

정보보호론 실습

워게임 / Webhacking.kr

실습 내용

- 실습 사이트 소개
- 회원가입 문제 확인
- 회원가입 문제 풀이
- Q & A

실습 사이트 소개

Wargame.kr (<http://webhacking.kr/>)



회원가입 문제 확인

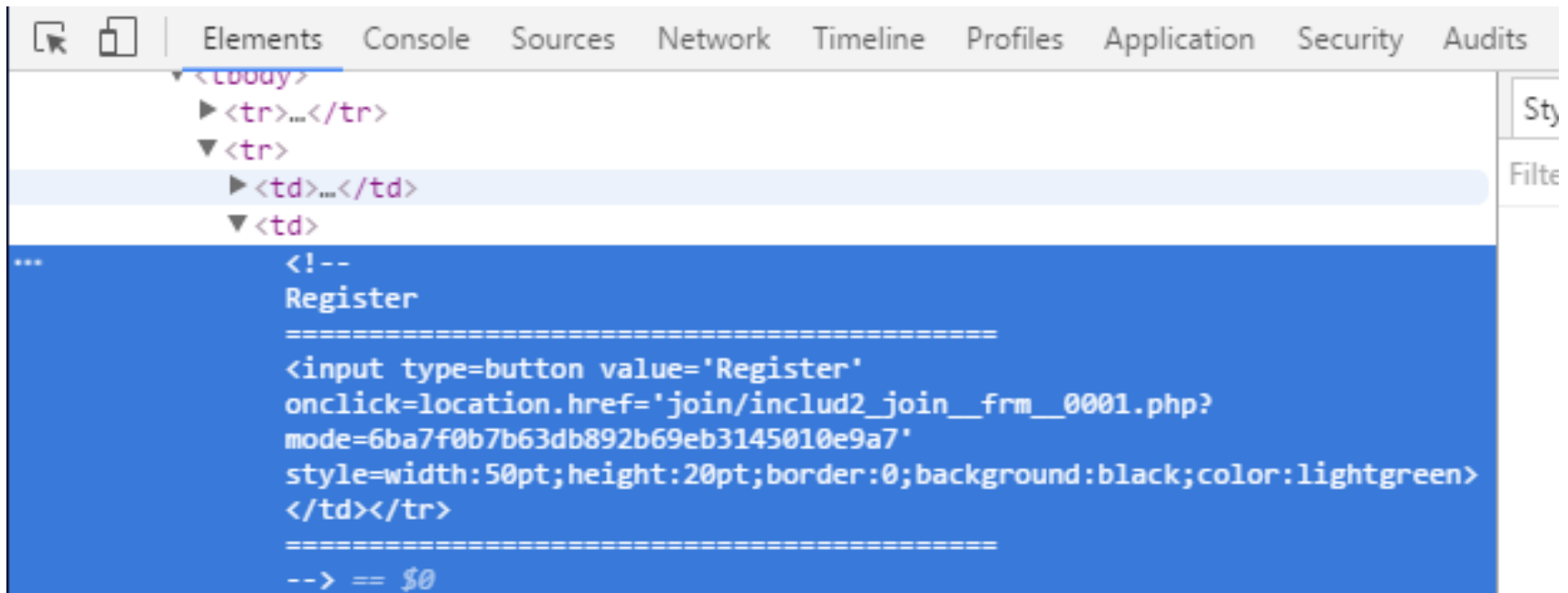
- 회원가입 문제 확인
- 회원가입 버튼 찾기
- **Base64 Decode** 사이트 = <http://www.convertstring.com/ko/EncodeDecode/Base64Decode>



회원가입 문제 풀이

• 가입페이지 찾기. 첫번째 방법

- '무엇을 해킹하는 문제일까?' 고민
- 소스코드 확인(F12)
- 페이지 소스 코드 분석 -> URL 붙여넣기(더블클릭 or 오른쪽클릭 편집)



The screenshot shows the 'Elements' panel of a web browser's developer tools. The DOM tree is expanded to show a table structure. The selected element is a table cell containing a button. The button's HTML code is displayed in the right-hand pane, showing an `onclick` event handler that triggers a PHP script. The button has a black background and light green text.

```
...  
<!--  
Register  
=====
```

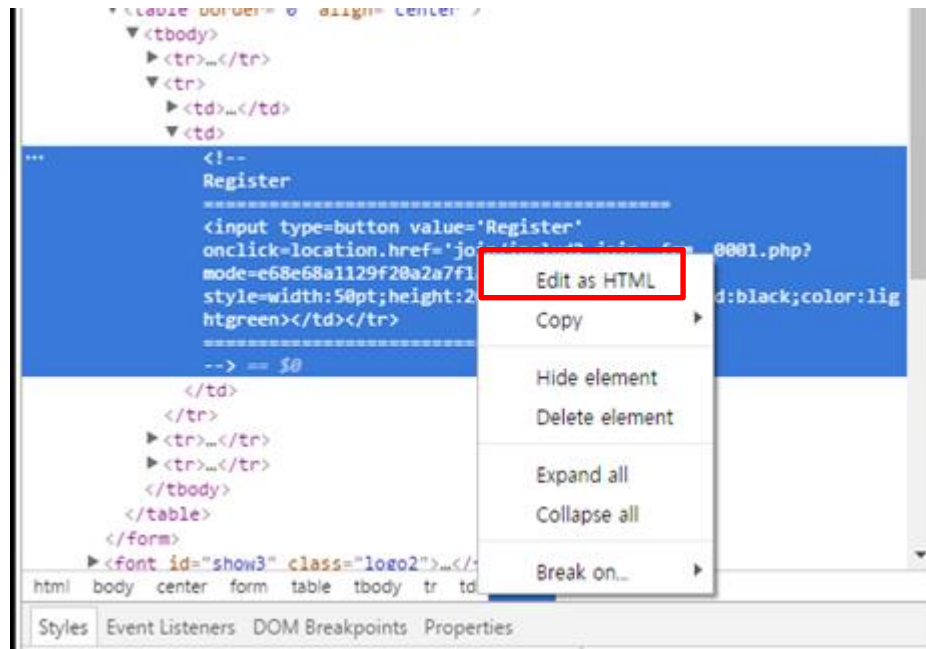
```
<input type=button value='Register'  
onclick=location.href='join/includ2_join_frm_0001.php?  
mode=6ba7f0b7b63db892b69eb3145010e9a7'  
style=width:50pt;height:20pt;border:0;background:black;color:lightgreen>  
</td></tr>  
=====
```

```
--> == $0
```

회원가입 문제 풀이

가입페이지 찾기. 두번째 방법

HTML 편집 -> 주석을 없앴



회원가입 문제 풀이

가입페이지



Register

ID

PW

EMAIL

decode me

[Submit]

Decode me 부분을 해결해야 한다.

회원가입 문제 풀이

디코딩 사이트 등에서 해결

http://tools.web-max.ca/encode_decode.php

Base64 설명 =

<https://ko.wikipedia.org/wiki/%EB%B2%A0%EC%9D%B4%EC%8A%A464>

Specify data to encode / decode

VFZSRk0weHFSVE5NYWtVMVQwTTBNVTFSUFQwPQ==

Encode / hash options

Base64 encode Base85 encode URL encode

MD4 hash MD5 hash SHA1 hash

Decode options

Base64 decode Base85 decode

URL decode

Encode / hash / encryption or decode / decryption results:

TVRFM0xqRTNMakU1T0M0MU1RPT0=

회원가입 문제 풀이

3번째 디코딩에서 IP가 나오는 것을 확인
디코딩 값을 회원가입 정보에 입력

Encode / hash / encryption or decode / decryption results:

[117.17.198.51](#)

```
Warning: eregi() [function.eregi]: REG_EESCAPE in  
/home/hosting_users/webhacking/www/join/includ2_join_frm_0001.php on line 54
```

Welcome to the Webhacking.kr
dont forget it!

ip

id

pw

email

회원가입 문제 풀이

- nykim@seoultech.ac.kr 메일 전송
- 둘 중 하나 화면 캡처하여
2017날짜_이름(학번,과목).jpg 형식으로 보내면
완료



Q & A

참고 문헌 :