

Informationssicherheit und IT-Forensik

– Übung –

UEB-02 – Websicherheit

- Wie war die Einheit in der Vorlesung?
- Viele neue Konzepte?
- Alles verstanden? Wie sieht es aus mit:
 - XSS?
 - SQLi?
 - ...

heise online **heise+**

IT **Mobiles** **Entertainment** **Wissen** **Netzpolitik** **Wirtsch**

TOPTHEMEN: **DSGVO** **WINDOWS 10** **ANDROID** **AMAZON** **KI** **ELEKTROAUTOS**

Security > 7-Tage-News > 02/2019 > **Netzwerkhelperlein von Cisco: Mittels Standard-Kennwort z**

Alert! **UPDATE** 14:26 Uhr | Security

Netzwerkhelperlein von Cisco: Mittels Standard-Kennwort zum Neustart

Cisco hat wichtige Sicherheitsupdates für verschiedene Produkte veröffentlicht. Keine Lücke gilt als kritisch.

Von Dennis Schirmmacher



heise online **heise+**

IT **Mobiles** **Entertainment** **Wissen** **Netzpolitik** **Wirtschaft**

TOPTHEMEN: **DSGVO** **WINDOWS 10** **ANDROID** **AMAZON** **KI** **ELEKTROAUTOS**

Security > 7-Tage-News > 02/2019 > **Kühlsysteme mit schwachem Standardpasswort übers Internet...**

17:35 Uhr | Security

Kühlsysteme mit schwachem Standardpasswort übers Internet manipulierbar

Um nicht eiskalt von Angreifern erwischt zu werden, sollten Betreiber von Kühlsystemen der Firma Resource Data Management umgehend das Standardpasswort ändern.

Von Olivia von Westernhagen




heise online **heise+**

IT **Mobiles** **Entertainment** **Wissen** **Netzpolitik** **Wirtschaft** **Jobs**

TOPTHEMEN: **FOSDEM** **EMOTET** **E-AUTO** **WINDOWS 10** **RASPI 4**

Security > 7-Tage-News > 01/2020 > **Jetzt handeln! Exploit-Code für kritische Citrix-Lücke gesichtet**

 **Alert!**

Jetzt handeln! Exploit-Code für kritische Citrix-Lücke gesichtet

Es könnten Angriffe auf Citrix Application Delivery Controller und Gateway bevorstehen. Bislang gibt es nur einen Workaround. Patches sollen folgen.


Datenleck an der Uni Erlangen Nürnberg:

Datenleck an der Uni Erlangen Nürnberg:



TRENDS & NEWS | NEWS

 **Hartmut Gieselmann**  01.02.2020

 **Datenleck, Datenschutz, DSGVO, Erlangen, Medizin, MHBA, Nürnberg, Universität**

Am Lehrstuhl für Gesundheitsmanagement wurden persönliche Daten von über 800 Studierenden auf einem Web-Server freigegeben - darunter Passwörter im Klartext.

IT Wissen Mobiles Security Developer Entertainment Netzpolitik

TOPTHEMEN: NASA BITCOIN AMAZON CORONAVIRUS WINDOWS 10 E-AUTO

heise online > News > 02/2021 > Jetzt updaten: Kritische Lücke aus VMware ESXi und vCenter Server...



Alert!

Jetzt updaten: Kritische Lücke aus VMware ESXi und vCenter Server beseitigt

Drei Lücken mit Einstufungen von "Moderate" bis "Critical" betreffen neben ESXi und vCenter Server indirekt auch Cloud Foundation. Es gibt aktive Angriffe.

Lesezeit: 1 Min.  In Pocket speichern



IT Wissen Mobiles Security Developer Entertainment Netzpolitik W

TOPTHEMEN: NASA BITCOIN AMAZON CORONAVIRUS WINDOWS 10 E-AUTO

heise online > News > 02/2021 > Hackerangriff auf Trinkwasser: Immer gleiches Passwort, Windows 7 und...

Hackerangriff auf Trinkwasser: Immer gleiches Passwort, Windows 7 und Teamviewer

Nach dem vereitelten Hackerangriff auf die Trinkwasserversorgung einer Stadt in Florida wird deutlich, wie schlecht die IT-Sicherheit vor Ort war.

Lesezeit: 2 Min.  In Pocket speichern

   305



IT Wissen Mobiles Security Developer Entertainment Netzpolitik Wirtschaft Journal

TOPTHEMEN: MWC UKRAINE-KRIEG WINDOWS 11 KRYPTOWÄHRUNGEN REPARATUR ALERT!



Alert!

Jetzt patchen! Kritische Sicherheitslecks in APC Smart

In den APC Smart-UPS von Schneider Electric könnten Angreifer Sicherheitslücken ausnutzen, um einzuschleusen oder die Geräte außer Funktion zu setzen.

Lesezeit: 2 Min. In Pocket speichern



IT Wissen Mobiles Security Developer Entertainment Netzpolitik Wirtschaft Journal

TOPTHEMEN: MWC UKRAINE-KRIEG WINDOWS 11 KRYPTOWÄHRUNGEN REPARATUR ALERT! ANZE



Alert!

NAS: Sicherheitslücke in Synology DSM erlaubt Ausführen von beliebigen Befehlen

Angreifer könnten beliebige Befehle auf Synology-NAS-Geräten ausführen. Der Hersteller arbeitet an einer Patches. Erste stehen bereit.

Lesezeit: 1 Min. In Pocket speichern



heise online > Security > Jetzt patchen! Zehntausende Qnap-NAS hängen verwundbar am Internet

Jetzt patchen! Zehntausende Qnap-NAS hängen verwundbar am Internet

Angreifer könnten direkt über das Internet an einer kritischen Sicherheitslücke in Netzwerkspeichern von Qnap ansetzen.

Lesezeit: 2 Min.  In Pocket speichern

   22



(Bild: Photon photo/Shutterstock.com)

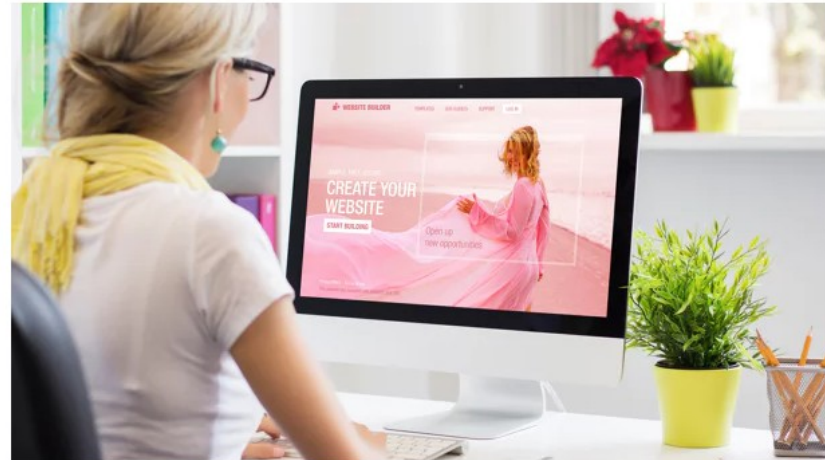
01.02.2023 11:49 Uhr | Security

CMS Typo3: Hochriskante XSS-Lücke ermöglicht Unterschieben von schädlichem HTML

Im Content-Management-System Typo3 könnten Angreifer eine Cross-Site-Scripting-Lücke ausnutzen, um schädlichen HTML-Code einzuschleusen. Updates stehen bereit.

Lesezeit: 2 Min.  In Pocket speichern

   6



(Bild: Shutterstock/Kaspars Grinvalds)

09.02.2023 14:34 Uhr | Security

heise online > Security > Sicherheitslücke in Webmailer Roundcube wird angegriffen



Alert!

Sicherheitslücke in Webmailer Roundcube wird angegriffen

Angreifer attackieren eine Sicherheitslücke in dem Webmail-Programm Roundcube. Ein Update steht bereits länger bereit.

Lesezeit: 2 Min. In Pocket speichern



(Bild: Pavel Ignatov/Shutterstock.com)

14.02.2024 09:32 Uhr | Security

Von Dirk Knop



Alert!

Webkonferenz-Tool Zoom: Rechteausweitung durch kritische Schwachstelle

Zoom warnt vor mehreren Schwachstellen in den Produkten des Unternehmens. Eine gilt als kritisches Sicherheitsrisiko.

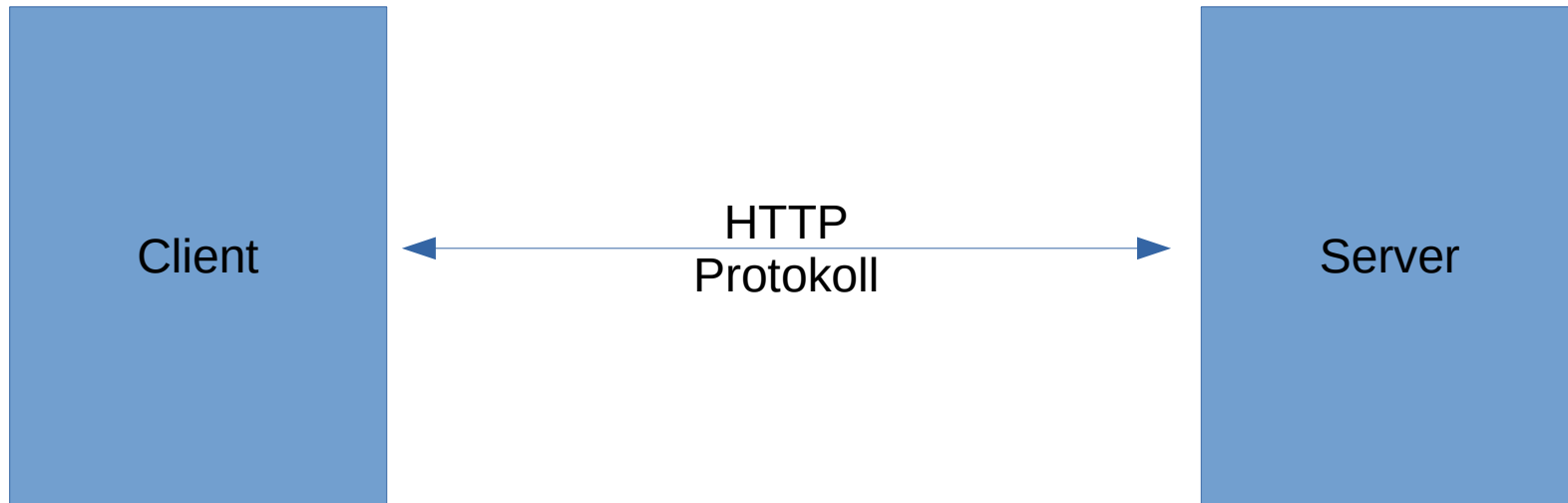
Lesezeit: 2 Min. In Pocket speichern



(Bild: Shutterstock/Andrey_Popov)

14.02.2024 11:55 Uhr | Security

Von Dirk Knop



- Server lauscht auf einem festen Port
 - 80 für HTTP
 - 443 für HTTPS
- Client kann, wann immer er es möchte, versuchen, diesen Port zu kontaktieren
- Dabei spricht er das HTTP-Protokoll (mit vorherigem Schlüsselaustausch bei HTTPS)

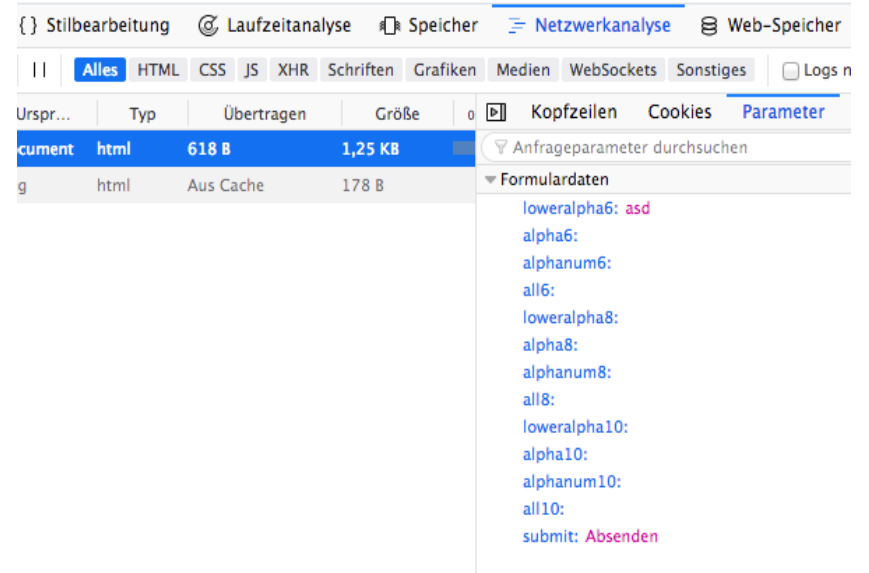
- Verschiedene Arten von Anfragen
 - GET
 - POST
 - HEAD, PUT, DELETE, OPTIONS, ...
- Wichtig sind vor allem die ersten beiden Typen
 - GET – „bitte gib mir Daten“
 - POST – „hier sind Daten für dich“
(vereinfacht dargestellt)

- Rufen Sie „per Hand“ eine Webseite ab
- Finden Sie eine beliebige Seite mit unverschlüsseltem HTTP (gar nicht mehr so leicht heutzutage)
 - z.B: <http://ard.de> (2019) <http://uni-koeln.de> (2020) <http://gnu.org> (2021)
 - <https://whynohttps.com> hilft
 - <http://neverssl.com>
- In der Kali-Kommandozeile:
 - Eine Verbindung mit Port 80 herstellen: `nc neverssl.com 80 -Cv`
 - HTTP sprechen:
 - „GET /“ eintippen, nachdem die Verbindung hergestellt wurde

- <https://www.portal.uni-koeln.de/searchresult.html?q=Testsuche>
- <https://> – Protokoll
- www.portal.uni-koeln.de – Host (Domain/Webseite)
- [/searchresult.html](https://www.portal.uni-koeln.de/searchresult.html) – Pfad
- [?q=Testsuche](https://www.portal.uni-koeln.de/searchresult.html?q=Testsuche) – Parameter

- POST `http://example.com/login.php`
 - Keine Logindaten als Parameter an die URL angehängt
 - Trotzdem werden irgendwo die Daten übertragen, denn ein Login ist erfolgreich
- Lösung: `user=admin&password=123456` wird als Datenteil in der Anfrage übertragen, für den Anwender „unsichtbar“

- Öffnen Sie im Webbrowser die Entwicklertools (F12)
- Klicken Sie auf Netzwerkanalyse / Network
- Senden Sie im Webbrowser ein Formular ab
 - z.B. im VPN unter <http://matrix.seiberkreim.com>
- Untersuchen Sie die gesendeten Daten



Die Grundausstattung einer Webseite

- **HTML**
 - Textauszeichnungssprache (vergleichbar zu z.B. LaTeX, Markdown)
 - `<h1>Text</h1>` – der Text stellt eine Überschrift dar
 - `<p>Text</p>` – der Text ist ein einzelner Absatz
 - `<a>Text` – der Text ist eine Verlinkung (ein „Anker“)

Die Grundausstattung einer Webseite

- **CSS**
 - Regelt die optische Gestaltung von Webseiten
 - z.B.: Eine Überschrift soll in Schriftgröße 22 und fett dargestellt werden
 - Hier lauern schon die ersten Probleme, da CSS eine sehr mächtige Designsprache ist, es gibt fortgeschrittene Webangriffe auf CSS-Basis

Die Grundausstattung einer Webseite

■ **JavaScript**

- Statische HTML+CSS-Webseiten sind nicht modern und interaktiv genug
- clientseitig Code ausführen: Die Webanwendung von einer Textseite zu einem interaktiven Programm machen
- „wenn der Nutzer mit der Maus über diesen Knopf fährt, färbe ihn grau ein“
- „wenn der Nutzer eine monoalphabetische Substitution durchführen will, schicke seinen Text nicht an den Server, sondern verschlüssele das direkt im Webbrowser
- „I built a role playing game in JavaScript. You can, too. Here's how.“
<https://www.freecodecamp.org/news/learning-javascript-by-making-a-game-4aca51ad9030/>

- Möchte man nicht nur statische Webseiten ausliefern, sondern interaktiv auf die Eingaben des Anwenders reagieren, benötigt man auf der Seite des Webserver Programmcode, der beim Aufruf der Webseite ausgeführt wird
- Klassischerweise benutzt man dafür PHP, aber auch C-Programme, Java-Applets, Python-Skripte, nodeJS, Ruby, ... können über das Web erreichbar gemacht werden
- Übertragene Parameter landen automatisch in den Variablen `$_GET` und `$_POST` und können wie normale Variablen verarbeitet werden

```
print("Guten Tag, Ihr Name ist $_GET['name']");
```

- Laden Sie den Code der Seite <http://matrix.seiberkreim.com/dummyformular/> herunter
 - erfordert VPN-Verbindung
- Lesen Sie den Code und vollziehen Sie nach, wie mit den übergebenen Variablen gearbeitet wird

Hinweis: Dieser Code ist weder schön noch sicher!

XSS

- Nutzt man alle Techniken zusammen, kann man Probleme erzeugen
 - Ein Client (Browser), der Javascript fröhlich ausführt
 - Ein Webserver, der Eingaben ungefiltert entgegen nimmt und diese in seine Antwort einbaut

Server: `print("Sie haben nach $_GET['q'] gesucht");`

Angreifer: `http://example.de/search.php?q=<script>alert(1)</script>`

Warum ist es gefährlich, wenn ein Angreifer es schafft, JavaScript auszuführen?

- Verändern der Webseite („Defacement“)
- Zugriff auf Cookies (übernehmen von Login-Sessions)
- Auslesen von auf der Webseite dargestellten Informationen (Kontonummer? HIV-Status?)

Wir unterscheiden grob zwischen zwei Varianten (es gibt weitere, fortgeschrittenere Techniken)

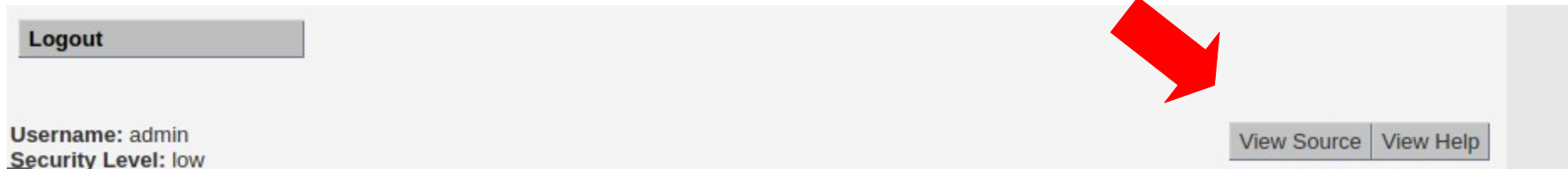
- Reflektives XSS
 - Angreifer kann einen URL-Parameter kontrollieren und darüber JavaScript ausführen
- Stored XSS
 - Angreifer kann persistent Daten auf einer Webseite hinterlegen, die anschließend von anderen Benutzern angesehen werden (etwa ein Gästebucheintrag mit Schadcode)

- Rufen Sie <http://matrix.seiberkreim.com> in Kali auf und loggen Sie sich in DVWA ein
 - Stellen Sie sicher, dass die Sicherheitsstufe im Menüpunkt „DVWA Security“ auf „Low“ steht
- Bringen Sie sowohl *reflected* als auch *stored* ein JavaScript zur Ausführung
- Gängiges JavaScript zum Testen:
 - `<script>alert(1)</script>`, zeigt eine Pop-Up-Meldung

Was kann man dagegen tun?

- JavaScript abschalten
 - keine echte Lösung, schränkt Funktionalität stark ein
- Plugins installieren (z.B. NoScript)
 - Besser, aber keine echte Lösung
 - Hat nicht jeder, hilft nur begrenzt gut
- Also muss der Webseitenbetreiber seine Anwendung absichern

- Wir schauen uns drei Ansätze an, um Webseiten serverseitig abzusichern
- dazu einen eigenen Webserver mit PHP in Kali starten:
 - `sudo systemctl start apache2`
 - Quellcode unter `/var/www/html/xss.php` ablegen
 - Ist im Webbrowser dann über „`localhost/xss.php`“ erreichbar
 - Siehe auch „`how_to_webserver.txt`“ in `aufgaben/01_websicherheit`
- Quellcode der Reflected-XSS-Anwendung gibt es in DVWA:



Ansatz 1: Blacklisting / Denylisting / Blocklisting

- ```
If strpos($input, '<script>') !== false) {
 die("XSS detected!");
}
```
- Prüft die Eingabe gegen eine „schwarze Liste“ von verbotenen Parametern
- Bitte selbst implementieren (vorher Kopie des Quellcodes anlegen) und alle Einfallstore absichern
- Ist das sicher? Was denken Sie?

## Ansatz 1: Blocklisting

- `<img src=x onerror=alert(1)>`
- Es gibt verschiedene Wege, JavaScript auszuführen
- Natürlich kann man auch `<img>` noch herausfiltern, aber Kernproblem:
  - Mit Blocklisting definieren wir, welche bösen Eingaben wir kennen. Kennt der Angreifer auch nur eine Eingabe mehr als wir, hat er gewonnen.

## Ansatz 2: Bereinigung

- `$name=strip_tags($_REQUEST['name']);`  
„strip\_tags — Strip HTML and PHP tags from a string“  
- <https://php.net>
- Es gibt verschiedene Funktionen in PHP, die derartige Aufgaben übernehmen
- Bitte selbst implementieren (weitere Kopie) und alle Einfallstore absichern
- Ist das sicher? Was denken Sie?

## Ansatz 2: Bereinigung

Ist das sicher?

- Hängt von der Funktion und vom Einsatz ab!
- In unserem Beispielfall: Möglicherweise

Unsicheres Beispiel:

- [www.example.de/showimage.php?img=4711.jpg](http://www.example.de/showimage.php?img=4711.jpg)

```
[...]

[...]
```

- Angreifbar, etwa mit `showimage.php?img=x%20onerror="alert(1)"`
- Kernproblem: Derartige Funktionen sind auch „nur“ Blocklisting auf hohem Niveau. Es gibt einige gute Funktionen dieser Art, aber es besteht stets die Gefahr, dass sich eine neue Möglichkeit auftut, sie zu umgehen.



## Ansatz 3: Whitelisting / Allowlisting

- ```
if(preg_match('/[^\a-z_\-0-9]/i', $string))  
{  
    die("Invalid string");  
}
```
- Wir drehen die Blocklist um. Alles was unser „weißen Liste“ entspricht, darf bleiben
- In diese Fall: Groß- und Kleinbuchstaben, Zahlen, Unterstrich, Bindestrich
- Bitte selbst implementieren (weitere Kopie) und alle Einfallstore absichern
- Ist das sicher? Was denken Sie?

Ansatz 3: Allowlisting

- Hängt davon ab, wie die Allowlist definiert wird
- Lässt man nur simple ASCII-Zeichen zu, hat man es sehr leicht
- In manchen Kontexten muss man aber mehr Eingaben erlauben (etwa ein CMS-System, in dem Nutzer ihre Beiträge mit HTML anreichern dürfen)
- JavaScript braucht nicht viele Zeichen: <http://www.jsfuck.com/>

- sichere Programmierung ist sehr schwer, man kann an vielen Stellen vieles falsch machen
- Frameworks können dabei helfen, Probleme zu lösen
- Für PHP gibt es z.B. Symfony
 - Hilft mit „Validation Constraints“, Eingaben zu überprüfen (etwa: ist die Eingabe eine gültige E-Mailadresse?)
 - <https://symfony.com/doc/current/reference/constraints.html>
- verschiedene moderne Webtechniken können dabei helfen, XSS zu erschweren
 - X-XSS-Protection-Header
 - Content-Security-Policy-Header
 - ...

- die Welt des modernen Webs entwickelt sich stets weiter
- Neue Verteidigungstechniken, aber auch Angriffsmöglichkeiten entstehen
- Der beste Schutz vor XSS verhindert nicht, dass der Programmierer Fehler in der Businesslogik macht:
 - Wenn der Preis eines Produkts im Warenkorb clientseitig per JavaScript gespeichert und beim Absenden nicht vom Server überprüft wird, kann man einen BMW auch für 1€ kaufen.

SQLi

- Annahme: Webserver soll Daten persistent speichern können
- Dazu benötigt er eine Datenbank, aus der PHP Daten holen und dort auch wieder ablegen kann
- Klassischerweise benutzt man dafür MySQL, aber auch PostgreSQL, SQLite, ...
- Sprache, um mit einer Datenbank zu sprechen: SQL

Datenbanktabelle
„users“

username	password
admin	123456
martin	winfoinfo123

- `SELECT * FROM users WHERE username="admin" and password="123456";`
- In PHP z.B. mit der Funktion `mysqli_query()` an die Datenbank schicken
- Es gibt nicht nur `SELECT`, sondern auch `UPDATE`, `INSERT INTO`, `DROP`, `GRANT`,

- Wir kombinieren wieder das Problem von ungefiltertem Input und unsauberer Programmierung

Server:

```
mysqli_query(SELECT * FROM users WHERE username=$_POST["user"]  
and password=$_POST["password"]);
```

Angreifer: username=admin, password=foobar"%20R%20"1"="1

Was passiert?

```
SELECT * FROM users WHERE username="$_POST['user']" and  
password="$_POST['password']");
```

legitimer Nutzer: username=martin, password=winfoinfo123

```
SELECT * FROM users WHERE username="martin" and  
password="winfoinfo123");
```

Angreifer: username=admin, password=foobar"%20OR%20"1"="1

```
SELECT * FROM users WHERE username="admin" and  
password="foobar" OR "1"="1");
```

UNION SELECT

- Verbindung von zwei verschiedenen Tabellen
- `SELECT name FROM students UNION SELECT name FROM professors;`
- Liefert mir alle Namen von Studenten und Professoren
- Problem? Verbindung von zwei verschiedenen Tabellen!

Warum ist es gefährlich, wenn ein Angreifer es schafft, eine SQL Injection auszuführen?

- Umgehen von Logins
 - password=1“ OR “1“=“1
- Auslesen von Passwörtern/Zugangsdaten
 - SELECT artikel UNION SELECT password FROM users;

Warum ist es gefährlich, wenn ein Angreifer es schafft, eine SQL Injection auszuführen?

- Anlegen neuer oder Manipulation bestehender Logins
 - UPDATE users SET password="hacked" WHERE username="hacker" AND username="admin";
- Angriffe auf das Betriebssystem des Datenbankservers
 - SQL erlaubt ggf. das Lesen von lokalen Dateien, Ausleiten von Informationen über HTTP, Ausführen von Kommandozeilenbefehlen
- ...

- Rufen Sie erneut <http://matrix.seiberkreim.com/dvwa> auf
- Sehen Sie sich die „SQL-Injection“-Aufgabe an und listen Sie mindestens alle fünf Benutzer mit einer SQL-Abfrage auf.
 - Optional: Exfiltrieren Sie die Passwörter der Benutzer aus der Datenbank
- Wenn gelöst: Sichern Sie die Lücke (theoretisch) ab!
 - Wer mag kann die Anwendung dazu lokal bei sich in Betrieb nehmen, das Aufsetzen einer eigenen Datenbank sprengt aber den Rahmen der Übung.

Lösung:

- Auflisten aller User: `' OR '1' = '1`
- Ausgeben der Passwörter:
 - Namen aller Spalten identifizieren:
`' UNION SELECT 0,column_name FROM information_schema.columns
where table_name='users';-- -`
- Ausgeben von Nutzernamen und Passwörtern:
`' UNION SELECT 0, concat(user_id, ",", "user, ",", password)
from users;-- -`

- Welchen Weg haben Sie zum Absichern gewählt?
- Der Königsweg: **Prepared Statements**
- Der SQL-Query wird mit Platzhaltern vorpräpariert und dann bei Bedarf ausgefüllt
- ```
$s=$conn->prepare("SELECT * FROM users WHERE username=? AND password=?");
$s->bind_param("ss", $user, $pass); //zwei Variablen vom Typ s(string)
$s->execute();
```

- SQL Injections können sehr gefährlich werden
- Prepared Statements helfen, das Problem zu lösen
- Frameworks helfen auch:
  - Abstraktionsschichten wie ORM (Object Relational Mapping)
- Aber auch hier: Gegen die Fehler in der Businesslogik helfen keine Prepared Statements