BLACKLIST

개인정보 검출 보고서

개인정보 검출 보고서

www.target-shop.kro.kr/

일시	2023년 11월 23일
탐지분야	웹사이트 검증
보안등급	B

BLACKLIST

1. 프로젝트 개요

2. 페이지 분석 결과

3. 개인정보 처리

4. 개인정보 가명화 처리 방침

프로젝트 개요

본 보고서의 내용을 인용할 때는 반드시 인용 가능한 데이터인지 확인하고, 가명화 처리가 되지 않은 데이터는 인용할 수 없음을 주의해야 합니다.

검출된 데이터는 정확하지 않을 수 있으며, 만일 개인정보가 검출되었다면 해당 URL에 검출되지 않은 개인정보가 있는지 확인하는 것이 필요합니다.

개인정보 검출 정도에 따라 심각도가 A, B, C, D 총 4단계로 나뉩니다. (D: 주의, C: 경고, B: 심각, A: 서버 중지)

개인정보 유출은 평판 손상, 수익 손실, 신뢰성 저하 등의 문제를 야기할 수 있습니다.

유출된 정보를 검출하여 개인 정보 처리의 중요성과 위험성을 논의하며, 동시에 완화 전략을 제시하고자 합니다.

분석 결과

www.target-shop.kro.kr/

구분	문제 개수
이름	2
도로명 주소	1
전화번호	1
이메일	1

[검출된 정보 확인]

개인정보 처리

2020년 8월, 정부의 데이터 3법이 시행되면서 데이터 활용을 위한 가명정보 개념이 도입되며, 개인정보 또는 개인신용정보에 대하여 가명처리(비식별조치)한 가명정보를 정보주체의 동의 없이 이용⊠제공할 수 있습니다

Blacklist는 수집한 개인정보를 주체에게 제공하고, 가명화 처리 방법을 제공합니다. 수집한 개인정보는 보고서에 작성된 즉시 데이터를 삭제합니다. 개인정보를 상업적으로 이용하지 않음을 알려드립니다

개인의 존엄과 가치를 구현하기 위하여 2011년 개인정보 보호법이 제정 · 시행되었습니다.

개인정보 가명화

```python
#python
import re

def mask_names(text, names_to_mask):
    # 각 이름에 대해 정규 표현식을 사용하여 마스킹 처리
    for name in names_to_mask:
        text = re.sub(r'\b' + re.escape(name) + r'\b', lambda x: '*' * len(x.gro
up()), text)
    return text

  # 주어진 텍스트
text = "개인정보가 검출된 소스코드"

  # 개인정보 마스킹할 이름들
names_to_mask = ["검출된 개인정보"]

  # 개인정보 마스킹 처리
masked_text = mask_names(text, names_to_mask)

print(masked_text)
```

이 코드는 mask_names 함수를 사용하여 주어진 텍스트에서 각 이름을 찾아서 '*'로 마스킹 처리합니다.

개인정보 검출 시에는 삭제를 우선시해야 하며, 가명화는 선택적으로 사용되어야 합니다. 가명화된 데이터 역시 보안에 취약할 수 있으므로 민감한 정보의 경우 적절한 안전성을 고려해야 합니다.

개인정보 처리 가이드라인은 2020년 9월에 발표되었으며, 2021년 10월에 개정되었습니다. 가명처리 영역 전체 흐름도에 나오는 단계를 지키며 개인정보 가명화 처리가 이루어지는 것이 바람직합니다.