Hack-me.org 29번

Apple Online Store

Xero

박준혁 (한국디지털미디어고등학교 1학년)

2011-09-20

wnsgurzxc@nate.com

들어가면 다음과 같이 메시지들과 함께 폼이 보인다.
그러나 폼은 작동하지 않는다.

또한 소스를 보아도 아무 수상한 점이 보이지 않는다.
여러 시도를 거치다 애플이라는 말에 User-Agent 체크문제라 생각해 파로스로 Request를 트랩을 걸고 User-Agent를 애플의 것으로 바꾸어 들어가보았다.
User-Agent: Mozilla/5.0 (iPhone ; U; CPU iPhone OS 3_1_2 like Mac OS X;ko-kr) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7D11 Safari/528.16
Host: hack-me.org

그러자 다음과 같이 다른 페이지가 나타났다.

Hightlight로 본 소스이다.

해석하자면 get형식으로 id변수에 admin 값을 주고 post형식으로 pass변수에 cherishcat 값을 주고 쿠키의 level값이 랜덤으로 1~5에서 생성된 값과 같으면 된다.

```
<? error_reporting(0); ini_set('display_errors', 0); if (!defined("_HACK_ME_")) exit; $secret_password = '????????????????????????????????'; // :) echo "Welcome to Apple mobile store!<br><br><img src = '/images/apple.jpg'><br><br><a href = /show_source.php?file=prob21_apple&type=source target=_blank>Source</a><br> <a href = /show_source.php?file=prob21_apple&type=highlight target=_blank>Highlight</a><br><br>"; if(isset($_GET['id']) &&isset($_POST['pass']) &&isset($_SESSION['userID'])) { if($_GET['id'] == 'admin' && $_POST['pass'] == 'cherishcat') { if($_COOKIE['level'] == rand(1, 5)) echo
```

"Hellooooooo! {$_GET['id']}, Long time no see! Password is <!--" . $secret_password . "-->₩n
"; else echo "boooooooooooooo!₩n
"; } else { echo "Welcome guest₩n
"; } } ?>

파로스로 트랩을 걸어서 위의 소스대로 처리해 답을 얻어보자.
POST 값을 보낼것이므로 post형식으로 바꾸고 주소에 id=admin을 추가했다.
그리고 post형식이므로 content-type을 추가했고 쿠키에 level도 추가하였다.
POST http://hack-me.org/index.php?p=challs&prob=Apple+Online+Store&id=admin HTTP/1.1
Accept: */*
Referer: http://hack-me.org/index.php?p=challs
Accept-Language: ko-KR
User-Agent: Mozilla/5.0 (iPhone ; U; CPU iPhone OS 3_1_2 like Mac OS X;ko-kr) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7D11 Safari/528.16
Host: hack-me.org
Proxy-Connection: Keep-Alive
Pragma: no-cache
Cookie: PHPSESSID=1jo4534p0g8ccr8fcrgn0h9ee6; level=3
Content-Type: application/x-www-form-urlencoded
pass=cherishcat

쿠키의 level 값을 1~5까지 랜덤으로 비교하므로 약간의 운이 필요하다.
level값이 틀리면 boooooooooooo!라는 문자열을 나타내고 맞으면 답을 출력한다.

Level 값이 맞으면 다음과 같이 password is 라는 문자열이 나온다.

보이지 않아서 소스를 보았더니 <!--Sending_get_and_post_variable_together--> 라는 주석이 있고 인증에 성공했다.

Key : Sending_get_and_post_variable_together