SN (상)	데이터 평문 전송
취약점 개요	
점검목적	■ 서버와 클라이언트 간 통신 시 데이터의 암호화 전송 미흡으로 정보 유출의 위험을 방지하고자 함
보안위협	■ 웹상의 데이터 통신은 대부분 텍스트 기반으로 이루어지기 때문에 서버와 클라이언트 간에 암호화 프로세스를 구현하지 않으면 간단한 도청(Sniffing) 을 통해 정보를 탈취 및 도용할 수 있음
참고	※ **Sniffing:** 스니퍼(sniff: 냄새를 맡다, 코를 킁킁거리다)를 이용하여 네트워크상의 데이터를 도청하는 행위 ※ 소스코드 및 취약점 점검 필요
조치방법	사이트의 중요정보 전송구간(로그인, 회원가입, 회원정보관리, 게시판 등) 암호화 통신(https, 애플리케이션방식) 적용
보안설정 방법	

* 웹상에서의 전송 정보를 제한하여 불필요한 비밀번호, 주민등록번호, 계좌정보와 같은 중요정보의 전송을 최소화하여야 하며, 중요정보에 대해서는 반드시 SSL 등의 암호화 통신을 사용하여 도청으로부터의 위험을 제거함
* 쿠키와 같이 클라이언트 측에서 노출되는 곳에 비밀번호, 인증인식 값, 개인정보 등의 정보를 기록하지 않음
* 암호화 전송 시 프로토콜 설계의 결함이 있는 SSLv2, SSLv3, TLSv1.0, TLSv1.1은 비활성화 필수, TLSv1.2 이상 사용을 권장함

※ 웹 서버 별 상세 설정

■ Apache

```
httpd-ssl.conf 또는 ssl.conf의 SSL 관련 VirtualHost 설정에 아래를 추가
SSLProtocol all -SSLv2 -SSLv3 -TLSv1 -TLSv1.1
```

■ IIS

[SSL v2 사용 안 함]
[HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Control₩SecurityProviders₩SCHANNEL₩Protocols₩SSL 2.0₩Server]
하위에 '새로만들기' > 'DWord(32비트)' 값 선택 > 이름 부분에 'Enabled' 입력 > 데이터 부분에 '0' 입력 > 시스템 재부팅

[SSL v3 사용 안함]
[HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Control₩SecurityProviders₩SCHANNEL₩Protocols₩SSL 3.0₩Server]
하위에 '새로만들기' > 'DWord(32비트)' 값 선택 > 이름 부분에 'Enabled' 입력 > 데이터 부분에 '0' 입력 > 시스템 재부팅