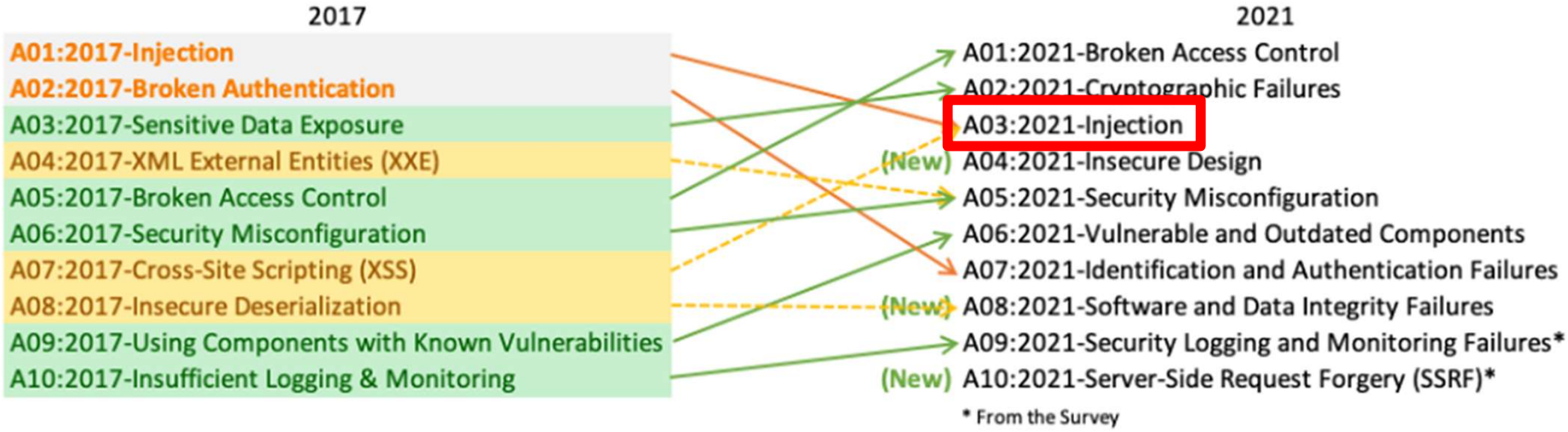
XSS(Cross Site Scripting) 취약점

XSS(Cross Site Scripting) 취약점

XSS 취약점 소개

- **클라이언트 스크립트를 이용하여 사용자에게 특정 행위를 하도록 만드는 취약점**
  - 대표적인 클라이언트 스크립트 언어 : JavaScript, VBScript



XSS(Cross Site Scripting) 취약점

XSS 취약점 소개

- **클라이언트 스크립트를 이용하여 사용자에게 특정 행위를 하도록 만드는 취약점**
  - 대표적인 클라이언트 스크립트 언어 : JavaScript, VBScript

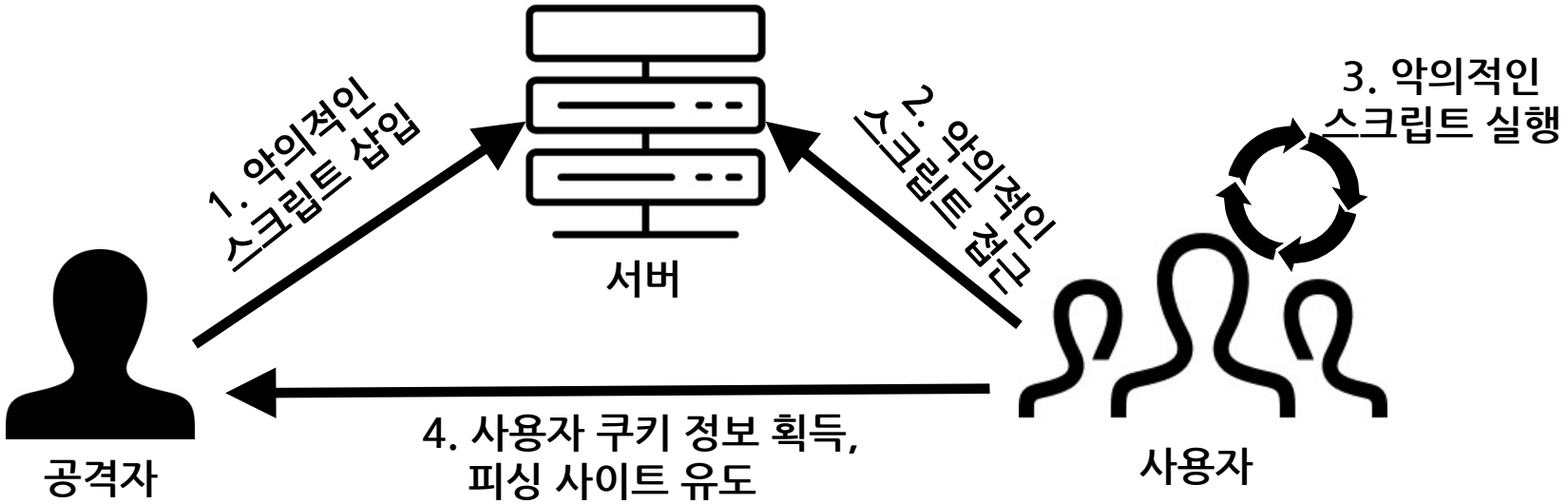
Web 취약점 분석·평가 항목

점검항목	항목 중요도	항목코드
버퍼 오버플로우		
포맷스트링		
LDAP 인젝션		
운영체제 명령 실행		
SQL 인젝션		
SSI 인젝션		
XPath 인젝션		
디렉터리 인덱싱		
정보 누출		
악성 콘텐츠		
크로스사이트 스크립팅		
약한 문자열 강도		
불충분한 인증		
취약한 패스워드 복구		
크로스사이트 리퀘스트 변조(CSRF)	상	CF
세션 예측	상	SE
불충분한 인가	상	IN
불충분한 세션 만료	상	SC
세션 고정	상	SF
자동화 공격	상	AU
프로세스 검증 누락	상	PV
파일 업로드	상	FU
파일 다운로드	상	FD
관리자 페이지 노출	상	AE
경로 추적	상	PT
위치 공개	상	PL
데이터 평문 전송	상	SN
쿠키 변조	상	CC

XSS(Cross Site Scripting) 취약점

XSS 취약점 공격 유형

- 악성코드 배포
- 다른 사용자 권한 획득
- 피싱 사이트 유도



XSS(Cross Site Scripting) 취약점

Stored XSS 취약점 공격

- 데이터베이스에 저장되어 실행되는 공격
- 게시판 글 작성, 쪽지 보내기, 1:1문의 등에서 발생

Reflected XSS 취약점 공격

- 사용자 요청 데이터에 의해 실행되는 공격
- 데이터베이스에 저장되지 않고,
  사용자 요청으로 인해 발생하므로 특정 링크를 클릭하도록 유도해야 함
- 대표적으로 검색 기능 등에서 발생

XSS(Cross Site Scripting) 취약점

실습

- 공격 실습
- 우회 기법 실습
- BeEF 활용한 사회공학적 기법 실습

XSS(Cross Site Scripting) 취약점

BeEF 활용

- BeEF는 The Browser Exploitation Framework의 약자
- 웹 브라우저에 초점을 맞춘 침투 테스트 도구
- 하나 이상의 웹 브라우저를 연결하여 지시된 명령 모듈을 시작하고 브라우저 컨텍스트 내에서 시스템에 대한 추가 공격을 시작하기 위한 교두보로 사용

XSS(Cross Site Scripting) 취약점

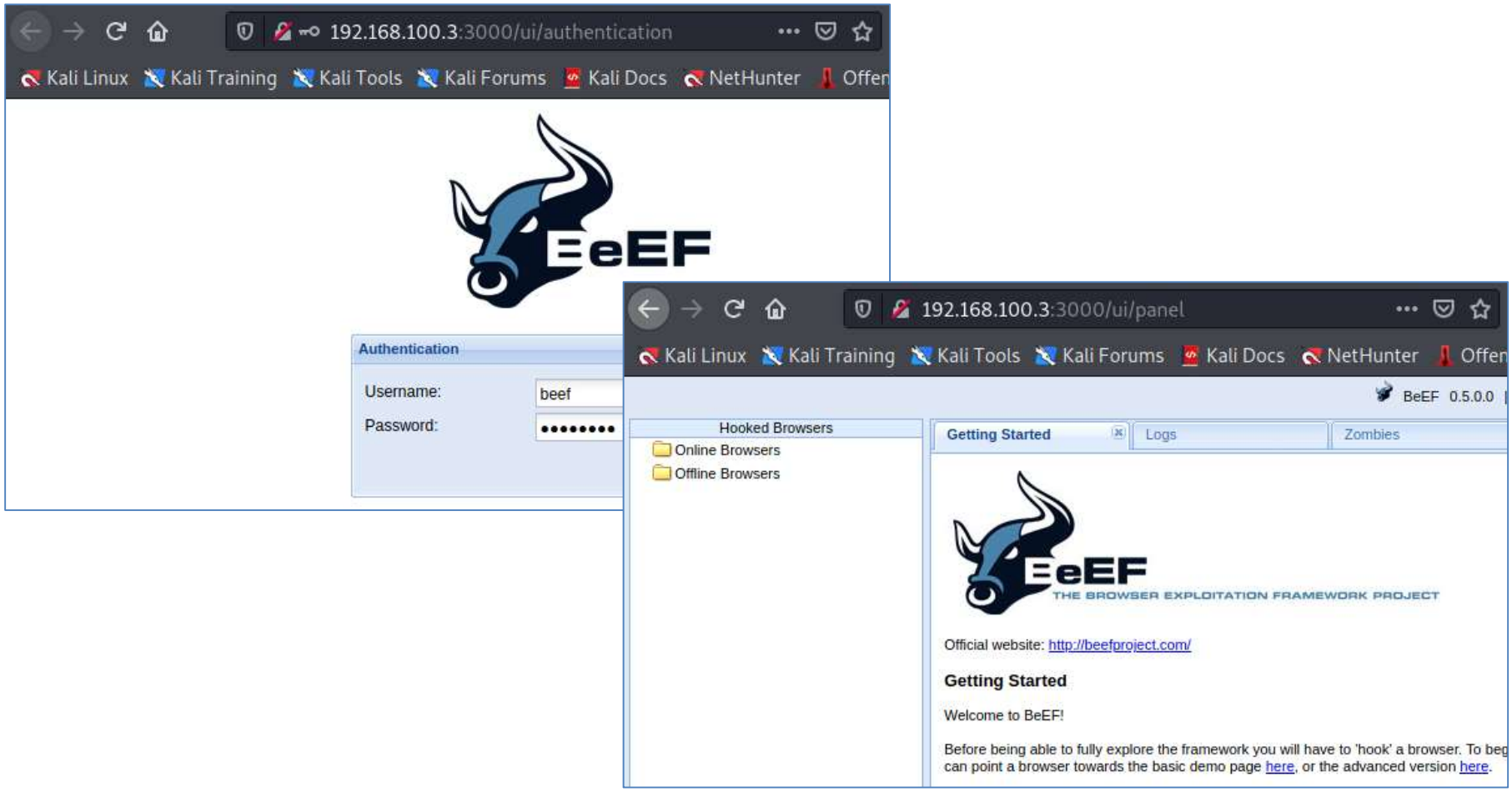
BeEF 설치 및 실행

sudo apt install beef-xss -y
sudo ./beef-xss
변경할 비밀번호 입력(잘 기억해두세요!)
firefox http://kali_linux_ip:3000/ui/panel

```
[ 9:50:49][*] 303 modules enabled.
[ 9:50:49][*] 2 network interfaces were detected.
[ 9:50:49][*] running on network interface: 127.0.0.1
[ 9:50:49]    |   Hook URL: http://127.0.0.1:3000/hook.js
[ 9:50:49]    |_  UI URL:   http://127.0.0.1:3000/ui/panel
[ 9:50:49][*] running on network interface: 192.168.100.3
[ 9:50:49]    |   Hook URL: http://192.168.100.3:3000/hook.js
[ 9:50:49]    |_  UI URL:   http://192.168.100.3:3000/ui/panel
[ 9:50:49][*] RESTful API key: d8768be3017653cdbeb10dd21e0b911da665d43b
[ 9:50:49][!] [GeoIP] Could not find MaxMind GeoIP database: '/var/lib/GeoIP/GeoLite2-City.mmdb'
[ 9:50:49]    |_  Run geoipupdate to install
[ 9:50:49][*] HTTP Proxy: http://127.0.0.1:6789
[ 9:50:49][*] BeEF server started (press control+c to stop)
```

XSS(Cross Site Scripting) 취약점

BeEF 설치 및 실행

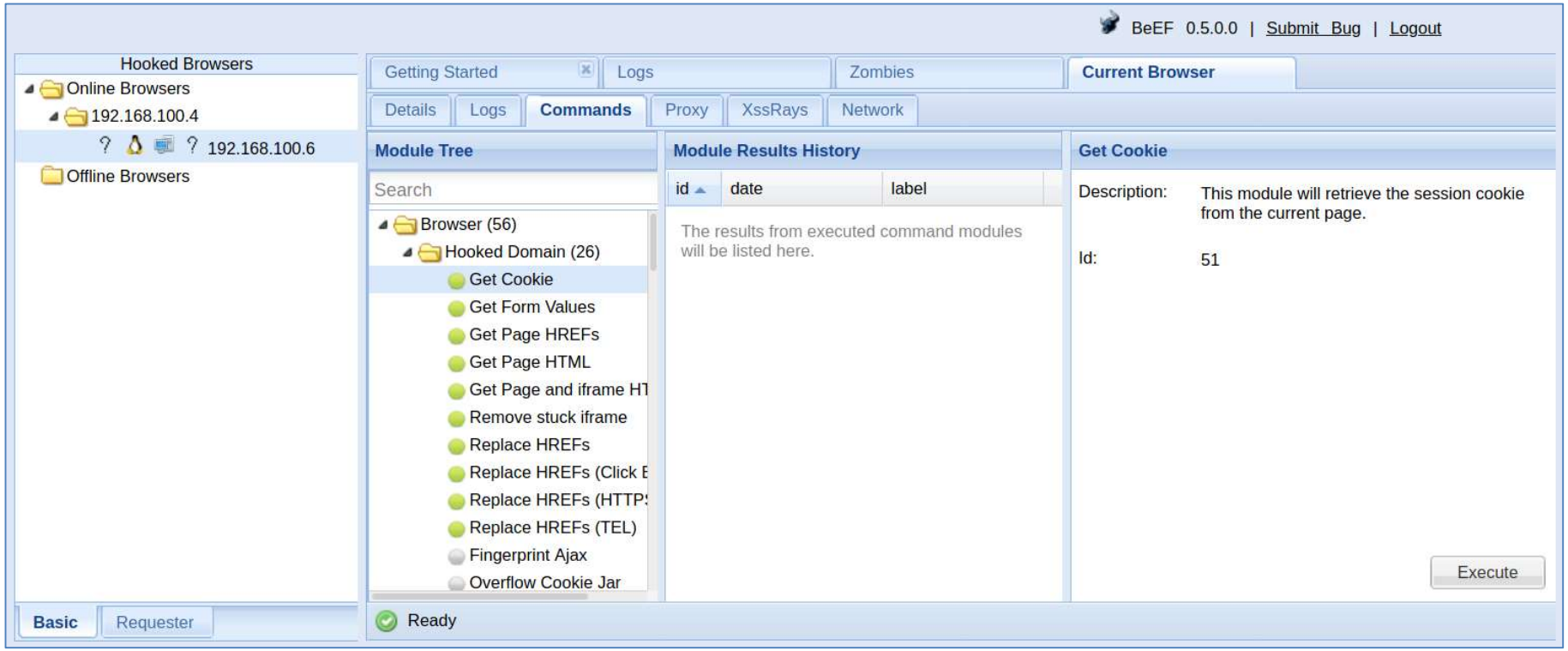


XSS(Cross Site Scripting) 취약점

BeEF 활용

XSS(Cross Site Scripting) 취약점

BeEF 활용

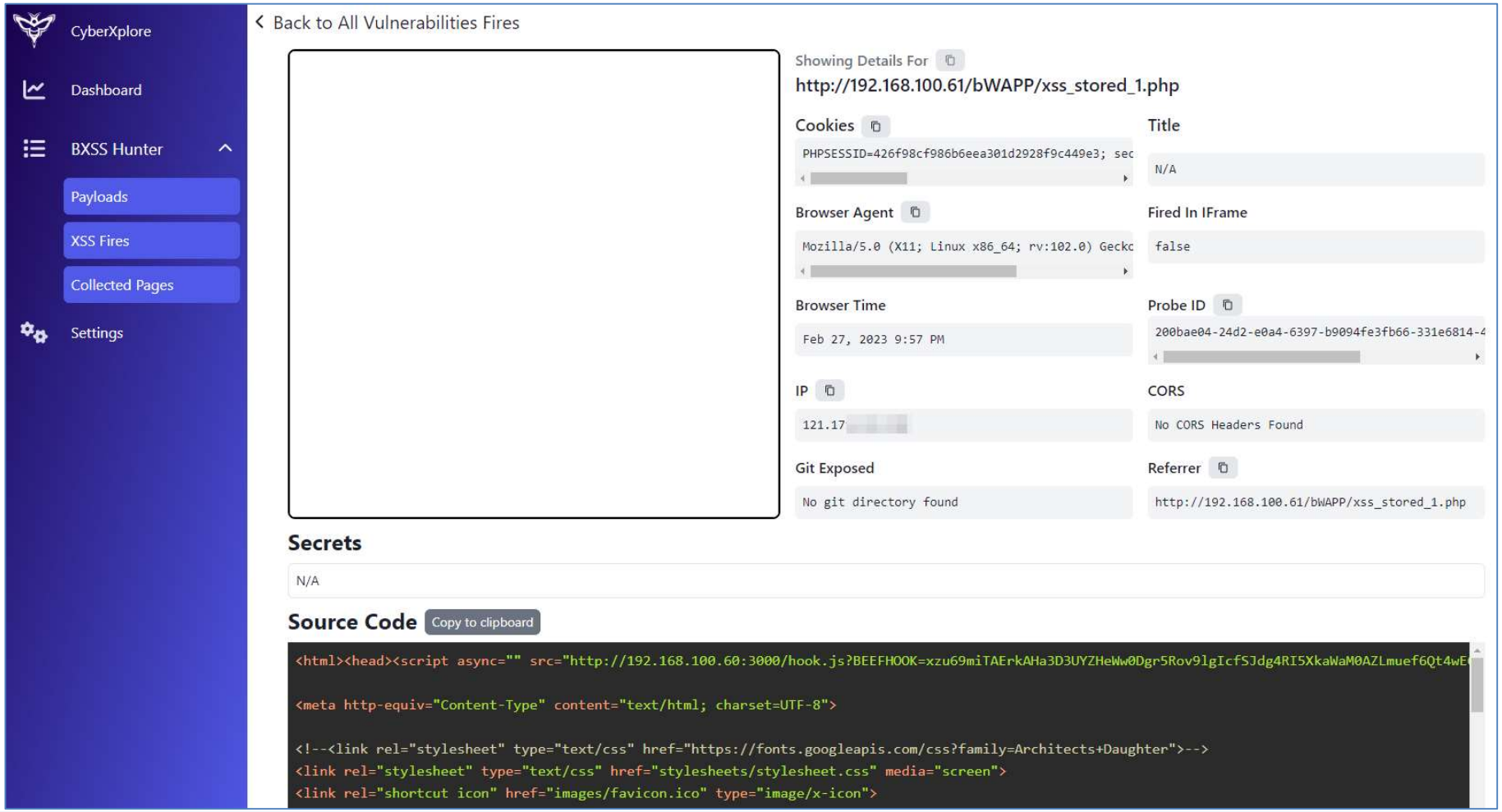


Green(초록)	목표 시스템에 유효한 공격: 사용자에게 보이지 않음
Orange(주황)	목표 시스템에 유효한 공격: 사용자에게 권한 확인과 같은 메세지 박스 등이 보여 지기 때문에 사용자가 탐지할 수 있음
Grey(회색)	목표 시스템에 유효한 공격인지 검증 필요
Red(빨간색)	목표 시스템에 유효한 공격이 아님

XSS(Cross Site Scripting) 취약점

BXSS Hunter 활용

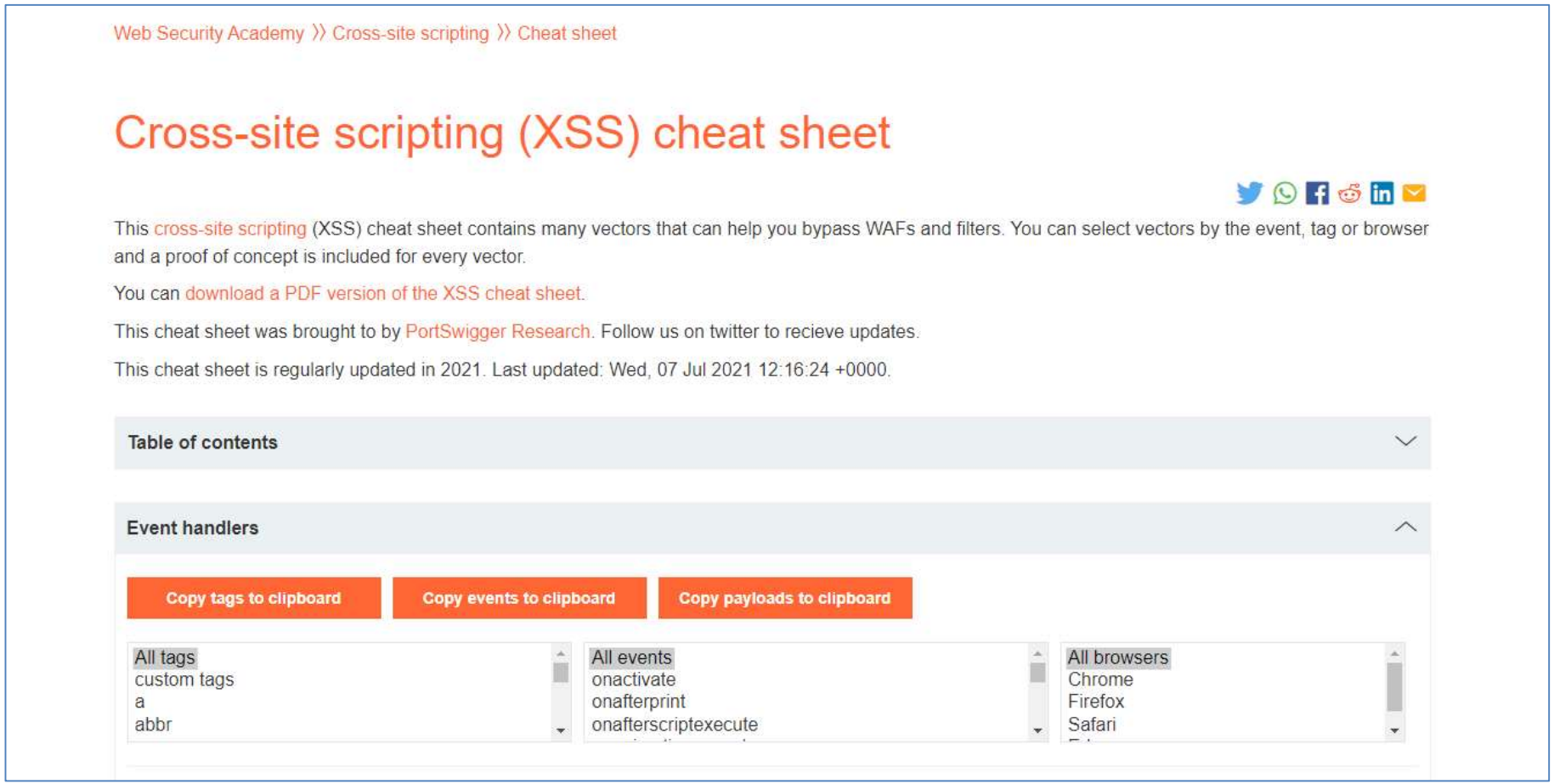
- 악성 수집 서버를 활용하여 사용자의 정보 획득



XSS(Cross Site Scripting) 취약점

Cross-site scripting (XSS) cheat sheet

- https://portswigger.net/web-security/cross-site-scripting/cheat-sheet



XSS 취약점 대응방안

대응방안 : 입력 값에 대한 길이 제한

http://test.co.kr/board_idx=“><script>alert(document.cookie);</script>

이렇게 길게 허용할 필요 있나?

?????

board_write_ok_sec.asp

```
71  Dim ls_Name:    If HasValue(GMFORM.Form("name")) Then ls_Name = Mid(GMFORM.Form("name"),1,10) Else ls_Name = ""
72  Dim ls_Email:   If HasValue(GMFORM.Form("email")) Then ls_Email = Mid(GMFORM.Form("email"),1,20) Else ls_Email = ""
73    Dim ls_Content: If HasValue(GMFORM.Form("content")) Then ls_Content = GMFORM.Form("content") Else ls_Content = ""
74    Dim li_Html:    If HasValue(GMFORM.Form("bHtml")) Then li_Html = GMFORM.Form("bHtml") Else li_Html = 0
75    If (CInt(li_Html)=1) Then
76        ls_Content = GMFORM.Form("TextContent")
77    ElseIf (CInt(li_Html)=2) Then
78        ls_Content = GMFORM.Form("HtmlContent")
79    End If
80  Dim ls_Title:   If HasValue(GMFORM.Form("title")) Then ls_Title = Mid(GMFORM.Form("title"),1,10) Else ls_Title = ""
```

	idx	code	title	name	pwd	email
1	688	1149530558	1234567890	1234567890	1	12345678901234567890

XSS 취약점 대응방안

대응방안 : 입력 값 필터링

```
public static String strTags(String source)
{
String [] oldString = {"<html", "</html", "<meta", ....중략...."</style", "script:", "cookie", "document."};
String [] newString = {"<hHTML", "</hHTML", "<hMETA", " .....중략... "script :", "cook!e","d0cument ."};
return strReplaceIgnoreCase(source, oldString, newString);
}
```

board_write_ok_sec.asp

```
71  Dim ls_Name:    If HasValue(GMFORM.Form("name")) Then ls_Name = GMFC
72  Dim ls_Email:   If HasValue(GMFORM.Form("email")) Then ls_Email = GM
73  Dim ls_Content: If HasValue(GMFORM.Form("content")) Then ls_Content
74  Dim li_Html:    If HasValue(GMFORM.Form("bHtml")) Then li_Html = GME
75  If (CInt(li_Html)=1) Then
76      ls_Content = GMFORM.Form("TextContent")
77  ElseIf (CInt(li_Html)=2) Then
78      ls_Content = GMFORM.Form("HtmlContent")
79      ls_Content = Replace(ls_Content,"<script
80      ls_Content = Replace(ls_Content,"</scrip
81  End if
```

보안 > 서비스 ?
보안 < 서비스 ?

XSS 취약점 대응방안

대응방안 : 입력 값 필터링

변환 대상	변환 값	변환 대상	변환 값
<	&lt;	)	&#41;
>	&gt;	(	&#40;
#	&#35;	&	&#38;
"	&quot;	'	&#x27;
/	&#x2F;		

XSS 취약점 대응방안

대응방안 : 입력 값 필터링

- /var/www/bWAPP/xss_stored_1.php

```
while($row = $recordset->fetch_object())
{

    if($_COOKIE["security_level"] == "2")
    {



?>
        <tr height="40">

            <td align="center"><?php echo $row->id; ?></td>
            <td><?php echo $row->owner; ?></td>
            <td><?php echo $row->date; ?></td>
            <td><?php echo xss_check_3($row->entry); ?></td>

        </tr>

<?php
```

XSS 취약점 대응방안

대응방안 : 입력 값 필터링

- /var/www/bWAPP/functions_external.php

```
function xss_check_3($data, $encoding = "UTF-8")
{

    // htmlspecialchars - converts special characters to HTML entities
    // '&' (ampersand) becomes '&amp;'
    // '"' (double quote) becomes '&quot;' when ENT_NOQUOTES is not set
    // "'" (single quote) becomes '&#039;' (or &apos;) only when ENT_QUOTES is set
    // '<' (less than) becomes '&lt;'
    // '>' (greater than) becomes '&gt;'

    return htmlspecialchars($data, ENT_QUOTES, $encoding);

}
```