



# ZAP JENKINS PLUGIN

Goran Sarenkapa

ZAP Jenkins Plugin Project Lead

# WHAT IS ZAP?

- An easy to use webapp pentest tool
- Completely free and open source
- An OWASP flagship project
- Ideal for beginners
- But also used by professionals
- Ideal for devs, esp. for automated security tests
- Becoming a framework for advanced testing

See [here](#) for more information.

# REQUIREMENTS



Firefox



ZAP



Jenkins

Install



Setup



Run

# ZAP JENKINS PLUGIN – FEATURES

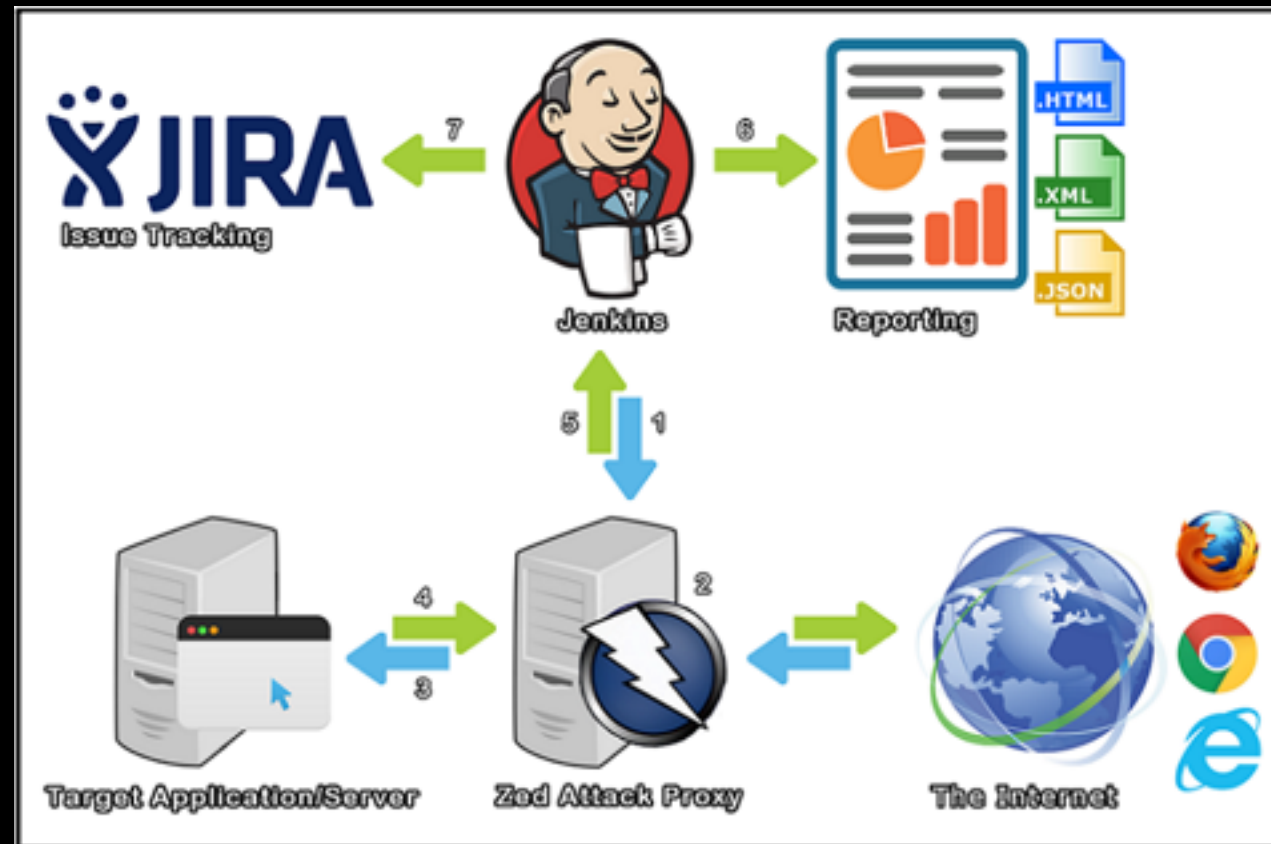
- Manage Sessions (Load or Persist)
- Define Context (Name, Include URLs and Exclude URLs)
- Attack Contexts (Spider Scan, AJAX Spider, Active Scan)

You can also:

- Setup Authentication (Form Based or Script Based)
- Run as Pre-Build as part of a [Selenium](#) Build
- Generate Reports (



# ZAP IN A CI ENVIRONMENT



**JIRA**  
Issue Tracking



Jenkins



Reporting



Target Application/Server



Zed Attack Proxy



The Internet





# JENKINS

1. Download [desired war release](#) (Requires Jenkins 1.580.1+ to run)
2. Create a Jenkins folder and extract the WAR file into it.
3. Create a JENKINS\_HOME environment variable.
4. Start Jenkins from the cmd line with

```
%JAVA_HOME%\bin\java.exe -jar %JENKINS_HOME%\jenkins.war
```
5. Install the following plugins:
  - [EnvInject Plugin](#)
  - [Summary Display Plugin](#)
  - [HTML Publisher Plugin](#)
  - [zap\\_plugin](#)
6. Set Jenkins to run on 127.0.0.1:8080



# ZAP

1. Download [release](#) (Requires ZAP Weekly [2016-09-05](#) or later)
2. Create a ZAP folder and extract the files into it.
3. Create a ZAPROXY\_HOME environment variable.
4. Modify zap.bat
  - java %jvmopts% -jar zap-D-2016-09-05.jar %\*To
  - java %jvmopts% -jar %ZAPROXY\_HOME%\zap-D-2016-09-05.jar %\*
5. Start ZAP from the cmd line with
  - `%ZAPROXY_HOME%\zap.bat -installdir %ZAPROXY_HOME%`



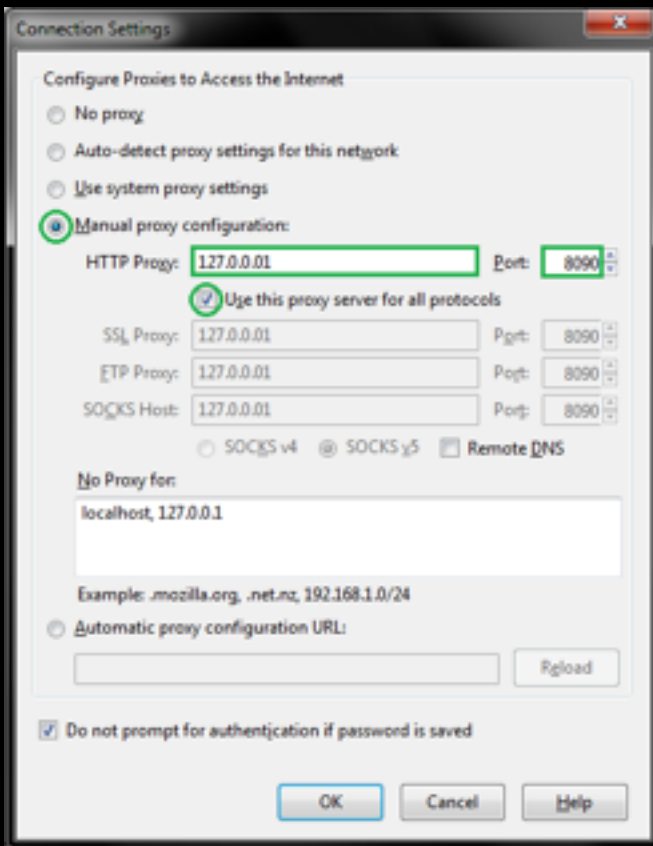


# FIREFOX

1. Download a selenium supported version of Firefox
  - ZAP supports one of the following [versions](#) of Firefox.
  - Download and install a [supported release](#).



# FIREFOX – LOCAL PROXY SETTINGS



The host and port set here should be the SAME set in ZAP and in the ZAP Jenkins plugin.



# ZAP – LOCAL PROXY SETTINGS

Local Proxy

Local Proxy

Address (eg localhost, 127.0.0.1)

Port (eg 8080)

Set your browser proxy setting using the above. The HTTP port and HTTPS port must be the same port as above.

Remove Unsupported Encodings

Always unzip gzipped content

Security Protocols

SSLv2Hello  SSL 3  TLS 1  TLS 1.1  TLS 1.2

The host and port set here should be the SAME set in Firefox and in the ZAP Jenkins plugin.

ZAP



Tools



Options



Local Proxy



# JENKINS – LOCAL PROXY SETTINGS

**ZAP**

Default Host  ?

Configure the default ZAP host (e.g. "localhost"). It can be overridden for each job. (from [Official ZAP Jenkins Plugin](#))

Default Port  ?

Configure the default ZAP port (e.g. "8090"). It can be overridden for each job. (from [Official ZAP Jenkins Plugin](#))



The host and port set here should be the SAME set in ZAP and in Firefox.



# ZAP – MAP YOUR SITE

- Map your site and Configure the Job to [Execute ZAP](#)

Or

- Write a Selenium Script and Configure the Job to [Execute ZAP as part of a Selenium Build](#)

- Recycle Bin
- 1000.jpg
- Network
- stacktrace.txt
- Control Panel
- Gonah
- Mozilla Firefox
- ZAP Jenkins Plugin
- ZAP Current
- Jenkins WAR Start
- Blue Jeans
- owasp\_zap...

Untitled Session - OWASP ZAP D-2016-09-05

File Edit View Analyse Report Tools Online Help

Standard Mode

Sites +

Contexts

- Default Context
- Sites

History Search Alerts Output +

Filter:OFF

Id	Req. Timestamp	Method	URL
----	----------------	--------	-----


Alerts 0 0 0 0 0 0

Mozilla Firefox Start Page


Firefox Search or enter address

Search

mozilla



Search

 All new, all private, all the time. [Get Firefox Focus](#), the browser for iPhone always in private browsing mode.

Downloads Bookmarks History Add-ons Sync Options Restore Previous Session



# JENKINS – NEW JOB

1. Create a new Freestyle project
2. Restrict the build to the desired machine
  - (Slave or Master, machine on which ZAP is installed and the build will be run)
3. Run the Build to create the workspace

Desktop environment showing various icons and a terminal window.

Terminal window content:

```

INFO: Loaded all jobs
Nov 20, 2016 11:02:30 PM hudson.model.AsyncPeriodicWork$1$1
INFO: Started Download metadata
Nov 20, 2016 11:02:30 PM hudson.model.AsyncPeriodicWork$1$1
INFO: Finished Download metadata, 0 ms
Nov 20, 2016 11:02:31 PM org.springframework.context.support
INFO: Refreshing org.springframework.web.context.support
licationContext]; startup date [Sun Nov 20 23:02:3
Nov 20, 2016 11:02:31 PM org.springframework.context.support
INFO: Bean factory for application context [org.sp
]: org.springframework.beans.factory.support.Default
Nov 20, 2016 11:02:31 PM org.springframework.beans.factory
INFO: Pre-instantiating singletons in org.springfr
ining beans [authenticationManager]; root of facto
Nov 20, 2016 11:02:31 PM org.jenkinsci.main.module
INFO: Started SSHD at port 54423
Nov 20, 2016 11:02:31 PM jenkins.InitReactorRunner
INFO: Completed initialization
Nov 20, 2016 11:02:31 PM org.springframework.context.support
INFO: Refreshing org.springframework.web.context.support
licationContext]; startup date [Sun Nov 20 23:02:3
Nov 20, 2016 11:02:31 PM org.springframework.context.support
INFO: Bean factory for application context [org.sp
]: org.springframework.beans.factory.support.Default
Nov 20, 2016 11:02:31 PM org.springframework.beans.factory
INFO: Pre-instantiating singletons in org.springfr
ining beans [filter,legacy]; root of factory hiera
Nov 20, 2016 11:02:31 PM hudson.WebAppMain$3 run
INFO: Jenkins is fully up and running
  
```

Browser window showing the Jenkins Dashboard at localhost:8080.

Page title: Jenkins

Navigation menu:

- New Item
- People
- Build History
- Manage Jenkins
- My Views
- Credentials

Build Queue:

No builds in the queue.

Build Executor Status:

- 1 Idle
- 2 Idle

S	W	Name ↓	Last Success	Last Failure	Last Duration
		demo	2 hr 9 min - #5	2 hr 31 min - #2	39 sec

Legend: RSS for all RSS for failures RSS for just latest builds

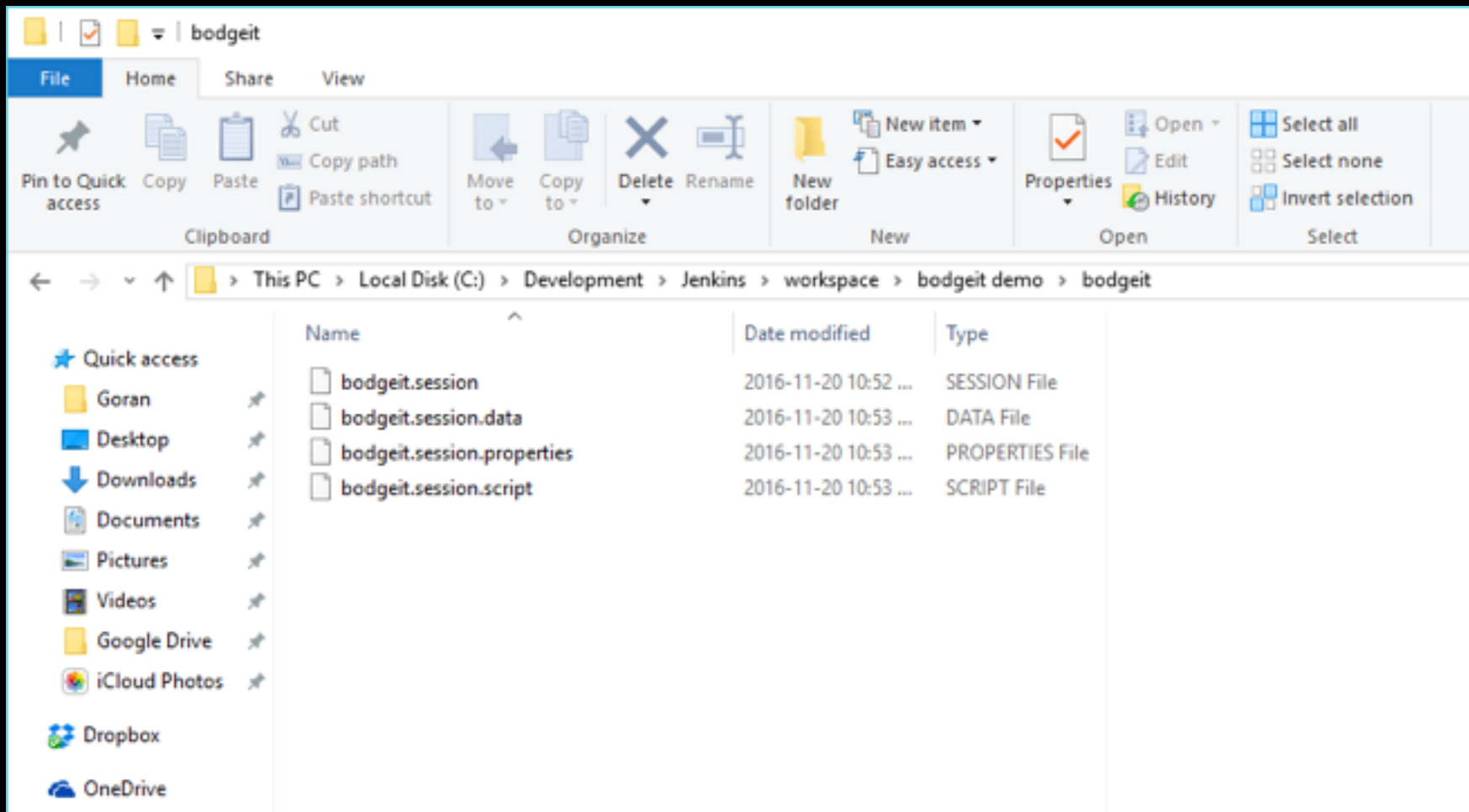
Page generated: Nov 20, 2016 11:03:17 PM EST [REST API](#) Jenkins ver. 2.19.3

Windows taskbar showing the Start button, search icon, task view icon, and several application icons. The system tray on the right shows the date and time: 11:03 PM 2016-11-20.





# JENKINS – SESSION VISIBILITY

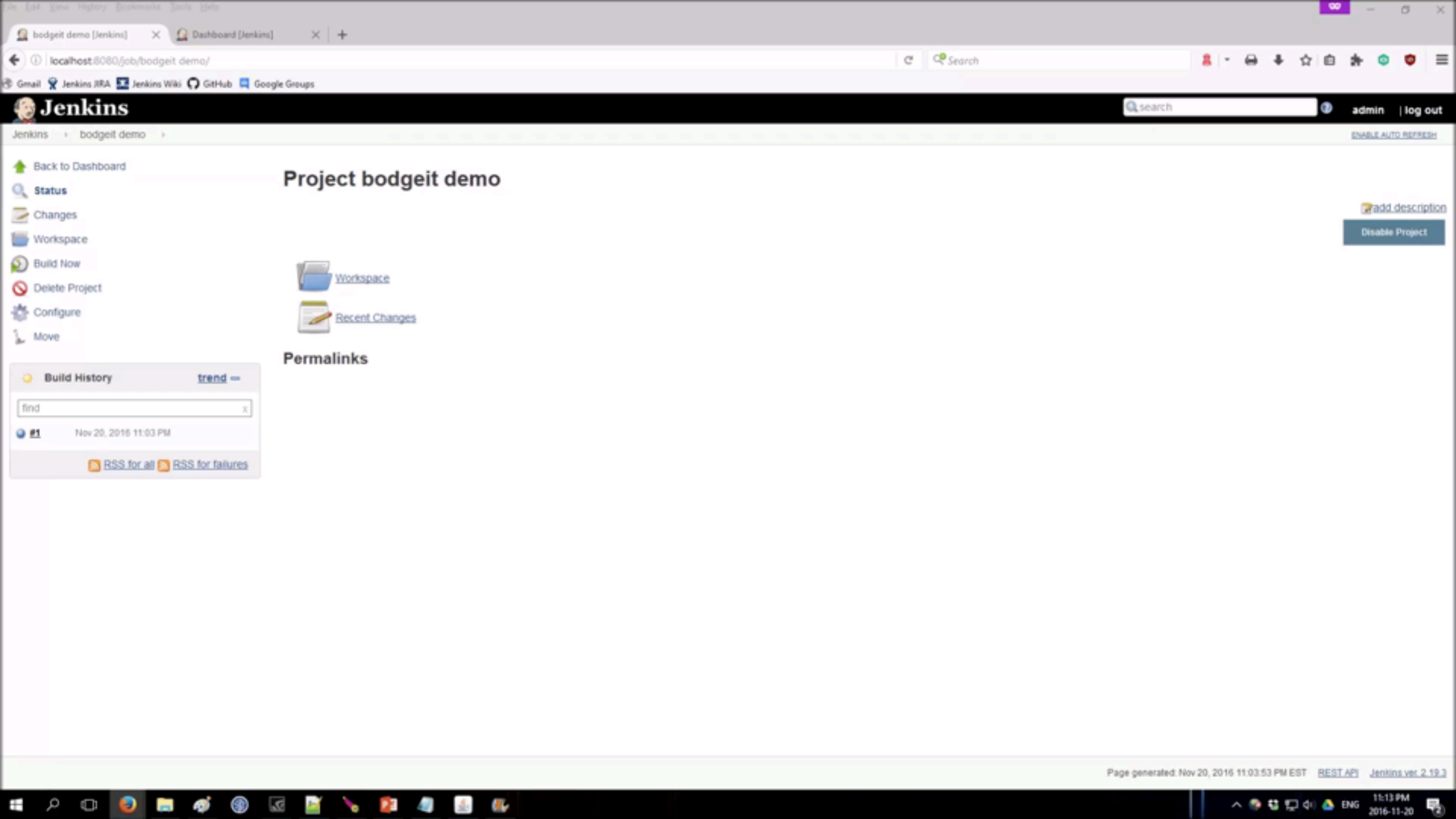


- Copy the previously persisted session from the ZAP UI into the Job's workspace.



# JENKINS – JOB CONFIG

1. Add an **Execute ZAP** build step
2. Add an **Archive the Artifacts** post-build action
3. Add a **Publish HTML Reports** post-build action



- Back to Dashboard
- Status
- Changes
- Workspace
- Build Now
- Delete Project
- Configure
- Move

## Project bodgeit demo

- Workspace
- Recent Changes

- add description
- Disable Project

### Permalinks

**Build History** trend

Nov 20, 2016 11:03 PM

RSS for all RSS for failures



OWASP ZAP Current

Untitled Session - budget - OWASP ZAP D-2016-09-05

File Edit View Analyse Report Tools Online Help

Standard Mode

Sites

- Contexts
  - Default Context
  - budget2
- Sites
  - http://127.0.0.1:9080

History Search Alerts Output

Alerts (14)

- Anti CSRF Tokens Scanner (12)
- Cross Site Scripting (Reflected)
- Application Error Disclosure
- Buffer Overflow (38)
- Format String Error (38)
- HTTP Parameter Override (10)
- Integer Overflow Error (37)
- X-Frame-Options Header Not Set (58)
- Absence of Anti-CSRF Tokens (43)
- Cookie No HttpOnly Flag (2)
- Password Autocomplete in Browser (13)
- Web Browser XSS Protection Not Enabled (59)
- X-Content-Type-Options Header Missing (50)
- Loosely Scoped Cookie (3)

Alerts 2 6 5 1

Dashboard [Jenkins]

localhost8080/jenkins/

Back to budget demo JENKINS\_ZAP\_VULNERABILITY\_REPORT\_2

14 Loosely Scoped Cookie

Site: http://127.0.0.1

# ONE TO ONE ALERTS

## Summary of Alerts

Risk Level	Number of Alerts
High	2
Medium	6
Low	5
Informational	1

## Alert Details

High	Anti CSRF Tokens Scanner	Top
Description	<p>A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf.</p> <p>CSRF attacks are effective in a number of situations, including:</p> <ul style="list-style-type: none"> <li>The victim has an active session on the target site.</li> <li>The victim is authenticated via HTTP auth on the target site.</li> <li>The victim is on the same local network as the target site.</li> </ul> <p>CSRF has primarily been used to perform an action against a target site using the victim's privileges, but recent techniques have been discovered to disclose information by gaining access to the response. The risk of information disclosure is dramatically increased when the target site is vulnerable to XSS, because</p>	

# THANK YOU!

- Documentation: See the [Wiki](#) for more details.
- Questions: Ask on our [Google Group](#).
- Issue Tracking: Report on the [Jenkins JIRA](#) for the project, please read the [JIRA guidelines](#) before reporting an issue.
- Your feedback will drive our future development and determine which features we focus on.