yettiesoft

웹사이트 개인정보 유출 사례 및 보안 대책

2023.03.23

G-PRIVACY 2023

2023 정부·공공·기업 개인정보보호&정보보안 컨퍼런스

회사 소개

예티소프트는?

국내 최초 웹 표준
보안 메일 솔루션

국내 최초 웹 표준
웹 보안 솔루션

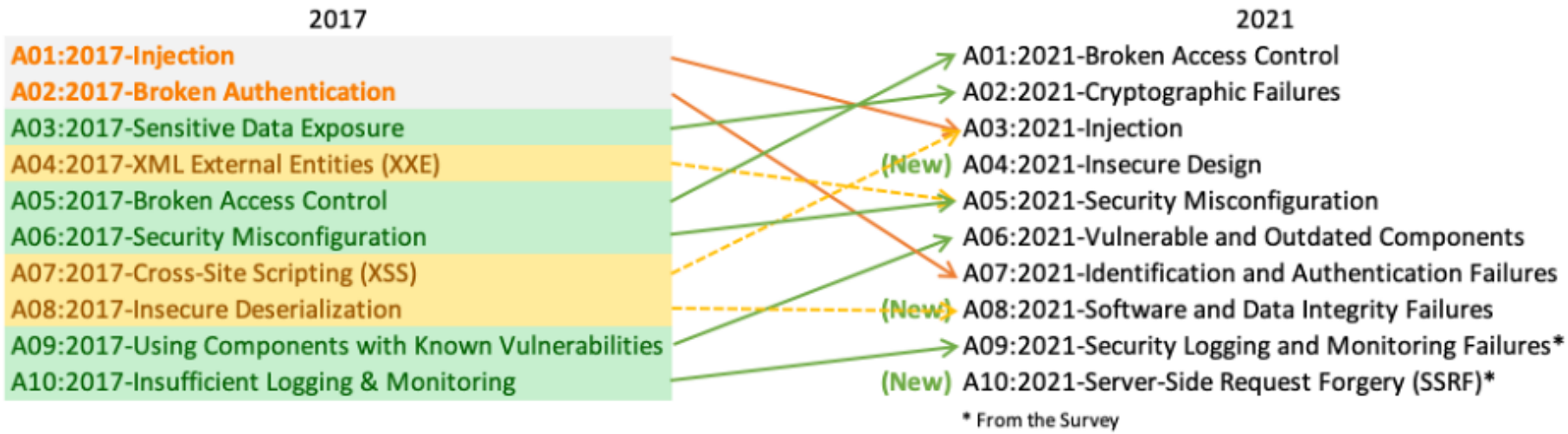
국내 최초 **HTML5** 기반
공동 인증 솔루션

국내 최초 **HTML5** 기반
간편인증 솔루션

인터넷 환경에서 안전하고 편리한 사용자 환경을 만들고자 항상 새로운 방법을 고민하는 회사

OWASP로 보는 웹 서비스의 다양한 보안 취약점

OWASP Top 10



A03:2017- Sensitive Data Exposure / A02:2021-Cryptographic Failures

중요 정보 유출에 집중해서

A03:2017- Sensitive Data Exposure / A02:2021-Cryptographic Failures

민감 데이터를 불필요하게 저장하지 말 것

사용 후 즉시 폐기하거나 토큰화 등을 통해서 사용

시큐어 코딩

주요 기밀 데이터(비밀번호,신용카드 등)는 추가적인 보호가 필요

- 적절한 암호화 (알고리즘, 작동 모드 / 설정 등)
- HTTPS (가능하면 HSTS)

HTTPS와 주요 암호화 기능 사용

보안 취약점으로 인한 주요 사고 사례

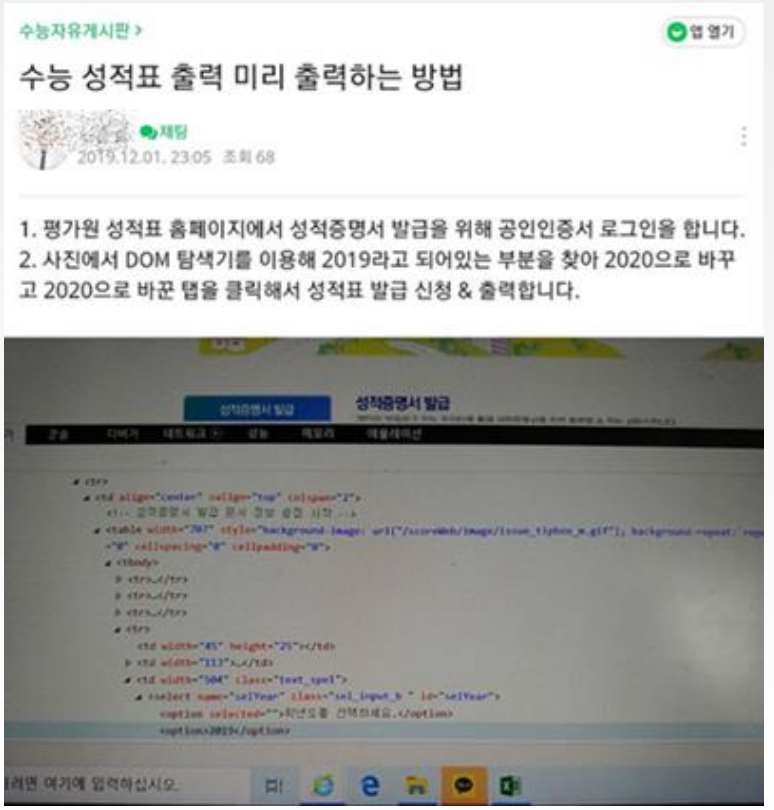
수능 성적표 유출 (2019년)

동작 방식

- 개발자 도구를 이용한 DOM 위변조

대응 방안

- 서버에서 관련 예외처리
- 난독화 등 DOM 자체에 대한 보안



연합뉴스: "수능 성적 확인했다" 성적 발표 이틀 앞두고 '인증 대란'

보안 취약점으로 인한 주요 사고 사례

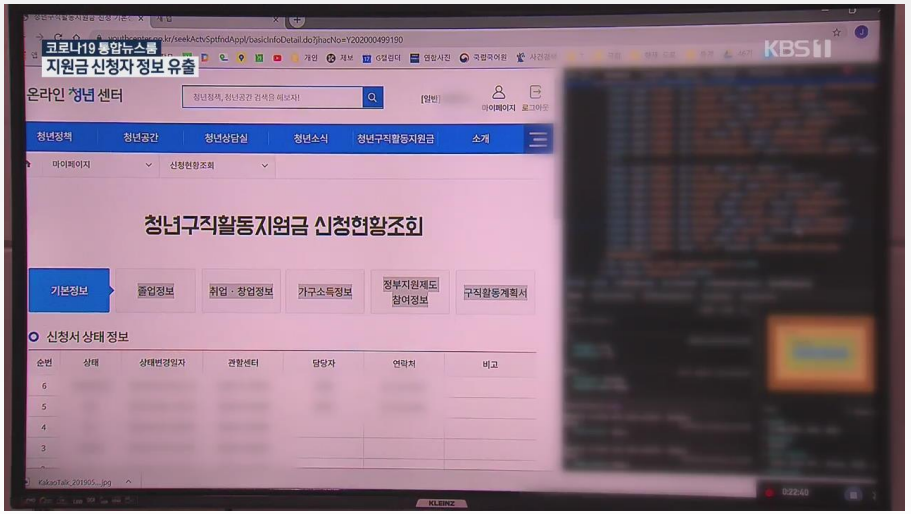
'청년 구직지원금' 개인 정보 유출 (2020년)

동작 방식

- 개발자 도구를 이용한 DOM 위변조

대응 방안

- 서버에서 관련 예외처리
- 난독화 등 DOM 자체에 대한 보안



KBS: 18만 명 신청한 '청년구직지원금'...사이트 개인정보 관리 허술

보안 취약점으로 인한 주요 사고 사례

KT 개인정보 유출 (2014년)

동작 방식

- Proxy Tool(Paros)를 이용한 파라미터 위변조

대응 방안

- 서버에서 인증에 관련한 적절한 처리
- 파라미터 암호화/ 난독화를 통한 통신 구간에 대한 보안

산업일보: KT 개인정보 유출한 해커, 홈피 수천만번 접속에도 감지 못해
보안뉴스: KT해킹! 해커는 어떤 취약점을 노렸나?

보안 취약점으로 인한 주요 사고 사례

공공아이핀 해킹 (2015년)

동작 방식

- Proxy Tool(Paros)를 이용한 파라미터 위변조
- 본인인증 관련 파라미터 변조를 통해 절차 우회

대응 방안

- 파라미터 암호화 / 난독화를 통한 통신 구간에 대한 보안
- DOM 변경의 경우 난독화 등 DOM 자체에 대한 보안

YTN: 본인인증 무력화 '파라미터 위변조' 해킹
IT WORLD: '아이핀 너마저', 공공아이핀 시스템 해킹으로 75만개 아이핀 부정 발급

보안 취약점으로 인한 주요 사고 사례

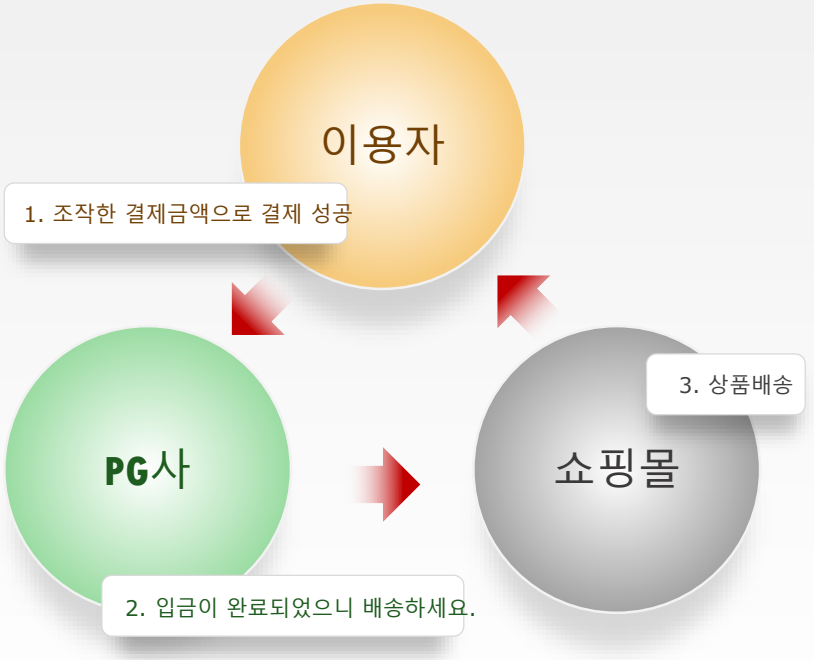
쇼핑몰 결제대금 조작 (2016년)

동작 방식

- Proxy Tool(Paros)를 이용한 파라미터 위변조
- 결제 금액과 실제 물건의 금액을 비교하지 않아서 발생

대응 방안

- 쇼핑몰,PC간의 금액 비교 등 적절한 처리
- 파라미터 암호화/난독화를 통한 통신 구간에 대한 보안
- DOM 변경의 경우 난독화 등 DOM 자체에 대한 보안



보안뉴스: 쇼핑몰 결제대금 어떻게 조작했나? 프록시 툴 악용한 해킹

여러가지 권고 사항

전자금융감독규정 개정안 (2016년 ~)

무결성 보장: 위변조 방지 / 난독화

제6절 전자금융업무

제34조(전자금융거래 시 준수사항) 금융회사 또는 전자금융업자는 전자금융거래와 관련하여 다음 각 호의 사항을 준수하여야 한다.

5. 금융회사 또는 전자금융업자는 전자금융거래에서 이용자에게 제공하거나 거래를 처리하기 위한 전자금융거래프로그램(거래전문포함)의 위·변조 여부 등 무결성을 검증할 수 있는 방법을 제공할 것

"인터넷 이용환경 개선을 위한 기술 안내서 (KISA, 2016)

SSL 환경에서 난독화/암호화 필요성

웹 표준 환경에서 자바스크립트를 이용하여 Application Level의 Encryption을 구현하여 사용하는 것을 권장하고 있으며 Application Level Encryption의 가용한 구성은 다음과 같다.

- 강력한 보안구성을 SSL/TLS Transport Layer 상에서 운용한다.
- Encryption/Decryption을 수행하는 자바스크립트에 대한 보호 대책을 적용한다.

공공 웹사이트 플러그인 제거 가이드라인 (2018)

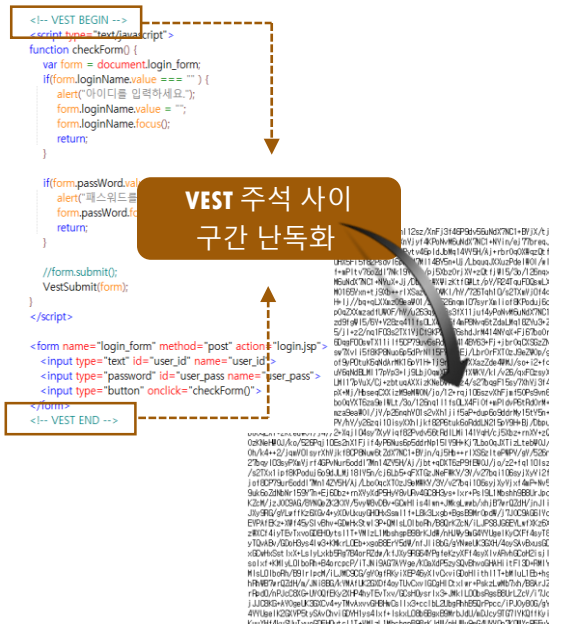
다양한 보안 방안 가이드

소스보기 제어(우클릭)	자바스크립트 이벤트 제어 코드(소스난독화 처리)
개발자도구 보기 제어	자바스크립트 이벤트 제어 코드(소스난독화 처리) 클라이언트 자바스크립트, 서버 유효성 검사
소스 보기	소스보기 화면에 마우스 제어 우클릭 이벤트 제어를 통한 화면 조회보호, 클라이언트 자바스크립트, 서버 유효성 검사

보안 취약점에 대한 대응 방안

DOM 위 · 변조

HTML 소스코드 난독화

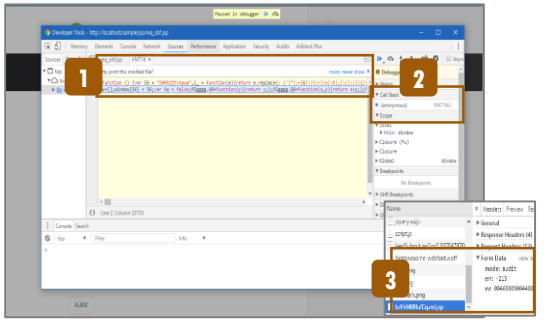


DOM영역 숨김

- 실제 소스에서는 자바스크립트 호출부와 함수 부분이 존재
- 개발자도구의 DOM영역(Elements 탭)에서는 자바스크립트가 숨겨져 디버깅 불가

안티 디버깅

- 디버깅 시도 시 관련 로그를 서버로 전송
- 난독화 된 스크립트 내부에서 디버깅 포인트가 발생하여 스크립트 로직 분석이 불가능
- Call Stack 부분 (anonymous) 로 표기되어 스크립트 콜 스택 분석이 불가능



보안 취약점에 대한 대응 방안

Proxy를 이용한 파라미터 위·변조

원론적으로는 **Proxy**를 이용한 중간자 공격

대응의 기본은 **HTTPS**

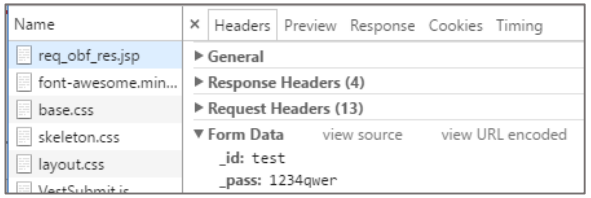
HTTPS로 **Proxy**를 사용한 보안성 심의를 통과할 수 있나?

Proxy를 사용해서 중간에서 풀어볼 수 없는 보안 대책 필요

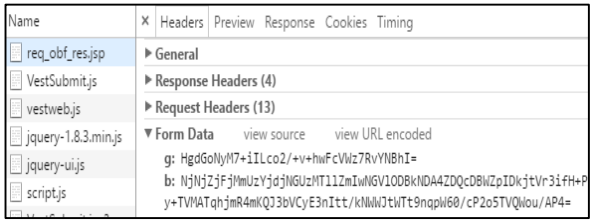
VestWeb 파라미터 난독화

- Submit, ajax 를 이용한 Request 파라미터를 매번 다른 Key를 이용하여 난독화
- Submit, Ajax, Encrypt, Decrypt 함수 제공

• **난독화 적용 전**



• **난독화 적용 후**



결론

시큐어 코딩 및 **HTTPS** 등은 기본적으로 적용

사람이 빠뜨릴 수 있는 부분에 대해 자동화를 통해 웹 서비스의 보안을 향상 시켜야 함

Q & A

Any Question?

감사합니다

yettiesoft