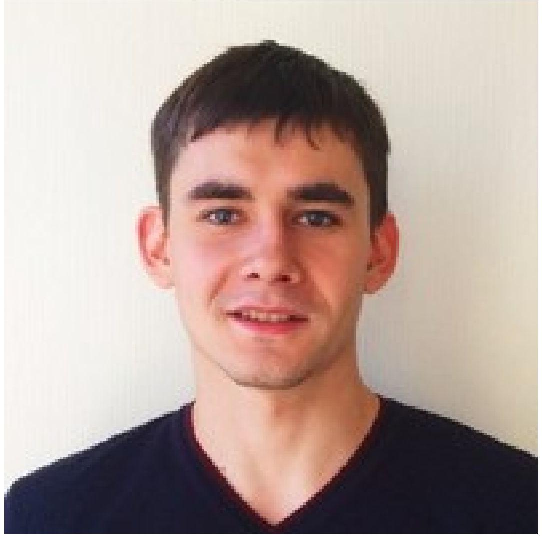
HOW TO AVOID SECURITY VULNERABILITIES OF AEM

Andrey Pinchuk
Certified Senior AEM Developer at Axamit

AXAMIT

Speaker



Andrey Pinchuk

Professional Experience:

- Back-end development;
- 5 years IT-engineering;
- Senior AEM Developer.

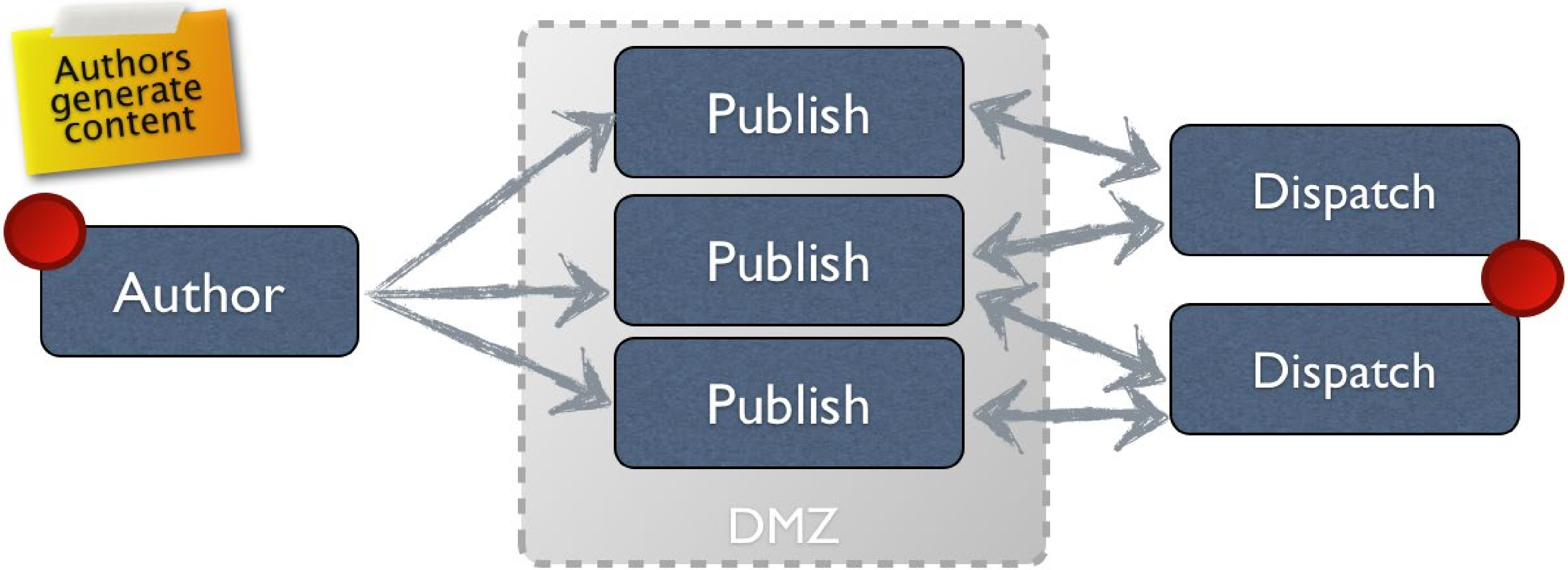
Key Solutions:

- Adobe Analytics
- Adobe Campaign
- Dynamic Media

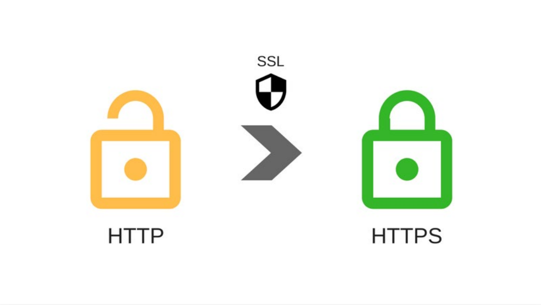
Agenda

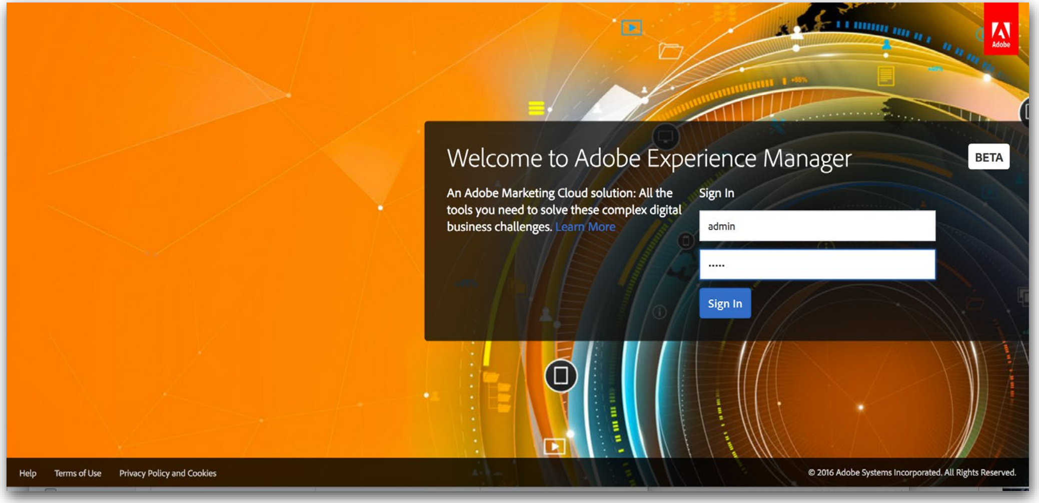
1. AEM Author Security
2. AEM Publish Security
3. Dispatcher security
4. CSRF Protection Framework
5. Denial of Service (DoS) Attacks

General overview



General Tips





Welcome to Adobe Experience Manager

An Adobe Marketing Cloud solution: All the tools you need to solve these complex digital business challenges. Learn More

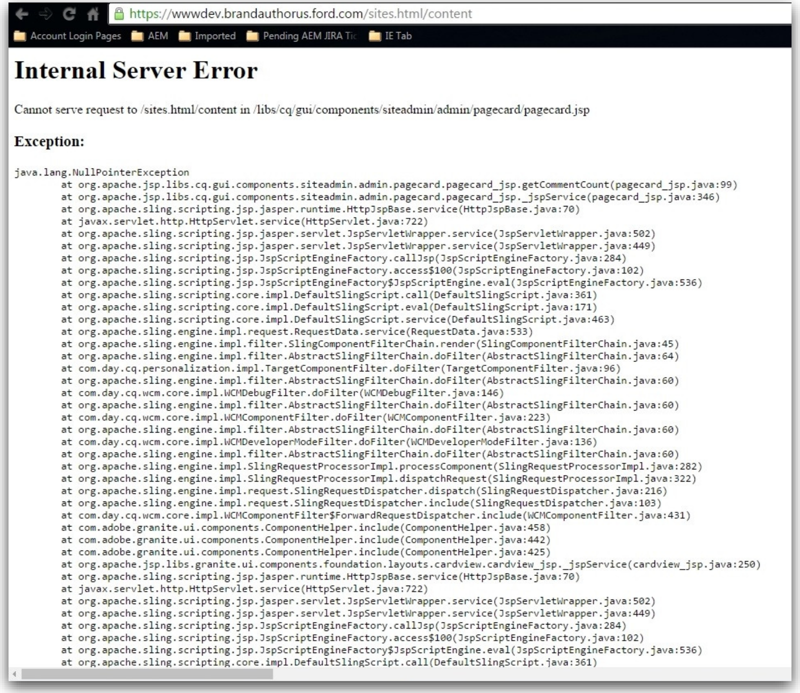
Sign In

admin

.....

© 2016 Adobe Systems Incorporated. All Rights Reserved.

General Tips

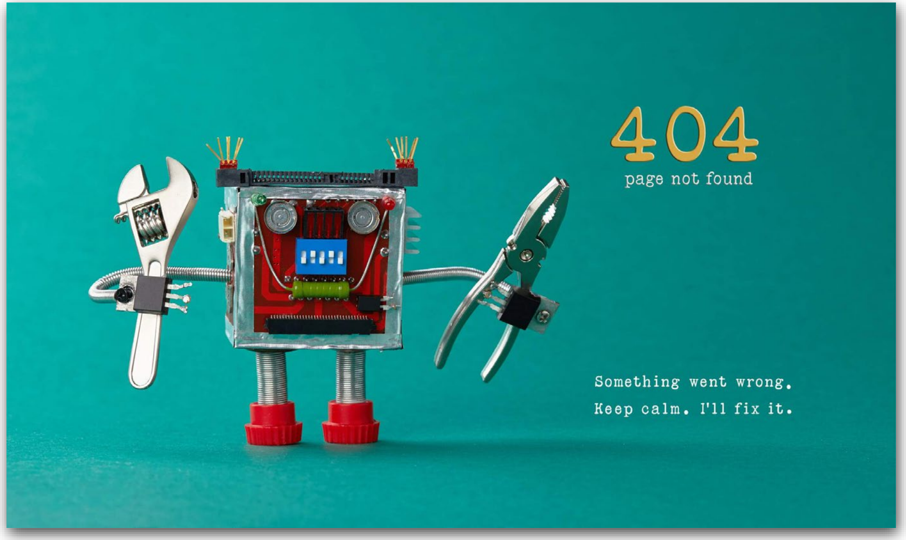


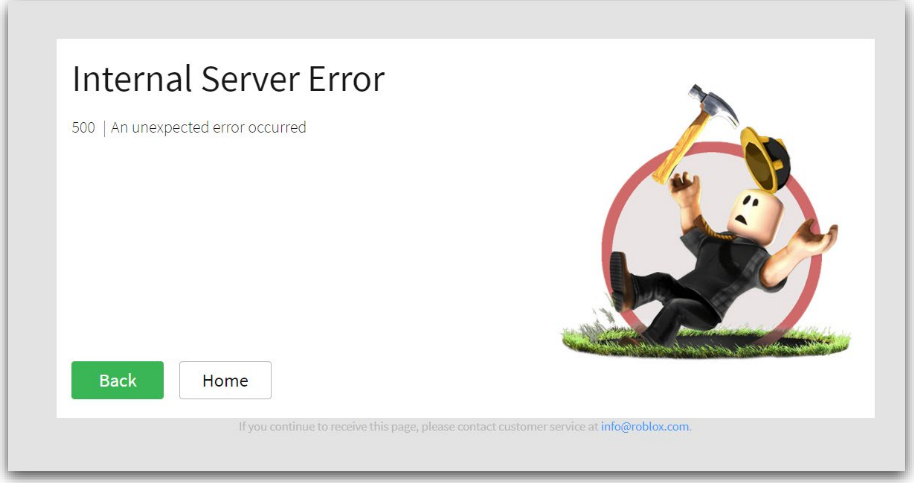
Internal Server Error

Cannot serve request to /sites.html/content in /libs/cq/gui/components/siteadmin/admin/pagecard/pagecard.jsp

Exception:

```
java.lang.NullPointerException
        at org.apache.jsp.libs.cq.gui.components.siteadmin.admin.pagecard.pagecard_jsp.getCommentCount(pagecard_jsp.java:99)
        at org.apache.jsp.libs.cq.gui.components.siteadmin.admin.pagecard.pagecard_jsp._jspService(pagecard_jsp.java:346)
        at org.apache.sling.scripting.jsp.jasper.runtime.HttpJspBase.service(HttpJspBase.java:70)
        at javax.servlet.http.HttpServlet.service(HttpServlet.java:722)
        at org.apache.sling.scripting.jsp.jasper.servlet.JspServletWrapper.service(JspServletWrapper.java:502)
        at org.apache.sling.scripting.jsp.jasper.servlet.JspServletWrapper.service(JspServletWrapper.java:449)
        at org.apache.sling.scripting.jsp.JspScriptEngineFactory.callJsp(JspScriptEngineFactory.java:284)
        at org.apache.sling.scripting.jsp.JspScriptEngineFactory.access$100(JspScriptEngineFactory.java:102)
        at org.apache.sling.scripting.jsp.JspScriptEngineFactory$JspScriptEngine.eval(JspScriptEngineFactory.java:536)
        at org.apache.sling.scripting.core.impl.DefaultSlingScript.call(DefaultSlingScript.java:361)
        at org.apache.sling.scripting.core.impl.DefaultSlingScript.eval(DefaultSlingScript.java:171)
        at org.apache.sling.scripting.core.impl.DefaultSlingScript.service(DefaultSlingScript.java:463)
        at org.apache.sling.engine.impl.request.RequestData.service(RequestData.java:533)
        at org.apache.sling.engine.impl.filter.SlingComponentFilterChain.render(SlingComponentFilterChain.java:45)
        at org.apache.sling.engine.impl.filter.AbstractSlingFilterChain.doFilter(AbstractSlingFilterChain.java:64)
        at com.day.cq.personalization.impl.TargetComponentFilter.doFilter(TargetComponentFilter.java:96)
        at org.apache.sling.engine.impl.filter.AbstractSlingFilterChain.doFilter(AbstractSlingFilterChain.java:60)
        at com.day.cq.wcm.core.impl.WCMDebugFilter.doFilter(WCMDebugFilter.java:146)
        at org.apache.sling.engine.impl.filter.AbstractSlingFilterChain.doFilter(AbstractSlingFilterChain.java:60)
        at com.day.cq.wcm.core.impl.WCMComponentFilter.doFilter(WCMComponentFilter.java:223)
        at org.apache.sling.engine.impl.filter.AbstractSlingFilterChain.doFilter(AbstractSlingFilterChain.java:60)
        at com.day.cq.wcm.core.impl.WCMDeveloperModeFilter.doFilter(WCMDeveloperModeFilter.java:136)
        at org.apache.sling.engine.impl.filter.AbstractSlingFilterChain.doFilter(AbstractSlingFilterChain.java:60)
        at org.apache.sling.engine.impl.SlingRequestProcessorImpl.processComponent(SlingRequestProcessorImpl.java:282)
        at org.apache.sling.engine.impl.SlingRequestProcessorImpl.dispatchRequest(SlingRequestProcessorImpl.java:322)
        at org.apache.sling.engine.impl.request.SlingRequestDispatcher.dispatch(SlingRequestDispatcher.java:216)
        at org.apache.sling.engine.impl.request.SlingRequestDispatcher.include(SlingRequestDispatcher.java:103)
        at com.day.cq.wcm.core.impl.WCMComponentFilter$ForwardRequestDispatcher.include(WCMComponentFilter.java:431)
        at com.adobe.granite.ui.components.ComponentHelper.include(ComponentHelper.java:458)
        at com.adobe.granite.ui.components.ComponentHelper.include(ComponentHelper.java:442)
        at com.adobe.granite.ui.components.ComponentHelper.include(ComponentHelper.java:425)
        at org.apache.jsp.libs.granite.ui.components.foundation.layouts.cardview.cardview_jsp._jspService(cardview_jsp.java:250)
        at org.apache.sling.scripting.jsp.jasper.runtime.HttpJspBase.service(HttpJspBase.java:70)
        at javax.servlet.http.HttpServlet.service(HttpServlet.java:722)
        at org.apache.sling.scripting.jsp.jasper.servlet.JspServletWrapper.service(JspServletWrapper.java:502)
        at org.apache.sling.scripting.jsp.jasper.servlet.JspServletWrapper.service(JspServletWrapper.java:449)
        at org.apache.sling.scripting.jsp.JspScriptEngineFactory.callJsp(JspScriptEngineFactory.java:284)
        at org.apache.sling.scripting.jsp.JspScriptEngineFactory.access$100(JspScriptEngineFactory.java:102)
        at org.apache.sling.scripting.jsp.JspScriptEngineFactory$JspScriptEngine.eval(JspScriptEngineFactory.java:536)
        at org.apache.sling.scripting.core.impl.DefaultSlingScript.call(DefaultSlingScript.java:361)
```



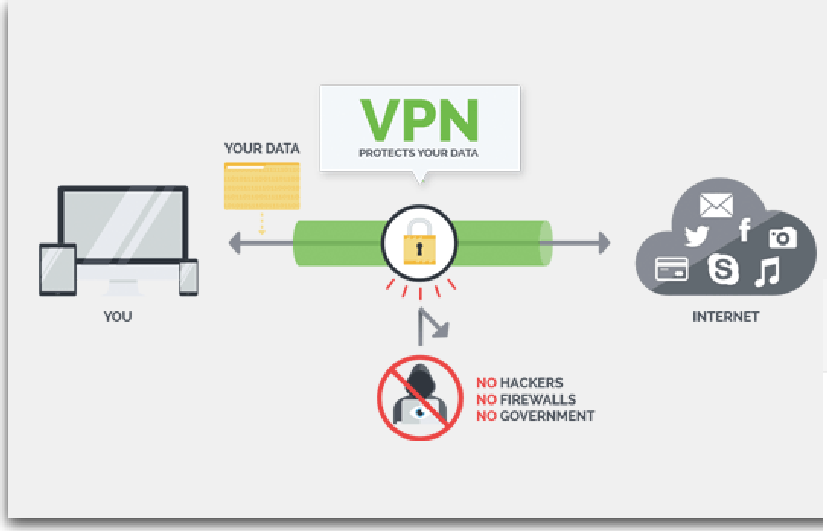


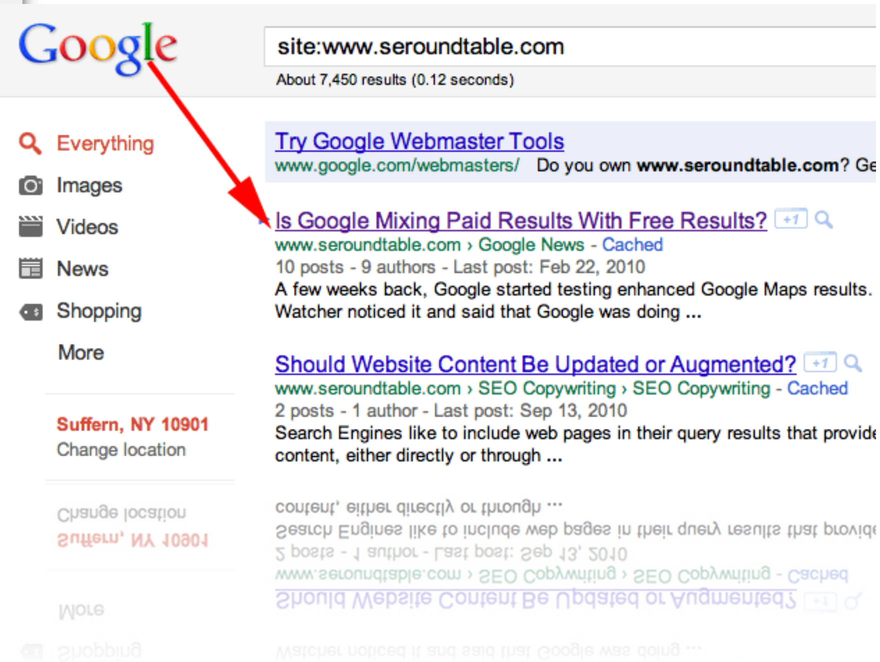
Internal Server Error

500 | An unexpected error occurred

If you continue to receive this page, please contact customer service at info@roblox.com.

AEM Author Security





site:www.seroundtable.com

About 7,450 results (0.12 seconds)

Try Google Webmaster Tools
www.google.com/webmasters/ Do you own **www.seroundtable.com**? Ge

Is Google Mixing Paid Results With Free Results?
www.seroundtable.com › Google News - Cached
10 posts - 9 authors - Last post: Feb 22, 2010
A few weeks back, Google started testing enhanced Google Maps results. Watcher noticed it and said that Google was doing ...

Should Website Content Be Updated or Augmented?
www.seroundtable.com › SEO Copywriting › SEO Copywriting - Cached
2 posts - 1 author - Last post: Sep 13, 2010
Search Engines like to include web pages in their query results that provide content, either directly or through ...

Suffern, NY 10901
Change location

AEM Author Security

4. Create a separate replication user to use in replication agent configuration.

- Admin should not be used for replicating anywhere.

5. Limit the number of users in admin groups.

6. CRXDE in prod author should be limited to certain users.

AEM Publish Security

1. Publish instances should not be accessible to an outside of the intranet.

2. Anonymous permissions should be checked & make sure not every directory accessible.

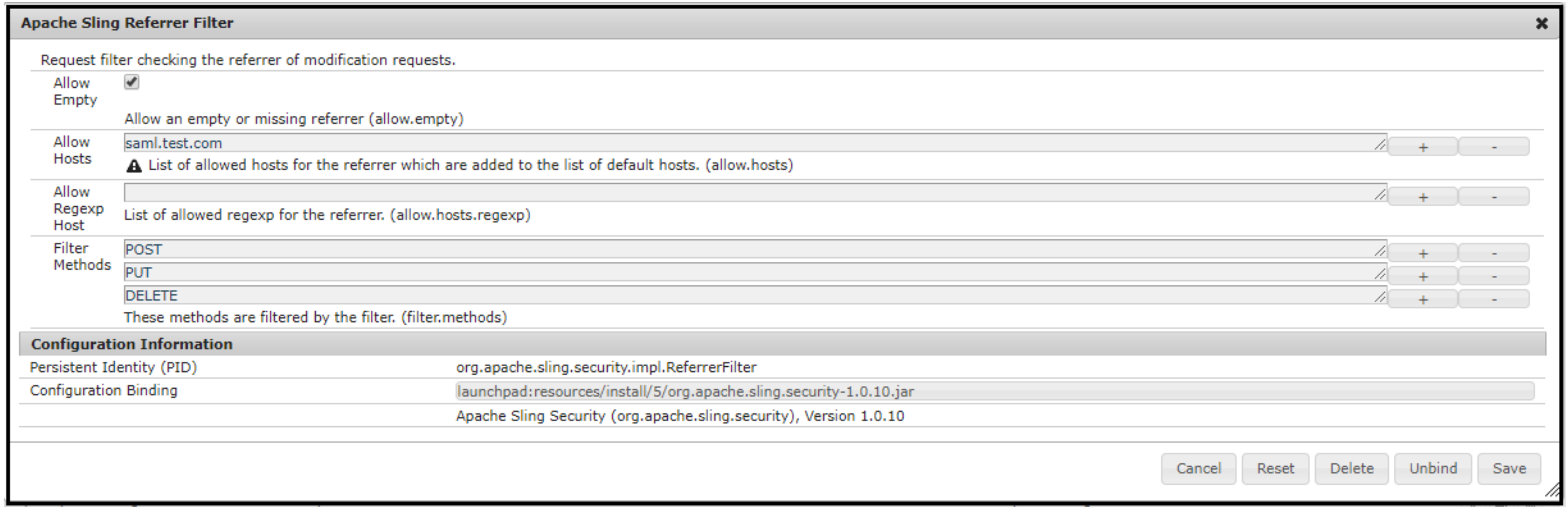
3. **Apache Sling Referrer Filter** must be configured to handle unwanted publish requests.

4. The cross-site forgery framework should be enabled to filter requests.

5. All default tools (CRXDE) etc should be disabled.

6. Not all users should be able to install packages directly.

AEM Publish Security - Apache Sling Referrer Filter



Apache Sling Referrer Filter

Request filter checking the referrer of modification requests.

Allow Empty ☑

Allow an empty or missing referrer (allow.empty)

Allow Hosts: saml.test.com

⚠ List of allowed hosts for the referrer which are added to the list of default hosts. (allow.hosts)

Allow Regexp Host:

List of allowed regexp for the referrer. (allow.hosts.regexp)

Filter Methods: POST, PUT, DELETE

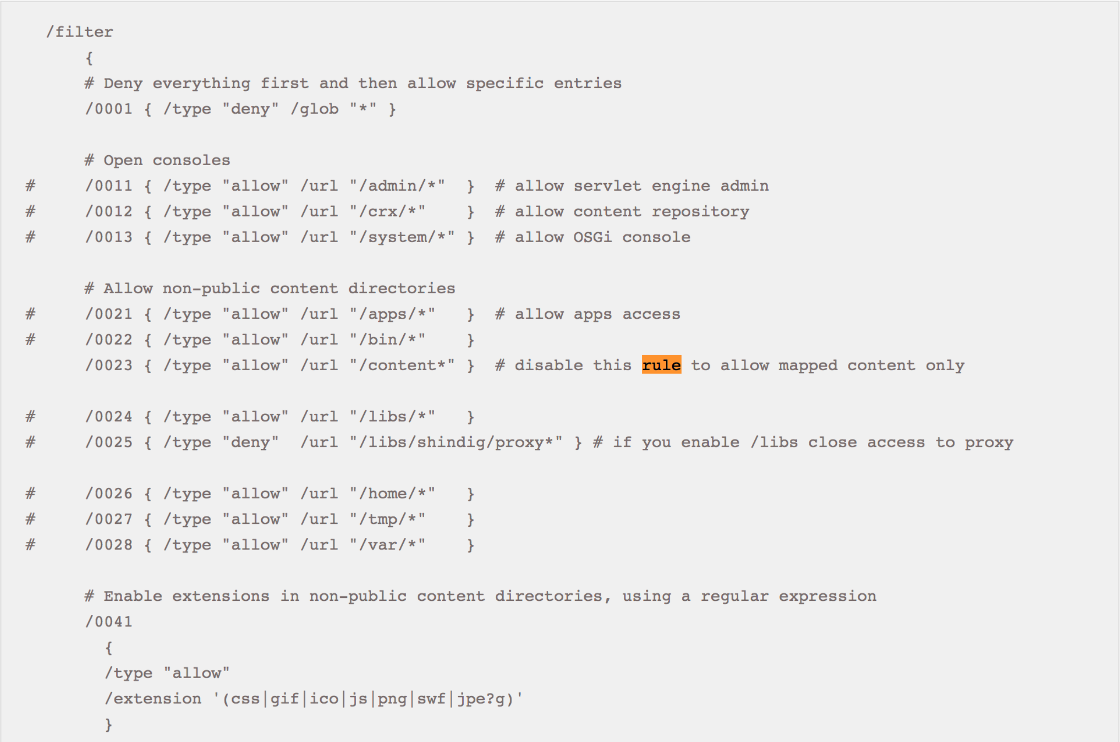
These methods are filtered by the filter. (filter.methods)

Configuration Information

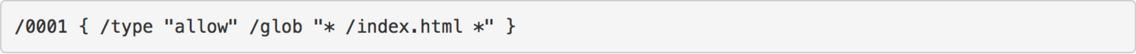
Persistent Identity (PID)	org.apache.sling.security.impl.ReferrerFilter
Configuration Binding	launchpad:resources/install/5/org.apache.sling.security-1.0.10.jar
	Apache Sling Security (org.apache.sling.security), Version 1.0.10

Dispatcher security

1. Check rules & filters in dispatcher.any configuration file



```
  /filter
      {
      # Deny everything first and then allow specific entries
      /0001 { /type "deny" /glob "*" }

      # Open consoles
#     /0011 { /type "allow" /url "/admin/*"  }  # allow servlet engine admin
#     /0012 { /type "allow" /url "/crx/*"    }  # allow content repository
#     /0013 { /type "allow" /url "/system/*" }  # allow OSGi console

      # Allow non-public content directories
#     /0021 { /type "allow" /url "/apps/*"   }  # allow apps access
#     /0022 { /type "allow" /url "/bin/*"    }
      /0023 { /type "allow" /url "/content*" }  # disable this rule to allow mapped content only

#     /0024 { /type "allow" /url "/libs/*"   }
#     /0025 { /type "deny"  /url "/libs/shindig/proxy*" } # if you enable /libs close access to proxy

#     /0026 { /type "allow" /url "/home/*"   }
#     /0027 { /type "allow" /url "/tmp/*"    }
#     /0028 { /type "allow" /url "/var/*"    }

      # Enable extensions in non-public content directories, using a regular expression
      /0041
        {
        /type "allow"
        /extension '(css|gif|ico|js|png|swf|jpe?g)'
        }
```

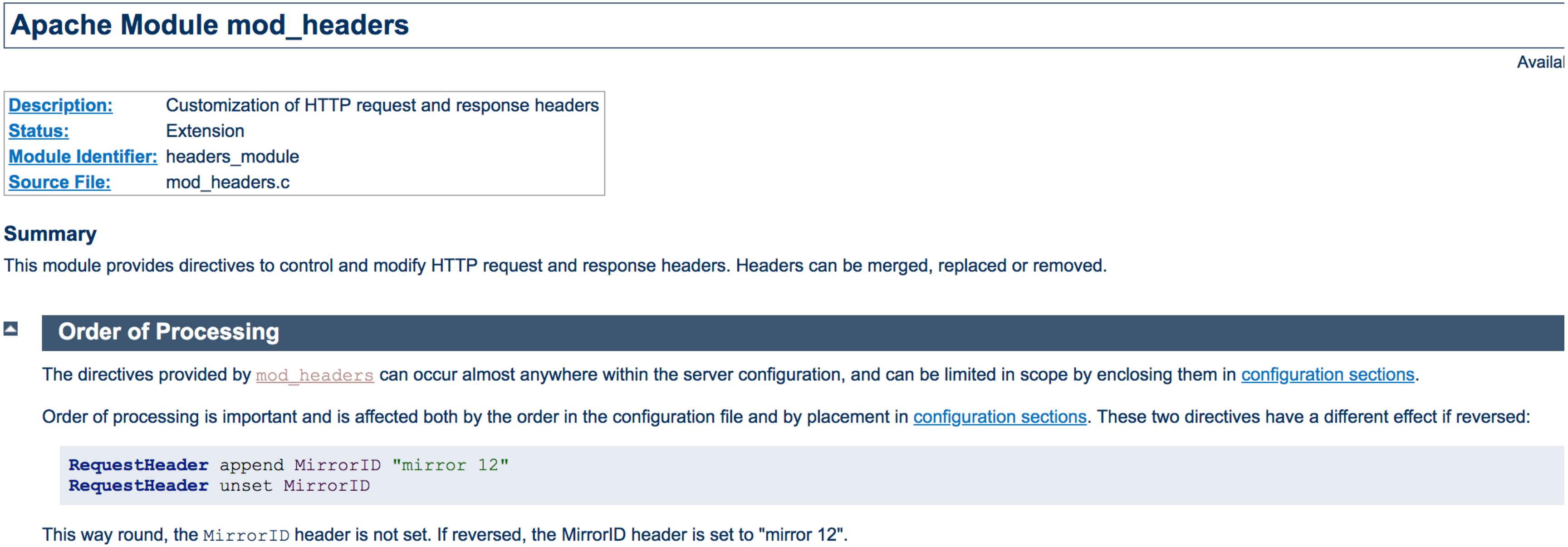


```
/0001 { /type "allow" /glob "* /index.html *" }
```

Dispatcher security

2. Limit the request headers information.

Request headers are passed in every request to AEM publish based on dispatcher configuration.



Apache Module mod_headers

Availal

Description:	Customization of HTTP request and response headers
Status:	Extension
Module Identifier:	headers_module
Source File:	mod_headers.c

Summary

This module provides directives to control and modify HTTP request and response headers. Headers can be merged, replaced or removed.

Order of Processing

The directives provided by mod_headers can occur almost anywhere within the server configuration, and can be limited in scope by enclosing them in configuration sections.

Order of processing is important and is affected both by the order in the configuration file and by placement in configuration sections. These two directives have a different effect if reversed:

```
RequestHeader append MirrorID "mirror 12"
RequestHeader unset MirrorID
```

This way round, the MirrorID header is not set. If reversed, the MirrorID header is set to "mirror 12".

Dispatcher security

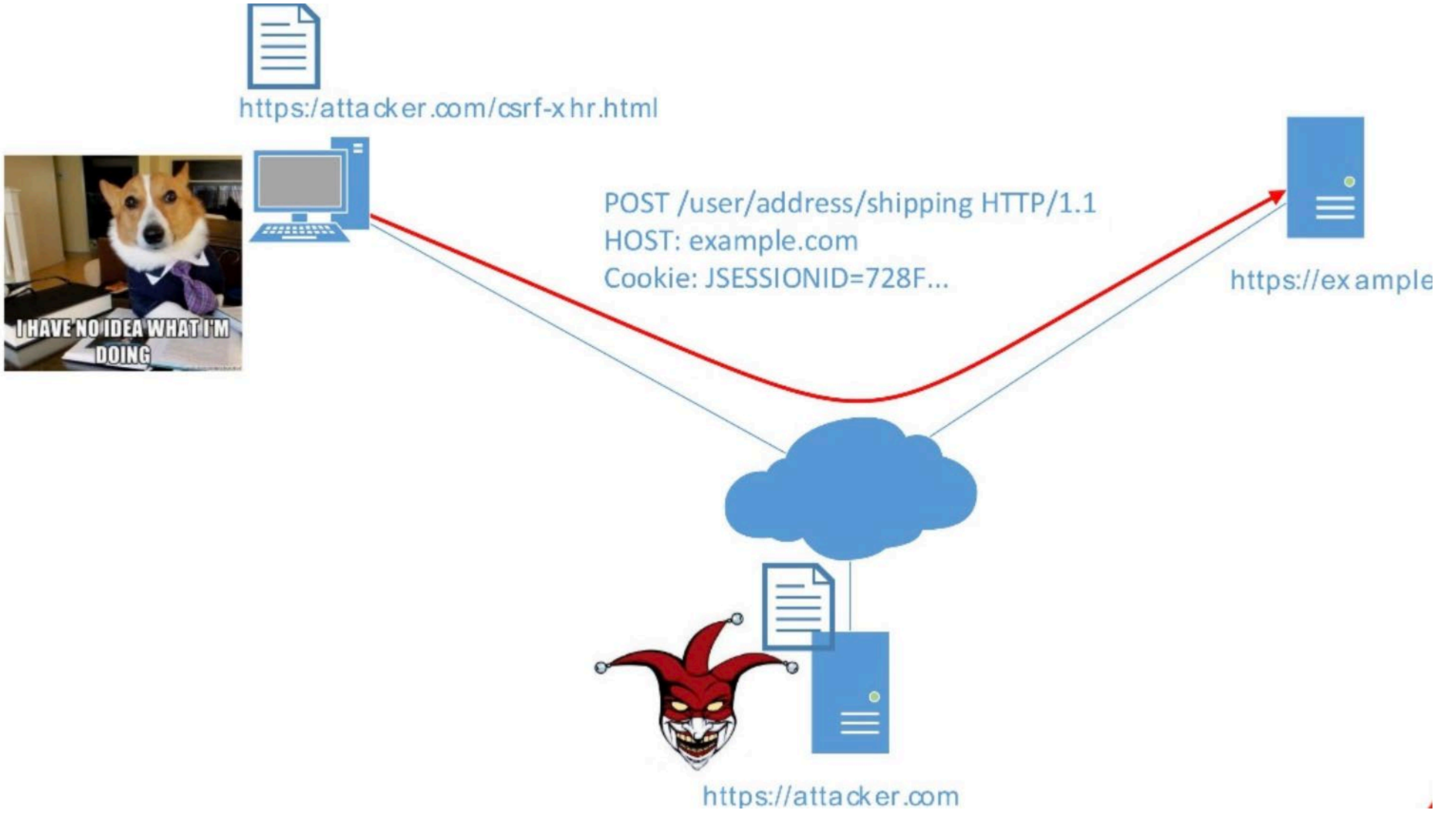
3. Do not allow cross-origin requests. Set the SAME origin header at the web server level.

4. Proper input validation should be done in POST Requests & dispatcher filter should allow only certain POST requests

5. Caching of selectors & URL extensions should be defined.

!Not every selector or extension should be cacheable. DOS or DDOS attacks are very easy to do in AEM application.

Cross Site Request Forgery (CSRF)



https:/attacker.com/csrf-xhr.html

```
POST /user/address/shipping HTTP/1.1
HOST: example.com
Cookie: JSESSIONID=728F...
```

https://example

https://attacker.com

Protect against Cross-Site Request Forgery

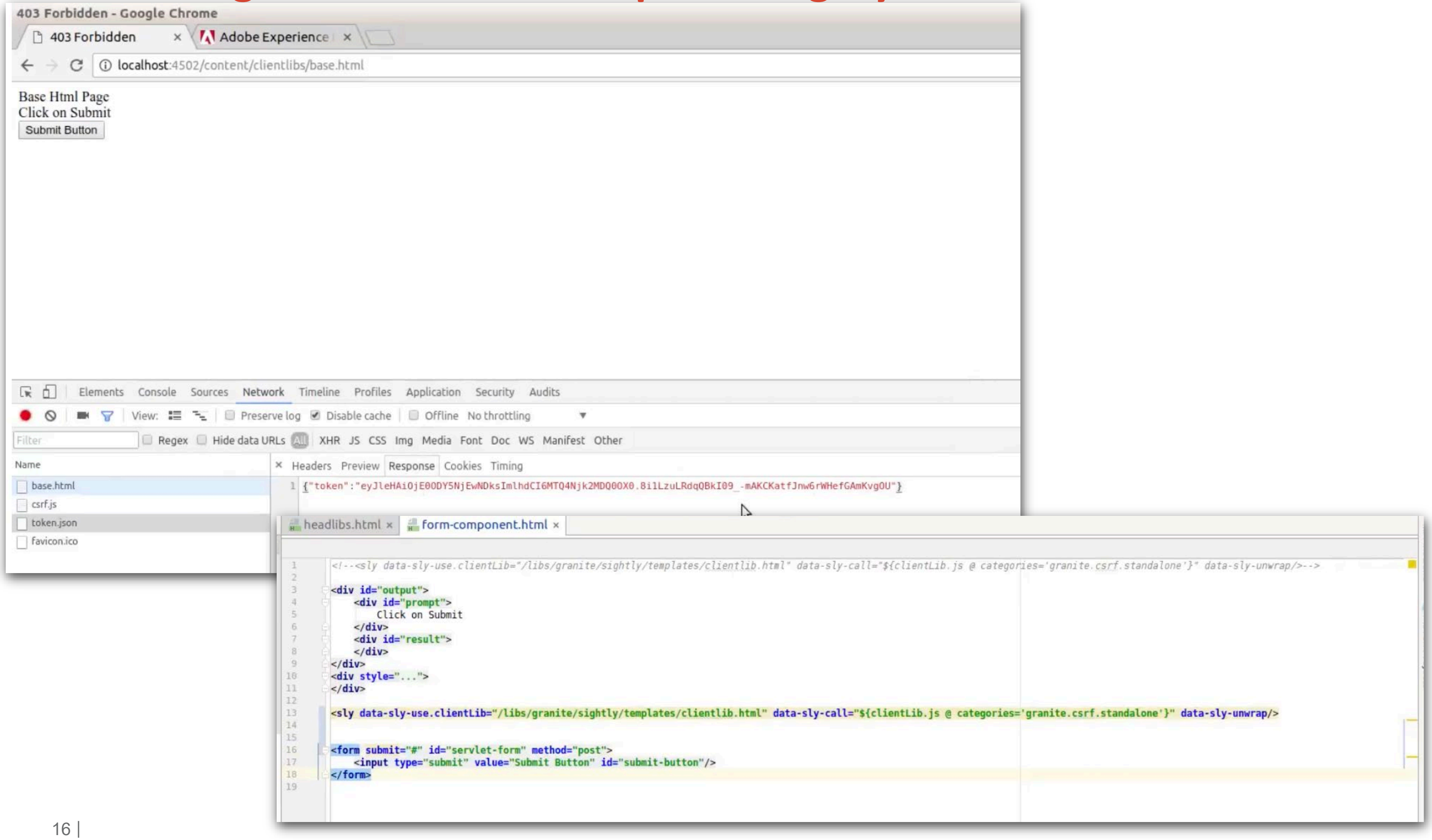
AEM 6.1 ships with a mechanism that helps protect against Cross-Site Request Forgery attacks, called the CSRF Protection Framework.

The Sling Referrer Filter

The referrer filter service is an OSGi service that allows you to configure:

- which http methods should be filtered;
- whether an empty referrer header is allowed
- a white list of servers to be allowed in addition to the server host.

Protect against Cross-Site Request Forgery


403 Forbidden - Google Chrome
403 Forbidden
Adobe Experience
localhost:4502/content/clientlibs/base.html
Elements Console Sources Network Timeline Profiles Application Security Audits
View:
☐ Preserve log ☑ Disable cache ☐ Offline No throttling
Filter ☐ Regex ☐ Hide data URLs All XHR JS CSS Img Media Font Doc WS Manifest Other
Name
base.html
csrf.js
token.json
favicon.ico
Headers Preview Response Cookies Timing
headlibs.html
form-component.html

Base Html Page
Click on Submit
Submit Button

```
{"token":"eyJleHAiOjE0ODY5NjEwNDksImlhdCI6MTQ4Njk2MDQ0OX0.8ilLzuLRdqQBkI09_-mAKCKatfJnw6rWHefGAmKvgOU"}
```

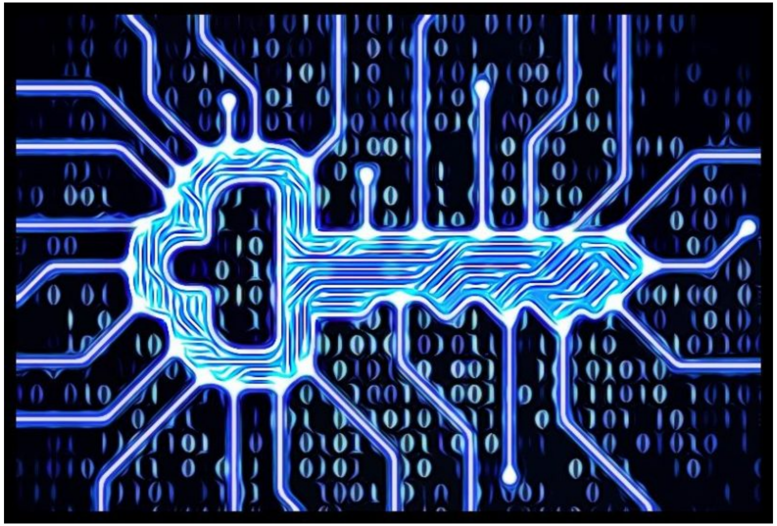
```html
<!--<sly data-sly-use.clientLib="/libs/granite/sightly/templates/clientlib.html" data-sly-call="${clientLib.js @ categories='granite.csrf.standalone'}" data-sly-unwrap/>-->

<div id="output">
    <div id="prompt">
        Click on Submit
    </div>
    <div id="result">
    </div>
</div>
<div style="...">
</div>

<sly data-sly-use.clientLib="/libs/granite/sightly/templates/clientlib.html" data-sly-call="${clientLib.js @ categories='granite.csrf.standalone'}" data-sly-unwrap/>


<form submit="#" id="servlet-form" method="post">
    <input type="submit" value="Submit Button" id="submit-button"/>
</form>
```

Protect against Cross-Site Request Forgery

The framework makes use of tokens to guarantee that the client request is legitimate

Dependencies
Any component that relies on the **granite.jquery** dependency will benefit from the CSRF Protection Framework automatically. If this is not the case for any of your components,
you must declare a dependency to **granite.csrf.standalone** before you can use the framework.

Replicating the Crypto Key
In order to make use of the tokens, you need to replicate the **/etc/keys/hmac** binary to all of the instances in your deployment.



Generating the CSRF token

1. An authenticated user can only generate the CSRF token. It implies unauthenticated access to the system is prevented.

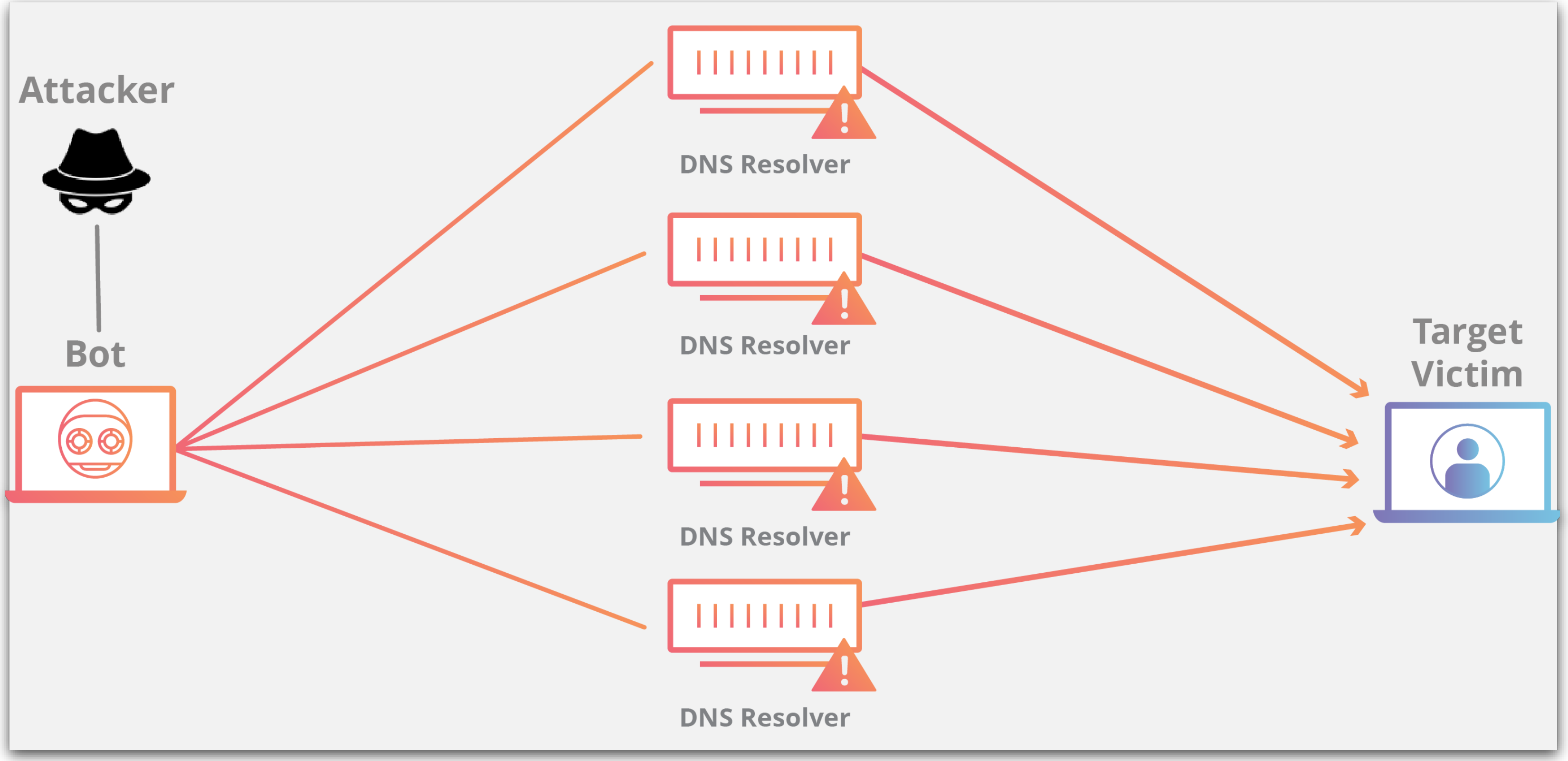
2. Accessing **/libs/granite/csrf/token.json** will generate the token as {“token”:”ey….U0”}.

3. This token will consists of two values. {“exp”:,”iat”:}.

Injection: The generated token has to be sent as a header to the post request like CSRF-TOKEN:.

NOTE: The dispatcher configuration need to allow the url **/libs/granite/csrf/token.json** and CSRF-TOKEN header.

Denial of Service (DoS/DDos) Attacks



AXAMIT

What can we do?

- Control the selectors in your application, so that you only serve the explicit selectors needed and return 404 for all others.

- Prevent the output of an unlimited number of content nodes.

In particular the JSON renderer which can transverse the tree structure over multiple levels.

- **http://localhost:4502/.json** could dump the whole repository in a JSON representation.

- This would cause significant server problems.

For this reason **Sling** sets a limit on the number of maximum results.

To limit the depth of the JSON rendering you can set the value for:
JSON Max results (**json.maximumresults**).
Use a firewall to filter access to your instance.

Questions & Answers

www.adobe.com.by
fb.com/groups/AEMBelarus/

AXAMIT