Security (보안, 방화벽)

- description : 보안과 관련된
- author : 주레피
- email : dhan@repia.com
- lastupdate : 2020-03-02

방화벽 허용 간단 확인 법

방화벽을 확인하기 위해서는 출발지, 목적지 포트가 필요하며 출발지는 아래 코드를 실행하는 PC의 IP 대역이 된다.

```
C:\사용자\repia> telnet ${IP} ${PORT}
```

> 방화벽이 없을 경우 즉시 응답이 오며, 서비스 유형을 판단할 수 있다.
> 응답이 늦어지면 방화벽이 있을 경우가 대부분이며, 방화벽 솔루션 이외에 OS 자체내의 방화벽도 고려하여야 한다.
> telnet 클라이언트가 없을 경우 아래의 설치법을 활용하여 설치하도록 한다.

Encoding, Decoding

온라인 Base64 인코딩, 디코딩
JAVA-BASE64-인코딩-디코딩하기

Telnet 설치

Window10
Window7

CentOS7
CentOS6

시큐어코딩 가이드

한국인터넷징흥원(KISA) 기술안내서 가이드
JAVA 시큐어코딩 가이드

- 코딩가이드_java_v1.2_수정_-웹용.pdf

XSS 보안 대책 → CSP(콘텐츠 보안 정책)

구글 콘텐츠 보안 정책
Content Security Policy (CSP)

참조

OPENEG 기술자료 참조
제로트러스트 개념

CA 서명 인증서를 사용

```
인정서(Certificate)의 begin date와 expire date가 유효해야 한다.
hostname 값이 맞아야 한다.
폐기(revoked)되지 않아야 한다.
SHA2 이상의 알고리즘으로 서명되어야 한다.
신뢰할 수 있는 CA 업체의 서명을 받은 인증서여야 한다.
```

패스워드 설정 규칙

```
1. 3가지 유형으로 9자리 이상이어야 함(대/소문자, 특수기호, 숫자 각1개 이상 포함)
2. 초기 패스워드는 변경 후 사용
3. 90일마다 패스워드를 강제 변경
4. 비밀번호 변경 후 최소 10일 간 재 변경은 불가능
5. 직전 4개의 패스워드를 기업(1년 내 재사용 금지)
6. ID와 동일한 패스워드 사용 불가
7. 자동 로그인 사용 불가
8. 연속 5번 패스워드 입력 실패 시 계정 잠금(10분 후 자동 해제)
9. 타 시스템과 동일 패스워드 사용 금지

클라이언트 사이드의 입력값 검증은 신뢰할 수 없으므로(쉽게 우회 가능), 중요 기능은
반드시 서버 사이드에서 구현하는 것이 원칙

초기 패스워드는 알 수 없게 생성하고, 개별적으로 전달(SMS, 메일)
```

용어

SHA2(샤투)

주레피, 방화벽

From:
http://125.132.25.164/dokuwiki/ - **문제를 잘 정의하는 것은 문제를 절반 해결한 것이다. - 2023.12**

Permanent link:
http://125.132.25.164/dokuwiki/doku.php?id=wiki:security&rev=1593498655

Last update: **2022/03/10 19:52**