Fachhochschule Nordwestschweiz
Hochschule für Technik

Cyber Security Labor (cysL)

Inhalt

Inhalt

Vorbereitung

Recherche

Nehmen sie sich einmal das folgende Skript vor:

```
1  // setup sql connection
2  require_once("mysqlsetup.inc");
3
4  // verify credentials
5  $query="select * from usertable WHERE user='".$_REQUEST['username']."' and password='".md5sum($_REQUEST['password'])."';";
6  $rows=$sql->query($query);
7  if($rows->size()!=1) {
8          echo "Login failed for user "+$_REQUEST['username']+" ... is your password or username correct?";
9          die();
10 }
11 // user has provided valid credentials
12 echo "Hello ".$row->get("truename")." nice to see you again";
```

Was ist hier schlecht?

Zum lesen oder anschauen ...

Directory Traversal Attacken
Eine Kurzeinführung in Cross-Side-Scripting

Begriffe

Cross-Side-Scripting (XSS), SQL-Injection, Path/Directory-Traversal-Attacken.

Spass mit Sicherheit

Die Gefahren von Twitter-Bots (?)

Twitter-Bot

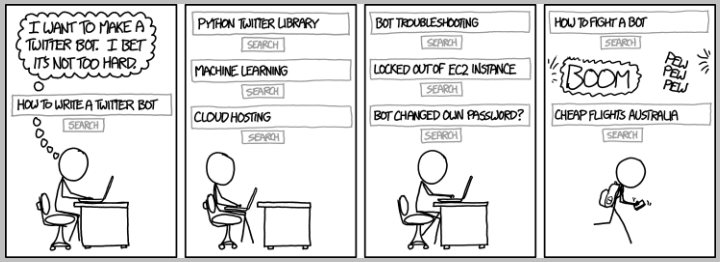

Abbildung: Programmieren mit Google

Quelle: XKCD

Web-Basierte Angriffe

Cross-Side-Scripting

Webbasierte Angriffe

- Persistent
  Dies erfolgt typischerweise in einem Blog, einer Kommentarfunktion oder einem Gästebuch. Es gibt aber auch andere Formen. Beispielsweise über den Upload von Files, Verlinkung von ungeprüften Quellen oder via Datenbank-Einträgen
- Non-Persistent
  Die einfachste Attacke. Sie erfolgt üblicherweise über einen untergeschobenen Link (meistens im Zusammenhang mit einem Phishing- oder Whaling-Mail).
- DOM-Based
  Hier wird der untergeschobene Link aus der DOM des Browsers geladen.

Web-Basierte Angriffe

Directory/Path-Traversal-Attack

Das Prinzip

Lokale Files werden ausserhalb des Server-Roots geladen und übermittelt. Dies erfolgt über…

- Backreferencing
  Normalerweise über verwendung des “..”-Hardlinks
- Logische Links
  Diese können auch Files (oder Verzeichnisse) ausserhalb des Roots referenzieren.

Häufig wird diese Attacke mit Obfuscation eingesetzt.

Ein paar Beispiele

http://www.foo.bar/index.php?getFile=../../../../etc/passwd
http://www.foo.bar/index.php?getFile=..%2F..%2F..%2F..%2Fetc%2Fpasswd
http://www.foo.bar/%69%6E%64%65%78%2E%70%68%70%3F%67%65%74%46%69%6C%65%3D%2E%2E%2F%2E%2E%2F%2E%2E%2F%2E%2E%2F%65%74%63%2F%70%61%73%73%77%64

Repetition und Aufgabe

Aufgabe

Heute versuchen wir uns im realen Internet zu bewegen. Versuchen sie doch einemal Seiten mit Webformularen zu finden, die für XSS-Attacken anfällig sind. Suchen sie primär einfache, kleine Webseiten. Es ist unwahrscheinlich, dass sie eine XSS-Attacke in einem etablierten CMS finden. Versuchen sie doch einmal, ob sie die Codezeile
“<script>alert(’vulnerable’);</script>” in eine Seite einfügen können.
Falls Sie etwas entdecken (damit rechne ich) überlegen sie sich doch, was sie jetzt machen. Sie müssen diese Schwachstelle verantwortungsvoll bewirtschaften. “Responsible Disclosure” ist der richtige Term dafür.

Repetition und Aufgabe

Nächster Block

Nächster Termin

Einreichen Übung 1 vor Beginn der Lektion 8 am 04.11.2025 (in 82204 Tagen)