EYEON-X · ASSESSMENT REPORT

침투 테스트 종합 보고서 — 샘플 고객사

2026-10-12 10:50:40

CONFIDENTIAL

리포트 생성	2026-10-12 10:50:40

종합 평가 (총평)

▸ **전체 위험도:** 심각(Critical). 샘플 고객사 대상 점검에서 총 67건을 확인했으며, 이 중 Critical 30건·High 37건, 실제 악용으로 침투에 성공한 항목이 56건입니다(검증 완료 67건).

▸ **주요 취약점:** 대표적으로 민감 정보 노출(CWE-200) 21건, 중요 기능 인증 누락(CWE-306) 6건, 스푸핑에 의한 인증 우회(CWE-290) 6건, 하드코딩된 자격증명(CWE-798) 5건, 부적절한 접근 통제(CWE-284) 4건, SQL 인젝션(CWE-89) 4건 유형이 확인되었습니다. 자격증명 노출·인젝션·접근통제 미흡 등 공격 표면 전반에 걸쳐 위험이 분포합니다.

▸ **침투 시나리오:** 1) 자격증명 노출/하드코딩 → MinIO 레지스트리 [제품A 콘솔] 소스에서 DB자격(O 2) SQL Injection → [제품A 통합관리자] ajax4 무인증 관리자 계정 열거 3) IDOR/접근제어 → XFF 우회로 운영 관리자 가입폼 조직도·직급·내선 — 정찰에서 시작해 초기 침투·실행을 거쳐 수평 이동, 최종 임팩트(데이터 열람·계정 장악 등)까지 이어졌습니다.

▸ **비즈니스·규제 영향:** 실증된 침투는 개인정보·인증정보 유출과 서비스 무단 조작으로 이어질 수 있어, 개인정보보호법 등 규제 위반과 대외 신뢰도 손상 리스크가 있습니다.

▸ **긴급 조치:** Critical 취약점을 최우선으로 즉시 조치하고, 노출된 시크릿·자격증명은 즉시 폐기·재발급하십시오. 실증된 침투 경로의 진입점을 우선 차단한 뒤 수정 후 재점검(retest)으로 실제 해결 여부를 확인하십시오.

▸ **권고 보안 체계:** 인증 누락 — 민감 기능 인증 필수화 / 하드코딩된 자격증명 — 시크릿 매니저(Vault)로 이관, 노출 크리덴셜 즉시 폐기·재발급 / SQL 인젝션 — 파라미터라이즈드 쿼리/ORM 표준화 및 WAF 도입. 아울러 정기 취약점 스캔·의존성(SCA) 점검과 최소권한 접근통제를 상시 운영 프로세스에 포함하십시오.

전체 이벤트	67	침투	56
모든 발견 사항		악용 성공 · 침투 확인	

요약

심각 (Critical)	67	30	37	56
종합 위험등급	총 발견	Critical	High	🎯 침투(실제 악용)

▶ 작업 내용 (수행 이력)

+ 펼치기

🎯 침투(실제 악용 확인) 판정 기준

아래 중 하나가 확인된 경우에만 🎯 실제 악용 확인으로 표기합니다. 취약점이 존재하거나 주입 가능하다는 것만으로는 인정하지 않습니다.

- 실제 명령 실행 결과 확인 — id/whoami 출력, root 계정 라인, NT AUTHORITY 등 OS 반환값
- 대역외(OOB/OAST) 콜백 실제 수신 — 대상 서버가 외부로 실제 요청을 보낸 것이 관측됨
- 실제 파일 내용·DB 데이터 확보 흔적 — win.ini, information_schema, UNION SELECT 등
- 자산(계정·자격증명·세션·쿠키·토큰·DB·웹쉘·관리자 권한 등)을 실제로 확보·탈취·유출·장악 (완료형만 — "가능하다"류 잠재성 표현은 제외)
- 개인정보 실제 값(전화·이메일·주민등록·카드번호)을 추출
- 웹쉘 등 악성 파일 업로드 3단 실증 — ① 저장 경로 확인(응답에 저장된 파일 URL/경로 반환) · ② 접근 가능(그 URL로 GET 200 회수) · ③ 실행 확인(회수 응답에서 코드 평가 결과·id/whoami·uname 등 OS 시그니처). 3단 모두 충족될 때만 업로드 취약점 자체도 침투로 판정.
- XSS 실행 실증 + 세션 탈취 가능 — ① XSS(CWE-79)의 스크립트가 실제 실행됨(응답에 raw 반사 · alert / [MASKED_PW] 발화 · OAST 콜백 수신) · ② 세션 탈취 가능 조건이 함께 확인됨(세션 쿠키 HttpOnly 미설정으로 document.cookie 접근 가능 · exfil 채널(fetch/XHR/이미지 픽셀·OAST)로 쿠키 외부 전송 실증 · 실제 유출된 세션 값 확인 중 하나). 두 요건 모두 충족될 때 침투로 판정.

boolean / [MASKED_PW] 블라인드 SQLi의 응답 차이처럼 "주입 가능함"만 증명된 경우는 실제 악용 확인으로 인정하지 않습니다(취약점 확증(confirmed)과는 별개 단계).

심각도별 요약

심각도	건수
Critical	30
High	37
Medium	0
Low	0

심각도	건수
Info	0

▼ 발견사항 목차

– 접기

NO.	심각도	명칭	경로	설명
1	CRITICAL 🎯	[제품A 통합관리자] 가입 API(/main/ajax1) 무인증 관리자 계정 신청·생성 실증	https://admin.example.com/main/ajax1	공격자가 IP 제한을 위장 우회해 관리자 가입 API를 호출, "정상적으로 신청되었습니다" 응답과 함께 실제로 관리자 계정을 생성했습니다.
2	CRITICAL 🎯	SQLi(DBA)로 수백개 고객사 DB 평문 자격증명(계정·비번·공인IP·DBMS) 대량 유출 — root 포함 (CWE-798)	https://cloud-staging.example.com/member/login/auth	공격자가 로그인 SQLi로 SMS 게이트웨이 DB를 덤프해, 수백 개 고객사 데이터베이스의 접속 계정·평문 비밀번호·공인 IP를 한 번에 확보했습니다. root 계정까지 ...
3	CRITICAL 🎯	MinIO 레지스트리 [제품A 콘솔] 소스에서 DB자격([redacted]=공인 IP/root)·복호화키·결제 가맹점키 유출 (CWE-798)	https://s3-console.example.com/api/v1/buckets/harbor-bucket/objects/download	공격자가 MinIO 레지스트리에서 [제품A 통합관리자] 소스 이미지를 내려받아 앱 설정 파일을 확보, DB 접속 자격과 암호화 키, 결제 가맹점 키를 획득했습니다. 특히 모니터링...
4	CRITICAL 🎯	SQLi→LFI로 DB설정(server.cnf) 읽기 — Galera SST 자격증명 평문·클러스터 토폴로지·관리계정 유출 (CWE-260)	https://cloud-staging.example.com/member/login/auth	공격자가 로그인 SQLi로 DB 서버 설정 파일을 읽어, 데이터베이스 복제(Galera) 자격증명과 클러스터 내부 IP·관리자 계정명을 평문으로 확보했습니다. 내부 DB ...
5	CRITICAL 🎯	SQLi(DBA+FILE)로 DB 서버 임의 파일 읽기 — LOAD_FILE('/etc/passwd') 원문 유출 (SQLi→LFI, CWE-22)	https://cloud-staging.example.com/member/login/auth	공격자가 로그인 폼의 아이디 파라미터에 SQL 구문을 넣어, 데이터베이스 최고 권한으로 서버의 시스템 파일(/etc/passwd)을 그대로 읽어냈습니다. 같은 방법으로 설...
6	CRITICAL 🎯	MinIO 멀티테넌트 격리 실패 — 고객사([고객사-은행] 등) 버킷 파일 실제 다운로드 (교차 테넌트 데이터 유출, CWE-284)	https://s3-console.example.com/api/v1/buckets/[redacted]-bucket/objects/download	공격자가 공개 MinIO 콘솔에 루트로 로그인해, 서로 다른 고객사([고객사-은행] 등)의 개인정보 처리방침 문서와 이미지·백업을 임의로 내려받았습니다. 멀티테넌트 격리가 깨...
7	CRITICAL 🎯	SQLi(DBA)로 관리자 자격·OTP/2차 인증 우회 플래그·평문 비번찾기 답변 유출 — OTP예외 관리자 계정탈취 경로 (CWE-200)	https://cloud-staging.example.com/member/login/auth	공격자가 로그인 SQLi로 관리자 계정의 비밀번호 해시·비번찾기 평문 답변, 그리고 "OTP·2차인증 예외" 플래그까지 빼냈습니다. OTP 예외로 표시된 관리자([redacted]...
8	CRITICAL 🎯	MinIO 백업 버킷에서 고객사 Laravel 앱 DB 전체 덤프 유출 — bcrypt 사용	https://s3-console.example.com/api/v1/bu	공격자가 MinIO 백업 버킷에서 고객사 사이트 DB 백업(partner.gz)을 내려받아, 사용자

NO.	심각도	명칭	경로	설명
		자 해시·세션·API 토큰 포함 (CWE-200)	ckets/backup/objects/download	비밀번호 해시·세션·API 토큰이 담긴 DB 전체를 확보했습니다. 이로...
9	CRITICAL 🎯	MinIO 콘솔로 PBX 통화녹음(WAV)·일일 DB백업(GZIP) 실다운로드 — 음성PII·백업 데이터 유출 (CWE-200)	https://s3-console.example.com/api/v1/buckets/pbx/objects/download	공격자가 공개 MinIO 관리 콘솔에 유출된 루트 계정으로 로그인해, PBX 통화 녹음(WAV)과 일일 DB/사이트 백업(GZIP)을 실제로 내려받았습니다. 음성 개인정보...
10	CRITICAL 🎯	MinIO Console 공개 노출 + 루트 자격증명 로그인 성공 — [redacted] 버킷(TB급 프로덕션·백업) 전면 장악 (CWE-284)	https://s3-console.example.com/api/v1/login	공격자가 공개된 MinIO 관리 콘솔(s3-console.example.com)에 유출된 루트 계정으로 로그인해, [redacted] 버킷(백업 [redacted]·프로덕션 지도데이터 9...
11	CRITICAL 🎯	SQLi로 [redacted] 모니터링 DB 덤프 — 다수 고객사 서버 인프라 토폴로지(IP·역할·OS) 대량 유출	https://cloud-staging.example.com/member/login/auth	공격자가 로그인 SQL 인젝션 한 번으로 모니터링 시스템 DB를 덤프해, 여러 고객사의 서버 IP·역할(WEB/DB/CDN/SMS 등)·운영체제가 담긴 인프라 지도를 통째...
12	CRITICAL 🎯	SQLi로 객체스토리지 사용자 평문 비밀번호·토큰 유출 ([MASKED_PW_1] 등)	https://cloud-staging.example.com/member/login/auth	공격자가 로그인 SQL 인젝션으로 객체스토리지 계정 비밀번호([MASKED_PW_1] 등)와 아직 만료되지 않은 접근 토큰을 평문 그대로 빼냈습니다.
13	CRITICAL 🎯	SQL Injection (sqlmap 확인) — MySQL (MariaDB fork)	https://cloud-staging.example.com/member/login/auth	공격자가 로그인 아이디 칸에 SQL 구문을 넣어, 인증 없이 회사의 세금계산서 데이터베이스(사업자등록번호·거래처 상호·주소·담당자·공급가액/세액)를 통째로 내려받았습니다....
14	CRITICAL 🎯	[제품A 통합관리자] X-Forwarded-For 우회로 무인증 관리자 계정 생성·인증 통과 (CWE-290)	https://admin.example.com/main/ajax1	공격자가 관리자 IP로 위장하는 헤더를 붙여 회사 관리자 시스템에 자기 계정을 만들고, 그 계정으로 관리자 인증까지 통과했습니다.
15	CRITICAL 🎯	유출 [redacted] API 키로 [제품A SSO] 위임 인증 무인증 접근 — 계정 열거·잠금(DoS) 실증 (CWE-306)	https://admin.example.com/api/admin/v1/sso	공격자가 SQL로 빼낸 보안플랫폼의 인증 키를 써서, 회사 관리자 시스템의 통합 로그인(SSO) 인증 서비스에 로그인 없이 접근해 계정 상태를 알아내고 관리자 계정을 잠가...
16	CRITICAL 🎯	SQLi로 IP 화이트리스트 [redacted]·허용 휴대폰 [redacted] 추출 — XFF/OTP 우회 정밀 위장 가능 (CWE-200)	https://cloud-staging.example.com/member/login/auth	공격자가 관리자용 IP 허용 목록과 휴대폰 허용 목록을 SQL로 빼내, 회사 내부 네트워크로 위장하거나 OTP 발송 대상을 사칭할 수 있게 됐습니다.
17	CRITICAL 🎯	관리자 비밀번호 찾기 답변 평문 저장 — SQLi로 추출돼 계정탈취 가능 (CWE-256)	https://cloud-staging.example.com/member/login/auth	공격자가 로그인 창의 SQL 구문으로 관리자 계정의 '비밀번호 찾기 답변'을 평문으로 빼내, 그 답변으

NO.	심각도	명칭	경로	설명
				로 비밀번호를 재설정해 관리자 계정을 가로챌 수 있게 됐습니다.
18	CRITICAL 🎯	개발 클라우드/패널 로그인 SQLi — DB 사용자·스키마·소스경로 유출 (CWE-89)	`https://cloud-staging.example.com/member/login/auth`	공격자가 로그인 창의 SQL 구문으로 관리자 콘솔의 API 키 25개를 평문으로 빼내, 방화벽·메시지 발송·관리자 정보 API에 접근할 수 있게 됐습니다.
19	CRITICAL 🎯	통합회원 무인증 임시비밀번호 발급 IDOR — 임의 회원(관리자 포함) 비밀번호 리셋 (CWE-639)	`https://mypage.example.com/member/sleep_lock/imsi_pass_create_proc2`	공격자가 로그인 없이 회원 번호만 바꿔 넣은 주소를 열어, 다른 회원의 비밀번호를 강제로 임시 비밀번호로 바꿔버렸습니다.
20	CRITICAL 🎯	MinIO 루트 자격증명으로 오브젝트 스토리지 전량 장악 — 고객사 운영 DB백업(PII·결제시크릿·관리자 해시) 실제 유출 (CWE-284)	`https://api.example.com`	공격자가 유출된 스토리지 관리자 키를 그대로 써서, 사업자가 운영하는 오브젝트 스토리지에서 고객사 운영 데이터베이스 백업 파일을 통째로 내려받았습니다. 그 파일 안에는 대...
21	CRITICAL 🎯	[SMS_SVC] SMS 서비스 회원 DB 덤프 노출 → 평문 ID·bcrypt 해시·주민번호 암호값·사업자/은행정보 유출 (impactProven)	`https://api.example.com/[CUST_E]/*-[SMS_SVC].gz`	공격자가 스토리지에서 고객사의 문자서비스 회원 DB를 내려받아 로그인 아이디·비밀번호 해시·주민번호 암호값·사업자·은행계좌까지 통째로 빼냈다.
22	CRITICAL 🎯	MMS 게이트웨이 일별 발송 로그 DB 노출 → 수신자 전화번호·메시지 본문 대량 유출 (impactProven)	`https://api.example.com/gateway/[redacted]-MM_MSG_*.gz`	공격자가 스토리지에서 문자발송 시스템의 일별 로그 DB를 내려받아 수신자 전화번호와 메시지 본문을 수만 건 단위로 빼냈다.
23	CRITICAL 🎯	MinIO 루트 크리덴셜 → 고객 SMS/MMS DB(2GB)·Laravel biz DB·Docker 레지스트리·암호화폐 프로젝트 백업 일괄 열람 (impactProven)	`https://api.example.com`	공격자가 MinIO 루트 비밀번호 하나로 스토리지에 저장된 고객사의 SMS/MMS 발송 데이터베이스(2GB, 전화번호·메시지 본문)와 웹앱 DB, 도커 이미지, 암호화폐 ...
24	CRITICAL 🎯	MinIO 루트 자격증명 유출 → [redacted] 버킷·DB백업·SMS/MMS 개인정보 실제 열람 (impactProven)	`https://api.example.com`	공격자가 MinIO 루트 계정을 무인증으로 탈취한 뒤, 저장소 [redacted] 개 버킷을 열람하고 그중 DB 백업·SMS/MMS 발송 데이터를 실제로 내려받아 고객 전화번호와 메...
25	CRITICAL 🎯	MinIO CVE-2023-28432 루트 자격증명 무인증 유출 → 객체스토리지 전체 장악	`https://api.example.com/minio/bootstrap/v1/verify`	공격자가 인증 없이 MinIO 부트스트랩 API를 호출해 서버 환경변수(오브젝트 스토리지 루트 계정·비밀번호)를 통째로 탈취, [redacted] 버킷(DB 백업·통화녹음 등)을 열람...
26	HIGH 🎯	[제품A 통합관리자] ajax4 무인증 관리자 계정 열거 — admin·[redacted]·dev·example + 로그인 방식 노출	`https://admin.example.com/main/ajax4`	공격자가 관리자 계정 문의 API와 SQL 주입을 이용해 관리자 계정 150개의 아이디와 일부 실명·이메일까지 빼냈습니다.

NO.	심각도	명칭	경로	설명
27	HIGH 🎯	[제품A 통합관리자] 관리자 비밀번호 무솔트 SHA-256 저장 — 해시 크랙으로 평문 복원 실증	https://cloud-staging.example.com (admin_masked.admin_masked.[redacted])	관리자 비밀번호가 솔트 없이 SHA-256 해시로만 저장되어, 공격자가 해시를 빼내면 약한 비밀번호는 금방 평문으로 복원할 수 있었습니다.
28	HIGH 🎯	[제품A 통합관리자] IP 제한이 X-Forwarded-For 로 우회됨 — 내부 가입 API 외부 동작	https://admin.example.com/main/ajax1	공격자가 요청 헤더에 출처를 "127.0.0.1"로 적어 보내, "내부에서만 허용"이라는 IP 제한을 우회하고 관리자 가입 기능에 접근했습니다.
29	HIGH 🎯	ERP([redacted]/[redacted]) 게이트웨이 서명보호 우회 — 무인증 get_token으로 내부설정·DB명·테넌트·adminSeq 유출 + SSO 세션생성 엔드포인트 노출	https://erp.example.com/gw/gw050B01	공격자가 로그인 없이 ERP의 토큰 발급 API(get_token)를 호출해 서명 재료를 받아낸 뒤, 이를 계산해 내부설정 API를 호출했습니다. 그 결과 관리자 식별자·테...
30	HIGH 🎯	MinIO harbor-bucket Docker레지스트리로 [제품A 통합관리자] 소스이미지 유출 — PHP 5.3.29(EOL)·앱소스 [redacted] 노출 (CWE-540)	https://s3-console.example.com/api/v1/buckets/harbor-bucket/objects/download	공격자가 MinIO의 Docker 레지스트리에서 [제품A 통합관리자] 소스 이미지를 내려받아, 콘솔의 소스코드와 단종된 PHP 5.3.29 기반을 확인했습니다. 화이트박스 공격과...
31	HIGH 🎯	MinIO [CUST_C]([redacted] 블록체인) 소스코드·systemd·RPC노드(XXX.XXX.XXX.XXX) 유출 (CWE-540)	https://s3-console.example.com/api/v1/buckets/[CUST_C]-backup/objects/download	공격자가 노출된 스토리지 계정으로 블록체인 봇 백업 버킷에 접속해, 운영 소스코드와 서버 배치 스크립트, 그리고 실제 블록체인 노드 접속 주소(XXX.XXX.XXX.XXX)...
32	HIGH 🎯	MinIO bleve 검색인덱스에서 실제 SMS 메시지 원문·수신번호 대량 유출 (인증문자 포함, CWE-200)	https://s3-console.example.com/api/v1/buckets/bleve/objects/download	공격자가 MinIO bleve 버킷의 SMS 검색 인덱스 백업을 내려받아, 실제 발송 문자메시지의 수신번호와 본문(예약·임시비밀번호 등)을 대량 확보했습니다.
33	HIGH 🎯	MinIO dump-storage2 버킷 SMS 게이트웨이 super-admin 자격·클라이언트 비밀번호·라우팅 설정 유출 (CWE-798)	https://s3-console.example.com/api/v1/buckets/dump-storage2/objects/download	공격자가 MinIO dump-storage2 버킷에서 SMS 게이트웨이 자격 덤프를 내려받아, 최고관리자 계정의 비밀번호 해시와 클라이언트 비밀번호·라우팅·화이트IP 설정...
34	HIGH 🎯	MinIO [CUST_E]-[CUST_D] 버킷([CUST_D] 테넌트) 평문 Telegram 봇 토큰·발신번호 유출 (CWE-798)	https://s3-console.example.com/api/v1/buckets/[CUST_E]-[CUST_D]/objects/download	공격자가 노출된 스토리지 관리자 계정으로 메신저 백업 버킷에 접속해, 그 안의 평문 Telegram 봇 토큰을 그대로 꺼냈습니다. 이 토큰 하나로 해당 고객사의 텔레그램 ...
35	HIGH 🎯	MinIO [CUST_E] 버킷 메시징 플랫폼 DB 덤프에서 평문 Telegram 봇 토큰·사업자번호·계좌번호 유출 (CWE-798)	https://s3-console.example.com/api/v1/buckets/[CUST_E]/objects/download	공격자가 MinIO [CUST_E] 버킷에서 메시징 플랫폼 DB 덤프를 내려받아, 평문 Telegram 봇 토큰과 사업자등록번호·계좌번호·연락처를 확보했습니다. 봇 탈취와 사...

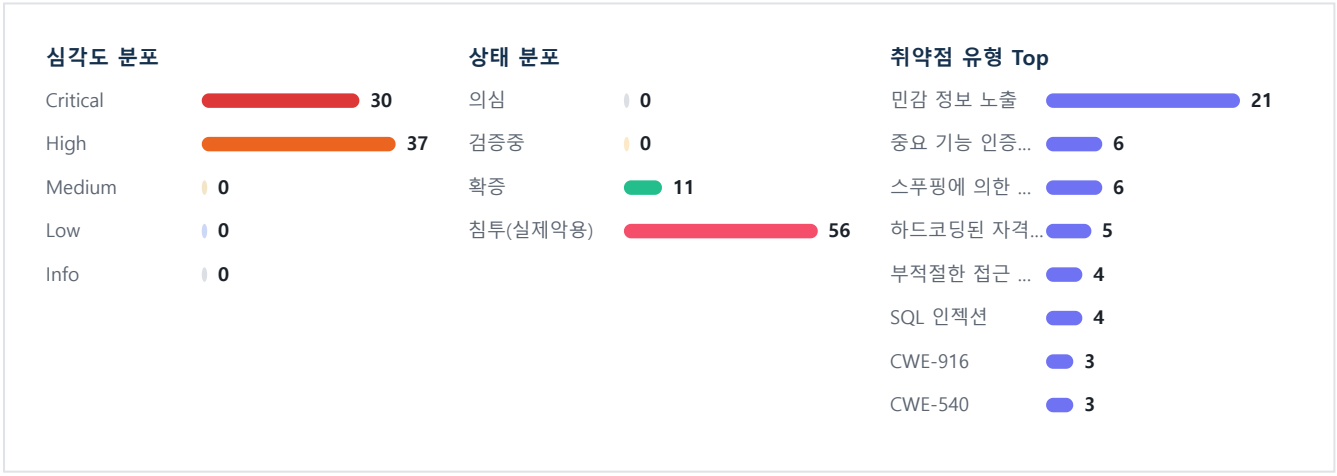
NO.	심각도	명칭	경로	설명
36	HIGH 🎯	MinIO dump-storage 버킷 SMS 게이트웨이 사업DB 덤프 실제 다운로드 — 실사용자 bcrypt 해시·청구·발신번호 유출 (CWE-200)	https://s3-console.example.com/api/v1/buckets/dump-storage/objects/download	공격자가 MinIO dump-storage 버킷의 SMS 게이트웨이 사업 DB 덤프를 내려받아, 실제 사용자의 비밀번호 해시와 청구·발신번호 데이터를 확보했습니다.
37	HIGH 🎯	MinIO 관리 API로 [redacted] 객체 멀티테넌트 인벤토리 실제 추출 (CWE-200)	https://s3-console.example.com/api/v1/buckets	공격자가 공개 MinIO 콘솔에 루트로 로그인해, [redacted] 객체에 달하는 다수 고객사의 스토리지 전체 인벤토리(버킷·용량·고객사명)를 한 번에 수집했습니다.
38	HIGH 🎯	MinIO gateway 버킷에 SMS 게이트웨이 메시지 DB 덤프([redacted]건) 노출 — 발신/수신번호·메시지 구조 유출 (CWE-200)	https://s3-console.example.com/api/v1/buckets/gateway/objects/download	공격자가 MinIO gateway 버킷의 SMS 게이트웨이 메시지 DB 덤프([redacted]개 일일분)를 내려받아, 고객 SMS 발송 이력(수신자 번호·메시지 본문) 구조를 확...
39	HIGH 🎯	MinIO 콘솔 admin API로 멀티테넌트 고객사 그룹·서비스계정 키·정책 노출 (CWE-200)	https://s3-console.example.com/api/v1/users	공격자가 공개 MinIO 콘솔에 루트 계정으로 로그인해, 이 스토리지에 담긴 다수 고객사([redacted] 테넌트 명단·서비스계정 키·버킷 구조를 한 번에 수집했...
40	HIGH 🎯	SQL Injection (sqlmap 확인) — MySQL unknown (MariaDB fork)	https://cloud-staging.example.com/member/login/auth	sqlmap이 https://cloud-staging.example.com/member/login에서 SQL 인젝션을 확인했습니다. DBMS: MySQL unknow...
41	HIGH 🎯	약한 비밀번호 해시 크랙 — 1/6건 복원	(오프라인 해시)	획득한 해시 2건 중 1건이 약한-비밀번호 사전 대입으로 복원되었습니다. 솔트 없는/약한 해시(MD5·SHA1 등)와 약한 비밀번호 정책의 조합으로, 유출 시 즉시 계정 ...
42	HIGH 🎯	[제품A 통합관리자] IP 제한이 X-Forwarded-For 로 우회됨 — 내부 가입 API 외부 동작 (CWE-290)	https://admin.example.com/main/ajax1	공격자가 요청 헤더에 내부 화이트리스트 IP를 위조해, 외부에서 차단돼야 할 내부 관리자 가입·비밀번호 검증 API를 그대로 호출했습니다. 이를 통해 비밀번호 정책과 조직...
43	HIGH 🎯	easycloud 운영 로그인 SQLi 지점 확인 — 따옴표로 500/200 응답차이 (CWE-89)	https://cloud.example.com/member/login/auth	공격자가 운영 클라우드 포털 로그인 아이디에 따옴표 하나를 넣자 서버가 내부 오류(500)를 냈고, 이를 주석으로 닫자 정상 응답으로 바뀌어 SQL 주입 지점이 확인됐습니...
44	HIGH 🎯	XFF 우회로 운영 관리자 가입폼 조직도·직급·내선 디렉토리 노출 (CWE-200)	https://admin.example.com/?act=join	공격자가 '사내 IP로 위장'하는 헤더만 붙여, 관리자 가입 화면의 조직도·직급·내선 체계를 통째로 열람했습니다.

NO.	심각도	명칭	경로	설명
45	HIGH 🎯	파일서버 무인증 업로드 파일 삭제 IDOR — [redacted]만으로 타인 파일 삭제 (CWE-639)	https://file.[redacted]ple.com/common/upfile3/ajax10	공격자가 파일 서버의 업로드 목록에서 다른 사람이 올린 개인정보·사업자인증서 파일을 로그인 없이 내려받고, 파일 번호만으로 삭제도 할 수 있었습니다.
46	HIGH 🎯	ownCloud 10.0.4 updater.secret 미설정 — 업데이터 엔드포인트 무인증 공개 (CWE-1188)	https://data.example.com/updater/index.php	공격자가 오래된 파일공유 시스템의 업데이트 관리 화면이 잠금장치 없이 열려 있는 것을 확인했습니다.
47	HIGH 🎯	파일서버 무인증 업로드 파일 목록 덤프 — 파일명·SHA1 경로·공개 URL 221건 노출 (CWE-639)	https://file.[redacted]ple.com/common/upfile/ajax2	공격자가 파일 서버의 업로드 목록을 로그인 없이 통째로 조회해, 저장된 모든 첨부 파일의 이름과 다운로드 주소를 알아냈습니다.
48	HIGH 🎯	ERP [redacted] 무인증 내부 구성·DB 스키마명·그룹 정체 노출 (CWE-200)	https://erp.example.com	공격자가 로그인 없이 ERP의 숨은 설정 화면을 열어, 내부 데이터베이스 이름·시스템 구성·운영 그룹 정보를 통째로 봤습니다.
49	HIGH 🎯	ERP [redacted] 무인증 토큰 발급기 노출 → SSO 세션 생성기 인증 게이트 우회 (CWE-306)	https://erp.example.com	공격자가 ERP 로그인 뒤에 숨어 있는 '무인증 토큰 발급기'가 인터넷에 그대로 열려 있는 것을 발견하고, 그것으로 로그인 없이 서명 토큰을 만들어 SSO 세션 생성 화면...
50	HIGH 🎯	내부 보안플랫폼(ISP) 인터넷 노출 + 로그인 계정 열거 — Harbor 소스 유출과 체이닝 (CWE-204)	https://isp.example.com	공격자가 공개된 보안 점검 플랫폼 로그인 창에 아이디만 바꿔 넣어, 어떤 관리자 계정이 실제로 존재하는지를 서버 응답 문구 차이로 알아냈습니다.
51	HIGH 🎯	운영 [제품A 통합관리자] (admin.example.com) 관리자 계정 열거 — admin·[redacted] 실증 (WAF POST 우회)	https://admin.example.com/main/ajax4	공격자가 운영 관리 콘솔에 계정명 후보를 넣어보는 것만으로 실제 존재하는 관리자 계정(admin, [redacted])을 가려냈다.
52	HIGH 🎯	[제품A 통합관리자] 무인증 OTP 문자 발송(CWE-799) — id만으로 임의 계정에 SMS 인증코드 발송	https://[redacted].dev-sample.com/main/ajax5	공격자가 아이디만 넣어 관리자 계정에 인증 문자를 마음대로 보내고, 어떤 계정에 휴대폰이 등록됐는지도 알아냈습니다.
53	HIGH 🎯	Harbor 이미지에서 내부 보안플랫폼(ISP) 전체 소스 유출 — SSO URL·기본 HMAC 시크릿 하드코딩	https://api.example.com/harbor-bucket/docker/registry/v2/blobs/sha256/08/[MASKED_SHA_HASH]/data	공격자가 스토리지의 도커 이미지에서 내부 보안 점검 플랫폼의 소스코드를 통째로 꺼내, SSO 주소와 기본 비밀키를 확보했다.
54	HIGH 🎯	crossdomain.xml이 내부 개발·테스트 서브도메인 661개(개발자 계정명 포함) 노출	https://www.example.com/crossdomain.xml	회사 웹사이트의 옛 Flash 설정 파일이 내부 개발자·테스트 서버 661개 목록을 누구에게나 공개했다.
55	HIGH 🎯	[SMS_SVC] 회원 bcrypt 해시 크랙 성공 → 평문 자격증명 획득	https://api.example.com/[CUST_E]/2025-02	공격자가 노출된 오브젝트 스토리지에서 고객사 문자 발송 서비스

NO.	심각도	명칭	경로	설명
		([redacted])	-09-[redacted]-[SMS_SVC].gz	DB 백업을 내려받은 뒤, 아이디 뒤에 느낌표만 붙인 약한 비밀번호로 회원 계정 2개의 실제 비밀번호를 풀어...
56	HIGH 🎯	Laravel biz DB 백업 노출 → 관리자 계정 bcrypt 해시·개인정보·세션 토큰 유출 (impactProven)	https://api.example.com/dump-storage/2024-05-31-[redacted]-biz.gz	공격자가 스토리지에서 웹앱 DB 백업을 내려받아 관리자 계정의 비밀번호 해시·이메일·전화번호와 세션 토큰을 확보했다.
57	CRITICAL	[제품A 통합관리자] 인증 우회로 관리 전용 페이지 무단 접근(세션 탈취) — 비인증 302 vs 인증 200 실증	https://admin.example.com/admin/total_member	공격자가 DB에서 관리자 비밀번호([MASKED_PW_4])를 복원하고 IP 위장으로 2차 인증을 우회해 관리자로 로그인, 비인증 시엔 302(거부)이던 관리 페이지가 인증 후 2...
58	CRITICAL	www.dev-sample.com [제품A 호스팅] 관리자 X-Forwarded-For 우회로 IP 접근제어 무력화 + ajax4 무인증 관리자 계정 정보 열거	https://www.dev-sample.com/main/ajax1	공격자가 요청 출처를 "127.0.0.1(로컬)"로 위장해 IP 제한을 우회하고, 관리자 가입 기능으로 무단 계정을 만들었습니다. 서버는 "정상적으로 신청되었습니다"로 응...
59	CRITICAL	www.dev-sample.com [제품A 호스팅] 관리자 X-Forwarded-For 우회로 IP 접근제어 무력화 + ajax4 무인증 관리자 계정 정보 열거	https://www.dev-sample.com/main/ajax1	공격자가 요청 출처를 "127.0.0.1(로컬)"로 위장해 IP 제한을 우회하고, 관리자 가입 기능에 접근했습니다. 동시에 관리자 계정의 존재와 로그인 방식까지 로그인 없...
60	CRITICAL	[제품A 통합관리자] 가입 API(/main/ajax1) 무인증 관리자 계정 신청·생성 실증 (CWE-306)	https://admin.example.com/main/ajax1	공격자가 로그인 없이 관리자 가입 API를 직접 호출해 임의의 관리자 계정을 신청·생성했습니다. 이로써 인증 없이 관리 시스템에 계정을 만들 수 있습니다(주민번호·연락처 ...
61	CRITICAL	[제품A 통합관리자] OTP 2차 인증 우회 — sso=Y 클라이언트 파라미터로 OTP 게이트 건너뜀	https://admin.example.com/?act=login	공격자가 DB에서 관리자 비밀번호 해시를 빼내 약한 비밀번호([MASKED_PW_4])를 복원하고, 출처를 내부(127.0.0.1)로 위장해 2차 인증을 우회한 뒤, [제품A 통합관리자]...
62	HIGH	[제품A 통합관리자] ajax4 무인증 관리자 계정 열거 — admin·[redacted]·dev·example + 로그인 방식 노출 (CWE-200)	https://admin.example.com/main/ajax4	공격자가 로그인 없이 계정 검증 API를 호출해 관리자 계정 ID 목록(admin·[redacted]·dev·example)과 로그인 방식을 수집했습니다. 비밀번호 공격의 표적이 노...
63	HIGH	[제품A 통합관리자] IP 제한이 X-Forwarded-For 로 우회됨 — 내부 가입 API 외부 동작 (CWE-290)	https://admin.example.com/main/ajax1	공격자가 요청 헤더에 내부 화이트리스트 IP를 위조해, 외부에서 차단([redacted]돼야 할 내부 관리자 API가 비밀번호 정책 검증(코드 [redacted]까지 도달하도록 만들었...

NO.	심각도	명칭	경로	설명
64	HIGH	**[제품A 통합관리자] ajax4가 비밀번호 검증 없이 로그인 방식(local/OTP) 노출**	`https://admin.example.com/main/ajax4`	공격자가 관리자 로그인 API에 틀린 비밀번호를 넣어도 서버가 '[제품A]·example·dev·mail 계정은 OTP 없이 비밀번호만으로 로그인 된다'는 정보를 그대로 돌려줍니다.
65	HIGH	**업로드 필터 우회 정황 — 위험 확장자 55개 변형 수락**	`https://file.[redacted]ple.com/common/upfile3/ajax3`	공격자가 이미지 파일 안에 PHP 코드를 숨겨 업로드했지만, 서버가 .gif 형식으로만 저장하고 실행하지 않아 코드는 동작하지 않았습니다.
66	HIGH	**ownCloud 10.0.4(2017, EOL) + PHP 7.0.33 노출 — 버전·CVE 12건 공격면**	`https://data.example.com/status.php`	공유 서버가 무인증 응답으로 정확한 구버전·기술스택을 알려 줘, 공격자가 이 버전에 맞는 취약점을 골라 공격할 수 있게 된다.
67	HIGH	**노출 가능 경로/파일 — /crossdomain.xml (HTTP 200)**	`https://www.example.com/crossdomain.xml`	콘텐츠 발견으로 /crossdomain.xml 가 HTTP 200로 응답합니다(text/html; charset=UTF-8, 32279B). 백업·설정·버전관리·시크릿 성...

발견사항 현황



침투 (Cyber Kill-Chain)

노드를 클릭하면 요약과 상세로 이동 버튼이 표시됩니다.

확인된 공격 경로를 진입 벡터별로 분리해 정찰(스캐닝)부터 임팩트까지 단계별 그래프로 나타냈습니다. 위 → 아래로 공격이 진행되며(같은 단계의 여러 노드는 병렬), 각 노드는 MITRE ATT&CK 단계·CWE·심각도를 표기합니다. 총 19개 경로.

노드 테두리=심각도 Critical High Medium Low Info 🎯 침투(실제 악용 확인)

출처 SRC 소스확인 PEN 모의해킹 S+P 양쪽 · **화살표 색** = 분기점(한 취약점에서 갈라지는 경로) 구분

침투 경로 1: 자격증명 노출/하드코딩 → MinIO 콘솔 admin API로 멀티테넌트 고객 · 🎯 임팩트 도달 (28단계)

🌐 대상 `s3-console.example.com` `isp.example.com` `api.example.com`

📝 경로 요약

이 경로는 **초기 침투 단계의 "MinIO CVE-2023-28432 루트 자격증명 무인증 유출 → 객체스토리지 전체 장악"** (민감 정보 노출 (CWE-200))에서 출발해 총 **28단계** (초기 침투 → 임팩트·목표달성)로 진행됩니다.

최종적으로 **"MinIO CVE-2023-28432 루트 자격증명 무인증 유출 → 객체스토리지 전체 장악"**, **"MinIO 콘솔 admin API로 멀티테넌트 고객사 그룹·서비스계정 키·정책 노출"** 외 24건에서 **실제 침투(악용)가 실증되었습니다.**

취약 지점: `https://api.example.com/minio/bootstrap/v1/verify` — **민감 정보 노출(CWE-200)**.



🌐 api.example.com · 1건

초기 침투	Pentest	🎯 MinIO CVE-2023-28432 루트 자격증명 무인증 유출 → 객체스토리지 전체 장악 → 상세 https://api.example.com/minio/bootstrap/v1/verify · 실제 자산(계정·데이터·파일 등)을 확보·유출·탈취한 것으로 확인	민감 정보 노출(CWE-2 CRITICAL

🌐 api.example.com · 8건

임팩트·목표달성	Pentest	🎯 MinIO 루트 자격증명 유출 → [redacted] 버킷·DB백업·SMS/MMS 개인정보 실제 열람 (impactProven) → 상세 https://api.example.com · 실제 자산(계정·데이터·파일 등)을 확보·유출·탈취한 것으로 확인	부적절한 접근 통제(CW CRITICAL
임팩트·목표달성	Pentest	🎯 MinIO 루트 자격증명으로 오브젝트 스토리지 전량 장악 — 고객사 운영 DB백업(PII·결제시크릿·관리자 해시) 실제 유출 (CWE-284) → 상세	부적절한 접근 통제(CW CRITICAL

		https://api.example.com · 실제 자산(계정·데이터·파일 등)을 확보·유출·탈취한 것으로 확인	
임팩트·목표달성	Source→Pentest	🎯 MinIO 루트 크리덴셜 → 고객 SMS/MMS DB(2GB)·Laravel biz DB·Docker 레지스트리·암호화폐 프로젝트 백업 일괄 열람 (impactProven) → 상세 https://api.example.com · 실제 자산(계정·데이터·파일 등)을 확보·유출·탈취한 것으로 확인	민감 정보 노출(CWE-2(CRITICAL
임팩트·목표달성	Pentest	🎯 MMS 게이트웨이 일별 발송 로그 DB 노출 → 수신자 전화번호·메시지 본문 대량 유출 (impactProven) → 상세 https://api.example.com/gateway/[redacted]-MM_MSG_*.gz · 실제 자산(계정·데이터·파일 등)을 확보·유출·탈취한 것으로 확인	민감 정보 노출(CWE-2(CRITICAL
임팩트·목표달성	Pentest	🎯 [SMS_SVC] SMS 서비스 회원 DB 덤프 노출 → 평문 ID·bcrypt 해시·주민번호 암호값·사업자/은행정보 유출 (impactProven) → 상세 https://api.example.com/[CUST_E]/*-[SMS_SVC].gz · 실제 자산(계정·데이터·파일 등)을 확보·유출·탈취한 것으로 확인	민감 정보 노출(CWE-2(CRITICAL
임팩트·목표달성	Source→Pentest	🎯 Harbor 이미지에서 내부 보안플랫폼(ISP) 전체 소스 유출 — SSO URL·기본 HMAC 시크릿 하드코딩 → 상세 https://api.example.com/harbor-bucket/docker/registry/v2/blobs/sha256/08/[MASKED_SHA_HASH]/data · 실제 자산(계정…	CWE-540 HIGH
임팩트·목표달성	Pentest	🎯 Laravel biz DB 백업 노출 → 관리자 계정 bcrypt 해시·개인정보·세션 토큰 유출 (impactProven) → 상세 https://api.example.com/dump-storage/2024-05-31 [redacted] biz.gz · 실제 자산(계정·데이터·파일 등)을 확보·유출·탈취한 것으로 확인	민감 정보 노출(CWE-2(HIGH
임팩트·목표달성	Pentest	🎯 [SMS_SVC] 회원 bcrypt 해시 크랙 성공 → 평문 자격증명 획득 ([redacted]) → 상세 https://api.example.com/[CUST_E]/2025-02-09-[redacted]-[SMS_SVC].gz · 실제 자산(계정·데이터·파일 등)을 확보·유출·탈취한 것으로 확인	CWE-916 HIGH
🌐 **s3-console.example.com** · 18건			
임팩트·목표달성	Pentest	🎯 MinIO 레지스트리 [제품A 콘솔] 소스에서 DB자격([redacted]=공인IP/root)·복호화키·결제 가맹점키 유출 (CWE-798) → 상세 https://s3-console.example.com/api/v1/buckets/harbor-bucket/objects/download · 실제 자산(계정·데이터·파일 등)을 확보·유출·탈취한 것으로 확인	하드코딩된 자격증명(CV CRITICAL
임팩트·목표달성	Pentest	🎯 MinIO 멀티테넌트 격리 실패 — 고객사([고객사-은행] 등) 버킷 파일 실제 다운로드 (교차 테넌트 데이터 유출, CWE-284) → 상세 https://s3-console.example.com/api/v1/buckets/[redacted]-bucket/objects/download · 실제 자산(계정·데이터·파일 등)을 확보·유출·탈취한 것으로 확인	부적절한 접근 통제(CW CRITICAL
임팩트·목표달성	Pentest	🎯 MinIO 백업 버킷에서 고객사 Laravel 앱 DB 전체 덤프 유출 — bcrypt 사용자 해시·세션·API 토큰 포함 (CWE-200) → 상세 https://s3-console.example.com/api/v1/buckets/backup/objects/download · 실제 자산(계정·데이터·파일 등)을 확보·유출·탈취한 것으로 확인	민감 정보 노출(CWE-2(CRITICAL
임팩트·목표달성	Pentest	🎯 MinIO 콘솔로 PBX 통화녹음(WAV)·일일 DB백업(GZIP) 실다운로드 — 음성PII·백업 데이터 유출 (CWE-200) → 상세 https://s3-console.example.com/api/v1/buckets/pbx/objects/download · 실제 자산(계정·데이터·파일 등)을 확보·유출·탈취한 것으로 확인	민감 정보 노출(CWE-2(CRITICAL
임팩트·목표달성	Pentest	🎯 MinIO Console 공개 노출 + 루트 자격증명 로그인 성공 — [redacted] 버킷(TB급 프로덕션·백업) 전면 장악 (CWE-284) → 상세 https://s3-console.example.com/api/v1/login · 실제 자산(계정·데이터·파일 등)을 확보·유출·탈취한 것으로 확인	부적절한 접근 통제(CW CRITICAL
임팩트·목표달성	Pentest	🎯 MinIO 관리 API로 [redacted] 객체 멀티테넌트 인벤토리 실제 추출 (CWE-200) → 상세 https://s3-console.example.com/api/v1/buckets · 실제 자산(계정·데이터·파일 등)을 확보·유출·탈취한 것으로 확인	민감 정보 노출(CWE-2(HIGH
임팩트·목표달성	Pentest	🎯 MinIO 콘솔 admin API로 멀티테넌트 고객사 그룹·서비스계정 키·정책 노출 → 상세 https://s3-console.example.com/api/v1/users · 실제 자산(계정·데이터·파일 등)을 확보·유출·탈취한 것으로 확인	민감 정보 노출(CWE-2(HIGH

임팩트·목표달성	Pentest	🎯 MinIO 콘솔 admin API로 멀티테넌트 고객사 그룹·서비스계정 키·정책 노출 (CWE-200) → 상세 https://s3-console.example.com/api/v1/users · 실제 자산(계정·데이터·파일 등)을 확보·유출·탈취한 것으로 확인	민감 정보 노출(CWE-2(HIGH
임팩트·목표달성	Pentest	🎯 MinIO bleve 검색인덱스에서 실제 SMS 메시지 원문·수신번호 대량 유출 (인증문자 포함, CWE-200) → 상세 https://s3-console.example.com/api/v1/buckets/bleve/objects/download · 실제 자산(계정·데이터·파일 등)을 확보·유출·탈취한 것으로 확인	민감 정보 노출(CWE-2(HIGH
임팩트·목표달성	Source→Pentest	🎯 MinIO [CUST_C]([redacted] 블록체인) 소스코드·systemd·RPC노드 (XXX.XXX.XXX.XXX) 유출 (CWE-540) → 상세 https://s3-console.example.com/api/v1/buckets/[CUST_C]-backup/objects/download · 실제 자산(계정·데이터·파일 등)을 확보·유출·탈취한 것으로 확인	CWE-540 HIGH
임팩트·목표달성	Pentest	🎯 MinIO dump-storage 버킷 SMS 게이트웨이 사업DB 덤프 실제 다운로드 — 실사용자 bcrypt 해시·청구·발신번호 유출 (CWE-200) → 상세 https://s3-console.example.com/api/v1/buckets/dump-storage/objects/download · 실제 자산(계정·데이터·파일 등)을 확보·유출·탈취한 것으로 확인	민감 정보 노출(CWE-2(HIGH
임팩트·목표달성	Pentest	🎯 MinIO dump-storage2 버킷 SMS 게이트웨이 super-admin 자격·클라이언트 비밀번호·라우팅 설정 유출 (CWE-798) → 상세 https://s3-console.example.com/api/v1/buckets/dump-storage2/objects/download · 실제 자산(계정·데이터·파일 등)을 확보·유출·탈취한 것으로 확인	하드코딩된 자격증명(CV HIGH
임팩트·목표달성	Pentest	🎯 MinIO gateway 버킷에 SMS 게이트웨이 메시지 DB 덤프([redacted]건) 노출 — 발신/수신번호·메시지 구조 유출 (CWE-200) → 상세 https://s3-console.example.com/api/v1/buckets/gateway/objects/download · 실제 자산(계정·데이터·파일 등)을 확보·유출·탈취한 것으로 확인	민감 정보 노출(CWE-2(HIGH
임팩트·목표달성	Source→Pentest	🎯 MinIO harbor-bucket Docker레지스트리로 [제품A 통합관리자] 소스이미지 유출 — PHP 5.3.29(EOL)·앱소스 [redacted] 노출 (CWE-540) → 상세 https://s3-console.example.com/api/v1/buckets/harbor-bucket/objects/download · 실제 자산(계정·데이터·파일 등)을 확보·유출·탈취한 것으로 확인	CWE-540 HIGH
임팩트·목표달성	Pentest	🎯 MinIO [CUST_E] 버킷 메시징 플랫폼 DB 덤프에서 평문 Telegram 봇 토큰·사업자번호·계좌번호 유출 (CWE-798) → 상세 https://s3-console.example.com/api/v1/buckets/[CUST_E]/objects/download · 실제 자산(계정·데이터·파일 등)을 확보·유출·탈취한 것으로 확인	하드코딩된 자격증명(CV HIGH
임팩트·목표달성	Pentest	🎯 MinIO [CUST_E]-[CUST_D] 버킷([CUST_D] 테넌트) 평문 Telegram 봇 토큰·발신번호 유출 (CWE-798) → 상세 https://s3-console.example.com/api/v1/buckets/[CUST_E]-[CUST_D]/objects/download · 실제 자산(계정·데이터·파일 등)을 확보·유출·탈취한 것으로 확인	하드코딩된 자격증명(CV HIGH
임팩트·목표달성	Source→Pentest	MinIO [CUST_A] 테넌트 소스코드 유출 — 무검증 파일업로드 (getfile.php)·PHP 5.2.17 EOL (CWE-540) → 상세 https://s3-console.example.com/api/v1/buckets/[CUST_A]-admin-dev/objects/download	제한 없는 파일 업로드(C HIGH
임팩트·목표달성	Source→Pentest	MinIO [CUST_A] 테넌트 소스코드 유출 — 무검증 파일업로드 (getfile.php)·PHP 5.2.17 EOL (CWE-540) → 상세 https://s3-console.example.com/api/v1/buckets/[CUST_A]-admin-dev/objects/download	CWE-540 HIGH
🌐 **isp.example.com** · 1건			
임팩트·목표달성	Source→Pentest	🎯 내부 보안플랫폼(ISP) 인터넷 노출 + 로그인 계정 열거 — Harbor 소스 유출과 체이닝 (CWE-204) → 상세 https://isp.example.com · 실제 자산(계정·데이터·파일 등)을 확보·유출·탈취한 것으로	CWE-204 HIGH