

APÉNDICE B. DATOS DE ENTRENAMIENTO Y PRUEBA

En esta sección se incluyen los datos representativos en protocolo HTTP de las cinco categorías utilizadas por el IDS (Normal, Inyección, Path, SQL y XSS). 70% de esos datos fueron utilizados como entrenamiento y el 30% restante se usó como datos de prueba. Todos los archivos correspondientes a estos datos están disponibles en el CD adjunto a este documento.

El formato de los datos es el de cadenas de caracteres de tamaño variable.

NORMAL - 285 datos

&@_@=@&@_@	/@.exe/@@@	/@-@/@.asp
&@_@=@.txt	/@.exe/@_@	/@-@/@.bat
&@=@/@&@=@	/@.exe/_@_	/@-@/@.cfm
&@=@/@&@_	/@.exe?@=@	/@-@/@.cgi
&@=@&@_@=@	/@/&@=@.ph	/@-@/@.exe
&@=@&@=@/@	/@/@&@_@=	/@-@/@.inc
&@=@_@&@=@	/@/@&@=@&@	/@-@/@.php
&@=@&@=@/@	/@/@&@=@@	/@-@/@.plx
&@=@_@&@=@	/@/@&@=@@@	/@-@/@.txt
&@=@_@&@=@	/@/@.@.@.	/@-@/@_@.@
./@&@=@&@=@	/@/@.@.@.p	/@-@/@_@.c
./@/@&@=@&	/@/@.@@@@	/@-@/@_@.p
./@/@.ini	/@/@.cfm?@	/@-@/@_@/@
./@/@/@.ex	/@/@.ini@@	/@-@/@_@@@
./@/@/@.cgi	/@/@.mdb@@	/@-@/@_@_@
./@/@/@.	/@/@.nsf@@	/@-@-@.@@@
.\@ \@.ini&	/@/@.php@@	/@-@-@.jsp
.cgi?@_@=@	/@/@.php@@	/@-@@@@@@@@
.cgi?@=&@=	/@/@.txt@@	/@@@@@@@@@@
.exe/@_@.e	/@/@/@.@.	/@-@@@@@@@@
.php&@_@=@	/@/@/@.@.	/@@@@@@@@@@
.php?@=@/@	/@/@/@.@/@	@&@[@][@]=
.txt&@=@/@	/@/@/@.@@@	@&@_@=@&@_
/&@=@.php&	/@/@-@@@@@@	@&@=@/@&@_
/@&@=@&@=@	/@/@@@@@@@@@	@&@=@&@_@=
/@&@=@@@&@	/@/@_@.@@@	@&@=@&@=@/
/@.@.@/	/@/@_@.@_@	@&@=@&@=@-
/@.@.@.@.	/@/@_@.asp	@&@=@&@=@&
/@.@.@.php	/@/@_@.cgi	@&@=@&@=@_
/@.@.@.php	/@/@_@.htm	@&@=@.@&@_
/@.@/@@@@@	/@/@_@.log	@&@=@.php&
/@.@@@@@@@@@	/@/@_@.nsf	@.@.@/@.js
/@.asa@@@@	/@/@_@.php	@.@?@=@&@=
/@.asp@@@@	/@/@_@/@.p	@.@?@=@/@/
/@.asp@@@@	/@/@_@@@@@	@.cgi?@_@=
/@.bat@@@@	/@/@_@_@.p	@.cgi?@=&@
/@.cfm?@=@	/@/@_@_@_@	@.cgi?@=@&
/@.cfm@@@@	/@/@=@.@&@	@.dll/_@_@
/@.cgi?@=@	/@-@.@-@.h	@.exe/@_@.
/@.cgi@@@@	/@-@/@/@/	@.exe/_@_@
/@.dbm@@@@	/@-@/@.@/@	@.exe?@=@&
/@.dll/_@_@	/@-@/@.@@@	@.php&@_@=

@.php?@=@/
 @.txt&@=@/
 @/&@=@.php
 -@/./@/./@.
 -@/./@/./@.php
 -@/./@/./@.txt
 -@/./@/./@.xml
 -@/./@/./@.@
 @/./@/./@.@/
 @/./@/./@.as
 @/./@/./@.e
 @/./@/./@.ex
 -@/./@/./@/./@
 @/./@/?@=@&@=
 @/./@&@&@_@=
 -@/./@-@.@/./@
 -@/./@-@.cgi
 @/./@-@.inc.
 -@/./@-@/./@.p
 @/./@-@/./@.ph
 @/./@-@/./@/./@.
 @/./@-@/./@-@.
 -@/./@@@@@@@@@
 @/./@_@.@_@_@
 -@/./@_@.cgi
 -@/./@_@.php
 -@/./@_@/./@.p
 @/./@_@/./@.ph
 @/./@_@_@.ph
 -@/./@_@_@_@_@
 @/./@_@_@_@_@.
 @/./@=@.@&@=
 @/?@=@&@=@&
 @/?@=@&@=@/./@
 @-@&@=@@@@@
 @-@.@-@.ht
 @-@.cgi?@=
 @-@/./@/./@/./@
 @-@/./@.@/./@=
 @-@/./@.cgi/
 -@@@@@@@@@@@@@
 @@@@@@@@@@@@@@
 @-@=@@@@@@@@@@
 @[@][@]=@&
 @\@.ini&@=
 @][@]=@&@=
 @]=@&@=@&@
 @_@&@=@/./@/
 @_@&@=@&@=
 @_@&@=@_@&
 @_@.@?@=@
 @_@.cgi?@=
 @_@.exe?@=
 @_@/./@.dll/
 @_@/./@.exe/
 @_@/./@/./@.cg
 @_@/./@/./@.ph
 @_@/./@/./@_@
 @_@/./@_@_@/./@
 @_@_@.@.cg

@_@_@_@.@.
 @_@=@/./@/./@
 @_@=@&@_@=
 @_@=@&@=@&
 @_@=@&@=@.
 @_@=@.txt&
 @_@=@://./@/
 @_@=@://./@/
 @_@=@@@@@@
 @=*&@=@&@=
 @=*&@=@@@@
 @=./@.asp@@
 @=./@/./@&@=@.
 @=./@/./@&@_@
 @=./@/./@@@@
 @=./@/./@@@@@
 @=:@=@&@=@
 @=@&@[@][@
 @=@&@_@=@&
 @=@&@=@/./@/
 @=@&@=@&@=
 @=@&@=@.@&
 @=@&@=@.ph
 @=@&@=@://
 @=@&@=@-@-
 @=@&@=@@@@
 @=@&@=@_@&
 @=@&@=@_@&
 @=@.@&@_@
 @=@.@&@=@/./@
 @=@.@.org
 @=@.php&@_
 @=@.txt&@=
 @=@://./@/./@
 @=@://./@@@@
 @=@-@-@&@=
 @=@-@@@@@@
 @=@@@@@@@@
 @=@@@@@@@@
 @=@_@&@=@/
 @=@_@&@=@/./@
 @=@_@&@=@&
 @=@_@&@=@_
 @=@_@@@@@@
 [@][@]=@&&
 [@]=@&@=@&
 \@.ini&@=
 \@.ini&@=@
 \@ \@ \@.ini&@
 _@&@=@/./@/./@&
 @&@=@&@@
 _@&@=@&@=@
 @&@=@@&@
 _@/./@.dll/
 _@/./@.exe/
 _@/./@.exe/
 _@/./@.cgi
 _@/./@.php
 @/./@/./@@
 @/./@@_@
 @/./@@/./@.

@@.@.cgi
 @@/./@.dll
 @@/./@.exe
 @@/./@.pwd
 @@/./@_@/
 @@ \@.cnf
 @@_@.@.c
 _@=@&@=@&@
 _@=@&@=@.@
 _@=@.txt&@
 =*&@=@&@=
 =./@/./@&@=@.p
 =./@/./@&@_@=
 =@&@_@=@&@
 =@&@=@.@&@
 =@&@=@.php
 =@&@=@://@
 =@&@=@-@-@
 =@&@=@_@&@
 =@.@&@_@_@
 =@.@&@=@/./@
 =@.php&@_@
 =@.txt&@=@/
 =@-@-@&@=
 =@_@&@=@/./@/
 =@_@&@=@&@
 =@_@&@=@_@
 asp&@=@&@
 cgi?@=@&@=
 exe?@=@&@=
 hp&@_@=@.t
 jsp?@=@&@=
 p&@=@&@=@
 p&@_@=@.tx
 php&@_@=@.
 php?@=@&@=
 php?@=@/./@.
 sp&@=@&@=
 t&@=@/./@&@=
 txt&@=@/./@/./@
 xt&@=@/./@/./@

PATH – 260 datos

"."/./@/./@
 "/./@/./@.ini
 %@..%@..%@
 %@..%@..%@
 %@..%@../@
 %@..%@../@
 %@..%@/./@/./@
 %@../@/./@/./@
 %@../@/./@/./@
 %@/./@/./@.e
 %00/./@
 %00html

&@=.././	//@	@../@
&@=..\.\	/@/@/@/@	@..@../@
&@=.././	/@/@&@=..	@..@../@
&@=@&@=../	..@../@/@/	@..@../@/@
*&@=@&@=..	..@..@..	@..@../@/@/
*.@@@.jsp	..@..@../	@..\.\@
*//.././	..@..@/@/	@..\@
"/././@/	..@../././	@..\@
"/@/@.in	..@//././	@//@
..%@..%@..%	..@=.././.	@.@=.././
..%@..%@..%	..\.\.\.	@. /@
..%@..%@../	..\.\.\@.	@.ini&@=..
..%00@	..Â_..Â_../	@.ntf+++++
..%@..%@..	..Â_..Â_../	@.php @
..box//..	..Â..Â..Â	@/%00@
..nsf//..	./.%@..%@.	@/*//../
..nsf//..	./.%@..%@.	@/./%@/./%@/
.././././	./..//./	@/./%@/./@/
../././//	./..//@.ba	@/./%@/./@/.
../././@	./..//@.in	@/./%@/./@/.
.././@/@/	./...@/./.	-@/..%@..%
.././@/@/	./...@//./	@/..%@..%@
../...//.	./...box//.	-@/...//.
../...//@	./...nsf//.	@/...//.
../@	./...nsf//.	@/./././.
../@%00@	./././././	@/./@/./@/
../@&@=@&@	././@/./@/.	-@/..@..
../@/@/@/	././@/./@/.	@/..@..@
../@/@&@=.	././<@>@('	@/..\@
../@/@&@=@	./..@..@.	@/..€Ç^-..€
..@/./././	./..\@	@/..Â£..Â£
..@//././	./..€Ç^-..€Ç	@/..ÂÂ..ÂÂ
..@/@/@/@	./..Â..Â.	@/./@/./@/.
..\.\.\.	./..Â..Â.	-@//.%@/./%
..\.\.\.	./..Â_..Â_.	@//.%@/./%@
..\.\.\@	./..Â_..Â_.	@//./././
..\.\@	./..Â././@/	@////@
..\.\@.in	./..Â././@.	@///@
..\.\@.\@.	//.%@/./%@/	@//@
..\@	//...//...	-@//@/./@/.
..\@\@.ini	//...//@.b	@-@/...//.
..\@	//...//@.i	@-@/..@..
..€Ç^-../@/	//./././	@-@//.%@/.
..€Ç^-..€Ç^-	////@	@-@-@=..\.
..Â../@/	/@/./././.	-@-@=..//.
..box//../	/@/././@/./	@-@=.././
..nsf//../	/@/..@..	-@-@=..\.
..nsf//../	/@/\.\.\	@-@=..\.\
./"/./@/@.	/@-@/..%@.	@[@]=.././
././././	/@-@/...//	@]=.././.
././././	/@-@/..@.	@_/@/..%@.
./././//@	/@-@//.%@/	@_/@/..%@.
./././@&	/@-@//@/./@/	-@=..\.\.
./././@.	@..%@..%@/	@=..\.\.
./././@/	@..%@..%@/	@= ././ /
./././@/	@..%@../@.	@=&@=../.
././@&@=@	@..%@../@/	@=.././.
././././	@..%@/./@/./	@=.././.
//...//..	@..%2f@	@=.././@
//...//@.	@..%5c@	@=@&@=../.

@=@&@=..\.
 @=@:\&@=@&
 [@]=.././.
 \.\.\.\.
 \.\.\@.i
 \.\.\@.\@
 \.\@.\@.in
]/..%@\%@\%
 _/@/..%@\%@\%
 _/@/..%@\%@\%
 _@&@=.././.
 _@/..%@\%@\%
 @@=|./.
 _@=.././.
 _@=|././.
 _@=@&@=.././.
 _@=@&@=..\.
 |.%2F.|@
 |./|./|.
 |./|./@/@
 |@..\@
 ^./@/@/@.
 ^..€^../@
 ^..€^..€^
 ^..Á^../@/
 ^..Á^..Á^.
 ++++++.nsf
 ++++++++++
 =@&@=..\.
 =@:\&@=@&@
 =@:\@.\@.in
 =@_@&@=../.
 £../@/@/@.
 Â..ÂÂ..ÂÂ.
 Â../@/@/@
 Â..Â../@
 Â..Â./.
 Â^../@/@/@
 Â^..Â^../@
 Â^..Â^..Â^
 Â£../@/@/@
 Â£..Â£../@
 Â£..Â£..Â£
 ÂÂ../@/@/@
 ÂÂ..ÂÂ../@
 ÂÂ..ÂÂ..ÂÂ
 box//../.
 Ç^../@/@/@
 Ç^..€^.././
 Ç^..€^..€
 exe/@_@.ex
 f//.././.
 f//.././.
 f+++++++++
 i&@=..\.\.
 ini&@=..\.
 ini.@.txt
 ni&@=..\.
 nsf//.././.
 nsf//.././.

ntf+++++++
 ox//.././.
 php&@=.././.
 php?@=@://@
 sf//.././.
 sf//.././.
 x//.././.
 xe/@_@.exe

INYECCIÓN-143 datos

&@=";@ "
 &@=;@ /@/@
 '@
 .@/@=;@ @.
 .bat?&
 .bat|@ @:\.
 .EXE? -@ @
 .exe|@
 /@&@_@=;@
 /@.@/@=;@
 /@.bat|@ @
 /@/@ /@/@|
 /@/@.@/@=
 /@/@.bat|@
 /@/@|&@_@
 /@/@|&@_@=
 /@;@ /@/@|
 "; @ `@ `
 `; @ `@ `;
 ;&@=/@/@ /
 ;@ /@/@
 ;@ /@/@|&
 ;@ /@/@|?@
 ;@ @|@
 ;@|@
 ? -n @:\PATH;//@
 ?%0a@
 ?@_@=@&@=|
 ?@=%0a@&@=@
 ?@=;@&@=/@/
 ?@=@&@=;@
 ?|@
 @ /@/@@@@
 @ /@/@|?@=
 @ @:\@.ini
 @&@_@=;@;
 @&@=;@ /@/
 @&@=;@ /@|
 @&@=@&@=|/
 @&@=|/@/@|
 @&@=|@ /@/
 @&@=+'@'=
 '@(@ @
 @.@.org |
 @.@/@=;@ @
 @.bat?&
 @.bat?&

@.bat?&@+@
 @.bat?|@ .
 @.bat|@ @:
 @.cgi?'%0a/
 @.cgi?@=%0a@
 @.cgi?@=;&
 @.EXE? -@
 @.exe|@
 @.exe|@ @:
 @/@ /@/@|
 @/@&@_@= ;
 @/@.@/@=;@
 @/@.bat|@
 @/@;@ /@/@
 @/@|&@_@=@
 @/@=;@ @.@
 @;@|@
 @?/c+@
 @?@%0a@
 @?@=&@=;@
 @?@=;@ /@
 @?@=@&@=;@
 @?|@
 @?|=@
 @ @ @ /@/@&
 -@-@&@=";@
 @-@&@=";@
 @-@&@=;@ /
 @ @ @ @ /@/@
 @-@-@&@=";
 @_@=@';@ @ @
 @|&@_@=@&@
 @|@
 @|@ " @ " @
 @+@+@;\+/@
 @ = @ /@/@@
 @=" -@|@ "
 @=";@ "
 @=";@ "
 @=%0a@
 @=/@/@&@=;
 @=;&@
 @=;@ /@/@@
 @=;@ /@/@|
 @=;@"@
 @=;@|"
 @=;@|@
 @=@ @ @ @_
 @=@ @ @ @ @ @
 @=@";@
 @=@%0a@
 @=@&@=;@ /
 @=@&@=|@ /
 @=@&@=|@ @
 @=@&@=+'@'
 @=@;@|@
 @=@-@&@=;@
 @=@ @ @ @ /@
 @=' @ @ @ @ @ @
 @=@_@&@=;@

```
@=@|&@
@=@|@
@=@+@:@.@.
@='/@/@`@`@
@=' @ @ ` @
@=|/@/@/@|
@=|@
@=|@ /@/@|
@=|@|@|@|@|@|@|@
@="'&+&@=@
@=+'@"'=+'
_@=@&@_@=@<
|&@_@=@&@&@=
|@ " @ " @
|@ /@/@|&@
|@ @:\@|\@.
=" -@|@ "
=":@
=":@ "; @
=%0a@
=&@=;@ /@/
=;&@
=;&@=@/@@
=@ /@/@|&
=@ @|@
=@"@
=@|"@
=@:@|@
=@|&@
=@` @
=@|@
at|@ @:\@|
bat|@ @:\@|
cgi?@=%0a/
cgi?@=&@=;
t|@ @:\@|\@
```

SQL – 11 datos

```
'--@
' @ @
' @ 1==1--@
' group @
' having @
' OR 1==1--@
' UNION @
'; @ @
'; insert @
'; SELECT @
'union @ select
```

XSS – 74 datos

```
)</@>.jsp
")</@>/@.@
"@")</@>/@
"@:"> <@:@
"@:"><@:@>
"@\"></@>.
"><@>@(@)<
&@;@&@;@('
&@=<@>@</@
&@=<@>@=@;
("@"></@>/
)</@:@></
('');&@;/
('');</@>
('')</@>.
(@)</@><!--
.@></@>&@=
.jsp/<@>@ (
/&@;@&@;@ (
/@.jsp/<@>
/@/@/<@>@ (
/@/<@>@(@.
/@:@></@:@
/</@><@>@ (
/<@>@("@" )
/<@>@(''@')
:<@>@(''@')
;@&@;@(''@'
;@(''@');&@
;</@>&@=@&@
;</@>&@=<@>
@ @())</@:
@ @())</@:@
@ @="@.@"?
@ " @ @())</
@")</@>/@.
@&@;@(''@')
@&@_@=<@>@
@&@="><@>@
@&@=@&@=<@>
@&@=@:<@>@
@&@=<@>@.@
@&@=<@>@</
@&@=<@>@=@
@(@.@)</@>
@(\"'@'\")</
@.@);</@>&
@.@)</@>&@
'@;@
`@ `;@();@
|@||@|
~/<@>@(@.@
</@:@></@
</@:@></@:
</@>&@=@&@
</@>&@=<@>
<@:@> <@
```

```
<@:@> <@:
<@:@>@ " @:
<@>@(''@')<
=@&@="><@>
=@&@=@:<@>
=@&@=<@>@.
=@&@=<@>@<
=@&@=<@>@=
=@:<@>@(''@
=@; </@>&@=
=<@>@(@)</
=<@>@(@.@)
=<@>@.@(@.
=<@>@.@</@
=<@>@=@;</
p/<@>@(''@'
sp/<@>@
```