

CSE 406 PROJECT REPORT

# GOBUSTER : A Content Discovery Tool

*Report Prepared by:*

ABRAR MAHMUD - 1905097

SHAHRIAR RAJ - 1905105

*Supervised by:*

A.K.M MEHEDI HASAN

DEPARTMENT OF CSE, BUET

# Contents

<b>1</b>	<b>Introduction</b>	<b>2</b>
1.1	<u>Key Features of Gobuster</u>	2
1.2	Why use Gobuster?	2
<b>2</b>	<b>Installation</b>	<b>3</b>
<b>3</b>	<b>Source Code Overview</b>	<b>3</b>
3.1	cli	3
3.2	libgobuster	5
3.3	gobusterdir	6
3.4	gobusterdns	7
3.5	gobustervhost	8
3.6	gobusterfuzz	9
3.7	gobustergcs	9
3.8	gobusters3	10
3.9	gobustertftp	10
<b>4</b>	<b>Documentation</b>	<b>11</b>
4.1	DIR	12
4.2	DNS	14
4.3	VHOST	15
4.4	FUZZ	17
4.5	GCS	18
4.6	S3	20
4.7	TFTP	21
<b>5</b>	<b>Demonstration</b>	<b>22</b>
5.1	DIR	22
5.2	DNS	25
5.3	VHOST	26
5.4	FUZZ	26
5.5	GCS	27
5.6	S3	31
5.7	TFTP	31

# 1 Introduction

Gobuster is a powerful, open-source tool designed to enumerate files and directories on web/application servers. It is written in Go, making it capable of doing high-performance work. Gobuster is commonly used by cybersecurity professionals, including penetration testers and ethical hackers, to discover hidden resources within web servers and DNS structures that are not typically visible or linked from the main pages of a website.

The tool operates by using wordlists that contain numerous filenames, directory names, or subdomains. These wordlists are used as the basis to systematically check for the existence of resources on the target server or domain. Gobuster can identify potentially unsecured files, directories, and subdomains that might expose sensitive information or reveal insights about the backend structure of the web application, thus highlighting areas that may require further investigation or immediate security measures. The tool is mainly Linux-based.

## 1.1 Key Features of Gobuster

- **Directory/File Enumeration:** Quickly identifies hidden or unlisted directories and files on web servers by brute-forcing URIs using wordlists.
- **DNS Subdomain Enumeration:** Discovers subdomains by brute-forcing domain name systems, helping to map out a target's DNS structure.
- **Virtual Host Scanning:** Can identify virtual hosts configured on web servers.
- **Support for Various Protocols:** Works with HTTP, HTTPS, and supports other schemes by integrating with proxy servers.
- **Customizable:** Supports various flags and configurations to customize scans, including setting custom headers, using cookies, and ignoring SSL/TLS certificate warnings.
- **Concurrent Processing:** Utilizes the Go language's powerful concurrency features to perform multiple requests or queries simultaneously, significantly speeding up the enumeration process.
- **Flexible:** Allows users to exclude certain response sizes, specify status codes to find or ignore, and even resume interrupted scans.

## 1.2 Why use Gobuster?

- It is free and OpenSource
- It is fast and easy to run
- Can be used with customized wordlists
- Supports various protocols beyond HTTP/HTTPS like FTP

Gobuster is popular in the cybersecurity community for its simplicity, speed, and effectiveness. It's an essential tool in the vulnerability assessment and penetration testing processes, aiding in the early stages of assessment by providing insights into possible points of entry and areas requiring deeper security analysis. Whether used for educational purposes, ethical hacking, or professional cybersecurity assessments, Gobuster serves as a critical component in the toolkit of modern security practitioners, emphasizing the importance of proactive security measures and thorough digital infrastructure examination.

## 2 Installation

### Pre Requirements for Gobuster Installation:

- Linux (Preferably Kali Linux)
- go (atleast version 1.16)

#### Installing go:

```
sudo apt update
sudo apt install golang-go
```

#### Installing gobuster:

```
sudo apt install gobuster
```

## 3 Source Code Overview

Gobuster is a content discovery tool written in **go** language. The source code link can be found in the following link: [\[1\]](#)

Each mode of operation is implemented in a different folder in gobuster. Short description of each part is given below:

### 3.1 cli

The cli directory is used for parsing the command line argument and showing output to the console or to a file. If we look at the file **gobuster.go** in the cli folder, we can find some goroutine functions.

- **resultWorker:** It listens for results from **libgobuster.Gobuster** on a channel, formats the results into a string, and prints them to the console or to an output file.
- **errorWorker:** It listens for errors from **libgobuster.Gobuster** on a channel and prints the errors.
- **messageWorker:** It listens for log messages from **libgobuster.Gobuster** on a channel and prints the log messages based on their levels(debug, error and info).

```

func resultWorker(g *libgobuster.Gobuster, filename string, wg *sync.WaitGroup) {
    defer wg.Done()

    var f *os.File
    var err error
    if filename != "" {
        f, err = os.Create(filename)
        if err != nil {
            g.Logger.Fatalf("error on creating output file: %v", err)
        }
        defer f.Close()
    }

    for r := range g.Progress.ResultChan {
        s, err := r.ResultToString()
        if err != nil {
            g.Logger.Fatalf(err)
        }
        if s != "" {
            s = strings.TrimSpace(s)
            _, _ = fmt.Printf("%s\n", TERMINAL_CLEAR_LINE, s)
            if f != nil {
                err = writeToFile(f, s)
                if err != nil {
                    g.Logger.Fatalf("error on writing output file: %v", err)
                }
            }
        }
    }
}

```

Figure 1: resultWorker Function

```

func errorWorker(g *libgobuster.Gobuster, wg *sync.WaitGroup) {
    defer wg.Done()

    for e := range g.Progress.ErrorChan {
        if !g.Opts.Quiet && !g.Opts.NoError {
            g.Logger.Error(e.Error())
            g.Logger.Debug(" %v", e)
        }
    }
}

// messageWorker outputs messages as they come in, this needs to be a range and should not handle
// the context so the channel always has a receiver and libgobuster will not block.
func messageWorker(g *libgobuster.Gobuster, wg *sync.WaitGroup) {
    defer wg.Done()

    for msg := range g.Progress.MessageChan {
        if !g.Opts.Quiet {
            switch msg.level {
            case libgobuster.LevelDebug:
                g.Logger.Debug(msg.Message)
            case libgobuster.LevelError:
                g.Logger.Error(msg.Message)
            case libgobuster.LevelInfo:
                g.Logger.Info(msg.Message)
            default:
                panic(fmt.Sprintf("invalid level %d", msg.level))
            }
        }
    }
}

```

Figure 2: errorWorker and messageWorker Function

```

func progressWorker(ctx context.Context, g *libgobuster.Gobuster, wg *sync.WaitGroup) {
    defer wg.Done()

    tick := time.NewTicker(cliProgressUpdate)

    for {
        select {
        case <-tick.C:
            printProgress(g)
        case <-ctx.Done():
            // print the final progress so we end at 100%
            printProgress(g)
            fmt.Println()
            return
        }
    }
}

```

Figure 3: progressWorker Function

- **progressWorker**: It uses a ticker to print the progress at regular intervals.

The **Gobuster** function is the main entry point of the CLI. It sets up the environment, initializes **libgobuster.Gobuster**, and starts goroutines for workers. It first prints the Gobuster version and configuration details. Then it runs the Gobuster scan with the given context, waits for it to complete, and cleans up after.

```

// Gobuster is the main entry point for the CLI
func Gobuster(ctx context.Context, opts *libgobuster.Options, plugin libgobuster.GobusterPlugin, log libgobuster.Logger) error {
    // Verify flags
    if opts == nil {
        return fmt.Errorf("please provide valid options")
    }

    if plugin == nil {
        return fmt.Errorf("please provide a valid plugin")
    }

    ctxCancel, cancel := context.WithCancel(ctx)
    defer cancel()

    gobuster, err := libgobuster.NewGobuster(opts, plugin, log)
    if err != nil {
        return err
    }

    if !opts.Quiet {
        log.Println(version)
        log.Println("By @Hackplayers (@hackplayers) & Christian Rehnauer (@firefart)")
        log.Println("Gobuster v" + gobuster.Version)
        if err := gobuster.GetConfigString(); err != nil {
            return fmt.Errorf("error on creating config string: %w", err)
        }
        log.Println(c)
        log.Println(version)
        gobuster.Logger.Printf("Starting gobuster in %s mode", plugin.Name())
        if opts.WordlistOffset > 0 {
            gobuster.Logger.Printf("Loading the first %d elements...", opts.WordlistOffset)
        }
    }
}

```

Figure 4: Gobuster Function

## 3.2 libgobuster

The libgobuster directory declares the basic interface of our gobuster object. We can see the basic interface of the gobuster object in the libgobuster.go file of the current folder. The opts parameter defines the mode of operation and the related flags of that mode.

```

// Gobuster is the main object when creating a new run
type Gobuster struct {
    Opts *Options
    Logger Logger
    plugin GobusterPlugin
    Progress *Progress
}

// NewGobuster returns a new Gobuster object
func NewGobuster(opts *Options, plugin GobusterPlugin, logger Logger) (*Gobuster, error) {
    var g Gobuster
    g.Opts = opts
    g.plugin = plugin
    g.Logger = logger
    g.Progress = NewProgress()
    return &g, nil
}

```

Figure 5: Structure of a Gobuster Object

Each mode of operation extends this struct to show their outputs.

```

func (g *Gobuster) Run(ctx context.Context) error {
    defer close(g.Progress.ResultChan)
    defer close(g.Progress.ErrorChan)
    defer close(g.Progress.MessageChan)

    if err := g.plugin.PreRun(ctx, g.Progress); err != nil {
        return err
    }

    var workerGroup sync.WaitGroup
    workerGroup.Add(g.Opts.Threads)

    wordchan := make(chan string, g.Opts.Threads)

    // Create goroutines for each of the number of threads
    // specified.
    for i := 0; i < g.Opts.Threads; i++ {
        go g.worker(ctx, wordchan, &workerGroup)
    }

    scanner, err := g.getWordlist()
    if err != nil {
        return err
    }
}

```

Figure 6: Run function of a Gobuster Object

The **Run** function creates a word channel, takes words as inputs and then uses the **worker** function. In the worker function, the **processWord** function does all mode

```

func (g *Gobuster) worker(ctx context.Context, wordChan <-chan string, wg *sync.WaitGroup) {
    defer wg.Done()
    for {
        select {
        case <-ctx.Done():
            return
        case word, ok := <-wordChan:
            // worker finished
            if !ok {
                return
            }
            g.Progress.IncrementRequests()

            wordCleaned := strings.TrimSpace(word)
            // Skip "comment" (starts with #), as well as empty lines
            if strings.HasPrefix(wordCleaned, "#") || len(wordCleaned) == 0 {
                break
            }

            // Mode-specific processing
            err := g.plugin.ProcessWord(ctx, wordCleaned, g.Progress)
            if err != nil {
                // do not exit and continue
                g.Progress.ErrorChan <- err
                continue
            }

            select {
            case <-ctx.Done():
            case <-time.After(g.opts.Delay):
            }
        }
    }
}

```

Figure 7: Worker function of a Gobuster Object

specific operations. All modes implement this function differently.

Besides, in the **http.go** file in this folder, an http connection is set up to send and receive data from the target url.

```

func NewHttpClient(opt *Options) (*HttpClient, error) {
    var proxyURLFunc func(*http.Request) (*url.URL, error)
    var client *http.Client
    proxyURLFunc = http.ProxyFromEnvironment

    if opt == nil {
        return nil, fmt.Errorf("options is nil")
    }

    if opt.Proxy != "" {
        proxyURL, err := url.Parse(opt.Proxy)
        if err != nil {
            return nil, fmt.Errorf("proxy url is invalid (%w)", err)
        }
        proxyURLFunc = http.ProxyURL(proxyURL)
    }

    var redirectFunc func(req *http.Request, via []*http.Request) error
    if !opt.followRedirect {
        redirectFunc = func(req *http.Request, via []*http.Request) error {
            return http.ErrUseLastResponse
        }
    } else {
        redirectFunc = nil
    }

    tlsConfig := tls.Config{
        InsecureSkipVerify: opt.NoTLSValidation,
        // enable TLS 1.2 and 1.3 support
        MinVersion: tls.VersionTLS12,
    }

    client = &http.Client{
        Transport: &http.Transport{
            Proxy: proxyURLFunc,
            RedirectFunc: redirectFunc,
            TLSClientConfig: &tlsConfig,
        },
    }
}

```

Figure 8: Setting up an http connection

### 3.3 gobusterdir

This mode is used to find hidden directories in a website. If we go to the file **gobusterdir.go** and view the **processWord** function, then we can see that it does the following:

- It constructs the full URL by appending the given word from the word list to the base URL, like **example.com/word** format. It ensures that the base URL ends with a slash and removes any leading slashes from the word.
- It allows for multiple attempts in case of timeout errors based on the values of the flags.
- Then the function sends an http request using **d.http.Request**.
- As a result, we get status code, size of response from the return value, and the result is sent to the result channel.

```

func (d *gobusterDir) ProcessWord(ctx context.Context, word string, progress *lipgaster.Progress) error {
    suffix := ""
    if d.options.useSlash {
        suffix = "/"
    }
    entity := fmt.Sprintf("%s%s", word, suffix)

    // make sure the url ends with a slash
    if !strings.HasSuffix(d.options.url, "/") {
        d.options.url = fmt.Sprintf("%s/", d.options.url)
    }

    // prevent double slashes by removing leading /
    if strings.HasPrefix(entity, "/") {
        // get rid of first / and trim it
        _ = utf8.DecodeRuneInString(entity)
        entity = entity[1:]
    }
    url := fmt.Sprintf("%s%s", d.options.url, entity)

    tries := 1
    if d.options.retryOnTimeout && d.options.retryAttempts > 0 {
        // add it so it will be the overall max requests
        tries += d.options.retryAttempts
    }
}

```

Figure 9: Constructing URL in Directory mode

```

315 var httpHeader
316 var header http.Header
317 for i := 1; i <= tries; i++ {
318     var err error
319     statusCode, httpHeader, err = d.httpRequest(ctx, url, lipgaster.RequestOptions{})
320     if err != nil {
321         // check if it's a timeout and if we should try again and try again
322         // otherwise the timeout error is raised
323         if netErr, ok := err.(net.Error); ok && netErr.Timeout() && i != tries {
324             continue
325         } else if strings.Contains(err.Error(), "invalid control character in url") {
326             // the error is wrong and so it's printed out and ignore it
327             // gobuster will not quit
328             progress.ResultChan <- err
329             continue
330         } else {
331             return err
332         }
333     }
334     break
335 }
336 if statusCode != 0 {
337     resultStatus := false
338     if d.options.statusCodesInBlacklist.length() > 0 {
339         if !d.options.statusCodesInBlacklist.contains(statusCode) {
340             resultStatus = true
341         }
342     } else if d.options.statusCodesInWhitelist.length() > 0 {
343         if d.options.statusCodesInWhitelist.contains(statusCode) {
344             resultStatus = true
345         }
346     } else {
347         return fmt.Errorf("StatusCodes and StatusCodesInBlacklist are both not set which should not happen")
348     }
349 }

```

Figure 10: Sending an http request in directory mode

### 3.4 gobusterdns

The DNS mode is used to find subdomains of a website. In DNS mode, the tool appends words in front of the domain name and sends DNS queries to verify which subdomains exist. If we go to the file **gobusterdns.go** and view the **processWord** function, then we can see that it does the following:

```

func (d *gobusterDNS) ProcessWord(ctx context.Context, word string, progress *lipgaster.Progress) error {
    subdomain := fmt.Sprintf("%s.%s", word, d.options.domain)
    if !d.options.domain && !strings.HasPrefix(subdomain, ".") {
        // add a . to indicate this is the full domain and we do not want to traverse the search domain on the system
        subdomain = fmt.Sprintf("%s.", subdomain)
    }

    ips, err := d.dnsLookup(ctx, subdomain)
    if err != nil {
        if !d.isWildcardIPs() || !d.wildcardIPs.ContainsAny(ips) {
            result := result{
                subdomain: subdomain,
                found:      true,
                showIPs:    d.options.showIPs,
                showName:   d.options.showName,
                showURL:    d.options.showURL,
            }
            if d.options.showIPs {
                result.IPs = ips
            } else if d.options.showName {
                cname, err := d.dnsLookupCNAME(ctx, subdomain)
                if err == nil {
                    result.CNAME = cname
                }
            }
            progress.ResultChan <- result
        } else if d.globalopts.Verbose {
            progress.ResultChan <- result{
                subdomain: subdomain,
                found:      false,
                showIPs:    d.options.showIPs,
                showName:   d.options.showName,
            }
        }
    }
    return nil
}

```

Figure 11: processWord function in DNS mode

- It constructs the subdomain by appending the current word to the specified Domain, like **word.example.com** format.
- It performs a DNS lookup for the constructed subdomain using the **dnsLookup** method. If there is no error, it checks for wildcards and ensures the subdomain is not part of the wildcard IPs.
- If **ShowIPs** option is enabled, it includes the resolved IPs in the result. Then it sends the results to the result channel.



- For each word in the wordlist, it either reports the successful resolution of the subdomain or, if in **Verbose** mode, reports when a subdomain is not found.

### 3.5 gobustervhost

For looking for sites that are hosted virtually by the same website, we send http requests to the same website with different hostname in header. If we go to the file **gobuster-vhost.go** and view the **processWord** function, then we can see that it does the following:

- First it constructs the subdomain name from the given word file.

```
func (v *GobusterVhost) ProcessWord(ctx context.Context, word string, progress *llgobuster.Progress) error {
    var subdomain string
    if v.options.AppendDomain {
        subdomain = fmt.Sprintf("%s.%s", word, v.domain)
    } else {
        // wordlist needs to include full domain
        subdomain = word
    }

    tries := 1
    if v.options.RetryOnTimeout && v.options.RetryAttempts > 0 {
        // add it so it will be the overall max request
        tries += v.options.RetryAttempts
    }

    statuscode, size, header, body, err := v.HTTPRequest(ctx, v.options.URL, llgobuster.RequestOptions{Host: subdomain, ReturndBody: true})
    if err != nil {
        // check if it's a timeout and if we should try again and try again
        // otherwise the timeout error is raised
        if neterr, ok := err.(net.Error); ok && neterr.Timeout() && i != tries {
            continue
        } else if strings.Contains(err.Error(), "invalid control character in url") {
            // do gobuster will not quit
            progress.ResultChan <- err
            continue
        } else {
            return err
        }
    }
    break
}
```

Figure 12: Constructing Subdomain in vhost mode

- Then it sends an http request to the subdomain and gets response body, response size and status code as a response.

```
var statusCode int
var size int64
var header http.Header
var body []byte
var i int64 = 1
for i <= tries; i++ {
    statuscode, size, header, body, err := v.HTTPRequest(ctx, v.options.URL, llgobuster.RequestOptions{Host: subdomain, ReturndBody: true})
    if err != nil {
        // check if it's a timeout and if we should try again and try again
        // otherwise the timeout error is raised
        if neterr, ok := err.(net.Error); ok && neterr.Timeout() && i != tries {
            continue
        } else if strings.Contains(err.Error(), "invalid control character in url") {
            // do gobuster will not quit
            progress.ResultChan <- err
            continue
        } else {
            return err
        }
    }
    break
}
```

Figure 13: Get Response in vhost mode

- Now we need to see if the response body is the same as default response body or error response body. So, we send an http request to the domain name to get **normal body**. We also send abnormal request using a **uuid generator** and save the response body as **abnormal body**.
- Finally, we compare our response with normal and abnormal body. If there's no match with either, we can be sure that the response body is from a different website. Thus, we get a new website hosted by the base domain.

```
// subdomain must not match default vhost and non-existent vhost
// or verbose mode is enabled
found := body != nil && bytes.Equal(body, v.normalbody) && bytes.Equal(body, v.abnormalbody)
if (found && !v.options.ExcludeLengthBased.Contains(int(size))) || v.globalopts.Verbose {
    resultStatus := false
    if found {
        resultStatus = true
    }
    progress.ResultChan <- Result{
        found:    resultStatus,
        vhost:    subdomain,
        StatusCode: statusCode,
        Size:     size,
        Header:   header,
    }
}
return nil
```

Figure 14: Compare Responses in vhost mode

## 3.6 gobusterfuzz

Fuzzing is the process of finding different parameters on a website. In FUZZ mode, we can insert content from wordlists into different places of a website and check the responses to understand which parameters are valid for that website. If we go to the file **gobusterfuzz.go** and view the **processWord** function, then we can see that it does the following:

- First, the function replaces the **FuzzKeyword** (a placeholder for the fuzzed payload) in the target URL with the current word from the wordlist.

```
func (d gobusterfuzz) ProcessWord(ctx context.Context, word string, progress *logbuster.Progress) error {
    url := strings.ReplaceAll(d.options.URL, FuzzKeyword, word)
    requestOptions := logbuster.RequestOptions{}

    if len(d.options.Headers) > 0 {
        requestOptions.ModifiedHeaders = make([]logbuster.HTTPHeader, len(d.options.Headers))
        for i := range d.options.Headers {
            requestOptions.ModifiedHeaders[i] = logbuster.HTTPHeader{
                Name: strings.ReplaceAll(d.options.Headers[i].Name, FuzzKeyword, word),
                Value: strings.ReplaceAll(d.options.Headers[i].Value, FuzzKeyword, word),
            }
        }
    }

    if d.options.RequestBody != "" {
        data := strings.ReplaceAll(d.options.RequestBody, FuzzKeyword, word)
        buffer := strings.NewReader(data)
        requestOptions.Body = buffer
    }

    // fuzzing of basic auth
    if strings.Contains(d.options.Username, FuzzKeyword) || strings.Contains(d.options.Password, FuzzKeyword) {
        requestOptions.UpdateBasicAuthUsername = strings.ReplaceAll(d.options.Username, FuzzKeyword, word)
        requestOptions.UpdateBasicAuthPassword = strings.ReplaceAll(d.options.Password, FuzzKeyword, word)
    }

    tries := 1
    if d.options.RetryInterval && d.options.RetryAttempts > 0 {
        // add 1 as it will be the overall max requests
        tries += d.options.RetryAttempts
    }
}
```

Figure 15: Constructing URL in fuzz mode

- Then it sends an http request to the target URL.

```
var statusCode int
var size int64
for i := 1; i <= tries; i++ {
    var err error
    statusCode, size, err = d.http.Request(ctx, url, requestOptions)
    if err != nil {
        // check if it's a timeout and if we should try again and try again
        // otherwise the timeout error is raised
        if netErr, ok := err.(net.Error); ok && netErr.Timeout() && i != tries {
            continue
        } else if strings.Contains(err.Error(), "invalid control character in url") {
            // put error in error chan so it's printed out and ignore it
            // so gobuster will not quit
            progress.ErrorChan <- err
            continue
        } else {
            return err
        }
    }
    break
}

if statusCode != 0 {
    resultStatus := true
    if d.options.ExcludeLengthParsed.Contains(int(size)) {
        resultStatus = false
    }

    if d.options.ExcludeStatusCodesParsed.Length() > 0 {
        if d.options.ExcludeStatusCodesParsed.Contains(statusCode) {
            resultStatus = false
        }
    }
}
```

Figure 16: Sending request in fuzz mode

- We get the status code, response size and body. Upon examining these, we can determine which parameters are valid for the website.

## 3.7 gobustergcs

This mode is used to find publicly available gcs buckets. If we go to the file **gobustergcs.go** and view the **processWord** function, then we can see that it does the following:

- First, the function constructs the target URL with the current word from the wordlist, like this **https://storage.googleapis.com/storage/v1/b/bucket/o** format.

```

func (s *gobuster3) processWord(ctx context.Context, word string, progress *illogbustertftp.Progress) error {
    // only check for valid bucket names
    if !isInvalidBucketName(word) {
        return nil
    }

    bucketURL := fmt.Sprintf("https://storage.googleapis.com/storage/v1/b/%s/o/%s?recursive=true", word, s.options.WordlistPath)

    tries := 1
    if s.options.RetryTimeout < 0 {
        // add it to the total number of requests
        tries += s.options.RetryAttempts
    }

    var statusCode int
    var body []byte
    for i := 1; i <= tries; i++ {
        var err error
        statusCode, _, body, err = s.HttpRequest(ctx, bucketURL, illogbustertftp.RequestOptions{ResponseBody: true})
        if err != nil {
            // check if it's a timeout and if we should try again and try again
            // otherwise the timeout error is raised
            if netErr, ok := err.(net.Error); ok && netErr.Timeout() && i != tries {
                continue
            } else if strings.Contains(err.Error(), "invalid control character in url") {
                // put error in error channel so it's printed out and ignore it
                // as gobuster will not read
                progress.ErrorChan <- err
                continue
            } else {
                return err
            }
        }
        break
    }
}

```

Figure 17: Constructing URL and getting response in gcs mode

- Then it sends an http request to the target URL.
- We get the status code, response size and body. From there after clicking on the media links, we can find the publicly available gcs buckets.

### 3.8 gobusters3

This mode works almost identically to gcs. The difference is in the url that is required to access public S3 buckets of amazon. If we go to the file **gobusters3.go** and view the **processWord** function, then we can see that it does the following:

- First, the function constructs the target URL with the current word from the wordlist, like this **https://bucket.s3.amazonaws.com/** format.
- Then it sends an http request to the target URL.

```

func (s *gobusters3) processWord(ctx context.Context, word string, progress *illogbustertftp.Progress) error {
    // only check for valid bucket names
    if !isInvalidBucketName(word) {
        return nil
    }

    bucketURL := fmt.Sprintf("https://s3.amazonaws.com/%s/%s?recursive=true", word, s.options.WordlistPath)

    tries := 1
    if s.options.RetryTimeout < 0 {
        // add it to the total number of requests
        tries += s.options.RetryAttempts
    }

    var statusCode int
    var body []byte
    for i := 1; i <= tries; i++ {
        var err error
        statusCode, _, body, err = s.HttpRequest(ctx, bucketURL, illogbustertftp.RequestOptions{ResponseBody: true})
        if err != nil {
            // check if it's a timeout and if we should try again and try again
            // otherwise the timeout error is raised
            if netErr, ok := err.(net.Error); ok && netErr.Timeout() && i != tries {
                continue
            } else if strings.Contains(err.Error(), "invalid control character in url") {
                // put error in error channel so it's printed out and ignore it
                // as gobuster will not read
                progress.ErrorChan <- err
                continue
            } else {
                return err
            }
        }
        break
    }
}

```

Figure 18: Constructing URL and getting response in s3 mode

- We get the status code, response size and body. From there we can visit the links and see which files are accessible.

### 3.9 gobustertftp

Tftp servers are a type of ftp servers, but with less protection. Tftp servers don't require any password to access them. We can use brute forcing of gobuster to find some filenames in a particular tftp server. If we go to the file **gobustertftp.go** and view the **processWord** function, then we can see that it does the following:

- First, the client is connected to the given server address.
- Then we enumerate our word file for words and send an http request to the server to find the target file with the same name there.

```
// ProcessWord is the process implementation of gobusterTftp
func (d *GobusterTftp) ProcessWord(ctx context.Context, word string, progress *libgobuster.Progress) error {
    c, err := tftp.NewClient(d.options.Server)
    if err != nil {
        return err
    }
    c.SetTimeout(d.options.Timeout)
    wt, err := c.Receive(word, "octet")
    if err != nil {
        // file not found
        if d.globalopts.Verbose {
            progress.ResultChan <- Result{
                filename: word,
                found:     false,
                errorMessage: err.Error(),
            }
        }
        return nil
    }
    result := Result{
        filename: word,
        found:     true,
    }
    if n, ok := wt.(tftp.IncomingTransfer).Size(); ok {
        result.Size = n
    }
    progress.ResultChan <- result
    return nil
}
```

Figure 19: Connecting to server and getting response in tftp mode

- As tftp does not have any protection, we can get the files by the same name returned. Thus, we can find the files in our tftp server.

## 4 Documentation

Running the features in gobuster is very straightforward. We just need to run the commands for the specific mode in gobuster. We can see the basic modes of operation using the **gobuster --help** command.

```
$ gobuster --help
Usage:
  gobuster [command]
```

### Available Commands:

```
completion  Generate the autocompletion script for the
              specified shell
dir          Uses directory/file enumeration mode
dns          Uses DNS subdomain enumeration mode
fuzz         Uses fuzzing mode. Replaces the keyword FUZZ in the
              URL, Headers and the request body
gcs          Uses gcs bucket enumeration mode
help         Help about any command
s3           Uses aws bucket enumeration mode
tftp         Uses TFTP enumeration mode
version      shows the current version
vhost        Uses VHOST enumeration mode (you most probably want
              to use the IP address as the URL parameter)
```

### Flags:

```
--debug          Enable debug output
--delay duration Time each thread waits between
requests (e.g. 1500ms)
```

<code>-h, --help</code>	help for gobuster
<code>--no-color</code>	Disable color output
<code>--no-error</code>	Don't display errors
<code>-z, --no-progress</code>	Don't display progress
<code>-o, --output string</code> defaults to stdout)	Output file to write results to (
<code>-p, --pattern string</code> patterns	File containing replacement
<code>-q, --quiet</code> noise	Don't print the banner and other
<code>-t, --threads int</code> default 10)	Number of concurrent threads (
<code>-v, --verbose</code>	Verbose output (errors)
<code>-w, --wordlist string</code> use STDIN.	Path to the wordlist. Set to - to
<code>--wordlist-offset int</code> wordlist (defaults to 0)	Resume from a given position in the

## 4.1 DIR

The basic structure of dir mode is given below:

```
gobuster dir -u https://example.com -w parameters.txt
```

- dir: DIR mode of operation
- -u: The URL string
- -w: Path to the wordlist file

We can find more about the flags using the command **gobuster dir --help**

```
$ gobuster dir --help
Uses directory/file enumeration mode
```

```
Usage:
gobuster dir [flags]
```

```
Flags:
-f, --add-slash                Append / to each
request
--client-cert-p12 string      a p12 file to use for
options TLS client certificates
--client-cert-p12-password string the password to the p12
file
--client-cert-pem string      public key in PEM
format for optional TLS client certificates
--client-cert-pem-key string  private key in PEM
format for optional TLS client certificates (this key needs to
have no password)
-c, --cookies string          Cookies to use for the
requests
```

-d, --discover-backup	Also search for backup files by appending multiple backup extensions
--exclude-length string	exclude the following content lengths (completely ignores the status). You can separate multiple lengths by comma and it also supports ranges like 203-206
-e, --expanded	Expanded mode, print full URLs
-x, --extensions string	File extension(s) to search for
-X, --extensions-file string	Read file extension(s) to search from the file
-r, --follow-redirect	Follow redirects
-H, --headers stringArray	Specify HTTP headers, -H 'Header1: val1' -H 'Header2: val2'
-h, --help	help for dir
--hide-length	Hide the length of the body in the output
-m, --method string	Use the following HTTP method (default "GET")
--no-canonicalize-headers	Do not canonicalize HTTP header names. If set header names are sent as is.
-n, --no-status	Don't print status codes
-k, --no-tls-validation	Skip TLS certificate verification
-P, --password string	Password for Basic Auth
--proxy string	Proxy to use for requests [http(s)://host:port] or [socks5://host:port]
--random-agent	Use a random User-Agent string
--retry	Should retry on request timeout
--retry-attempts int	Times to retry on request timeout (default 3)
-s, --status-codes string	Positive status codes (will be overwritten with status-codes-blacklist if set). Can also handle ranges like 200,300-400,404.
-b, --status-codes-blacklist string	Negative status codes (will override status-codes if set). Can also handle ranges like 200,300-400,404. (default "404")
--timeout duration	HTTP Timeout (default 10s)
-u, --url string	The target URL
-a, --useragent string	Set the User-Agent string (default "gobuster/3.6")
-U, --username string	Username for Basic Auth

#### Global Flags:

--debug	Enable debug output
--delay duration	Time each thread waits between

requests (e.g. 1500ms)	
--no-color	Disable color output
--no-error	Don't display errors
-z, --no-progress	Don't display progress
-o, --output string	Output file to write results to (defaults to stdout)
-p, --pattern string	File containing replacement patterns
-q, --quiet	Don't print the banner and other noise
-t, --threads int	Number of concurrent threads (default 10)
-v, --verbose	Verbose output (errors)
-w, --wordlist string	Path to the wordlist. Set to - to use STDIN.
--wordlist-offset int	Resume from a given position in the wordlist (defaults to 0)

## 4.2 DNS

The basic structure of dns mode is given below:

```
gobuster dns -d example.com -w subdomains.txt
```

- dns: DNS mode of operation
- -d: The base URL string
- -w: Path to the wordlist file

We can find more about the flags using the command **gobuster dns --help**

```
$ gobuster dns --help
```

Uses DNS subdomain enumeration mode

Usage:

```
gobuster dns [flags]
```

Flags:

-d, --domain string	The target domain
-h, --help	help for dns
--no-fqdn	Do not automatically add a trailing dot to the domain, so the resolver uses the DNS search domain
-r, --resolver string	Use custom DNS server (format server.com or server.com:port)
-c, --show-cname	Show CNAME records (cannot be used with '-i' option)
-i, --show-ips	Show IP addresses
--timeout duration	DNS resolver timeout (default 1s)
--wildcard	Force continued operation when wildcard found

Global Flags:	
<code>--debug</code>	Enable debug output
<code>--delay duration</code>	Time each thread waits between
<code>requests (e.g. 1500ms)</code>	
<code>--no-color</code>	Disable color output
<code>--no-error</code>	Don't display errors
<code>-z, --no-progress</code>	Don't display progress
<code>-o, --output string</code>	Output file to write results to (
<code>defaults to stdout)</code>	
<code>-p, --pattern string</code>	File containing replacement
<code>patterns</code>	
<code>-q, --quiet</code>	Don't print the banner and other
<code>noise</code>	
<code>-t, --threads int</code>	Number of concurrent threads (
<code>default 10)</code>	
<code>-v, --verbose</code>	Verbose output (errors)
<code>-w, --wordlist string</code>	Path to the wordlist. Set to - to
<code>use STDIN.</code>	
<code>--wordlist-offset int</code>	Resume from a given position in the
<code>wordlist (defaults to 0)</code>	

## 4.3 VHOST

The basic structure of vhost mode is given below:

```
gobuster vhost -u https://example.com -w words.txt
```

- vhost: VHOST mode of operation
- -u: The base URL string
- -w: Path to the wordlist file

We can find more about the flags using the command **gobuster vhost --help**

```
$ gobuster vhost --help
```

```
Uses VHOST enumeration mode (you most probably want to use the IP
address as the URL parameter)
```

Usage:

```
gobuster vhost [flags]
```

Flags:

<code>--append-domain</code>	Append main domain from
<code>URL to words from wordlist. Otherwise the fully qualified</code>	
<code>domains need to be specified in the wordlist.</code>	
<code>--client-cert-p12 string</code>	a p12 file to use for
<code>options TLS client certificates</code>	
<code>--client-cert-p12-password string</code>	the password to the p12
<code>file</code>	
<code>--client-cert-pem string</code>	public key in PEM
<code>format for optional TLS client certificates</code>	



```

    --client-cert-pem-key string          private key in PEM
format for optional TLS client certificates (this key needs to
have no password)
-c, --cookies string                    Cookies to use for the
requests
    --domain string                      the domain to append
when using an IP address as URL. If left empty and you specify
a domain based URL the hostname from the URL is extracted
    --exclude-length string              exclude the following
content lengths (completely ignores the status). You can
separate multiple lengths by comma and it also supports ranges
like 203-206
-r, --follow-redirect                  Follow redirects
-H, --headers stringArray              Specify HTTP headers, -
H 'Header1: val1' -H 'Header2: val2'
-h, --help                             help for vhost
-m, --method string                    Use the following HTTP
method (default "GET")
    --no-canonicalize-headers            Do not canonicalize
HTTP header names. If set header names are sent as is.
-k, --no-tls-validation                Skip TLS certificate
verification
-P, --password string                  Password for Basic Auth
    --proxy string                      Proxy to use for
requests [http(s)://host:port] or [socks5://host:port]
    --random-agent                      Use a random User-Agent
string
    --retry                             Should retry on request
timeout
    --retry-attempts int                Times to retry on
request timeout (default 3)
    --timeout duration                  HTTP Timeout (default
10s)
-u, --url string                        The target URL
-a, --useragent string                  Set the User-Agent
string (default "gobuster/3.6")
-U, --username string                  Username for Basic Auth

```

#### Global Flags:

```

    --debug                             Enable debug output
    --delay duration                    Time each thread waits between
requests (e.g. 1500ms)
    --no-color                          Disable color output
    --no-error                          Don't display errors
-z, --no-progress                      Don't display progress
-o, --output string                     Output file to write results to (
defaults to stdout)
-p, --pattern string                    File containing replacement
patterns
-q, --quiet                             Don't print the banner and other
noise

```

<code>-t, --threads int</code>	Number of concurrent threads (default 10)
<code>-v, --verbose</code>	Verbose output (errors)
<code>-w, --wordlist string</code>	Path to the wordlist. Set to - to use STDIN.
<code>--wordlist-offset int</code>	Resume from a given position in the wordlist (defaults to 0)

## 4.4 FUZZ

The basic structure of fuzz mode is given below:

```
gobuster fuzz -u https://example.com?FUZZ=test -w parameters.txt
```

- fuzz: FUZZ mode of operation
- -u: The URL string
- -w: Path to the wordlist file

We can find more about the flags using the command **gobuster fuzz --help**

```
$ gobuster fuzz --help
```

Uses fuzzing mode. Replaces the keyword FUZZ in the URL, Headers and the request body

Usage:

```
gobuster fuzz [flags]
```

Flags:

<code>-B, --body string</code>	Request body
<code>--client-cert-p12 string</code>	a p12 file to use for options TLS client certificates
<code>--client-cert-p12-password string</code>	the password to the p12 file
<code>--client-cert-pem string</code>	public key in PEM format for optional TLS client certificates
<code>--client-cert-pem-key string</code>	private key in PEM format for optional TLS client certificates (this key needs to have no password)
<code>-c, --cookies string</code>	Cookies to use for the requests
<code>--exclude-length string</code>	exclude the following content lengths (completely ignores the status). You can separate multiple lengths by comma and it also supports ranges like 203-206
<code>-b, --excludestatuscodes string</code>	Excluded status codes. Can also handle ranges like 200,300-400,404.
<code>-r, --follow-redirect</code>	Follow redirects
<code>-H, --headers stringArray</code>	Specify HTTP headers, -H 'Header1: val1' -H 'Header2: val2'
<code>-h, --help</code>	help for fuzz

-m, --method string	Use the following HTTP
method (default "GET")	
--no-canonicalize-headers	Do not canonicalize
HTTP header names. If set header names	are sent as is.
-k, --no-tls-validation	Skip TLS certificate
verification	
-P, --password string	Password for Basic Auth
--proxy string	Proxy to use for
requests [http(s)://host:port] or [socks5://host:port]	
--random-agent	Use a random User-Agent
string	
--retry	Should retry on request
timeout	
--retry-attempts int	Times to retry on
request timeout (default 3)	
--timeout duration	HTTP Timeout (default
10s)	
-u, --url string	The target URL
-a, --useragent string	Set the User-Agent
string (default "gobuster/3.6")	
-U, --username string	Username for Basic Auth

#### Global Flags:

--debug	Enable debug output
--delay duration	Time each thread waits between
requests (e.g. 1500ms)	
--no-color	Disable color output
--no-error	Don't display errors
-z, --no-progress	Don't display progress
-o, --output string	Output file to write results to (
defaults to stdout)	
-p, --pattern string	File containing replacement
patterns	
-q, --quiet	Don't print the banner and other
noise	
-t, --threads int	Number of concurrent threads (
default 10)	
-v, --verbose	Verbose output (errors)
-w, --wordlist string	Path to the wordlist. Set to - to
use STDIN.	
--wordlist-offset int	Resume from a given position in the
wordlist (defaults to 0)	

## 4.5 GCS

The basic structure of gcs mode is given below:

```
gobuster gcs -w bucket-names.txt
```

- gcs: gcs mode of operation
- -w: Path to the wordlist file

We can find more about the flags using the command **gobuster gcs --help**

```
$ gobuster gcs --help
```

Uses gcs bucket enumeration mode

Usage:

```
gobuster gcs [flags]
```

Flags:

```
--client-cert-p12 string          a p12 file to use for
options TLS client certificates
--client-cert-p12-password string  the password to the p12
file
--client-cert-pem string           public key in PEM
format for optional TLS client certificates
--client-cert-pem-key string       private key in PEM
format for optional TLS client certificates (this key needs to
have no password)
-h, --help                        help for gcs
-m, --maxfiles int                max files to list when
listing buckets (only shown in verbose mode) (default 5)
-k, --no-tls-validation           Skip TLS certificate
verification
--proxy string                    Proxy to use for
requests [http(s)://host:port] or [socks5://host:port]
--random-agent                    Use a random User-Agent
string
--retry                           Should retry on request
timeout
--retry-attempts int             Times to retry on
request timeout (default 3)
--timeout duration                HTTP Timeout (default
10s)
-a, --useragent string            Set the User-Agent
string (default "gobuster/3.6")
```

Global Flags:

```
--debug                          Enable debug output
--delay duration                 Time each thread waits between
requests (e.g. 1500ms)
--no-color                       Disable color output
--no-error                       Don't display errors
-z, --no-progress               Don't display progress
-o, --output string              Output file to write results to (
defaults to stdout)
-p, --pattern string             File containing replacement
patterns
-q, --quiet                     Don't print the banner and other
noise
-t, --threads int               Number of concurrent threads (
default 10)
-v, --verbose                   Verbose output (errors)
```

```
-w, --wordlist string      Path to the wordlist. Set to - to
                           use STDIN.
    --wordlist-offset int  Resume from a given position in the
                           wordlist (defaults to 0)
```

## 4.6 S3

The basic structure of s3 mode is given below:

```
gobuster s3 -w bucket-names.txt
```

- s3: s3 mode of operation
- -w: Path to the wordlist file

We can find more about the flags using the command **gobuster s3 --help**

```
$ gobuster s3 --help
Uses aws bucket enumeration mode
```

```
Usage:
  gobuster s3 [flags]
```

```
Flags:
  --client-cert-p12 string      a p12 file to use for
options TLS client certificates
  --client-cert-p12-password string  the password to the p12
file
  --client-cert-pem string      public key in PEM
format for optional TLS client certificates
  --client-cert-pem-key string   private key in PEM
format for optional TLS client certificates (this key needs to
have no password)
-h, --help                    help for s3
-m, --maxfiles int            max files to list when
listing buckets (only shown in verbose mode) (default 5)
-k, --no-tls-validation       Skip TLS certificate
verification
  --proxy string              Proxy to use for
requests [http(s)://host:port] or [socks5://host:port]
  --random-agent              Use a random User-Agent
string
  --retry                    Should retry on request
timeout
  --retry-attempts int        Times to retry on
request timeout (default 3)
  --timeout duration          HTTP Timeout (default
10s)
-a, --useragent string        Set the User-Agent
string (default "gobuster/3.6")
```

Global Flags:

<code>--debug</code>	Enable debug output
<code>--delay duration</code> requests (e.g. 1500ms)	Time each thread waits between
<code>--no-color</code>	Disable color output
<code>--no-error</code>	Don't display errors
<code>-z, --no-progress</code>	Don't display progress
<code>-o, --output string</code> defaults to stdout)	Output file to write results to (
<code>-p, --pattern string</code> patterns	File containing replacement
<code>-q, --quiet</code> noise	Don't print the banner and other
<code>-t, --threads int</code> default 10)	Number of concurrent threads (
<code>-v, --verbose</code>	Verbose output (errors)
<code>-w, --wordlist string</code> use STDIN.	Path to the wordlist. Set to - to
<code>--wordlist-offset int</code> wordlist (defaults to 0)	Resume from a given position in the

## 4.7 TFTP

The basic structure of tftp mode is given below:

```
gobuster tftp -s tftp.example.com -w common-filenames.txt
```

- tftp: tftp mode of operation
- -s: The target tftp server
- -w: Path to the wordlist file

We can find more about the flags using the command **gobuster tftp -help**

```
$ gobuster tftp --help
Uses TFTP enumeration mode
```

```
Usage:
gobuster tftp [flags]
```

```
Flags:
-h, --help            help for tftp
-s, --server string    The target TFTP server
--timeout duration    TFTP timeout (default 1s)
```

```
Global Flags:
--debug                Enable debug output
--delay duration        Time each thread waits between
requests (e.g. 1500ms)
--no-color              Disable color output
--no-error              Don't display errors
-z, --no-progress      Don't display progress
```

-o, --output string	Output file to write results to (defaults to stdout)
-p, --pattern string	File containing replacement patterns
-q, --quiet	Don't print the banner and other noise
-t, --threads int	Number of concurrent threads (default 10)
-v, --verbose	Verbose output (errors)
-w, --wordlist string	Path to the wordlist. Set to - to use STDIN.
--wordlist-offset int	Resume from a given position in the wordlist (defaults to 0)

## 5 Demonstration

We will see some demonstration of the 7 different modes of gobuster.

### 5.1 DIR

In the directory mode, we scan for hidden directories and vulnerable files in the websites. A demonstration of directory busting: **First Example:**

```
$ gobuster dir -u https://cse.buet.ac.bd -w test_wordlist.txt -t 25
```

Here we are searching for vulnerable files in cse.buet.ac.bd. The output files are below:

```

=====
[*] Url: https://cse.buet.ac.bd
[*] Method: GET
[*] Threads: 25
[*] Wordlist: small.txt
[*] Negative status codes: 404
[*] User Agent: gobuster/3.6
[*] Expanded: true
[*] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
[[2x]https://cse.buet.ac.bd/.htaccess (Status: 403) [Size: 200]
[[2x]https://cse.buet.ac.bd/.hta (Status: 403) [Size: 200]
[[2x]https://cse.buet.ac.bd/.gitattributes (Status: 403) [Size: 200]
[[2x]https://cse.buet.ac.bd/.gitignore (Status: 403) [Size: 200]
[[2x]https://cse.buet.ac.bd/.httpasud (Status: 403) [Size: 200]
[[2x]https://cse.buet.ac.bd/admin (Status: 307) [Size: 0] [--> https://cse.buet.ac.bd/login]
[[2x]https://cse.buet.ac.bd/@ (Status: 400) [Size: 1134]
[[2x]https://cse.buet.ac.bd/contribute.json (Status: 403) [Size: 200]
[[2x]https://cse.buet.ac.bd/ht (Status: 301) [Size: 315] [--> https://cse.buet.ac.bd/ht/]
[[2x]https://cse.buet.ac.bd/index.php (Status: 200) [Size: 32092]
[[2x]https://cse.buet.ac.bd/moodle (Status: 301) [Size: 319] [--> https://cse.buet.ac.bd/moodle/]
[[2x]https://cse.buet.ac.bd/new (Status: 301) [Size: 316] [--> https://cse.buet.ac.bd/new/]
[[2x]https://cse.buet.ac.bd/option (Status: 307) [Size: 1] [--> https://cse.buet.ac.bd/login]
[[2x]https://cse.buet.ac.bd/research (Status: 301) [Size: 321] [--> https://cse.buet.ac.bd/research/]
[[2x]https://cse.buet.ac.bd/javascript (Status: 301) [Size: 323] [--> https://cse.buet.ac.bd/javascript/]
=====
Finished
  
```

Figure 20: Output of the dir mode on cse.buet.ac.bd

We get cse.buet.ac.bd/javascript. If we further scan cse.buet.ac.bd/javascript, we get the following output:

```

=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: https://cse.buet.ac.bd/javascript
[+] Method: GET
[+] Threads: 25
[+] Wordlist: small.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Expanded: true
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====

[[2Khttps://cse.buet.ac.bd/javascript/.htpasswd (Status: 403) [Size: 280]

[[2Khttps://cse.buet.ac.bd/javascript/.htaccess (Status: 403) [Size: 280]

[[2Khttps://cse.buet.ac.bd/javascript/.hta (Status: 403) [Size: 280]

[[2Khttps://cse.buet.ac.bd/javascript/jquery (Status: 301) [Size: 330] [--> https://cse.buet.ac.bd/javascript/jquery/]

=====
Finished
=====

```

Figure 21: Output of the dir mode on cse.buet.ac.bd/javascript

If we scan further on cse.buet.ac.bd/javascript/jquery, then we get the following output:

```

=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: https://cse.buet.ac.bd/javascript/jquery
[+] Method: GET
[+] Threads: 25
[+] Wordlist: small.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Expanded: true
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====

[[2Khttps://cse.buet.ac.bd/javascript/jquery/.htaccess (Status: 403) [Size: 280]

[[2Khttps://cse.buet.ac.bd/javascript/jquery/.hta (Status: 403) [Size: 280]

[[2Khttps://cse.buet.ac.bd/javascript/jquery/.htpasswd (Status: 403) [Size: 280]

[[2Khttps://cse.buet.ac.bd/javascript/jquery/jquery (Status: 200) [Size: 271809]

=====
Finished
=====

```

Figure 22: Output of the dir mode on cse.buet.ac.bd/javascript/jquery

We got a hidden file cse.buet.ac.bd/javascript/jquery/jquery which can be accessed. If we access the url, we get:



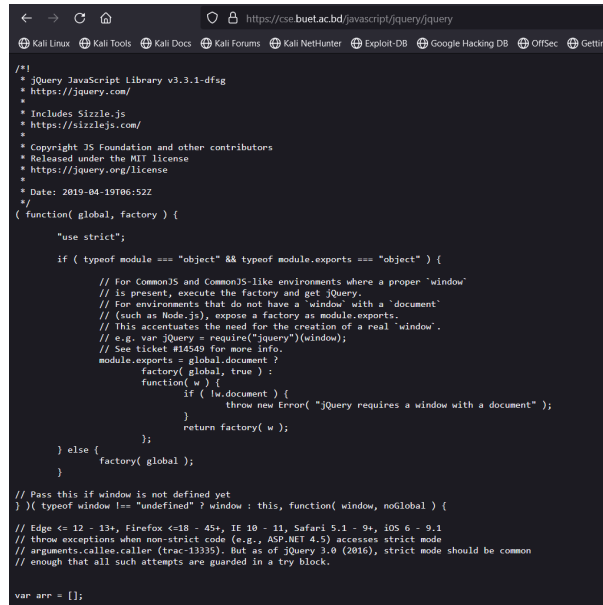


Figure 23: Accessing `cse.buet.ac.bd/javascript/jquery/jquery`

**Second Example:** We will now solve a ctf problem using gobuster. We can find the problem statement here: [Problem](#)

We can get a look at the problem too.

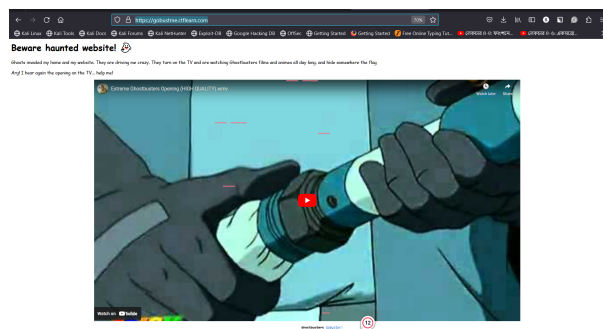


Figure 24: Problem Statement of gobustme

For solving the problem we scan the website using directory busting. The given Command:

```
gobuster dir -u https://gobustme.ctflearn.com -w common1.txt
```

The output for this is as follows:

```

1 Gobuster v3.6
2 by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
3
4 [-] Url: https://gobustme.ctflearn.com/
5 [-] Method: GET
6 [-] Threads: 25
7 [-] Wordlist: common1.txt
8 [-] Negative Status codes: 404
9 [-] User Agent: gobuster/3.6
10 [-] Expanded: true
11 [-] Timeout: 10s
12
13 Starting gobuster in directory enumeration mode
14
15 [2K]https://gobustme.ctflearn.com/.well-known/http-opportunistic (Status: 200) [Size: 32]
16
17 [2K]https://gobustme.ctflearn.com/call (Status: 301) [Size: 169] [→ http://gobustme.ctflearn.com/call/]
18
19 [2K]https://gobustme.ctflearn.com/carpet (Status: 301) [Size: 169] [→ http://gobustme.ctflearn.com/carpet/]
20
21 [2K]https://gobustme.ctflearn.com/flag (Status: 301) [Size: 169] [→ http://gobustme.ctflearn.com/flag/]
22
23 [2K]https://gobustme.ctflearn.com/flag (Status: 301) [Size: 169] [→ http://gobustme.ctflearn.com/flag/]
24
25 [2K]https://gobustme.ctflearn.com/flag (Status: 301) [Size: 169] [→ http://gobustme.ctflearn.com/flag/]
26
27 [2K]https://gobustme.ctflearn.com/index.html (Status: 200) [Size: 2713]
28
29 [2K]https://gobustme.ctflearn.com/shadow (Status: 301) [Size: 169] [→ http://gobustme.ctflearn.com/shadow/]
30
31 [2K]https://gobustme.ctflearn.com/skin (Status: 301) [Size: 169] [→ http://gobustme.ctflearn.com/skin/]
32
33 Finished
34
35
36

```

Figure 25: output of scanning gobustme

We can access [Flag hidden Site](#) and get the flag.

The flag: CTFlearngh0sbu5t3rs4ever

## 5.2 DNS

By dns busting, we can discover the subdomains of a site. We can again take cse.buet.ac.bd as example.

**The command for the discovery:**

```
$ gobuster dns -d cse.buet.ac.bd -w subdomains-top1million-5000.txt -t 25
```

**The discovery:**

```

=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Domain: cse.buet.ac.bd
[+] Threads: 25
[+] Timeout: 1s
[+] Wordlist: subdomains-top1million-5000.txt
=====
Starting gobuster in DNS enumeration mode
=====

[2K]Found: moodle.cse.buet.ac.bd

[2K]Found: ra.cse.buet.ac.bd

=====
Finished
=====

```

We have found 2 subdomains of cse.buet.ac.bd. One is moodle and another is ra.

### 5.3 VHOST

Now using vhost mode we will try to access the subdomains.

### The Command:

```
$ gobuster vhost -u google.com -w subdomains-top1million-5000.txt -t 25 --append-domain
```

## The Output:

[illegible]

Figure 26: Output of the vhost mode on google.com

## 5.4 FUZZ

In this mode, we replace the word **FUZZ** by a word of the word file each time and find valid parameters for the url. We are using a word file from Seclists from this link[3] For demonstration, we are using the following command:

```
gobuster fuzz -u https://play.picoctf.org/practice?FUZZ=1 -w /
  home/piyal/SecLists/Discovery/Web-Content/BurpSuite-ParamMiner
  /lowercase-headers -b 400,301 > fuzz2.txt
```

Different parts of the command are explained below:

- fuzz: fuzz mode of operation
- -u: The target url, with the word **FUZZ**, that will be replaced by a word from the word file
- -w: Path to the wordlist file
- -b: The status code 400 and 301 are blocked, so we will not get any response with status code 400 or 301
- : fuzz2.txt: The output will be written to fuzz2.txt file

```

260round: [Status:403] [length:15683] [word-accepted] https://play.picoctf.org/practice/accepted-1
260round: [Status:403] [length:15754] [word-accept-language] https://play.picoctf.org/practice/accept-language-1
260round: [Status:403] [length:15872] [word-access-control-allow-credentials] https://play.picoctf.org/practice/access-control-allow-credentials-1
260round: [Status:200] [length:2466] [word-accept-application] https://play.picoctf.org/practice/accept-application-1
260round: [Status:403] [length:15813] [word-access-control-allow-headers] https://play.picoctf.org/practice/access-control-allow-headers-1
260round: [Status:200] [length:2466] [word-access-control-allow-methods] https://play.picoctf.org/practice/access-control-allow-methods-1
260round: [Status:200] [length:2466] [word-access-control-request-headers] https://play.picoctf.org/practice/access-control-request-headers-1
260round: [Status:200] [length:2466] [word-accept-encoding] https://play.picoctf.org/practice/accept-encoding-1
260round: [Status:200] [length:2466] [word-accept-ranges] https://play.picoctf.org/practice/accept-ranges-1
260round: [Status:200] [length:2466] [word-accept-encoding] https://play.picoctf.org/practice/accept-encoding-1
260round: [Status:200] [length:2466] [word-accept-charset] https://play.picoctf.org/practice/accept-charset-1
260round: [Status:200] [length:2466] [word-accept-version] https://play.picoctf.org/practice/accept-version-1
260round: [Status:200] [length:2466] [word-accesskey] https://play.picoctf.org/practice/accesskey-1
260round: [Status:200] [length:2466] [word-access-control-allow-origin] https://play.picoctf.org/practice/access-control-allow-origin-1
260round: [Status:200] [length:2466] [word-action] https://play.picoctf.org/practice/action-1
260round: [Status:200] [length:2466] [word-admin] https://play.picoctf.org/practice/admin-1
260round: [Status:200] [length:2466] [word-access-control-expose-headers] https://play.picoctf.org/practice/access-control-expose-headers-1
260round: [Status:200] [length:2466] [word-age] https://play.picoctf.org/practice/age-1

```

Figure 27: Output of the fuzz mode

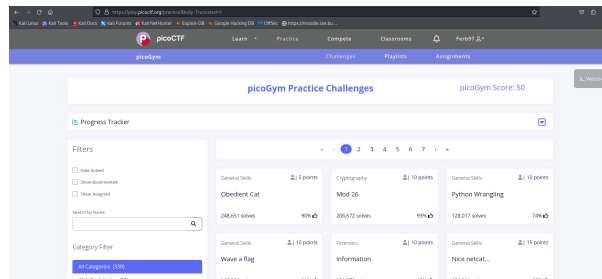


Figure 28: Output result of the fuzz mode

The output is shown below:

We can select a link from the file and view the contents of the link:

Here, the **FUZZ** got replaced by the word **truncated**, and we can see the results. This means **truncated** is a valid parameter to the website. The attackers can use this mode to find valid parameters to launch attacks by injecting values in the parameters.

## 5.5 GCS

GCS mode finds the publicly available buckets from google cloud storage for a given word file. For demonstration, we are using the text file **s3words.txt**. We run the following command:

```
gobuster gcs -w s3words.txt -t 10 > gcs1.txt
```

Different parts of the command are explained below:

- gcs: gcs mode of operation
- -w: Path to the wordlist file
- -t: number of threads
- : gcs1.txt: The output will be written to gcs1.txt file

The output is shown below:

If we paste this link, we will get an output like the following:

The **mediaLink** part contains the link for the file. All files are not accessible here. So, if we want to access the links, we may get a status 403 code. To find out which links are

```

10
11 Starting gobuster in GCS bucket enumeration mode
12
13
14 [2K]https://storage.googleapis.com/storage/v1/b/101/o
15
16 [2K]https://storage.googleapis.com/storage/v1/b/4ever/o
17
18 [2K]https://storage.googleapis.com/storage/v1/b/500/o
19
20 [2K]https://storage.googleapis.com/storage/v1/b/777777/o
21
22 [2K]https://storage.googleapis.com/storage/v1/b/ao2/o
23
24 [2K]https://storage.googleapis.com/storage/v1/b/a12345678/o
25
26 [2K]https://storage.googleapis.com/storage/v1/b/a4e/o
27
28 [2K]https://storage.googleapis.com/storage/v1/b/a79/o
29
30 [2K]https://storage.googleapis.com/storage/v1/b/aa11/o
31
32 [2K]https://storage.googleapis.com/storage/v1/b/aa25/o
33
34 [2K]https://storage.googleapis.com/storage/v1/b/aadhaar/o
35
36 [2K]https://storage.googleapis.com/storage/v1/b/aagc/o
37
38 [2K]https://storage.googleapis.com/storage/v1/b/abbas/o
39
40 [2K]https://storage.googleapis.com/storage/v1/b/abcbac/o
41
42 [2K]https://storage.googleapis.com/storage/v1/b/abcd1234/o
43
44 [2K]https://storage.googleapis.com/storage/v1/b/ability/o

```

Figure 29: Output of the gcs mode

```

{
  kind: "storage#object",
  wE: {
    kind: "storage#object",
    id: "101/EP_9.mp3/15376567579368",
    v etLink: "https://www.googleapis.com/storage/v1/b/101/o/EP_9.mp3",
    w etLink: "https://www.googleapis.com/storage/v1/b/101/o/EP_9.mp3?generation=15376567579368&alt=media",
    name: "EP_9.mp3",
    bucket: "101",
    generation: "15376567579368",
    metageneration: "1",
    contentType: "audio/mpeg",
    storageClass: "REGIONAL",
    size: "43572528",
    md5hash: "8a9d8f22d0c2d4c5",
    crc32c: "9b11f0e",
    etag: "C0b08722d0c2d4c5",
    timeCreated: "2018-09-22T22:53:07.578Z",
    updated: "2018-09-22T22:53:07.578Z",
    timeStorageClassUpdated: "2018-09-22T22:53:07.578Z"
  }
}
{
  kind: "storage#object",
  id: "101/EP_9.mp3/15376567579368",
  v etLink: "https://www.googleapis.com/storage/v1/b/101/o/EP_9.mp3?generation=15376567579368&alt=media",
  w etLink: "https://www.googleapis.com/storage/v1/b/101/o/EP_9.mp3?generation=15376567579368&alt=media",
  name: "EP_9.mp3",
  bucket: "101",
  generation: "15376567579368",
  metageneration: "1",
  contentType: "audio/mpeg",
  storageClass: "REGIONAL",
  size: "43572528",
  md5hash: "8a9d8f22d0c2d4c5"
}

```

Figure 30: Output Media Link of the gcs mode

The billing account for the viewing project is disabled in state closed

Status	Method	Domain	File	Initiator	Type	Transformed	Size	Time	Log
Failed	GET	storage.googleapis.com	EP_9.mp3/15376567579368&alt=media	document	text	435 B	70 B	2018-09-22T22:53:07.578Z	Failed
Failed	GET	storage.googleapis.com	EP_9.mp3/15376567579368&alt=media	document	text	435 B	70 B	2018-09-22T22:53:07.578Z	Failed
Failed	GET	storage.googleapis.com	EP_9.mp3/15376567579368&alt=media	document	text	435 B	70 B	2018-09-22T22:53:07.578Z	Failed

Figure 31: Failed Output of the gcs mode

accessible, we write a python file named **find\_working\_links.py**. The function of the python file is explained below:

- It reads the output from **gcs1.txt** file.
- Then it formats the so they can be used to find files.
- The formatted links are then written to **formatted\_links.txt** file.
- Now, we read the **formatted\_links.txt** file and send request.
- If the status code of the response is 200, we extract the **mediaLink** part and send request to know if the media exists.
- If we get a status response 200, we write the **link**, **mediaLink** and **File type** to **working\_links.txt** file.
- Thus we get all the working media links in **working\_links.txt** file.

```

1 import requests
2 import re
3
4 # Read from output file
5 with open("gcs1.txt", "r") as txt:
6     string = txt.read()
7
8 # Format links
9 links = re.findall(r'https://[^\s]+', string)
10
11 # Write to output file
12 with open("formatted_links.txt", "w") as output:
13     for link in links:
14         output.write(link+"\n")
15

```

Figure 32: Code for formatting the gcs output

```

# Find working links
with open("formatted_links.txt", "r") as linkfile, open("working_links.txt", "w") as worklinkfile:
    # Read all links
    links = linkfile.readlines()
    working_links_count = 0
    for link in links:
        link = link.strip()
        try:
            response = requests.get(link)
            # See inside the links if we get a success code
            if(response.status_code == 200):
                json_data = response.json()
                if "items" in json_data and len(json_data["items"]) > 0:
                    # Get media link
                    media_link = json_data["items"][0].get("mediaLink")
                    content_type = json_data["items"][0].get("contentType")
                    media_link_response = requests.get(media_link)
                    if media_link_response.status_code == 200:
                        # Output to file if media link is accessible
                        working_links_count += 1
                        print(media_link)
                        worklinkfile.write(str(working_links_count) + ", link: " + link + "\n")
                        worklinkfile.write("media link: " + media_link + "\n")
                        worklinkfile.write("file type: " + content_type + "\n\n")
        except Exception as e:
            print(f'({str(e)})')

```

Figure 33: Code for finding available medias from the formatted gcs output

The formatted links and found available media links are given below from the output files.

If we paste the available media links, we can find the available media files. The **output files**, python code and necessary files are given in the following github link: [\[2\]](#)

Figure 34: Links after formatting the gcs output

Figure 35: Available medias from the formatted gcs output



## 5.6 S3

In this mode, gobuster looks up for the words in the word files for amazon s3 buckets. Here, we have used a modified file, named **s3wordsv1.txt**. The command for this mode is given below:

```
gobuster s3 -w s3wordsv1.txt -t 10 > s34.txt
```

Different parts of the command are explained below:

- s3: s3 mode of operation
- -w: Path to the wordlist file
- -t: number of threads
- : s34.txt: The output will be written to s34.txt file

The output for this command is given below:

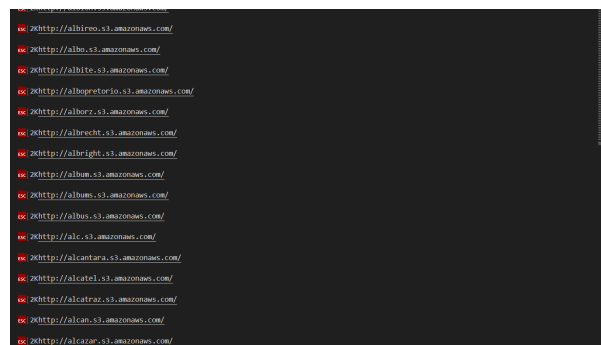


Figure 37: Output of the s3 mode

Most of the links are not accessible. They show the code **AccessDenied**.

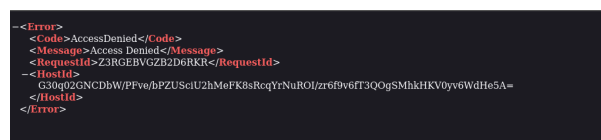


Figure 38: Output Access Denied the s3 mode

We found a link that gives us two links.

We can view the files by putting the file name after the link separated by a slash. Thus we can get publicly available amazon s3 bucket files.

The files that we found are given in the github link [\[2\]](#).

## 5.7 TFTP

TFTP (Trivial File Transfer Protocol) is a simple file transfer protocol. It does not have any authentication protocol like ftp servers. So, it is not suitable for remote networks. Rather, it is set up in a local environment. We set up a tftp server on localhost in **ubuntu**(as we faced some problems setting it up on kali linux), following this link



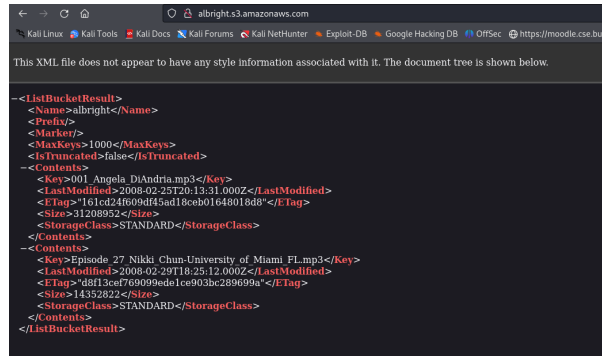


Figure 39: Output Success for the s3 mode

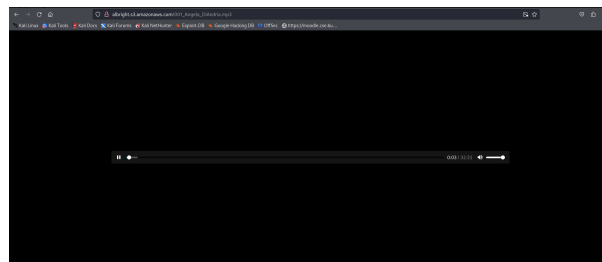


Figure 40: Output File for the s3 mode

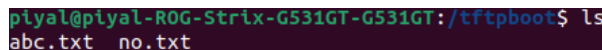


Figure 41: Files in the tftp server

[4]. <https://www.addictivetips.com/ubuntu-linux-tips/set-up-a-tftp-server-on-ubuntu-server/>.

The tftp server was set up on the directory **/tftpboot**. It had the following files: Then we used gobuster to enumerate over the files and find any file mentioned in the **tftp-words.txt** file. The contents of the word file is given below: The command for this

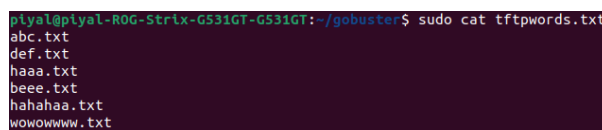


Figure 42: Word File for the tftp mode

operation is given below:

```
./gobuster tftp -s 127.0.0.1 -w tftpwords.txt
```

Different parts of the command are explained below:

- tftp: tftp mode of operation
- -w: Path to the wordlist file
- -s: Link to the tftp server

As we had to set up gobuster on ubuntu for this mode and ubuntu does not support the latest gobuster version, so we built an executable file to run gobuster from the github

code. For this reason, we need to run the executable file each time using `./gobuster`. As the word file contains `abc.txt`, we found the `abc.txt` file. But `no.txt` file was not found as it was not in the word file. Thus, we can find files on our tftp server using gobuster.

```
piyal@piyal-ROG-Strix-G531GT-G531GT:~/gobuster$ ./gobuster tftp -s 127.0.0.1 -w
tftpwords.txt
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Server: 127.0.0.1:69
[+] Threads: 10
[+] Timeout: 1s
[+] Wordlist: tftpwords.txt
=====
Starting gobuster in TFTP enumeration mode
=====
Found: abc.txt
Progress: 7 / 8 (87.50%)
=====
Finished
=====
```

Figure 43: Output for the tftp mode

## References

- [1] *Github Repo For Gobuster*. URL: <https://github.com/OJ/gobuster/>.
- [2] *Github Repo For Output Files and Modes*. URL: <https://github.com/ferb97/CSE406-Security-Project/>.
- [3] *SecLists (Repo with wordlists we used)*. URL: <https://github.com/danielmiessler/SecLists>.
- [4] *TFTP Setup*. URL: <https://www.addictivetips.com/ubuntu-linux-tips/setup-a-tftp-server-on-ubuntu-server/>.