바나프레소 웹사이트 주문 취약점 보고

공격 시나리오 : 바나프레소 자체 할인 쿠폰 소유자 또는 구매자가
쿠폰 사용시 해당 쿠폰의 정보를 분석해서,

임의로 가짜 쿠폰을 대입하여 적용 가능

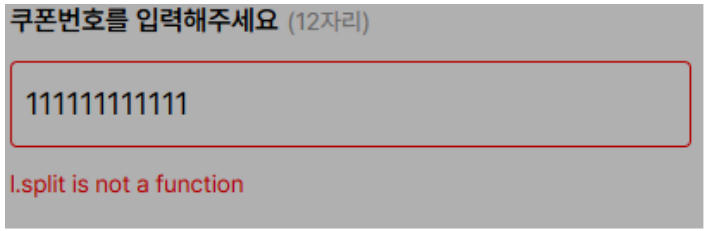
문제점 원인 : 쿠폰, 최종 결제 금액 유효성 체크 등이 **결제 직전** 서버에서 이루어지지 않고 있습니다.

※ 웹사이트의 최종 사용자 (브라우저 이용자) 는 얼마든지 임의로 자바스크립트 등을 조작하여
서버에 API 요청을 할 수 있습니다.

1. 결제 페이지에 쿠폰 사용 기능이 있어서 어떻게 적용 되는지 JS로직을 검토 해보았습니다.

usePayment.js – 쿠폰 유효성 검증 코드 일부

```
    };
const ue = await Z.query("8198E2E4D3DA4C690708274FF0BE4F32", {
    nFCode_NOUSE: 0,
    nANo_NOUSE: 0,
    sPhone_NOUSE: "",
    sCouponID: x
})
  , {err_msg: R} = ue.params;
```



위 서버 응답 데이터의 모델정보에서 apply, title 등 알기 쉬운 키 값이 보여 apply 키가 할인금액 값으로 추측하여 임의로 값을 넣고 적용한 결과

추가로 split함수로 기타 정보를 파싱하는 것을 파악하여
기존 가지고 있는 실제 쿠폰을 대입 및 값을 참고만(실제 사용하진 않음) 하여
정상 값을 넣고, 할인 금액만 변경 했습니다.

2. 실제 임의 쿠폰이 등록된 모습

제휴사(카카오 등) 쿠폰 번호를 입력하여 사용해주세요. 이벤트 쿠폰은 앱 혹은 키오스크에서 사용가능합니다.

쿠폰 0장 0원

해킹쿠폰 3300원

유효기간 :
사용 가능 매장:직영/가맹점(통합)

· 총 주문금액

총 주문수량	1
총 주문금액	4,300
할인금액	0
쿠폰할인	0

· 결제금액 4,300원

취소 결제하기

스탬프 적립 (선택)

휴대폰 번호

쿠폰 적용 메뉴 선택

쿠폰 적용할 메뉴를 선택해주세요.

유자셔벗아메리카노
4300
쿠폰적용 - 해킹쿠폰

적용취소선택완료

확인

· 결제금액 4,300원

취소 결제하기

쿠폰 1장 -3,300원

해킹쿠폰 3300원

유효기간 :
사용 가능 매장:직영/가맹점(통합)
적용메뉴: 유자셔벗아메리카노(-3300원)

· 총 주문금액

총 주문수량	1
총 주문금액	4,300
할인금액	0
쿠폰할인	-3,300

· 결제금액 1,000원

취소 결제하기

스탬프 적립 (선택)

휴대폰 번호

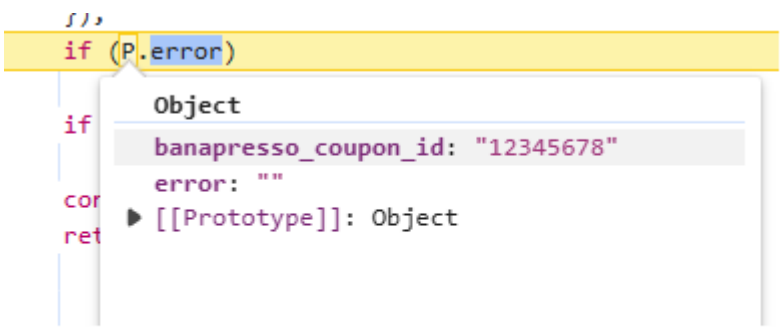
됩니다.

3. 최종 결제 직전에 한번 더 쿠폰 검증 우회

a. 정상 쿠폰 인지 한번 더 체크 하는데 이 역시 클라이언트에서 임의 변조 가능 합니다.

```
mutationFn: async ({labelCouponList: e, userCode: K}) => {
    const {params: P} = await Z.query("FC1E0762BEE68916812135109FD6D6C3", {
        ano: 0,
        temp_coupon_id: e.map( ({tempID: T}) => T).join(),
        result: e.map( ({result: T}) => T).join()
    });
    if (P.error)
        throw new Error(P.error);
    if (!P.banapresso_coupon_id)
        throw new Error("쿠폰조회 오류 입니다.");
    const x = P.banapresso_coupon_id.split(",");
    return e.map( (T, U) => ({
        T
```

b. 임의 변조된 모습



4. 조작된 쿠폰으로 최종 결제

4,300원 유자셔벗아메리카노 메뉴를 1,000원에 결제