

Web Hacking Basic

for ICEWALL Mentoring

조성준

Contents

- About
- 해킹을 왜 할까?
 - CTF
 - Bug Bounty
 - Cyber War
- 회합 과제 관련 Q&A
- Web
 - HTML
 - Javascript
 - PHP
 - SQL

About



조성준 (a.k.a. DelspoN)

Security Researcher

한양대학교 17학번 4학년 휴학

~~원자력공학과 전공~~

컴퓨터소프트웨어학부 전공

2019년도 ICEWALL 회장

국내외 컨퍼런스 발표 경험

Pwning Centrally-Controlled Smart Home / HITB AMS
Smart Home Hacking in Real World / CODEGATE Conf.

취약점 분석 경험

리눅스 커널, WD NAS, 금융 보안 프로그램, 네이버 취약점 등

국내외 해킹 대회 출전 경험

TrendMicro CTF Final 10th, Quals 3rd

DVP Blockchain CTF 3rd

국방부 주최 사이버작전경연대회 Final 7th, Quals 1st

국정원 주최 사이버공격방어대회 Final 8th, Quals 4th

국제해킹방어대회 CODEGATE CTF Final 7th, Quals 4th

...

해킹을 왜 할까?

- for fun → CTF
- for money → Bug Bounty
- for power → Cyber War

CTF = 해킹대회

해킹 관련 문제를 푼다

대회 시간이 깊 (큰 대회는 보통 24~72시간)

온라인 예선, 오프라인 본선

본선 가면 비행기, 호텔 지원 해주는 곳도 있음 = 대회 겸 여행 굿!

인생에 많은 깨달음과 도움을 줌

CTF = 해킹대회

해킹 관련 문제를 푼다?

서버에 정답이 저장되어 있는 문제

프로그램을 분석해서 정답률 구하는 문제 (시리얼키 크랙이랑 비슷)

암호를 해독해서 답을 구하는 문제

...

DEF CON CTF

미국 라스베가스에서 개최

상금은 없지만 세계 최고 권위의 CTF



CODEGATE CTF

학생부, 대학생부, 일반부

예선 2월 온라인

본선 4월 코엑스

상금 많음



사이버공격방어대회

Attack & Defense 방식

예선 9월 온라인

본선 10월 제주도, 부산, ...

상금 많음

국정원 주최



사이버작전경연대회

구 화이트햇콘테스트

예선 8월 온라인

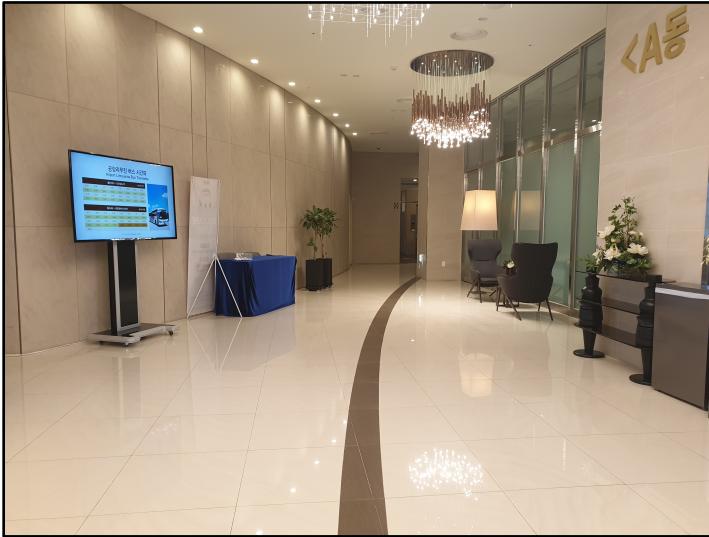
본선 9월 서울 어딘가의 호텔

상금 많음

국방부 주최



사이버공격방어대회



Samsung CTF

개인전

예선 ?월 온라인

본선 8월 양재 삼성리서치

상금 미침

매년 개최하지는 않음



버그바운티

기업의 취약점을 찾아주면 포상을 주는 제도
돈을 벌 수 있음

버그바운티

PWN2OWN (CTF는 아님)

세계 최대 버그바운티 대회

상금이 수십만 달러 수준

윈도우, 크롬, 등이 타겟



TREND MICRO
Securing Your Journey to the Cloud



Hewlett Packard Enterprise

2016 Pwn2Own: Master of Pwn		
Name	Points	Award
Tencent Security Team Sniper	38	\$142500
JungHoon Lee	25	\$145000
360Vulcan Team	25	\$132500
Tencent Security Team Shield	10	\$40000
Tencent Xuanwu	0	\$0

Last updated at 18:30



버그바운티

<https://www.krcert.or.kr/consult/software/vulnerability.do>

<https://bugbounty.naver.com/ko/>

<https://ridi.dev/bounty.html>

<https://security.samsungmobile.com/rewardsProgram.smsb>

KISA, 네이버, 리디북스, 삼성, 해커원, 라인 등

KISA 버그바운티

3,6,9,12월 평가

소프트웨어 취약점

서버 건드리는 취약점은 평가 안함

S/W 신규 취약점

▶ > 상담 및 신고 > S/W 신규 취약점

대검찰청, 경찰청, 인터넷진흥원, 금융기관 등을 사칭하는
파싱사이트, 파싱 문자로 인한 금전적 피해가 발생하고 있습니다.
사이트 접속 시 바로 개인정보를 입력하지 말고 사이트 주소를 확인하시고 주의해 주십시오

S/W 신규 취약점 신고포상제

2012년 10월부터 소프트웨어 신규 보안 취약점 신고포상제를 실시합니다.
포상금 지급을 위한 평가는 분기별로 실시하며, 분기별 우수 취약점을 선정하여 평가 결과에 따라 최고 1,000만원의 포상금이 지급됩니다.
신고포상을 원하는 경우 아래의 신고 양식을 다운로드 받아 작성하여, 관련파일에 첨부하여 주시기 바랍니다.

- 참가대상 : 국내외 거주하는 한국인

- 신고대상 취약점 : '소프트웨어'에 대한 보안 취약점으로 최신버전의 소프트웨어 영향을 줄 수 있는 신규 보안취약점(제로데이 취약점)
※ 기타 자세한 사항은 포상제 FAQ 참조

- 평가 및 포상 일정 : 분기별 평가를 실시하여 포상금을 지급(3, 6, 9, 12월에 평가 및 포상 실시)

- 주의사항 : 실제 서비스 중인 웹사이트나 시스템(서버, 네트워크, 보안장비 등)에 정보통신서비스 제공자의 동의를 받지 않고 정당한 접근권한 없이 또는 허용된 접근 권한을 넘어 취약점을 발굴하는 행위는 정보통신망 침입행위로 간주될 수 있으므로 평가 및 포상대상에서 제외됨은 물론, 법에 의해 처벌 받을 수 있습니다.
(정보통신망 이용촉진 및 정보보호 등에 관한 법률 제48조제1항, 제기조제1항제9호및제2항 참고)
※서비스 취약점 발굴을 허용하는 공동운영사의 경우 제외

취약점 신고포상제 공동운영사인 한글과컴퓨터, 네이버, 카카오, 키카오뱅크, 네오위즈게임즈, 이스트시큐리티, 이니텍, 잉카인터넷, LG전자, 지니언스, 앤랩, 헬리우드, 엑스블록시스템즈, 블록체인오아시스, 글로스퍼, 에스지에이솔루션즈, 소테리아, 휴네시온은 정보보호 활동을 장려, 정보보호 문화 확산 등 정보보호 분야 발전을 위해 노력하는 기업입니다.



* XE(XpressEngine) CMS는 자체 취약점 신고 포상제를 운영하고 있습니다.

* 네이버 Service, Application 은 자체 취약점 신고 포상제를 운영하고 있습니다. (<http://bugbounty.naver.com/ko>)

[신고서 양식\(한글\)](#) [신고서 양식\(워드\)](#) [신고포상제 안내문](#) [신고포상제 FAQ](#) [운영 안내서](#)

NAVER 버그바운티

웹 취약점

앱 취약점

하단의 최신버전 어플리케이션에서 발생하는 취약점을 대상으로 합니다.

- 네이버 툴바
- 네이버 백신
- 클라우드 탐색기

3. 포상

취약점	예시	포상금액
Account takeover	Authentication Bypass	USD ~\$3,000
Remote Code Execution	Ability to send packets containing arbitrary system call to server	USD ~\$3,000
Full access to filesystem or database	SQL Injection	USD ~\$3,000
Execute code on the client	XSS	USD ~\$500
Logical flaw Bugs	Sensitive actions, Purchase Bypass	USD ~\$300
Other security vulnerabilities	Information Leakage, CSRF, SSRF	USD ~\$300

- CSRF 취약점은 다음의 기능만 대상으로 합니다 : 네이버 회원 정보, 네이버 카페 관리, 네이버 블로그 관리

- 포상금은 취약점의 위험도와 보고서 등을 종합적으로 검토하여 주어집니다.

- 사용자의 개입이 많이 필요한 경우 포상 금액이 줄어들 수 있습니다.

- 새로운 방식의 공격 기법이나 버그타입에 대해서는 좀 더 많은 포상금이 주어질 수 있습니다.

버그바운티 예시

Cyber War

국가간 사이버 전쟁

정보 획득을 통해 안전, 우위, 권력 획득

공격자가 누구인지 명확히 알아내기 어려움

APT???

Cyber War

goitgo.tistory.com › ... ▾

2016년 2/5일 방글라데시 중앙은행(SWIFT) 해킹사건

2016년 2/5일 방글라데시 중앙은행(SWIFT) 해킹사건. 미래해커. 2017. 4. 24. 21:40 댓글수0 공감수0. 일시: 2016년 2/5일 방글라데시 중앙은행이 한화 약 966억원을 ...

www.boannews.com › media › view ▾

PC버전 - 보안뉴스

2018. 2. 20. - 사이버 공격자들의 SWIFT 해킹 사례는 요 몇 년 사이 끊임없이 등장하고 있다. 특히 2016년 초에 발생한 방글라데시중앙은행 사건이 유명하다.

www.bbc.com › korean › news-41584327 ▾

북한의 사이버전 능력을 보여주는 5대 해킹 사건 - BBC News ...

2017. 10. 12. - 스위프트 전산망 해킹. 이 사건은 ... 해커들은 방글라데시 중앙은행의 서버에 악성코드를 심어 놓고 스위프트(SWIFT) 시스템 접속 정보를 훔쳐냈다.

ko.wikipedia.org › wiki › 농협_전산망_마비_사태 ▾

농협 전산망 마비 사태 - 위키백과, 우리 모두의 백과사전

검찰은 농협해킹이 조선민주주의인민공화국의 사이버 테러에 의한 것으로 결론났다. 조사결과에 따르면 서버 유지보수를 맡은 외주업체 직원 한국IBM 직원 한모 씨 ...
경과 · 대한민국 검찰의 수사 · 원인 · 비판과 의문점

namu.wiki › 농협 전산 사고 ▾

농협 전산 사고 - 나무위키

2020. 4. 28. - 농협이 금융권에서 일하는 전산 개발자들에게 공공의 적이 된 사건. ... 가뜩이나 불과 며칠 전 현대캐피탈 전산망 해킹으로 인한 개인정보 유출 사태 ...

Cyber War

www.yna.co.kr › view › AKR20170112082300009 ▾

"러시아 해킹에 대규모 정전"…지난달 우크라 사고 조사결과 ...

2017. 1. 12. - (서울=연합뉴스) 김수진 기자 = 러시아의 해킹 전력화 논란 속에 우크라이나가 작년 12월 대규모 정전 사태의 원인으로 러시아의 사이버 공격을 지목 ...

www.donga.com › news › article › all ▾

러시아, 美탄핵 사태 촉발한 '우크라이나 가스회사' 해킹 : 뉴스 ...

2020. 1. 14. - 미국 대선을 앞두고 러시아가 움직이고 있다. 뉴욕타임스(NYT)는 13일(현지시간) 러시아 해커들이 우크라이나 가스회사 '브리스마'를 해킹했다고 ...

www.hankookilbo.com › News › Read ▾

"러시아, 트럼프 탄핵 사유 '우크라 스캔들' 관련 해킹 시도"

2020. 1. 14. - ... 우크라이나 스캔들'로 트럼프 대통령이 탄핵 위기에 직면한 가운데 이번에는 러시아 해커들이 헌터 바이든이 일했던 우크라이나 가스 회사를 해킹 ...

news.chosun.com › site › data › html_dir › 2020/01/15 ▾

러시아 또 美대선 개입?...러 해커, 바이든 아들 다닌 우크라이나 ...

2020. 1. 15. - 2020년 미국 대선을 앞두고 러시아군 해커들이 우크라이나 가스회사를 해킹하면서 러시아의 미국 대선 개입 의혹이 또다시 불거지고 있다.

동영상



트럼프, 러시아 해킹 사건은 "정치적 마녀 사냥" / YTN (Yes! Top ...)

YTN NEWS

YouTube - 2017. 1. 7.



트럼프, 해킹 보고 무시...'러시아는 나의 혈맹' / YTN (Yes! Top ...)

YTN NEWS

YouTube - 2017. 1. 8.



트럼프, 첫 회견에서 러시아 대선 개입 인정 / YTN (Yes! Top ...)

YTN NEWS

YouTube - 2017. 1. 12.

www.voakorea.com › world ▾

[뉴스따라잡기] 러시아 해킹 논란 | Voice of America – Korean

2017. 1. 11. - 도널드 트럼프 미국 대통령 당선인이 미국 대선 해킹 논란과 관련해 배후에 러시아가 있다는 사실을 인정했습니다. 하지만 러시아 정부는 계속 이를 ...

news.chosun.com › site › data › html_dir › 2016/12/12 ▾

"러시아가 트럼프 당선 도왔다"… CIA의 해킹 조사 결론 파문 ...

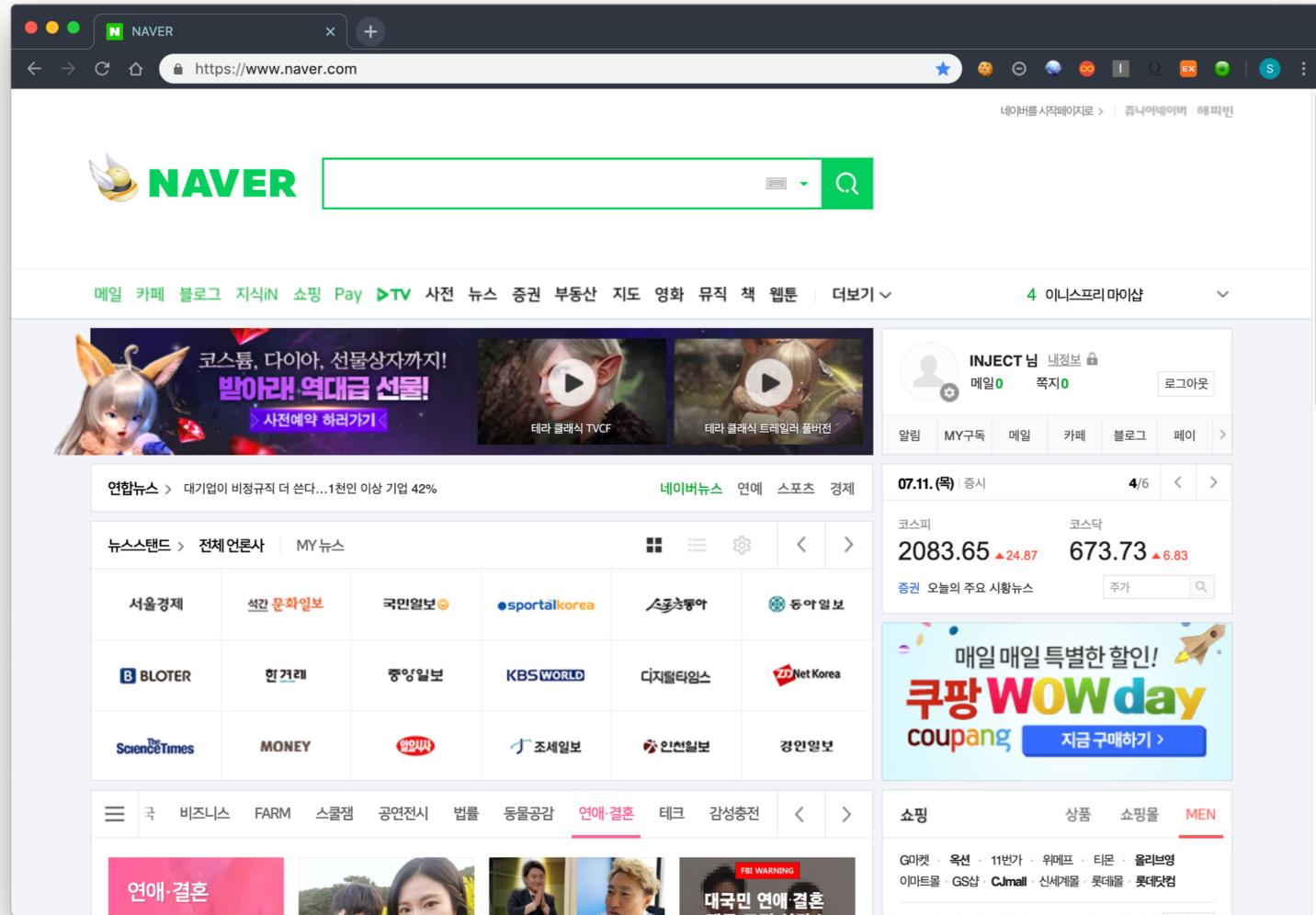
2016. 12. 12. - 미국 중앙정보국(CIA)이 올해 대선에서 러시아가 도널드 트럼프 당선인이 승리할 수 있도록 지원했다는 결론을 내렸다고 워싱턴포스트(WP)가 9일(...

www.hankookilbo.com › News › Read ▾

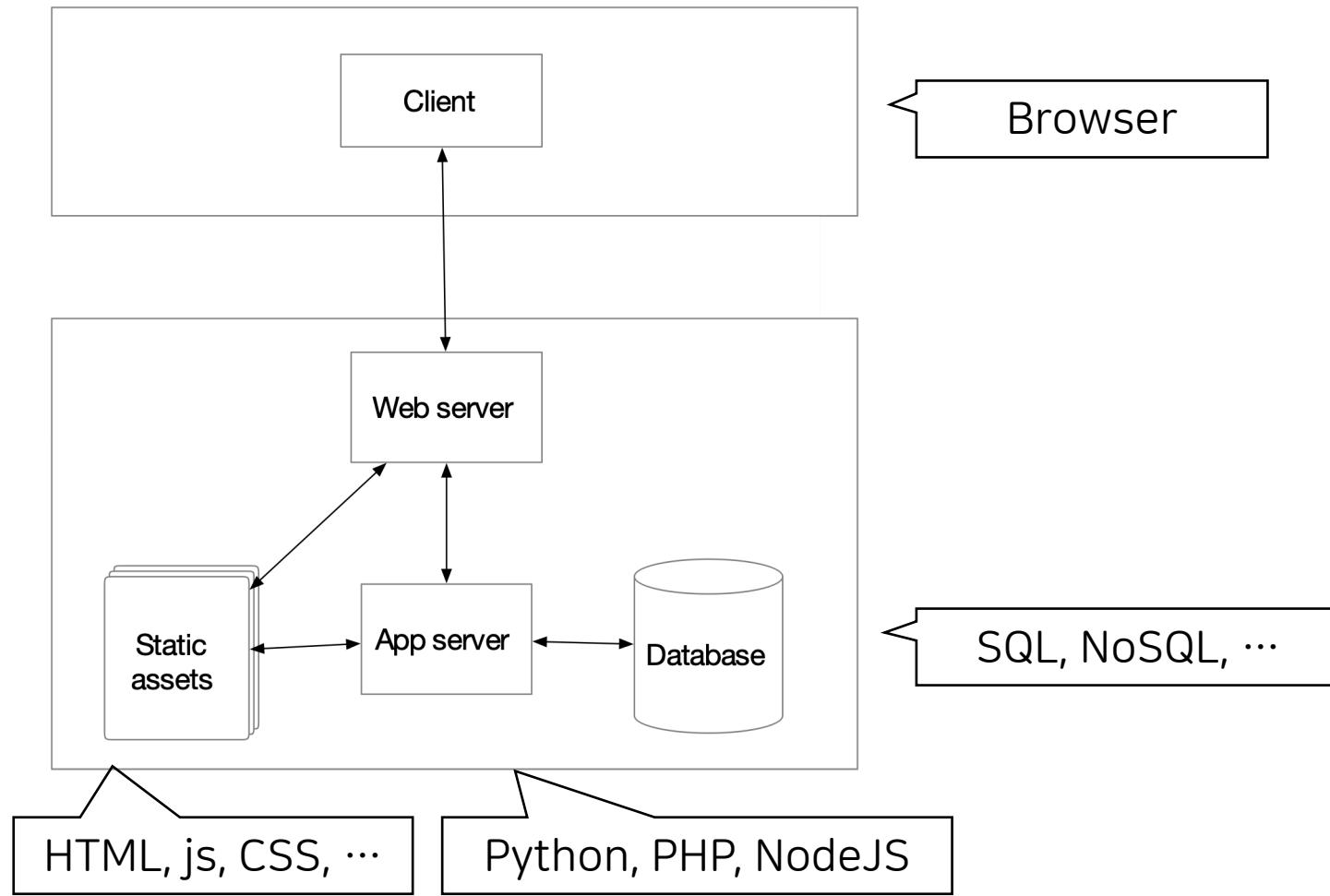
"러시아, 트럼프 탄핵 사유 '우크라 스캔들' 관련 해킹 시도"

2020. 1. 14. - 게티이미지뱅크도널드 트럼프 미국 대통령이 우크라이나를 상대로 민주당 유력 대선 후보인 조 바이든 전 부통령과 그의 아들 헌터 바이든에 대해 ...

Web



Web : Architecture



Web : Browser



A screenshot of the original NAVER homepage. The page features a dark header with the NAVER logo and a search bar. Below the header is a banner for a game. The main content area includes news feeds from various sources like SBS, KBS, and Naver News. There are also sections for sports, finance, and shopping. A sidebar on the right shows a user profile and a weather forecast for Seoul.

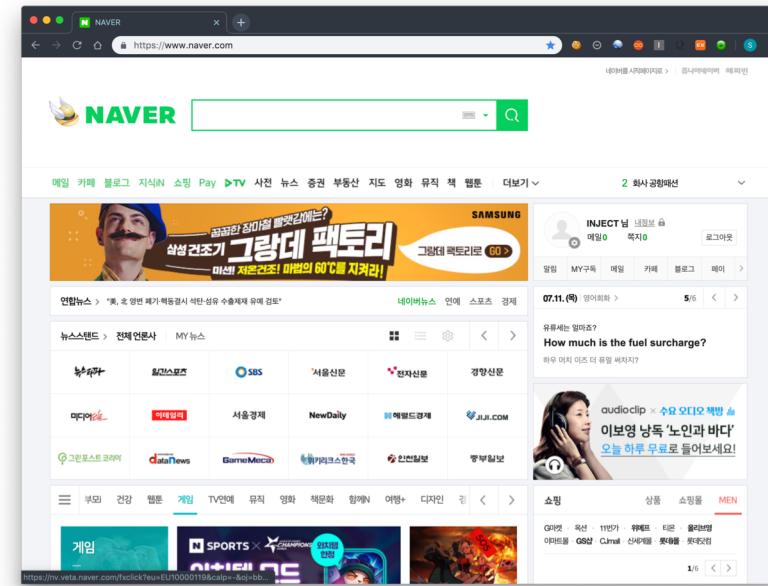
A screenshot of the modernized NAVER homepage. The design is lighter and more minimalist. It features a prominent search bar at the top. The main content area is organized into columns for news, sports, and other services like Keep and Trend. A banner for Coupang is visible. The overall layout is cleaner and more user-friendly compared to the original version.

Web : Browser

1. 브라우저는 (웹서버로부터) 가공된 데이터를 입력 받는다.
2. 렌더링하여 보여준다.

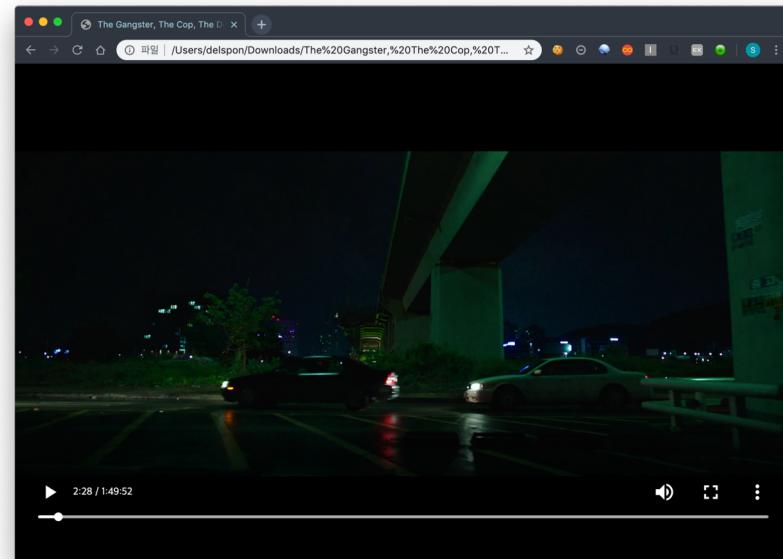
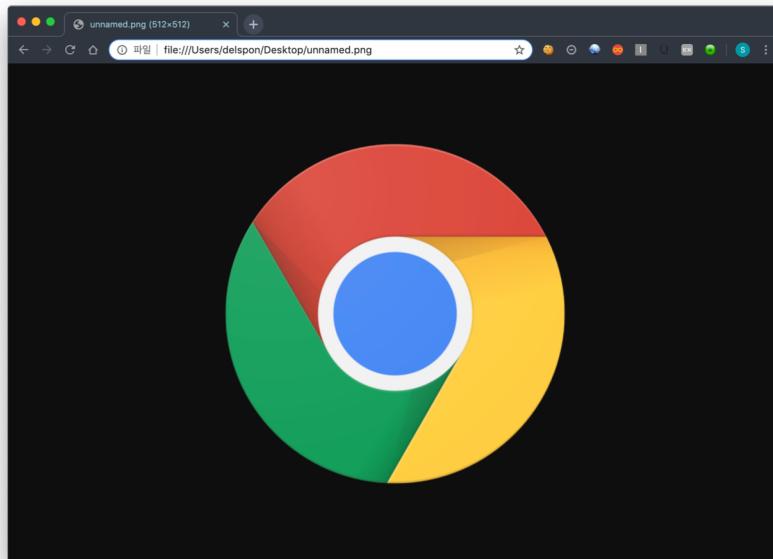
```
view-source:https://www.naver.com
```

```
<html lang="ko">
<head>
<meta charset="utf-8">
<meta name="referrer" content="origin">
<meta http-equiv="Content-Type" content="text/javascript">
<meta http-equiv="Content-StyleType" content="text/css">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=1100">
<meta name="apple-mobile-web-app-title" content="NAVER" />
<meta name="apple-mobile-web-app-capable" content="yes" />
<meta name="description" content="네이버 웹에서 다양한 정보와 유용한 컨텐츠를 만나 보세요!"/>
<meta property="og:title" content="네이버" />
<meta property="og:image" content="https://www.naver.com/>
<meta property="og:url" content="https://a.pstatic.net/static/www/mobile/edit/2016/0705/mobile_212852414260.png" />
<meta name="twitter:card" content="summary" />
<meta name="twitter:title" content="네이버 웹에서 다양한 정보와 유용한 컨텐츠를 만나 보세요!"/>
<meta name="twitter:url" content="https://www.naver.com/" />
<meta name="twitter:image" content="https://a.pstatic.net/static/www/mobile/edit/2016/0705/mobile_212852414260.png" />
<meta name="twitter:description" content="네이버 웹에서 다양한 정보와 유용한 컨텐츠를 만나 보세요!"/>
<link rel="shortcut icon" type="image/x-icon" href="/favicon.ico?1" />
<link rel="stylesheet" type="text/css" href="https://pm.pstatic.net/css/main_v190709.css"/>
<link rel="stylesheet" type="text/css" href="https://pm.pstatic.net/css/webfont_v170623.css"/>
<link rel="stylesheet" type="text/css" href="https://ssl.pstatic.net/static/search/pc/css/api_atcmp_190612.css"/>
<script type="text/javascript" src="https://pm.pstatic.net/jo/nlog_v181107.js"></script>
<script type="text/javascript" src="https://ssl.pstatic.net/tveta/libs/assets/ja/common/min/probe.min.js"></script>
<script type="text/javascript">
var nsc = 'navertop.v3';
document.domain = 'naver.com';
var jindoAII = '';
var iframeLazyload = false;
if (!('window.console') || !('window.console.log')){window.console=function(){}}
var isLogin = "inject";
function refreshLcs(etc) {etc = etc ? etc : {} ; if(document.cookie.indexOf("nrefreshx=1") != -1) {etc["mrf"] = "1"}; else {etc["pan"] = "gam"};return etc;}
</script>
<title>NAVER</title>
</head>
```



Web : Browser

1. 브라우저는 (웹서버로부터) 가공된 데이터를 입력 받는다.
2. 렌더링하여 보여준다.



Web : Browser

INJECT 님 메일 0 쪽지

알림 MY구독 메일

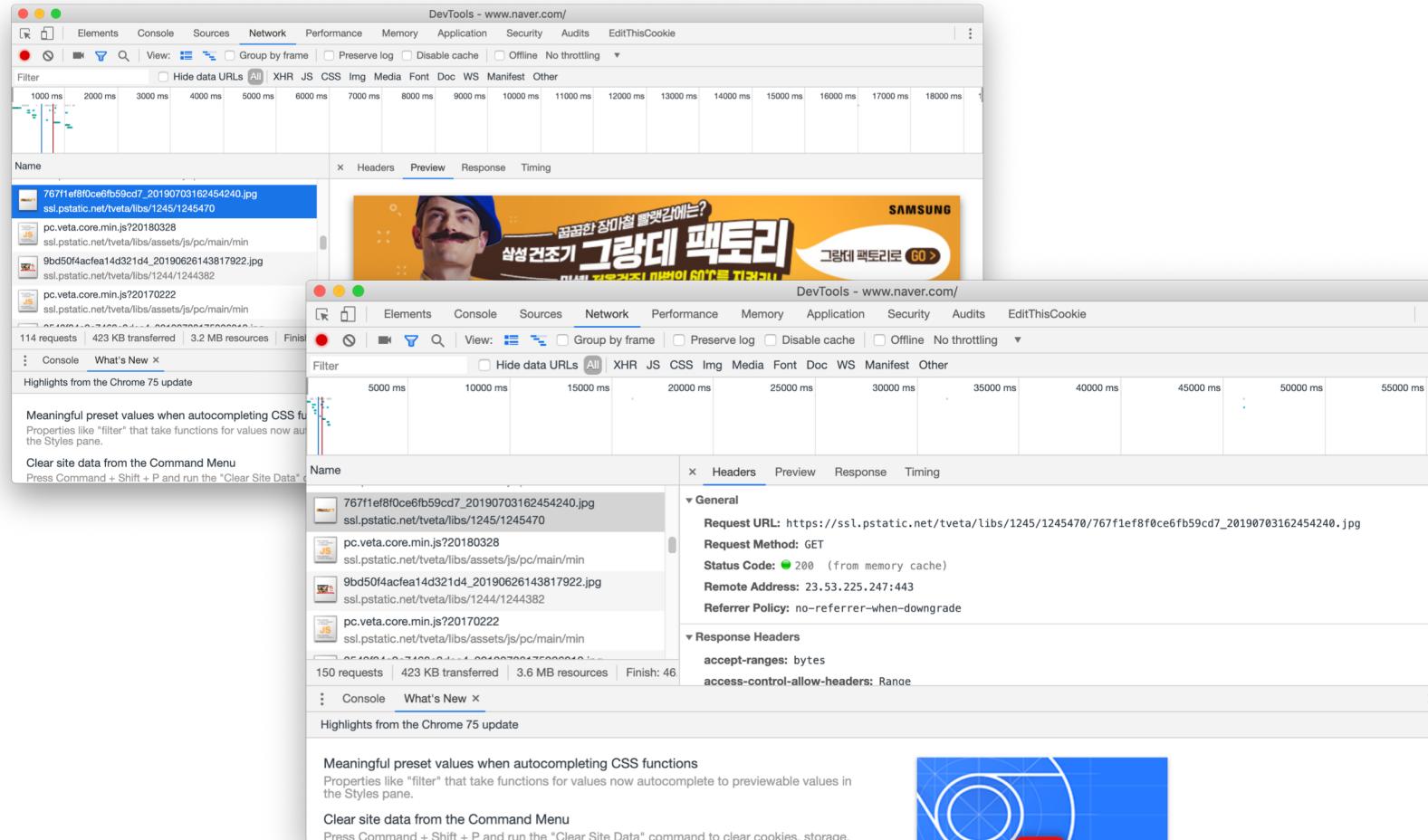
DevTools - www.naver.com/

Insole Sources Network Performance Memory Application Security Audits EditThisCookie

```
<div id="da_iframe_time" name="da_iframe_time" src="https://nv.veta.naver.com/fxshow?su=SU10079&nrefreshx=0" data-veta-preview="main_time" title="광고" style="width:120px; marginheight:0px; marginwidth:0px; scrolling=no; frameborder=0">
```

```
> html>
  ig="ko">
</head>
  nload="initAd()" marginwidth="0" marginheight="0">
    id="da_timeboard">
      v class="content">
        iv id="addiv" class="ad">
          <a href="https://nv.veta.naver.com/fxclick?eu=EU10000120&calp=-&o=j=bbC87fref30A8...6c989907cah41ccc2fe5cd61b56cfelts=uwPtywllVTDFr9nr7THJdhA%3D%3D&ui=shrs=Y&" id="ac_hanner_a" target="_blank">
             == $0
          </a>
        </div>
      </div>
    </div>
  </div>
</body>
```

Web : Browser



HTML

```
<h1>My First Heading</h1>

<p>My first paragraph.</p>



<iframe src="https://www.afreeca.com"></iframe>

<a href="https://www.naver.com">Let's go</a>
```

HTML

```
<h1>My First Heading</h1>
```

```
<p>My first paragraph.</p>
```

Javascript

```

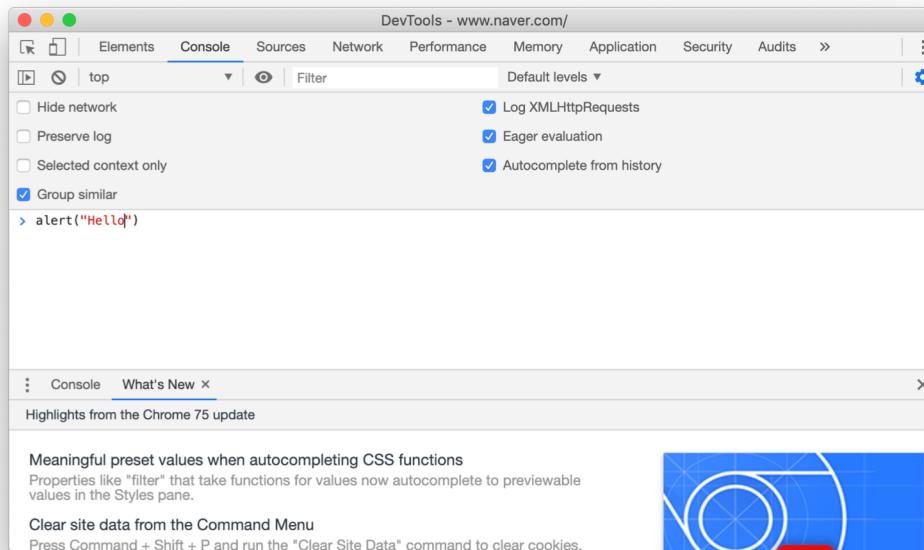
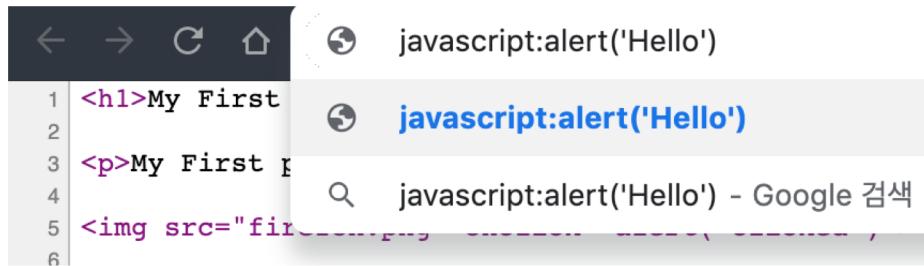
```

```
<iframe src="https://www.afreeca.com"></iframe>
```

```
<a href="https://www.naver.com">Let's go</a>
```

Javascript

```
<script>  
...  
</script>
```



Javascript

```
<script>  
  
var x = 5;  
var y = 6;  
var z = x + y;  
alert(z);  
  
</script>
```

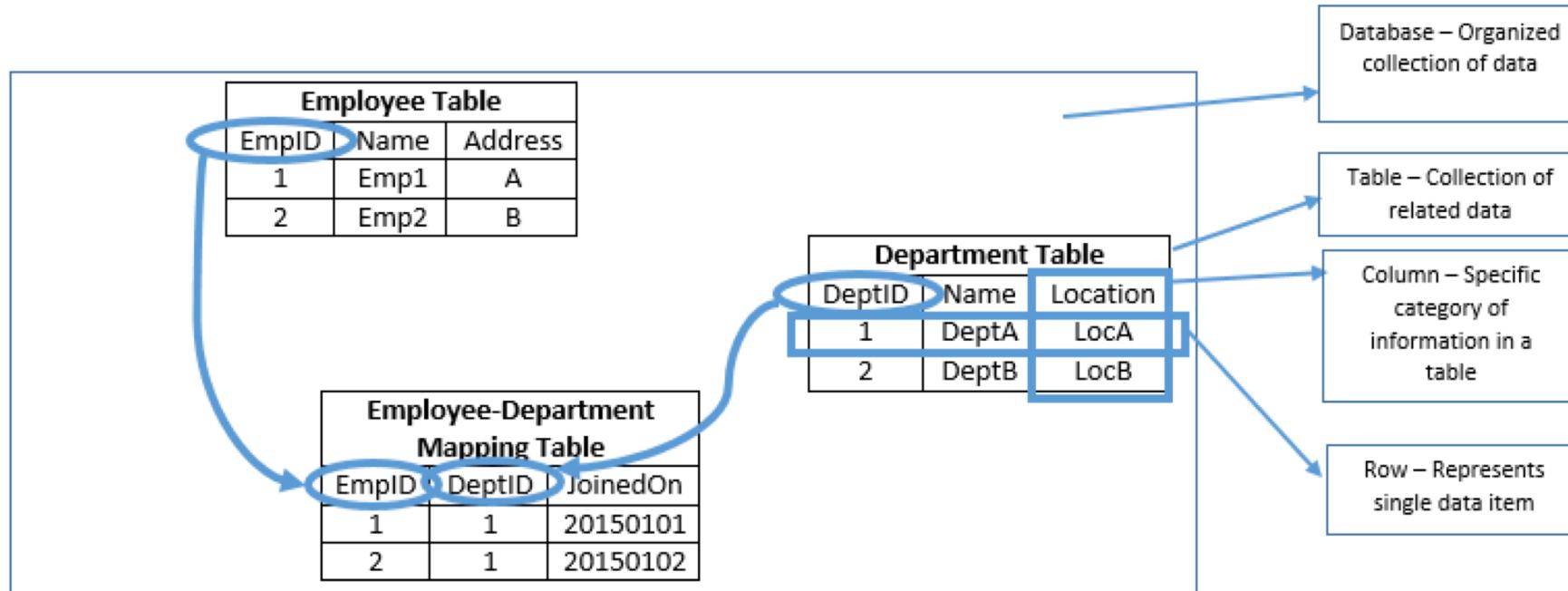
```
<script>  
  
var a="https://";  
var b="www.naver.com";  
location.href = a+b;  
  
</script>
```

PHP

```
<?php  
echo "Hello World";  
?>
```

```
<?php  
$a = "Hello ";  
$b = "World";  
echo $a.$b  
?>
```

SQL



SQL

<https://www.w3schools.com/sql/>

추천 과제

<https://www.w3schools.com/sql> HOME부터 Order by까지 읽고 실습

<https://www.w3schools.com/html> HTML Links, Images, Iframes, Javascript 읽고 실습

<https://www.w3schools.com/js> JS Location, Popup alert, Cookie 읽고 실습