Fortify Audit Workbench

Developer Workbook

wordpress-scan_audited

Table of Contents

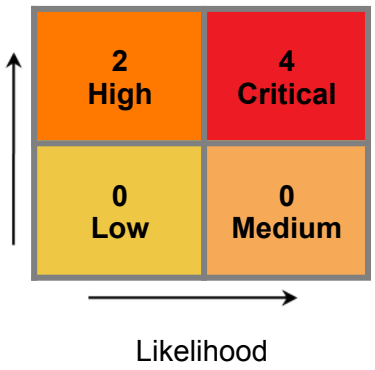
Executive Summary

This workbook is intended to provide all necessary details and information for a developer to understand and remediate the different issues discovered during the wordpress-scan_audited project audit. The information contained in this workbook is targeted at project managers and developers.

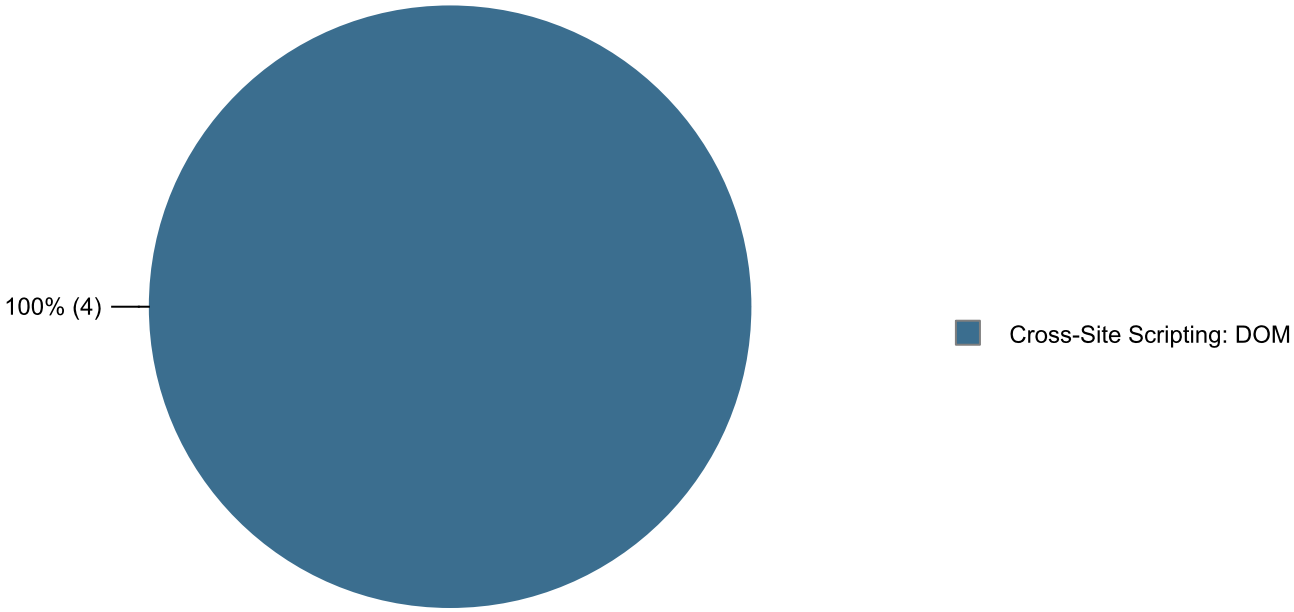
This section provides an overview of the issues uncovered during analysis.

Project Name:	wordpress-scan_audited
Project Version:	
SCA:	Results Present
WebInspect:	Results Not Present
WebInspect Agent:	Results Not Present
Other:	Results Not Present

Issues by Priority



Top Ten Critical Categories



Project Description

This section provides an overview of the Fortify scan engines used for this project, as well as the project meta-information.

SCA

Date of Last Analysis:	May 16, 2022, 2:35 PM	**Engine Version:**	21.2.3.0005
Host Name:	sp-scan02	**Certification:**	VALID
Number of Files:	41	**Lines of Code:**	2,833

Rulepack Name	Rulepack Version
Fortify Secure Coding Rules, Community, Cloud	2022.1.0.0007
Fortify Secure Coding Rules, Community, PHP	2022.1.0.0007
Fortify Secure Coding Rules, Community, Universal	2022.1.0.0007
Fortify Secure Coding Rules, Core, JavaScript	2022.1.0.0007
Fortify Secure Coding Rules, Core, PHP	2022.1.0.0007
Fortify Secure Coding Rules, Core, Universal	2022.1.0.0007
Fortify Secure Coding Rules, Extended, Configuration	2022.1.0.0007
Fortify Secure Coding Rules, Extended, Content	2022.1.0.0007
Fortify Secure Coding Rules, Extended, JavaScript	2022.1.0.0007

Issue Breakdown by Fortify Categories

The following table depicts a summary of all issues grouped vertically by Fortify Category. For each category, the total number of issues is shown by Fortify Priority Order, including information about the number of audited issues.

Category	Fortify Priority (audited/total)				Total Issues
	Critical	High	Medium	Low	
Cookie Security: Overly Broad Path	0	2 / 2	0	0	2 / 2
Cross-Site Scripting: DOM	4 / 4	0	0	0	4 / 4

Results Outline

Cookie Security: Overly Broad Path (2 issues)

Abstract

A cookie with an overly broad path can be accessed through other applications on the same domain.

Explanation

Developers often set cookies to be accessible from the root context path ("/"). This exposes the cookie to all web applications on the domain. Because cookies often carry sensitive information such as session identifiers, sharing cookies across applications can cause a vulnerability in one application to compromise another application. **Example 1:** Imagine you have a forum application deployed at `http://communitypages.example.com/MyForum` and the application sets a session ID cookie with path "/" when users log in to the forum. For example:

```
  setcookie("mySessionId", getSessionID(), 0, "/",
"communitypages.example.com", true, true);
```

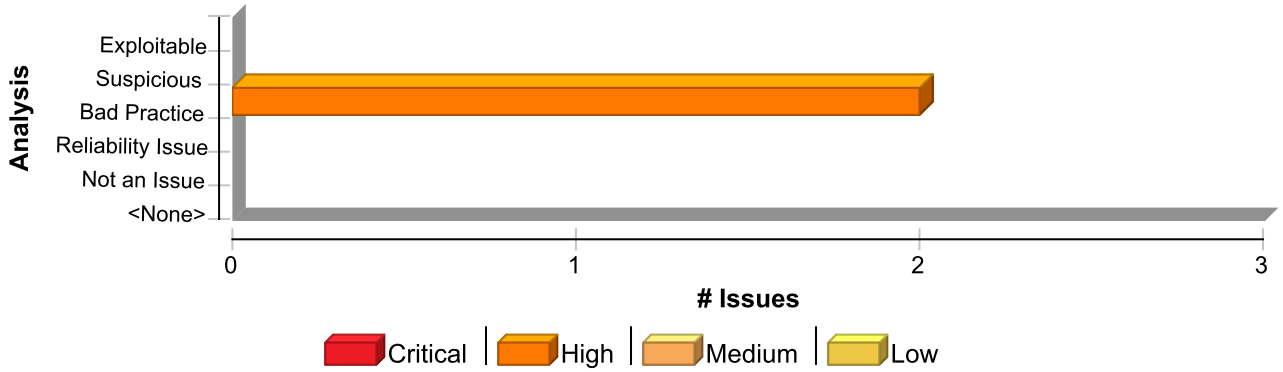
Suppose an attacker creates another application at `http://communitypages.example.com/EvilSite` and posts a link to this site on the forum. When a user of the forum clicks this link, the browser will send the cookie set by `/MyForum` to the application running at `/EvilSite`. By stealing the session ID, the attacker can compromise the account of any forum user that browsed to `/EvilSite`. In addition to reading a cookie, it might be possible for attackers to perform a Cookie Poisoning attack by using `/EvilSite` to create its own overly broad cookie that overwrites the cookie from `/MyForum`.

Recommendation

Make sure to set cookie paths to be as restrictive as possible. **Example 2:** The following code shows how to set the cookie path to "/MyForum" for the example in the Explanation section.

```
setcookie("mySessionId", getSessionID(), 0, "/MyForum",
"communitypages.example.com", true, true);
```

Issue Summary



Engine Breakdown

	SCA	WebInspect	SecurityScope	Total
Cookie Security: Overly Broad Path	2	0	0	2
Total	**2**	**0**	**0**	**2**

Cookie Security: Overly Broad Path — High

Package: saml

saml/class-eidlogin-saml.php, line 479 (Cookie Security: Overly Broad Path) — High

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Semantic)

Audit Details

Analysis Bad Practice

Audit Comments

aelchlepp: Fri May 20 2022 10:59:38 GMT+0200 (CEST)
if used in subdirectory this might be a problem

Sink Details

Sink: setcookie()
Enclosing Method: process_saml_response_data()
File: saml/class-eidlogin-saml.php:479
Taint Flags:

```
476
477  $cookie_id_cookie = filter_var( wp_unslash( $_COOKIE[ self::COOKIE_NAME ] ), FILTER_SANITIZE_STRING );
478  // Delete the cookie by setting its expiration date to the past.
479  setcookie( self::COOKIE_NAME, '', time() - 1, '/', '', true, true );
480
481  if ( $cookie_id_cookie !== $cookie_id_response ) {
482  $msg = sprintf(
```

saml/class-eidlogin-saml.php, line 177 (Cookie Security: Overly Broad Path) — High

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Semantic)

Audit Details

Analysis Bad Practice

Audit Comments

aelchlepp: Fri May 20 2022 10:59:38 GMT+0200 (CEST)
if used in subdirectory this might be a problem

Sink Details

Sink: setcookie()
Enclosing Method: saml_login()
File: saml/class-eidlogin-saml.php:177
Taint Flags:

```
174  // Create a random unique ID and save it in a cookie.
175  $cookie_id = Eidlogin_Helper::random_string();
176  Eidlogin_Helper::write_log( $cookie_id, 'Created unique cookie id: ' );
177  setcookie( self::COOKIE_NAME, $cookie_id, time() + 60 * 5, '/', '', true, true );
178
179  // Data we need to continue after returning.
```

Cookie Security: Overly Broad Path	High
Package: saml	
saml/class-eidlogin-saml.php, line 177 (Cookie Security: Overly Broad Path)	**High**

```
180   $continue = array(
```

Cross-Site Scripting: DOM (4 issues)

Abstract

Sending unvalidated data to a web browser can result in the browser executing malicious code.

Explanation

Cross-site scripting (XSS) vulnerabilities occur when: 1. Data enters a web application through an untrusted source. In the case of DOM-based XSS, data is read from a URL parameter or other value within the browser and written back into the page with client-side code. In the case of reflected XSS, the untrusted source is typically a web request, while in the case of persisted (also known as stored) XSS it is typically a database or other back-end data store. 2. The data is included in dynamic content that is sent to a web user without validation. In the case of DOM-based XSS, malicious content is executed as part of DOM (Document Object Model) creation, whenever the victim's browser parses the HTML page. The malicious content sent to the web browser often takes the form of a JavaScript segment, but can also include HTML, Flash or any other type of code that the browser executes. The variety of attacks based on XSS is almost limitless, but they commonly include transmitting private data like cookies or other session information to the attacker, redirecting the victim to web content controlled by the attacker, or performing other malicious operations on the user's machine under the guise of the vulnerable site. **Example 1:** The following JavaScript code segment reads an employee ID, `eid`, from a URL and displays it to the user.

```
<SCRIPT>
var pos=document.URL.indexOf("eid=")+4;
document.write(document.URL.substring(pos,document.URL.length));
</SCRIPT>
```

Example 2: Consider the HTML form:

```
  <div id="myDiv">
    Employee ID: <input type="text" id="eid"><br>
    ...
    <button>Show results</button>
  </div>
  <div id="resultsDiv">
    ...
  </div>
```

The following jQuery code segment reads an employee ID from the form, and displays it to the user.

```
  $(document).ready(function(){
    $("#myDiv").on("click", "button", function(){
      var eid = $("#eid").val();
      $("resultsDiv").append(eid);
      ...
    });
  });
```

These code examples operate correctly if the employee ID from the text input with ID `eid` contains only standard alphanumeric text. If `eid` has a value that includes metacharacters or source code, then the code will be executed by the web browser as it displays the HTTP response. **Example 3:** The following code shows an example of a DOM-based XSS within a React application:

```
let element = JSON.parse(getUntrustedInput());
ReactDOM.render(<App>
    {element}
</App>);
```

In `Example 3`, if an attacker can control the entire JSON object retrieved from `getUntrustedInput()`, they may be able to make React render `element` as a component, and therefore can pass an object with `dangerouslySetInnerHTML` with their own controlled value, a typical cross-site scripting attack. Initially these might not appear to be much of a vulnerability. After all, why would someone provide input containing malicious code to run on their own computer? The real danger is that an attacker will create the malicious

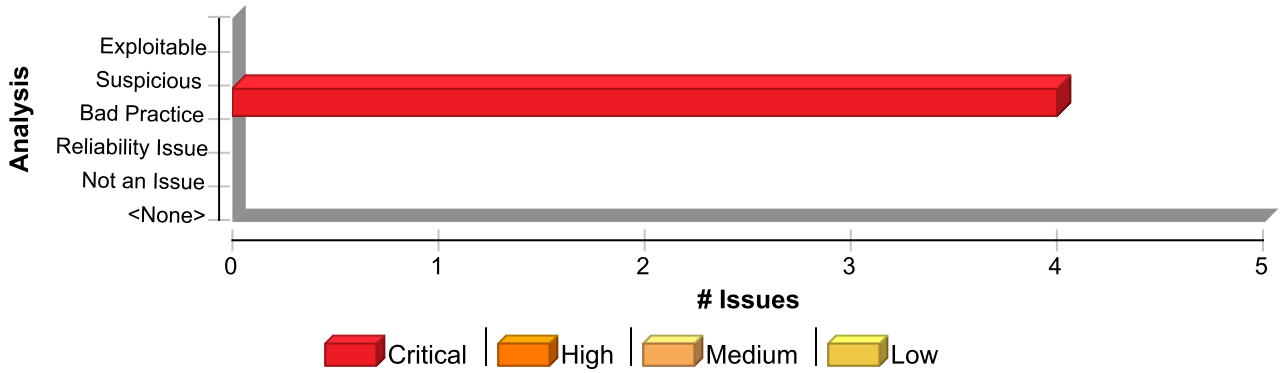
URL, then use email or social engineering tricks to lure victims into visiting a link to the URL. When victims click the link, they unwittingly reflect the malicious content through the vulnerable web application back to their own computers. This mechanism of exploiting vulnerable web applications is known as Reflected XSS. As the example demonstrates, XSS vulnerabilities are caused by code that includes unvalidated data in an HTTP response. There are three vectors by which an XSS attack can reach a victim: - Data is read directly from the HTTP request and reflected back in the HTTP response. Reflected XSS exploits occur when an attacker causes a user to supply dangerous content to a vulnerable web application, which is then reflected back to the user and executed by the web browser. The most common mechanism for delivering malicious content is to include it as a parameter in a URL that is posted publicly or emailed directly to victims. URLs constructed in this manner constitute the core of many phishing schemes, whereby an attacker convinces victims to visit a URL that refers to a vulnerable site. After the site reflects the attacker's content back to the user, the content is executed and proceeds to transfer private information, such as cookies that may include session information, from the user's machine to the attacker or perform other nefarious activities. - The application stores dangerous data in a database or other trusted data store. The dangerous data is subsequently read back into the application and included in dynamic content. Persistent XSS exploits occur when an attacker injects dangerous content into a data store that is later read and included in dynamic content. From an attacker's perspective, the optimal place to inject malicious content is in an area that is displayed to either many users or particularly interesting users. Interesting users typically have elevated privileges in the application or interact with sensitive data that is valuable to the attacker. If one of these users executes malicious content, the attacker may be able to perform privileged operations on behalf of the user or gain access to sensitive data belonging to the user. - A source outside the application stores dangerous data in a database or other data store, and the dangerous data is subsequently read back into the application as trusted data and included in dynamic content.

Recommendation

The solution to XSS is to ensure that validation occurs in the correct places and checks are made for the correct properties. Because XSS vulnerabilities occur when an application includes malicious data in its output, one logical approach is to validate data immediately before it leaves the application. However, because web applications often have complex and intricate code for generating dynamic content, this method is prone to errors of omission (missing validation). An effective way to mitigate this risk is to also perform input validation for XSS. Web applications must validate their input to prevent other vulnerabilities, such as SQL injection, so augmenting an application's existing input validation mechanism to include checks for XSS is generally relatively easy. Despite its value, input validation for XSS does not take the place of rigorous output validation. An application might accept input through a shared data store or other trusted source, and that data store might accept input from a source that does not perform adequate input validation. Therefore, the application cannot implicitly rely on the safety of this or any other data. This means that the best way to prevent XSS vulnerabilities is to validate everything that enters the application and leaves the application destined for the user. The most secure approach to validation for XSS is to create an allow list of safe characters that are permitted to appear in HTTP content and accept input composed exclusively of characters in the approved set. For example, a valid username might only include alphanumeric characters or a phone number might only include digits 0-9. However, this solution is often infeasible in web applications because many characters that have special meaning to the browser must be considered valid input after they are encoded, such as a web design bulletin board that must accept HTML fragments from its users. A more flexible, but less secure approach is to implement a deny list, which selectively rejects or escapes potentially dangerous characters before using the input. To form such a list, you first need to understand the set of characters that hold special meaning for web browsers. Although the HTML standard defines which characters have special meaning, many web browsers try to correct common mistakes in HTML and might treat other characters as special in certain contexts. This is why we do not recommend the use of deny lists as a means to prevent XSS. The CERT(R) Coordination Center at the Software Engineering Institute at Carnegie Mellon University provides the following details about special characters in various contexts [1]: In the content of a block-level element (in the middle of a paragraph of text): - "<" is special because it introduces a tag. - "&" is special because it introduces a character entity. - ">" is special because some browsers treat it as special, on the assumption that the author of the page intended to include an opening "<", but omitted it in error. The following principles apply to attribute values: - In attribute values enclosed in double quotes, the double quotes are special because

they mark the end of the attribute value. - In attribute values enclosed in single quote, the single quotes are special because they mark the end of the attribute value. - In attribute values without any quotes, white-space characters, such as space and tab, are special. - "&" is special when used with certain attributes, because it introduces a character entity. In URLs, for example, a search engine might provide a link within the results page that the user can click to re-run the search. This can be implemented by encoding the search query inside the URL, which introduces additional special characters: - Space, tab, and new line are special because they mark the end of the URL. - "&" is special because it either introduces a character entity or separates CGI parameters. - Non-ASCII characters (that is, everything greater than 127 in the ISO-8859-1 encoding) are not allowed in URLs, so they are considered to be special in this context. - The "%" symbol must be filtered from input anywhere parameters encoded with HTTP escape sequences are decoded by server-side code. For example, "%" must be filtered if input such as "%68%65%6C%6C%6F" becomes "hello" when it appears on the web page. Within the body of a : - Semicolons, parentheses, curly braces, and new line characters must be filtered out in situations where text could be inserted directly into a pre-existing script tag. Server-side scripts: - Server-side scripts that convert any exclamation characters (!) in input to double-quote characters (") on output might require additional filtering. Other possibilities: - If an attacker submits a request in UTF-7, the special character '<' appears as '+ADw-' and might bypass filtering. If the output is included in a page that does not explicitly specify an encoding format, then some browsers try to intelligently identify the encoding based on the content (in this case, UTF-7). After you identify the correct points in an application to perform validation for XSS attacks and what special characters the validation should consider, the next challenge is to identify how your validation handles special characters. If special characters are not considered valid input to the application, then you can reject any input that contains special characters as invalid. A second option is to remove special characters with filtering. However, filtering has the side effect of changing any visual representation of the filtered content and might be unacceptable in circumstances where the integrity of the input must be preserved for display. If input containing special characters must be accepted and displayed accurately, validation must encode any special characters to remove their significance. A complete list of ISO 8859-1 encoded values for special characters is provided as part of the official HTML specification [2]. Many application servers attempt to limit an application's exposure to cross-site scripting vulnerabilities by providing implementations for the functions responsible for setting certain specific HTTP response content that perform validation for the characters essential to a cross-site scripting attack. Do not rely on the server running your application to make it secure. For any developed application, there are no guarantees about which application servers it will run on during its lifetime. As standards and known exploits evolve, there are no guarantees that application servers will continue to stay in sync.

Issue Summary



Engine Breakdown

	SCA	WebInspect	SecurityScope	Total
Cross-Site Scripting: DOM	4	0	0	4
Total	**4**	**0**	**0**	**4**

Cross-Site Scripting: DOM — Critical

Package: admin.js

admin/js/eidlogin-admin.js, line 568 (Cross-Site Scripting: DOM) — Critical

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Data Flow)

Audit Details

Analysis Bad Practice

Audit Comments

aelchlepp: Fri May 20 2022 10:57:09 GMT+0200 (CEST)
There is no reason to use innerHTML here

Source Details

Source: Read responseText
From: lambda
File: admin/js/eidlogin-admin.js:565

```
562  const errorMsg = 'Certificate Rollover could not be prepared';
563  var xhr = new XMLHttpRequest();
564  xhr.addEventListener('load', (e) => {
565  let resp = JSON.parse(e.target.responseText);
566  if (e.target.status == 200 && resp.status == 'success') {
567  certNewDiv.innerHTML = '... ' + resp.cert_new;
568  certNewEncDiv.innerHTML = '... ' + resp.cert_new_enc;
```

Sink Details

Sink: Assignment to certNewEncDiv.innerHTML
Enclosing Method: lambda()
File: admin/js/eidlogin-admin.js:568
Taint Flags: JS_OBJECT_CONTROLLED, WEB, XSS

```
565  let resp = JSON.parse(e.target.responseText);
566  if (e.target.status == 200 && resp.status == 'success') {
567  certNewDiv.innerHTML = '... ' + resp.cert_new;
568  certNewEncDiv.innerHTML = '... ' + resp.cert_new_enc;
569  buttonRolloverExec.disabled = false;
570  spanRolloverExec.classList.add('hidden');
571
```

admin/js/eidlogin-admin.js, line 567 (Cross-Site Scripting: DOM) — Critical

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Data Flow)

Audit Details

Analysis Bad Practice

Cross-Site Scripting: DOM — Critical

Package: admin.js

admin/js/eidlogin-admin.js, line 567 (Cross-Site Scripting: DOM) — Critical

Audit Comments

aelchlepp: Fri May 20 2022 10:57:09 GMT+0200 (CEST)
There is no reason to use innerHTML here

Source Details

Source: Read responseText
From: lambda
File: admin/js/eidlogin-admin.js:565

```
562  const errorMsg = 'Certificate Rollover could not be prepared';
563  var xhr = new XMLHttpRequest();
564  xhr.addEventListener('load', (e) => {
565  let resp = JSON.parse(e.target.responseText);
566  if (e.target.status == 200 && resp.status == 'success') {
567  certNewDiv.innerHTML = '... ' + resp.cert_new;
568  certNewEncDiv.innerHTML = '... ' + resp.cert_new_enc;
```

Sink Details

Sink: Assignment to certNewDiv.innerHTML
Enclosing Method: lambda()
File: admin/js/eidlogin-admin.js:567
Taint Flags: JS_OBJECT_CONTROLLED, WEB, XSS

```
564  xhr.addEventListener('load', (e) => {
565  let resp = JSON.parse(e.target.responseText);
566  if (e.target.status == 200 && resp.status == 'success') {
567  certNewDiv.innerHTML = '... ' + resp.cert_new;
568  certNewEncDiv.innerHTML = '... ' + resp.cert_new_enc;
569  buttonRolloverExec.disabled = false;
570  spanRolloverExec.classList.add('hidden');
```

admin/js/eidlogin-admin.js, line 614 (Cross-Site Scripting: DOM) — Critical

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Data Flow)

Audit Details

Analysis	Bad Practice

Audit Comments

aelchlepp: Fri May 20 2022 10:57:09 GMT+0200 (CEST)
There is no reason to use innerHTML here

Source Details

Source: Read responseText
From: lambda
File: admin/js/eidlogin-admin.js:612

Cross-Site Scripting: DOM — Critical

Package: admin.js

admin/js/eidlogin-admin.js, line 614 (Cross-Site Scripting: DOM) — Critical

```
609  const errorMsg = 'Certificate Rollover could not be executed';
610  var xhr = new XMLHttpRequest();
611  xhr.addEventListener('load', (e) => {
612  let resp = JSON.parse(e.target.responseText);
613  if (e.target.status == 200 && resp.status == 'success') {
614  certActDiv.innerHTML = '... ' + resp.cert_act;
615  certActEncDiv.innerHTML = '... ' + resp.cert_act_enc;
```

Sink Details

Sink: Assignment to certActDiv.innerHTML
Enclosing Method: lambda()
File: admin/js/eidlogin-admin.js:614
Taint Flags: JS_OBJECT_CONTROLLED, WEB, XSS

```
611  xhr.addEventListener('load', (e) => {
612  let resp = JSON.parse(e.target.responseText);
613  if (e.target.status == 200 && resp.status == 'success') {
614  certActDiv.innerHTML = '... ' + resp.cert_act;
615  certActEncDiv.innerHTML = '... ' + resp.cert_act_enc;
616  certNewDiv.innerHTML = __('No new certificate prepared yet.', 'eidlogin');
617  certNewEncDiv.innerHTML = __('No new certificate prepared yet.', 'eidlogin');
```

admin/js/eidlogin-admin.js, line 615 (Cross-Site Scripting: DOM) — Critical

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Data Flow)

Audit Details

Analysis Bad Practice

Audit Comments

aelchlepp: Fri May 20 2022 10:57:09 GMT+0200 (CEST)
There is no reason to use innerHTML here

Source Details

Source: Read responseText
From: lambda
File: admin/js/eidlogin-admin.js:612

```
609  const errorMsg = 'Certificate Rollover could not be executed';
610  var xhr = new XMLHttpRequest();
611  xhr.addEventListener('load', (e) => {
612  let resp = JSON.parse(e.target.responseText);
613  if (e.target.status == 200 && resp.status == 'success') {
614  certActDiv.innerHTML = '... ' + resp.cert_act;
```

Cross-Site Scripting: DOM — Critical

Package: admin.js

admin/js/eidlogin-admin.js, line 615 (Cross-Site Scripting: DOM) — Critical

```
615  certActEncDiv.innerHTML = '... ' + resp.cert_act_enc;
```

Sink Details

Sink: Assignment to certActEncDiv.innerHTML
Enclosing Method: lambda()
File: admin/js/eidlogin-admin.js:615
Taint Flags: JS_OBJECT_CONTROLLED, WEB, XSS

```
612  let resp = JSON.parse(e.target.responseText);
613  if (e.target.status == 200 && resp.status == 'success') {
614  certActDiv.innerHTML = '... ' + resp.cert_act;
615  certActEncDiv.innerHTML = '... ' + resp.cert_act_enc;
616  certNewDiv.innerHTML = __('No new certificate prepared yet.', 'eidlogin');
617  certNewEncDiv.innerHTML = __('No new certificate prepared yet.', 'eidlogin');
618
```