웹 해킹의 역사와 동향

202112021 박채우

웹 해킹의 시작

초기의 해킹 공격은 전화조작(phone phreaking)에서 시작되었다.

그러다 1980년대에 IBM에서 개인용 컴퓨터를 개발하면서 해킹의 주 대상은 컴퓨터, 즉 시스템 해킹으로 넘어갔다.

웹 해킹의 시작

1990년 유럽 입자물리 연구소의 팀 버너스리가 최초의 웹인 WWW를 개발한다.

1993년에는 모자이크의 개발

1994년에는 넷스케이프 내비게이터

1995년에는 IE가 공개되었다.

웹 해킹의 시작

1990년대 후반까지만 하더라도 해킹의 주 대상은 시스템 해킹이었다. 그러나 IDS과 방화벽 기술의 개발로 대부분의 포트가 공격을 차단하였다.

2000년대 초반부터 공격자들은 유일하게 열려있는 80포트, 즉 웹을 주 공격대상으로 삼기 시작했다.

웹 해킹의 시작

방화벽과 IDS가 없던 과거 : 어디에서나 접속이 가능한 오픈된 상황

방화벽과 IDS가 개발된 이후 : 웹이 외부와의 유일한 접점이 되었기 때문에 웹 해킹이 발전하게 됨

웹 해킹의 유형

SQL 인젝션	커맨드 인젝션	XPath 인젝션
XXE 인젝션	XSS	CSRF
파일 업로드 취약점	파일 다운로드 취약점	파라미터 변조 취약점
웹 페이지 접근 제어 부재	페이지 내 중요 정보 노출	WAS 취약점
프레임 워크 취약점		

웹 해킹의 유형

- SQL 인젝션
  - 파라미터에 SQL 쿼리를 입력해서 공격자가 의도한대로 DB와 임의의 정보를 주고 받는 공격
  - 웹 해킹의 가장 대부분을 차지한다.

- 커맨드 인젝션
  - 공격자가 악의적으로 시스템을 구동하는 명령에 자신의 의도대로 작성해서 명령을 보내는 것

웹 해킹의 유형

- Xpath 인젝션
  - SQL인젝션과 비슷하게 Xpath 쿼리문을 전송해 노드들의 정보를 얻어내는 공격

- XXE 인젝션
  - 공격자가 외부 엔티티를 이용해 공격자가 의도하는 외부 명령어를 실행시키는 공격

웹 해킹의 유형

- Xss 공격
  - 크로스 사이트 스크립팅 공격이라고도 하며 공격자가 스크립트 문을 삽입해 피해자가 접속할 때 스크립트가 실행

- CSRF 공격
  - 크로스 사이트 요청 위조 공격은 Xss와 유사하지만 위조된 요청을 서버에 전송해 서버에서 스크립트가 실행

웹 해킹의 유형

- 파일 업로드 취약점
  - 악성파일을 업로드 하여 해당 파일을 서버에서 실행시키는 공격
- 파일 다운로드 취약점
  - 다운로드 주소 변경 등으로 권한이 없는 파일까지 다운이 가능하도록 하는 공격
- 파라미터 변조 취약점
  - 특정한 입력정보가 들어오면 해당 내용을 강제로 다른 정보로 조작시키는 공격

웹 해킹의 유형

- 웹 페이지 접근 제어 부재
- 페이지 내 중요 정보 노출
- WAS 취약점
- 등등…

CVE-2022-21169

CVE-2023-50569

CVE-2022-39287

CVE-2023-35036

CVE-2023-34362

CVE-2021-26644

디렉토리 리스팅 : CVE-2022-30625

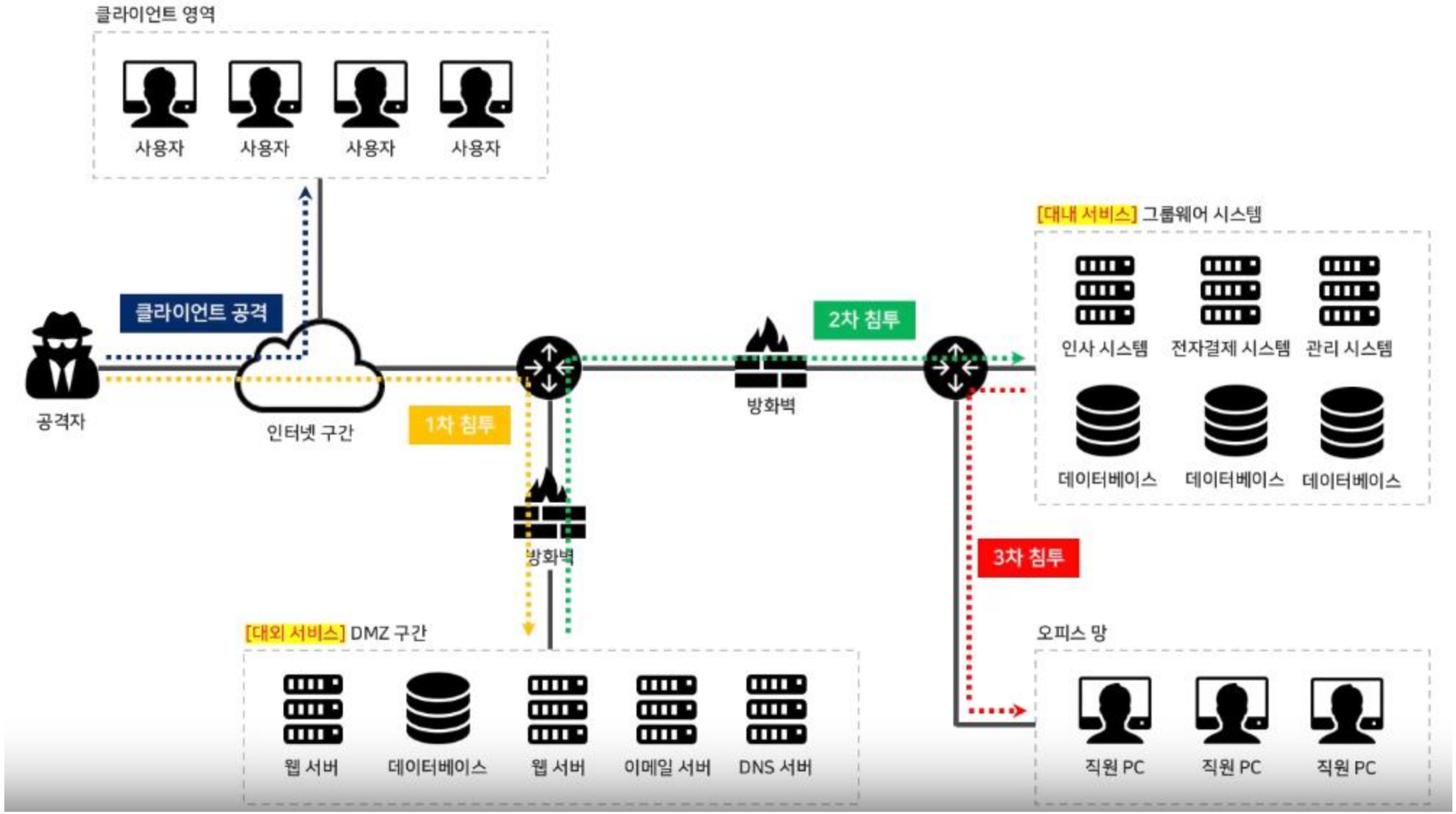
파일 업로드 : CVE-2021-26642

파일 다운로드 : CVE-2023-20077

웹 해킹의 목적?

웹 해킹의 주 목적은 관리자 권한의 탈취이다.

웹 해킹 하나로 공격이 끝나는 것이 아닌 관리자의 권한을 탈취함으로써 시스템에 대한 공격을 수행시키는 것이 가장 큰 목적이다.


클라이언트 영역
사용자
사용자
사용자
사용자
클라이언트 공격
공격자
인터넷 구간
1차 침투
방화벽
2차 침투
[대내 서비스] 그룹웨어 시스템
인사 시스템
전자결제 시스템
관리 시스템
데이터베이스
데이터베이스
데이터베이스
3차 침투
방화벽
[대외 서비스] DMZ 구간
웹 서버
데이터베이스
웹 서버
이메일 서버
DNS 서버
오피스 망
직원 PC
직원 PC
직원 PC

웹 해킹의 동향

과거에는 웹 서버의 데이터베이스에 집중적으로 공격을 가했다.

하지만 현재는 고가의 서버와 전문가들의 보안 활동 및 취약점 공개로 서버에 직접 침투하는 것이 힘들어졌다.

현재 공격자들은 서버가 아닌 개인 사용자를 타겟으로 하여 원하는 정보를 탈취하기 시작했다.

웹 해킹의 동향

클라우드의 발달로 많은 서비스들이 클라우드를 통해 제공되는 만큼 공격자들은 클라우드의 취약점에도 많은 관심을 두고 있다.

클라우드가 한번 털리면 그 밑의 모든 서비스들이 연쇄적으로 공격당하기 때문

웹 해킹의 동향

어떠한 새로운 공격 기법이 공개가 되는 것이 아닌 기존의 알려진 유명한 공격이 지속적으로 이루어 지고 있음

이미 알려진 공격들을 막는 코드를 개발자가 까먹었거나 해당 코드에서 오류가 생기는 것을 공격자들이 파악하며 공격을 수행함

웹 해킹의 동향

새로운 공격 기법은 자주 알려지는 것은 아니지만 기존의 공격 기법을 보완한 새로운 공격 툴은 끊임없이 발견된다.

직전 페이지의 취약점들을 찾는 행위들이 이러한 새로운 툴을 통해 발견이 되는 경우가 많다.

You can't defeat the threats of the present with tools from past.