WO(중)	웹 메소드 설정 공격
취약점 개요	
점검목적	■ 사용 가능한 Http Method를 확인하고 세션이 인증되어 있지 않은 상태에서의 PUT, DELETE, HEAD와 같은 Method 허용 여부 확인
보안위협	■ 해당 취약점이 존재할 경우 허가되지 않은 공격자가 이를 이용하여 웹 서버에 파일 생성, 삭제 및 수정이 가능
참고	※ 운영상 지원되어야 하는 Method 가 있다면 확인 후 적용 필요
조치방법	※ 취약점 조치 시 WEB 운영자 담당자와 협의하여 영향도 검토 후 중기 적용 필요
보안설정 방법	

■ 확인방법

- OPTIONS 메서드를 이용한 점검 수행하여 불필요한 메서드가 설정되어 있는지 확인
  오픈나루 12 opennaru.com
  telnet [웹사이트 URL 또는 IP][사용포트 – 일반적으로는 80](엔터)
  telnet> OPTIONS * HTTP/1.0(엔터 2번)

- httpd.conf 파일 /[apache_home]/conf/httpd.conf 에서 확인

- HTTP Method 를 일부 항목으로 제한

Apache 웹 서버는 GET, POST, PUT, DELETE, CONNECT, OPTIONS, PATCH, PROPFIND, PROPPATCH, MKCOL, COPY, MOVE, LOCK, UNLOCK 등의 다양한 Method 를 지원함
이 Method 들은 WebDAV나 telnet을 이용해 해당 Method를 요청하는 경우 서버에 임의의 파일을 생성하거나, 삭제 할 수 있음
※ 웹 서버 별 상세 설정

■ Apache

```
<Directory /home>
        AllowOverride FileInfo AutoConfig Limit
        Options MultiViews Indexes SymLinksIfOwnerMatch IncludesNoExec
        <Limit OPTIONS PROPFIND>
                Order allow,deny
                Allow from all
        </Limit>
        <LimitExcept GET POST>
                Order deny,allow
                Deny from all
        </LimitExcept>
</Directory>
```

※ 위와 같이 설정하면 정상적으로 Apache 웹 서버에 로그인 권한을 가진 사용자 외의 사용자는 제한된 Method 인 PUT DELETE COPY MOVE PATCH MKCOL Method를 사용할 수 없음