Cross-Site Scripting (XSS)

Cross-Site Scripting (XSS) vulnerabilities affect web applications and APIs alike. An XSS vulnerability may allow an attacker to execute arbitrary JavaScript code within the target's browser and result in complete web application compromise if chained together with other vulnerabilities. Our Cross-Site Scripting (XSS) module covers XSS in detail.

Proceed to the end of this section and click on `Click here to spawn the target system!` or the `Reset Target` icon. Use the provided Pwnbox or a local VM with the supplied VPN key to reach the target API and follow along.

Suppose we are having a better look at the API of the previous section, `http://<TARGET IP>:3000/api/download`.

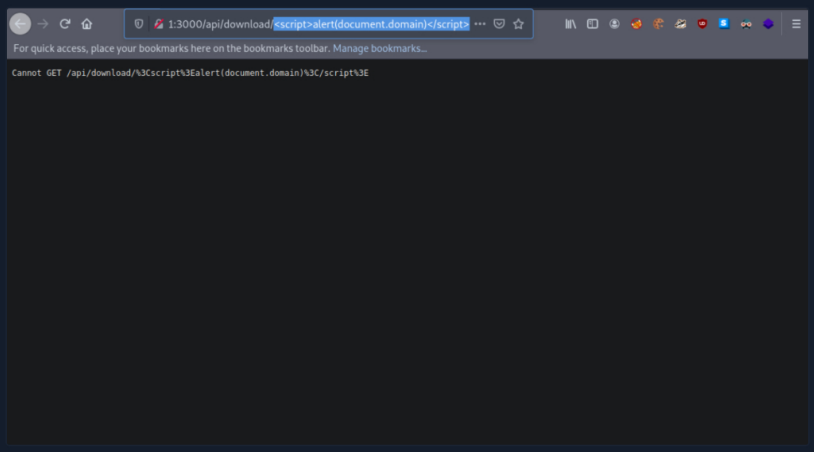
Let us first interact with it through the browser by requesting the below.

`test_value` is reflected in the response.

Let us see what happens when we enter a payload such as the below (instead of *test_value*).

Code: javascript

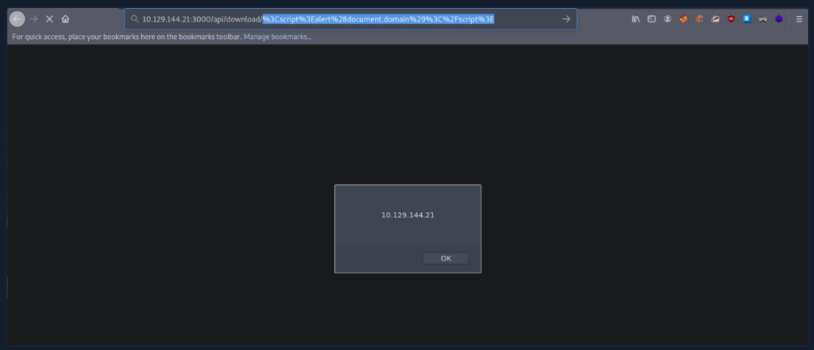
```
<script>alert(document.domain)</script>
```



It looks like the application is encoding the submitted payload. We can try URL-encoding our payload once and submitting it again, as follows.

Code: javascript

```
%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E
```



Now our submitted JavaScript payload is evaluated successfully. The API endpoint is vulnerable to XSS!

? Go to Questions

Table of Contents

Web Service & API Fundamentals

- Introduction to Web Services and APIs
- Web Services Description Language (WSDL)

Web Service Attacks

- SOAPAction Spoofing
- Command Injection
- Attacking WordPress' 'xmlrpc.php'

API Attacks

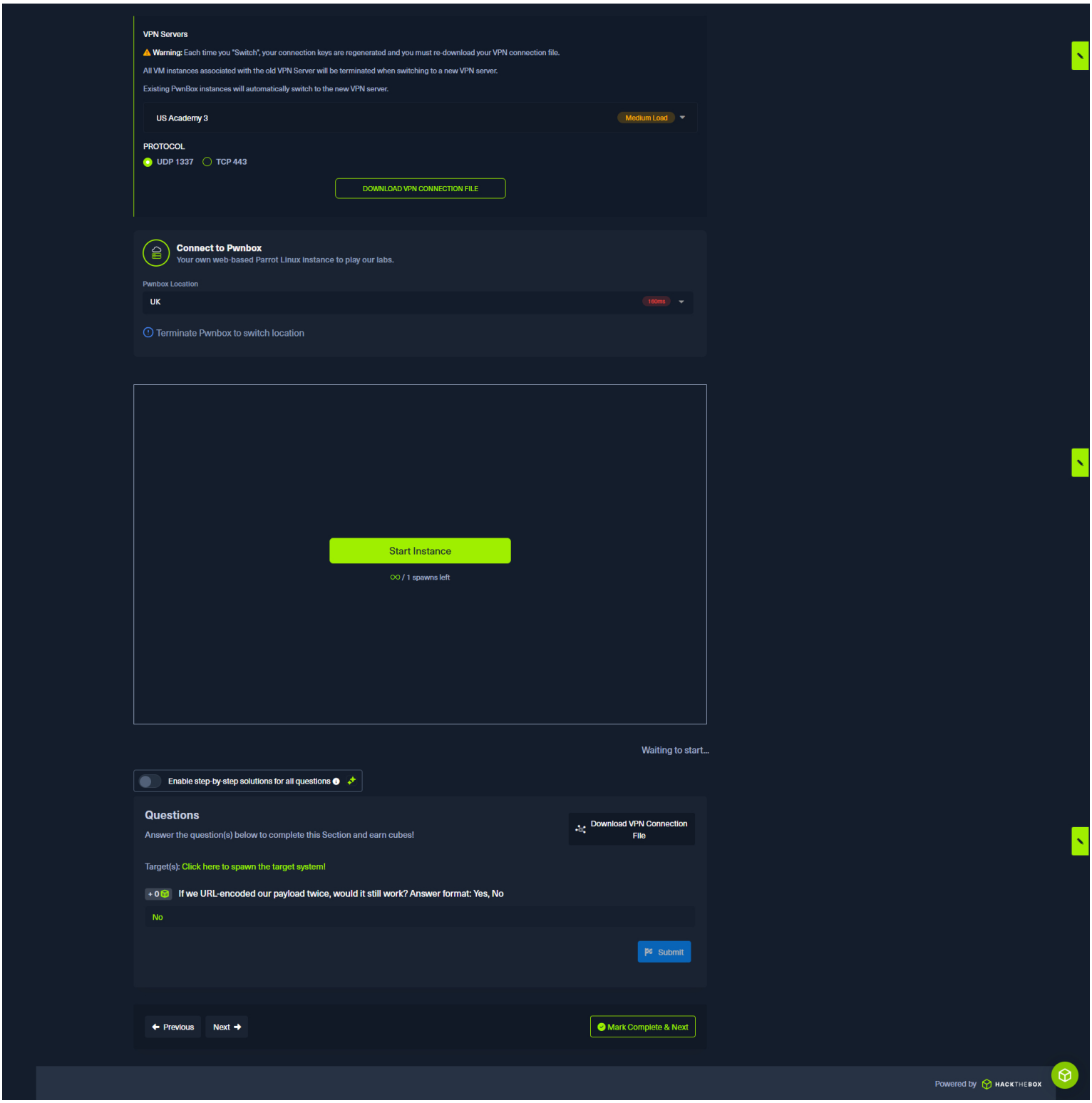
- Information Disclosure (with a twist of SQLi)
- Arbitrary File Upload
- Local File Inclusion (LFI)
- Cross-Site Scripting
- Server-Side Request Forgery (SSRF)
- Regular Expression Denial of Service (ReDoS)
- XML External Entity (XXE) Injection
- Web Service & API Attacks - Skills Assessment

My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left


VPN Servers
Warning: Each time you "Switch", your connection keys are regenerated and you must re-download your VPN connection file.
All VM instances associated with the old VPN Server will be terminated when switching to a new VPN server.
Existing PwnBox instances will automatically switch to the new VPN server.
US Academy 3
Medium Load
PROTOCOL
UDP 1337
TCP 443
DOWNLOAD VPN CONNECTION FILE
Connect to Pwnbox
Your own web-based Parrot Linux instance to play our labs.
Pwnbox Location
UK
160ms
Terminate Pwnbox to switch location
Start Instance
∞ / 1 spawns left
Waiting to start...
Enable step-by-step solutions for all questions
Questions
Answer the question(s) below to complete this Section and earn cubes!
Download VPN Connection File
Target(s): Click here to spawn the target system!
+ 0
If we URL-encoded our payload twice, would it still work? Answer format: Yes, No
No
Submit
Previous
Next
Mark Complete & Next
Powered by HACKTHEBOX