
INetCop Security Advisory #2006-0x82-029

Title: zeroboard XSS IP session bypass exploit vulnerability.

0x01. Description

제로보드는 국내에서 대중적으로 사용되는 웹 게시판입니다.

저희 INetCop Security에서는 최신 버전의 제로보드 4.1 pl 7 (2005. 4. 4)에서 XSS (Cross Site Script) 취약점을 발견하였습니다. 기본적으로 제로보드는 사용자의 session이 해킹에 악용되지 않도록 다음과 같은 알고리즘을 사용하여 cookie exploit (spoofing, sniffing) 공격을 차단하고 있습니다.

로그인 후, 세션 처리 부분: --

bbs/login_check.php:

```
24 // 회원로그인이 성공하였을 경우 세션을 생성하고 페이지를 이동함
25     if($member_data[no]) {
26
27         if($auto_login) {
28             makeZBSessionID($member_data[no]);
29         }
30
31         // 4.0x 용 세션 처리
32         $zb_logged_no = $member_data[no];
33         $zb_logged_time = time();
34         $zb_logged_ip = $REMOTE_ADDR; <---- 로그인 시, IP 기록
35         $zb_last_connect_check = '0';
36
37         session_register("zb_logged_no");
38         session_register("zb_logged_time");
39         session_register("zb_logged_ip");
40         session_register("zb_last_connect_check");
```

--

현재 세션 사용자의 IP가 다를때 차단하는 부분: --

bbs/lib.php:

```

94             // 세션 값을 체크하여 로그인을 처리
95             } elseif($HTTP_SESSION_VARS["zb_logged_no"]) {
96
97                 // 로그인 시간이 지정된 시간을 넘었거나 로그인
아이피가 현재 사용자의 아이피와 다를 경우 로그아웃 시킴
98                 if(time()-$HTTP_SESSION_VARS["zb_logged_time"]>
$_zbDefaultSetup["login_time"]||$HTTP_SESSION_VARS["zb_logged_ip"]!=$REMOTE_ADDR)
{
99
100                 $zb_logged_no=""; // 세션 초기화
101                 $zb_logged_time="";
102                 $zb_logged_ip="";
103                 session_register("zb_logged_no");
104                 session_register("zb_logged_ip");
105                 session_register("zb_logged_time");
106                 session_destroy();
107
108                 // 유효할 경우 로그인 시간을 다시 설정
109                 } else {

```

--

해당 코드는 일반적인 cookie exploit을 적절하게 차단하고 있는 것처럼 보입니다.

그러나, 이번 취약점을 분석하는 과정에서 IP session 무력화 기법을 이용하여 해당 알고리즘을 우회할 수 있는 새로운 공격 가능성을 발견하게 되었습니다.

공격 방법에 대한 자세한 사항은 다음 레퍼런스를 참고하시기 바랍니다.

URL: http://x82.inetcop.org/h0me/papers/iframe_tag_exploit.txt

결과적으로, 해커가 관리자의 브라우저를 통해 임의의 코드를 관리자 세션 권한으로 실행할 수 있게 됩니다.

0x02. Vulnerable Packages

Vendor site: <http://www.nzeo.com/>

Zeroboard 4.1 pl 7 버전을 포함한 이하 버전

-zb41pl7.tar.Z

0x03. Exploit

이 문제점에 대해서 두 가지의 Proof-of-Concept exploit을 보유하고 있습니다.

정확한 XSS 취약점은 메모함의 제목 부분과 사용자 자신의 정보를 기록하는 email, homepage 입력란 에서 발생합니다. 관리자가 사용자의 레벨 권한을 수정하기 위해 사용자 정보 페이지에 접속했을 때, 공격 코드가 실행될 수 있으며, 가장 일반적으로 악의적인 코드를 쪽지 제목에 포함시켜 전달하는 공격 방법이 있습니다.

공격 결과, 해커는 관리자 웹 페이지 header 포함 기능을 통해 임의의 PHP 공격 코드를 Injection 하여 시스템 내부 명령을 실행할 수 있습니다. 또한, 관리자의 패스워드를 변경하거나, 일반사용자의 권한을 관리자의 권한으로 상승시킬 수 있습니다.

INetCop Security에서는 exploit이 악용되는 사례가 없도록 하기 위해 POC 공격 코드를 제공하지 않을 것입니다. POC 공격 코드를 시험한 결과는 다음과 같습니다.

```
[x82@localhost html]$ ./0x82-zer0user
0x82-zer0user - Zeroboard 4.1 pl7 send message iframe+ XSS exploit
Usage: 0x82-zer0user [-options] [arguments]

    -t [host]      - Host address
    -c [port]      - Host port number
    -b [name]      - Board name
    -i [id]        - Normal user id
    -p [passwd]    - User password
    -u [path]      - zboard url path
    -h            - Help screen.

Ex> 0x82-zer0user -t localhost -b free -i hax0r -p pass -u 'zboard/bbs'
[x82@localhost html]$ █
```

POC exploit code 실행 과정:

호스트 주소, 게시판 경로 및 이름, 게시판 일반사용자 id와 password 정보를 적어서 실행합니다.

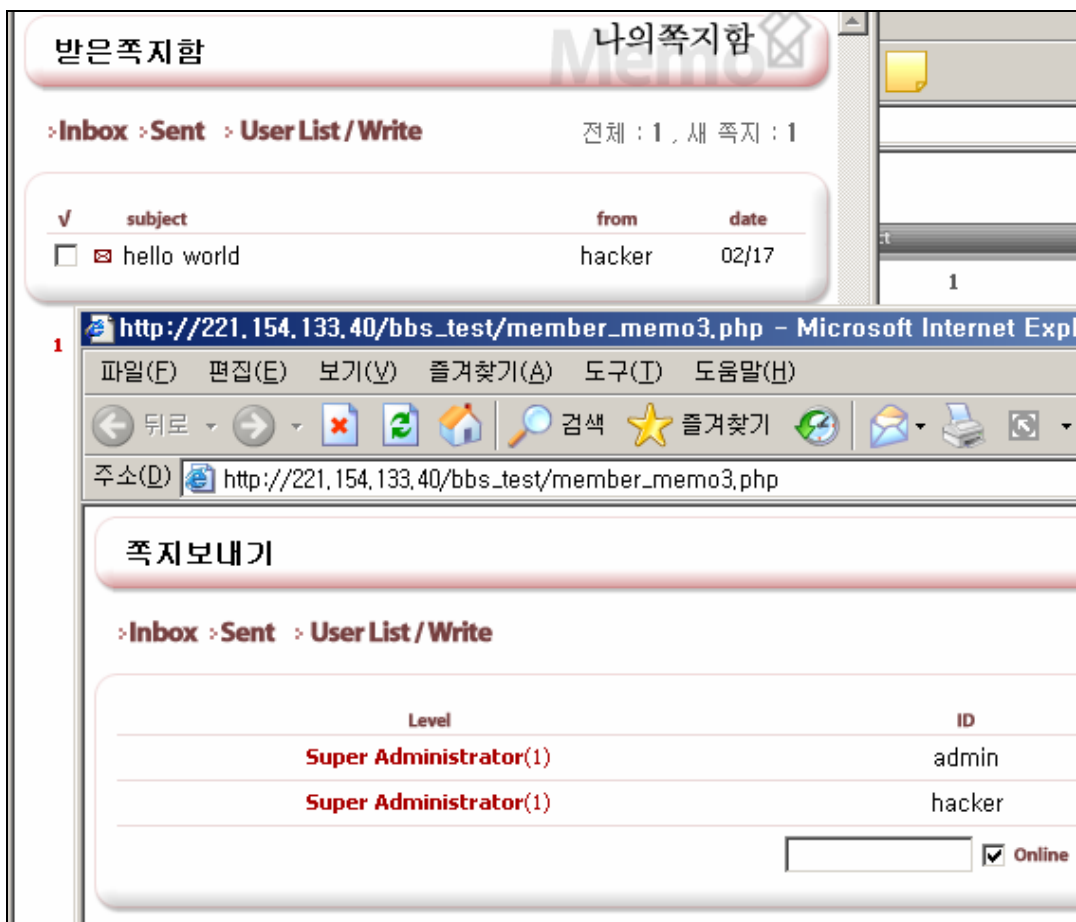
```
[x82@localhost html]$ ./0x82-zer0user -t 221.154.133.40 -bboard1 -i hacker -p 1212 -u 'bbs_test'

0x82-zer0user - Zeroboard 4.1 p17 send message iframe+ XSS exploit

[+] login success.
[+] group_no is 1
[+] member_no is 9
[+] exploit send successfully.

[x82@localhost html]$ █
```

exploit을 통해 공격 코드를 admin 사용자에게 보냅니다.



관리자가 쪽지 함에 접속하자 (이미 제목에서 공격코드가 실행되므로) 현재 접속 중이던 일반 사용자의 권한이 Super Administrator로 상승되는 것을 볼 수 있습니다. 이 밖에도, 게시판 그룹 header 포함 기능을 통해 시스템 내부 명령어 실행이 가능합니다. (해커에 의한 원격 명령어 실행 공격 가능)

0x04. Patch

INetCop Security에서는 해당 취약점을 보안하기 위해 총 두 가지의 patch 코드를 작성하여 배포합니다. patch 코드 다운로드 URL은 다음과 같습니다.

URL: http://inetcop.net/upfiles/Zeroboard-4.1_pl7_patch.tgz

2006년 02월 25일 벤티의 정식 patch가 발표되었습니다. 정식 patch 코드를 다운로드 하려면 다음 URL을 방문해주세요.

URL: http://www.nzeo.com/bbs/zboard.php?id=cgi_bugreport2&no=5406

감사합니다.

--

By "dong-houn yoU" (Xpl017Elz), in INetCop(c) Security.

MSN & E-mail: [szoahc\(at\)hotmail\(dot\)com](mailto:szoahc@hotmail.com),
[xploit\(at\)hackermail\(dot\)com](mailto:xploit@hackermail.com)

INetCop Security Home: <http://www.inetcop.org>

My World: <http://x82.inetcop.org>

GPG public key: <http://x82.inetcop.org/h0me/pr0file/x82.k3y>

--