

# 컴퓨터보안 실습

## 워게임 연계형 웹해킹 문제 (NATAS) 실습

# 실습 목표

---

- 실습 내용 및 목표

- 앞서 실습한 웹 분석 및 기초문제를 토대로 연계형 웹해킹 문제를 실습한다.
- 1-3 단계의 풀이시간은 5분, 4-5단계는 10분으로 하며 이후 풀이과정을 보고 학습한다.
- 각 문제 풀이 및 과정 캡처 후 제출
  - kor\_moon@naver.com

# NATAS 준비

- 준비 및 URL 설명

<http://natasX.natas.labs.overthewire.org>

- X를 통해 각단계의 레벨 넘버를 입력하여 X단계문제 페이지로 접속
- 비밀번호는 문제를 풀면 다음 레벨 계정의 패스워드가 주어지므로 해당 패스워드로 접속이 가능

- 시작

- [Natas0]
- Username: natas0
- Password: natas0
- URL: <http://natas0.natas.labs.overthewire.org>

# 풀이 : NATAS 0

- 페이지 소스보기를 하면 주석으로 적혀 있는 패스워드를 발견할 수 있음

```
<html>
<head><link rel="stylesheet" type="text/css" href="http://www.overthewire.org/vargames/natas/level.css"></head>
<body>
<h1>natas0</h1>
<div id="content">
You can find the password for the next level on this page.
<!--The password for natas1 is gtVrDuiDfck831PqWsLEZy5gyDz1clto -->
</div>
</body>
</html>
```

# 풀이 : NATAS 1

- 마우스 이벤트가 막혀있으므로 다른 방법을 이용



```
<html>
<head><link rel="stylesheet" type="text/css" href="http://www.overthewire.org/wargames/natas/level.css"></head>
<body oncontextmenu="javascript:alert('right clicking has been blocked!');return false;">
<h1>natas1</h1>
<div id="content">
You can find the password for the
next level on this page, but rightclicking has been blocked!
<!--The password for natas2 is ZluruAth0k702HqmDeT1Uij2Zv#y2uBi -->
</div>
</body>
</html>
```

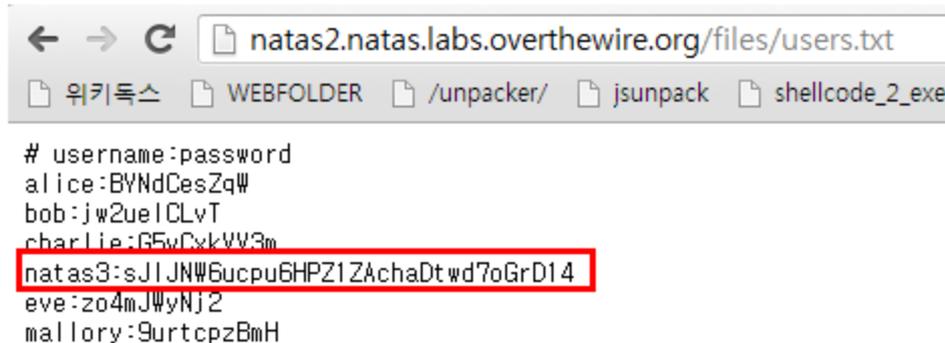
# 풀이 : NATAS 2

- 해당 페이지에서는 패스워드를 찾을 수 없으므로 다른 페이지를 찾아봐야 함

```
<html>
<head><link rel="stylesheet" type="text/css" href="http://www.overthewire.org/wargames/natas/level.css"></head>
<body>
<h1>natas2</h1>
<div id="content">
There is nothing on this page

</div>
</body></html>
```

- 페이지에는 표시가 되지 않았지만 이미지가 하나 링크되어 있음(패스워드와 관련이 없음)
- 하지만 파일경로 주소를 유추할수 있음

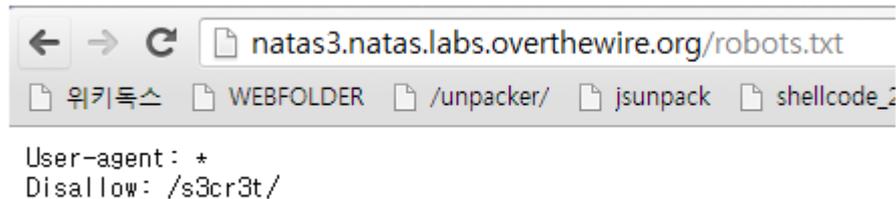


```
← → ↻ natas2.natas.labs.overthewire.org/files/users.txt
[ 위키독스 ] [ WEBFOLDER ] [ /unpacker/ ] [ jsunpack ] [ shellcode_2_exe ]

# username:password
alice:BYNdCesZq#
bob:jw2ue1CLvT
charlie:G5vCvkVV3m
natas3:sJIJNW6ucpu6HPZ1ZAchaDtd7oGrD14
eve:zo4mJWynJ2
mallory:9urtcpzBmH
```

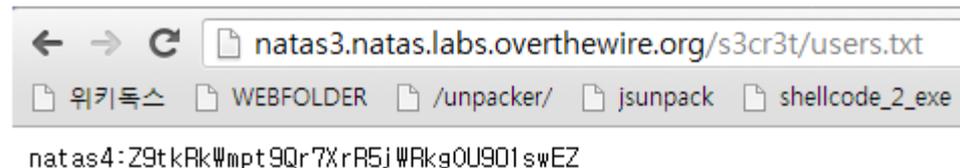
# 풀이 : NATAS 3

구글봇이 크롤링을 하지 못하는 까닭으로 대표적인 것은 robots.txt 파일이 있음



```
← → ↻ natas3.natas.labs.overthewire.org/robots.txt
위키독스 WEBFOLDER /unpacker/ jsunpack shellcode_2
User-agent : *
Disallow : /s3cr3t/
```

접근하지 못하게 설정되어 있는 디렉토리가 하나 이고 디렉터리에 있는 user.txt 파일을 오픈하면 계정정보가 존재



```
← → ↻ natas3.natas.labs.overthewire.org/s3cr3t/users.txt
위키독스 WEBFOLDER /unpacker/ jsunpack shellcode_2_exe
natas4:Z9tkRk#mpt9Qr7XrR5jWRkg0U901swEZ
```

# 풀이 : NATAS 4

natas4.shtml 파일에 접근이 금지 되었고 접근 할 수 있는 방법은 natas5 계정의 문제 도메인을 통해서만 접근이 가능하다고 함

natas5의 패스워드를 모르기 때문에 해당 페이지에 접속한 것으로 위 말은 말이 되지 않는다. 그렇다면 간단하게 패킷을 조작하여 natas5의 도메인인것으로 위장

```
GET / HTTP/1.1
Host: natas4.natas.labs.overthewire.org
Proxy-Connection: keep-alive
Cache-Control: max-age=0
Authorization: Basic bmFOYXMO0lo5dGtSaIdtcHQ5UXI3WHJSNWpXUmtN1U5MDFzd0Va
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/27.0.1453.116 Safari/537.36
Referer: http://natas5.natas.labs.overthewire.org/
Accept-Encoding: gzip, deflate, sdch
Accept-Language: ko-KR,ko;q=0.8,en-US;q=0.6,en;q=0.4
Cookie: __utma=176859643.1742905105.1372047281.1372047281.1372047281.1;
__utmb=176859643.15.10.1372047281; __utmc=176859643;
__utmsz=176859643.1372047281.1.1.utmcsr=google|utmccn=(organic)|utmcmd=organic|utmctr=(not%20provided)
```

http 헤더를 보면 referer 필드가 존재한다. 해당 필드는 접속 페이지 이전에 어디서 접속하였는지 표시해주는 필드이다. 그러므로 해당 필드를 natas5의 문제 도메인으로 조작 하여 접속함

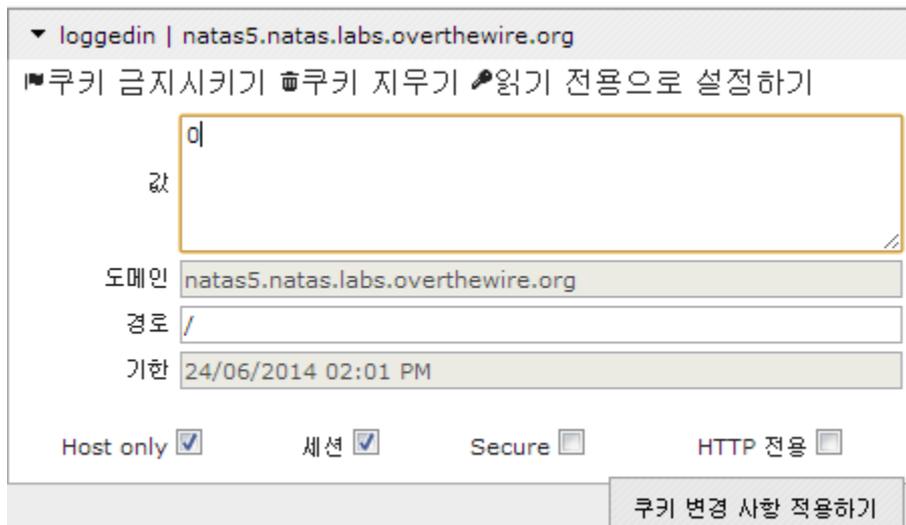
# 풀이 : NATAS 5

엑세스를 요구하며 로그인페이지가 나옴

로그인을 해서 들어왔는데 로그인이 되지 않았다면 우리는 두 가지를  
경우를 생각할 수 있음

- 쿠키의 로그인을 판별하는 어떤 변수의 값이 잘못 설정된 경우
- 로그인 세션이 해제된 경우

## 1차로 쿠키값을 확인



The screenshot shows a browser's developer tools window with the 'loggedin' cookie selected. The 'Value' field contains the number '0'. The 'Domain' is 'natas5.natas.labs.overthewire.org', the 'Path' is '/', and the 'Expires' is '24/06/2014 02:01 PM'. At the bottom, there are checkboxes for 'Host only' (checked), '세션' (checked), 'Secure' (unchecked), and 'HTTP 전용' (unchecked). A button at the bottom right says '쿠키 변경 사항 적용하기'.

loggedin 라는 쿠키변수의  
값이 0이기 때문에  
1로바꾸어 유효하게  
만들어 다시 페이지를  
불러옴

Q & A