

CYBERTECH AWARENESS PROGRAM CYBERSECURITY AWARENESS AND EDUCATIONAL OUT-REACH

PBURLINGTON, VT

Burpsuite



Security Testing





The Kali Guides provided to you by the Cyber Tech Awareness team are meant for educational purposes ONLY.

The tools covered in the Kali Guides can be used for malicious purposes, but should not be used as such.

The CyberTech Awareness team and the Leahy Center for Digital Forensics and Cybersecurity is NOT responsible any malicious activity conduced with aid from these Kali Guides.

Only use this tool on domains, addresses, files and resources that you have permission to.

Brief Summary

A suite of tools used for penetration testing web applications to check for exploitable security vulnerabilities. Its tools are capable of capturing data, converting that data into different formats, scanning for vulnerabilities, and more.

Penetration Testing:

 A form of ethical hacking where a hacker tests a system's security by simulating an attack, finding the vulnerabilities and exploits that could harm the system, but without causing any damage and then documenting and reporting the findings.

Network Protocol:

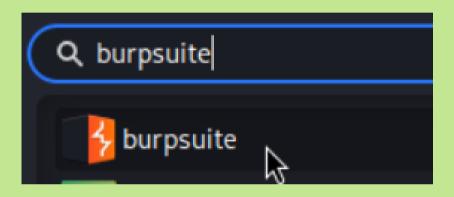
 A universal language for communication between different devices. Each protocol has a set of rules that regulates communications and/or data processing across networks.

HTTP request:

 A network protocol made by a client that is delivered to a server to access a resource on the server. HTTP requests are deployed when accessing content (text, images, video) on the web!

How to Access Burpsuite

Burpsuite is an application on your desktop, so you can type in "burpsuite" in your terminal to access it, or you can click on the application itself.



| ľ | 2 | | | | | | B | urp Suite Com | munity Edition | v2023.10.1.1 | Temporary | Project | | | \odot \odot |
|---|-------------------|------------------|------------|----------------------------------|--|----------|--------------|---------------|----------------|---------------|-----------------|---|-----------------|-------|-----------------|
| | urp Pr Dashboz | | Intruder | | View Help | | Collaborator | <i>c</i> | Decoder | <i>c</i> | 1 | Organizer | Extensions | Learn | (ii) Setti |
| | Lear | n, exp etting | starte | | Intruder ver urp Suite ick start tutorial | Repeater | Collaborator | Sequencer | Decoder | | | a guided vie | deo tour | Learn | Mide this tab |
| ľ | | Startho | | - with our qu | | ta | | | ~ | feat | | | bupsoite | | |
| | See | e how to | use Burp S | tutorials Suite's main | features and | | | Ę | - | Lear Suite | n how to find r | i ty Academy nore vulnerabili | | k | Rider(*) |
| | | | | rt Center our Burp Suit | e questions her | e. | | | | | | witter ige community, | and stay in the | | •€ |

This is the burpsuite window that should pop up!

Example 1: Proxy HTTP Request Intercept and Alteration

| Dashboard Target Proxy Intruder | Repeater 0 | Collaborator | Sequencer | Decoder | Comparer | Logger | Organizer | Extensions | Learn |
|--|----------------------------------|--------------|--------------|------------|-------------|------------|------------|--------------|--------|
| Intercept HTTP history WebSockets history | Proxy s | ettings | | | | | | | |
| 🖉 🔒 Request to https://www.google.com:443 [142.2 | 51.35.164] | | | | | | | | |
| Forward Drop Intercept is | on Actio | n Op | en browser | | | | | | |
| Pretty Raw Hex | | | | | | | | | 🖬 \n ≡ |
| <pre>1 GET /search?q=google&oq=google&gs_lc 2 Host: www.google.com 3 Sec-Ch-Ua: "Chromium";v="117", "Not; 4 Sec-Ch-Ua-Mobile: ?0 5 Sec-Ch-Ua-Platform: "Linux" 0 Upgrade-Insecure-Requests: 1 7 User-Agent: Mozilla/5.0 (Windows NT : 8 Accept: text/html,application/xhtml+xml,appl: 9 X-Client-Data: CNzzygE= 0 Sec-Fetch-Site: none 1 Sec-Fetch-Mode: navigate 2 Sec-Fetch-User: 71 3 Sec-Fetch-Dest: document 4 Accept-Encoding: gzip, deflate, br 5 Accept-Language: en-US,en;q=0.9 5 Connection: close</pre> | A=Brand";v="8" 10.0; Win64; x | 64) AppleWe | ebKit/537.36 | (KHTML, li | ke Gecko) C | nrome/117. | 0.5938.132 | Safari/537.3 | |

What is this command doing?

The user is intercepting an HTTP request within a browser and forwarding the information to be analyzed later. While this intercept is occurring, the client on the browser will not be able to interact with browser elements until the intercept is stopped.

Request to _

• Specifies the HTTP request being intercepted

Forward

 Each time this button is pressed, information is saved about the intercepted request that will then appear under the "HTTP history" tab to be viewed

Intercept is on

• Pauses the request on the client's side until turned off

Raw data

• Displays many details about the intercepted request: host, useragent, etc

Example 1: Proxy HTTP Request Intercept and Alteration

| Name | <your here="" name=""></your> |
|---------|-------------------------------|
| Comment | hello there |
| | |
| | |
| | |
| | Submit |

This image shows the request that is being intercepted- to post a comment that reads "hello there".

| Dashboard Target | Proxy Intruder | Repeater | Collaborator | Sequencer | Settings | | | | |
|--|--|---------------|--|-------------|------------|--|--|--|--|
| Decoder Comparer | Logger Organizer | Extensions | Learn | | | | | | |
| Intercept HTTP history | WebSockets history | Proxy setting | igs | | | | | | |
| Request to http://testphp.v | ulnweb.com:80 [44.228.249. | .3] | | | | | | | |
| Forward Drop | Interce Action | n Open br | Comment this item | * | HTTP/1 (?) | | | | |
| Pretty Raw Hex | | 🗊 \n 🗉 | Inspector | | ÷ 🐵 × | | | | |
| 1 POST /comment.php H 2 Host: testphp.vulnw 3 Content-Length: 99 | eb.com | | < Back | | < > | | | | |
| <pre>4 Cache-Control: max- 5 Upgrade-Insecure-Re 6 Origin: http://test</pre> | quests: 1 | | Path | | | | | | |
| 7 Content-Type: appli | cation/x-www-form-url | | Value | | | | | | |
| Chrome/117.0.5938.1 | 7.36 (KHTML, like Geo | | /comment.php Decoded from: URL path encoding ∨ ④ | | | | | | |
| .9, image/avif, image | on/xhtml+xml,applicat /webp,image/apng,*/*; | | | | | | | | |
| cation/signed-excha 10 Referer: | nge;v=b3;q=0.7 | | /comment.php | | | | | | |
| 11 Accept-Encoding: gz 12 Accept-Language: en 13 Connection: close 14 | -US, en; q=0.9 | Cano | el Ap | ply changes | | | | | |
| 15 name=%3Cyour+name+h Submit=Submit&phpac echo+%24_POS1%5Bcom | tion= | +there& | | | | | | | |
| ⑦ ۞ ← → Search | م | 0 highlights | | | | | | | |

The second image is the intercepted request, where the user can not only see the intercepted request but can type directly into the box to change the request as they wish.

Example 1: Proxy HTTP Request Intercept and Alteration

| Burp Project Intruder Repeater View Help | | | | | | |
|---|-------------------------------------|--|--|--|--|--|
| Dashboard Target Proxy Intruder Repeater | Collaborator Sequencer 🛞 Settings | | | | | |
| Decoder Comparer Logger Organizer Extensions | Learn | | | | | |
| Intercept HTTP history WebSockets history () Proxy setting | gs | | | | | |
| Request to http://testphp.vulnweb.com:80 [44.228.249.3] | | | | | | |
| Forward Drop Interce Action Open br | Comment this item 👋 HTTP/1 🕐 | | | | | |
| Pretty Raw Hex 🗐 🕅 🗏 | Inspector | | | | | |
| 1 GET /userinfo.php HTTP/1.1 | | | | | | |
| 2 Host: testphp.vulnweb.com 3 Content-Length: 99 | K Back K > | | | | | |
| <pre>4 Cache-Control: max-age=0 5 Upgrade-Insecure-Requests: 1 6 Origin: http://testphp.vulnweb.com</pre> | Path | | | | | |
| 7 Content-Type: application/x-www-form-urlencoded | Value | | | | | |
| 8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) | /userinfo.php | | | | | |
| Chrome/117.0.5938.132 Safari/537.36 | / as c a morphy | | | | | |
| <pre>9 Accept: text/html,application/xhtml+xml,application/xml;q=0</pre> | | | | | | |
| .9, image/avif, image/webp, image/apng, */*; q=0.8, appli | Decoded from: URL path encoding ∨ ④ | | | | | |
| <pre>cation/signed-exchange;v=b3;q=0.7 10 Referer:</pre> | /userinfo.php | | | | | |
| http://testphp.vulnweb.com/comment.php?aid=2 | | | | | | |
| 11 Accept-Encoding: gzip, deflate, br 12 Accept-Language: en-US,en;q=0.9 | Cancel Apply changes | | | | | |
| 13 Connection: close | | | | | | |
| 14 15 name=%3Cyour+name+here%3E&comment=goodbye+mwahaha& | | | | | | |
| Submit=Submit&phpaction= | | | | | | |
| echo+%24_POST%5Bcomment%5D%3B | | | | | | |
| | | | | | | |
| | | | | | | |
| ⑦ ⊕ ← > Search P 0 highlights | | | | | | |

This third image is the alterations that the user made to the request to make the commend read "goodbye mwahaha" and to redirect the user to a page that will not actually post the comment.

What is this command doing?

Whereas the first example showed a user intercepting an HTTP request, this example shows the user altering the request after intercepting it. When the intercept is turned off, the page will load on the web page as the altered version.

Example 2: Burpsuite Intruder

| Dashboard Tai | rget Proxy Intruder Repeater Collaborator Sequencer (3) Set | ings Attack | Save Columns | | | | | | |
|--|---|--|--|--|----------|----------|---|---------|-------------|
| Decoder Company | | Results | Positions Payloads | Resource p | ool : | Settings | | | |
| 1 × 2 × + | , | ∑ Fik | er: Showing all items | | | | | | |
| Positions Payload | s Resource pool Settings | Request | Payload | Status code | Error | Timeout | Length | Comment | |
| ⑦ Payload sets | Start attack | 0 | admin | 302 302 | | | 258 258 | | |
| You can define one Various payload typ Payload set: 1 Payload type: Sin | | 2 3 4 5 6 7 8 | test julia sarah tom ben jerny selene | 302 302 302 302 302 302 302 302 | | | 258 258 258 258 258 258 258 258 258 | | - |
| This payload type le | ets you configure a simple list of strings that are used as payloads. | Reques | t Response | | | | | | |
| | - #- !- | | c nesponse | | | | | | 1 |
| Paste | admin test | Pretty | Raw Hex | | | | | | : |
| Paste Load | test julia | Pretty 1 POST | Raw Hex /userinfo.php HTTP/1. | 1 | | | | | = v = |
| | test | Pretty 1 POST 2 Host 3 Cont | Raw Hex /userinfo.php HTTP/1. : testphp.vulnweb.com ent-Length: 26 | 1 | | | | | = v 5 |
| Load | test julia sarah tom ben | Pretty 1 POST 2 Host 3 Cont 4 Cach | Raw Hex /userinfo.php HTTP/1. : testphp.vulnweb.com ent-Length: 26 e-Control: max-age=0 | | | | | | : •• = |
| Load Remove Clear Deduplicate Add | test jula sarah tom ben | Pretty 1 POST 2 Host 3 Cont 4 Cach 5 Uppr 6 Orig 7 Cont 8 User Chro 9 Acce text | Raw Hex /userinfo.php HTTP/1. : testphp.vulnweb.com ent_Length: 26 e-Control: max.age=0 ade-Inscure-Requests: in: http://testphp.vul ent-Type: application, Agent: Mozilla/S.0 (% me/117.0.598.J32 Saf pt: /htal.application/xhtu | : 1 inveb.com findows NT 10 pri/537.36 nl+xml.applic | 0.0; Wir | 164; x64 | | | like Gecko) |
| Load Remove Clear Deduplicate | test jula sarah tom ben | Pretty 1 POST 2 Host 3 Cont 4 Cach 5 Uppr 6 Orig 7 Cont 8 User Chro 9 Acce text 1ica | Raw Hex /userinfo.php HTTP/1. : testphp.vulnweb.com ent-Length: 26 de-Insecure.Requests: in: http://testphp.vul ent-Type: application. -Agent: MozIlla/5.0 (% me/117.0.5938.132 Safa pt: | : 1 inveb.com findows NT 10 pri/537.36 nl+xml.applic | 0.0; Wir | 164; x64 | | | like Gecko) |

What is this command doing?

Using Burp Intruder, a command is being run to test if a list of usernames are valid within a specific website.

Payload settings

• Includes the list of usernames being tested. Can also be set up to scan for passwords.

Results

• What a hacker may be looking at is the Length column which shows the response time from a server. If there is an abnormal response time, it likely means that the server processed it differently than the other inputs

Request

• A further inspection of a specific request after a specific username input

Additional Resources:

Kali Linux Burpsuite Official Webpage: https://www.kali.org/tools/burpsuite/

Burp Suite documentation: https://portswigger.net/burp/documentation

Getting started with Burp Suite: https://portswigger.net/burp/documentation/desktop /getting-started

Burp Suite Training: https://portswigger.net/training

Burp Suite Guide: https://burpsuite.guide/