

whoami

- ◇ pentester @  PRAUDIT
- ◇ Prauditors csapattag
 - ◇ Hacktivity CTF kétszeres első helyezett
 - ◇ Global Cyberlympics 2012 Európa bajnok
- ◇ több Hacktivity, három DEF CON előadás



miért matek?

- ◇ segítséget kértek MATLAB-hoz
 - ◇ köszí az ötletet, Heni :)
- ◇ hatalmas software, rengeteg támadási felület
 - ◇ web szerverek,
 - ◇ cloud integráció,
 - ◇ clusterezés, stb.

tartalom

- ◆ Bang - MATLAB exec függvény
- ◆ The P-Files - MATLAB "titkosított" scriptek visszafejtése
- ◆ XORrow and Joy - MATLAB Mobile titkosított kommunikáció visszafejtése
- ◆ P.S I Pwn You - távoli parancsfuttatás egy MATLAB servlet-en keresztül
- ◆ EngineServlet-ering Disasters - mint az előző, de alap beállításokkal nem megy
- ◆ The Forged new Cookie - MATLAB Production Server auth bypass
- ◆ Dynamic Blaster - Mathematica "Dynamics" védelmek kijátszása
- ◆ Ergo Proxy - SOCKS4 proxy Mathematica-ban implementálva
- ◆ The Net - Wolfram Lightweight Grid Manager auth bypass + RCE
- ◆ Protocol - WSTP protokollt érintő sebezhetőségek
- ◆ The XML Connection - Maple XXE
- ◆ Remote Control - Maple remote control server/

servlet-ek a web.xml-ből

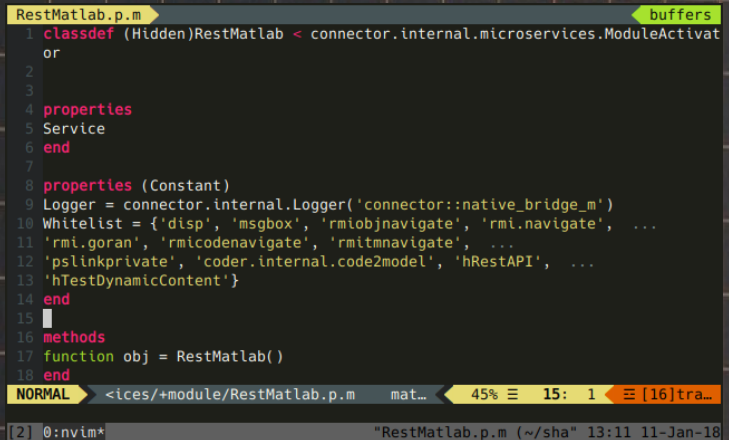
- ◆ AddOnServlet
- ◆ NonceGeneratorServlet
- ◆ EngineServlet
- ◆ PairingKeyJsonServlet
- ◆ MatlabServlet
- ◆ UploadServlet
- ◆ CometdServletHack

servlet-ek a web.xml-ből

- ◊ AddOnServlet
- ◊ NonceGeneratorServlet
- ◊ **EngineServlet**
- ◊ PairingKeyJsonServlet
- ◊ **MatlabServlet**
- ◊ UploadServlet
- ◊ CometdServletHack

P.S. I Pwn You

- ◆ MatlabServlet GET request-ben érkező kifejezéseket futtat
- ◆ localhost-ra korlátozott
- ◆ kifejezés whitelist



```
RestMatlab.p.m buffers
1 classdef (Hidden)RestMatlab < connector.internal.microservices.ModuleActivat
  or
2
3
4 properties
5 Service
6 end
7
8 properties (Constant)
9 Logger = connector.internal.Logger('connector::native_bridge_m')
10 Whitelist = {'disp', 'msgbox', 'rmlobjnavigate', 'rmi.navigate', ...
11 'rmi.goran', 'rmicodenavigate', 'rmitmnavigate', ...
12 'pslinkprivate', 'coder.internal.code2model', 'hRestAPI', ...
13 'hTestDynamicContent'}
14 end
15
16 methods
17 function obj = RestMatlab()
18 end
NORMAL <ices/+module/RestMatlab.p.m mat... 45% 15: 1 [16]tra...
[2] 0:nvim* "RestMatlab.p.m (~/sha" 13:11 11-Jan-18
```


P.S. I Pwn You

- ❖ a pslinkprivate egy wrapper a feval körül
- ❖ tetszőleges MATLAB parancs futtatása e-mail-en, weboldalon keresztül
- ❖ [http://localhost:31415/matlab/feval/pslinkprivate?arguments=\["system","calc"\]](http://localhost:31415/matlab/feval/pslinkprivate?arguments=[)

```
pslinkprivate.p.m buffers
1 function varargout = pslinkprivate(function_name, varargin)
2
3 [varargout{1: nargout}] = feval(function_name, varargin{1: end});
4
~
~
NORMAL <lyspace/pslink/pslink/pslinkprivate.p.m mat... 100% 4: 1
[4] 0:nvim* "pslinkprivate.p.m (~/" 11:44 13-Jan-18
```

The Net

- ◆ Lightweight Grid Manager
 - ◆ a Wolfram Research cluster megoldása
- ◆ Tomcat alapú web app a Mathematica kernelek kezeléséhez
- ◆ változtatásokhoz autentikációt igényel
- ◆ kernelek viszont azonosítás nélkül is indíthatók
 - ◆ védelem: IP whitelist

The Net



Tech Store
KnowledgeBase

All Topics ▼

SEARCH

Hardware & Software ▼

- [Student Computing Checklist](#)
- [Tech Store Catalog](#)
- [Campus Software Library](#)
- [WISC Software Catalog](#)
- [Apple Custom Builds](#)
- [Dell Custom Builds](#)
- [Shop@UW](#)

How To ▼

- [Schedule an Appointment](#)
- [Back up your files](#)
- [Install Office](#)
- [Install Antivirus](#)
- [Connect to UWNNet](#)
- [ResNet Registration](#)

Connect With Us ▼

- [Call \(608\)264-3648](#)
- [Find us on Facebook](#)
- [Follow us on Twitter](#)
- [See our YouTube channel](#)
- [Email Our Sales Team](#)

Support for Mathematica downloaded from the Campus Shared Library

You will request an activation key which will generate an email from Wolfram.

You will need to create a login on the Wolfram website to do this.

For Students please use this link:

[Student Mathematica Installations](#)

For Faculty, Staff & Departments please use this link:

[Faculty, Staff & Department Installations](#)

The generated email will have a link to download the media, or you can access it through the Campus Software Library site.

Mathematica Site License Number: L3288-3573

Links:

Support Forum:

<http://community.wolfram.com/>

Eligible users can download this software from the [Campus Software Library](#)

To better assist you with any issues that may occur when downloading software, all downloads are linked to a NetID.

The Net

```
web.xml buffers
487 <security-constraint>
488   <web-resource-collection>
489     <web-resource-name>ManagerWebApp</web-resource-name>
490     <description>Resources requiring administrative access</descript
491   ion>
492     <url-pattern>/ManagerProtected/*</url-pattern>
493     <url-pattern>/ManagerProtected</url-pattern>
494     <url-pattern>/Login/*</url-pattern>
495     <url-pattern>/Status/CloseKernel</url-pattern>
496     <url-pattern>/Status/CloseAllKernels</url-pattern>
497     <url-pattern>/KernelSettings/ServiceConfiguration/Save</url-patt
498   ern>
499     <url-pattern>/ServerSettings/Save</url-pattern>
500     <url-pattern>/Licensing/*</url-pattern>
501     <url-pattern>/Logging/SupportFile/Create</url-pattern>
502     <url-pattern>/Logging/SupportFile/Download</url-pattern>
503     <http-method>GET</http-method>
504     <http-method>POST</http-method>
505   </web-resource-collection>
```

The Net

```
server.xml buffers
130         clientAuth="false" sslProtocol="TLS" />
131     -->
132
133     <!-- Define an AJP 1.3 Connector on port 2374 -->
134     <Connector port="2374" protocol="AJP/1.3" redirectPort="2373" />
135
136
137     <!-- An Engine represents the entry point (within Catalina) that process
es
NORMAL conf/server.xml xml 64% 134: 1 [113]tr...
[2] 0:nvim*M 1:zsh- "server.xml (~/.shared/" 17:32 17-Jan-18
```


The Net

◆ HEAD autentikáció nélkül

- ◆ HEAD /WolframLightweightGrid/ServerSettings/Save?IPFilter= HTTP/1.1

◆ IP szűrő kijátszása AJP-vel

- ◆ a szűrő alkalmazás szinten van implementálva
- ◆ az AJP hazudik a forrás IP-ről

◆ +1: command injection

- ◆ HEAD
/WolframLightweightGrid/KernelSettings/ServiceConfiguration/Save?KernelCommand=false+`id`
HTTP/1.1

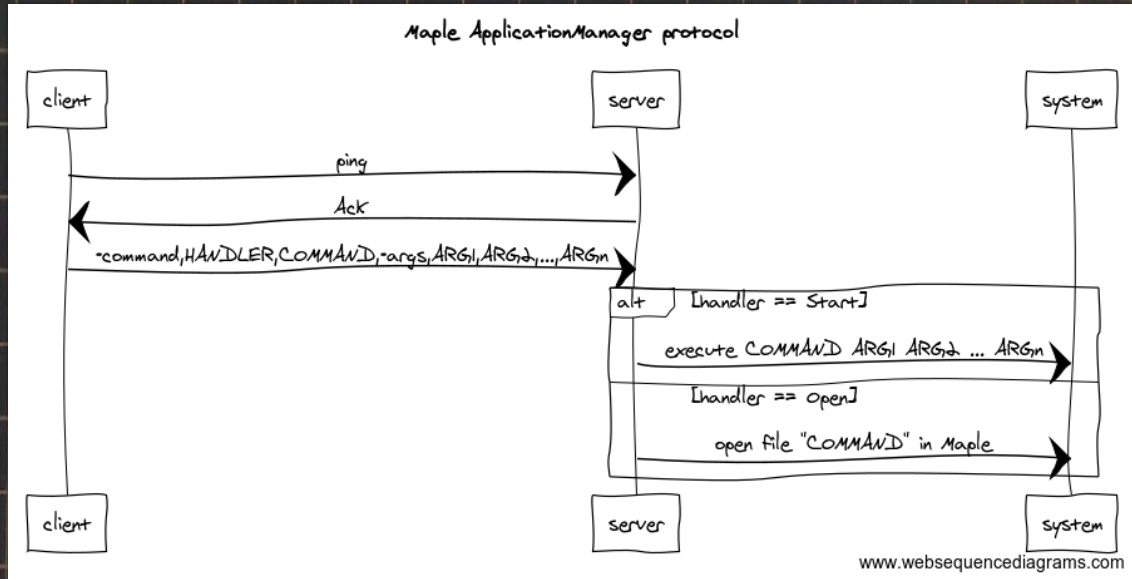
The XML Connection

- ◊ a Maple dokumentumok XML fájlok
- ◊ meglepetés: External Entity Expansion
- ◊ az áldozatnak meg kell nyitnia egy fájlt

Ports Wide Shut

- ◇ két szolgáltatás figyel a 0.0.0.0 IP-n
 - ◇ TCP/50170
 - ◇ TCP/19991
- ◇ az első csak olvas egy számot a socket-ről
 - ◇ a kernel így közli a launcher-rel, hogy hol figyel
- ◇ a második egy remote control szerver

Remote Control



Remote Control

- ◇ két magától értetődő kihasználási mód
- ◇ az Autoexecute használata
 - ◇ szükséges felhasználói beavatkozás
 - ◇ képes parancsokat futtatni

Remote Control

- ◇ két magától értetődő kihasználási mód
- ◇ az Autoexecute használata
 - ◇ szükséges felhasználói beavatkozás
 - ◇ képes parancsokat futtatni
- ◇ kombinálás az XXE-vel
 - ◇ nem szükséges felhasználói beavatkozás
 - ◇ csak SSRF és fájlok ellopása lehetséges

$$d = \epsilon m_0$$

Contact

- ◇ név: Tamas Szakaly
- ◇ mail: tamas.szakaly@praudit.hu
sghctoma@gmail.com
- ◇ PGP fingerprint:
4E1F 5E17 7A73 2C29 229A CD0B 4F2D 6CD0 9039 2984
- ◇ twitter: @sghctoma
- ◇ GitHub: <https://github.com/sghctoma>