UMGANG MIT EINGABEN IN WEBANWENDUNGEN

Meetup 21.02.2018 - Sergej Michel

WAS SIND EINGABEN IN WEBANWENDUNGEN?

https://www.posch.com/cms/wp-content/uploads/2016/03/holzhacker-posch-hackblitz-1086x725.jpg

HTTP REQUEST

POST https://www.wordpress-example.com/wp-login.php&exampleparam=value HTTP/1.1

Host: www.wordpress-example.com
User-Agent: Lynx/2.8.4rel.1 libwww-FM/2.14 SSL-MM/1.4.1 OpenSSL/0.9.6c
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://www.wordpress-example.com/wp-login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 128
Cookie: wordpress_test_cookie=WP+Cookie+check
Connection: keep-alive
Upgrade-Insecure-Requests: 1

log=admin&pwd=password&wp-submit=Log+In&redirect_to=https%3A%2F%2Fwww.wordpress-example.com&testcookie=1

DER UMGANG MIT EINGABEN

LÄNGE DER EINGABE SERVERSEITIG BESCHRÄNKEN

https://i.pinimg.com/originals/ee/2b/9d/ee2b9ddf255b5059e80492204365 63e7.jpg

AUF MÖGLICHE ZEICHEN BESCHRÄNKEN

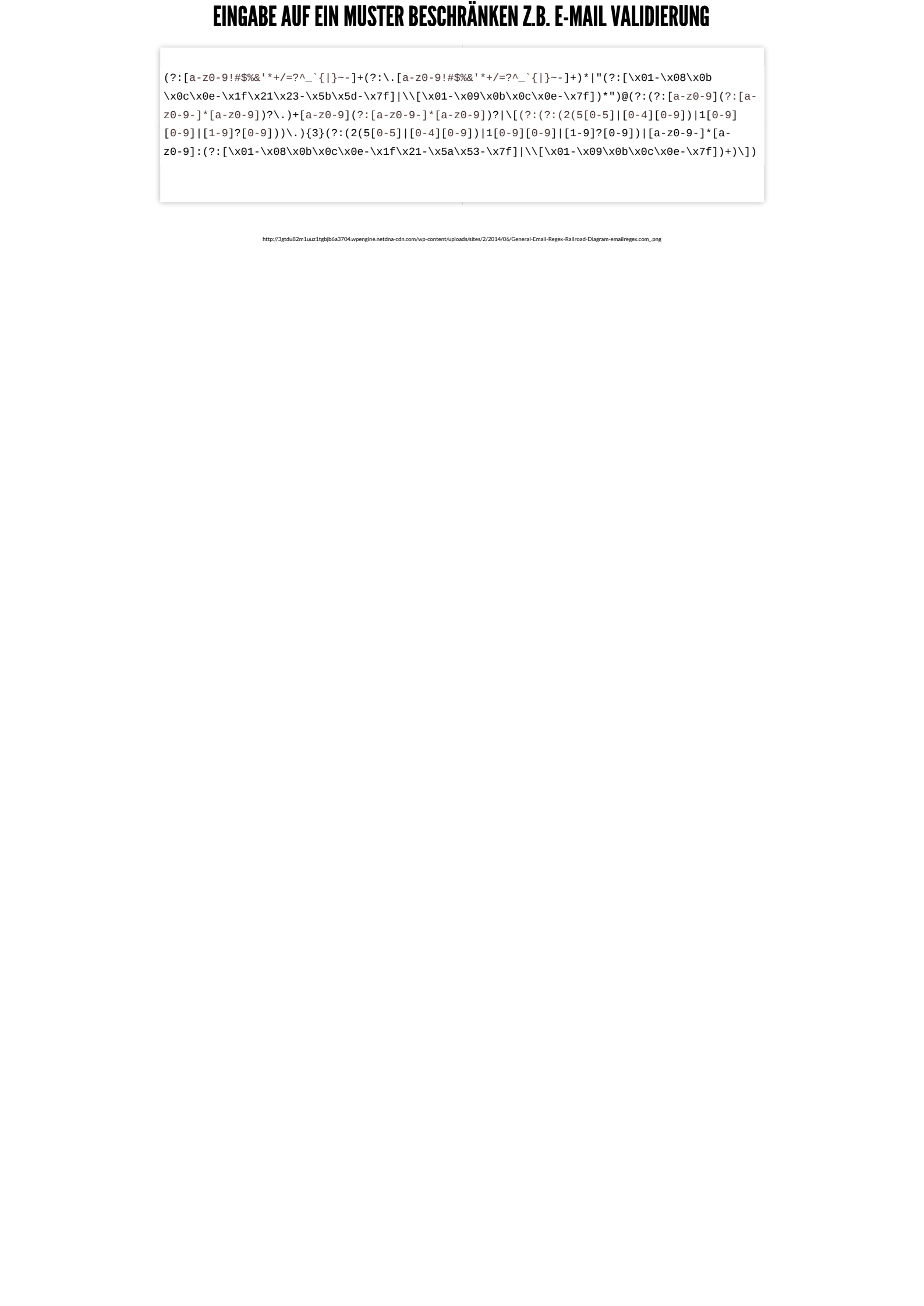
```
^[a-zA-Z0-9]+$
```

BESCHRÄNKEN AUF DATENTYPEN Z.B. INTEGER FÜR EINE ZAHL

```
Integer.valueOf(request.getParameter("number"));
```

EINGABE AUF EIN MUSTER BESCHRÄNKEN Z.B. E-MAIL VALIDIERUNG

```
(?:[a-z0-9!#$%&'*+/=?^_`{|}~-]+(?:\.[a-z0-9!#$%&'*+/=?^_`{|}~-]+)*|"(?:[\x01-\x08\x0b
\x0c\x0e-\x1f\x21\x23-\x5b\x5d-\x7f]|\\[\x01-\x09\x0b\x0c\x0e-\x7f])*")@(?:(?:[a-z0-9](?:[a-
z0-9-]*[a-z0-9])?\.)+[a-z0-9](?:[a-z0-9-]*[a-z0-9])?|\[(?:(?:(2(5[0-5]|[0-4][0-9])|1[0-9]
[0-9]|[1-9]?[0-9]))\.){3}(?:(2(5[0-5]|[0-4][0-9])|1[0-9][0-9]|[1-9]?[0-9])|[a-z0-9-]*[a-
z0-9]:(?:[\x01-\x08\x0b\x0c\x0e-\x1f\x21-\x5a\x53-\x7f]|\\[\x01-\x09\x0b\x0c\x0e-\x7f])+)\])
```



NEGATIVBEISPIEL FÜR VALIDIERUNG NACH MUSTERN

```
<script>*</script>
```

BYPASS:

```
<script>*</script>
```

```
<script%00>alert(1)</script>
<script>alert(1)<script>
<img src="0" onerror="alert(1)" />
<details/open/ontoggle="alert`1`">
<audio src onloadstart=alert(1)>
<marquee onstart=alert(1)>
<svg/onload=alert('XSS')>
```

XSS VERHINDERN:

```
& --> &amp;
< --> &lt;
> --> &gt;
" --> &quot;
' --> &#x27;
/ --> &#x2F;
```

NEGATIVBEISPIEL DATEIPFAD VALIDIERUNG

```
filename = Request.QueryString(“file”);
Replace(filename, “/”,”\”);
Replace(filename, “..\”,””);
```

BYPASS:

```
filename = Request.QueryString(“file”);
Replace(filename, “/”,”\”);
Replace(filename, “..\”,””);
```

```
file=..../////boot.ini
file=....\\....\\boot.ini
file= ..\..\boot.ini
```

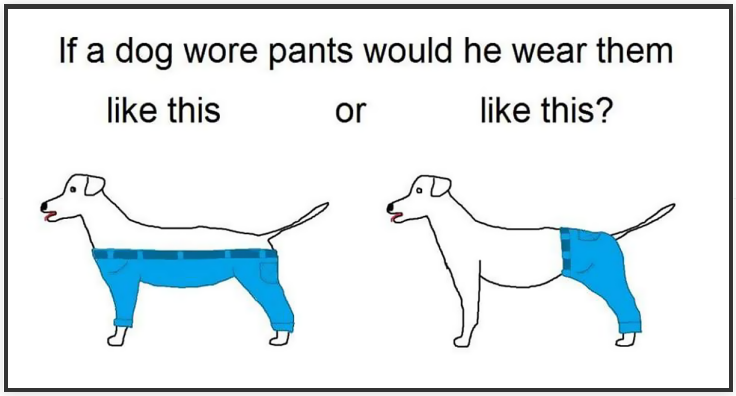
ANGRIFFSFLÄCHE REGEX BEISPIEL

```
^[a-zA-Z0-9]+$
```

EMPFEHLUNGEN

- Serverseite Prüfung
- First Line of Defense
- Injection Angriffe werden enorm erschwert
- Alle Eingaben prüfen
- Alle unbekannten Parameter werden per Default validiert

FRAGEN?



https://static.boredpanda.com/blog/wp-content/uploads/2015/12/tough-questions-funny-if-dog-wear-pants-fb.png