

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.

TGM Webshop

Hallo, test! [Abmelden](#)

Wollen Sie das TGM sponsorn?

Folgende Pakete stehen zur Auswahl

Einsteiger

\$0 / mo

Jobangebote für Absolventen
Spannende ITP-Projekte
Ferialpraktika

[Anfragen](#)

Unterstützer

\$1.000 / mo

Werbung in der Schule
Online-Werbung
Kooperationen im Unterricht

[Jetzt anfragen](#)

Visionär

\$100.000 / mo

Bewerbung im Unterricht
Kooperation bei Lehrinhalten
Benennung eines Klassenraumes

[Shut up and take my money](#)

Inspector Konsole Debugger Netzwerkanalyse Stilbearbeitung Laufzeitanalyse Speicher Web-Speicher Barrierefreiheit Anwendung

Cache-Speicher Cookies Indexed DB Local Storage Session Storage

Name	Wert	Domain	Path	Läuft ab / Höchststa...	Größe	HttpOnly	Secure	SameSi...	Zuletzt zugegriffen
user	dGVzdHxpZDoxfGlzVXNlcjoxfGlzQWRtaW46MA...	exercises.it...	/gk2	Sitzungsende	48	false	false	None	Tue, 05 Oct 2021 ...

Werte durchsuchen

Daten

user: "dGVzdHxpZDoxfGlzVXNlcjoxfGlzQWRtaW46MA%3D%3D"

Domain: "exercises.itsi.rocks"

Erstellt: "Tue, 05 Oct 2021 11:52:30 GMT"

Größe: 48

HostOnly: true

HttpOnly: false

Läuft ab / Höchstalter: "Sitzungsende"

Path: "/gk2"

SameSite: "None"

Secure: false

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

Download CyberChef

Last build: A month ago

Options

About / Support

Operations

Search...

Favourites

To Base64

From Base64

To Hex

From Hex

To Hexdump

From Hexdump

URL Decode

Regular expression

Entropy

Fork

Magic

Data format

Encryption / Encoding

Public Key

Arithmetic / Logic

Networking

Recipe

From Base64

Alphabet
A-Za-z0-9+/=

☒ Remove non-alphabet chars

STEP

BAKE!

Auto Bake

Input

start: 41
end: 42
length: 1

length: 44
Lines: 1

+

GVzdHxpZDoxfGZVXNlcjoxfGZQWRtaW46MARD3A==

Output

start: 31
end: 31
length: 0

time: 1ms
length: 31
Lines: 2

test | id:1 | isUser:1 | isAdmin:0
AU

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

Download CyberChef

Last build: A month ago

Options

About / Support

Operations

Search...

Favourites

To Base64

From Base64

To Hex

From Hex

To Hexdump

From Hexdump

URL Decode

Regular expression

Entropy

Fork

Magic

Data format

Encryption / Encoding

Public Key

Arithmetic / Logic

Networking

Recipe

To Base64

Alphabet
A-Za-z0-9+/=

STEP

BAKE!

Auto Bake

Input

length: 31
Lines: 2

+

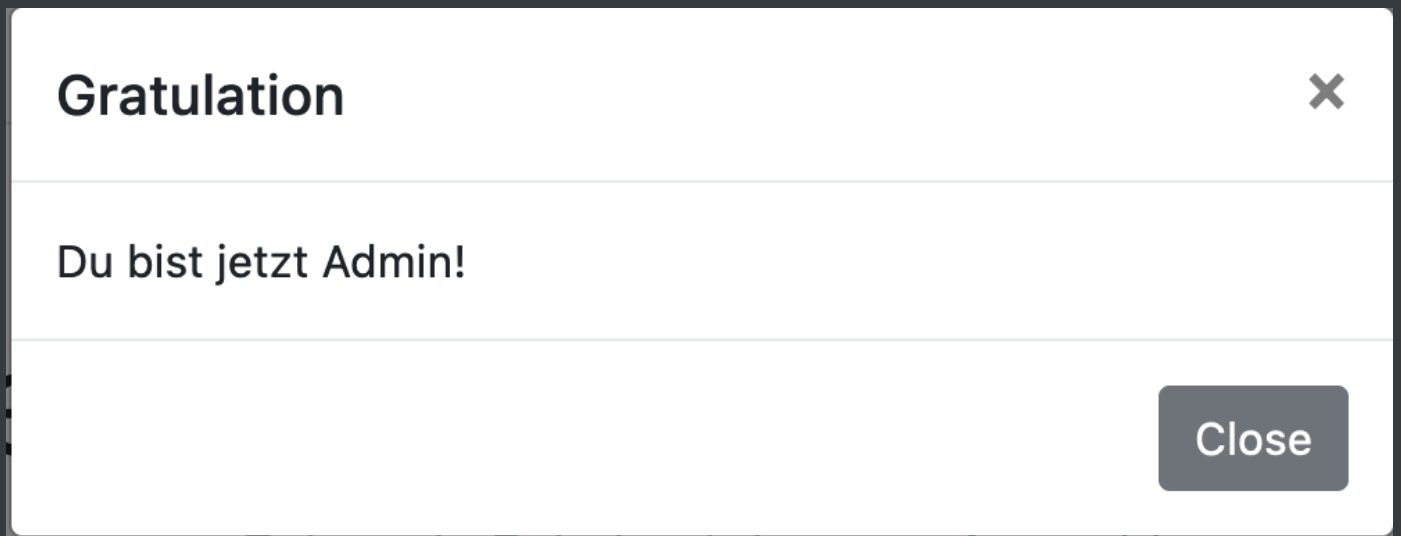
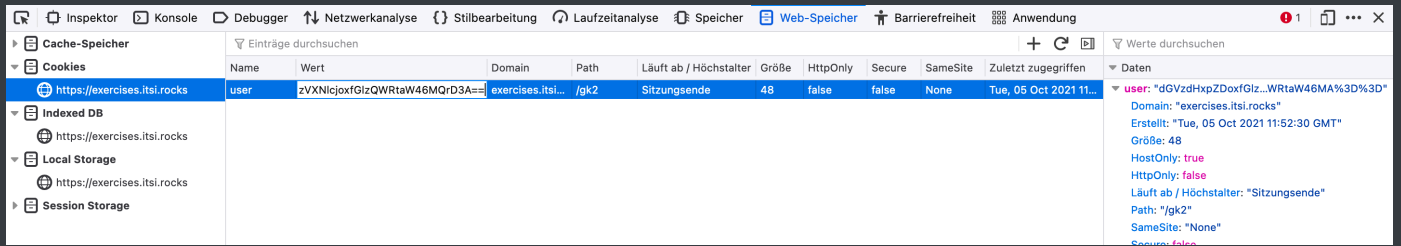
test | id:1 | isUser:1 | isAdmin:1 |
AU

Output

time: 2ms
length: 44
Lines: 1

GVzdHxpZDoxfGZVXNlcjoxfGZQWRtaW46MQrD3A==

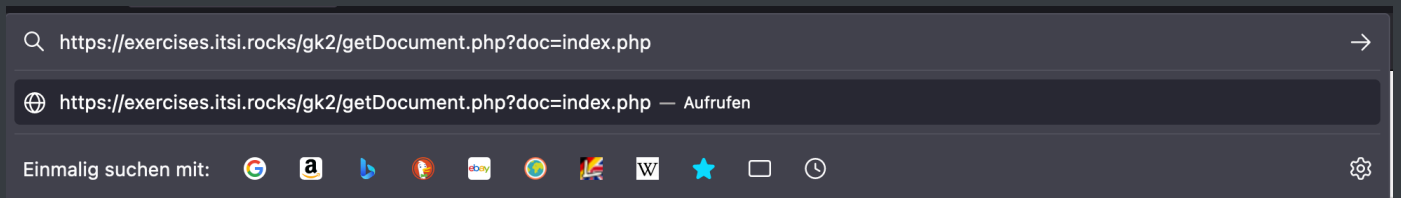
Den neu verschlüsselten Wert kopiert man und fügt man erneut bei den Cookies ein.



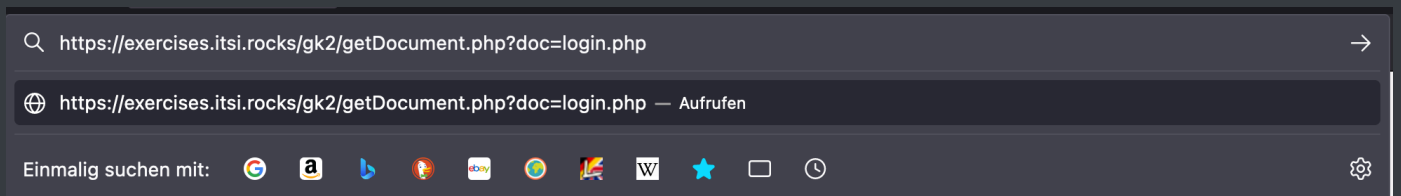
3) Ich habe mir den Quelltext der Seite angeschaut und mir ist aufgefallen das wenn man auf einen Downloadlink auf der Seite drückt die URL geändert wird



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.

```
10
11 class MyDB extends SQLite3
12 {
13     function __construct()
14     {
15         $this->open('database.sqlite', $flags = SQLITE3_OPEN_READONLY);
16     }
17 }
```

Dann habe ich auf dem gleichen Weg wie die php Dateien 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