

SecureGPT

인간GPT

조장 백주원

| 김다솔

| 김석준

| 이상완

목 차

- 01 주제선정 동기 및 필요성
- 02 서비스 목표 및 설명
- 03 웹사이트 설계 및 기능
- 04 기대효과

1. 주제 선정 동기 및 필요성

초등-중학교 '코딩 교육' 2025년부터 필수과목으로 - 동아일보



구현단계에서 보안취약점을 제거하면 유지보수단계에서 발생하는 비용보다 **25배** 정도 현저히 줄어든다.

1. 주제 선정 동기 및 필요성

- 관련사례




동아일보

<https://www.donga.com/news/Society/article/all> :

“출처 불확실한 '공문서 메일' 열지 마세요” ...

2012. 6. 28. — 안랩 보안대응센터(ASEC)는 27일 '국방융합기술.hwp'라는 제목의 파일에 악성코드가 숨겨진 사실을 확인했다고 밝혔다. 이에 앞서 보안회사인 잉카 ...

스택의 경계를 체크하지 않아 발생하는 버퍼 오버플로우 취약점



데일리시큐


유무선공유기

유무선공유기
다. 취약점이 확인된 기종은

2013. 4. 23.

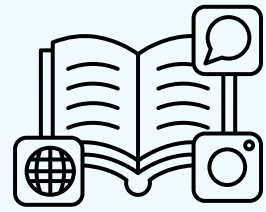
심각한 보안취약점 주의!

의 관리자페이지 로그인 인증우회 취약점이 발견됐
모델이다.

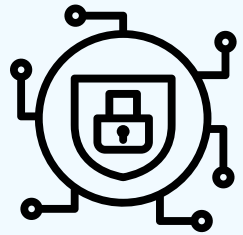


유효하지 않은 입력값의 대해 검증하지 않아 생긴 취약점

1. 주계 선정 동기 및 필요성



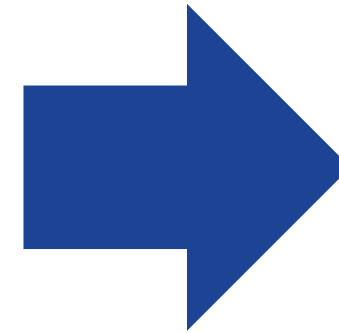
코딩교육 의무화



소프트웨어 개발 보안 적용 의무화



구현단계에서 시큐어코딩 적용 시
유지보수 비용절감



소프트웨어 취약점을 사전에
차단하여 안전성과 보안성을
보장해주는 시큐어 코딩 생성
서비스

SecureGPT

2. 서비스 목표 및 설명

시큐어 코딩이란?

소프트웨어 개발 시 안전한 코드를 제작하는 코딩기법

주된 갱점

- 1.올바르지 않은 메모리 접근
- 2.외부 입력 값에 대해 검증하지 않음
- 3.발생할 수 있는 오류에 대해 처리하지 않거나 부적절하게 처리함

• SecureGPT

Chat GPT API를 이용하여 사용자가 메모리 오버플로우와 커널의 취약점 등 시큐어 코딩을 할 수 있도록 서비스를 제공하여 보안솔루션을 제시하는 서비스를 목표로 함

3. 웹사이트 설계 및 기능 -코드 검사기

코드검사기

보안상식

퀴즈

C 언어 코드를 입력하세요...

전송

보안 취약점 분석	C언어 코드 입력 시 자동으로 해당 코 드에서 발생할 수 있는 보안 취약점을 분석	시큐어 코딩 적용	발견된 취약점을 기반으로 시큐어 코딩 기법을 적용하여 안전한 코드 로 수정
-----------------	---	-----------------	---

3. 웹사이트 설계 및 기능 -코드 검사기

구정 전

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>

main() {

    char buf[100] = { 0, };

    printf("문장을 입력하세요 : ");
    gets(buf);
    printf("입력한 문장은 다음과 같습니다.\n");
    printf("%s", buf);

}
```

구정 후

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>

int main() {
    char buf[100] = { 0 };

    printf("문장을 입력하세요 : ");
    fgets(buf, sizeof(buf), stdin);

    // Remove the newline character that fgets adds if necessary
    buf[strcspn(buf, "\n")] = 0;

    printf("입력한 문장은 다음과 같습니다.\n");
    printf("%s\n", buf);

    return 0;
}
```

- gets() 함수는 입력의 길이를 검증하지 않기 때문에 버퍼 오버플로우를 일으킬 수 있고 보안의 취약점을 노출

3. 웹사이트 설계 및 기능 -보안상식

코드검사기 보안상식 퀴즈

보안 취약점

다음은 C 언어 프로그램에서 발생할 수 있는 일반적인 보안 취약점입니다:

정수형 오버플로우

사용자가 제공하는 입력값을 사용하고 그 과정에서 정수형 오버플로우가 발생하는 경우 보안상 문제를 유발할 수 있습니다. 동적 메모리 할당을 위해 외부 입력값을 배열의 크기로 사용하는 경우 그 값이 음수가 아닌지 검사하는 작업이 필요합니다. 외부 입력값으로 배열에 접근할 경우, 입력값이 너무 클 때 음수가 되어 시스템에 문제가 발생할 수 있습니다.

예외처리로 오버플로우가 발생했는지 확인하고 처리해야 합니다.

메모리 버퍼 오버플로우

연속된 메모리 공간을 사용하는 프로그램에서 할당된 메모리의 범위를 넘어선 위치에 자료를 읽거나 쓰려고 할 때 발생합니다. 취약한 API를 사용하는 경우 발생할 수 있습니다. 특히, 문자열 저장 시 NULL 문자로 종료하지 않으면 의도하지 않은 결과를 가져오게 되므로 NULL 문자를 버퍼 범위 내에 삽입해 NULL 문자로 종료하도록 해야 합니다.

보안
상식

보다 쉽게 보안 개념을 이해할 수 있도록 자주 발생하는 보안 취약점에 대한 간단한 설명

3. 웹사이트 설계 및 기능 -퀴즈

코드검사기 보안상식 **퀴즈**

시큐어 코딩 퀴즈

퀴즈 1: 다음 중 정수형 오버플로우에 대한 설명으로 옳은 것을 선택하세요 (1개)

☐ 외부 입력값이 너무 커서 음수가 되어 시스템에 문제가 발생할 수 있다.

☐ 동적 메모리 할당을 사용하지 않는다.

☐ NULL 포인터를 참조할 때 발생한다.

제출

퀴즈 2: 다음 중 메모리 버퍼 오버플로우에 대한 설명으로 옳은 것을 선택하세요 (1개)

☐ 문자열 저장 시 NULL 문자로 종료하지 않으면 발생할 수 있다.

☐ 무한 루프에 의해 발생한다.

☐ 브라우저 캐시 설정으로 인해 발생한다.

제출

퀴즈

보안 상식에서 쉽게 접한 내용
들을 간단한 퀴즈를 통해 자연
스럽게 습득 가능

3. 웹사이트 설계 및 기능 -코드가이드

코드검사기

보안상식

퀴즈

코드 가이드

C 언어 시큐어 코딩 예시

문제가 되는 코드

정수형 오버플로우

```
#include

void vulnerable_function(int size) {
    char buffer[10];
    if (size < 0) {
        printf("음수 크기입니다!\n");
    }
    // 잠재적으로 음수 크기 또는 큰 크기를 허용하여 오버플로우 발생 가능
    char* ptr = (char*)malloc(size);
    if (ptr) {
        strcpy(ptr, buffer);
    }
}

int main() {
    int size = -1; // 음수 크기
    vulnerable_function(size);
    return 0;
}
```

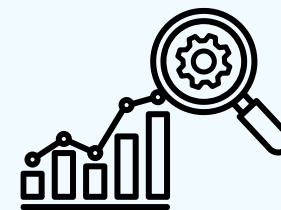
코드
가이드

소프트웨어 보안 개발 가이드를 참
고하여 시큐어 코드 예시를 작성

기대효과



유지보수단계에서 비용
절감과 신뢰성 향상



코드 품질 & 개발 효율성이
향상됨.



보안에 대한 접근성 향상,
사고를 예방하는 역량 강화

위 3가지 기대효과를 통해 실시간으로 보안 지식을 강화하고 코드 품질을 향상시킴

참고문헌

참고자료

- <https://www.donga.com/news/Society/article/all/20220822/115093902/1>
- 1.<https://www.donga.com/news/Society/article/all/20120628/47350682/2>
- 2.<https://www.dailysecu.com/news/articleView.html?idxno=4243>

인용논문

- 김준호, 전문석, 최원규, 이재승. (2014). 시큐어 코딩 의무화에 따른 소프트웨어 개발 효율성 및 신뢰성 향상으로 인한 파급효과에 대한 분석. 한국산학기술학회 학술대회논문집,, 435-436.
- 김태양, 박정훈. (2017-12-20). C언어 컴파일러의 소프트웨어 개발 보안. 한국정보과학회 학술 발표논문집, 부산.
- 노유정, 이주영, 목성균, 조은선. (2022-12-20). C_{hex}: 메모리 취약점 예외 처리를 지원하는 C 언어 확장. 한국정보과학회 학술발표논문집, 제주.
- 강석진, 최진영. (2016-12-21). 시큐어코딩 활성화를 위한 점검도구 확산 방안에 대한 연구. 한국정보과학회 학술발표논문집, 강원.

Q & A

감사합니다