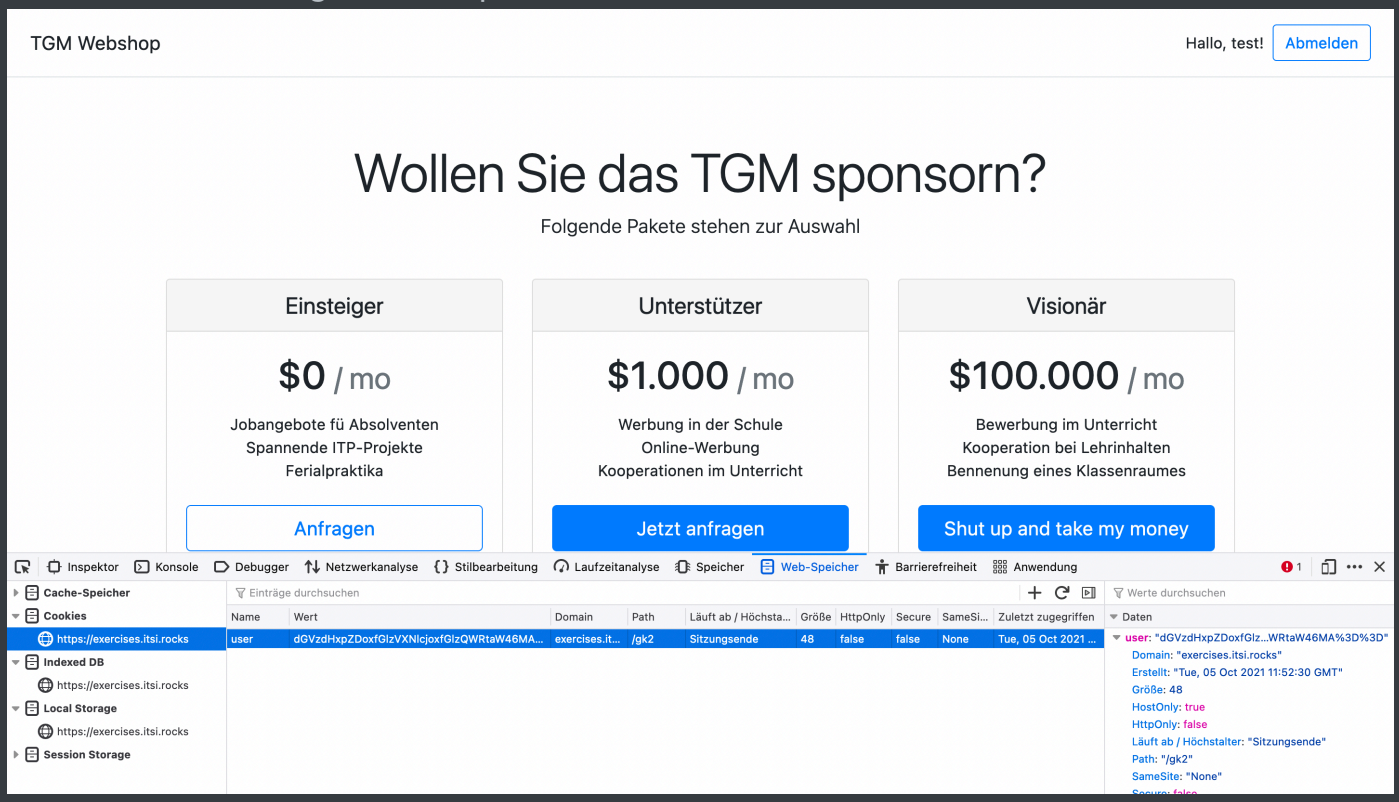
MEDT GK7.1 ITSI GK2 Kombinierte Angriffe auf Webseiten

von Simon Bachl 4CHIT

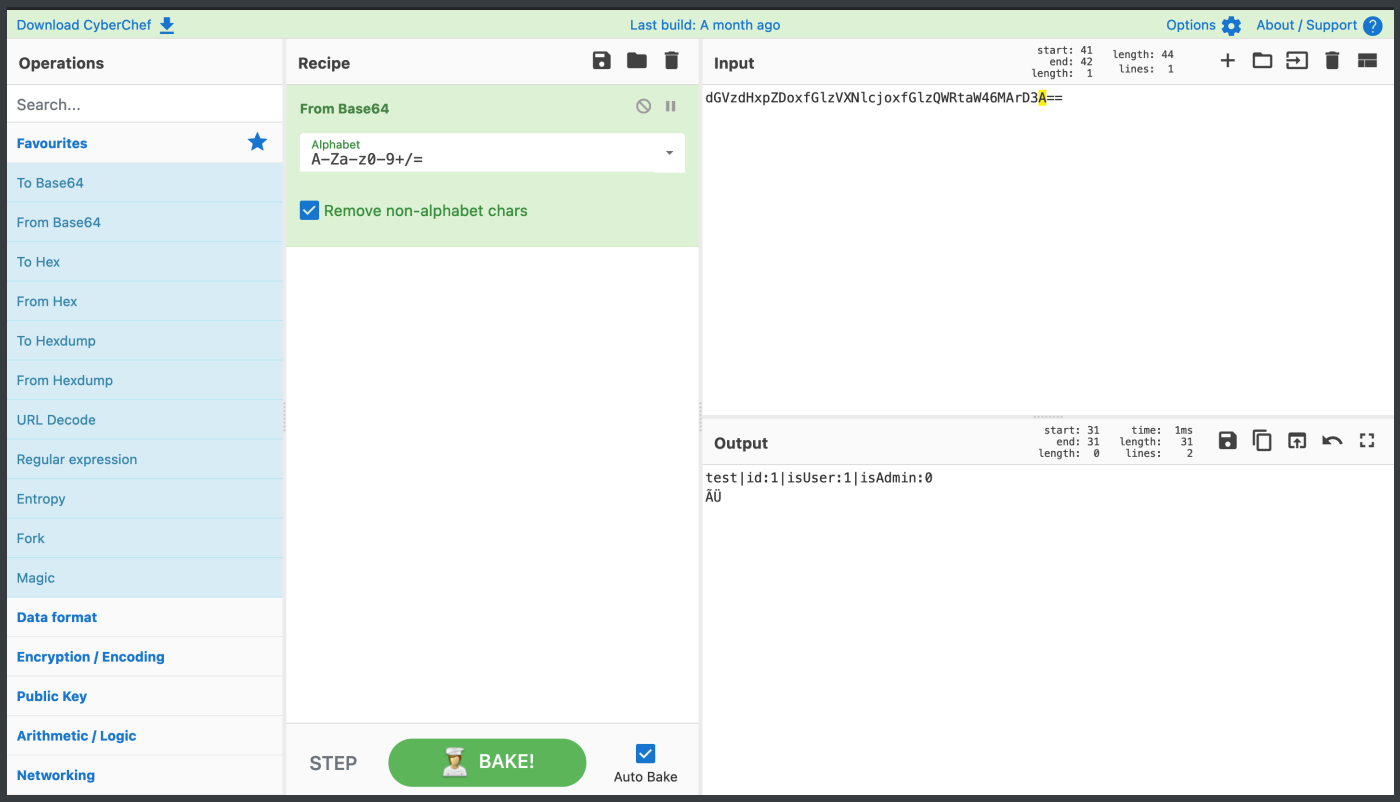
GK:

1) Die Anmeldung erfolgt durch eine SQL Injection. Wir geben im Loginfeld des Benutzers "' OR 1=1 --" ein. Im Hintergrund schaut das in etwa so aus:
"SELECT * FROM Benutzertabelle WHERE Ort = '' OR 1=1 --'". Mit diesem SQL Kommand sorgen wir dafür das der SELECT Befehl beendet und mit dem 1=1 auf des Benutzer auf true gesetzt wird, mit den -- sorgen wir dafür das alles danach auf einen Kommentar gesetzt wird, also das Passwort.

2) Der nächste Schritt ist es sich Adminrechte zu beschaffen. Zu aller erst lässt man sich seine Cookies anzeigen und kopiert den Wert.

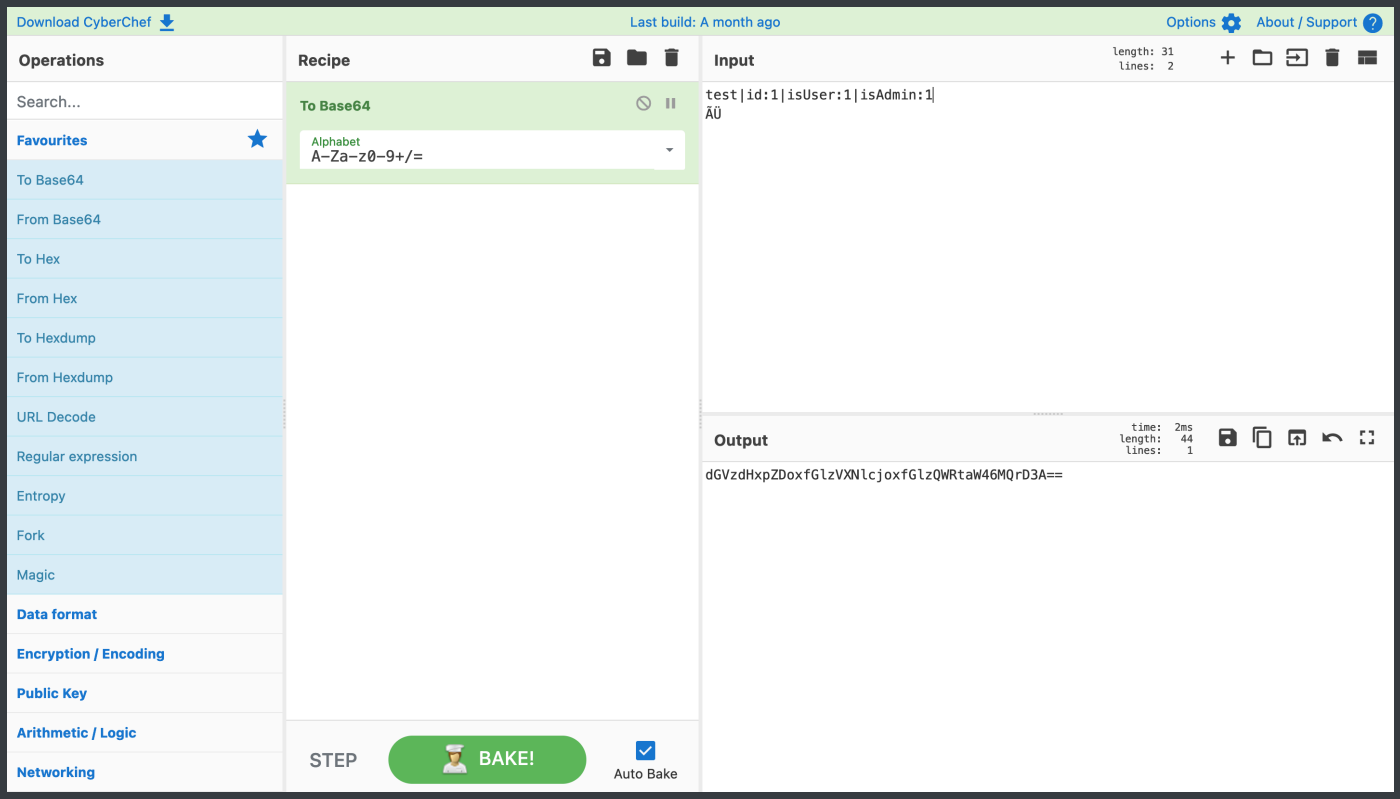


Den Wert fügen wir dann auf der Seite https://gchq.github.io/CyberChef/ ein

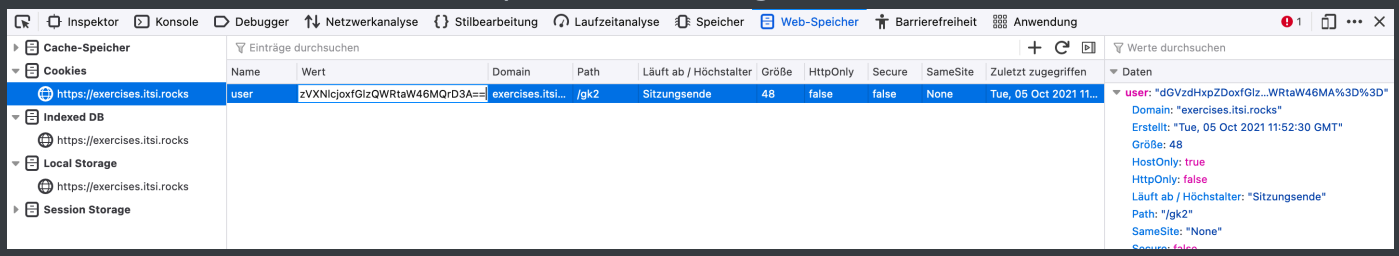


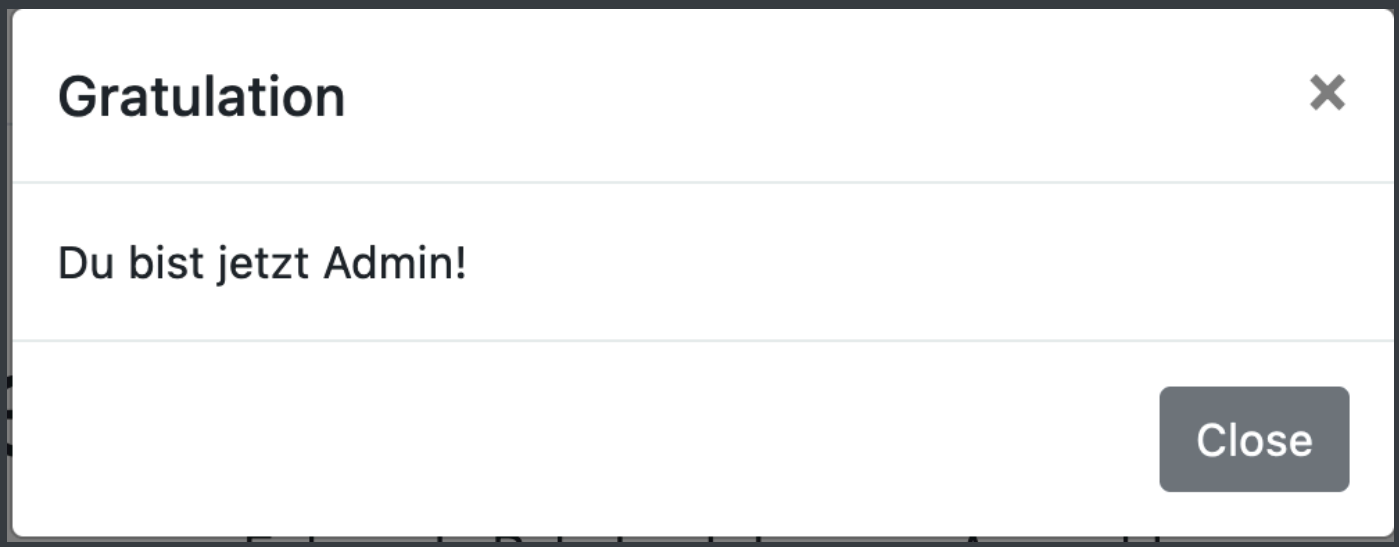
Den Wert entschlüsselt man dadürch.

Das entschlüsselte kopiert man fügt man oben ein und fügt bei dem Admin eine 1 ein und verschafft sich dadruch Adminrecht.



Den neu verschlüsselten Wert kopiert man und fügt man erneut bei den Cookies ein.

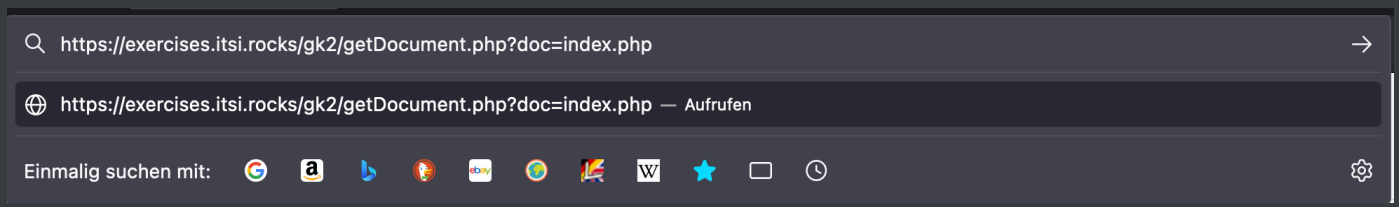




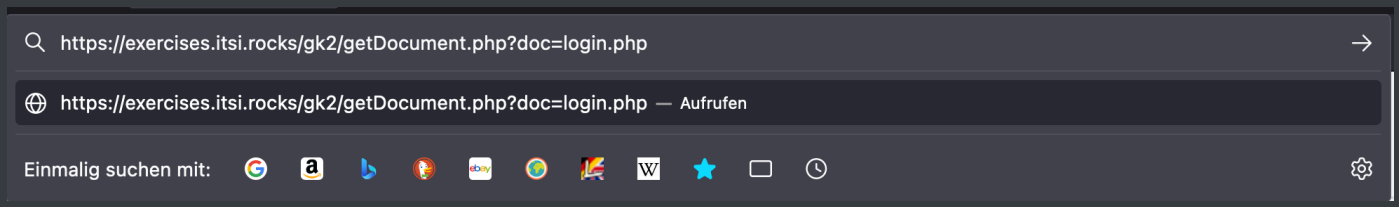
3) Ich habe mir den Quelltext der Seite angeschaut und mir ist aufgefallen das wenn man auf einen Downloadlink auf der Seite drückt die URL geändert wird

```
236 <h2> Im Moment sind leider keine weiteren Angebote verf&uuml;gbar.</h2>
237
238 <h3> Folgende Dokumente stehen zum Download: </h3>
239 <ul>
240     <li> <a href="getDocument.php?doc=documents/tgm.jpg">tgm.jpg</a> </li>
241     <li> <a href="getDocument.php?doc=documents/security.png">security.png</a> </li>
242     <li> <a href="getDocument.php?doc=documents/itsi-owasp-injections.pdf">itsi-owasp-injections.pdf</a> </li>
243     </div>
244       </div>
```

Durch die veränderung der URL kann man eine andere Datei runterladen wie zB die index.php was ich dann auch gemacht habe.



Das gleiche habe ich auch bei der login.php gemacht



Daraufhin habe ich beide geöffnet und geschaut wie die Datenbank heißt. In der index.php hat man den Filenamen der Datenbank gefunden.

```php
class MyDB extends SQLite3
{
    function __construct()
    {
        $this->open('database.sqlite', $flags = SQLITE3_OPEN_READONLY);
    }
}
```

Dann habe ich auf dem gleichen Weg wie die php Datein auch die Datenbank runtergeladen und in DB Browser for SQLite geöffnet.

Wenn man die Datenbank geöffnet hat geht man auf Daten durchsuchen und dann kann man die User auslesen

1	test	c6950b16eb377c99681a707f28befc04
2	chris	949de79c1bb85bd8e404c887de3043e4
3	user	92e9989866832dc00cc79e6a4f2d08c6

Schutz vor den Sicherheitslücken

SQL Injections: überprüfen ob die Eingabe überhaupt Sinn ergibt
Cookies: Diese nicht frei zugänglich machen
Travelpath: Whitelisten die der User benutzen darf