

Web Hacking

Khael Kugler



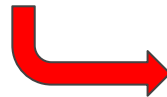
What is this “web”? Requests and Responses:

- HTTP requests and responses
- Request:
 - Asking a server for some data

```
Request
Pretty Raw Hex ↵ \n ≡
1 GET / HTTP/1.1
2 Host: khaalkugler.com
3 Sec-Ch-Ua: " (Not A:Brand);v="8", "Chromium";v="99"
4 Sec-Ch-Ua-Mobile: ?0
5 Sec-Ch-Ua-Platform: "Windows"
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.51
  Safari/537.36
8 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
  webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
9 Sec-Fetch-Site: none
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-User: ?1
12 Sec-Fetch-Dest: document
13 Accept-Encoding: gzip, deflate
14 Accept-Language: en-US,en;q=0.9
15 Connection: close
16
17
```

- Response:
 - The server sends that data

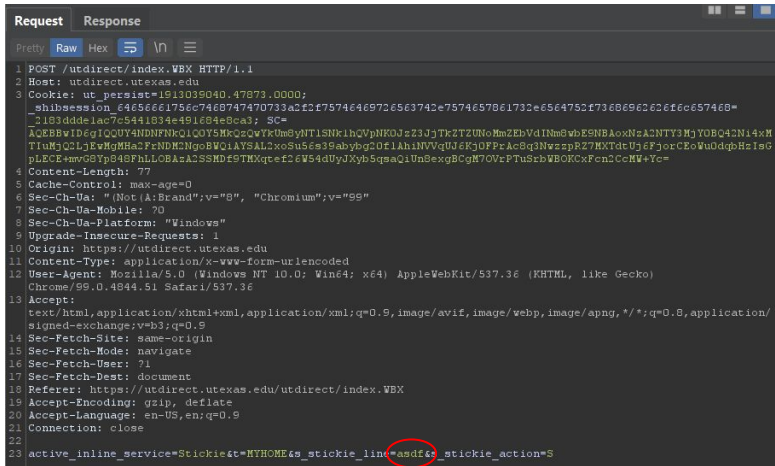
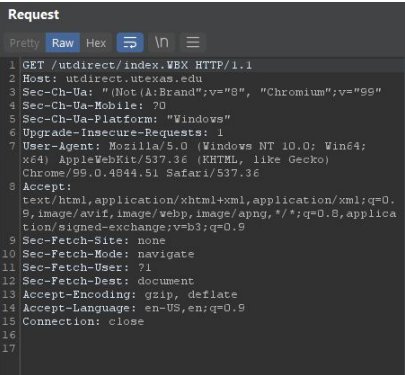
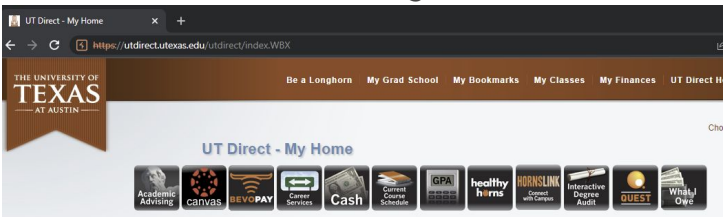
```
Request Response
Pretty Raw Hex Render ↵ \n ≡
1 HTTP/2 200 OK
2 Server: GitHub.com
3 Content-Type: text/html; charset=utf-8
4 Last-Modified: Mon, 29 Jan 2024 06:26:10 GMT
5 Access-Control-Allow-Origin: *
6 Etag: W/"65b746f5-1f1"
7 Expires: Mon, 29 Jan 2024 06:44:33 GMT
8 Cache-Control: max-age=600
9 X-Proxy-Cache: MISS
10 X-GitHub-Request-Id: EAC6:09F3:255A920:32AD4F1:65B746F5
11 Accept-Ranges: bytes
12 Date: Mon, 29 Jan 2024 06:35:38 GMT
13 Via: 1.1 varnish
14 Age: 0
15 X-Served-By: cache-dfw-kdfr8210167-DFW
16 X-Cache: HIT
17 X-Cache-Hits: 1
18 X-Timer: S1706510138.157890,VSO,VE72
19 Vary: Accept-Encoding
20 X-Fastly-Request-Id: b234be38928a6506de0d63daf293748ba9285d49
21 Content-Length: 497
```



```
<!DOCTYPE html>
<html>
  <head>
    <title>
      Khael's Website
    </title>
    <link rel="icon" type="image/x-icon" href="/images/favicon.ico">
    <link rel="stylesheet" type="text/css" href="style.css">
  </head>
  <body>
    <div text box>
      <p>
        Welcome! More stuff coming soon...
      </p>
      <p>
        My <a href="Resume_KhaelKugler.pdf">
          resume
        </a>
      </p>
      <p>
        My <a href="https://www.linkedin.com/in/khael-kugler/">
          LinkedIn
        </a>
      </p>
      <p>
        My <a href="https://github.com/KhaelK130/">
          GitHub
        </a>
      </p>
    </div>
  </body>
</html>
```

Two Important HTTP Requests

- GET Request:
 - Retrieving data from a server
- POST Request:
 - Sending data to a server



A quick cURL demonstration



How do I modify these requests?



- Burp Suite - acts as a proxy between you and the web page

Homepage:

The screenshot shows the Burp Suite interface with the following components:

- Tasks:** A section on the left with a filter dropdown set to "Running". It shows a task "1. Live passive crawl from Proxy (all traffic)" with details: "Add links. Add item itself, same domain and URLs in suite scope." (639 items added to site map), "Capturing: [On]" (559 responses processed, 0 responses queued).
- Issue activity [Pro version only]:** A table of detected issues.
- Event log:** A table of events.
- Advisory:** A section on the right for advisory information.

Issue type	Host	Path	Insertion point
1 Suspicious input transformation (reflected)	http://insecure-bank.com	/url-shorten	input parameter
2 SMTP header injection	http://insecure-website.c...	/contact-us	from parameter
3 Serialized object in HTTP message	http://insecure-bank.com	/blog	
4 Cross-site scripting (DOM-based)	http://insecure-bank.com	/	
5 XML external entity injection	https://vulnerable-website...	/product/stock	request body
6 External service interaction (HTTP)	https://insecure-website...	/product	Referer HTTP header
7 Web cache poisoning	http://insecure-bank.com	/contact-us	
8 Server-side template injection	http://insecure-bank.com	/user-homepage	input parameter
9 SQL injection	https://vulnerable-website...	/	Trackingid cookie
10 OS command injection	http://insecure-website...	/feedback/submit	subject parameter

Time	Type	Source	Message
15:42:25 3 Oct 2023	Error	Proxy	[2] Unknown host: nonexistent-domain.invalid
15:39:48 3 Oct 2023	Error	Proxy	[3] Invalid client request received. Dropped request looping back to same Proxy listener.
15:37:49 3 Oct 2023	Error	Proxy	[1] Failed to connect to 127.0.0.1
15:30:29 3 Oct 2023	Info	Proxy	Proxy service started on 127.0.0.1:8080

Burp Proxy

- Proxy Tab

The screenshot displays the Burp Suite interface, specifically the Proxy Tab. The top menu bar includes options like Burp, Project, Intruder, Repeater, View, and Help. Below the menu, there's a toolbar with icons for Dashboard, Target, Proxy, Intruder, Repeater, Collaborator, Sequencer, Decoder, Comparer, Logger, Extensions, Learn, and Organizer. The main window is divided into several sections:

- HTTP history:** A table listing intercepted HTTP requests. The table has columns for #, Host, Method, URL, Params, Edited, Status code, Length, MIME type, Extension, Title, Comment, TLS, and IP. The selected row (highlighted in blue) is a GET request to `https://api.ipify.org/` with a status code of 200 and a length of 171.
- Request:** A section showing the raw HTTP request details. It includes the method (GET), host (api.ipify.org), and various cookies and headers.
- Response:** A section showing the raw HTTP response details. It includes the status code (200 OK), server (nginx/1.25.1), date (Tue, 03 Oct 2023 20:44:54 GMT), and content type (text/plain).
- Inspector:** A section showing the request and response attributes, cookies, headers, and body.

The bottom of the interface features a search bar and navigation controls.

Using Repeater

[illegible][illegible]

Scoping out a target



Ok, I have a target...

How do I figure out the attack surface (for example, of utexas.edu)?

- Google Dorking
 - Searching for insecure sites index by Google
 - Very useful
- Exploring for sources of user input
 - Items like search boxes and HTML forms
- Automated scanners (dangerous; don't use without explicit permission)
 - E.g. UT bug bounty doesn't allow scanners



Google dorking utexas.edu

- UT's web surface is enormous
- Many old, out-of-date webpages to mess with
 - Lots of already known vulnerabilities
 - Pages last updated before I was born
- Google dork techniques are made plentiful online
 - Find a top 30 list and copy/paste for interesting files



Google

site:utexas.edu intitle:"Index of /"

Images News Videos Books Maps Shopping Flights Finance

About 4,820 results (0.29 seconds)

utexas.edu
http://www.cs.utexas.edu/manual/index-seo.php

ACL2 - Index-of
Index-of. (index-of k x) returns the index of the first occurrence of element k in list x if it exists, NIL otherwise. Index-of is like the Common Lisp ...

utexas.edu
https://orc.csres.utexas.edu/refmanual/ref.index.html

Index of Key Terms
This index is meant to direct the reader to key terms and concepts in this reference manual. It is not a comprehensive index that lists every occurrence of ...

utexas.edu
https://turbulence.oden.utexas.edu/data

Index of /data
Index of /data ; [PARENTDIR], Parent Directory ; [DIR], gridgen_avocet/, 2009-03-27 11:20 ; [DIR], channels/, 2014-09-10 13:47 ...

utexas.edu
https://turbulence.oden.utexas.edu/data

Index of /data
Index of /data ; [DIR], Tijk2/, 2008-09-08 13:45 ; [DIR], channels/, 2014-09-10 13:47 ; [DIR], gridgen_avocet/, 2009-03-27 11:20 ...

utexas.edu
http://www-udc.ig.utexas.edu/...

Index of /hp3
Name · Last modified · Size · Description, [PARENTDIR], Parent Directory, -, [TXT], Read me.txt, 2019-09-25 10:07, 441, [DIR], Task_1_Project_Manag.

Index of /data

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 gridgen_avocet/	2009-03-27 11:20	-	
 channels/	2014-09-10 13:47	-	
 Tijk2/	2008-09-08 13:45	-	
 Tijk/	2007-10-04 17:13	-	
 MKM/	2010-12-17 11:11	-	
 AJZM_old/	2007-02-01 13:58	-	
 AJZM/	2014-05-30 14:01	-	

Let's look at the CS

Images

Videos

News

Shopping

Maps

Books

Flights

Finance

About 3 results (0.27 seconds)



utexas.edu

https://web.ma.utexas.edu/cgi-bin/mp_upload_form

mp_arc upload page

This form allows you to include 1 file. If you need a new form for files, click [here](#). First time users, please read the instructions below, or click on the keyword ...



utexas.edu

<https://docdb.ph.utexas.edu/ut-demo/public/Doc...>

DocDB Instructions

To use this option, select "Archive **Upload**" under "**Upload** Type." When you **upload** your archive you will be asked for two additional pieces of information.



utexas.edu

https://web.ma.utexas.edu/cgi-bin/biz/post_form

UTMath Visitor Form

You'll need to **upload** your identification or social security card as an attachment and sign the Payee Information Form (PIF) electronically. Name of Your ...

Related searches



Cgi bin upload pdf



Cgi bin upload javascript

Submission Page for mp_arc Preprints

This form allows you to include **1 file**. If you need a new form for ☐ files, click [here](#). First time users, please read the [instructions](#) below, or click on the keyword for each entry field before filling out that part of the form.

REQUEST: archive paper

PASSWORD: nhNDD (can be ignored for now)

[FORMAT:](#)[KEYWORDS:](#)[AUTHORS:](#)[TITLE:](#)[ABSTRACT:](#)[COMMENTS:](#) (optional)[PAPER:](#)[Browse...](#) No file selected.

After clicking the button [Submit](#) to submit the above to mp_arc, please wait for the reply: You must respond to that reply before your paper can be archived.

If you need to reset the various form elements to their default states, you can press this button: [Reset To Default Values](#)



My Own Reconnaissance

- Compiled a list of 3000+ “utexas.edu” subdomains
- Attempted to connect to a webserver on each, so 99% should be live

Available here <https://khaelkugler.com/misc/subdomains.txt>:



Common Vulnerabilities



Cross-Site Scripting (XSS)

- Injecting JavaScript into a page
 - Generally through a URL or through stored page data (like a comment section)
- Easily the most common vulnerability on UT - it's basically free money



SQL Injection

- Accessing a SQL database without permission
- Usually via apostrophe or quotation mark

```
<?php
if( isset( $_REQUEST[ 'Submit' ] ) ) {
    // Get input
    $id = $_REQUEST[ 'id' ];

    // Check database
    $query = "SELECT first_name, last_name FROM users WHERE user_id = '$id'";
    $result = mysql_query($GLOBALS["__mysqli_ston"], $query ) or die( '

User ID:



test' OR 1=1;--



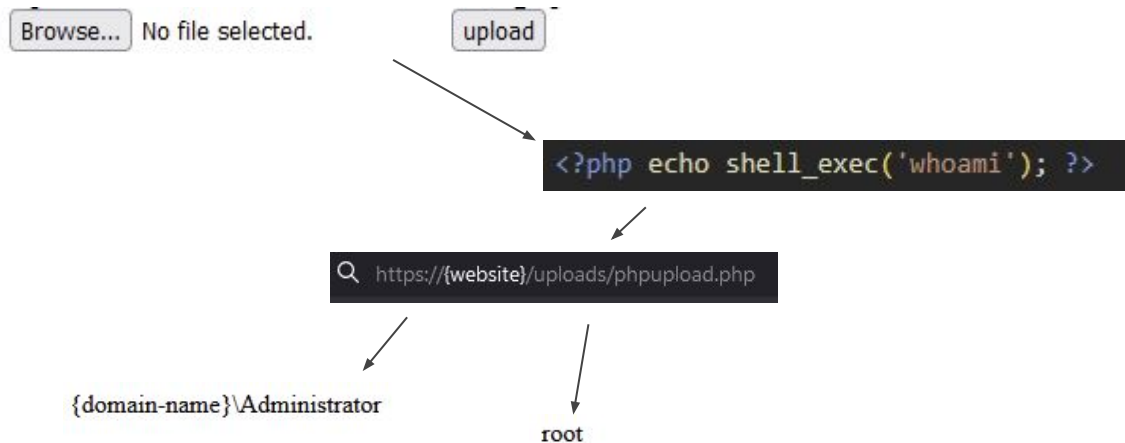
SELECT first_name, last_name FROM users WHERE user_id = 'test' OR 1=1;-- ';;


```

- Cs.utexas.edu databases

Arbitrary File Upload

- Uploading a dangerous file to a server, which it then executes
- More common than you'd expect
 - This is because many filetypes, like PHP, must be executed to be displayed
 - Thus, accessing a PHP file on a server will execute the PHP code inside



Default Credentials

- This is WAY more common than it should be
- With many services, the default credentials can be looked up
 - Usually admin/admin, guest/guest, test/test

This site is asking you to sign in.

Username

Password



User: admin

Password: admin

Some Other Common Vulnerabilities

- Poor Authorization Methods
 - I've found a couple serious examples of this on UT
- Cryptographic Failures
- Insecure Configurations
- Outdated Components
 - Look for service version numbers, and search them up



[Book.hacktricks.xyz](https://book.hacktricks.xyz) has explanations and exploitations of all of these



UT Bug Bounty

What you'll look for

Find all kinds of bugs on UT's domains

- Cross-site scripting (XSS) \$\$\$
- Remote Code Execution (RCE)
- SQL injection
- XML External Entity Injection (XXE)
- Authorization bypass/escalation
- Sensitive information leaks
- Cross-site request forgery (CSRF)

Be sure to log everything you find

What you won't do

- Run automated scanners
- Leak sensitive data
- Break stuff badly
- Mess with regular business operations
- Run ANY TESTING off of the UT VPN
- Share the vulnerabilities you find (like I DIDN'T just do)

Wanna get started?



Thanks! Questions???

