Cheatography

Web Application PenTesting Cheat Sheet

by blacklist_ via cheatography.com/121658/cs/24003/

Notes

References	
Bug bounty cheatsheet	https://m0chan.github.io/2019/12/17/Bug-Bounty-Cheetsheet.html
Hacktricks cheatsheet	https://book.hacktricks.xyz/bug-bounties-methodology
Tools introduction	https://medium.com/@hakluke
Learn	Understand concept from youtube Read reports on the web, medium, hackerone, twitter, reddit etc..
Practice	Docker websploit PortSwigger Academy
	https://portswigger.net/web-security
Resources	Pentester Lab free VM Another bug-hunting-methodology Another bug-hunting-methodology 2

Checklist

Understand the flow of application	Exploit it | 1Recon - 2 Checklist
Password reset	Change host header
No rate limit	

Bug Hunting Methodlogy

Jason Haddix	Bug-Hunter-Methodology
Approaching target	Recon APT28
Oneforall	Tool Guide Approach
Amass	
Nuclei	
Lazyrecon	
Burpsuite	
Ffuf	
WaybackURL	

Bug Hunting Methodlogy (cont)

Burp	Goto Scope and click use advanced scope control Now we can enter a "term" instead of a domain name Click on add and inside host field enter only the target name like office Pop-up will come up Click no as we still want stuff outside of this term Go back to Sitemap and open menu Click on first option: Show only in scope items Now you can see only those URL with only that term Select all relevant domains or open more and Click on Scan, So that we can crawl all these URLs Menu: Scan details: Select crawl option and you can see a list of URLs/Domains to scan Scan configuration: Click on select from Library and select Fastest Again select from library and select never stop crawl due to application errors Apply those 2 and proceed ahead Goto Resource pool: Click on create new resource pool, assign it a name click on Maximum concurrent requests: 50 Done Burp has started scanning the target to find more subdomains and maybe root domains. Use the dashboard to track the progress
Tools for Automation	
XSS	XSS Hunter
SSRF	Ssrf-Tool Hacktricks
SQL	SQLMAP

Checklist & Tools Test Cases that can be performed & Number of Tools that can be used for this methodology

SQL Injection

Second order SQL Injection	↯ Using this vulnerability we can change the password of the particular username ↯ For example ' -- and create a new account blacklist' -- ↯ ' is Single quote. Used to delineate a query with an unmatched quote
SQL injection ↯ second-order-sql	↯ What happens is there is a query like ↯ UPDATE users set password="new pass" where username="blacklist ' --" and password="this is for current password" ↯ Now when i sue this query after -- becomes just a comment which have no use now and it will directly changed the pass of old user

Tips & Tricks

Twitter

With great flexibility comes great power of messing things up	Having flexibility in web app development also means having facility in creating creating insecure code

SSRF

SSRF

SSRF (cont)

1) What it is (concept)	↯ In a Server-Side Request Forgery (SSRF) attack, the attacker can abuse functionality on the server to read or update internal resources. ↯ The attacker can supply or a modify a URL which the code running on the server will read or submit data to, and by carefully selecting the URLs, the attacker may be able to read server configuration such as AWS metadata, connect to internal services like http enabled databases or perform post requests towards internal services which are not intended to be exposed.
2) Where it can be (where to look for)	↯ SSRF exists when the server, as part of one of its features, fetches data or queries an internal or external resource. The key is that this request includes a value that the attacker can manipulate, potentially allowing the attacker to completely change the request being performed by the server.
3) Goal	↯ The user will need to modify the URL.
4) Automation Tool	↯ Hunt RMX (burp extension) ↯ Ssrfmap
SSRF Detecctor	↯ Detect-ssrf
Tips	↯ The more endpoints you find the more scope you have

SSRF (cont)

Tips	ϟ If you find a subdomain running and identify the service running i.e.-JIRA then you already know endpoints and can try them

AllThingsSSRF

SSRF_Guide

WebHackersWeapons

Cyber Kill Chain APT-28

Cyber Kill Chain	ϟ Phases of Pentesting, Recon and Information gathering is very important phase, A good penetration tester spends 90% of his time in widening the attack surface because he knows this is what its all about. Rest is just a matter of using the correct tools and techniques

1. Reconnaissance | Information Gathering
2. Footprinting | Scanning
3. Vulnerability Assessment | Vulnerability identification and analysis
4. Gaining Access | Exploitation
5. Maintaining Access | Post exploitation
6. Clearing Track

7 Reporting | Re-Testing

ϟ Penetration Testing - Its a process where each next step is dependent on the previous step, Goal is to test each and every vulnerability without overloading the client infrastructure

Professional Penetration Testing Process	🔑 E I F V E R

Cyber Kill Chain APT-28 (cont)

ϟ Engagement | RoE	🔑 Details about penetration test are established 🔑 Quotation: It is in terms of price and estimate of the time required to perform your Job. It depends upon the test is for a network or web application or whole organization, and also depends upon **type of engagement**- black, white, gray and complexity 🔑 Proposal Submittal: Write proposal keeping in mind clients needs and infrastructure. It should include understanding of client requirement and Approach & Methodology that will be used like automated scans or manual testing, or onsite testing. Also it should include the Risks & Benefit , value that pentest will bring to the organization. **Finally Proposal** should include the Scope of Engagement 🔑 Staying in Scope: Always verify if it is client property and you have written permission to conduct assessment on it. So that you dont break the law as few country have rules and regulations that you need to comply with. 🔑 Incident Handling: It is an procedure or set of instruction that needs to be executed by both the parties involved on how to proceed when an incident occurs. Or have a Emergency contact number that might help in incident handling for the client infrastructure. 🔑 Once an emergency contact is set, it should be worth adding a statement to the **Rules Of Engagement** 🔑 Legal Work: Organizations wants you to sign NDA (Non-Disclosure-Agreement). Moreover, as Security Laws vary from country to country you might need to hire a Lawyer. Thus confidentiality must remain, and data cannot be sold to third party, must be encrypted and kept private. 🔑 Finally, **RoE** is document that will define the scope of engagement and put on paper what Pentester is authorized to do and when, this includes the time window for your tests and your contacts in the client organization. And if something goes wrong there should a client contact whom you could coordinate activities or communicate in case something goes wrong

Cyber Kill Chain APT-28 (cont)

Information Gathering | Reconnais-sance	Most crucial stage for success. During this stage, pentester is an investigator who wants to harvest information about the client organization. Also dont engage before the dates as client should not miss a real attack vector. The RoE states if social engineering is allowed. Understanding the Business is an important part as it helps you to understand what is important for your client.
Footprinting & Scanning	
Vulner-ability Assessment	Vulnerability identification and analysis Manual or Automated
Exploitation (Gaining Access) | Post exploitation (Maintaining Access) | Clearing Tracks	Gaining Access & Maintaining Access & Clearing Track
Reporting	Consultancy: This might be required by the Organization after delivering the report as they might need further clarification or help regarding Pentesters Findings. After consultancy a pentester should keep report encrypted or better yet, destroy it.

Cyber Kill Chain APT-28 (cont)

Finally, Information Gathering & Fingerpri-nting is very important to ensure you make your **Target Wider**	Widening the Attack Surface. Sticking to the process is the real secret for an effective pentest. For eg - Highly motivated & Experienced Hacker spend most of their time investigating their victims and gathering information about them using as many sources as possible, this helps them launch highly targeted attacks that do not trigger alarms in the victim defense system. A successful and stealthy attack is made possible by a deep understanding of the target which comes from a thorough information gathering phase

Web Fundamentals

Pentesting Career	Ability to exploit web application and finding vulner-abilities in web servers and services
Protocol	HTTP used to transfer web pages and data from server to client and vice-versa
HTTP (request & response)	The client usually a web browser connects to a web server, i.e.- Apache HTTP Server and MS ISS
HTTP working	Works on Top of TCP Protocol First a TCP connection is established. Then client sends its requests and waits for response. The server processes the request and sends back the response along with a Status Code and Data

Web Fundamentals (cont)

Client ϟ SYN ϟ ACK GET /html ϟ Close Connection	Server ϟ SYN ACK ϟ HTML response
Format of HTTP Headers	ϟ Headers \r \n ϟ \r \n ϟ To end lines in HTTP, use \r (Carriage Return) & \n (New Line) characters ϟ Message Body ϟ Header_name : Header_value
HTTP Request Example	ϟ Request Method ϟ / PATH, the PATH tells the server which resource browser is asking for and there is Protocol version that tells the server how to communicate with the with the browser
Method header	ϟ GET - Used to retrieve, 200 code, returns XML or JSON ϟ POST - Used to send content body, i.e- Parameters and Data ϟ PUT - Update Capabilites ϟ DELETE - Delete a resource identified by a URI
Host header	ϟ HOST header field specifies the internet hostname and port number of the resource being requested ϟ A web server can host multiple websites. This header field tells the server which site the client is asking for ϟ The HOST value is obtained from the URI of the resource

Web Fundamentals (cont)

User-Agent header	ϟ Tells the server which client software is issuing the requests, a client could be Firefox, Google, Edge and a mobile app ϟ Also reveals the server the operating system version
Accept header	ϟ The browser sends the Accept Header field to specify which document type it is expecting in the Response ϟ text/html
Accept-Language header	ϟ Similarly, The browser can ask for a specific language in the response
Accept-Encoding header	ϟ The browser accepts two types of compression, gzip & deflate
Connection header	ϟ The connection header field allows the sender to specify that are desired for that particular connection ϟ i.e.- Connection : keep-alive, Future communications with the server will reuse the current connection
HTTP Response	ϟ When the server receives a request, it processes it and sends back an HTTP response to the client. The response has its own header format. Along with Page Content
Status line	ϟ Status code along with Protocol version
Date	ϟ Date represents the date and time at which the message was originated

Web Fundamentals (cont)

Cache-Control header	ϟ The server informs the client about cached content. Using cache content saves bandwidth as it prevents the client from re-requesting unmodified content.
Content-Type	ϟ Lets the client know how to interpret the body of the message. i.e. - text/html , charset=UTF-8
Content-E-ncoding	ϟ It extends Content-Type and If gzip then message body is compressed with the gzip
Server header	ϟ The server header field contains the header of the server that generated the content ϟ Very useful field during a Pentest to identify the software running on the Web server
Content-Length	

Status Codes