

버그 바운티 규칙 v4.0

업데이트 날짜:2019.12.06

버그 바운티 협약

DVP 플랫폼의 취약점 심사 기준을 보다 표준화하기 위해 BCSEC (바이마오후이) 와 PeckShield 가 버그 바운티 규칙을 작성하였으며 이 규칙은 DVP 커뮤니티의 의견에 따라 조율 및 수정될 수 있습니다.

포상 범위

A타입 : DVP 플랫폼에 가입되어 있는 바운티 기업이며 이 경우 기업에서 직접 수령하거나 거절합니다.

B 타입: DVP 플랫폼에 가입되어 있지 않은 기업이며 이 경우 포상 범위는 블록체인 관련 거래소, 가상화폐 토큰, 디앱, 지갑, 마이닝풀 등이 포함되며 해당 기업이 DVP 플랫폼에 가입하기전까지 DVP재단에서 대신 수령합니다.

주의사항: B타입 기업의 경우 고정적이지 않으며 실제 상황에 따라 C타입 기업으로 변경될 수 있습니다.

C 타입: DVP에서 수령하지 않는 기업이며 이 경우 DVP 재단의 포상범위에 속하지 않음을 명확히 규정합니다. 블록체인 관련 미디어 사이트(뉴스/기사 등) , 전자상거래 사이트(채굴기 판매 등) 블록체인/가상화폐와 직접적인 관련이 없거나 정상적으로 운영이 되고 있지 않는 기업 (스캠/사기 등) 등등이 이러한 경우에 포함됩니다

B 타입 기업 상세 설명:

아래의 포상금 기준은 B 타입 기업에만 적용되며 A 타입의 기업은 자체 포상금 기준이 있음을 명시합니다. **포상금은 취약점의 위험도와 절대적으로 연동되는것이 아니며 실질적으로 미칠 수 있는 영향 (이용 난이도, 위험 범위, 금전적 이익 취득 가능성여부)을 근거로 책정됩니다.** 만약 실질적 영향이 매우 낮은 경우 DVP의 **강등 규칙**에 따라 포상금이 낮아질 수 있습니다.

- 모든 유효 취약점과 위협 정보(threat information)는 아래의 3가지 조건을 충족해야 합니다. 1. 공개되지 않은 취약점 2. 패치되지 않은 취약점 3. 타 플랫폼에 제출되지 않은 취약점
- 제출한 취약점 타킷이 포상범위(토큰/퍼블릭체인/거래소/지갑/디앱/마이닝풀 등)에 속하지 않지만 블록체인 업계에서 충분한 영향력이 있을 경우 위협정보로 제출하실 수 있으며 포상금은 실제 위협 정도에 따라 책정됩니다.
- 심사위원은 제보된 취약점에 대하여 추측을 하지 않습니다. 취약점에 대한 상세한 설명으로 증명해야 하며 DVP는 이론상으로만 존재하는 취약점은 승인하지 않습니다.
- 제출한 취약점이 타킷 기업의 주요 업무에 속하지 않을 경우 **비핵심업무 취약점 기준**을 참고하여 주세요.

- 본 버그 바운티 규칙은 4.0버전으로 확실한 위협이 있지만 규칙에 명시되어 있지 않는 취약점 또는 포상금 기준이 불합리한 문제가 발생할 경우 커뮤니티의 의견에 따라 지속적으로 업그레이드 할 예정입니다.
- 취약점 포상금은 실제 심사 결과에 따라 책정되며 도표에 표시되어 있는ETH와 DVP 포상액은 해당 등급의 최고 금액입니다.
- DVP에서는 타깃 기업에 대해서도 등급 제도를 실시하며 취약점 제보시 해당 타깃의 등급을 확인할 수 있는 링크를 첨부해주셔야 합니다.
- 취약점/위험 정보가 DVP 버그 바운티 규칙으로 책정이 불가할 경우에는 CVSS 취약점 등급 기준과 실제 위험 정도에 따라서 판단됩니다.

포상금 기준

가상화폐 거래소

	Critical	High-risk	Mid-risk	Low-risk
1등급 (ETH)	31.2	14.4	4.7	0.6
2등급 (ETH)	5.2	2.3	1.0	0.3
3등급 (ETH)	1.6	0.8	0.4	0.2
4등급 (ETH+DVP)	1.2+640	0.6+320	0.3+160	0.1+80
5등급 (DVP)	256	128	64	6

거래소 등급 확인 사이트 : <https://www.feixiaohao.com/exchange/>

1등급 : 종합랭킹 상위 30

2등급 : 종합랭킹 상위 50

3등급 : 종합랭킹 상위 80

4등급 : 종합랭킹 상위 120

5등급 : feixiaohao에 수록되어 있지 않지만 매일 거래량이 있는 거래소.

Critical(심각한 위험) : 위협을 실현가능하다는 이론이 아닌 실제 시도를 통한 성공 증명이 필요함

- 원격으로 시스템 액세스 권한을 얻을 수 있음 ;
- 핵심업무의 심각한 디자인 /로직 결함 ;
- 고객 및 기업 자산에 영향을 미칠 수 있음 (송금, 결제 /가상화폐 프라이빗 키 유출 등이 포함됨) ;
- 매수/매도를 작동시키는 불법적인 작동을 통하여 시장을 조작할 수 있음 ;

High-risk(높은 위험) : 위협을 실현가능하다는 이론이 아닌 실제 시도를 통한 성공 증명이 필요함

- 서버의 접근 권한을 직접 획득할 수 있음 ;
- 소스코드나 SQL 입력 등 대량의 민감한 정보를 직접적으로 탈취할 수 있음 ;
- interaction 없이 직접적으로 대량의 유저 정보나 서버관리 직원의 ID를 도용할 수 있음. 사용자가 볼수 있는 페이지의 Stored XSS 혹은 관리자 서버에서 볼 수 있는 XSS 등 경우가 포함됨 . (서버 정보에 접근하여 정보를 탈취한 증명이 필요하며 증명하지 못할 경우 중간 또는 낮은 위험으로 분류 됨) ;

Mid-risk(중간 위험) : 위협을 실현가능하다는 이론이 아닌 실제 시도를 통한 성공 증명이 필요함

- 일부분 사용자 정보 노출 등 소량의 민감한 정보 노출.SSRF 내부 네트워크 정보 노출 등이 포함됨 ;
- 사용자 본인 계정 자체에만 영향을 미치는 디자인 결함/로직 결함 ;
- interaction이나 익스플로잇을 통하여 사용자의 ID를 도용할 수 있는 취약점. 자주 사용하지 않는 페이지 Stored XSS, 관리자 서버에서는 보이지 않는 XSS유형 취약점 등이 포함됨 ;
- 서비스 거부 결함 ;

Low-risk(낮은 위험) : 실제 시도를 통한 성공 증명이 없이 이론만으로 가능함.

- 민감하지 않은 정보 노출. Directory Traversal 등이 포함됨 ;
- URL Redirection ;
- 단문 메시지 인터페이스 남용 문제 등;
- 상호작용의 요구가 높은 사용자의 아이디를 탈취할 수 있는 취약점. 반사형 XSS, 일반 CSRF 등이 포함 ;
- 기타 실제 위협을 증명하기 어렵지만 이론상으로 존재하는 결함 ;

포상 대상에서 제외되는 경우 :

- SPF mail forge 결함
- 이용할 수 없는 self-xss / post형 반사 XSS
- 이메일 폭격
- 민감하지 않은 CSRF 결함
- 기타 위험성이 매우 낮은 취약점
- 사기/스캠 등 정상적으로 운영되고 있지 않은 사이트.

가상화폐 토큰

	Critical	High-risk	Mid-risk	Low-risk
1등급 (ETH)	39.0	27.0	7.5	1.2
2등급(ETH)	16.9	7.8	3.9	0.7

3등급(ETH)	6.5	3.6	1.0	0.4
4등급(ETH+DVP)	3.5+1280	1.1+640	0.5+320	0.2+160
5등급(DVP)	256.0	128.0	64.0	6.0

랭킹 확인 사이트: <https://coinmarketcap.com>

1등급 : 시총 랭킹 상위 30

2등급 : 시총 랭킹 상위 100

3등급 : 시총 랭킹 상위 400

4등급 : 시총 랭킹 400위 이하

5등급 : 시총 랭킹에 수록되어 있지 않지만 매일 거래량이 있는 토큰

Critical (심한 위험) : 위험을 실현가능 하다는 이론이 아닌 실제 시도를 통한 성공 증명이 필요함

- 원격으로 시스템 액세스 권한을 얻을 수 있음 ;
- 디지털 자산을 직접 탈취 할 수 있음 ;
- 심각한 민감한 정보 노출. 사용자의 프라이빗키, 비밀번호 등이 포함됨 ;

High-risk(높은 위험) : 위험을 실현가능 하다는 이론이 아닌 실제 시도를 통한 성공 증명이 필요함

- 서비스 응답 거부로 이어질 수 있음 ;
- 다량의 사용자 / 거래소에 영향을 주는 디자인 결함 / 로직 결함 ;
- 디지털 자산을 추가 발행하거나 소각할 수 있음;
- 스마트 컨트랙트의 중요한 기능의 서비스 응답 거부 ;

Mid-risk(중간 위험) : 위험을 실현가능 하다는 이론이 아닌 실제 시도를 통한 성공 증명이 필요함

- 로컬 권한 업그레이드로 이어질 수 있음 ;
- 사용자 본인 계정에만 영향을 주는 디자인 결함 / 논리적 결함;
- 간접적으로 높은 위험의 결함으로 이어질 수 있음 ;
- 일부 사용자의 디지털 자산을 추가하거나 소각할 수 있음. ;
- 스마트 컨트랙트내 혹은 사용자의 일부 자산을 제한적으로 탈취할 수 있음 ;

Low-risk (낮은 위험) :

- 일반 정보 노출;
- 낮은 위험의 디자인 결함 / 로직 결함;
- 시스템 자원 남용 또는 사용자 스팸을 일으킬 수 있는 루프;
- 이론상으로만 존재하는 결함. owner만 이용할 수 있는 결함 등이 포함됨;

지갑

	Critical	High-risk	Mid-risk	Low-risk
1등급(ETH)	31.2	14.4	4.7	0.6
2등급(ETH)	5.2	2.3	1.0	0.3
3등급(ETH)	1.6	0.8	0.4	0.2
4등급(ETH+DVP)	1.2+640	0.6+320	0.3+160	0.1+80
5등급(DVP)	256.0	128.0	64.0	6.0

랭킹 확인 사이트 : <https://www.feixiaohao.com/wallet/>

1등급 : 랭킹 상위 10

2등급 : 랭킹 상위 30

3등급 : 랭킹 상위 80

4등급 : 랭킹 80위 이하

5등급 : 랭킹에 수락되어 있지 않지만 지갑 사용자와 자산을 보유하고 있다는것을 증명할

수 있을 경우.

Critical (심한 위험) : 위협을 실현가능 하다는 이론이 아닌 실제 시도를 통한 성공 증명이 필요함

- 원격으로 서비스 / 클라이언트 액세스 권한을 얻을 수 있음 ;
- 많은 양의 디지털 자산을 탈취할 수 있음 ;
- 심각한 민감한 정보 노출. 사용자 프라이빗 키/ 비밀번호 등이 포함됨 ;

High-risk (높은 위험) : 위협을 실현가능 하다는 이론이 아닌 실제 시도를 통한 성공 증명이 필요함

- 대량의 민감한 정보 노출 ;
- 서비스 / 클라이언트의 서비스 요청 거부;
- 많은 양의 사용자 ID를 도용할 수 있음

Mid-risk (중간 위험) : 위협을 실현가능 하다는 이론이 아닌 실제 시도를 통한 성공 증명이 필요함

- 사용자 정보를 악의적인 변경할 수 있음
- 소량의 민감한 정보 노출

- 적은 양의 사용자 ID를 도용할 수 있음

Low-risk (낮은 위험) :

- 일반 정보 유출;
- 실제 위험이 매우 낮은 디자인 결함 / 로직 결함;
- 시스템 정보 난용 또는 사용자 스템을 일으킬 수 있는 루프;

마이닝 풀

	Critical	High-risk	Mid-risk	Low-risk
1등급	15 eth	10 eth	5 eth	1 eth
2등급	심사후 책정	심사후 책정	심사후 책정	심사후 책정

랭킹 확인 사이트 : <https://btc.com/stats/pool>

1등급 : 랭킹 상위 20

2등급 : 랭킹에 수록되어 있지 않지만 해시 레이트를 증명할 수 있는 경우.

Critical (심한 위험) : 위험을 실현가능 하다는 이론이 아닌 실제 시도를 통한 성공 증명이 필요함

- 원격으로 마이닝 풀에서 모든 권한을 얻을 수 있음;
- 모든 마이닝 풀 계산 전력을 원격 제어 가능;
- 마이닝 풀 보상이나 지갑의 자산을 탈취할 수 있음;

High-risk (높은 위험): 위험을 실현가능 하다는 이론이 아닌 실제 시도를 통한 성공 증명이 필요함

- 마이닝 풀이 필히 이행해야 할 필수 서비스의 거부를 유도 할 수 있음;
- 블록 보류 공격, 컴퓨팅 파워 위조 등과 같은 마이닝 풀의 이자 손실로 이어질 수 있음;
- 대량의 민감한 정보 노출을 유도할 수 있음;

Mid-risk (중간 위험): 위험을 실현가능 하다는 이론이 아닌 실제 시도를 통한 성공 증명이 필요함

- 디자인 결함 / 로직 결함;

Low-risk (낮은 위험)- 실제 시도를 통한 성공 증명이 필요하지 않으며 이론만으로 가능

- 적은 양의 정보 노출로 이어질 수 있음;
- 특정한 조건 하에서만 실제 효과를 가질 수 있음;

DApp

	Critical	High-risk	Mid-risk	Low-risk
1등급 (ETH)	29.3	18.0	7.5	0.6
2등급 (ETH)	16.9	7.8	3.9	0.3
3등급 (ETH)	6.5	3.6	1.0	0.2
4등급 (ETH+DVP)	3.5+1280	1.1+640	0.5+320	0.1+160
5등급 (DVP)	256.0	128.0	64.0	6.0

랭킹 확인 사이트 : <https://dapp.review/explore> (7天交易额) (7일 거래량 기준)

1등급 : 랭킹 상위 10

2등급 : 랭킹 상위 50

3등급 : 랭킹 상위 200

4등급 : 랭킹 200위 이하

5등급 : 랭킹에 수록되어 있지 않지만 DApp에 디지털 자산을 보유하고 있고 매일 거래량이 있는 경우 .

Critical (심한 위험): 위협을 실현가능 하다는 이론이 아닌 실제 시도를 통한 성공 증명이 필요함;

- 계약을 탈취할 수 있거나 다른 사용자의 디지털 자산을 사용자의 의도 없이 계약할 수 있음;

High-risk (높은 위험): 위협을 실현가능 하다는 이론이 아닌 실제 시도를 통한 성공 증명이 필요함

- 디지털 자산을 만들거나 소각 할 수 있음;
- 계약의 중요한 기능이나 서비스 거부를 사용할 수 있음;

Mid-risk (중간 위험): 위협을 실현가능 하다는 이론이 아닌 실제 시도를 통한 성공 증명이 필요함

- 일부 사용자의 디지털 자산을 추가하거나 소각 할 수 있음;

- 제한된 계약을 훔치거나 사용자의 디지털 자산을 사용자의 의도 없이 계약 할 수 있음;

Low-risk (낮은 위험): 실제 시도를 통한 성공 증명이 필요하지 않으며 이론만으로 가능

- 결함을 포함하여 이론적인 보안 결함은 소유자만이 악용할 수 있음;

위협 정보

Critical	High-risk	Mid-risk	Low-risk
3 eth	1.6 eth	0.6 eth	0.2 eth

Critical (심한 위험) :

- 블록체인 관련 대량의 민감한 정보 유출 및 관련 증거 있는 경우;
- 개인이 아닌 많은 양의 디지털 자산을 탈 취 할 수 있으며 관련 증거가 있는 경우;
- 블록체인 관련 미공개 취약점 및 관련 증거가 있는 경우

High-risk (높은 위험) :

- 블록체인 산업에 관련 기업이 공격당한 내용과 이에 대한 증명이 가능한 경우;
- 블록체인 산업 관련 기업에게 큰 범위의 공격을 진행중인 내용과 이에 대한 증명이 가능한 경우;
- 블록체인 관련 소프트웨어/하드웨어에 부정확한 수단이 있다는 증거를 제출하는 경우;
- 블록체인 산업 기업에 대한 새로운 공격 기술 ;

Mid-risk (중간 위험):

- 블록체인 관련 취약점이 이용되고 있는 상황과 관련 증거가 있는 경우;
- 블록체인 보안 업계에 공개되지 않은 보안 사건 제보 ;
- 블록체인 기업에 관한 민감한 정보 유출 ;

Low-risk (낮은 위험):

- 블록체인 산업에 포함된 기업의 낚시 사이트,App 등 제보;
- 블록체인 산업내의 불법 공격 관련 정보 제보 ;

비핵심 업무 취약점 기준

“비핵심 업무 취약점”란 블록체인 기업의 주요 비즈니스와 관련이 없는 취약점을 뜻합니다.

예시: 가상화폐 토큰, 지갑, DApp 등의 홈페이지 관련 취약점.

	High-risk	Low-risk
1등급 (ETH)	1.2	0.4

2등급 (ETH)	0.8	0.2
3등급 및 이하 (DVP)	256	

1등급 : 메인 비즈니스 기준에서 랭킹 1등급 ;

2등급 : 메인 비즈니스 기준에서 랭킹 2등급 ;

3등급 및 이하 : 메인 비즈니스 기준에서 랭킹 3등급 및 이하 ;

예시: 이더리움 토큰의 경우, 가상화폐 토큰 랭킹에서는 1위에 속하므로 바운티 기업은 1등급으로 분류되지만, 이더리움 토큰 자체가 아닌 홈페이지에서 발견된 웹취약점을 제보할 경우 "비핵심 업무 취약점"으로 분류됩니다.

High-risk (높은 위험): 위험을 실현가능 하다는 이론이 아닌 실제 시도를 통한 성공 증명이 필요함

- 원격으로 시스템 액세스 권한을 얻을 수 있으며 많은 양의 민감한 정보를 탈취할 수 있음(120개 이상);
- 민감한 정보를 볼 수 있는 데이터 베이스에 액세스할 수 있음;
- 민감한 정보를 볼 수 있는 이메일에 임의로 접근할 수 있음;
- 사용자 혹은 기업에 큰 영향을 미칠 수 있음;

Low-risk (낮은 위험): 위험을 실현가능 하다는 이론이 아닌 실제 시도를 통한 성공 증명이 필요함

- Stored XSS, 관리자 권한 증명이 가능한 경우;
- 민감하지 않은 이메일에 접근할 수 있음;
- 중요하지 않은 데이터 베이스에 임의로 접근할 수 있음 ;
- 적은 양의 민감한 정보가 유출됨 ;

강등 규칙

포상금은 취약점의 위험 정도, 정보 탈취의 난이도, 영향 범위, 손실의 크기에 따라 판단이 되며 실질적으로 미칠 수 있는 영향에 근거하여 책정됩니다. 실질적 영향이 매우 낮을 경우 DVP에서는 아래의 강등 조건에 따라 포상금이 낮아질 수 있습니다.

강등 조건:

- 테스트 환경의 데이터 및 데이터의 양이 매우 적음.
- 운영되고 있지 않거나 버려진 사이트 등의 타깃일 경우.
- 제한 조건을 포함하여 트리거 조건이 매우 까다로운 경우. 예를 들어서 특정된 계정을 이용하거나 특정된 브라우저에서만 발생이 가능한 XSS 취약점 등의 경우 해당 취약점의 포상금액이 강등 처리 됩니다.
- 동일한 타깃에서 3개 이상의 취약한 비밀번호 취약점.
- 강등의 범위는 최대 1등급을 초과하지 않습니다.

예시 1: 2등급 기업의 Mid-risk 취약점이 강등 될 경우 2등급 기업의 Low-risk 로 판정됩니다.

예시 2: 2등급 기업의 Low-risk 취약점이 강등 될 경우 3등급 기업의 Low-risk 로 판정됩니다.

”통용 취약점” 규칙

- 취약점 자체는 가치가 없으며, 가치는 해당 취약점을 이용하여 발생할 수 있는 피해로부터 파생되므로 취약점 포상액은 화이트 해커가 제보한 취약점 정보와 그 영향 범위와 정보 탈취의 난이도에 의해 결정됩니다.

참고 : 기본적으로 심사위원은 취약점이 위험을 가져올 수 있다고 선입견을 가지고 있지 않으며, 실제 시뮬레이션과 같은 모든 증거는 취약점 정보 제출 시에 포함되어 있어야 하며 이론적으로 가능하다고 추측하는 정보는 유효하지 않습니다.

- 버그 바운티 규칙에 적용되지 않는 취약점의 경우 DVP가 상황에 따라 승인하거나 승인하지 않을 권한이 있습니다.
- 동일한 취약점이 서로 다른 타깃에서 발생하며 3 번 이상 제보된 경우 해당 유형의 취약점은 “통용 취약점 ”으로 중복 취약점으로 분류됩니다. 중복된 취약점으로 기록되지만 동시에 타깃 기업이 승인 여부를 결정할 수 있는 상태로 분류됩니다.
- 포상금 기준의 타깃(퍼블릭체인, 거래소 등)은 기업 자체의 서비스에 한정됩니다. 만약 타깃 기업의 산하 다른 자산(공식 홈페이지, 어플리케이션 등)에서 취약점이 발견된다면, 실제 영업 상황에 따라서 등급이 낮아집니다.
- “통용 취약점”을 제보할 경우 해당 취약점이 발생하는 타깃 업체의 정확한 주소를 명시해야 하며 최소 5개 이상의 유효 타깃을 포함해야 합니다.
- “통용 취약점”을 제출할 경우 해당 취약점이 발생하는 기업중에 등급이 높은 기업을 기준으로 책정됩니다. 상위 3개의 기업은 일반적인 버그 바운티 규칙에 따라 각각 포상금이 지급되는것 외에 추가적으로 상위 3개 기업의 취약점 포상금의 평균 포상금이 지급됩니다. 즉 최종 포상금= 기업 등급이 상위 1.2.3 기업의 포상금 + 3개 기업의 포상금 총합/3
- 동일한 인터페이스로 인한 여러개의 취약점, 동일한 게시 시스템으로 인한 여러 페이지 보안 결함, 전체 사이트 보안 결함을 유발하는 프레임 워크, DNS로 인한 보안 문제 또는 다른 매개 변수가 있는 동일한 파일과 같이 동일한 소스에서 나온 결함은 하나의 취약점으로 취급됩니다.
- 타깃 서비스에 포함되어 있는 타사 제품 예를 들어서 WordPress, Flash, Apache , OpenSSL, SDK 등등 여러가지 소프트웨어 버전의 동일한 곳의 취약점은 한개의 취약점으로 간주됩니다.
- 같은 취약점이지만 2명이 제보할 경우 이후에 제출 된 취약점 이용 방법이 첫번째 제출한 이용 방법과 차이가 클 경우, 2개의 취약점 모두 심사에 통과되지만 이후 제출 된 보상의 일정 부분이 첫 번째 제출자에 지급됩니다.
- 제출자는 DVP에 이미 제보한 취약점을 다른곳에 공개하거나 타 플랫폼에 취약점 정보를 게시하거나 제출할 수 없습니다. DVP에서 부정행위를 발견할 경우 계정과 자산이 동결될 수 있습니다.
- **취약점 통합**
 - 전후 관계가 있는 1개 이상의 취약점은 취합하여 1개의 취약점으로 처리될 수 있으며 심사 결과에 따라 포상금은 높아질 수 있습니다. (예시: 백엔드 시스템에 들어갈 수 있는 취약점을 제보했다가 백엔드에서 SQL injection 취약점이 발생하는 경우) 이미 제보한 취약점에 관하여 추가적인 정보를 취득하였을 경우 해당 내용을 보충하여 더 높은 포상금을 받을 수 있습니다.
 - 하나의 취약점을 여러개로 나누어서 제출하는 경우, DVP는 이들을 하나로 통합하여 처리할 수 있으며 포상금은 그 중 최고 등급 기준으로 책정됩니다. 제출자가 악의적으로 취약점을 분할하여 제보할 경우 DVP에서는 악의적인 행위에 대한 확인을 거친 후 계정을 동결할 수 있습니다.
 - 다음과 같은 경우 제출자의 계정과 자산이 동결될 수 있습니다:

- 순서가 지정된 취약점에 대해 가장 마지막 순서의 취약점을 먼저 제출합니다. 예를 들어서 이메일 주소의 취약점을 발견하고 해당 이메일을 통하여 백엔드 관리자 계정을 탈취할 수 있지만 백엔드 탈취 부분을 먼저 제출하고 이메일 취약점을 나중에 제출하는 경우입니다.

• 취약점 테스트를 빌미로 발견한 취약점을 이용하여 사용자의 이익에 해를 끼치고 사용자의 비즈니스에 영향을 미치면 DVP는 포상금을 지급하지 않으며 해당 계정 및 자산을 동결할 수 있습니다.

• 명확한 설명이 없는 제출물의 경우 즉시 거부됩니다. 모든 취약점 제보에는 타겟 URL(웹사이트일 경우), 텍스트 세부 정보, 이미지 파일 및 명확한 설명 포함됩니다. 예를 들면:

- 타겟 기업의 웹 사이트 주소, 웹 사이트 주소가 없을 경우 별도의 설명이 필요합니다.
- 상세 정보에는 취약점과 관련된 모든 URL이 포함되어야 합니다.
- 취약점 증명이 모든 주요 단계를 나열해야 하며, 이는 심사위원이 추측이 아닌 오로지 제출된 설명에 근거하여 재현할 수 있어야 합니다.
- 취약점 관련 payload는 상세 정보 텍스트에 입력해야 하며 스크린 샷으로만 제출해서는 안 됩니다.
- GitHub 정보 노출, memcache, redis unauthorized access 등과 같은 정보 노출 유형 결함은 내용의 타당도 및 민감도에 따라 분류되며 격리 및 위험도가 낮은 노출은 무시할 수 있습니다
- 백엔드 취약점의 문제는 성공적인 탈취의 증거가 있어야 하며 그렇지 않을 경우에는 거부됩니다.
- 취약한 비밀번호 문제:
 - 동일한 제출자가 발견한 동일한 시스템의 서로 다른 취약한 비밀번호는 하나의 사례로 간주됩니다.
 - 기본 초기 비밀번호는 하나의 사례로 간주됩니다.
 - 중요하지 않은 시스템의 경우 첫 번째 제출된 취약한 비밀번호 취약점만 승인됩니다.
 - 필수 시스템 및 핵심 비즈니스의 경우, 순서대로 첫 2개의 취약점이 승인됩니다.

• 전후 관계가 있는 연결성 취약점의 경우 여러 사례로 분할하여 제출시 악의적인 경우 DVP에서 해당 계정을 동결할 수 있습니다.

- IIS 서비스 거부 또는 slow_http_dos 등과 같은 서비스 중단을 유발할 수 있는 테스트를 실행하면 안됩니다.
- 서비스에 PC 사이트와 모바일 웹 사이트가 모두 있고 동일한 인터페이스와 소스 코드를 사용하는 경우 PC/App/ 사이트의 동일한 결함으로 취급되며 주동적으로 통합하여 제보할 경우 상황에 따라 포상금이 높아질 수 있습니다. 다른 제보자가 제출할 경우 타겟 기업이 해당 취약점을 패치하기 전에는 중복된 취약점으로 취급됩니다.
- 정보 유출의 취약점에 관해서는 실제 탈취 후 피해 사례가 발생할 수 있는 제출물은 심각하거나 높은 위험으로 간주됩니다. 주요 서비스 구성 또는 소스 코드 노출은 중간 위험으로 간주되고 이용하기 어렵거나 또는 핵심 비즈니스와 관련이 없으며 낮은 위험 또는 거부할 수 있습니다.

공급업체 보호

하나의 시스템에서 동일한 유형의 높은 위험 결함(예 : SQL injection 등)이 3개 이상 발견되면 심사위원은 해당 시스템이 보호 기능이 없다고 간주하고 이후에 제출된 동일 유형의 취약점은 강등 처리 됩니다.

취약점 심사 분쟁

취약점 보고서 처리 과정에 제보자가 만약 처리 과정 , 취약점 등급, 포상금 지급 등에 관하여 의견 충돌이 있을 경우 취약점 상세 페이지에서 메시지를 남기거나 DVP 담당 직원에게 연락하여 의견을 제기할 수 있습니다. DVP는 취약점 제보자의 이익을 최우선으로 하는 원칙으로 바운티 제공 업체와 적극적으로 협상할 것이며 필요할 경우 보안 업계의 제3자 기업들을 동원하여 공정한 결과를 발표하도록 할 것입니다.

참고

본 버그 바운티 규칙은 [先知众测漏洞定级标准](#) 제3의 사이트 버그 바운티 플랫폼 취약점 등급 기준을 참고로 작성되었습니다.