

컴퓨터보안 실습

2주차

Wargame Challenge 문제풀이
(QR Code Puzzle, already got)

실습 내용

- 실습 사이트 소개
- 웹 해킹 및 웹 포렌식 기초
- Wargame QR Code Puzzle 문제 확인
- Wargame QR Code Puzzle 문제 풀이
- Wargame already got 문제 확인
- Wargame already got 문제 풀이

웹 해킹 및 웹 포렌식 기초

- 웹 해킹

- 웹 사이트의 취약점을 공격하는 기술적 위협으로, 웹 페이지를 통하여 권한이 없는 시스템에 접근하거나 데이터 유출 및 파괴와 같은 행위


- 웹 포렌식

- 사용자의 컴퓨터에 저장되어 있는 웹에 사용 흔적을 디지털 포렌식 방법을 이용하여 조사하는 것을 말함
웹 브라우저는 로그 정보(Cache, History, Cookie, Download List)를 파일로 남기는데 웹 포렌식은 이러한 로그 정보를 분석하는 것이 일반적임

실습 사이트 소개

- Wargame.kr (<http://wargame.kr/challenge>)
- 왼쪽 Join 눌러 회원가입 후에 Login

Wargame.kr v2.1



{not logged on}

Login Join

- Main
- Tutorial <
- Wargame <
- Achievement
- Free Board
- Magazine
- Favorites
- About

Welcome to Wargame.kr

Chat

[BBS mania] sakuya 영	2017-02-14 13:27:27
AlphaDT 여기 뭐하는데에어?	2017-02-14 14:47:35
[super hacker] KuroNeko 해킹 문제 주는 곳입니다	2017-02-14 20:30:21
ghost 해 # ㄹ가유	2017-02-15 05:05:33
ghost 해캠가TT ㄹ	2017-02-15 05:05:34
kawa1lg1rl 해캠가요	2017-02-15 05:06:15
socood 요 히사시부리	2017-02-15 15:50:29
[master] stypr 히사시부리다나~	2017-02-15 20:20:19
[master] jeong.su 이랏샤이마세!	2017-02-15 22:07:04

Login please.. Send

Online User

Guest / 110.10.*.196 Ranked No. 9999

Wargame QR Code Puzzle 문제 확인

- QR Code Puzzle 문제
(http://wargame.kr:8080/qr_code_puzzle/)
- QR코드 모바일 QR코드 다운로드
- QR코드 PC스캔방법
<http://www.onlinebarcodereader.com/>

QR Code Puzzle

QR CODE PUZZLE

300point / bughele

```
javascript puzzle challenge  
just enjoy!
```

FLAG

Auth

Start

Close



Wargame QR Code Puzzle 문제 풀이

• QR Code Puzzle 문제 접근 방법 및 풀이

- 우선 퍼즐을 맞추기 시도 -> 퍼즐을 맞추기 힘들게 되어있음
- > '무엇을 해킹하는 문제일까?' 고민 -> 소스코드 확인(F12)
- > QR 코드 파일이 기존 이미지에서 퍼즐파일로 바뀐 것으로 추측 -> F12의 통신하는 부분 Network을 들어감

```
▼ <body>
▼ <center> == $0
  <script type="text/javascript" src="http://ajax.googleapis.com/ajax/libs/jquery/1.6.1/jquery.min.js"></script>
  <script type="text/javascript" src="jquery.jqpuzzle.js"></script>
  <script type="text/javascript" src="jquery.color-RGBa-patch.js"></script>
  <script type="text/javascript" src="jquery.blockUI.js"></script>
  ▼ <script type="text/javascript">
    /**]
      $(function(){ $('#join_img').attr('src',unescape('%2f%69%6d%67%2f%71%72%2e%70%6e%67'));
        $('#join_img').jqPuzzle({rows:6,cols:6,shuffle:true,numbers:false,control:false,style:{overlap:false}});
        hide_pz();});
      function hide_pz(){
        var pz=$('#join_img div'); if(pz[pz.length-2]){(pz[1]).remove();$(pz[pz.length-2]).remove();}else{setTimeout("hide_pz()",5);}
      }
    /*]]&gt;*/
  &lt;/script&gt;
  ▼ &lt;style&gt;
    #join_img {padding:15px 15px 0 15px; border:2px solid #999; background-color:#444;}
  &lt;/style&gt;
  &lt;br&gt;
  &lt;h1&gt;QR Code Puzzle&lt;/h1&gt;
  &lt;br&gt;
  ▼ &lt;div class="jqPuzzle" id="join_img" style="width: 496px; height: 512px; text-align: left; overflow: hidden; display: block;"&gt;
    ▼ &lt;div class="jqp-wrapper" style="width: 496px; height: 496px; border-width: 0px; padding: 0px; margin: 0px; position: relative; overflow: hidden; display: block; visibility: inherit;"&gt;
      ▶ &lt;div class="jqp-piece" style="width: 81px; height: 81px; background-image: url("./img/qr.png"); border-width: 0px; margin: 0px; padding: 0px; position: absolute; overflow: hidden; display: block; visibility: inherit; cursor: default; left: 249px; top: 0px; background-position: 0px 0px;" current="3"&gt;...&lt;/div&gt;
      ▶ &lt;div class="jqp-piece" style="width: 81px; height: 81px; background-image: url("./img/qr.png"); border-width: 0px; margin: 0px; padding: 0px; position: absolute; overflow: hidden; display: block; visibility: inherit; cursor: default; left: 415px; top: 83px; background-position: -83px 0px;" current="11"&gt;...&lt;/div&gt;</pre></div>
```

Wargame QR Code Puzzle 문제 풀이

- **QR Code Puzzle** 문제 접근 방법 및 풀이
 - **Network** 에서 홈페이지와 통신할 때 주고 기존 **.png, .jpg** 파일을 올려서 주고 받을 것으로 예상이 됨 -> **F12**를 켜 상태에서 **F5**를 눌러 통신내역을 확인함 -> **qr.png** 파일이 나타남 -> 더블클릭 -> qr코드 스캔 후 **Auth** 값을 입력 -> 문제 **clear**
 - 웹 소스코드 보는 방법과 홈페이지 **HTML** 을 알게 되었고, 웹 해킹이라는 것은 다양한 접근 방법에서 나타나는 것임
 - **Ps.** 정말 이 해결 방법을 모른 사람들은 그림판으로 qr코드를 직접 캡처해서 하나하나 맞추는 후 스캔 하였다고 함.....

Wargame already got 문제 확인

- Already got 문제
(http://wargame.kr:8080/already_get/)

already got ×

200point / bughela

can you see HTTP Response header?

FLAG

Auth

Start

Close

you've already got key! :p

Wargame already got 문제 확인

- **Already got 문제 접근 방법 및 풀이**
 - 문제 영어 해석 -> 당신은 **HTTP Response header** 를 볼 수 있니?-> **Response** = 응답을 보내는 서버에 대한 정보 -> ‘무엇을 해킹하는 문제일까?’ 고민 -> 소스코드 확인(**F12**) -> **F12**의 통신하는 부분 **Network** 체크 -> **F12**를 켜 상태에서 **F5**를 눌러 통신내역을 확인함 -> 문제를 보면 **HTTP** 구조를 자세히 알아보라는 내용을 뜻함 -> **already_get/** 통신 상태 체크 -> **Response header** 부분을 열기 -> **Flag** 부분 확인 -> **Auth** 답은 **http response headers** 에 **flag** 부분에 보면 이미 나타나 있다는 것을 알려준 문제

Q & A

참고 문헌 :