Authentication Based Attacks

Tools in Kali Linux

Module #31

Cross Site Scripting (XSS)

Cross-site scripting (XSS) is a vulnerability found on web applications. XSS allows attackers to inject scripts into the website. These can be used to manipulate web server, or clients connecting to the webserver.

Cross-site scripting has accounted for a large majority of popular web-based attacks.

Cross-site scripting attacks have resulted in attackers defacing websites, distributing malware to clients, and stealing sensitive info from websites, such as credit card and other personal identifiable information.

Cross Site Scripting (XSS)

By leveraging XSS, an attacker does not target a victim directly. Instead, an attacker would exploit a vulnerability within a website or web application that the victim would visit, essentially using the vulnerable website as a vehicle to deliver a malicious script to the victim's browser.

While XSS can be taken advantage of within VBScript, ActiveX and Flash (although now considered legacy or even obsolete), unquestionably, the most widely abused is JavaScript – primarily because JavaScript is fundamental to most browsing experiences.

Working of a Cross Site Scripting (XSS)

In order to run malicious JavaScript code in a victim's browser, an attacker must first find a way to inject a payload into a web page that the victim visits.

an attacker could use social engineering techniques to convince a user to visit a vulnerable page with an injected JavaScript payload.

In order for an XSS attack to take place the vulnerable website needs to directly include user input in its pages.

An attacker can then insert a string that will be used within the web page and treated as code by the victim's browser.

Working of a Cross Site Scripting (XSS)

The following server-side pseudo-code is used to display the most recent comment on a web page.

```
print "<html>"
print "<h1>Most recent comment</h1>"
print database.latestComment
print "</html>"
```

The above page is vulnerable to XSS because an attacker could submit a comment that contains a malicious payload such as <script>doSomethingEvil();</script>.

Working of a Cross Site Scripting (XSS)

Users visiting the web page will get served the following HTML page.

```
<html>
<h1>Most recent comment:</h1>
<script>doSomethingEvil();</script>
</html>
```

When the page loads in the victim's browser, the attacker's malicious script will execute, most often without the user realizing or being able to prevent such an attack.

Dangers of a Cross Site Scripting (XSS)

JS has access to all the same objects the rest of the web page has, including access to cookies. Cookies are often used to store session tokens, if an attacker can obtain a user's session cookie, they can impersonate that user.

JS can use XMLHttpRequest to send HTTP requests with arbitrary content to arbitrary destinations.

JS in modern browsers can leverage HTML5 APIs such as accessing a user's geolocation, webcam, microphone and even the specific files from the user's file system. While most of these APIs require user opt-in, XSS in conjunction with some clever social engineering can bring an attacker a long way.

Miscellaneous tools

urlsnarf is a tool that outputs all requested URLs sniffed from HTTP traffic in Common Log Format (CLF, used by almost all web servers), suitable for offline post processing with your favorite web log analysis tool (analog, wwwstat, and so on).

To access urlsnarf, navigate to Sniffing/Spoofing | Network Sniffers and select urlsnarf.

To use urlsnarf, type urlsnarf –i and the interface you want to monitor. Urlsnarf will display it's listening.

```
Usage: urlsnarf [-n] [-i interface | -p pcapfile] [[-v] pattern [expression]]
root@kali:~# urlsnarf -i eth0
urlsnarf: listening on eth0 [tcp port 80 or port 8080 or port 3128]
```

Miscellaneous tools

Miscellaneous tools

acccheck is a password dictionary attack tool that targets windows authentication using the SMB protocol. acccheck is a wrapper script around the smbclient binary, and as a result, is dependent on it for its execution.

hexinject is a versatile packet injector and sniffer that provides a command-line framework for raw network access. hexinject is designed to work together with other command-line utilities, and for this reason it facilitates the creation of powerful shell scripts capable of reading, intercepting and modifying network traffic in a transparent manner. hexinject can inject anything into the network, as well as calculate the checksum and packet size fields of TCP/IP protocols.

Thank You