

Burp Extension Writing

Workshop - OWASP Bay Area

THANKS

/me: Sanoop Thomas @s4n7h0

- Chapter Moderator at Null Singapore
- 8+ years in Information Security
- Created Halcyon IDE – an IDE for Nmap Script Developers
 - <https://halcyon-ide.org/>
- Host SecTools Podcast at Infosec Campus
 - <https://infosecampus.com/>
- Barely get time to write blogpost, but presentations/talks are updated
 - <https://devilslab.in/>
- Presented at OWASP India, Nullcon Goa, HITBGSEC, ROOTCON, BlackHat Arsenal (USA, Asia) and Defcon

Key Points to Learning

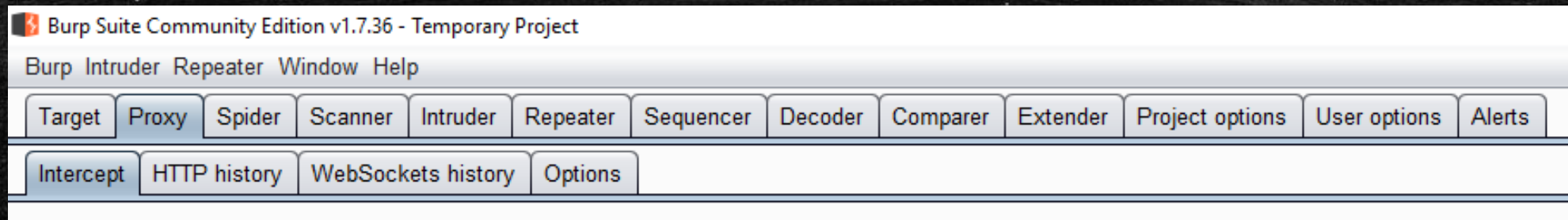
- Ask questions when in doubt
- Experiment with test cases
- Continue writing code after this session

Let's get started..

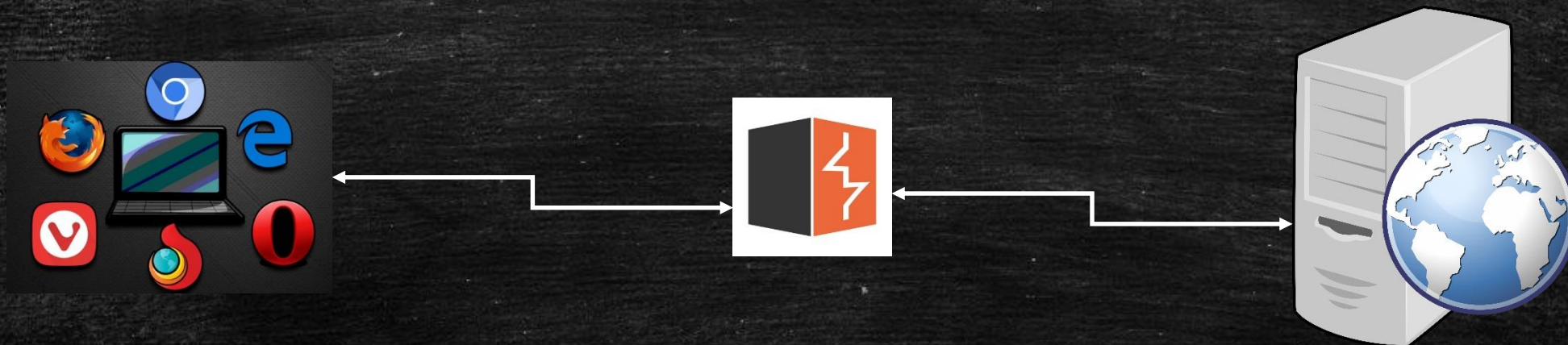
- Quick intro to Burp Suite
- Know the Features
- Understand extender APIs
- Write extensions
 - Java
 - Python

Burp Introduction

- One of the de-facto tool for AppSec
- Proxy at first, but compliments a bunch of other capabilities



How Burp Works



Practice Time

Exercise #: get started with burp

Burp Extensions

- API to Burp functionalities
- Extensions can be written in:
 - Java
 - Python (JPython)
 - Ruby (JRuby)

Extender Capabilities

- Process and modify HTTP requests and responses for all Burp tools.
- Access key runtime data, such as the Proxy history, target site map, and Scanner issues.
- Initiate actions like scanning and spidering.
- Implement custom scan checks and register scan issues.
- Customize the placement of attack insertion points within scanned requests.
- Provide custom Intruder payloads and payload processors.

Extender Capabilities (cont..)

- Query and update the Suite-wide target scope.
- Query and update the session handling cookie jar.
- Implement custom session handling actions.
- Add custom tabs and context menu items to Burp's user interface.
- Use Burp's native HTTP message editor within your own user interface.

Extender Capabilities (cont..)

- Customize Burp's HTTP message editor to handle data formats that Burp does not natively support.
- Analyze HTTP requests and responses to obtain headers, parameters, cookies, etc.
- Build, modify and issue HTTP requests and retrieve responses.
- Read and modify Burp's configuration settings.
- Save and restore Burp's state.

BApp Store

The BApp Store contains Burp extensions that have been written by users of Burp Suite, to extend Burp's capabilities.

Name	Installed	Rating	Popularity	Last updated	Detail
.NET Beautifier		☆☆☆☆☆	██████████	23 Jan 2017	
Active Scant++		☆☆☆☆☆	██████████	04 Sep 2018	Requires Burp...
Add & Track Custom Iss...		☆☆☆☆☆	██████████	16 Jan 2018	Requires Burp...
Add Custom Header		☆☆☆☆☆	██████████	18 Sep 2018	
Additional CSRF Checks		☆☆☆☆☆	██████████	09 Jan 2018	
Additional Scanner Checks		☆☆☆☆☆	██████████	12 Jan 2017	Requires Burp...
AES Payloads		☆☆☆☆☆	██████████	28 Aug 2015	Requires Burp...
Attack Surface Detector		☆☆☆☆☆	██████████	10 Oct 2018	
AuthMatrix		☆☆☆☆☆	██████████	02 Feb 2018	
Authz		☆☆☆☆☆	██████████	01 Jul 2014	
Auto Repeater		☆☆☆☆☆	██████████	04 Apr 2018	
Autorize		☆☆☆☆☆	██████████	09 Jul 2018	
AWS Security Checks		☆☆☆☆☆	██████████	18 Jan 2018	Requires Burp...
Backslash Powered Sca...		☆☆☆☆☆	██████████	10 Aug 2018	Requires Burp...
Batch Scan Report Gene...		☆☆☆☆☆	██████████	03 Oct 2017	Requires Burp...
Blazer		☆☆☆☆☆	██████████	01 Feb 2017	
Bradamsa		☆☆☆☆☆	██████████	02 Jul 2014	
Brida, Burp to Frida bridge		☆☆☆☆☆	██████████	04 Oct 2018	
Browser Repeater		☆☆☆☆☆	██████████	01 Jul 2014	
Buby		☆☆☆☆☆	██████████	14 Feb 2017	Requires Burp...
Burp Chat		☆☆☆☆☆	██████████	23 Jan 2017	
Burp CSJ		☆☆☆☆☆	██████████	23 Mar 2015	
Burp-hash		☆☆☆☆☆	██████████	28 Aug 2015	Requires Burp...
BurpSmartBuster		☆☆☆☆☆	██████████	22 Jan 2018	
Bypass WAF		☆☆☆☆☆	██████████	29 Mar 2017	
Carbonator		☆☆☆☆☆	██████████	23 Jan 2017	Requires Burp...
Cloud Storage Tester		☆☆☆☆☆	██████████	05 Oct 2017	Requires Burp...
CMS Scanner		☆☆☆☆☆	██████████	03 Oct 2017	Requires Burp...
CO2		☆☆☆☆☆	██████████	20 Jul 2017	
Code Dx		☆☆☆☆☆	██████████	06 Jun 2018	Requires Burp...
Collaborator Everywhere		☆☆☆☆☆	██████████	21 May 2018	Requires Burp...
Command Injection Attac...		☆☆☆☆☆	██████████	27 Jun 2018	
Commentator		☆☆☆☆☆	██████████	16 Jul 2018	
Content Type Converter		☆☆☆☆☆	██████████	23 Jan 2017	
Copy as Node Request		☆☆☆☆☆	██████████	10 Nov 2017	
Copy as PowerShell Req...		☆☆☆☆☆	██████████	31 Jan 2018	

.NET Beautifier

This extension beautifies .NET requests to make the body parameters more human readable. Built-in parameters like `__VIEWSTATE` have their values masked. Form field names have the auto-generated part of their name removed.

Requests are only beautified in contexts where they can be edited, such as the Proxy intercept view.

For example, a .NET request with the following body:

```
__VIEWSTATE=#2oiRIHfiohsdoigjKLA5g3ghajklg3SDGsjdg1SDJg9SDJGsdgjSGJDD
Sasdfja9sdjfasdfja0sdfja
... [1000 lines later] ...
&ctl100%24ctl100%24InnerContentPlaceHolder%24Element_42%24ctl100%24FrmLo
gin%24TxtUsername_intern
al=username&ctl100%24ctl100%24InnerContentPlaceHolder%24Element_42%24ct
100%24FrmLogin%24TxtPass
word_internal=password&ctl100%24ctl100%24InnerContentPlaceHolder%24Elem
ent_42%24ctl100%24BtnLogi
n=Login
```

will be displayed like this:

```
__VIEWSTATE=&TxtUsername_internal=username&TxtPassword_internal=passw
ords&BtnLogin=Login
```

This is done without compromising the integrity of the underlying message so you can edit parameter values and the request will be correctly reconstructed. You can also send the beautified messages to other Burp tools, and they will be handled correctly.

Author: Nadeem Douba
Version: 0.3
Source: <https://github.com/portswigger/dotnet-beautifier>
Updated: 23 Jan 2017

Rating: ☆☆☆☆☆

Popularity: ██████████

<https://portswigger.net/bappstore>

Lab Setup

- Burp Suite Community Edition
 - <https://portswigger.net/burp/>
- Extender APIs
- Test Application
- Development Environments
 - Java
 - Python

Extender API

The screenshot shows the Burp Suite Community Edition v1.7.36 interface. The main window displays the 'Burp Extender APIs' section. On the left, a list of API interfaces is shown, with 'IBurpCollaboratorClientContext' selected. The right pane displays the corresponding Java code for this interface, including package declarations, imports, and Javadoc comments. The code defines the 'IBurpCollaboratorClientContext' interface with methods for generating payloads and retrieving interactions. At the bottom, there are buttons for 'Save interface files' and 'Save Javadoc files', and a search bar with '0 matches'.

```
package burp;

/**
 * @(#) IBurpCollaboratorClientContext.java
 *
 * Copyright PortSwigger Ltd. All rights reserved.
 *
 * This code may be used to extend the functionality of Burp Suite Community Edition
 * and Burp Suite Professional, provided that this usage does not violate the
 * license terms for those products.
 */
import java.util.List;

/**
 * This interface represents an instance of a Burp Collaborator client context,
 * which can be used to generate Burp Collaborator payloads and poll the
 * Collaborator server for any network interactions that result from using those
 * payloads. Extensions can obtain new instances of this class by calling
 * <code>IBurpExtenderCallbacks.createBurpCollaboratorClientContext()</code>.
 * Note that each Burp Collaborator client context is tied to the Collaborator
 * server configuration that was in place at the time the context was created.
 */
public interface IBurpCollaboratorClientContext
{
    /**
     * This method is used to generate new Burp Collaborator payloads.
     *
     * @param includeCollaboratorServerLocation Specifies whether to include the
     * Collaborator server location in the generated payload.
     * @return The payload that was generated.
     *
     * @throws IllegalStateException if Burp Collaborator is disabled
     */
    String generatePayload(boolean includeCollaboratorServerLocation);














    /**
     * This method is used to retrieve all interactions received by the
     * Collaborator server resulting from payloads that were generated for this
     * context.
     *
     * @return The Collaborator interactions that have occurred resulting from
     * payloads that were generated for this context.
     */
    List<IBurpCollaboratorInteraction> getInteractions();
}
```

Setup for Java

- Create a project in your favourite IDE
- Create a package "burp" and copy all Extender API files
- Create a java class "BurpExtender"

- Download NetBeans project
 - <https://portswigger.net/burp/extender/examples/emptyextension.zip>
- This workshop will be using NetBeans version 8.2












File Edit View Navigate Source Refactor Run Debug Profile Team Tools Window Help

      <default config>       

Projects × Files Services — **BurpExtender.java** ×

Navigator

- BurpExtender
 - Source Packages
 - burp
 - BurpExtender.java**
 - IBurpExtender.java
 - IBurpExtenderCallbacks.java
 - IContextMenuFactory.java
 - IContextMenuItemInvocation.java
 - ICookie.java
 - IExtensionHelpers.java
 - IExtensionStateListener.java
 - IHttpListener.java
 - IHttpRequestResponse.java
 - IHttpRequestResponsePersisted.java
 - IHttpRequestResponseWithMarkers.java
 - IHttpService.java

Source History           

```
1 package burp;
2
3
4 public class BurpExtender implements IBurpExtender
5 {
6
7     @Override
8     public void registerExtenderCallbacks(IBurpExtenderCallbacks callbacks)
9     {
10         // your extension code here
11     }
12 }
13
14
```

Setup for Python

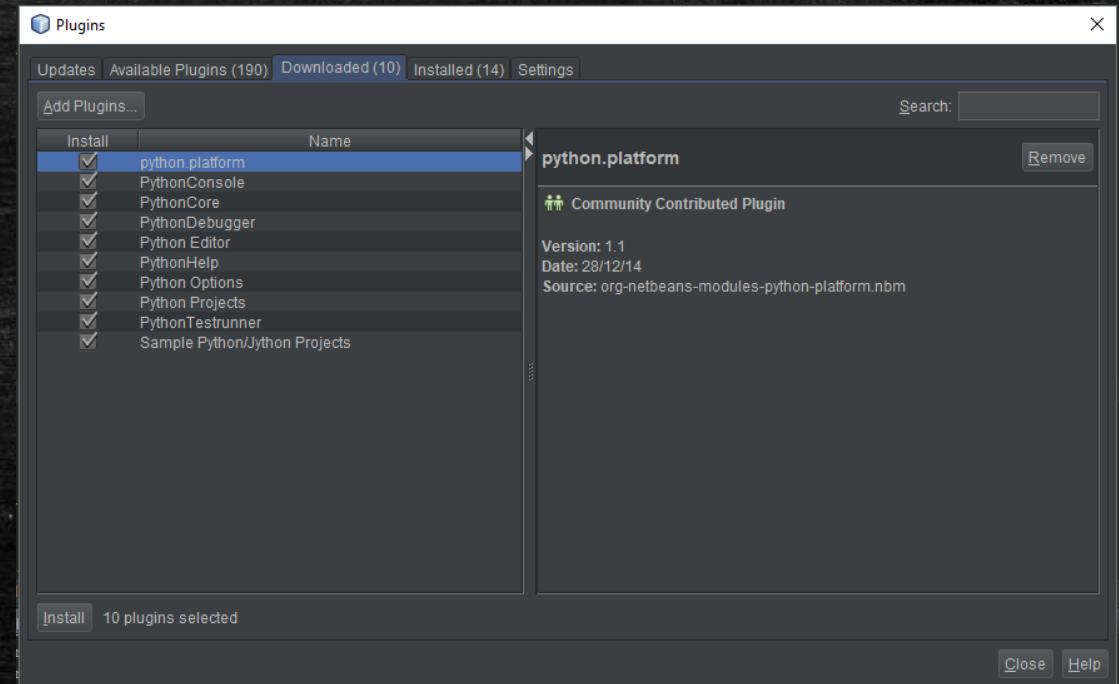
- Download Jython
 - <http://www.jython.org/downloads.html>
- Python Plugin for NetBeans IDE
 - <http://plugins.netbeans.org/plugin/56795>

Note: Because of the way in which Jython and JRuby dynamically generate Java classes, you may encounter memory problems if you load several different Python or Ruby extensions, or if you unload and reload an extension multiple times. If this happens, you will see an error like:

```
java.lang.OutOfMemoryError: PermGen space
```

You can avoid this problem by configuring Java to allocate more PermGen storage, by adding a `-XX:MaxPermSize` option to the command line when starting Burp. For example:

```
java -XX:MaxPermSize=1G -jar burp.jar
```



Practice Time

Exercise #: setup development environment

IBurpExtender

- All extensions must implement this interface.
- BurpExtender must implement this interface with one method
 - `void registerExtenderCallbacks (IBurpExtenderCallbacks callbacks)`
- Burp invokes `registerExtenderCallbacks ()` method when an extension is loaded

IBurpExtenderCallbacks

- Consists a set of callback methods for extensions to perform various actions within Burp
- Used to register extension settings
- This interface can handles stdout and stderr

IExtensionHelpers

- Build, analyse and modify HTTP requests and responses
- Toggle request's method between GET and POST
- Do encoding/decoding to request/response data
- Constructs scanner insertion point

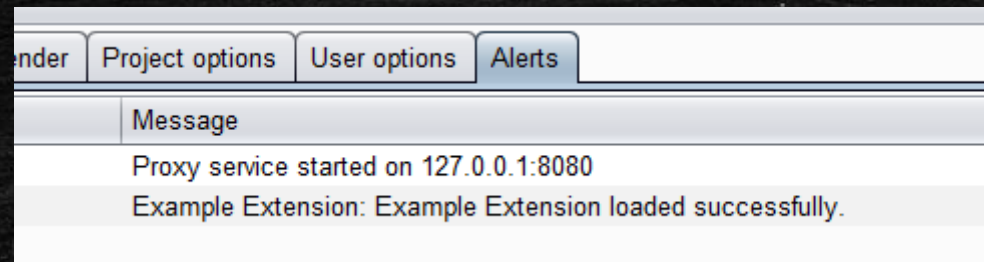
Handling stdout/stderr

- `callbacks.getStderr()`
- `callbacks.getStdout()`

```
private IBurpExtenderCallbacks callbacks;  
private PrintWriter stderr, stdout;  
  
@Override  
public void registerExtenderCallbacks(IBurpExtenderCallbacks callbacks)  
{  
    this.callbacks = callbacks;  
    stderr = new PrintWriter(callbacks.getStderr(), true);  
    stdout = new PrintWriter(callbacks.getStdout(), true);  
}
```

Extension Settings

- `callbacks.setExtensionName(String extName)`
- `callbacks.issueAlert(String msg)`



Practice Time

Exercise #: use stdout/stdErr for extension with alert on loading

Some useful methods

- IBurpExtenderCallbacks

- IHttpRequestResponse makeHttpRequest(IHttpService httpService, byte[] request);
- void registerHttpListener(IHttpListener listener);
- void registerProxyListener(IProxyListener listener);

- IExtensionHelper

- IRequestInfo analyzeRequest(byte[] request);
- IResponseInfo analyzeResponse(byte[] response);
- IParameter getRequestParameter(byte[] request, String parameterName);
- byte[] addParameter(byte[] request, IParameter parameter);
- byte[] toggleRequestMethod(byte[] request);
- byte[] buildHttpMessage(List headers, byte[] body);

- IRequestInfo

- List<String> getHeaders();
- List<IParameter> getParameters();

Practice Time

Exercise #: analyse server response for match

Debugging Tips

- Version updates may change APIs too. Use the latest
- Run burp from terminal
- Memory problems with Jython and Jruby
 - `java.lang.OutOfMemoryError: PermGen space`
- In case of above error, allocate more PermGen storage
 - `java -XX:MaxPermSize=1G -jar burp.jar`

Thanks

s4n7h0@infoseccampus.com
<https://twitter.com/s4n7h0>