워게임도 모르는 우리가 버그 바운티를 성공한 이야기

발표자 : 화이트햇 스쿨 3기 양채한, 김도형

POC SECURITY

Agenda

- Who Am I
- 버그바운티?
- 버그바운티 할 때 제일 중요한 것
- 중간 퀴즈
- 버그바운티 접근법
- 참여 소감(앞으로 목표)
- 마무리 게임

Who Am I

김도형

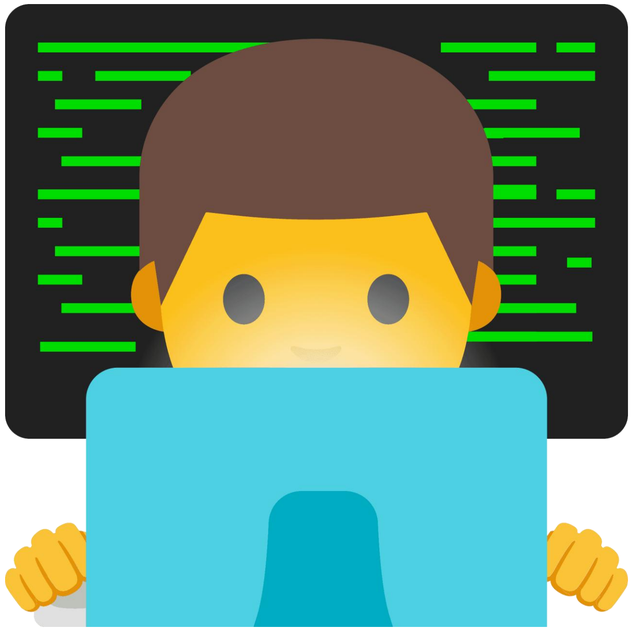
- 단국대학교부속소프트웨어고등학교 재학
- 교내 보안 동아리 부장
- 화이트햇 스쿨 3기
- 현대 오토에버 화이트 해커 양성교육

양채한

- 고려대학교 세종캠퍼스 인공지능사이버보안학과 재학
- Hspace 신규 해킹팀 운영진
- 화이트햇 스쿨 3기
- Cisco 인턴십 수료

POC SECURITY

버그 바운티란?



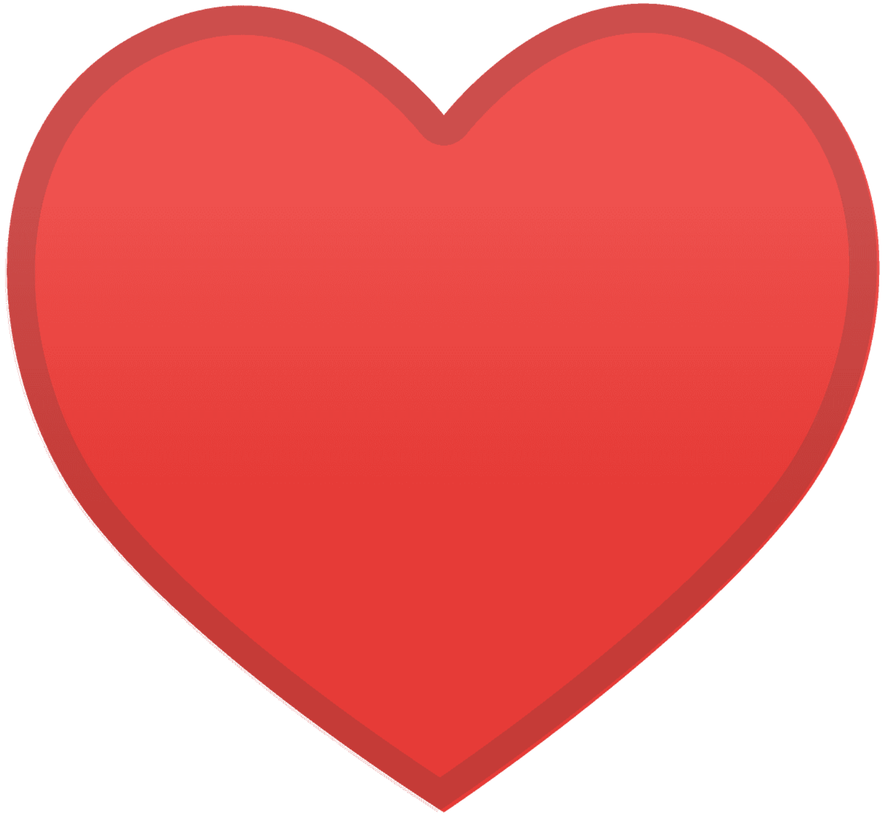
보안 취약점 신고포상제

기업의 서비스, 소프트웨어나 IT 인프라의 취약점을 발견하여
신고한 인원에게 포상금, 기타 보상을 지급하는
크라우드소싱기반의 침투 테스트 프로그램

POC SECURITY

버그 바운티에서 제일 중요한 것

버그 바운티에서 제일 중요한 것



버그 바운티 할 때 제일 중요한 것

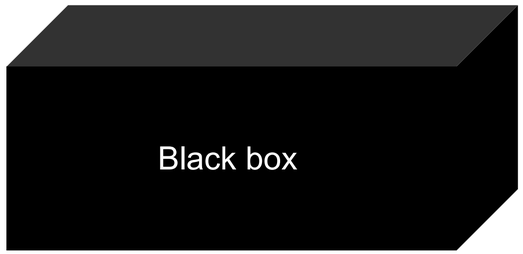
- 한국에서 발견된 보안 취약점에 부여되는 식별 번호

- 국내에서 제공해주는 넘버이기 때문에 본인이 기억하지 못하면 의미가 없을 수 있음.

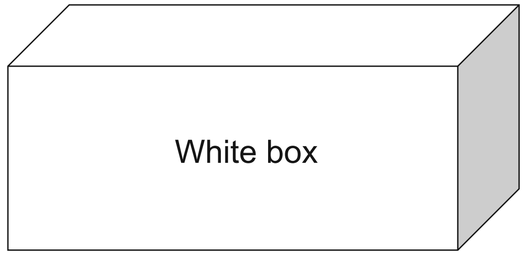
- 공개적으로 알려진 컴퓨터 보안 취약점에 대한 표준화된 식별 체계

- 해외에서 발급하는 식별번호로 KVE와 다르게 취약점 종류, 제보자 등이 검색 가능함.

버그 바운티 할 때 제일 중요한 것



웹 애플리케이션의 소스 코드를 보지 않고 외부 인터페이스나 구조를 분석하는 방법



개발된 소스 코드를 살펴보는 것을 통해 코드의 취약점을 찾는 방식

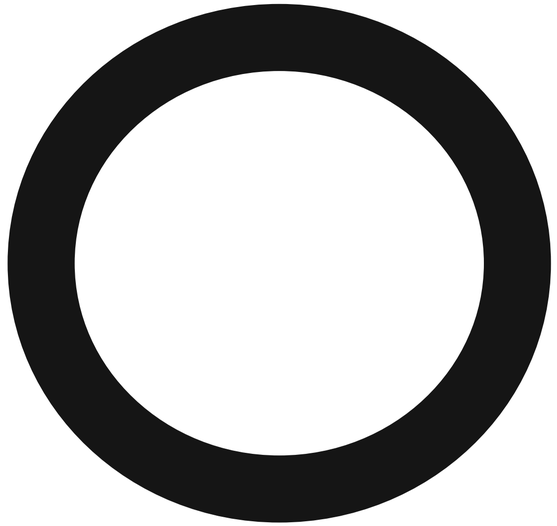
POC SECURITY

중간 퀴즈

1. 취약점을 제보하면 포상금이 있다?

중간 퀴즈

1. 취약점을 제보하면 포상금이 있다?



포상금은 5만원 이상 1천만원 이하의 범위에서 해당 정보보호 취약점으로 발생할 수 있는 침해사고의 범위·정도, 해당 정보보호 취약점의 악용의 용이성 등을 고려하여 과학기술정보통신부장관이 정하는 바에 따라 산정한다.

[정보통신망 이용촉진 및 정보보호 등에 관한 법률, 제47조의6]

POC SECURITY

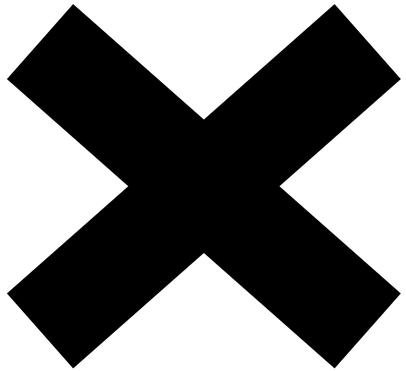
중간 퀴즈

2. 취약점을 제보하면 공개해도 된다?

POC SECURITY

중간 퀴즈

2. 취약점을 제보하면 공개해도 된다?



신고된 취약점은 포상 관련 평가, 취약점을 보완한 제품 개발을 위해 활용됩니다. 포상은 비공개된 취약점을 대상으로 하며 신고 후에도 아래와 같이 그 어떠한 목적으로도 KISA를 제외한 제3자에게 공개할 수 없습니다.

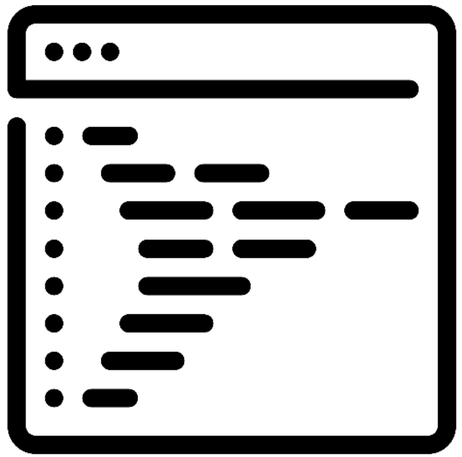
[KISA 취약점 정보 활용 및 비밀유지 조항]

POC SECURITY

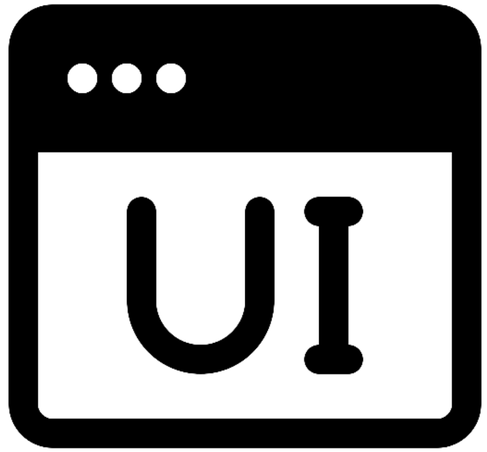
한번 해보자

http://43.200.178.100:8080/

버그바운티 접근법



Code auditing



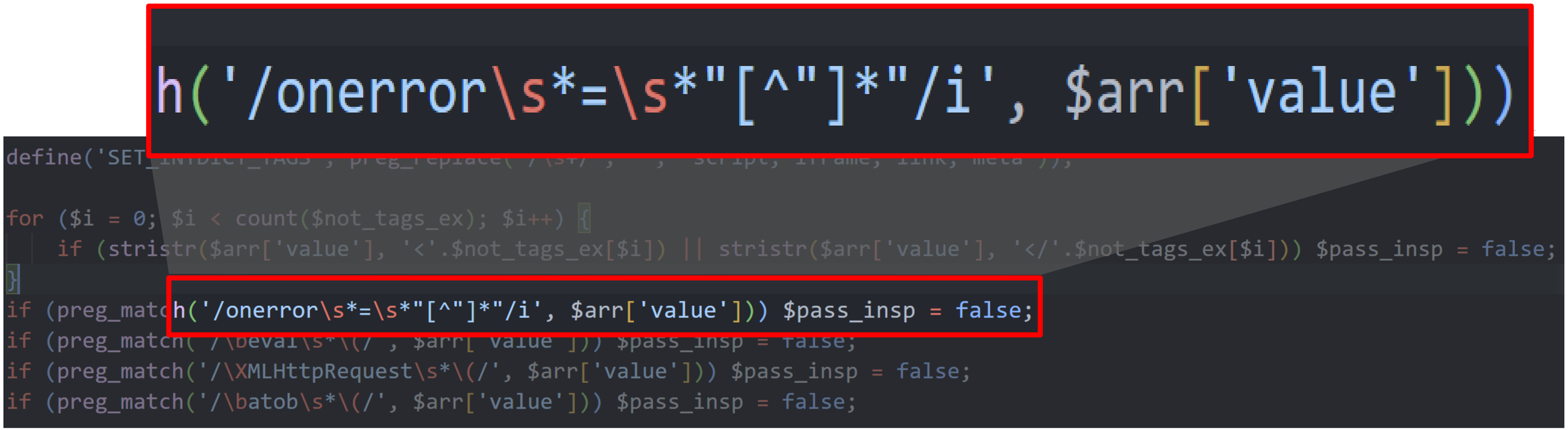
Vulnerable UI

버그바운티 접근법

```
define('SET_INTDICT_TAGS', preg_replace("/\s+/", "", 'script, iframe, link, meta'));

for ($i = 0; $i < count($not_tags_ex); $i++) {
    if (stristr($arr['value'], '<'.$not_tags_ex[$i]) || stristr($arr['value'], '</'.$not_tags_ex[$i])) $pass_insp = false;
}
if (preg_match('/onerror\s*=\s*"[^"]*"/i', $arr['value'])) $pass_insp = false;
if (preg_match('/\beval\s*\(/', $arr['value'])) $pass_insp = false;
if (preg_match('/\XMLHttpRequest\s*\(/', $arr['value'])) $pass_insp = false;
if (preg_match('/\batob\s*\(/', $arr['value'])) $pass_insp = false;
```

버그바운티 접근법



POC SECURITY

버그바운티 접근법

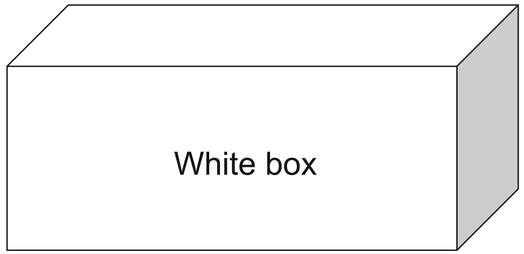
```
</head>
<body>
    <!--
        $sql = "SELECT board_id, board_title, board_date, user_id, board_locked
            FROM free_board
            WHERE `{$category}` LIKE '%{$search_term}%'
            ORDER BY board_id DESC";
-->
<nav class="navbar navbar-expand-lg navbar-dark bg-dark">
```

버그바운티 접근법

Code auditing

[장점]

- 웹사이트에 대한 이해도 향상
- 보안 개발 관점에서 강점



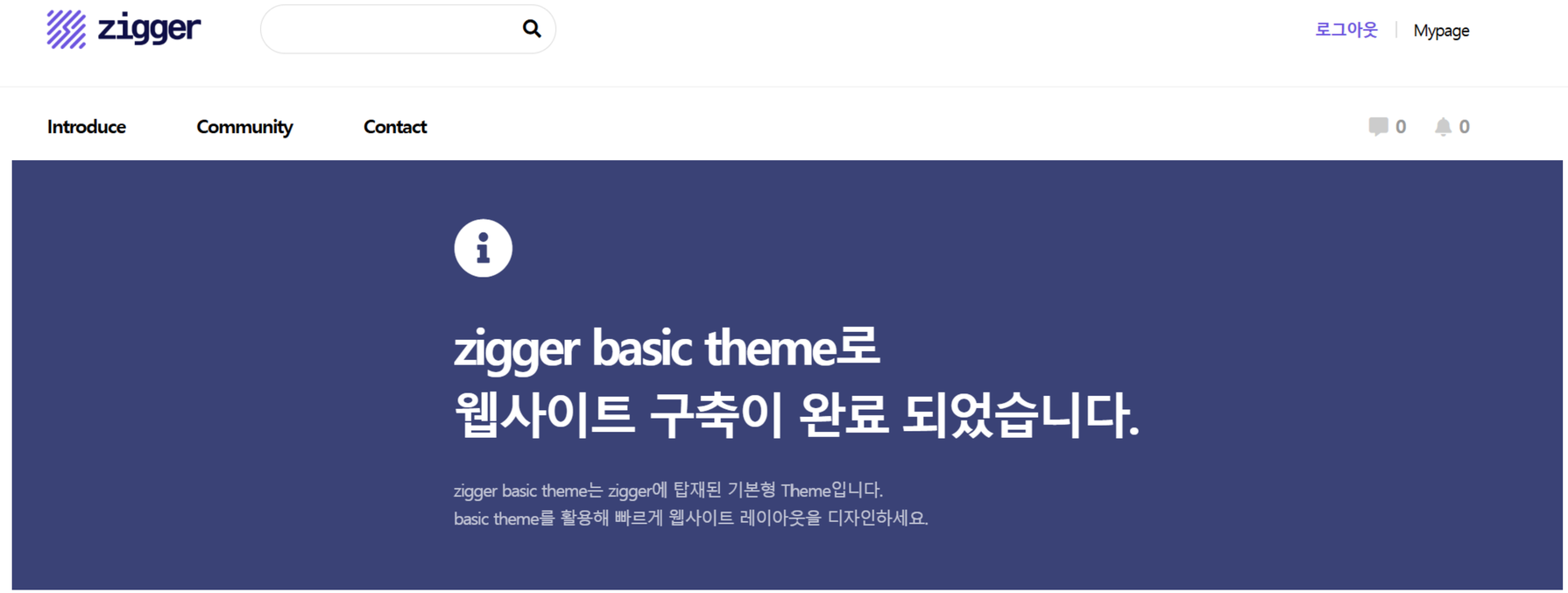
버그바운티 접근법

Code auditing

[단점]

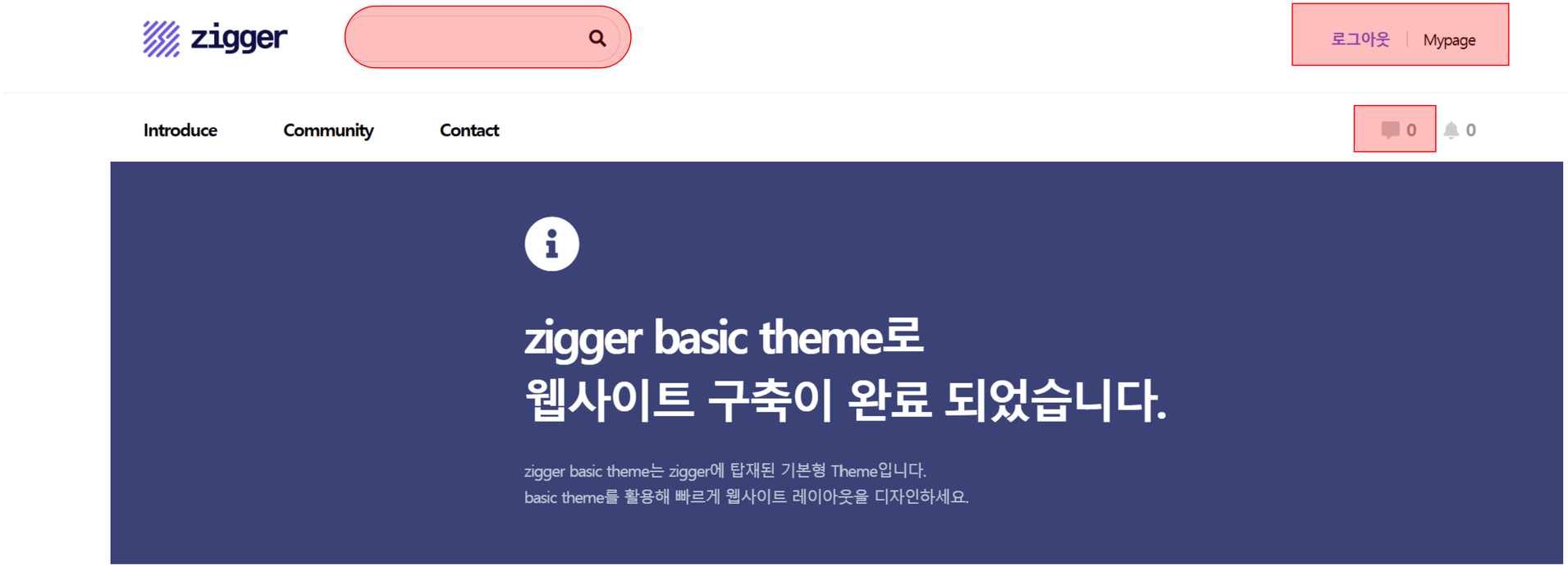
- 코드 전체를 이해하는 데 시간 소모
- 실제 응답 기반 공격 효과나 파급력 측정이 어려움

버그바운티 접근법



POC SECURITY

버그바운티 접근법



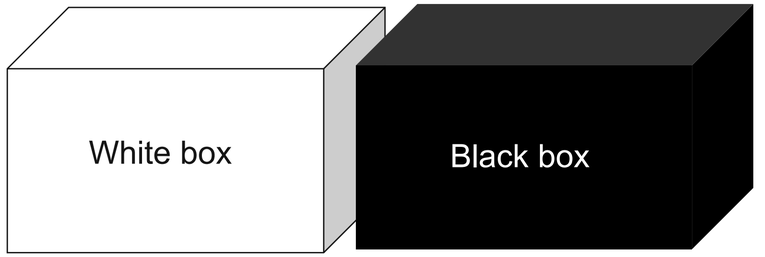
POC SECURITY

버그바운티 접근법

Vulnerable UI

[장점]

- 실제 요청에 따라 반응을 바로 확인 가능
- 사용자 관점에서 웹사이트 이상 동작 확인



버그바운티 접근법

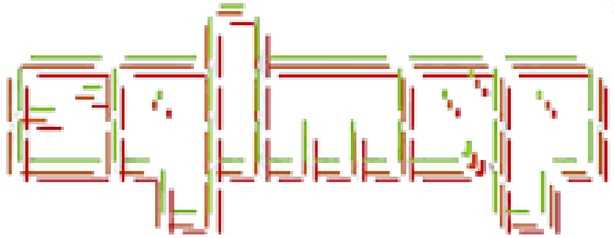
Vulnerable UI

[단점]

- UI에서 드러나지 않는 로직, 내부 API 탐지 어려움
- 근본 원인 추적 시 코드 필요

버그바운티 접근법

OWASP
Zed Attack Proxy



POC SECURITY

버그바운티 접근법

POC SECURITY

버그바운티 접근법

POC SECURITY

버그바운티 접근법

버그바운티 접근법

Program Scope

- `*.airbnb.com`
- All localized airbnb sites (e.g., `es.airbnb.com`, `it.airbnb.com`)

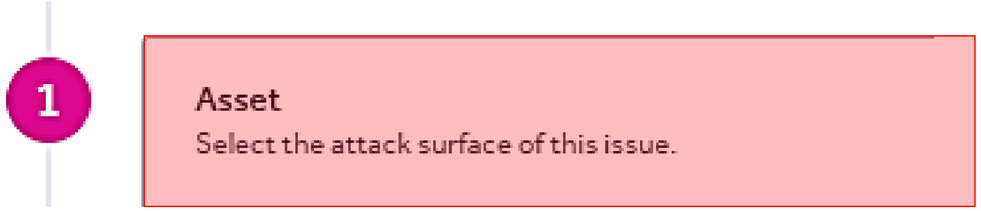
HackerOne Core Ineligible Findings

Vulnerabilities that may require hazardous testing. This type of testing must never be attempted unless explicitly authorized:

- Issues relating to excessive traffic/requests (e.g., DoS, DDoS)
- Any other issues where testing may affect the availability of systems
- Social engineering attacks (e.g., phishing, opening support requests)
- Attacks that are noisy to users or admins (e.g., spamming notifications or forms)
- Attacks against physical facilities

보고서 작성

보고서 작성



발생 url (scope)

Attackpoint (취약한 변수명)

보고서 작성

1 **Asset**
Select the attack surface of this issue.

2 **Weakness**
Select the type of the potential issue you have discovered.
Can't pick just one? Select the best match or submit a separate report for each distinct weakness.

공격 유형(취약점)

보고서 작성

1 **Asset**

Select the attack surface of this issue.

2 **Weakness**

Select the type of the potential issue you have discovered.

Can't pick just one? Select the best match or submit a separate report for each distinct weakness.

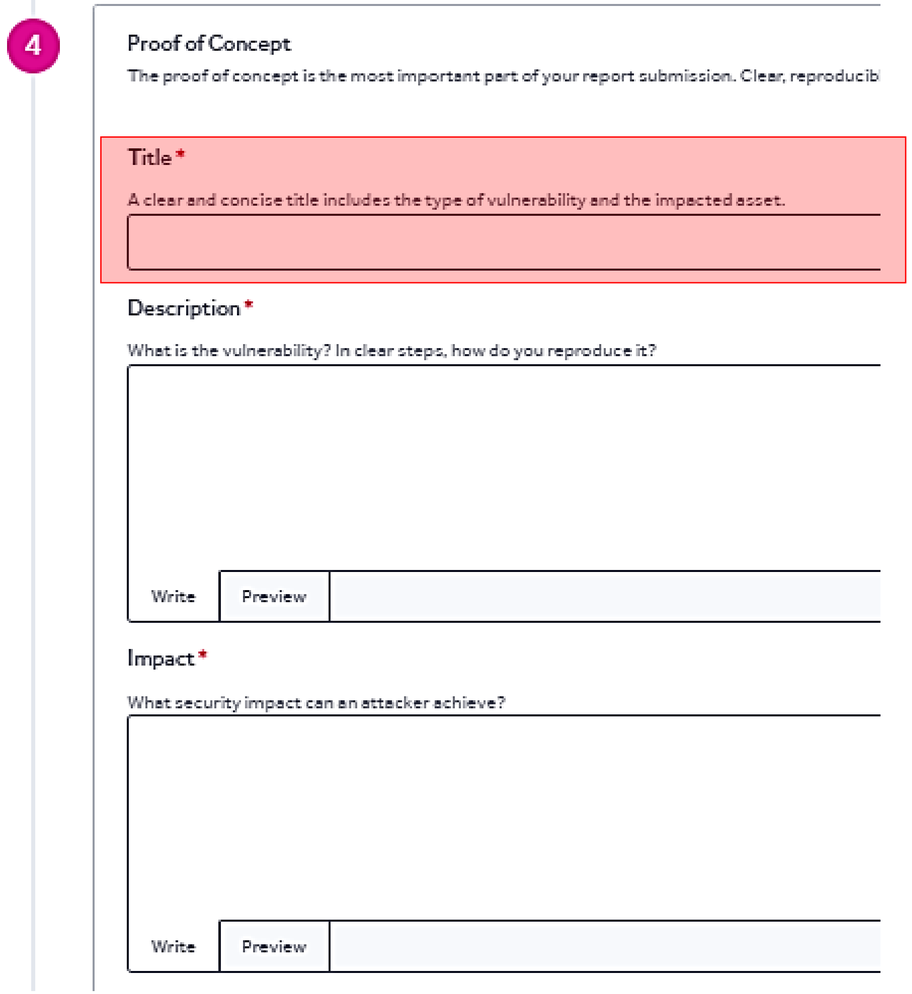
3 **Severity (optional)**

Estimate the severity of this issue.

- ○ Submit report without severity
- ◉ Submit report with severity

CVSS
COMMON VULNERABILITY SCORING SYSTEM

보고서 작성

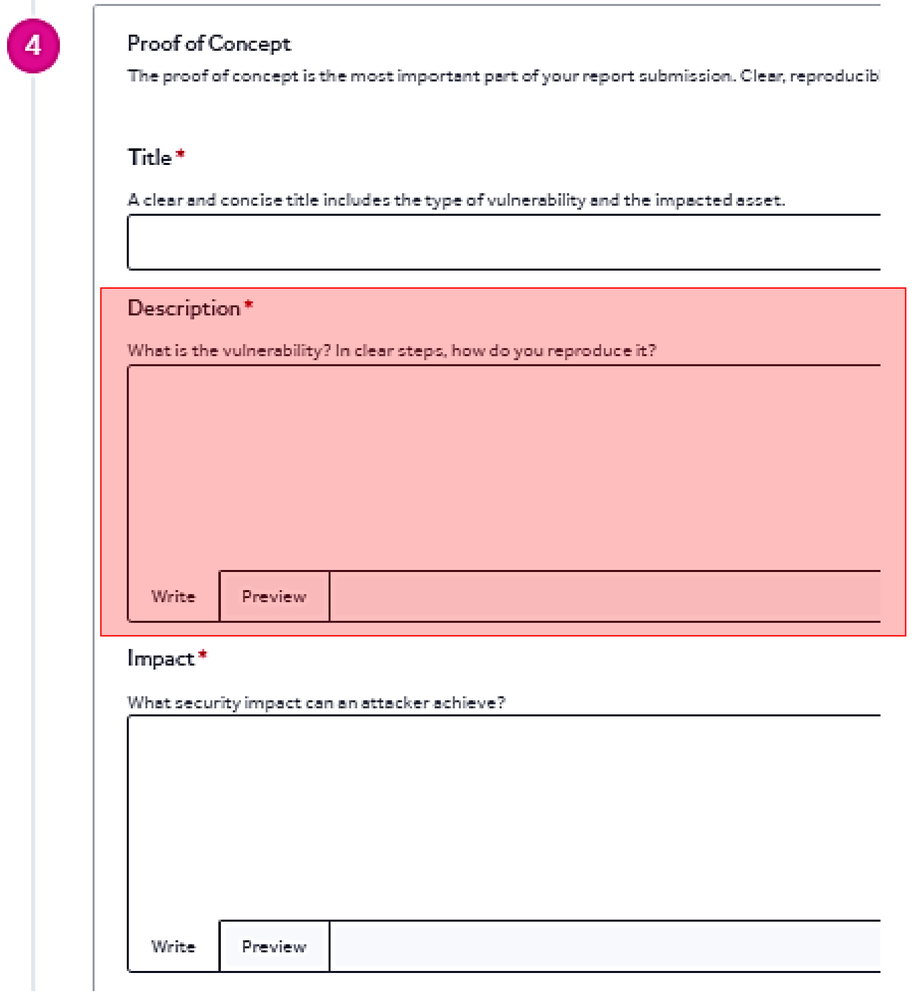


리포트 제목 : 발견 위치 + 공격 유형 (+ 공격 영향)

예) University IPMS 공지사항(view.do) HTML Injection을 통한 Stored XSS

POC SECURITY

보고서 작성



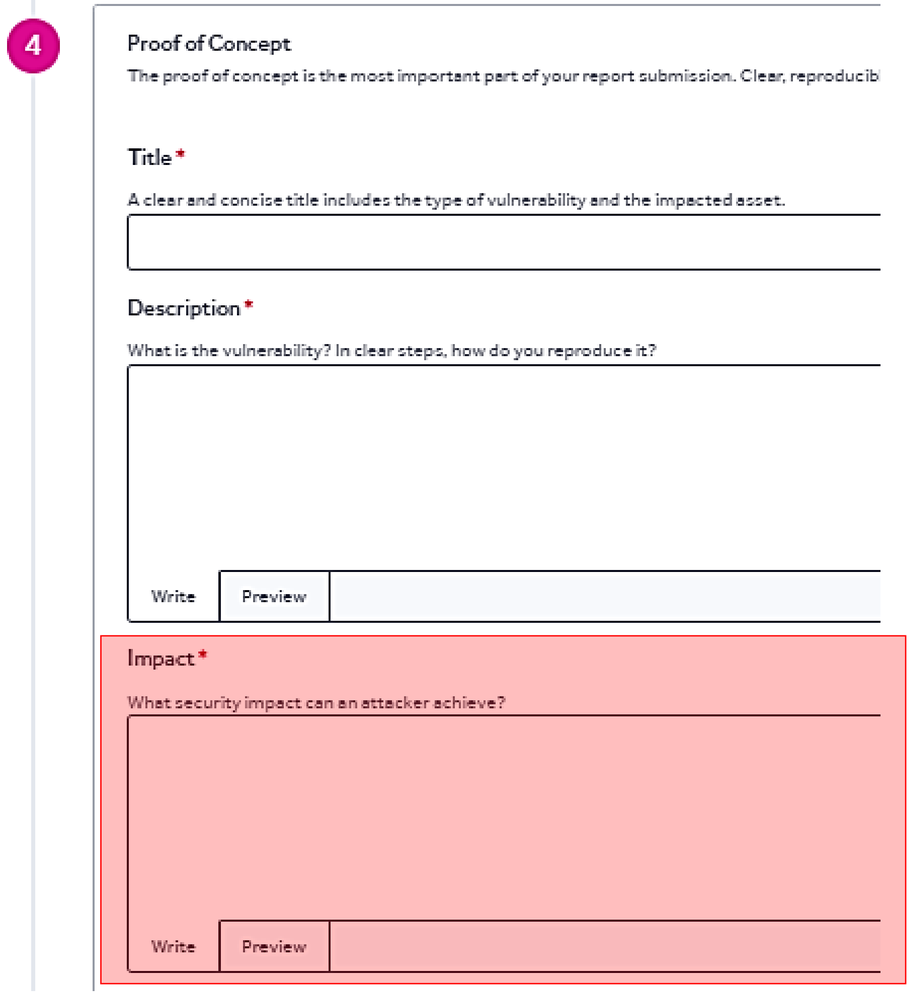
취약점 발견 방법

발생 원인

취약점 증명(PoC 디버깅 과정)

POC SECURITY

보고서 작성



취약점 악용 시나리오 (파급력)

조치방안

POC SECURITY

보고서 작성

안녕. 제보 고마워.

리포트 내용 대로 해봤는데, 정확하게 재현이 어렵다;;

리포트 보완해줘

보고서 작성

안녕. 제보 고마워.

리포트 내용 대로 해봤는데, 정확하게 재현이 어렵다;;

리포트 보완해줘

POC SECURITY

보고서 작성

안녕. 제보 고마워.

리포트 내용 대로 해봤는데, 정확하게 재현이 어렵다;;

리포트 보완해줘

(수정된 리포트)

보고서 작성

안녕. 제보 고마워.

리포트 내용 대로 해봤는데, 정확하게 재현이 어렵다;;

리포트 보완해줘

(수정된 리포트)

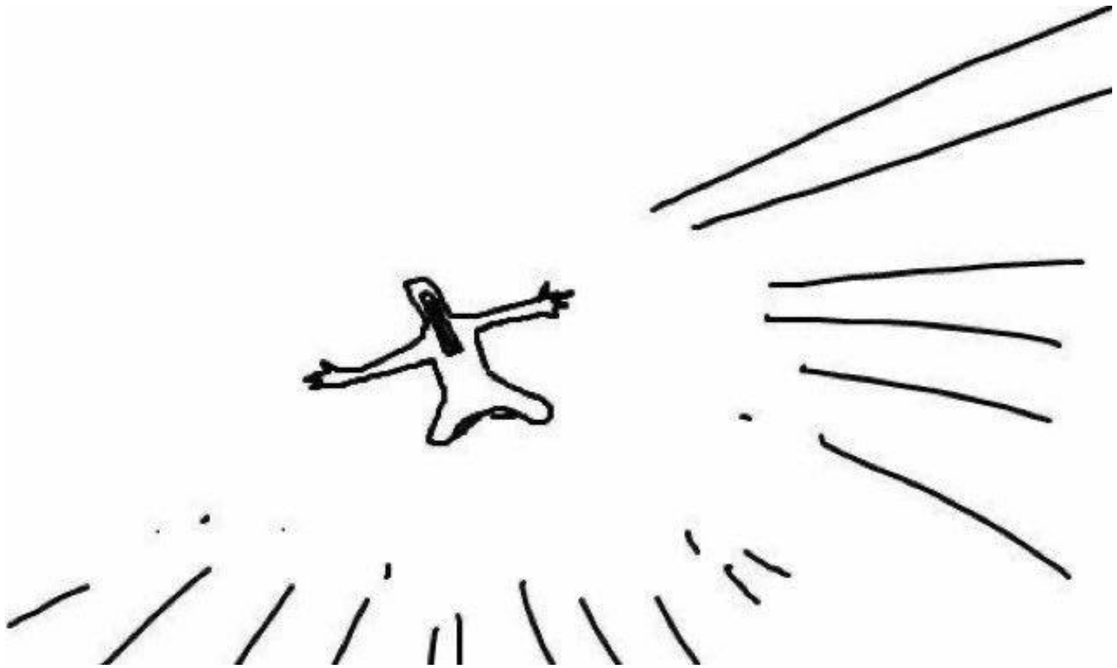
XSS 삽입 되며, 메인 페이지 접속 시 실행되는 것 확인 했어.

보고서 작성

안녕. 제보 고마워.

리포트 내용 대로 해봤는데, 정확하게 재현이 어렵다;;

리포트 보완해줘



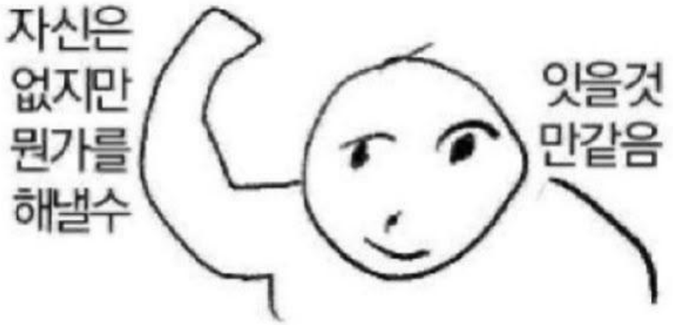
XSS 삽입 되며, 메인 페이지 접속 시 실행되는 것 확인 했어.

소감

1. 생각보다 취약한 웹 사이트가 많다.

2. 공부하고 싶은 취약점이 생겼다.

3. 워 게임은 중요하다.



감사합니다.

QnA

발표자 : 화이트햇 스쿨 3기 양채한, 김도형

POC SECURITY