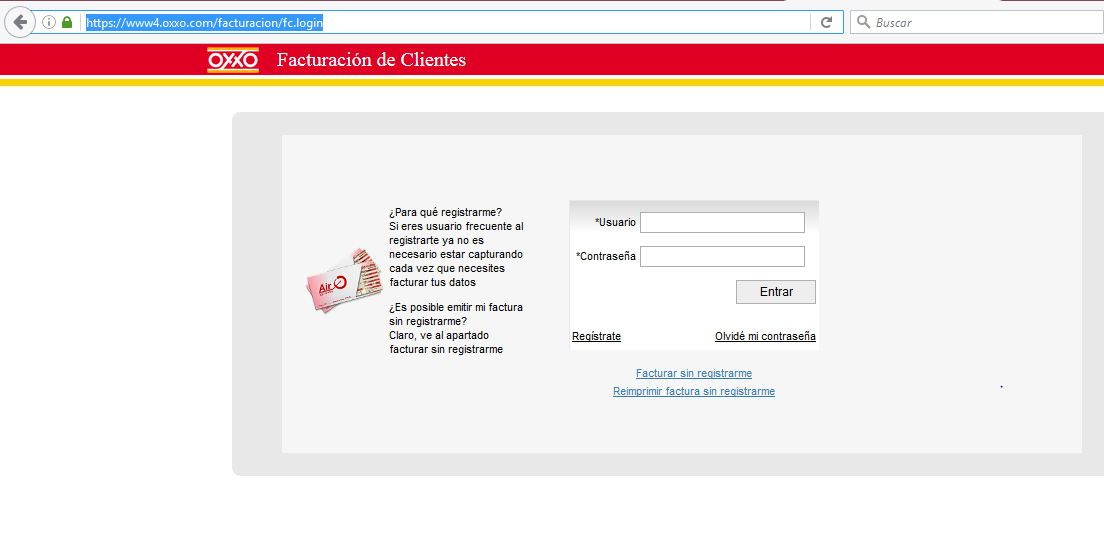
**CONTRASEÑA:**<script>alert(1);</script>



## <https://www4.oxxo.com/facturacion/fc.login>

**USUARIO:**[cddccd@yopmail.com](mailto:cddccd@yopmail.com)

**CONTRASEÑA:**<script>alert(1);</script>



## <http://www2.oxxo.com/AccessControl/login_form.jsp>

**USUARIO:**[cddccd@yopmail.com](mailto:cddccd@yopmail.com)

**Contraseña:**M5PF8H



De nada nos sirve escanear a cloudflafre,

Para intentar evadir ese sistema de protección debes basarte en los resultados arrojados en la etapa de investigación, si notas una ip que corresponda efectivamente al target sobre ese rango puedes trabajar, pero no encasillarte solo en ese rango ya que debes buscar mas rangos ips,

(Investiga que es y cómo funciona Cloudflare, siempre que veas una tecnología y no tengas idea que es, es bueno investigar un poco hacerca de ella y como evadirla)

# ESCANEO DE PUERTOS

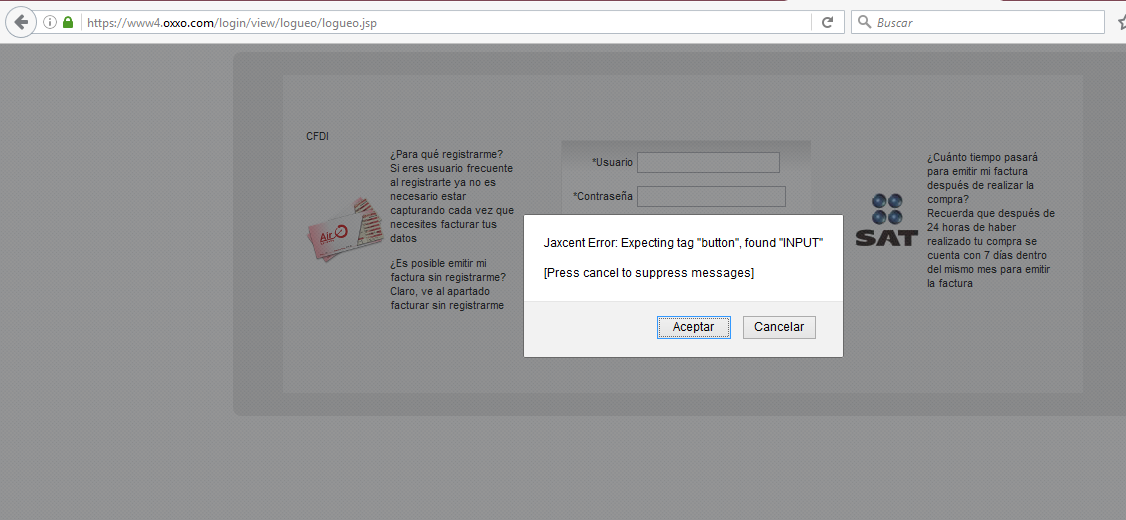
|  |  |  |
| --- | --- | --- |
| Puerto | Servicio | Descripcion |
| 1 | Icmp | Echo-replyttl 56 |
| 6 | Tcp | Proto-response ttl 255 |
| 80 | http | Cloudflarenginx |
| 443 | http | Cloudflarenginx |
| 2052 | http | Cloudflarenginx |
| 2053 | http | Nginx |
| 2082 | http | Cloudflarenginx |
| 2083 | http | Nginx |
| 2086 | http | Cloudflarenginx |
| 2087 | http | Nginx |
| 2095 | http | Cloudflarenginx |
| 2096 | http | Nginx |
| 8080 | http | Cloudflarenginx |
| 8043 | http | Cloudflarenginx |
| 8880 | http | Cloudflarenginx |

## Exploit para nginx



# Error url

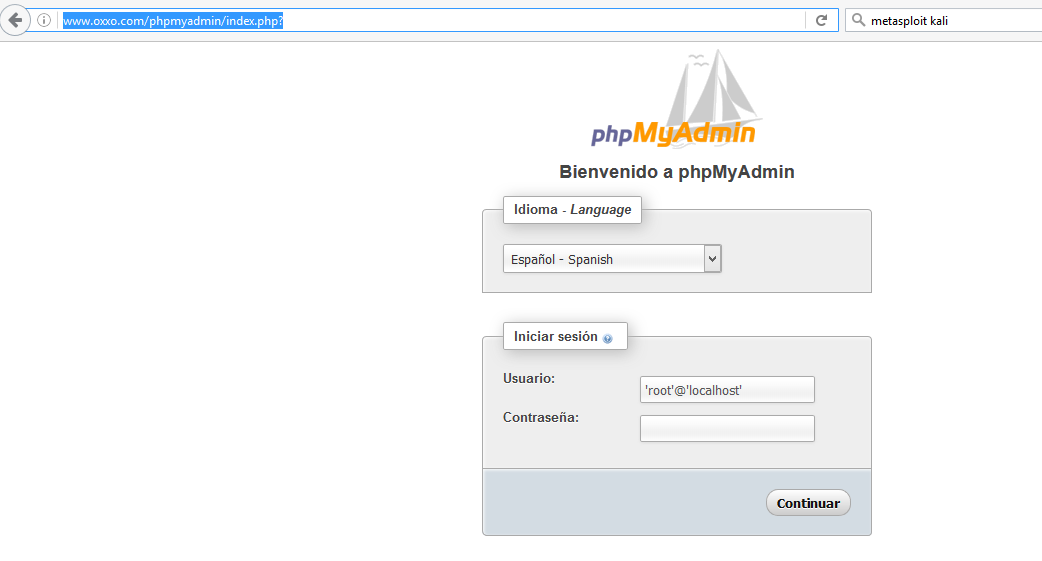
Error en el login<https://www4.oxxo.com/login/view/logueo/logueo.jsp> al ingresar el portal muestra errores de input para el boton



Phpmyadmin es un servicio, primero se enlistan los servicios en la etapa correspondiente, separando servicios de infraestructura de red y servicios web tal como: phpmyadmin, joomla, squid etc etc con sus respectivas versiones

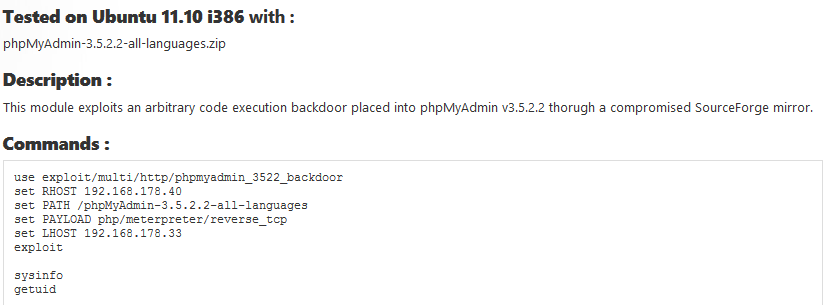
# PHPMYADMIN

<http://www.oxxo.com/phpmyadmin/index.php>



La etapa de explotación si es a lo ultimo, y cuando se explota se debe poner CVE de la vulnerabilidad, con que se pretende explotar, como se configura el exploit y resultados arrojados,

## Metaesploit para phpmyadmin



Faltaron bastantes etapas y tecncias por aplicar, el reporte esta muy incompleto, recordemos que los vectores de ataque nosotros los definimos conrespecto a las investigaciones previas, cada ip, dns, subdominio es un vector de ataque al cual se le debe de pasar independientemente todas las técnicas de ataques.