Dokumentation Übung 1

HTML/CSS

Mithilfe des HTML-Tags **<form>** habe ich ein Formular erstellt über welches der User seine Eingaben laut Angabe macht. Im HTML wird über das form-Attribut „**action**“ festgelegt wohin die Daten geschickt werden sollen und über das Attribut „**method**“ wird die HTTP-Methode festgelegt, für das Beispiel habe ich wie gefordert **POST** verwendet.

```
<form action="http://localhost/dasu/index.php" method="post">
```

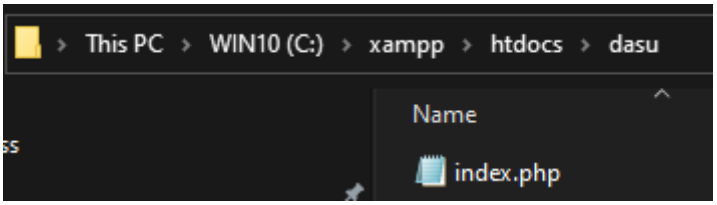
Drei Input Felder werden an das PHP-File geschickt:

- Passwortzeichenlänge
- Anzahl der Passwörter
- Alphabet

PHP

Den PHP-Server habe ich lokal über localhost laufen gelassen mithilfe des bekannten Tools „XAMPP“. Dies lädt man sich nur herunter und kann dann sofort per Mausklick den Apache Server starten, mehr ist nicht zu tun.

In dem **XAMPP** Folder **„htdocs“** habe ich dann einen Ordner erstellt „Dasu“ in dem mein **„index.php“** File liegt.



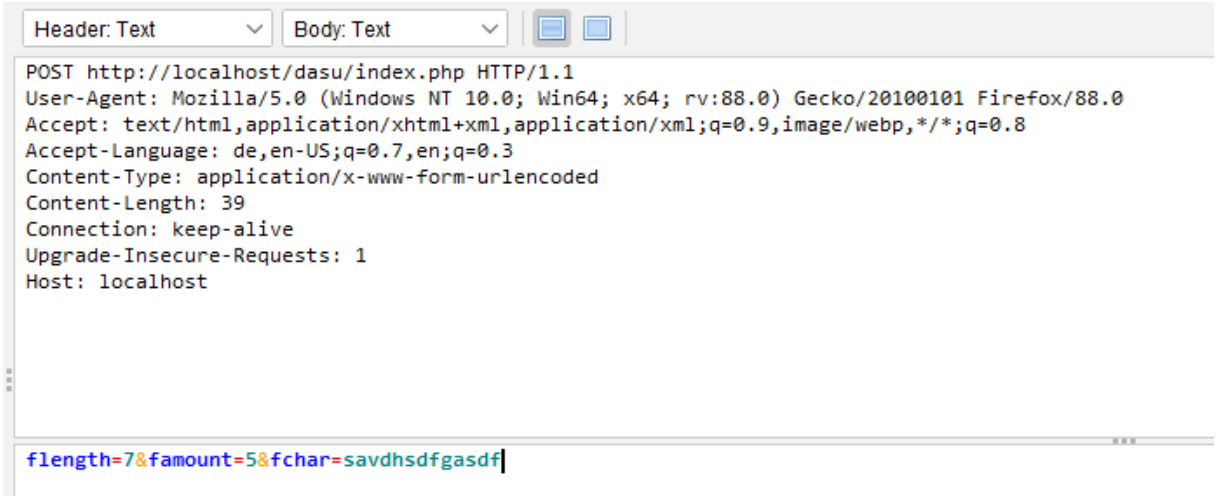
Dort ist die Logik der Passwortgenerierung gespeichert, die drei Parameter werden mithilfe der Methode $_Post übernommen und mit zwei weiteren Methoden substr() und str_shuffle() wird das Passwort zufällig generiert.

OWASP

Beobachtung der HTTP-Requests:

POST Request von der index.html zu dem localhost PHP Server

Request Header und Body:



Im Header sieht man einige Metadaten wie Zieladresse, User-Agent, Content-Type & -Length sowie den Host.
Im **Body** sieht man die mitgeschickten **Parameter**.

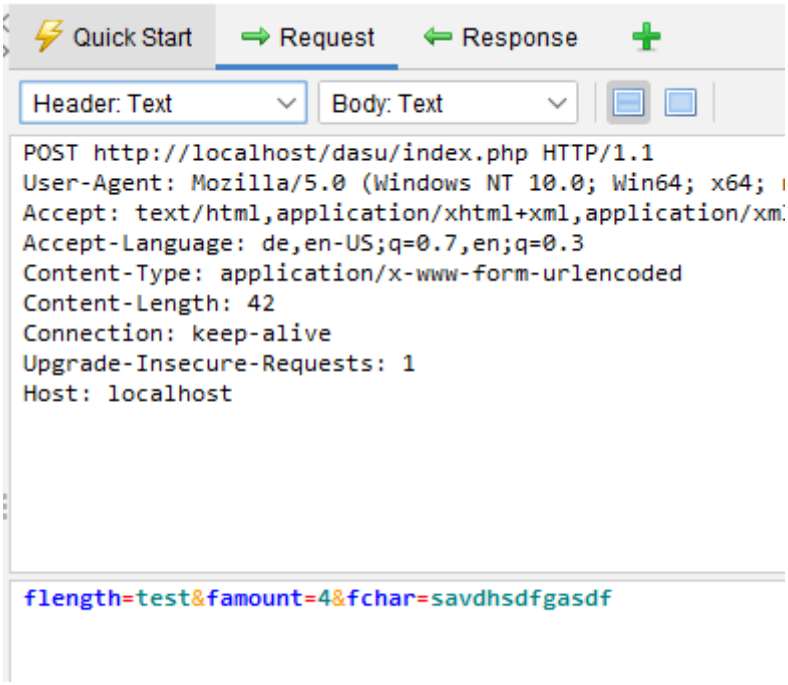
Response Header und Body:

Im Header sieht man wieder die Metadaten wie den Status Code, Datum und sogar Serverinformationen bzw. die PHP-Version.
Im Body sieht man die Antwort vom Server, sprich die generierten Passwörter.

Eingabebeschränkungen umgehen

Wenn man manuell versucht einen String in ein Int Feld einzugeben zB bei „Passwortzeichenlänge“ kommt eine Fehlermeldung „Bitte geben Sie eine Nummer ein“.

Mit dem Fuzzer von OWASP ZAP hat das jedoch gut funktioniert, im http request wurde statt einem int parameter flength=6, flength=test mitgeschickt und



Denial of Service

Trotz langer Recherche bin ich auf keine Möglichkeit gestoßen mit dem OWASP Zap Tool einen DoS Angriff auszuführen.