HTML injection – POC

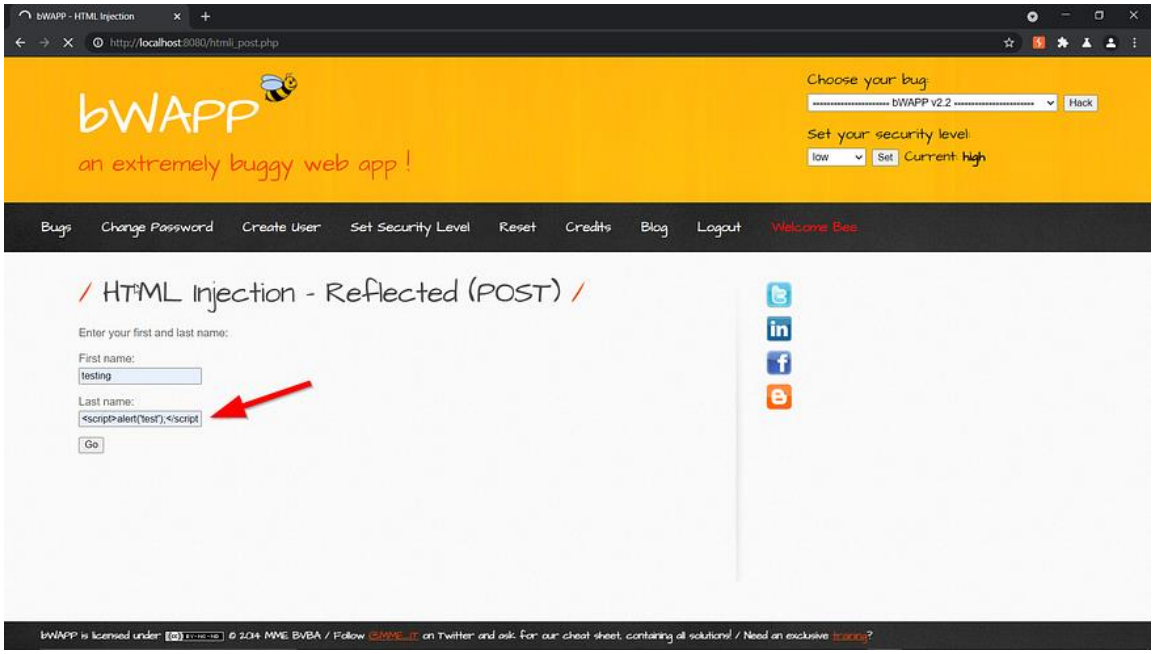
Description:

HTML injection is a type of injection vulnerability that occurs when a user is able to control an input point and is able to inject arbitrary HTML code into a vulnerable web page. This vulnerability can have many consequences, like disclosure of a user's session cookies that could be used to impersonate the victim, or, more generally, it can allow the attacker to modify the page content seen by the victims. Reflected GET attack scenario in which the input is sent in the URL, not the body.

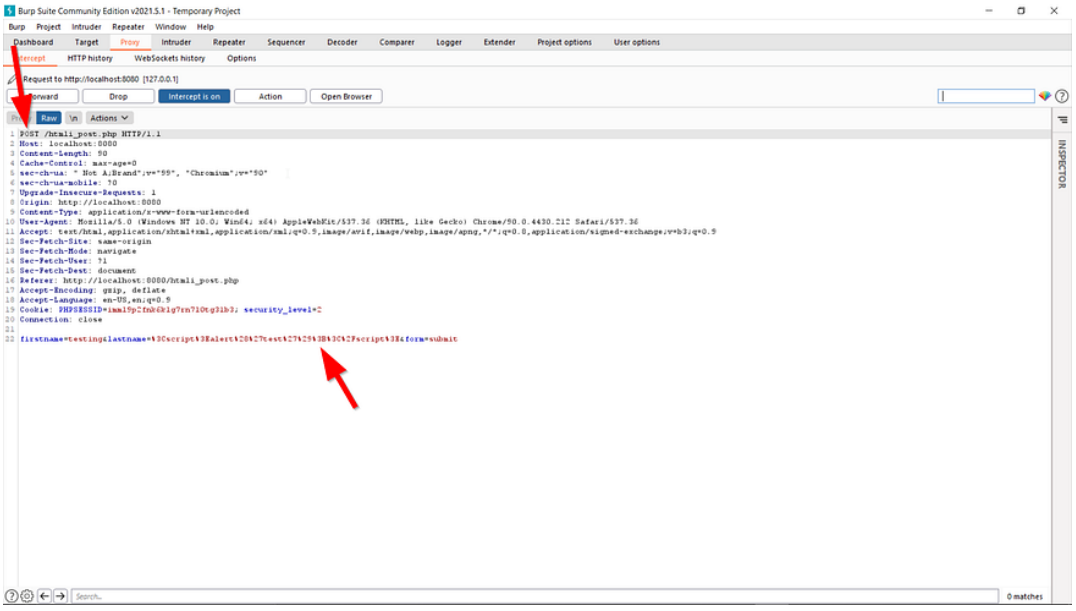
Reflected POST HTML Injection: is a little bit more difficult. It occurs when a malicious HTML code is being sent instead of correct POST method parameters.

Demo:

Security level : low

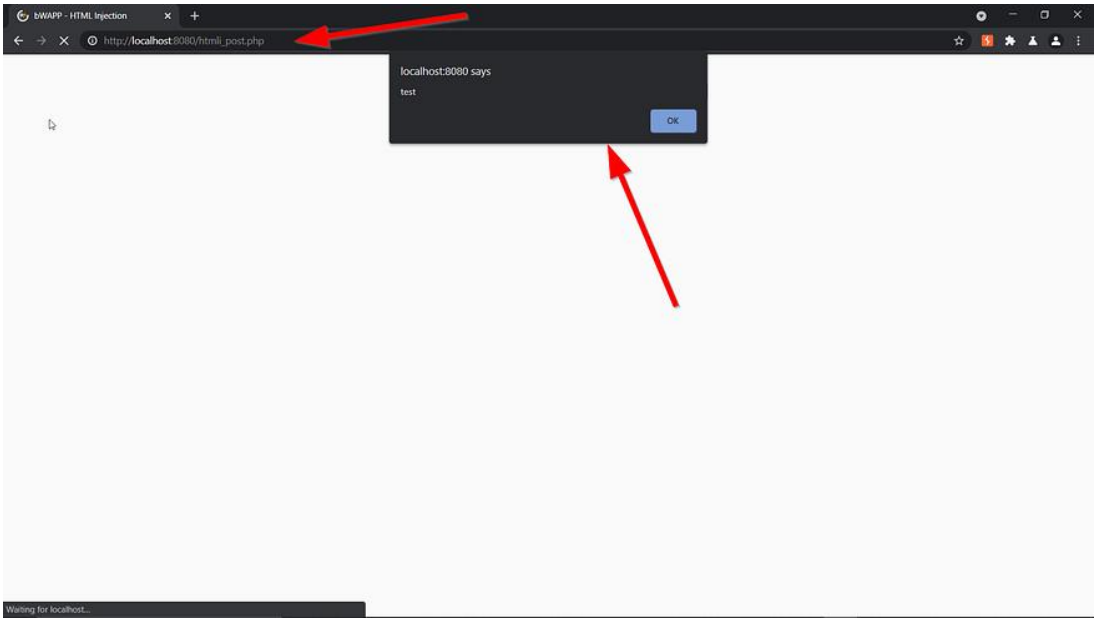


This works almost same as reflected get html injection but the only difference is that the injected code is sent through body of the request (POST method).



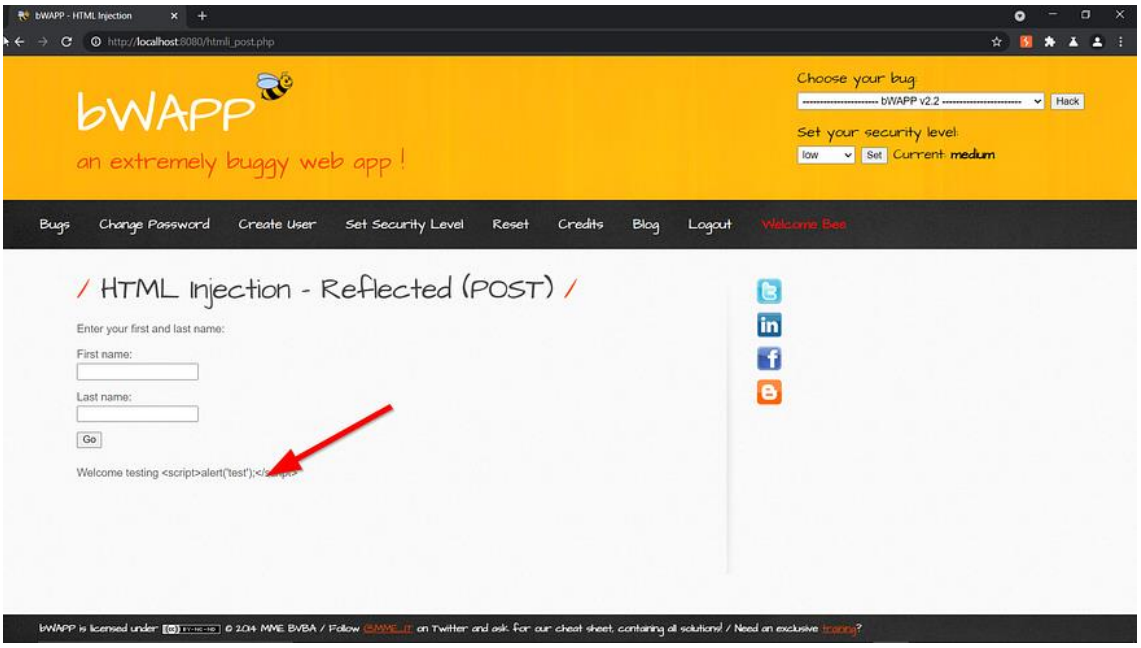
In the above example we can see that the <script>alert(‘test’);</script> is encoded and send via body of the request.

Press enter or click to view image in full size



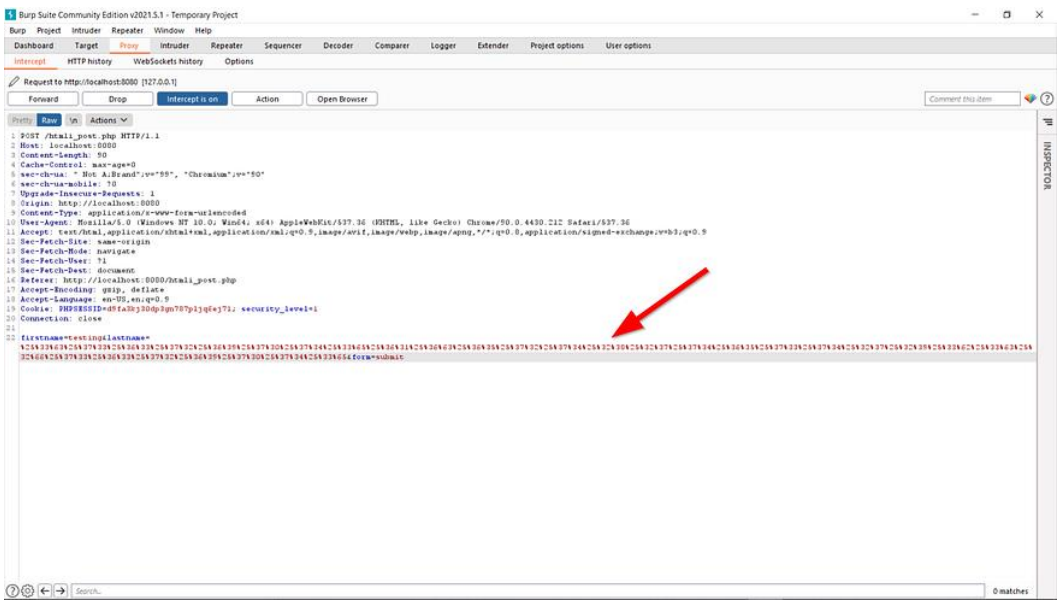
Then the arbitrary code is processed and executed. Also we can see that there is no parameter shown in the URL because it uses POST method.

Security level : medium



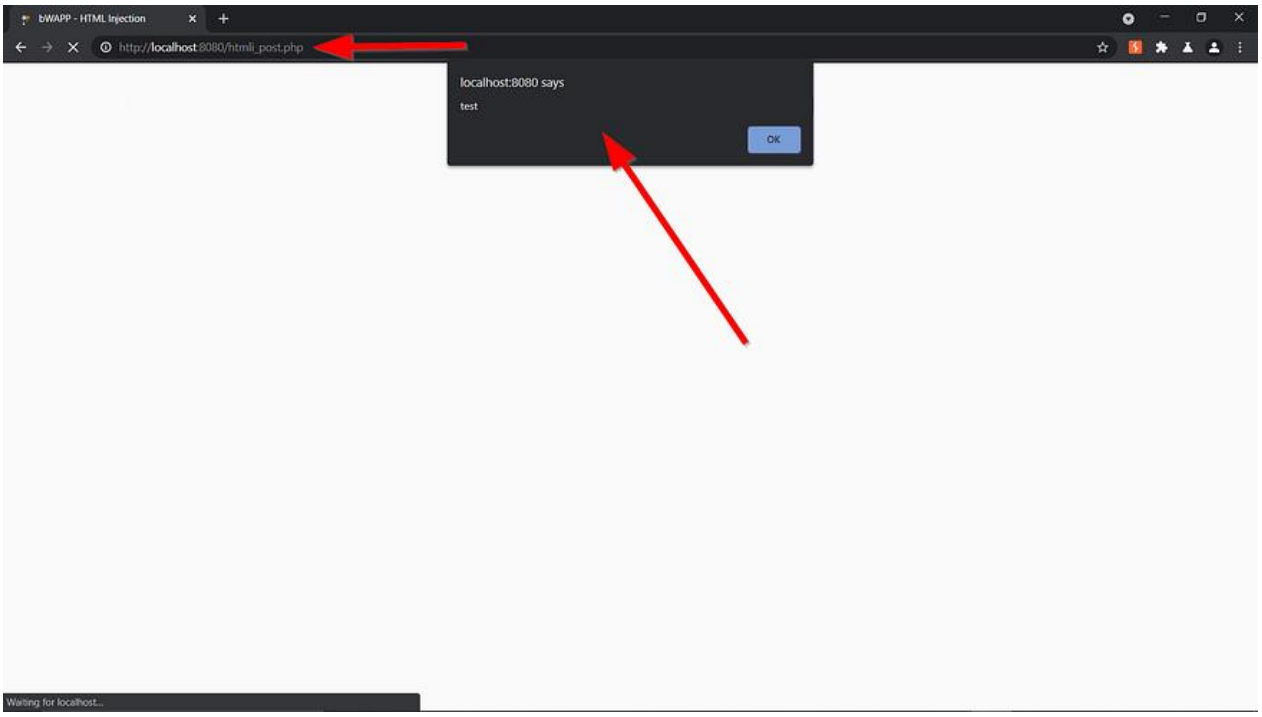
In the medium settings the application just returns the arbitrary code that we send.

Press enter or click to view image in full size



So we encode the <script>alert(‘test’);</script> which is %25%33%63%25%37%33%25%36%33%25%37%32%25%36%39%25%37%30%25%37%34%25%33%65%25%36%31%25%36%63%25%36%35%25%37%32%25%37%34%25%32%38%25%32%37%25%37%34%25%36%35%25%37%33%25%37%34%25%33%32%25%32%37%25%32%39%25%33%62%25%33%63%25%32%66%25%37%33%25%36%33%25%37%32%25%36%39%25%37%30%25%37%34%25%33%65 and pass it through the lastname parameter in the body of our request.

Press enter or click to view image in full size



Which bypasses the filter and executes the payload.