s2023-2 컴퓨터 보안

**Final Project**

Team GoodNight

21800213 김휘진, 22000216 나보림, 22100579 이진주

1. **발표 주제 및 목표**

* **주제**

웹 해킹: 파일 업로드 공격(File Upload Attack, webshell)

* **목표**

웹 서버 공격 방법 중 하나인 파일 업로드 공격의 원리와 취약점 보완을 위한 해결책을 알아본다.

1. **발표 개요 및 세부 진행 계획**

* 웹에서의 file upload 시스템
  + 자료 조사를 통해 웹 서버에서 file이 upload되고 사용자에게 제공되는 원리를 파악한다.
* file upload attack 영향 및 사례
  + 현재까지 발생한 file upload attack에 대해 소개한다.
* file upload attack 원리
  + 위에서의 원리에 기반하여 이루어질 수 있는 file upload attack의 방법과 원리를 조사하고 공부한다.
* file upload attack 시연
  + 시연을 위한 웹 서버 환경을 구축한다.
  + file upload attack을 적용해본다.
* file upload 취약점 예방법
  + file upload attack을 적용했을 때 발생하는 문제들을 예방하는 방법을 조사하고 소개한다.

1. **데모 또는 실험 계획**

* 시연을 위한 웹 서버를 구축한다.
* 서버 환경을 이용한 침투 시나리오를 계획한다.
* file upload attack을 시연해본다.
* 결과를 정리하고 이를 예방하기 위한 방법을 조사 및 적용해본다.

1. **일정 계획**

* **11주차**: 주제 확정 및 구체화
* **12주차**: 자료조사 및 서버 구축
* **13주차**: file upload attack 테스트
* **14주차**: 발표 자료 준비

1. **팀원 역할 분담**

* **김휘진** : 자료조사, 웹 가상환경 구축 및 공격 적용, 취약점 보완, 발표자료 준비 및 발표
* **나보림** : 자료조사, 웹 가상환경 구축 및 공격 적용, 취약점 보완, 발표자료 준비 및 발표
* **이진주** : 자료조사, 웹 가상환경 구축 및 공격 적용, 취약점 보완, 발표자료 준비 및 발표

시연

멍청이서버 -> 개멍청이

뚫리고 랜섬웨어 감염

멍청이서버 고치기 -> 최종테크 ( 확장자만 막아도 되지 않냐? 안된다 왜냐면 ~~)

파일업로드 서버 구현

<https://docs.google.com/document/d/1gbvh6CL9FW7bAwryT4j9sqG8y7mP6nBjQZJs-WUrMSw/edit?usp=sharing>

랜섬웨어 동작

<https://docs.google.com/document/d/11gJjJVbP9SoZSbp-ov3GNWPTRkLDyG6j8L_XYBBQxZg/edit>

권한상승 ref

* <https://wonder12.tistory.com/104>
* [https://0msherl0ck.github.io/web/post-file\_upload\_attack/](https://c0msherl0ck.github.io/web/post-file_upload_attack/)
* <https://m.blog.naver.com/yyj9301/221131531557>

파일업로드 공격 ref

* <https://wonder12.tistory.com/83>
* <https://www.bugbountyclub.com/pentestgym/view/57>
* <https://portswigger.net/web-security/file-upload>

웹쉘 ref

* <https://m.boannews.com/html/detail.html?idx=111990>
* <https://m.boannews.com/html/detail.html?idx=109163> (권한상승 oss 포함)

보완 ref

* <https://cheatsheetseries.owasp.org/cheatsheets/File_Upload_Cheat_Sheet.html>
* <https://wpgur.tistory.com/91>
* <http://blog.plura.io/?p=6079>

랜섬웨어 ref

* <https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/>

키로거 ref

* <https://www.fortinet.com/kr/resources/cyberglossary/what-is-keyloggers>

PPT

<https://docs.google.com/presentation/d/15_S5xksw-H31AsEvpO-PTYqdh0bibac5-w5hF_SQFoU/edit?usp=sharing>