본인확인서비스 이용기관 취약점 자체점검 체크리스트

기 관 명					
담 당 자		연 락 처		이 메 일	
작성일자	2024. 00. 00.				

순번	본인확인서비스 이용기관(웹사이트) 취약점 자체점검 항목	검토여부
1	**(불필요한 중요정보 평문 노출)** 본인확인 이후 회원가입 단계에서 이용자에게 불필요한 개인정보(CI/DI)가 평문으로 드러나지 않도록 조치하였는가?	Y/N □□
2	**(파라미터 변조)** 본인확인 이후 회원가입 과정에서 이용자가 입력한 데이터를 서버 또는 Web to Web으로 전송할 때, 본인확인 결과정보(이름, 생년월일, 인증 결과, 이용자의 CI/DI 등)를 다른 정보로 변조할 수 없도록 조치하였는가?	Y/N □□
3	**(입력정보 일치여부)** 본인확인기관(또는 대행사)으로부터 수신한 결과정보를 복호화한 값과 이용자가 입력한 값(회원가입 등) 및 신원확인 단계에서 입력한 값 간 일치 여부를 검증하였는가?	Y/N □□
4	**(데이터 재사용)** 동일 웹사이트에서 과거에 수집된 인증정보(암호화 데이터, 거래번호, 토큰, 세션 등)를 재사용하지 못하도록 조치하였는가?	Y/N □□
5	**(암호키/모듈 노출)** 본인확인서비스 테스트를 위한 샘플페이지 내 인증모듈 복호화 키와 실제 키가 동일하지 않도록 설정하고 해당 암호키/모듈이 노출되지 않도록 조치하였는가?	Y/N □□
6	**(프로세스 검증 누락)** 인증이 필요한 웹 사이트의 중요 페이지(관리자 페이지, 회원 변경 페이지 등)에 대한 접근통제를 수행하고 있는가?	Y/N □□
7	**(안전한 통신 프로토콜 사용)** 본인확인서비스 이용을 위해, 안전한 통신 프로토콜(TLS 1.2 이상)을 사용하고 있는가? **※ 모듈, API 이용기관만 해당되며, 전용망 이용기관은 해당 없음(NA)로 회신**	Y/N/NA □□

※ 문의처 : 본인확인서비스 대행사 담당자(이메일 등 연락처 작성)

안전한 본인확인서비스 제공을 위하여 상기 항목대로 자체점검을 진행하며, 아래의 보안가이드 내용에 준수할 것을 동의합니다.

※ 이용기관은 해당 내용에 대한 동의를 거부할 수 있습니다. 단, 동의를 거부할 경우 서비스 계약 및 제공이 불가할 수 있음을 알려 드립니다.

책임자 서명 : (인)

참 고 체크리스트 항목별 취약점 사례 및 조치방안

① **(불필요한 중요정보 평문 노출)** 본인확인 이후 회원가입 단계에서 이용자에게 불필요한 개인정보(CI/DI)가 평문으로 드러나지 않도록 조치하였는가?

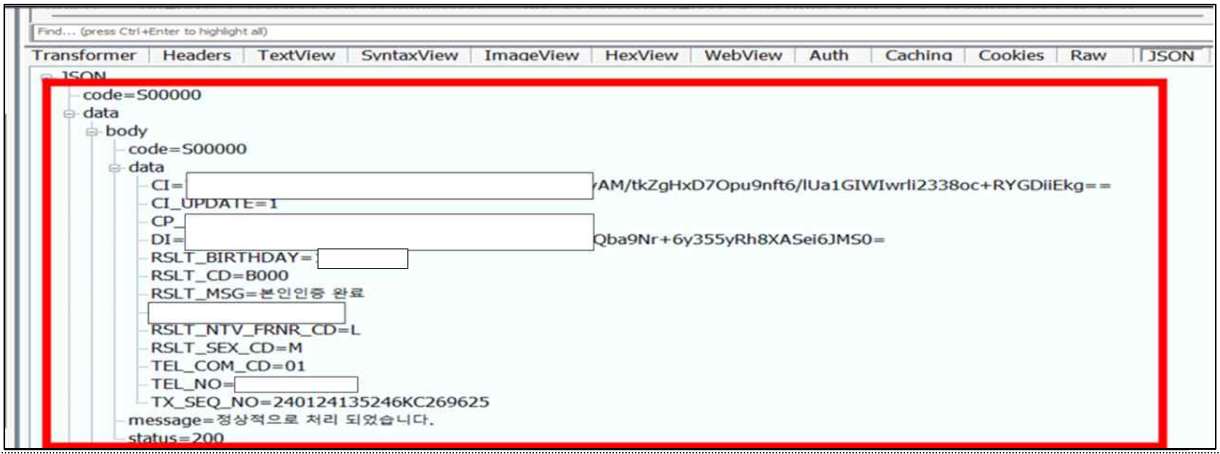
※ 주요 확인사항 : 본인확인 결과 데이터 처리 과정, 본인확인 완료 후 이용기관으로 전송되는 메시지 및 민감정보 전송 시 암호화 여부 등 확인

취약점 사례

○ 이용기관은 본인확인 결과정보를 활용하기 위해 Hidden tag를 이용하여 필요한 데이터를 A페이지에서 B페이지로 전달하는 방법을 사용하고 있으나, 회원가입에 필요한 정보뿐 만 아니라 이용자에게 노출될 필요가 없는 중요정보(CI/DI, CP코드 등)가 평문으로 노출

○ 해당 데이터를 수집 및 활용하여 타 서비스 부정가입 및 명의 도용 등 피해가 발생

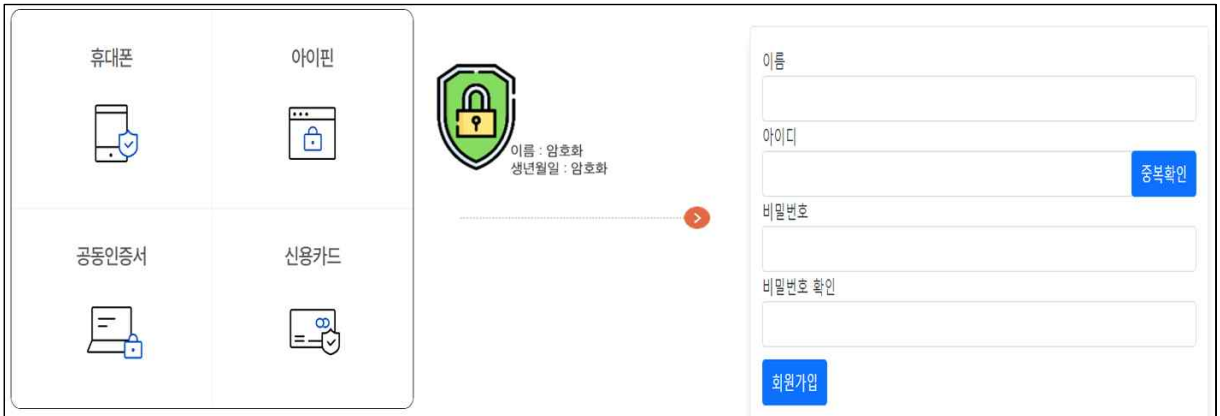
※본 이미지들은 샘플페이지로 실제 취약점이 존재하지 않음을 알립니다.



조치방안

○ 회원가입 단계에서 필요한 이용자의 개인정보는 암호 알고리즘을 사용하여 데이터 암호화 후 Hidden tag로 이용자 정보를 전달하여 정보 노출 최소화

○ 본인확인 결과를 페이지에서 넘기지 않고 세션과 같은 이용자를 식별 가능한 임시 데이터를 활용하여 복호화된 본인확인 결과 데이터 처리



※본 이미지들은 샘플페이지로 실제 취약점이 존재하지 않음을 알립니다.

Body

Name	Value
Keygb	1
Resultcd	0000
Mobilid	202401318354827
Mrchid	23120514
Ci	caef
Sex	f4b3
Foreigner	21e
Safeguard	
Cryptyn	Y
Mac	863
Commid	d48

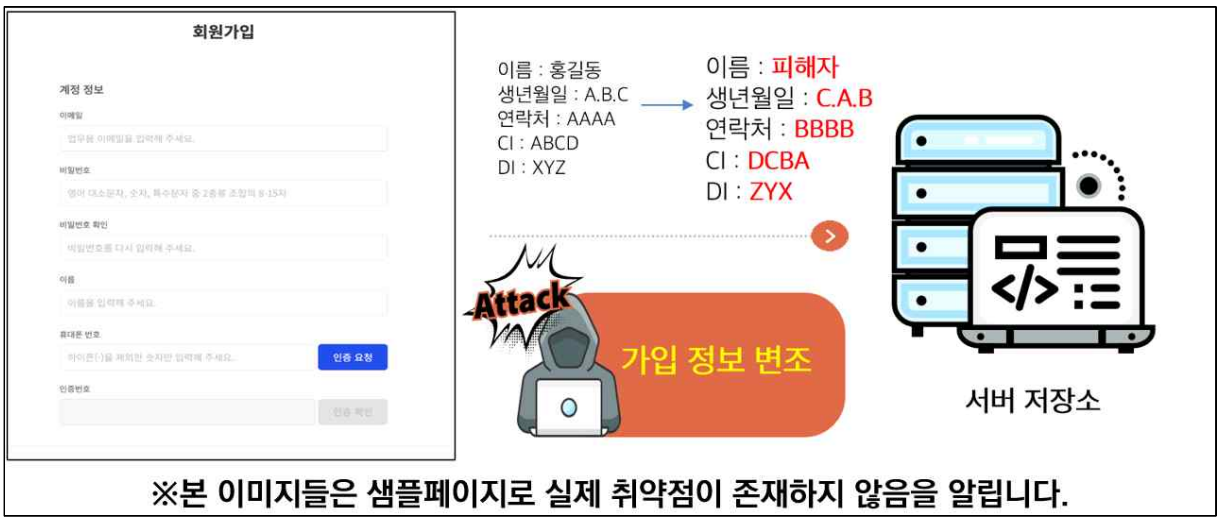
② **(파라미터 변조)** 본인확인 이후 회원가입 과정에서 이용자가 입력한 데이터를 서버 또는 Web to Web으로 전송할 때, 본인확인 결과정보(이름, 생년월일, 인증 결과, 이용자의 CI/DI 등)를 다른 정보로 변조할 수 없도록 조치하였는가?

※ 주요 확인사항 : 본인확인 결과정보의 보호조치 여부, 이용자가 입력데이터의 조작 가능 여부, 이용자 입력데이터와 본인확인 결과정보 및 신원확인 정보 간 일치 여부 확인

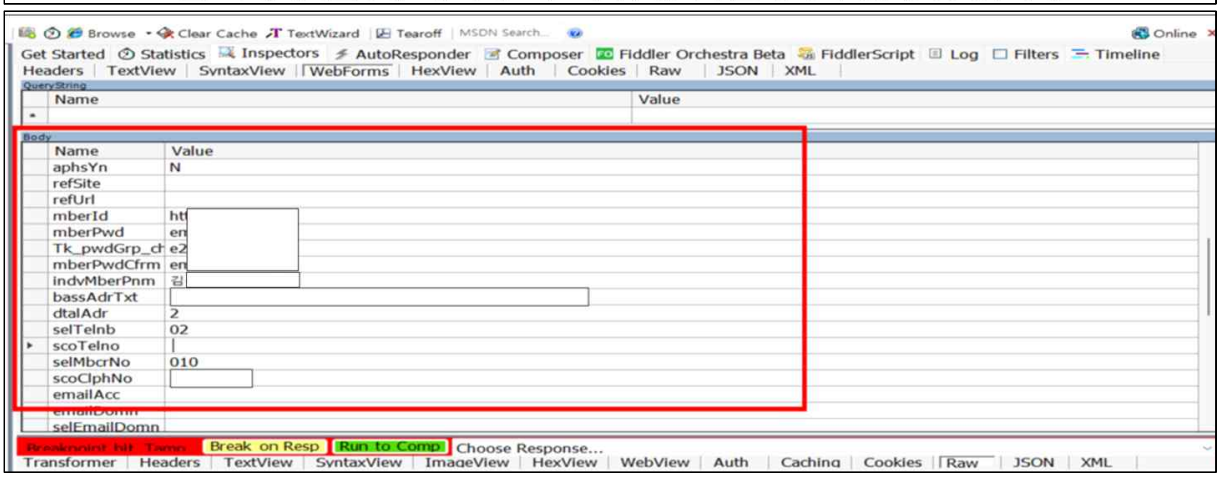
취약점 사례 1

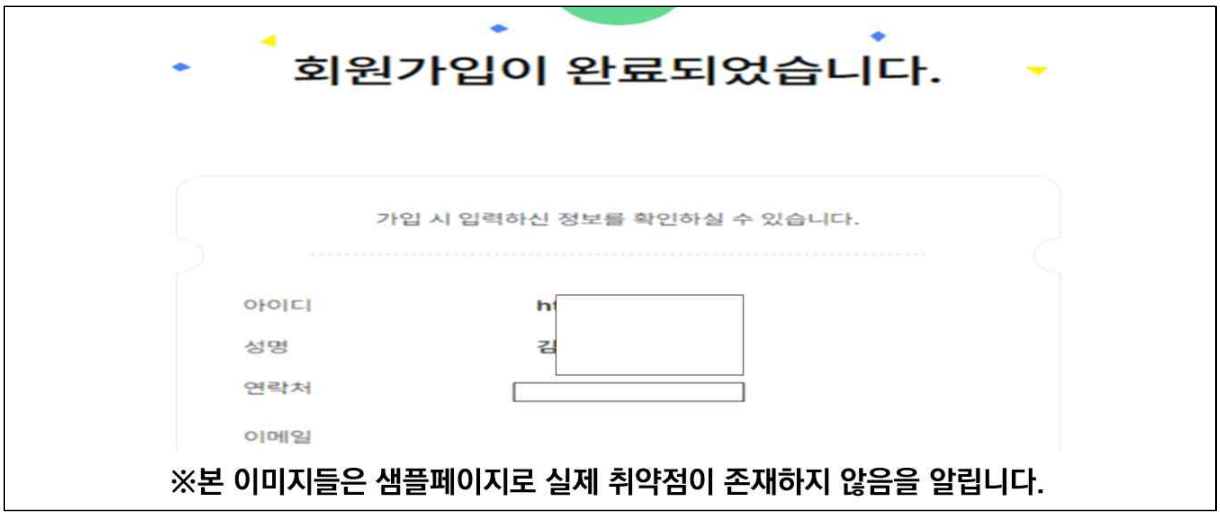
○ 이용자가 본인확인을 진행한 뒤 본인확인 결과정보를 웹페이지 이용기관의 서버로 전송할 때, 전송되는 패킷의 데이터 변조가 가능하여 본인확인 결과정보와 다른 정보가 서버에 전송될 경우, 타인 명의로 가입 가능

○ 이용자가 본인확인을 진행한 뒤 변경할 수 없는 Read-only 필드의 데이터를 포함하여 서버로 전송할 때, 해당 데이터들을 임의로 변조해 서버에 전송될 경우, 타인 명의 가입 가능



※본 이미지들은 샘플페이지로 실제 취약점이 존재하지 않음을 알립니다.



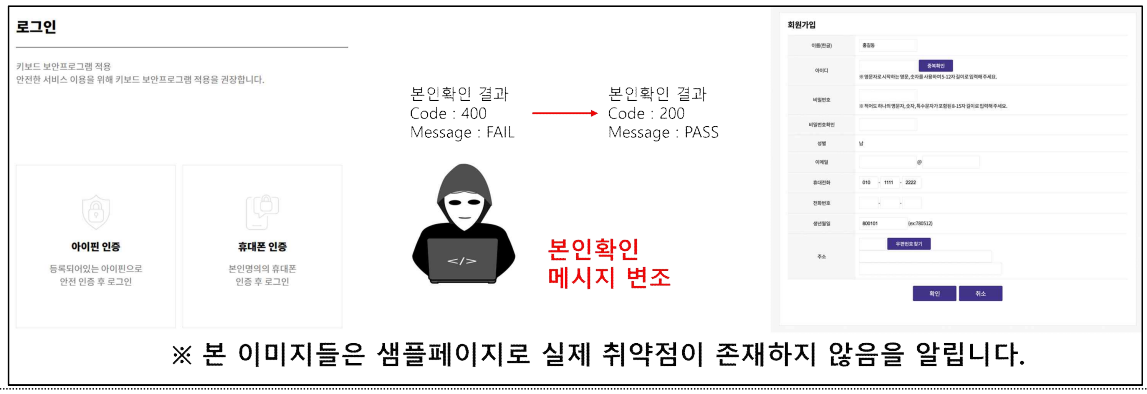


※본 이미지들은 샘플페이지로 실제 취약점이 존재하지 않음을 알립니다.

취약점 사례 2

○ 본인확인 결과 '실패' 메시지를 '성공' 메시지로 위·변조하여 회원가입 할 경우 타인 명의 가입이 가능

○ 이용자 조회, 비회원 조회와 같은 서비스를 본인확인 결과를 기반으로 제공하는 서비스에서 본인확인은 실패했지만, 서버에서 PASS&FAIL만 검증하여 임의로 결과를 PASS로 변조하여 타인의 서비스 이용 내역을 조회



※ 본 이미지들은 샘플페이지로 실제 취약점이 존재하지 않음을 알립니다.

③ **(입력 정보 일치 여부)** 본인확인기관(또는 대행사)으로부터 수신한 결과정보를 복호화한 값과 이용자가 입력한 값(회원가입 등) 및 신원확인 단계*에서 입력한 값 간 일치 여부를 검증하였는가?

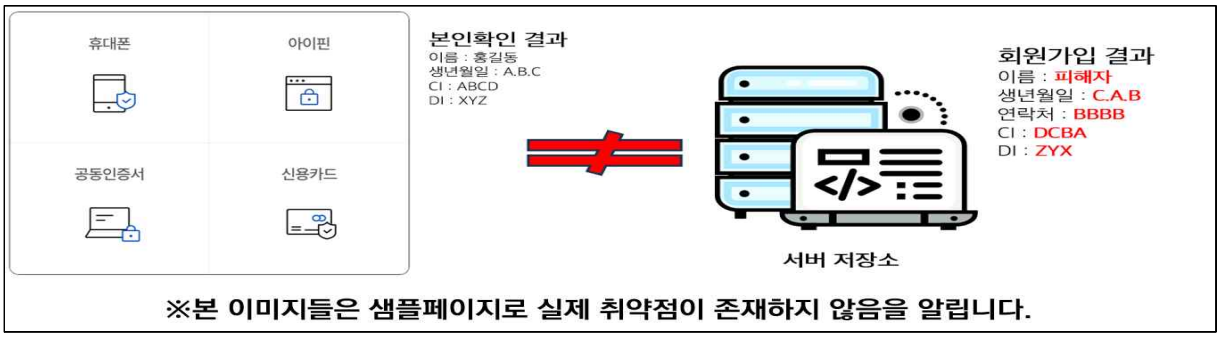
* 실명 확인, 본인확인, 계좌점유, 신분증 진위여부 등 복합적으로 신원 확인하는 절차

※ 주요 확인사항 : 이용자 입력데이터와 본인확인 결과정보 일치 여부, 신원확인 단계 간 입력데이터와 본인확인 결과정보 일치 여부, Sever Side 내 데이터 간 일치 여부 등 확인

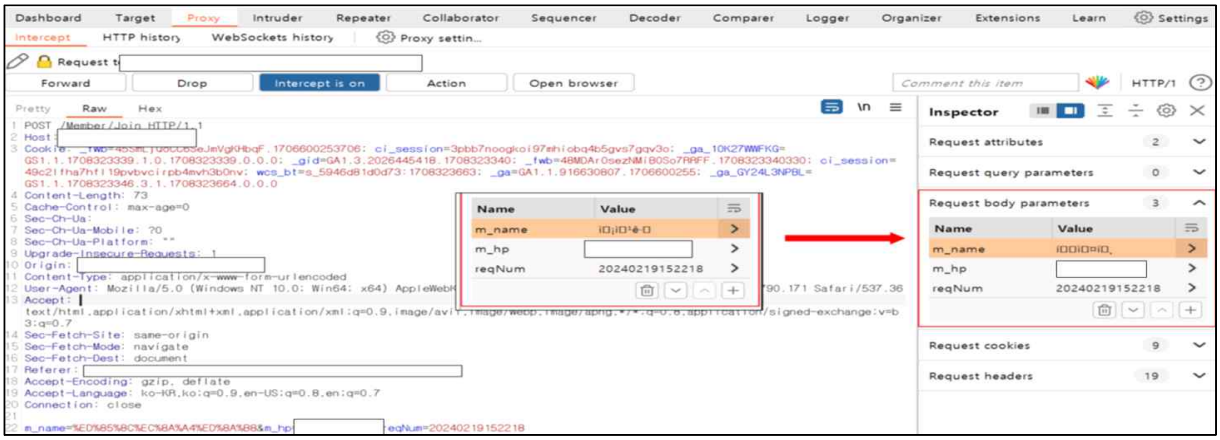
취약점 사례 1

○ 이용자가 본인확인 후, 본인확인 정보가 이용기관(웹사이트)에 전달되어 복호화 후 DB에 저장되지만, 파라미터 변조 등으로 본인확인 결과를 변조하여 전송해도 변조된 데이터를 DB에 저장

○ 웹 사이트에서 본인확인 결과와 DB에 저장될 데이터 간 일치 여부를 검증해야 하나, 이를 검증하지 않아 명의도용



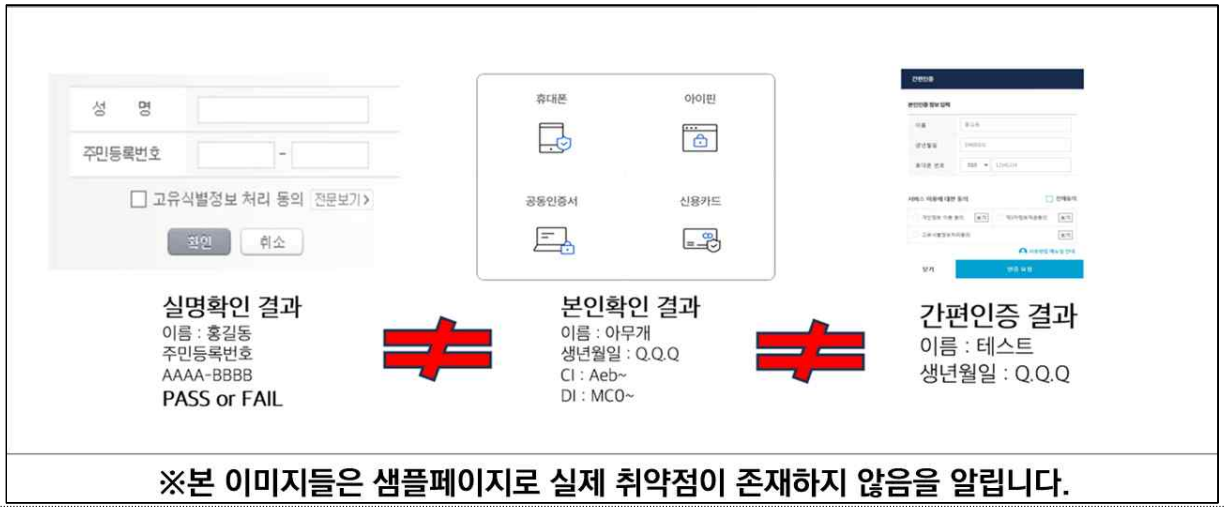
※본 이미지들은 샘플페이지로 실제 취약점이 존재하지 않음을 알립니다.



취약점 사례 2

○ 회원가입 단계 중 본인확인서비스 외 신원확인 방법을 복합적으로 수행하는 경우 신원확인 결과를 PASS&FAIL만 확인하고 본인확인 결과 기준 신원확인 데이터와 비교하지 않아 타인명의로 가입

○ 서비스 이용을 위해 하나 이상의 복합 신원확인을 진행할 때 본인확인 기준 다른 복합 신원확인 데이터 간 상호 검증을 진행하지 않아 타인명의로 서비스 제공. 본인확인, 실명인증, 간편인증을 수행하는 서비스에서 각 인증결과 및 입력데이터 상호비교를 하지 않아 본인확인은 A, 간편인증은 B로 진행하여 A와 B의 결과가 달라도 B의 명의로 서비스 제공



※본 이미지들은 샘플페이지로 실제 취약점이 존재하지 않음을 알립니다.

조치방안

○ 이용자가 입력한 값과 인증결과(실명인증, 본인확인, 간편인증등)가 동일한지 검증

○ 본인확인 결과와 같은 신뢰 가능한 데이터를 기준으로 이용자가 입력한 데이터를 교차 비교하여 일치 여부 검증, 이용자가 최초 입력정보와 해당 서비스의 마지막 단계 인증데이터를 서버에서 최종적으로 비교하도록 조치

○ 복합인증에서 발생하는 결과 값이 모두 동일한 이용자인지 교차검증 수행

④ **(데이터 재사용)** 동일 웹사이트에서 과거에 수집된 인증정보(암호화 데이터, 거래번호, 토큰, 세션 등)를 재사용하지 못하도록 조치하였는가?

※ 주요 확인사항 : 본인확인서비스 발생한 데이터에 대한 인증 횟수 제한, 만료 시간 설정여부 확인

취약점 사례

○ 공개된 공공 와이파이에 접근하여 이용자들의 본인확인 결과 데이터를 수집한 뒤 본인확인 결과 데이터 재사용

○ 공공 와이파이 등 외부 환경에서 타인 이미 성공한 본인확인 결과 메시지를 탈취하여 동일 웹사이트에 재사용하여 타인이 회원가입 가능

조치방안

○ 데이터 재사용 방지를 위한 인증 횟수 및 만료 기간 설정

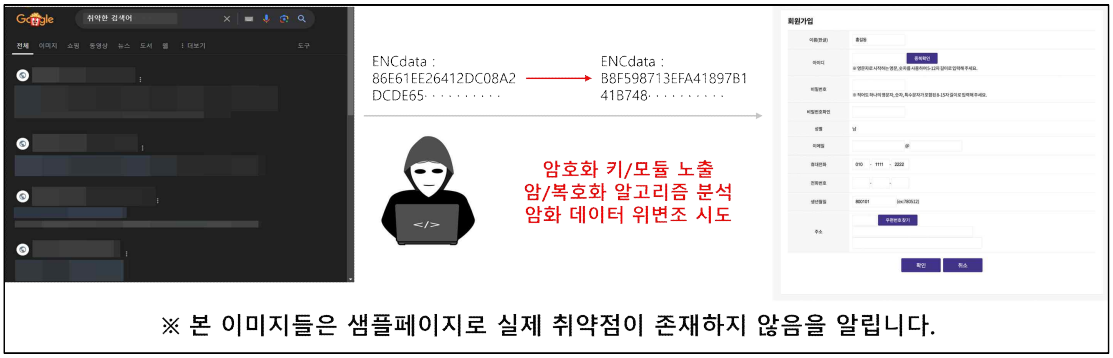
⑤ **(암호키/모듈 노출)** 본인확인서비스 테스트를 위한 샘플 페이지 내 인증모듈 복호화 키와 실제 키가 동일하지 않도록 설정하고 해당 암호키가 노출되지 않도록 조치하였는가?

※ 주요 확인사항 : 검색 엔진(구글, 네이버 등) 내 본인확인서비스 모듈 노출 여부, 서비스 암·복호화 키 노출 여부, 민감정보 노출 여부

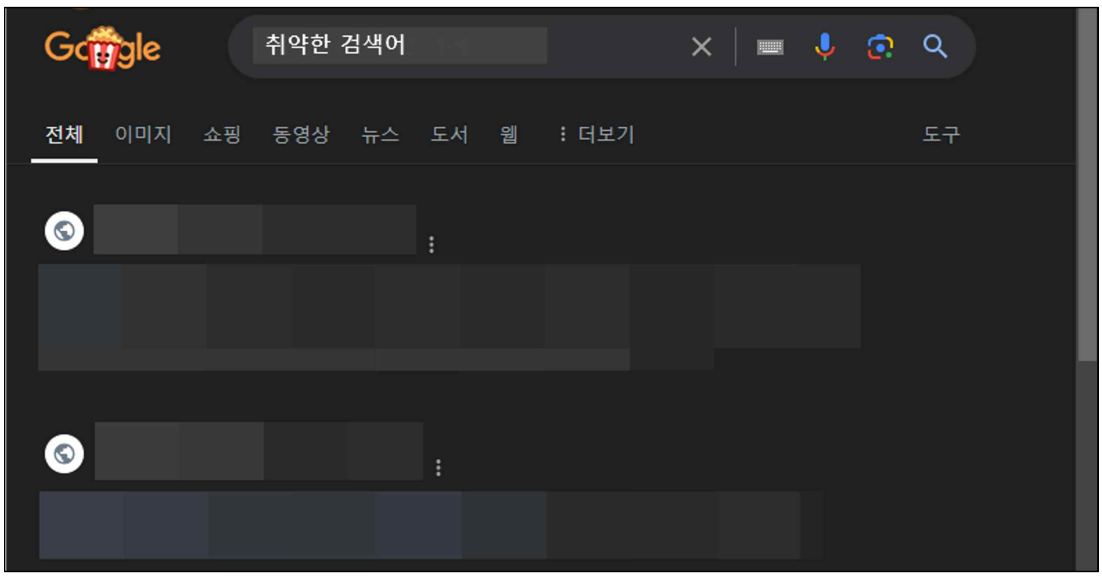
취약점 사례 1

○ 웹페이지 개발 및 테스트를 위해 만들어둔 임시 사이트가 남아있는 경우, 해당 사이트에 노출된 본인확인서비스 암호키를 사용하여 웹페이지와 이용자간 주고받는 본인확인 결과정보를 열람 및 탈취

○ 본인확인서비스 구축 중 이용기관이 사용하는 모듈, 암호키, 구축 방법을 블로그에 업로드. 공격자는 공개된 정보를 바탕으로 이용기관이 사용하는 모듈의 암호 알고리즘과 키를 분석해 암호화된 본인확인 결과 데이터의 이름, 생년월일 성별, CI/DI 등을 위·변조하여 가상의 인물로 회원가입이 가능



※ 본 이미지들은 샘플페이지로 실제 취약점이 존재하지 않음을 알립니다.



조치방안

○ 검색 엔진, 블로그, github 등과 같은 외부로 공개된 서비스에 본인확인 결과정보 암·복호화 키를 노출되지 않도록 설정하고 주기적으로 점검을 통해 확인

○ 크롤러가 웹 서버에 있는 중요 파일 경로에 접근하지 못하게 하도록 설정하거나 적절한 예외 처리를 통하여 본인확인 관련 페이지 노출 차단

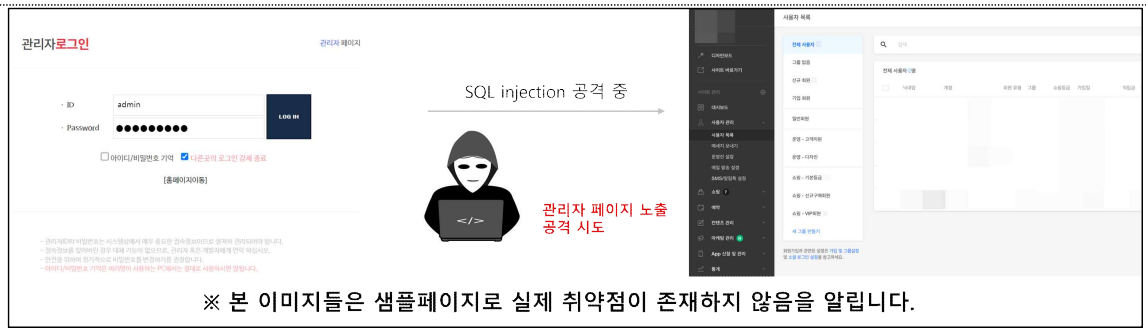
⑥ (프로세스 검증 누락) 인증이 필요한 웹 사이트의 중요 페이지(관리자 페이지, 회원변경 페이지 등)에 대한 접근통제를 수행하고 있는가?

※ 주요 확인사항 : 중요 페이지(회원정보 변경, 비밀번호 재설정)에 대한 접근통제 여부, 접근권한 검증 여부, 페이지 URL 직접 접속 가능 여부 등 확인

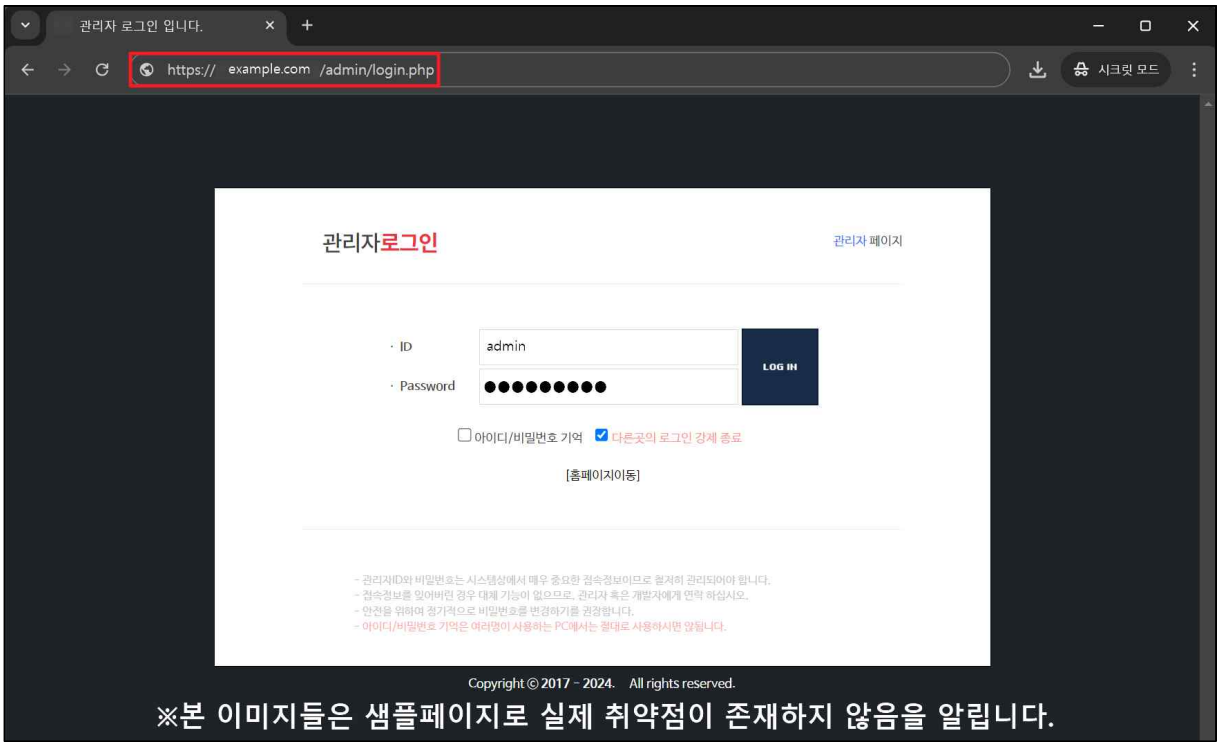
취약점 사례

○ 인증이 필요한 웹 사이트의 중요페이지에 대한 접근 제어가 미흡할 경우 하위 URL 직접 접근, 스크립트 조작 등의 방법으로 중요 페이지에 접근하여 고객의 개인정보 유출 및 조작

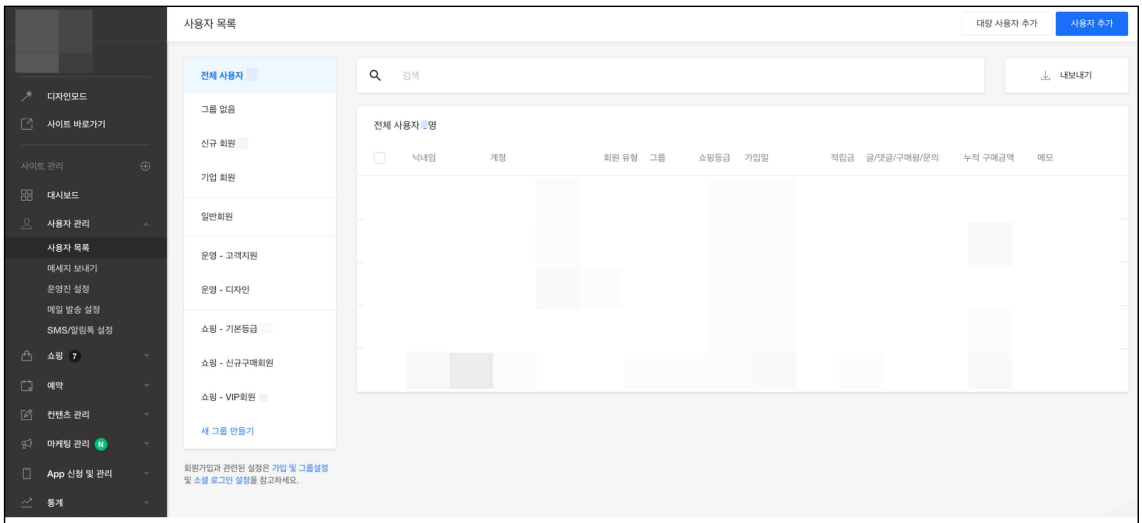
○ 쇼핑몰 사이트를 모두 관리 가능한 관리자 페이지를 유추하기 쉬운 경로인 ~/admin 등으로 구축될 경우, 해커가 해당 페이지에 접근하여 관리자 권한 탈취 및 서버에 존재하는 고객 개인정보 탈취



※ 본 이미지들은 샘플페이지로 실제 취약점이 존재하지 않음을 알립니다.



※본 이미지들은 샘플페이지로 실제 취약점이 존재하지 않음을 알립니다.



※ 본 이미지들은 샘플페이지로 실제 취약점이 존재하지 않음을 알립니다.

조치방안

○ 관리자 페이지 접근을 우회할 수 있는 경로를 차단하여야 하며, 페이지별 권한 매트릭스를 작성하여 페이지에 부여된 권한의 타당성을 체크한 후 권한을 기준으로 전 페이지에서 권한 체크가 이뤄지도록 구현

○ 인증이 필요한 모든 페이지에 대해 유효 세션임을 확인하는 프로세스 및 주요 정보 페이지에 접근 요청자의 권한 검증 로직을 적용

○ 유효 세션의 검증 및 페이지에 대한 접근권한을 Client Side Script에 의존할 경우 이용자가 임의로 수정할 수 있으므로 Server Side Script로 구현

⑦ **(안전한 통신 프로토콜 사용)** 본인확인서비스 이용을 위해, 안전한 통신 프로토콜(TLS 1.2 이상)을 사용하고 있는가?

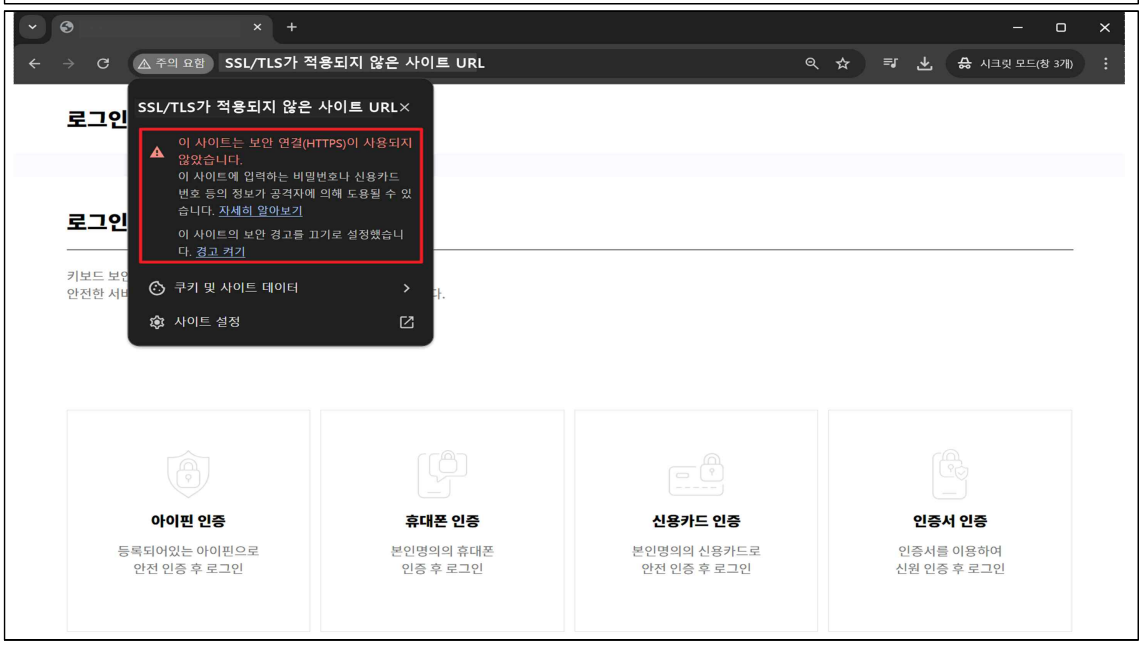
취약점 사례

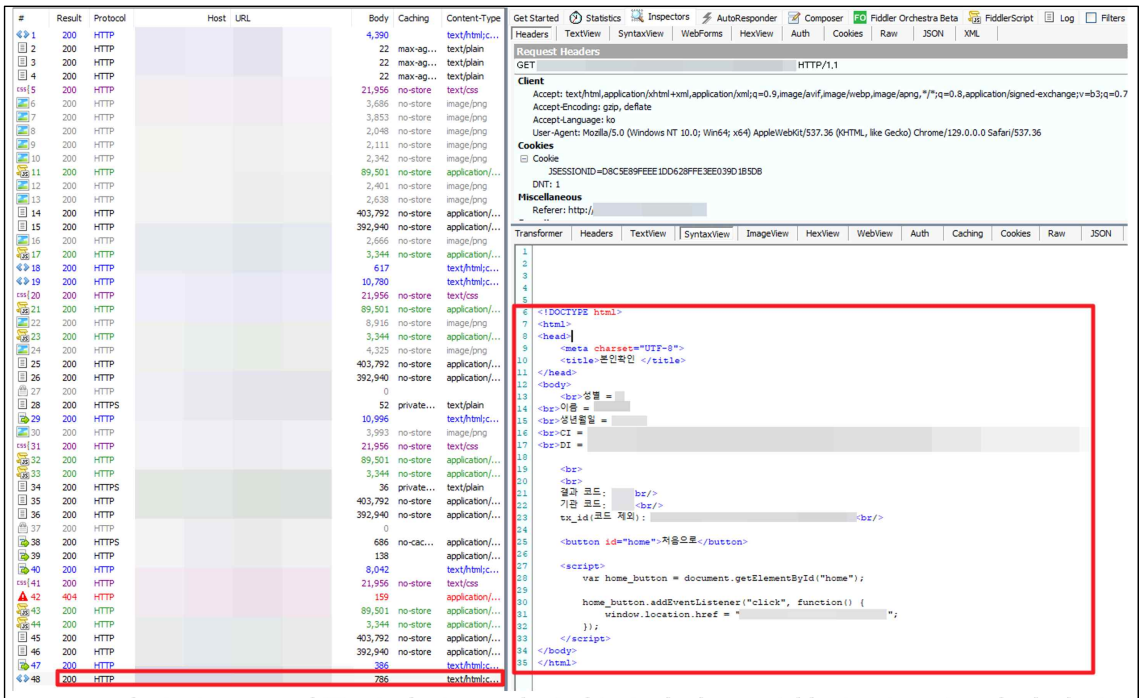
○ TLS 1.1 이하의 알고리즘은 POODLE 및 BEAST와 같은 여러 취약점에 대하여 취약한 버전이므로 안전하지 않은 알고리즘으로 Chrome, IE, Edge 등 주요 브라우저에서는 2020년부터 지원 중단됨. 주요정보통신기반시설 기술적 취약점 분석 평가 가이드에 따르면 암호화 전송 시 프로토콜 설계의 결함이 있는 SSLv2, SSLv3, TLSv1.0, TLSv1.1은 비활성화 필수 TLS 1.2 이상 사용을 명시

※ 개인정보의 안전성 확보조치 기준 제7조제4항 및 신용정보법 시행령 제18조의6 제7항제4호에 따라 안전한 통신 프로토콜 사용

○ 웹상의 데이터 통신은 대부분 텍스트 기반으로 이루어지기 때문에 서버간에 암호화 프로세스를 구현하지 않으면 회원가입 시 이용자의 중요정보가 간단한 도청(Sniffing)을 통해 탈취 및 도용 가능

※ 본 이미지들은 샘플페이지로 실제 취약점이 존재하지 않음을 알립니다.





※ 본 이미지들은 샘플페이지로 실제 취약점이 존재하지 않음을 알립니다.

조치방안

○ 웹상에서의 전송 정보를 제한하여 불필요한 비밀번호, 주민등록번호, 계좌정보와 같은 중요정보의 전송을 최소화하여야 하며, 중요정보에 대해서는 반드시 SSL 등의 암호화 통신을 사용하여 도청으로부터의 위험을 제거

○ 암호화 전송 시 프로토콜 설계의 결함이 있는 SSLv2, SSLv3, TLSv1.0, TLSv1.1은 비활성화 필수, TLSv1.2 이상 사용

○ 안전한 본인확인서비스 제공을 위해, 보안성이 검증된 안전한 SSL 프로토콜(TLS 1.2 이상)을 사용하여 통신