# 그누보드4 취약점 보고서

Written by MaJ3stY
Blog : http://maj3sty.tistory.com
작성일 : 2009.7.22

## 1. 이 글을 쓴 개요.

DB를 대상으로 한 공격이 오래되었음에도 불구하고 아직까지도 해당 취약점이 노출되어 있는 페이지가 많이 있습니다. 그중 하나로 그누보드를 이야기 할 수 있는데 최신버전(현재 : 4.31.11)에서도 이러한 공격에 이용되는 취약점을 발견하였습니다. 사실 예전에도 언급된 적이 있는 취약점입니다. 하지만 아직도 패치 되지 않은 점을 미뤄 봤을 때 암암리에 이 취약점을 악용하여 사이트 위변조와 같은 피해를 입힐 가능성이 크다고 할 수 있습니다. 많은 사람들이 그누보드를 애용하고 있는데 이러한 피해를 조금이나마 막아보고자 이렇게 글을 옮깁니다.

## 2. 취약점 소개.

그누보드 게시판마다 검색기능이 있습니다. 찾고자 원하는 게시물을 손쉽게 찾아주는 아주 고마운 기능입니다.
검색 기능을 이용하여 정상적으로 test를 검색했을 시 아래와 같은 URL 파라메터들이 보입니다.

&sca=&sfl=wr_subject%7C%7Cwr_content&stx=test&sop=and&x=20&y=6

참고로 %7C%7C 는 || 가 urlencoding 된 것입니다.
**wr_subject || wr_content** 부분을 **wr_subjecta || wr_content** 으로 조작하면 아래와 같이 쿼리문에 정보가 훤히 들어나 보이게 됩니다.(빨간색으로 칠한 것이 제가 삽입한 문자입니다.)

where ((INSTR(LOWER(wr_subject**a**), LOWER('test')) or INSTR(LOWER(wr_content), LOWER('test')))) and (wr_num between '-8623' and '1377')
1054 : Unknown column 'wr_subject**a**' in 'where clause'
error file : /gnuboard4/bbs/board.php

where 절 앞에는 생략하였습니다. **LOWER()** 함수를 이용하여 대문자를 소문자로 바꾸고 그것이 해당칼럼에 있는 문자열인지 **INSTR()** 함수로 찾아보는 쿼리문입니다. 하지만 해당 칼럼의 이름을 조작해주자 그러한 칼럼은 없다고 오류를 표시해줍니다.

## 3. 취약점 분석.

취약한 페이지는 에러메시지를 보면 board.php입니다. 하지만 board.php는 최종적으로 결과값을 표시해주는 페이지이기 때문에 에러파일로 명시된 것입니다. 실제 취약한 부분은 common.lib.php 와 list.php입니다.
common.lib.php 파일안에 **get_sql_search()** 함수가 선언되어있고 list.php에서 그 함수를 호출하여 최종 쿼리문을 완성하게 됩니다.

아래에 소스는 **get_sql_search()** 함수에서 문제가 되는 부분 입니다.

```
for ($k=0; $k<count($field); $k++) { // 필드의 수만큼 다중 필드 검색 가능 (필드1+필드2...)
$str .= $op2;
switch ($field[$k]) {
case "mb_id" :
case "wr_name" :
$str .= " $field[$k] = '$s[$i]' ";
break;
case "wr_hit" :
case "wr_good" :
case "wr_nogood" :
$str .= " $field[$k] >= '$s[$i]' ";
break;
// 번호는 해당 검색어에 -1 을 곱함
case "wr_num" :
$str .= "$field[$k] = ".((-1)*$s[$i]);
break;
// LIKE 보다 INSTR 속도가 빠름
default :
if (preg_match("/[a-zA-Z]/", $search_str))
$str .= "INSTR(LOWER($field[$k]), LOWER('$search_str'))";
else
$str .= "INSTR($field[$k], '$search_str')";
break;
}
```

필드수를 하나씩 늘려가며 다중 검색하는 루틴인데 받아오는 필드 값이 **wr_subject || wr_content** 이기 때문에 switch 문에 default: 로 이동하는 것입니다.
preg_match() 함수를 통해서 미리 지정된 정규식과 검색어를 비교한 후 참이 나와
**$str .= "INSTR(LOWER($field[$k]), LOWER('$search_str'))";** 부분을 실행하게 되는 것입니다. 만약 검색어에 숫자가 들어가게 되면 정규식과 맞지 않으므로 else 문으로 이동하여 **$str .= "INSTR($field[$k], '$search_str')";** 이 실행 될 것입니다.

이렇게 하여 **get_sql_search()** 함수의 동작은 끝나게 됩니다. list.php에서 **get_sql_search()** 함수를 호출하여

이러한 동작을 실행하게 되는 것이죠.

list.php 에 문제 되는 부분은 아래와 같습니다.

```
$sql_search = get_sql_search($sca, $sfl, $stx, $sop);
// get_sql_search 함수 호출

$sql_search .= " and (wr_num between '".$spt."' and '".($spt + $config[cf_search_part])."') ";
// 함수 호출 결과와 해당 문자열을 . 연산으로 합친다.

$sql = " select distinct wr_parent from $write_table where $sql_search ";
// $sql 변수에 해당 쿼리문과 $sql_search변수에 저장된 값을 이용하여 완성된 쿼리문을 저장.
```

이 과정 중에 함수를 호출하는 과정에서 오류를 일으키고 그 오류정보가 마지막 과정에 대입되어 쿼리문 전체가 오류페이지에 나타나는 것으로 생각 됩니다.
이 취약점을 아래와 테스트(지인 서버 그누보드 게시판)한 결과 제가 삽입한 쿼리문이 정상적으로 작동하는 것을 확인할 수 있었습니다.

**&sca=&sfl=wr_subject),LOWER(123))))+and+1=2+union+select+char(50)--+%7C%7Cwr_content&stx=test&sop=and**

**출력 결과 : (-1)**

출력 결과가 위와 같은 것은

```
// 번호는 해당 검색어에 -1 을 곱함
case "wr_num" :
$str .= "$field[$k] = ".((-1)*$s[$i]);
break;
```

이러한 루틴이 있기 때문입니다. char(49)로 할 경우 정상적으로 번호가 1인 게시물이 검색이 됩니다.
이 취약점을 통해 테스트 해본 기법은 극히 적지만 DB를 대상으로 한 공격이라면 대부분 가능 할 것이라고 예상이 됩니다.(**ex: SQL injection**)

## 4. 해결 방안

1) GET 방식으로 서버에 전송되는 칼럼 이름을 POST 방식으로 바꿔줘야 합니다.

2) 영어 소,대문자 정규식([a-z],[A-Z])과 숫자 정규식([0-9])를 만들어 이에 해당하는 문자만 입력받게 하는 것입니다.
특수문자들은 사용자가 공격을 하지 않는 이상 거의 쓰지 않는 문자 들 이기 때문에 입력을 받을 필요가 없습니다.

3) 오류에서 보이는 민감한 부분들을 최소화 하는 것입니다.
경로와 라인수만 출력을 한다던지, 아니면 쿼리문 전체가 아닌 오류부분만 출력이 되도록 하는 것입니다.
하지만 이 방법은 나중에 오류부분을 찾을 때 찾는 과정을 조금 복잡하게 만들 수도 있습니다.
**(제가 코딩을 능수능란하게 하지 못하고 임시로 작성한 코드를 테스트할 공간이 없어 검증하지 못하였기에 문서에  코드를 올리지 못 하였습니다.)**

## 5. 이 글을 마치며..

처음 쓰는 보고서이며 이러한 웹 어플리케이션을 분석해보는 것 또한 처음입니다.
제 나름대로 분석하고 쓴 것이므로 내용 또한 완벽하지 않고 위에서 제가 분석한 곳 중에 틀린 곳이나 애매한 곳 등이 있을 것으로 생각이 됩니다. 또한 해결방안을 제시하였지만 그것 또한 완벽하다고는 볼 수 없습니다.
이러한 것들은 조금 더 테스트를 거치신후에 완벽에 가까울 정도로 수정 하시는 것이 좋다고 생각합니다.
이 글로 인하여 이번 취약점이 꼭 패치 되길 바라겠습니다.
읽어주셔서 감사합니다.