Amphora Gate Standalone

EXPOSED

1. Descripción del producto

Amphora Gate es una plataforma para ofrecer servicios de acceso a Internet a los huéspedes de hoteles. Funciona estableciendo un filtrado por dirección MAC de las máquinas de los clientes, permitiendo y tarificando su acceso según la misma o incluso, dependiendo de la boca del switch que reciba la conexión.

2. Vulnerabilidad: Acceso gratuito

Para poder acceder a Internet, debemos conectar con un navegador a cualquier dirección web. Previamente, deberemos configurar nuestra tarjeta WiFi dejando los parámetros de forma automática, para recibir IP mediante DHCP, así como DNS y Gateway.

El sistema interceptará nuestra petición y nos redireccionará a una página propia https://amphora.local/gui/ticket_loginpage_fr.php?mac=00-de-ad-be-ef-00, siendo amphora.local un nombre asignado a uno de los interfaces de red (privados), que corresponderá con nuestro DNS y Gateway. Esta página nos solicita nuestro usuario y clave para darnos de alta en el sistema.

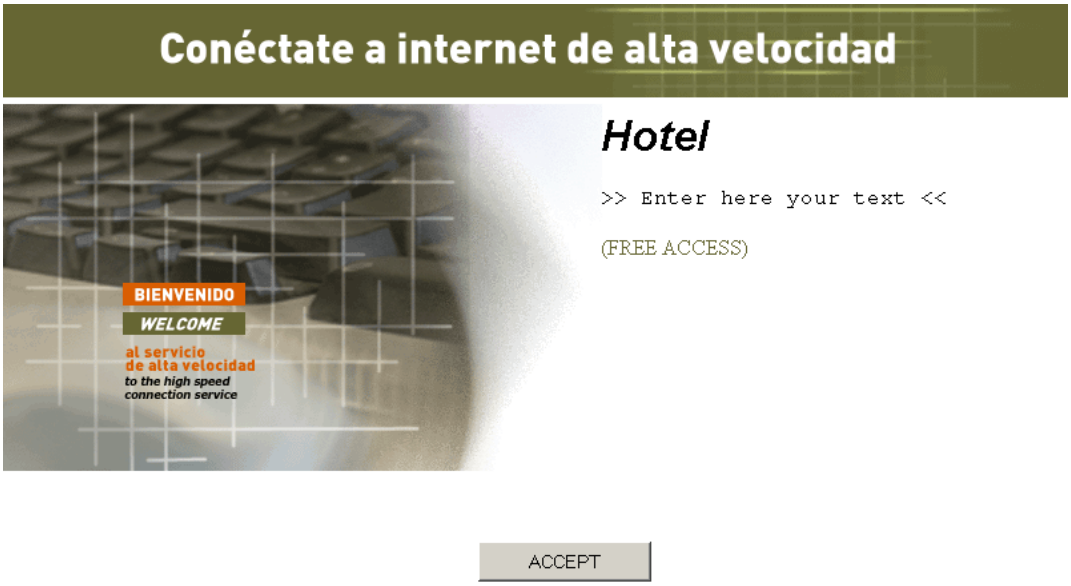
Si indagamos un poco, encontraremos que alguien olvidó configurar Apache de forma correcta… https://amphora.local/gui nos muestra los ficheros que tenemos a nuestra disposición, con nombres bastante descriptivos.

Index of /gui

Name	Last modified	Size	Description
Parent Directory	21-Jul-2003 23:55	-	
clock.php	09-Jul-2003 05:20	21k	
free_loginpage.php	09-Jul-2003 05:20	3k	
gif/	21-Jul-2003 23:55	-	
hab_loginpage_bottom..>	09-Jul-2003 05:20	8k	
hab_loginpage_defaul..>	09-Jul-2003 05:20	2k	
hab_loginpage_fr.php	09-Jul-2003 05:20	1k	
homepage.php	09-Jul-2003 05:20	2k	
homepage_kiosk.php	09-Jul-2003 05:20	1k	
hotel_loginpage.php	09-Jul-2003 05:20	2k	
libreria.php	20-Jul-2003 08:50	10k	
loginpage.php	09-Jul-2003 05:20	1k	
message.php	09-Jul-2003 05:20	1k	
sala_loginpage_botto..>	09-Jul-2003 05:20	4k	
sala_loginpage_defau..>	09-Jul-2003 05:20	2k	
sala_loginpage_fr.php	09-Jul-2003 05:20	1k	
ticket_loginpage_bot..>	09-Jul-2003 05:20	7k	
ticket_loginpage_def..>	09-Jul-2003 05:20	2k	
ticket_loginpage_fr.php	09-Jul-2003 05:20	1k	
txt_config_eng.php	09-Jul-2003 05:20	1k	

Distintas páginas de login, una de ellas muy curiosa (free_loginpage.php), así como distintos ficheros que parecen ser includes ya que su ejecución no devuelve ningún resultado.

Si probamos https://amphora.local/gui/free_loginpage.php …



Solo es necesario pulsar el botón de Aceptar para que nuestra MAC se añada a la lista de MACs autorizadas y tener conexión gratuita sin límite de tiempo.

3. Vulnerabilidad: Acceso al sistema de gestión

Dado que podemos navegar por el sistema de ficheros de Amphora a través de Apache, tratamos de encontrar algo más ya que las especificaciones indican que el sistema se puede controlar con un simple navegador web desde la recepción.

Indagando, encontramos que https://amphora.local/hotel/cualquierfichero deja el browser en un estado catatónico, ya que trata de redireccionarnos a una página que a su vez nos redirecciona a si misma, llamada /hotel/validacion.php

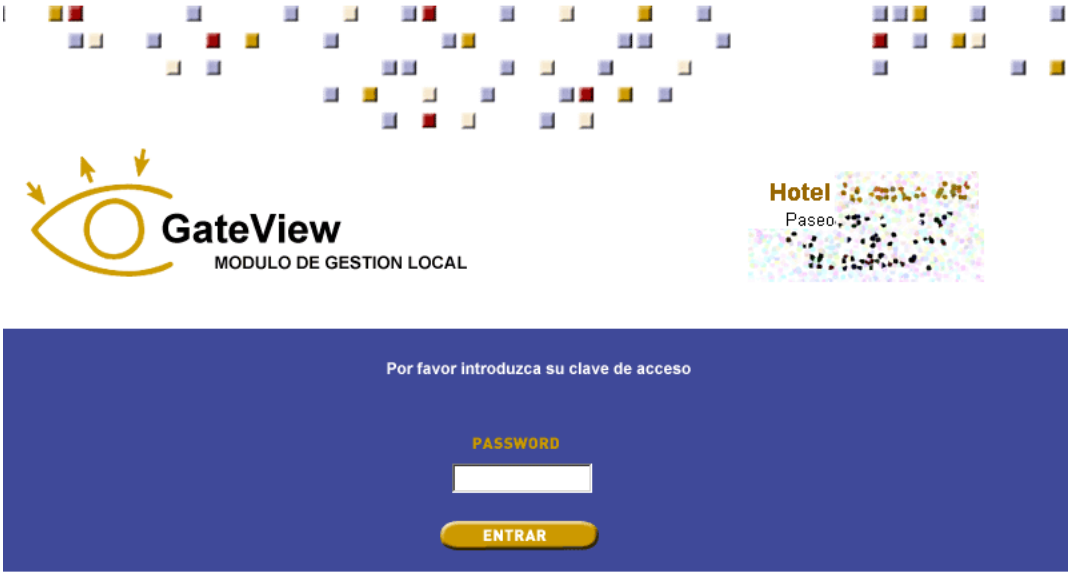
Un vistazo al código fuente de la misma, nos revela lo siguiente:

```
<td class="timeMenu">CLAVE SECRETA :  </td><td><input
name="clave_formulario" value="alfonso" style="width: 200px;"
maxlength="16" type="text"></td>
```

Parece que alguien quiere que encontremos algo....

Haciendo caso una vez más de la intuición y pensando que al que programo la redirección no le explicaron correctamente como descender de directorios, nos planteamos que la redirección como forma de protección podría querer referirse a ../validacion.php en lugar de a ./validacion.php

Comprobamos https://amphora.local/validacion.php y nos encontramos con la bienvenida:



Introducimos la clave conseguida anteriormente, y alehop… acceso completo al sistema de gestión de Amphora Gate.

Incluso podemos generar tickets y modificar sus características para utilizarlos con cualquier otra MAC en otro punto del hotel (esta ya tiene acceso libre gracias al free_loginpage.php).

4. Greetings and Disclaimer

Agradecimientos al Ilmo. Ayto. de Cartagena, así como al hotel que se prestó a nuestras pruebas de acceso.

Así mismo, a la organización y asistentes (aunque no sepáis quien soy y miréis con cara rara a los que entramos por la puerta llevando mas años asistiendo que cualquiera de vosotros) de la Undercon 2004 (gracias barrapunto!), así como a organización y asistentes a BlackCalderoCon 2004.

No se maltrataron físicamente animales menores de 18 años o 50 kg de peso (y si se hizo no hay pruebas que nos incriminen).

No se ha podido comprobar si se trata de una vulnerabilidad en este punto de acceso concreto, o si por el contrario se extiende al resto de los instalados por esta compañía. No obstante si alguien se encuentra interesado en financiar nuestros desplazamientos, puede donar alguna cantidad y en el momento que cubramos gastos, nos encanta viajar :) . Si no, siempre podéis tratar de explotar la vulnerabilidad vosotros (y contarnoslo).

Dedicado al Chupa.