



Universidad Nacional  
Autónoma de México

DIRECCIÓN GENERAL DE CÓMPUTO Y DE  
**TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN**

**03-marzo-2016**

# PROYECTO MODULO 2

“Manual de usuario”

Integrantes:

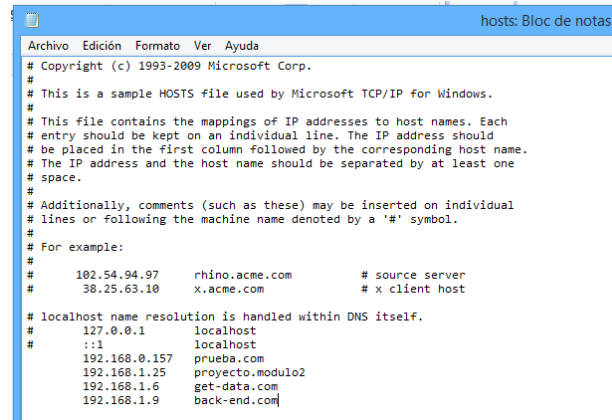
- Armenta Segura José Juan
- Morales Pablo Samuel Abraham
- Vega Tellez Jesus Antonio



**Programa de Becas de Formación en Seguridad  
Informática 10ª Generación**

## “AGREGAR UN ARTICULO”

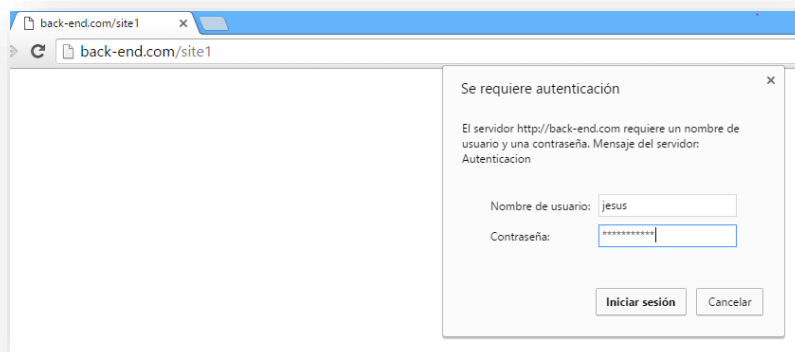
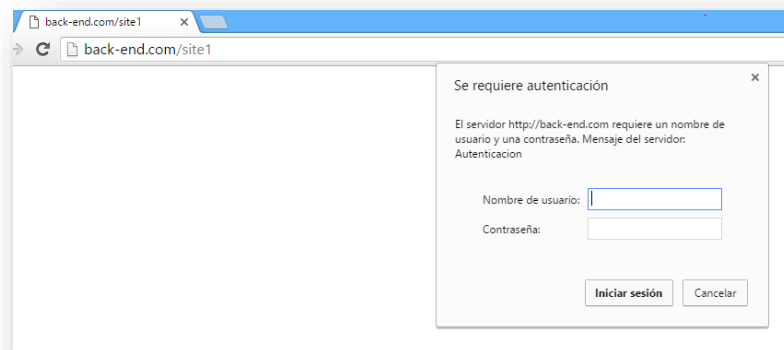
Para ingresar al **back-end** de drupal es necesario primero configurar el archivo hosts que se encuentra en la siguiente ruta C:\Windows\System32\drivers\etc\hosts y agregar la ip del servidor para poder acceder.



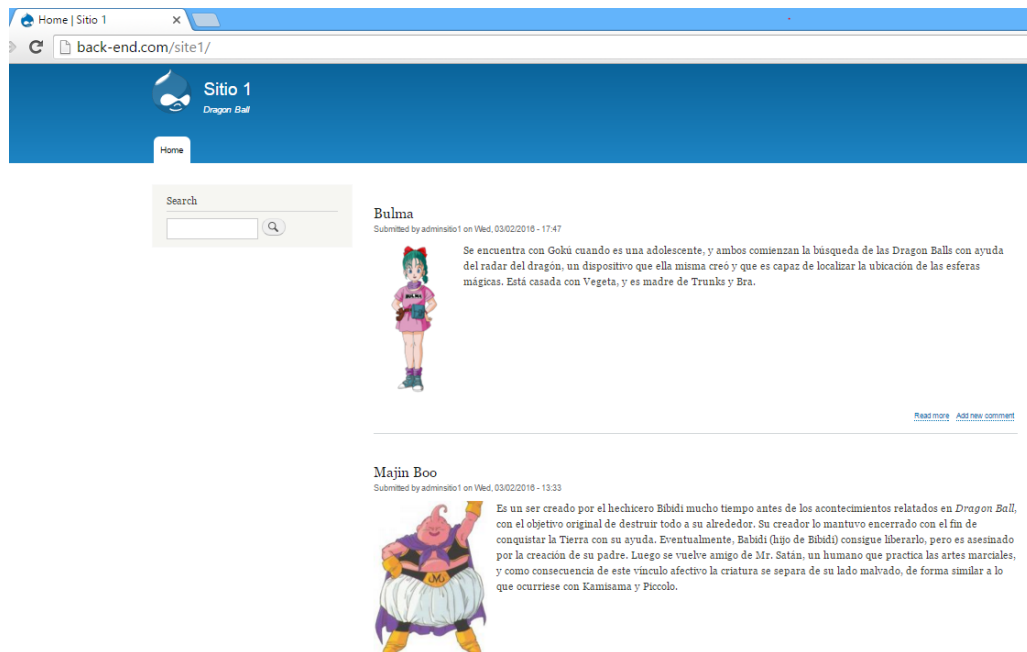
```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com   # source server
#       38.25.63.10      x.acme.com       # x client host

# localhost name resolution is handled within DNS itself.
#
#       127.0.0.1         localhost
#       ::1              localhost
#       192.168.0.157     prueba.com
#       192.168.1.25      proyecto.modulo2
#       192.168.1.6       get-data.com
#       192.168.1.9       back-end.com
```

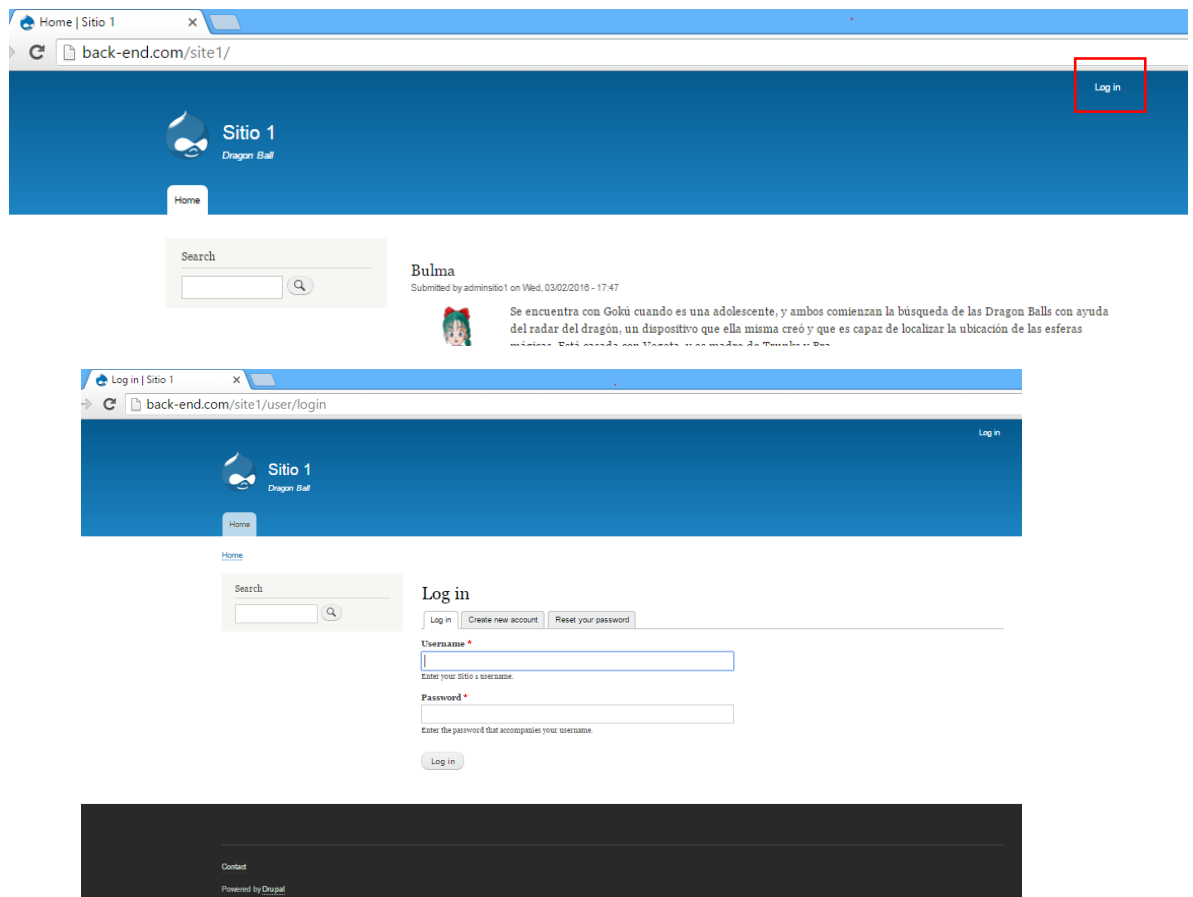
Ahora iremos a nuestro navegador e ingresaremos lo siguiente: <http://back-end/site1> podemos ver que nos pedirá una Autenticación de usuario; solo ingresamos nuestras credenciales y podemos entrar para ver el contenido.

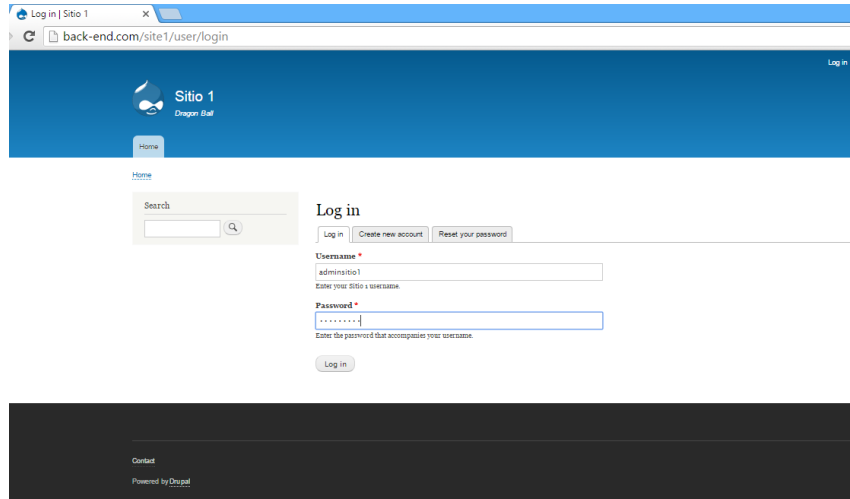


Esta es nuestra página principal del sitio1

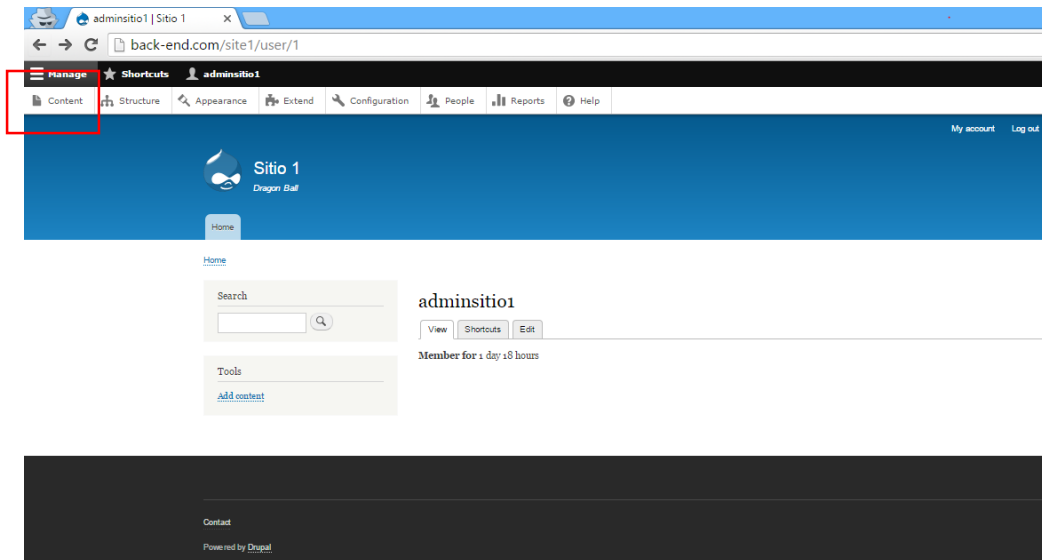


Si se quiere agregar contenido al sitio es necesario identificarse como un usuario de tipo administrador al sitio.

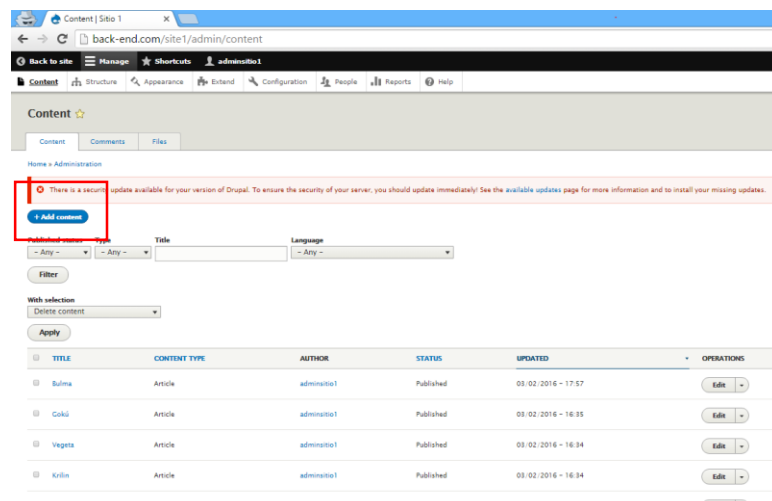




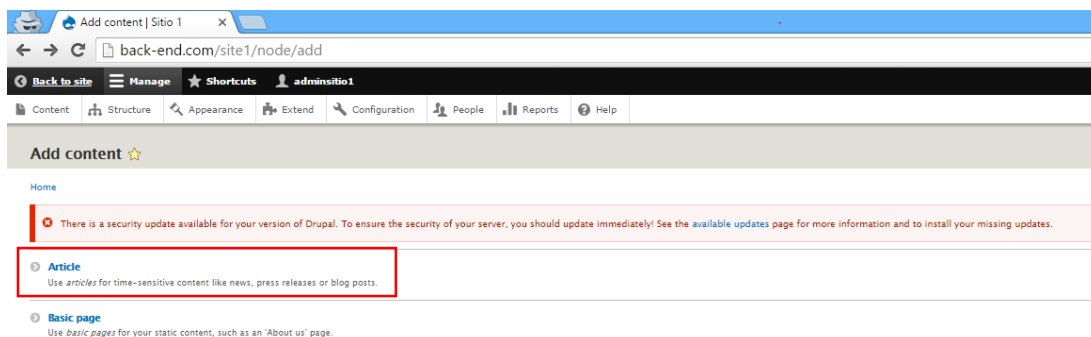
Nos mostrara una página así al ingresar al sitio1, y para agregar contenido nos iremos a CONTENT



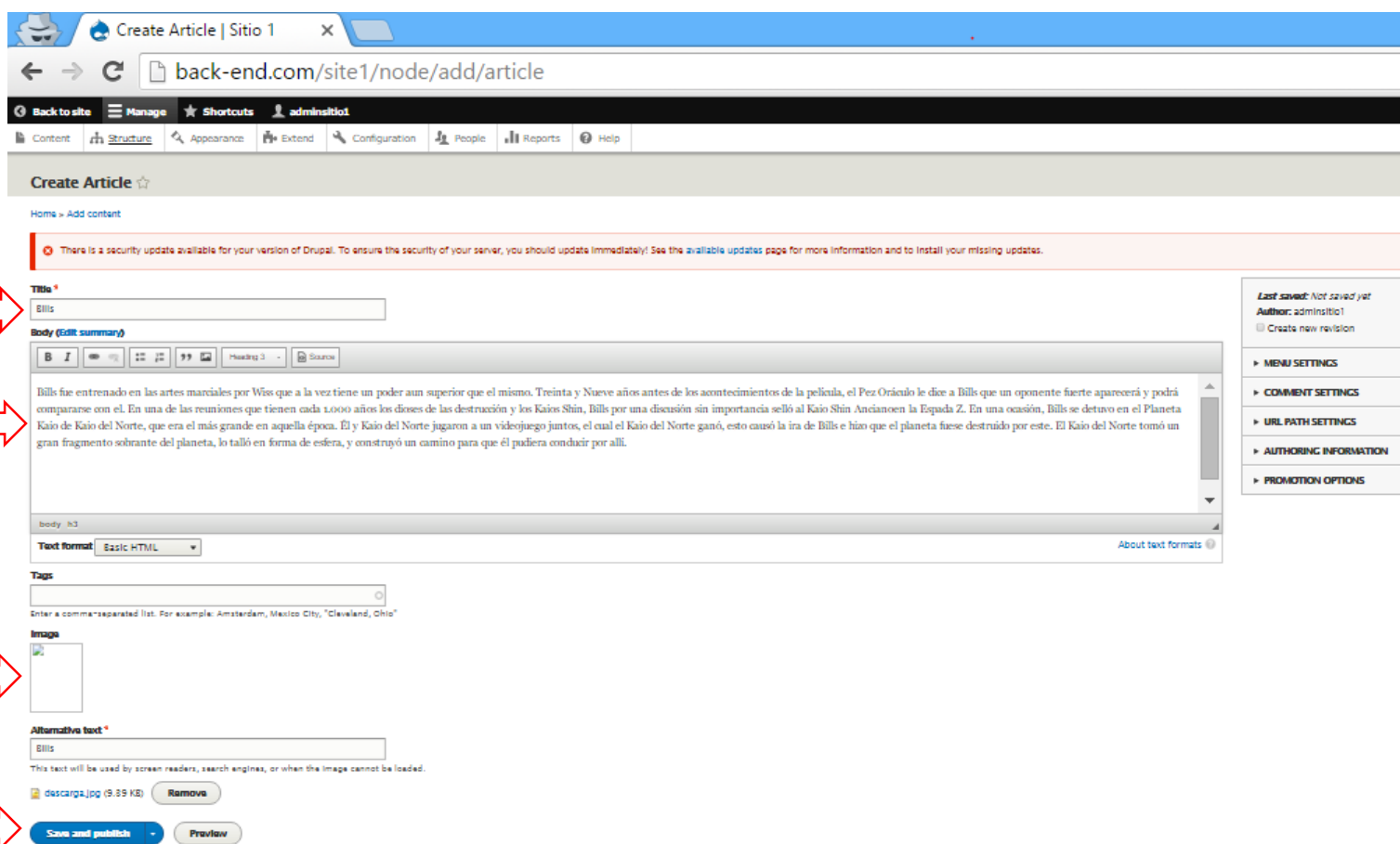
Veremos una pagina asi:



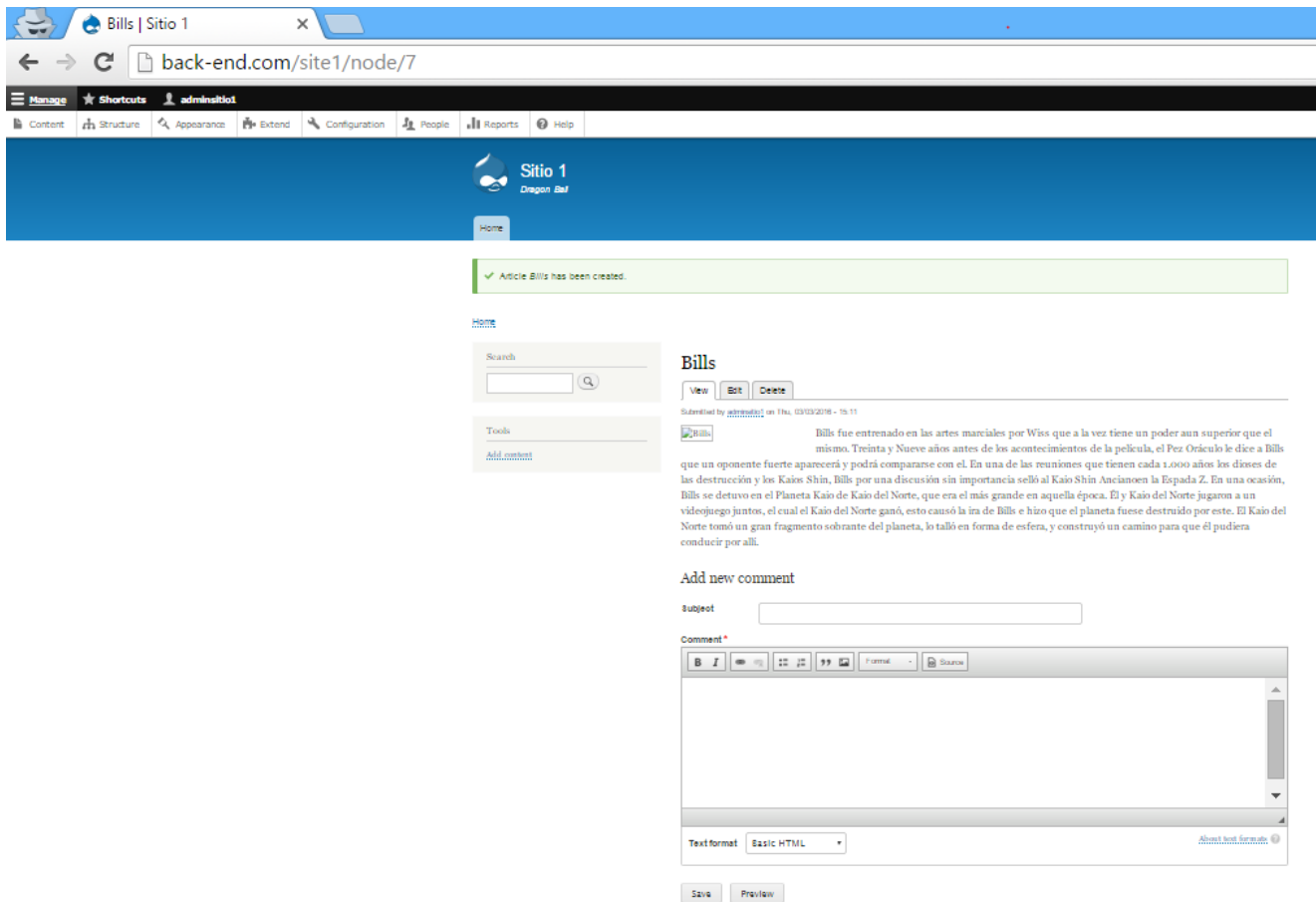
Al seleccionar la opción de Add Content, seleccionaremos Article para comenzar.



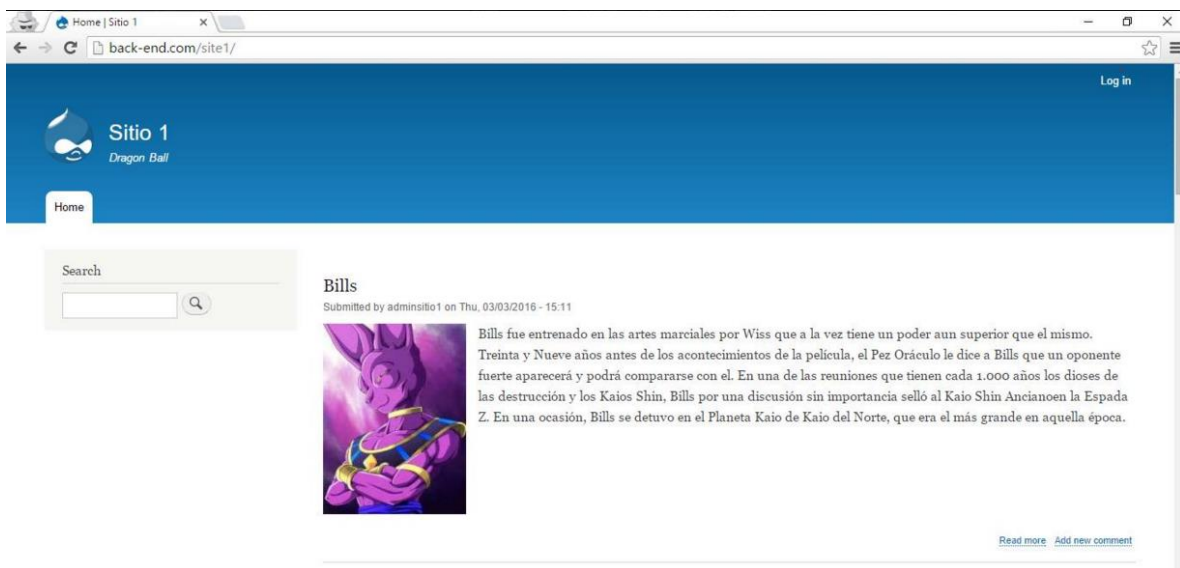
Ahora ingresamos un título, contenido y una imagen.



Nos mostrara la pagina de que se creo exitosamente el articulo que se ingreso.

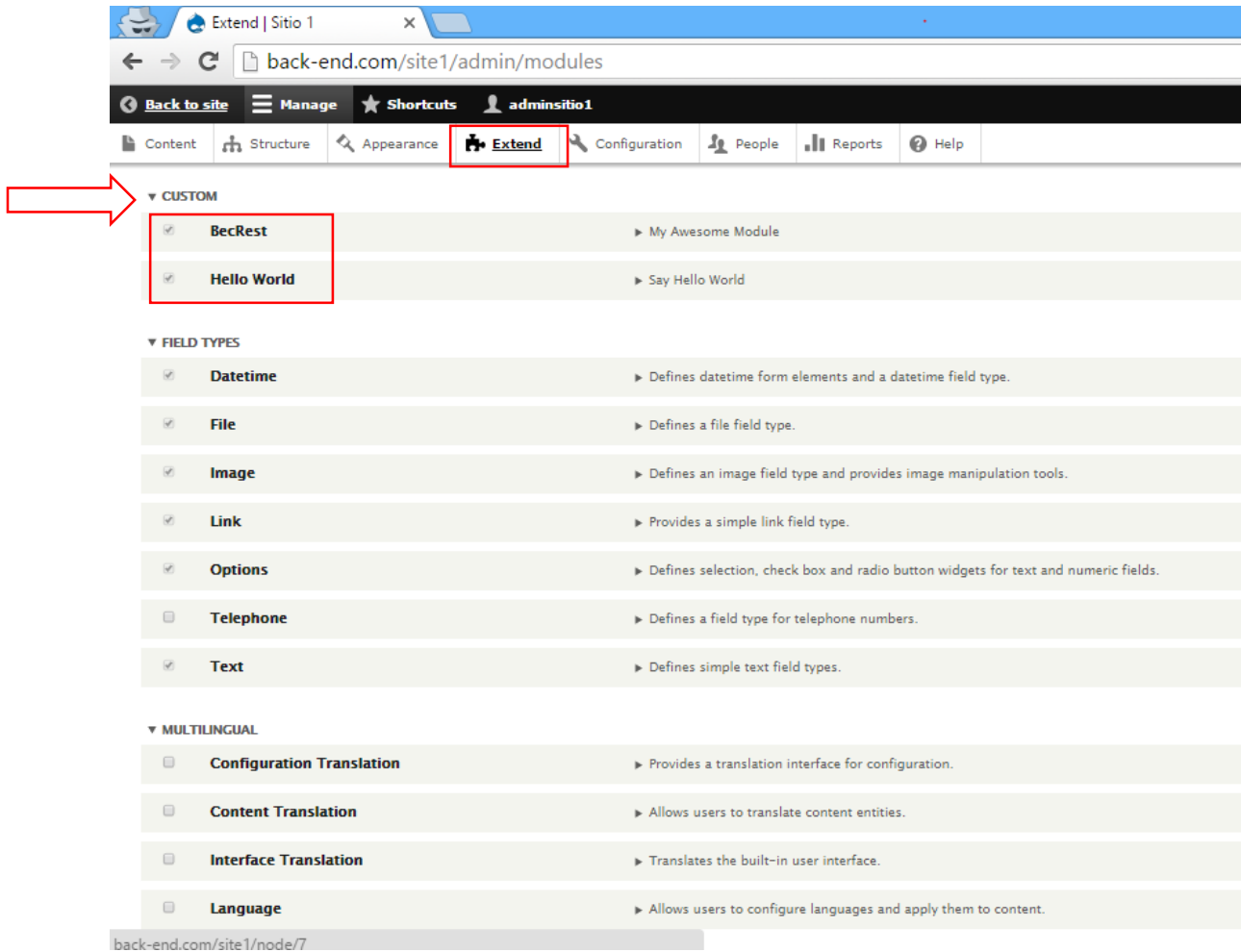


Esta es la vista de nuestro sitio.

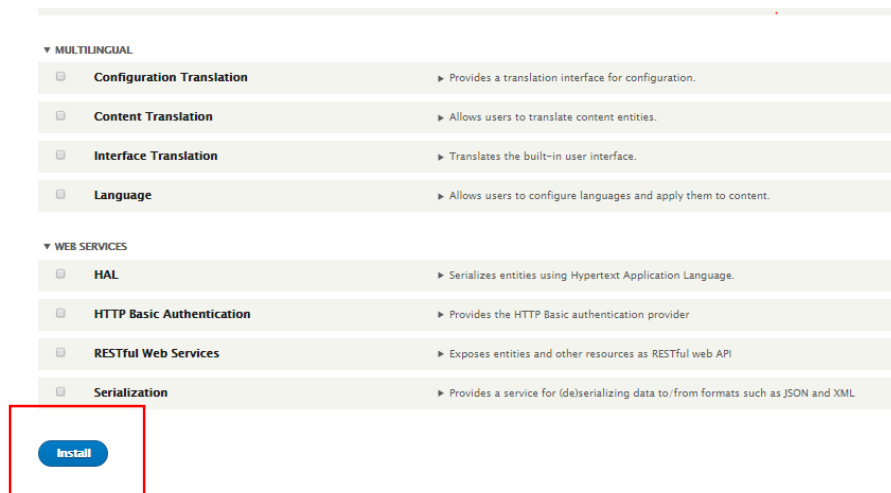


## “AGREGAR UN MODULO”

Lo que se debe de hacer para agregar un módulo es dar click en la pestaña de “EXTEND” y buscar la sección que dice “Custom”; y seleccionar los módulos a instalar.

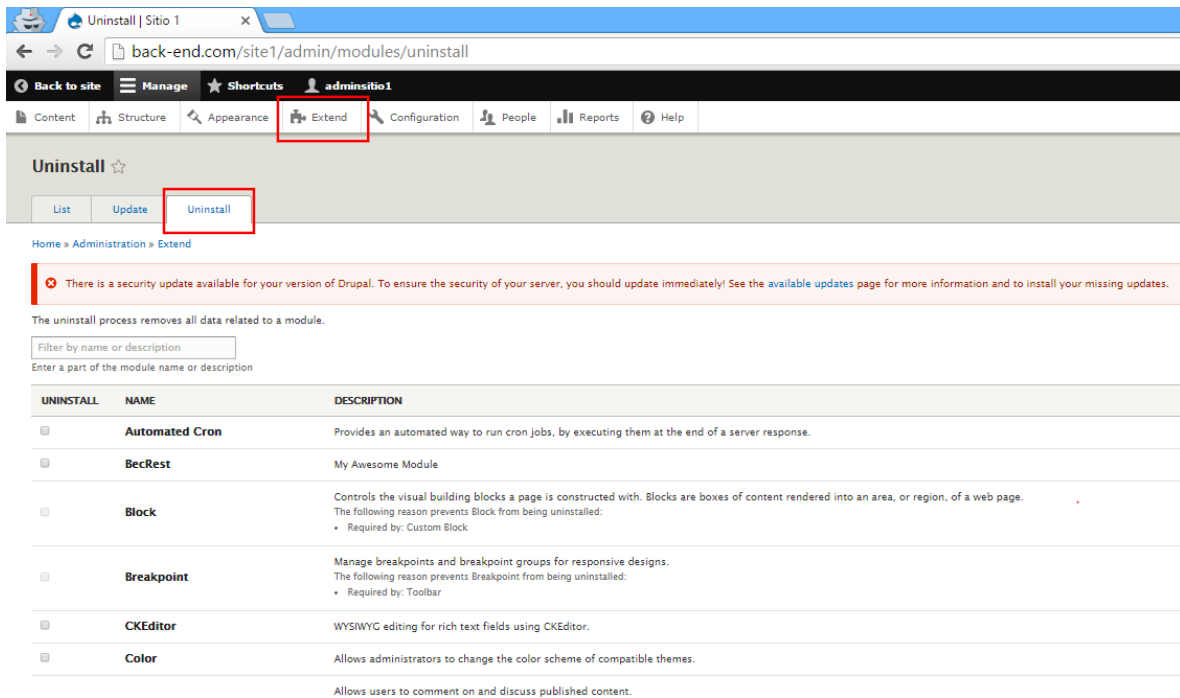


Y después solo se le da click en INSTALL



## “DESINTALAR UN MODULO”

Ingresamos EXTEND y seleccionamos la opción de Uninstall.



Uninstall

Home > Administration > Extend

There is a security update available for your version of Drupal. To ensure the security of your server, you should update immediately! See the [available updates](#) page for more information and to install your missing updates.

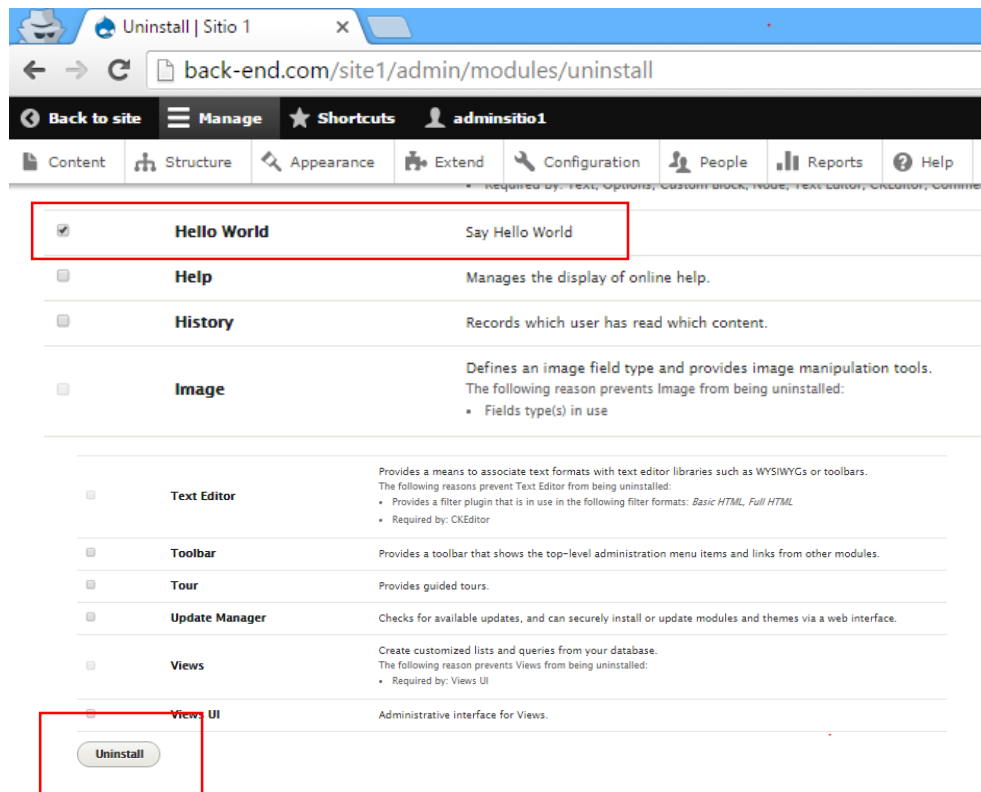
The uninstall process removes all data related to a module.

Filter by name or description  
Enter a part of the module name or description

UNINSTALL	NAME	DESCRIPTION
<input type="checkbox"/>	<b>Automated Cron</b>	Provides an automated way to run cron jobs, by executing them at the end of a server response.
<input type="checkbox"/>	<b>BecRest</b>	My Awesome Module
<input type="checkbox"/>	<b>Block</b>	Controls the visual building blocks a page is constructed with. Blocks are boxes of content rendered into an area, or region, of a web page. The following reason prevents Block from being uninstalled: <ul style="list-style-type: none"><li>Required by: Custom Block</li></ul>
<input type="checkbox"/>	<b>Breakpoint</b>	Manage breakpoints and breakpoint groups for responsive designs. The following reason prevents Breakpoint from being uninstalled: <ul style="list-style-type: none"><li>Required by: Toolbar</li></ul>
<input type="checkbox"/>	<b>CKEditor</b>	WYSIWYG editing for rich text fields using CKEditor.
<input type="checkbox"/>	<b>Color</b>	Allows administrators to change the color scheme of compatible themes.

Allows users to comment on and discuss published content.

Y seleccionamos el modulo a desinstalar; en este ejemplo lo haremos sobre “Hello World” y hasta abajo dar click en UNINSTALL.



Uninstall

back-end.com/site1/admin/modules/uninstall

Back to site Manage Shortcuts adminsitio1

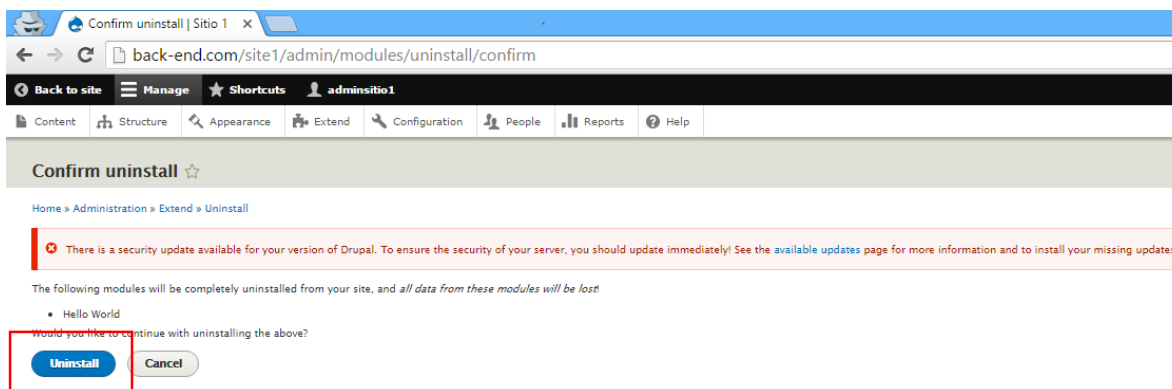
Content Structure Appearance Extend Configuration People Reports Help

<input checked="" type="checkbox"/>	<b>Hello World</b>	Say Hello World
<input type="checkbox"/>	<b>Help</b>	Manages the display of online help.
<input type="checkbox"/>	<b>History</b>	Records which user has read which content.
<input type="checkbox"/>	<b>Image</b>	Defines an image field type and provides image manipulation tools. The following reason prevents Image from being uninstalled: <ul style="list-style-type: none"><li>Fields type(s) in use</li></ul>
<input type="checkbox"/>	<b>Text Editor</b>	Provides a means to associate text formats with text editor libraries such as WYSIWYGs or toolbars. The following reasons prevent Text Editor from being uninstalled: <ul style="list-style-type: none"><li>Provides a filter plugin that is in use in the following filter formats: <i>Basic HTML</i>, <i>Full HTML</i></li><li>Required by: CKEditor</li></ul>
<input type="checkbox"/>	<b>Toolbar</b>	Provides a toolbar that shows the top-level administration menu items and links from other modules.
<input type="checkbox"/>	<b>Tour</b>	Provides guided tours.
<input type="checkbox"/>	<b>Update Manager</b>	Checks for available updates, and can securely install or update modules and themes via a web interface.
<input type="checkbox"/>	<b>Views</b>	Create customized lists and queries from your database. The following reason prevents Views from being uninstalled: <ul style="list-style-type: none"><li>Required by: Views UI</li></ul>
<input type="checkbox"/>	<b>Views UI</b>	Administrative interface for Views.

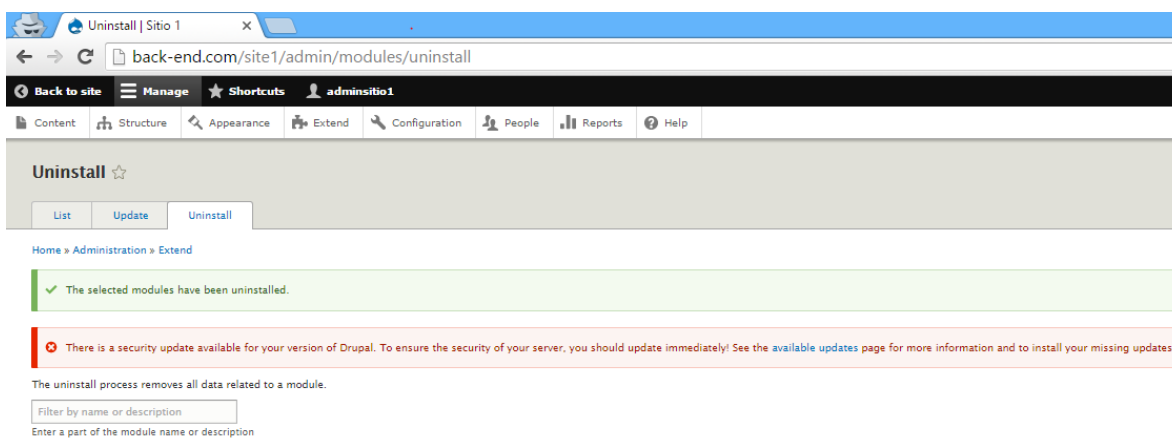
Uninstall



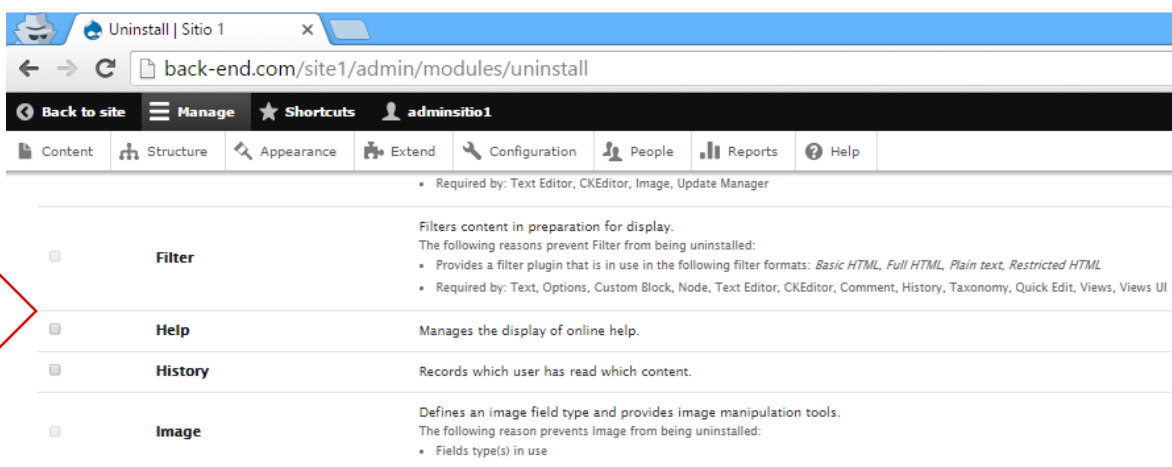
Nos volverá a preguntar si queremos desinstalar el modulo solo damos click en UNINSTALL



Mandara la página que dice que de desinstalo de manera exitosa el modulo

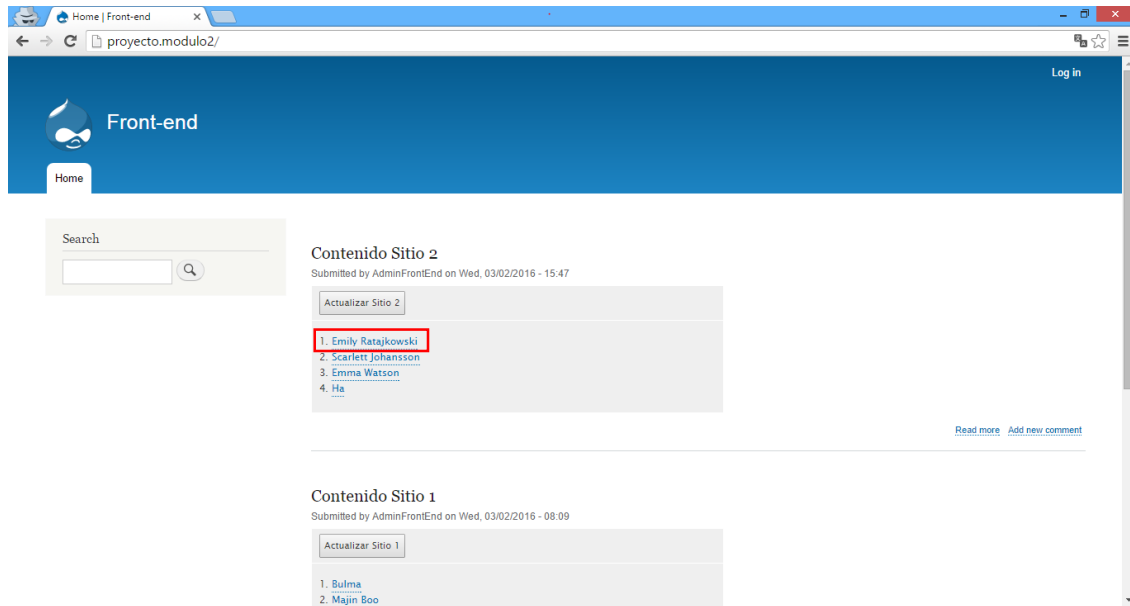


Y si buscamos el modulo ya no se encuentra en la lista

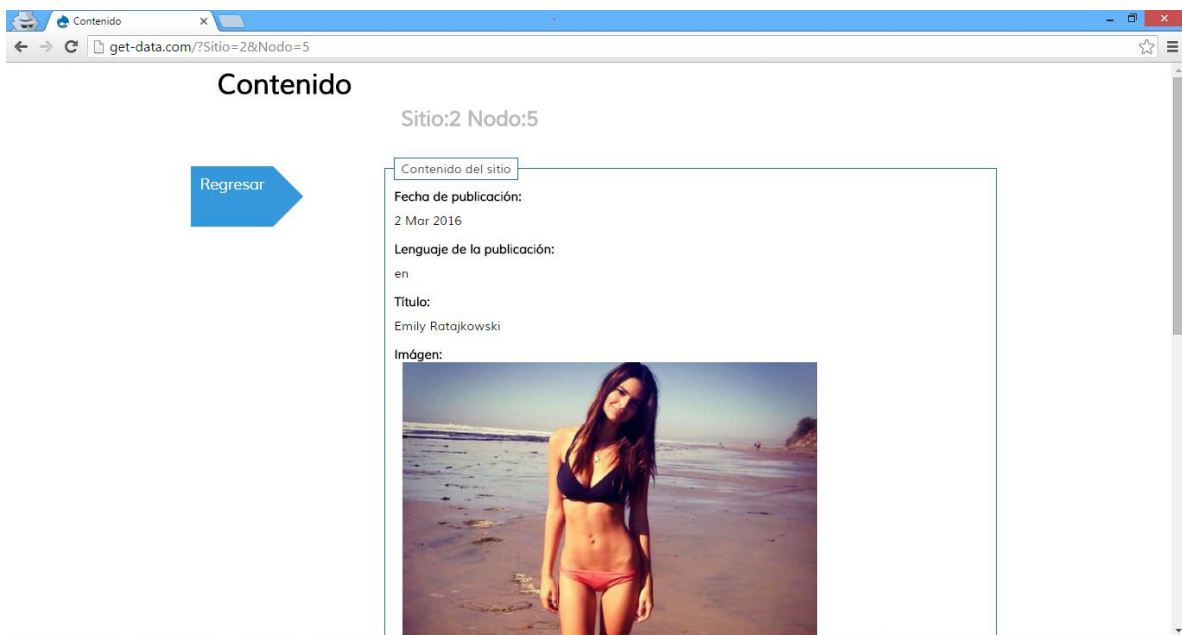


## “INGRESAR A SITIO POR MEDIO DE PROXY INVERSO”

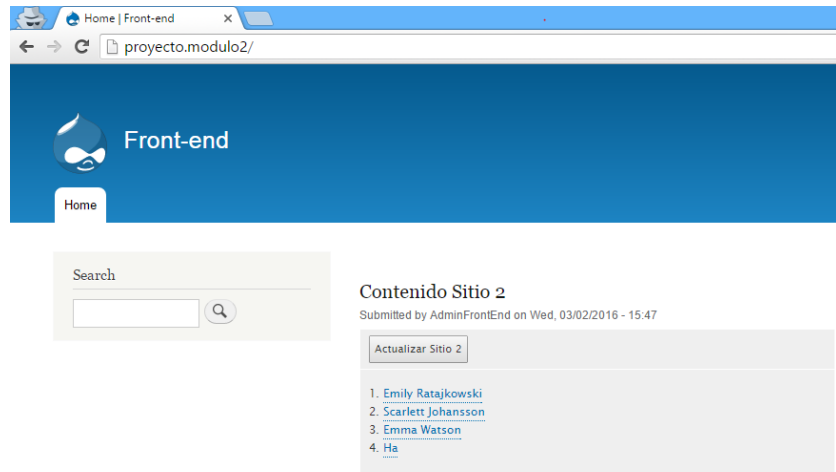
Lo primero que se debe de realizar es ingresar al nombre del server que se le haya asignado antes del re direccionamiento, en este caso es **proyecto.modulo2** que nos mandara a **back-end.com**.



Y si seleccionamos un artículo nos mandara esto:



Y si nos regresamos por medio del botón “REGRESAR” nos manda al inicio de la página.



### **“FUNCIONAMIENTO DEL PROXY INVERSO CON MODSECURITY”**

La manera en la que funciona es relativamente sencilla ya que se tiene un proxy que es el encargado de procesar las peticiones que se realicen al servidor, este toma la petición y si es “confiable” la deja pasar y la redirecciona al front-end, este sitio toma toda la información sobre los artículos que están alojados en el back-end y los muestra.

## “PROTECCION DEL FRONT-END”

Para poder cambiar los modos que tiene ModSecurity en el WAF entramos a el directorio **cd /usr/local/nginx/conf** y editamos el archivo **modsecurity.conf** y si se desea cambiar una de otra se cambia el texto; guardamos y salimos.

```
root@debian:~# cd /usr/local/nginx/conf/  
root@debian:/usr/local/nginx/conf# nano modsecurity.conf
```

### WAF-Solo detección

```
GNU nano 2.2.6 File: modsecurity.conf  
  
# -- Rule engine initialization -----  
  
# Enable ModSecurity, attaching it to every transaction. Use detection  
# only to start with, because that minimises the chances of post-installation  
# disruption.  
#  
SecRuleEngine DetectionOnly  
  
# -- Request body handling -----
```

### WAF-Apagado

```
GNU nano 2.2.6 File: modsecurity.conf  
  
# -- Rule engine initialization -----  
  
# Enable ModSecurity, attaching it to every transaction. Use detection  
# only to start with, because that minimises the chances of post-installation  
# disruption.  
#  
SecRuleEngine Off  
  
# -- Request body handling -----
```

### WAF-Encendido

```
GNU nano 2.2.6 File: modsecurity.conf  
  
# -- Rule engine initialization -----  
  
# Enable ModSecurity, attaching it to every transaction. Use detection  
# only to start with, because that minimises the chances of post-installation  
# disruption.  
#  
SecRuleEngine On  
  
# -- Request body handling -----  
  
# Allow ModSecurity to access request bodies. If you don't, ModSecurity
```

**Nota: En cada uno de los casos se reinicia el servicio nginx**

```
root@debian:/usr/local/nginx/conf# service nginx restart  
root@debian:/usr/local/nginx/conf#
```