

Financial Safety and Security in the Cyber World

October 2021

प्रगत संगणन विकास केन्द्र

CDAC (CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING), MOHALI

OBJECTIVE

The objective of this presentation is to educate and create awareness amongst the community on use of Technology, Internet Media and its implications on possible cyber crimes.





OUTLINE

- Recent trends and statistics
- Online transaction
- Methods of online transactional Processing
- What is Web Application?
- Cyber Crime
- Phishing
- Sessions and Cookies
- Session Mismanagement
- Password security
- One time password
- URL & Safe Web Browsing

AN UNEXPECTED SUCCESS...



1990s:
Basic
connectivity



2000s:
Application-specific
online content



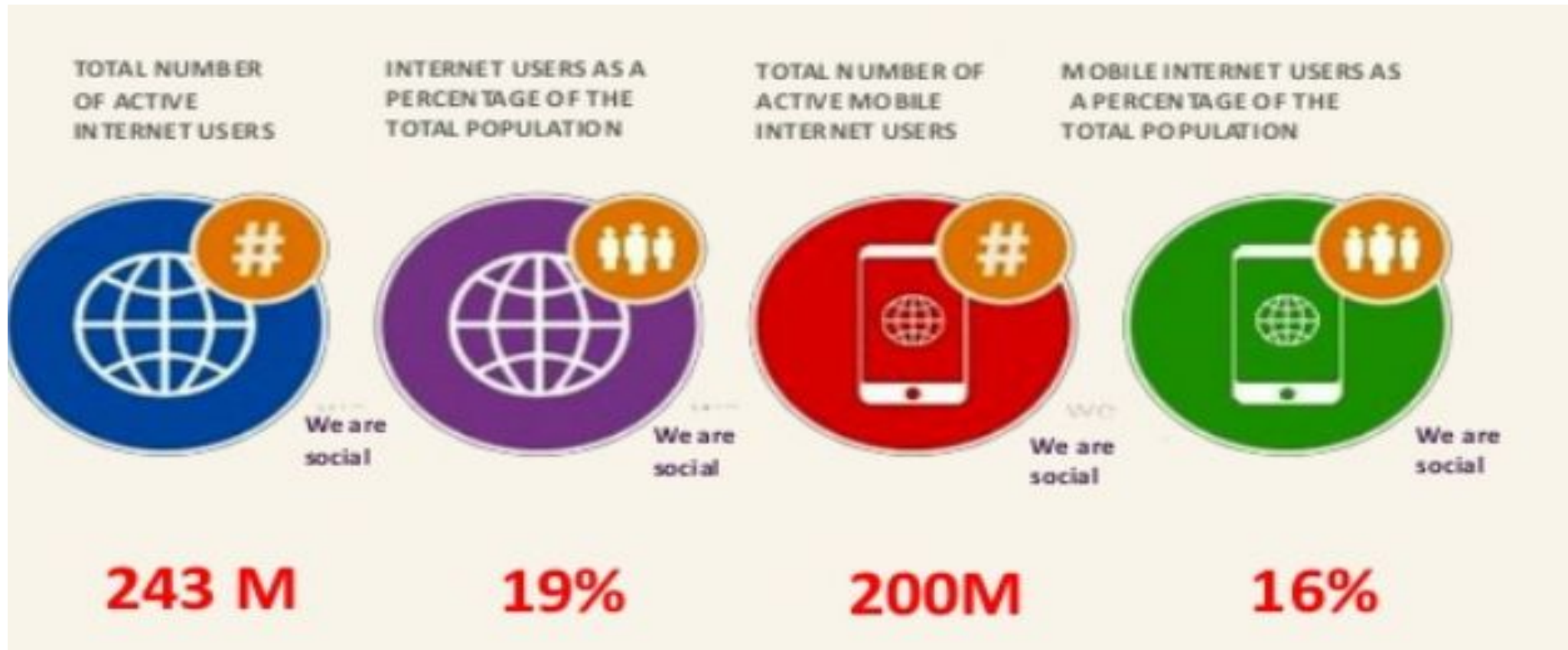
2010s:
Applications/data
in the "cloud"



2020s:
"IoT"

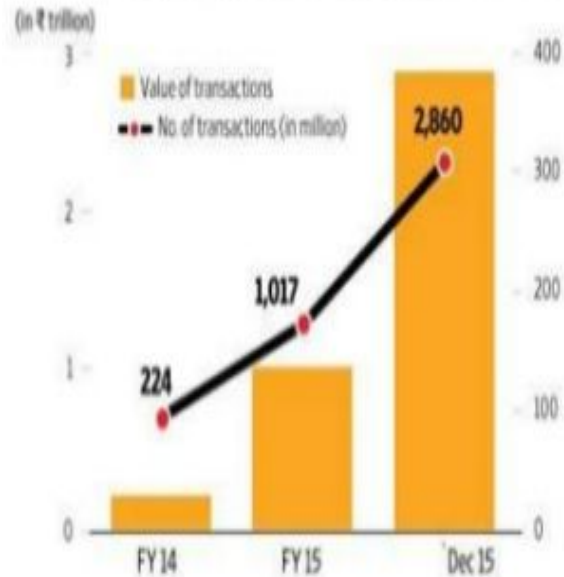
- Evolution of technology, usage and value
- Evolution of security problems and solutions
- Evolution never stops...

RECENT TRENDS AND STATISTICS

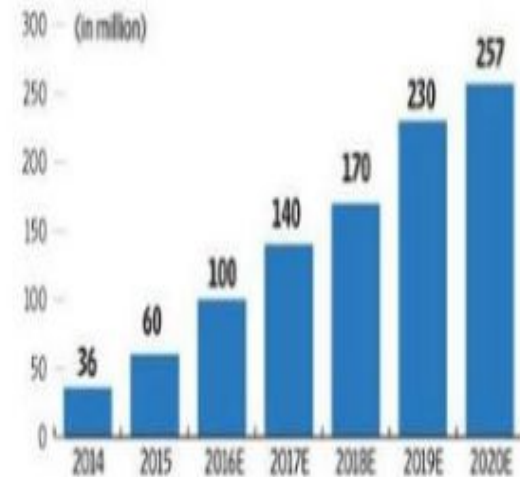


RECENT TRENDS AND STATISTICS

There has been exponential growth in mobile-based transactions.



Mobile banking users are likely to rise at a compounded annual growth rate of 27% during FY16-20.



Gift Cards



Virtual Cards/Digital Wallets/E-Wallets



General Purpose Debit Cards

RECENT TRENDS AND STATISTICS

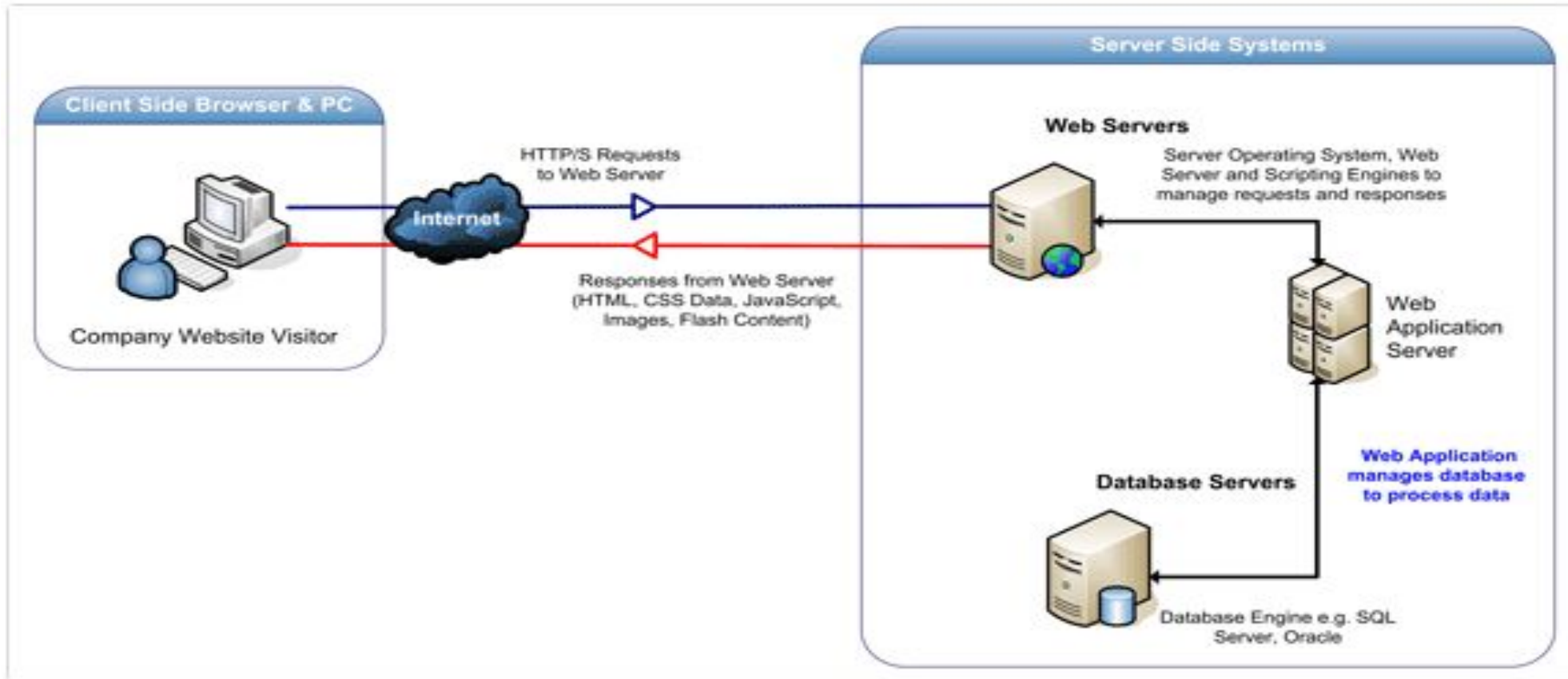




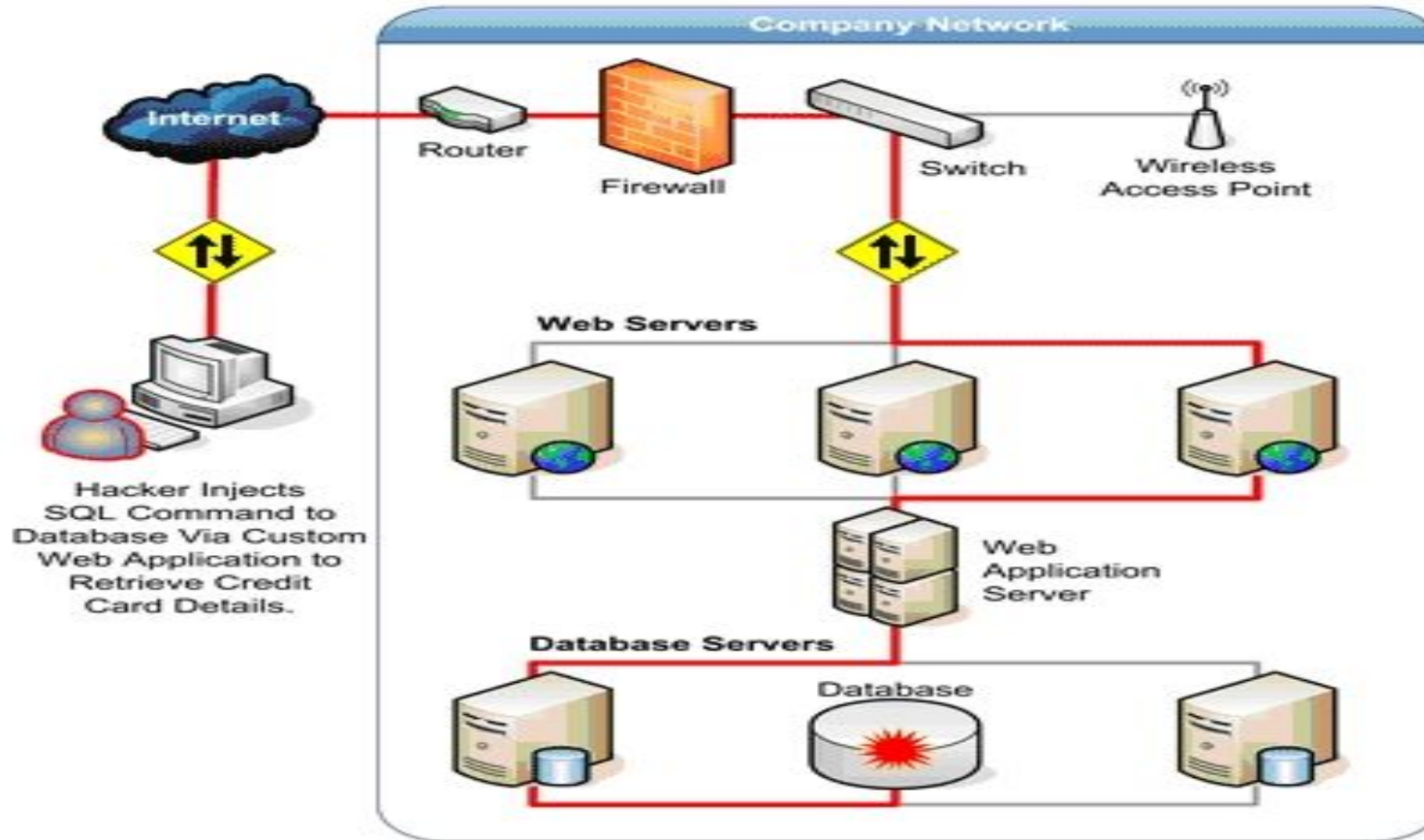
WHAT IS WEB APPLICATION?

- A web application is a client-server computer program which uses web browsers and web technology to allow its visitors to store and retrieve data to/from the database over the internet.
- A web application server are the programs that are used for hosting websites., deployed on a separate

CLIENT – SERVER COMMUNICATION



HOW AN ATTACKER ATTACKS



TYPE OF HACKERS

- 1) White Hat – Good guys. Report hacks/vulnerabilities to appropriate people.
- 2) Black Hat – Only interested in personal goals, regardless of impact.
- 3) Gray Hat – Somewhere in between.
 - Script Kiddies
 - Someone that calls themselves a ‘hacker’ but really isn’t
 - Ethical Hacker
 - Someone hired to hack a system to find vulnerabilities and report on them.
 - Also called a ‘sneaker’



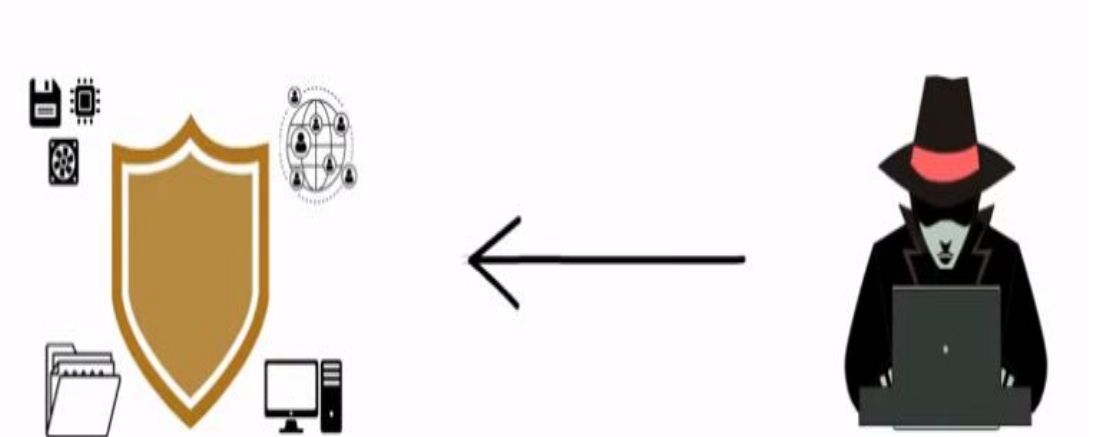
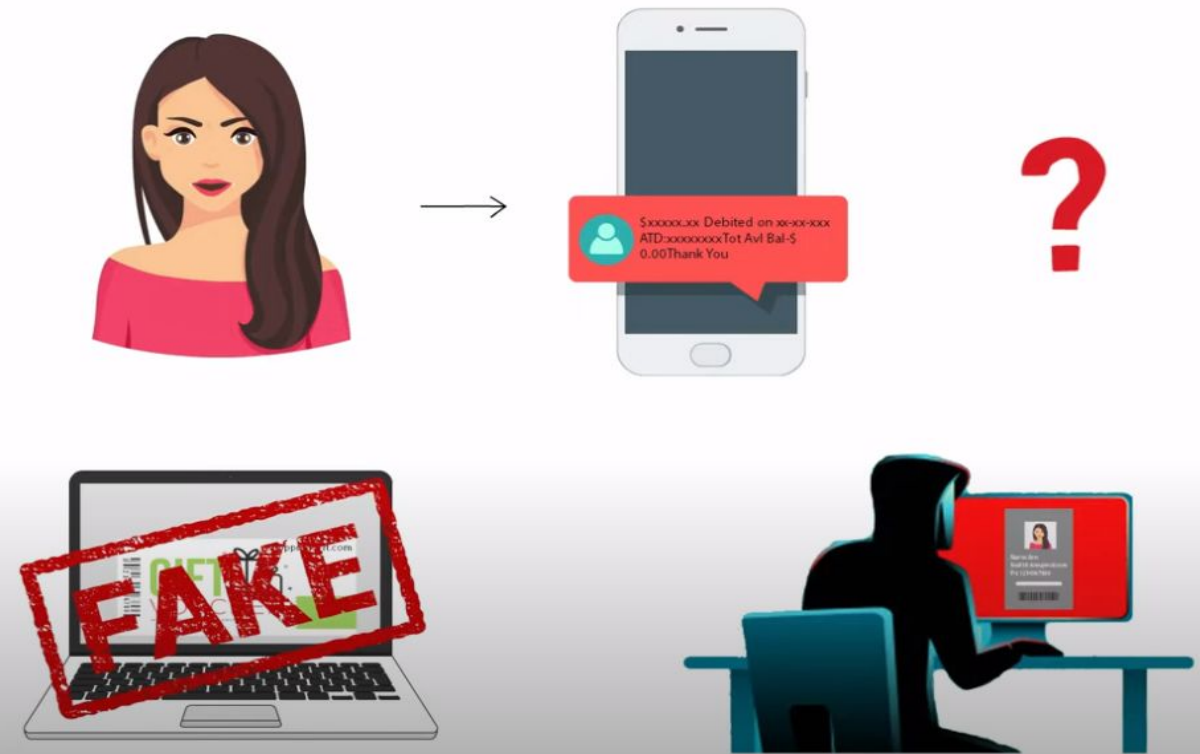
CYBER CRIME

- Internet has disadvantages is cyber crime- illegal activity committed on internet.
- Crime committed using a computer and the internet to steal data or information is cyber crime
- It is combination of information technology, The internet and Virtual reality.

CYBER CRIME



CYBER CRIME

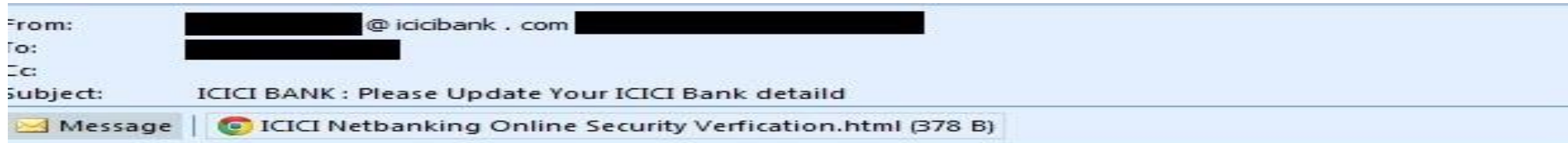




PHISHING

- “Fishing“ for information such as usernames, passwords, credit card details, other personal information
- Forged emails apparently from legitimate enterprises, direct users to forged websites

PHISHING



Net Banking Upgrade Notifications.

Dear ICICI Net Banking User,

ICICI Bank is constantly striving to provide you with more convenience, control, and security to assist in managing your finances online. As part of our ongoing efforts to operate on ISO requirements, and create an enhanced security portal for your online banking services, we have upgraded the ICICI Electronic-Sign Consent and Online Access. To Upgrade your account security status it is mandatory that you kindly Login to your online banking using the link specified below to update us on your account information.

Do kindly update your account profile by downloading the attached file

Note

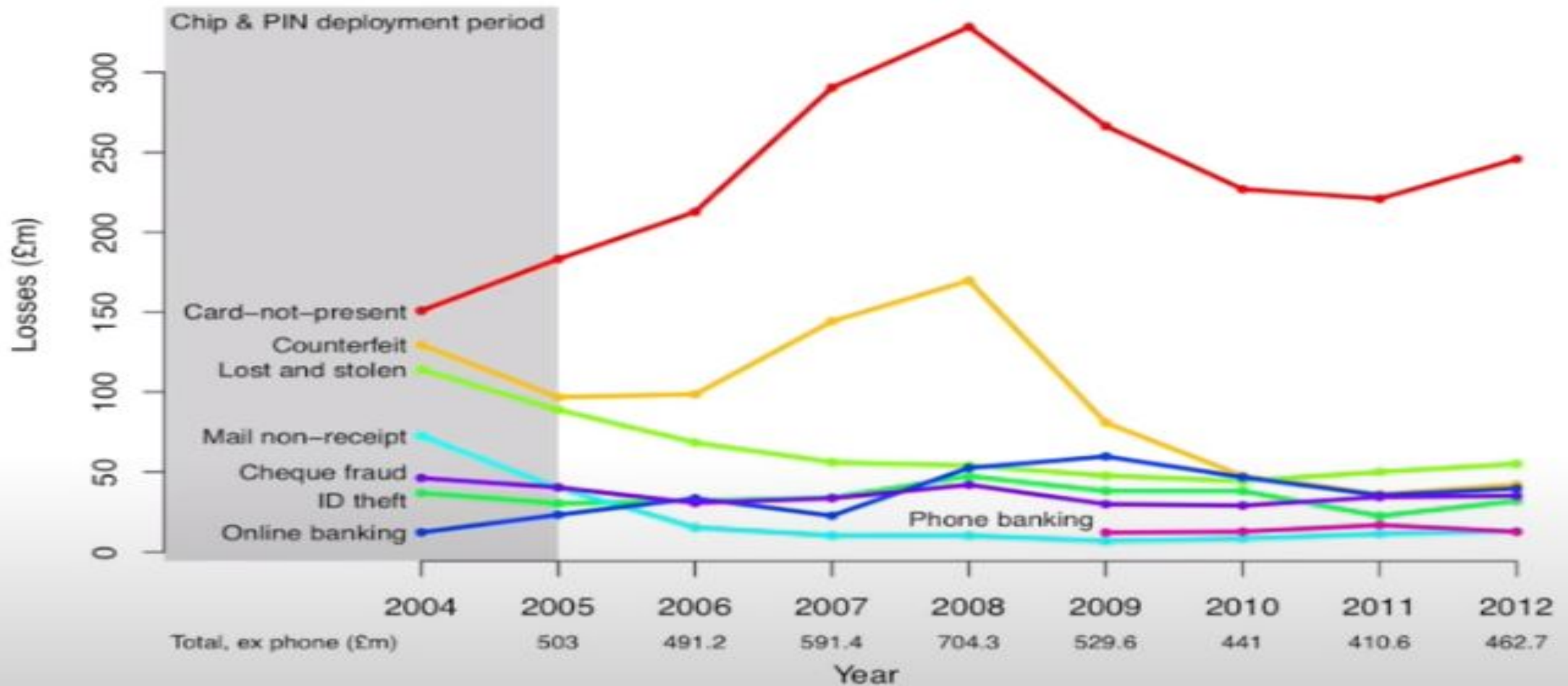
Failure to update your account details within seventy two (72) hours of receiving this notice could lead to account being suspended and online access restricted.

Thank you for your cooperation.

Sincerely,

**ICICI Bank Ltd.
Online Banking Security Unit**

UK fraud figures 2004–2012



PUNE FIRM WINS RS 60 LAKH IN DATA THEFT CASE

By Abhijit Sathe, Mumbai Mirror | Updated: Jun 22, 2013, 06.31 AM IST



A-

A+

Arhan Technologies's ex-staffer stole its business secrets and passed them on to a Japanese firm's Indian arm, his new employer

The state IT authority has ordered a Japanese engineering company's Indian arm to pay a Pune firm Rs 40 lakh for stealing the latter's confidential data, including e-mails, in bid to snatch its customers.

Endo Kogyo India Private Limited carried out the alleged theft of business secrets with the help of a former employee of the Pune firm, Arhan Technologies. The employee, Ashish Kalmegh, has also been asked to pay damages of Rs 20 lakh to Arhan.

Rajesh Aggarwal, secretary of the state information technology department, a quasi-judicial authority, gave the ruling in the case on Wednesday.

Ruling under IT act a first for state

This is the first time in Maharashtra that a commercial entity has been awarded compensation under the IT Act, which is generally used by the police to investigate cases where objectionable content has been shared online or through mobile networks.

Endo Kogyo India and its Japanese parent's lawyers did not argue or contest the ruling, saying they were in the process of challenging Aggarwal's earlier decision to admit the petition filed by Arhan Technologies.

ONLINE TRANSACTION

- Online transaction is a payment method in which the transfer of fund or money happens online over electronic fund transfer. Online transaction process (OLTP) is secure and password protected.
- Three steps involved in the online transaction are Registration, Placing an order, and, Payment.



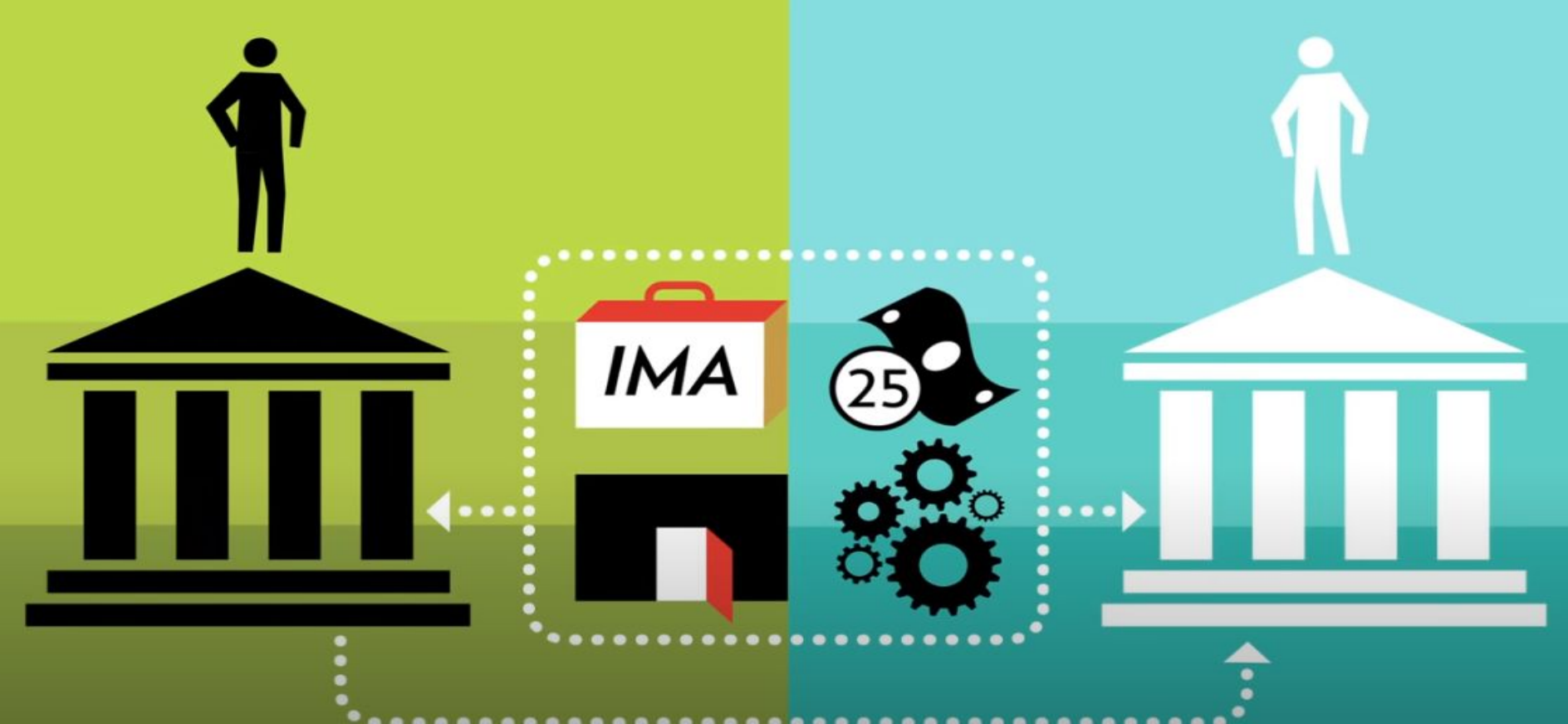
Online Transaction



ONLINE TRANSACTIONAL PROCESSING



ONLINE TRANSACTIONAL PROCESSING





ASSURE BEST OLTP SOLUTION



QUICK



RELIABLE



PCI COMPLIANT



TRUST



BACKUP



SAFE

METHODS OF ONLINE TRANSACTION





DATA PROTECTION

Computer data security is the process of preventing and detecting unauthorized use of your computer data.

It is concerned with 4 main areas –

- Confidentiality
- Integrity
- Availability
- Authentication



PASSWORD SECURITY

Why would someone wants to steal your password ?

Passwords are the only keys that prevent unauthorized entry to many systems.

Password Security Preventions –

- It should be separate for diff-2 email accounts.
- Don't ever reveal your passwords to anyone.
- Write down in a secure location.
- Change your passwords if compromised suspected.
- Add Complexity to passwords .



PASSWORD COMPLEXITY

- Choose at least 8 characters, including:
 - Uppercase
 - Lowercase
 - Numbers
 - Symbols such as @#\$%^&*()!~”
- Avoid simple words
- Don't pick names or nicknames of people
- Don't include repeated characters

EXAMPLE: H1ghc0ur7#1”34”5da



ONE TIME PASSWORD

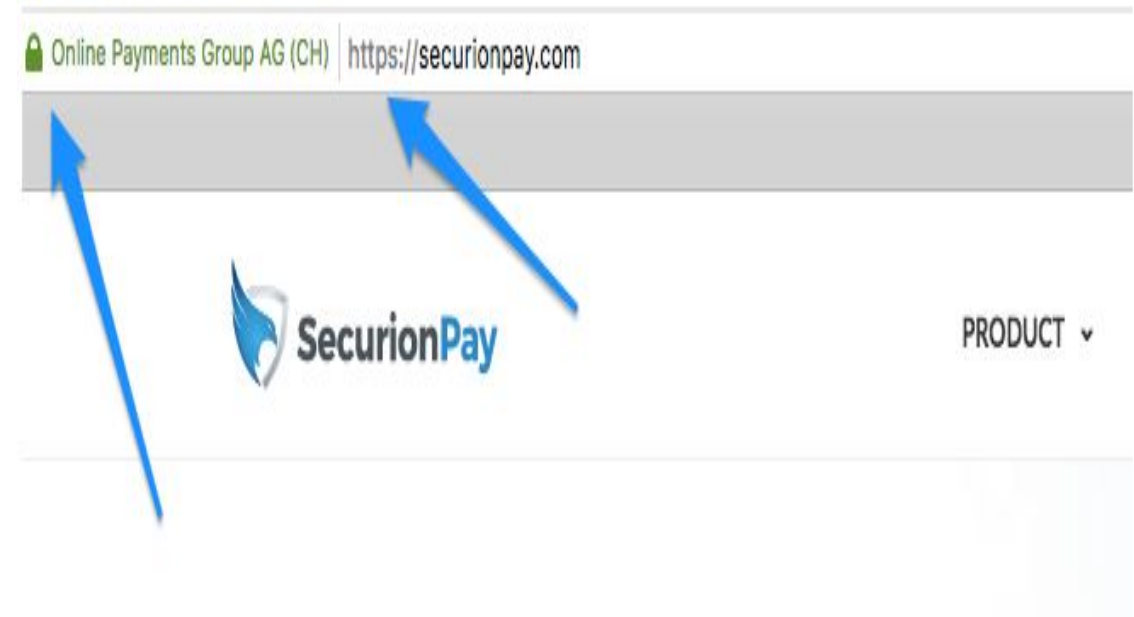
- One-time password (OTP) systems provide a mechanism for logging on to a network or service using a unique password that can only be used once, as the name suggests.
- A one-time password (OTP) is an automatically generated numeric or alphanumeric string of characters that authenticates a user for a single transaction or login session.
- An OTP is more secure than a static password, especially a user-created password, which can be weak and/or reused across multiple accounts.

TIME BASED ONE TIME PASSWORD

- An application can implement several methods for the user to authenticate itself.
 - Method A: What the user know- using username/password
 - Method B: What the user have- A device to generate a OTP(token)
 - Method C: What the user is- using fingerprints or face recognition.
- 1 Factor authentication- Method A
- 2 Factor authentication- Method A and B or C
- 3 Factor authentication- Method A,B,C

FINANCIAL SECURITY METHODS

- How do you provide secure online payments?





SESSIONS

Flow

- User submits login credentials, e.g. username and password
- Server verifies the credentials against DB
- Server creates a temporary user session
- Server issues a cookie with a session ID
- User sends the cookie with each request
- Server validates it against the session store and grants access
- When user logs out, server destroys the session and clears the cookie

COOKIES

- Secure – an option that does not allow for sensitive cookies and session tokens. Example: SSL stripping attacks.
- HttpOnly – an option that mitigates the effect of XSS attacks by preventing accessing sensitive cookies and session tokens.
- Set-Cookie: session=xxxxx; path=/; secure; httponly
- Why?
 - Limit the data exposed by our applications
 - Reduce attack surface from a data perspective

```
Set-Cookie: <cookie-name>=<cookie-value>
```


COOKIES STEALING

- Compromise the server or users browser
- Predict the cookie value
- Sniff the network

Cookie Theft

Sniffing



Cookie Theft

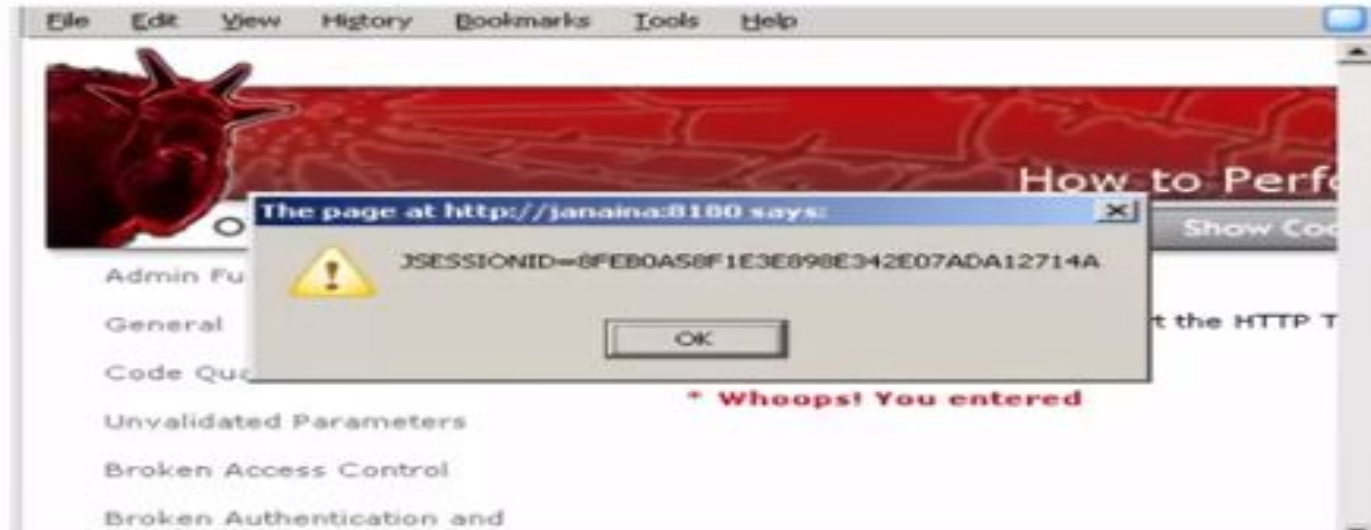
Sniffing



COOKIES

Cookie Theft

XSS - `<SCRIPT>alert(document.cookie);</SCRIPT>`



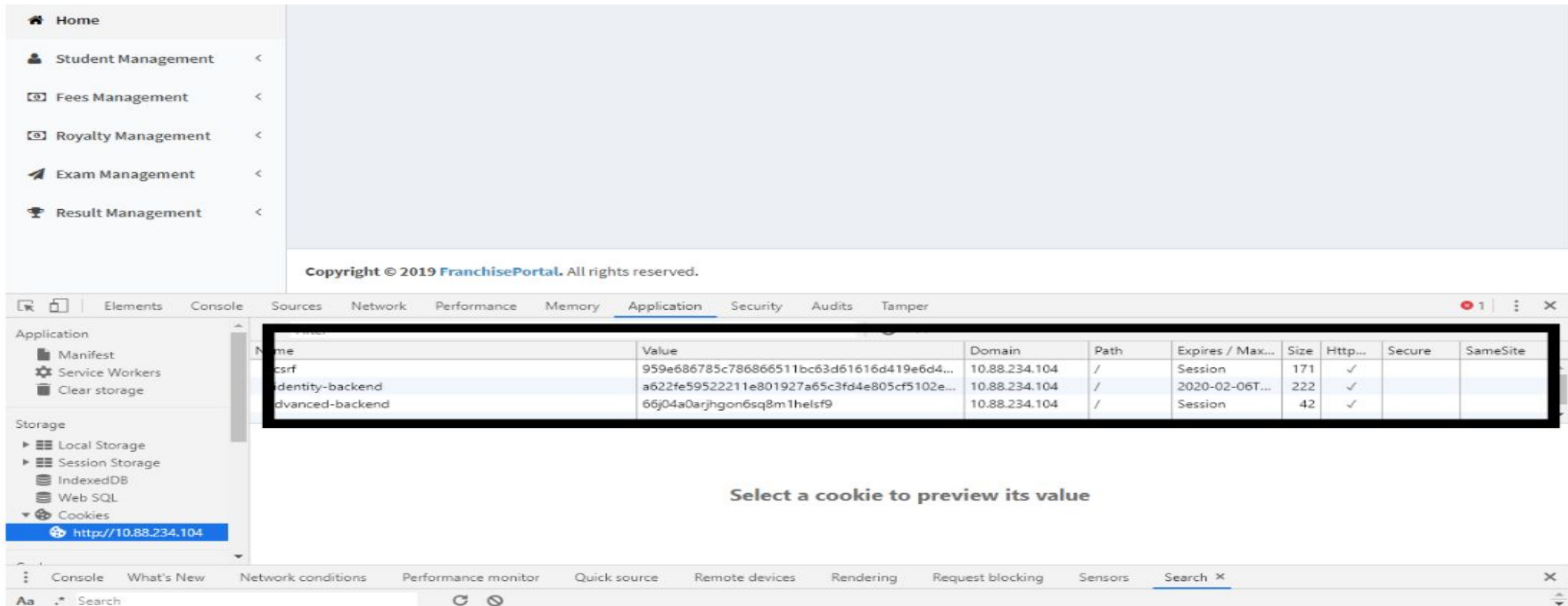


SESSION HIJACKING

- Session hijacking, sometimes also known as cookie hijacking is the exploitation of a valid computer session.
- A cookie must contain some amount of hard-to-guess data.
- The harder it is to forge a valid cookie, the harder is to break into legitimate user's session.
- If an attacker can guess the cookie used in an active session of a legitimate user, he/she will be able to fully impersonate that user.

ANALOGY OF SESSION HIJACKING

Step1: Login to the website and copy the cookie name and value along with the internal page.

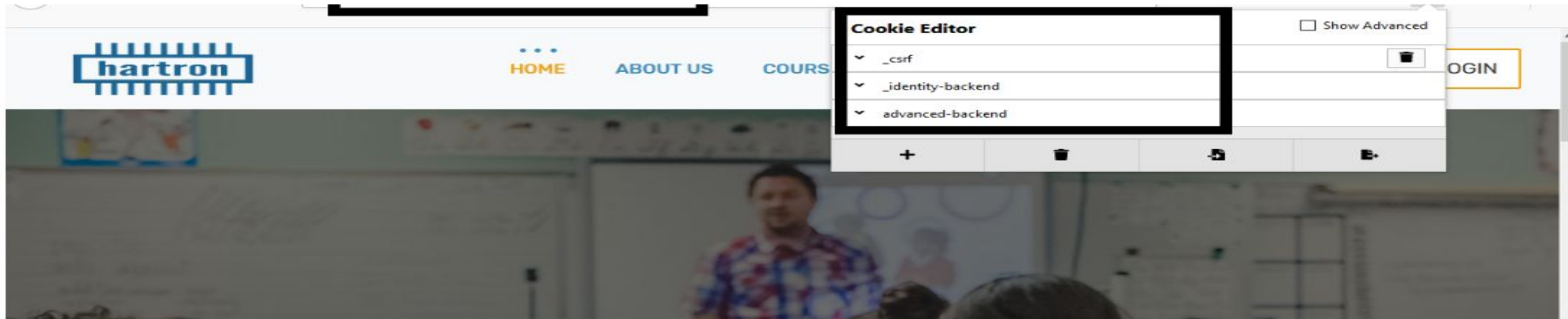


The image shows a web application interface with a sidebar menu and a main content area. The sidebar menu includes: Home, Student Management, Fees Management, Royalty Management, Exam Management, and Result Management. The main content area is mostly blank, with a footer that reads "Copyright © 2019 FranchisePortal. All rights reserved." Below the application is the Chrome DevTools Application tab, which displays a table of cookies. The table has columns for Name, Value, Domain, Path, Expires / Max..., Size, Http..., Secure, and SameSite. Three cookies are listed: csrf, identity-backend, and advanced-backend. The identity-backend cookie is highlighted. Below the table, there is a prompt: "Select a cookie to preview its value".

Name	Value	Domain	Path	Expires / Max...	Size	Http...	Secure	SameSite
csrf	959e686785c786866511bc63d61616d419e6d4...	10.88.234.104	/	Session	171	✓		
identity-backend	a622fe59522211e801927a65c3fd4e805cf5102e...	10.88.234.104	/	2020-02-06T...	222	✓		
advanced-backend	66j04a0arjhgon6sq8m1helsf9	10.88.234.104	/	Session	42	✓		

ANALOGY OF SESSION HIJACKING

Step2: Paste the cookie name and value along with the internal page in another system.



Step3: Refresh the internal page and it is successfully logged in.



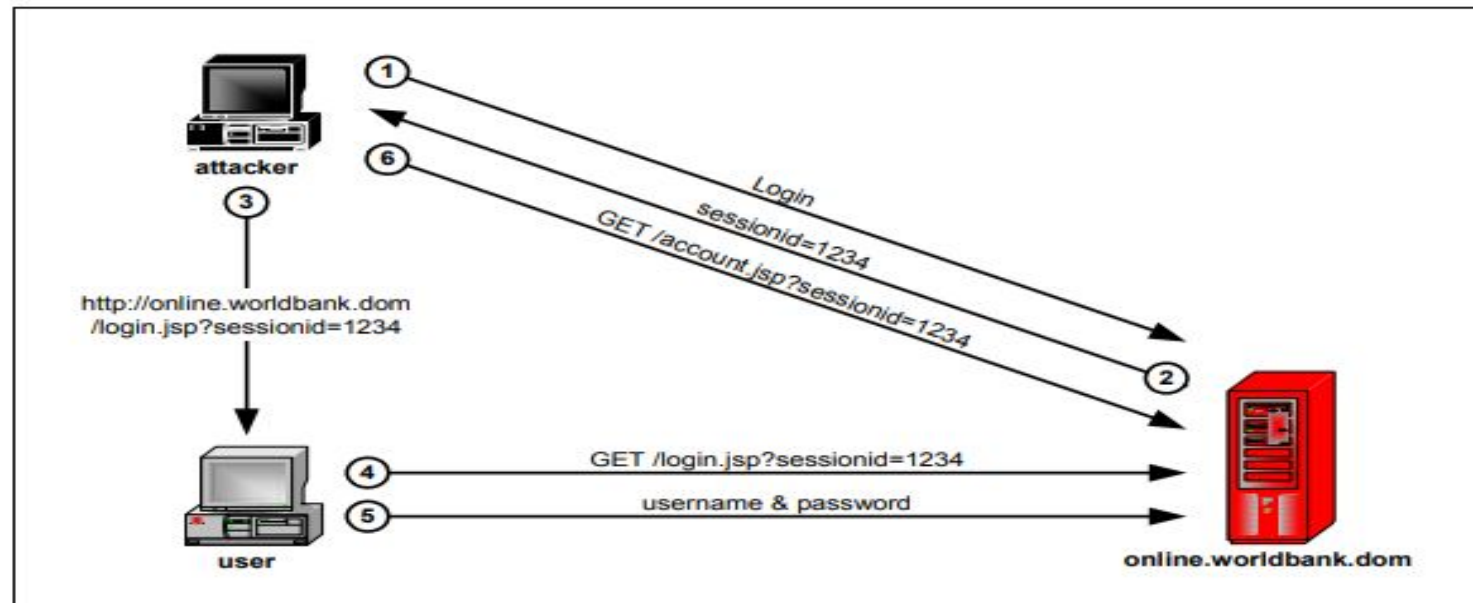


REMEDIATION OF SESSION HIJACKING

- Apply Secure and HttpOnly flags.
- Use of a long random number or string as the session key.
- Prevent guessing of valid session key through trial and error or brute force attacks.
- Use HTTPS to protect the session ID during transmission.

SESSION FIXATION

- Attacker tricks victim client into using session ID via some method, where method can be:
- Phishing email, containing web applications URL, where the session Id is usually used in URL
- Phishing email, where malicious script is injected and XSS forces client to use a specific session ID
- A hidden form field on a specially crafted login form page controlled by attacker



ANALOGY OF SESSION FIXATION

Cookie values before and after the login are same.

The top screenshot shows the Application tab in Chrome DevTools. The Cookies section is expanded, showing a table of cookies. The cookie named `_identity-backend` is highlighted, with its value `9614765fd7c3cf8263846cc0cd84b63829d0eb72f374ef4ba1be0a7e0cb74be9a%3A2%3A%7Bi%3A0%3Bs%3A17%3A%22_identity-backend%22%3B%3A1%3Bs%3A46%3A%22%5B1%2C%22U0cUMBYN0A2t26k_uq4S86cDyaeBzj%22%2C2592000%5D%22%3B%7D`.

Name	Value	Domain	Path	Expires / Max...	Size	Http...	Secure	SameSite
<code>_identity-backend</code>	<code>9614765fd7c3cf8263846cc0cd84b63829d0eb72f374ef4ba1be0a7e0cb74be9a%3A2%3A%7Bi%3A0%3Bs%3A17%3A%22_identity-backend%22%3B%3A1%3Bs%3A46%3A%22%5B1%2C%22U0cUMBYN0A2t26k_uq4S86cDyaeBzj%22%2C2592000%5D%22%3B%7D</code>	<code>10.88.234.104</code>	<code>/</code>	<code>2020-02-12T...</code>	<code>222</code>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
<code>advanced-backend</code>	<code>gebgu3vu0ud9B385b737z4nmgl</code>	<code>10.88.234.104</code>	<code>/</code>	<code>Session</code>	<code>42</code>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

The bottom screenshot shows the Cookie Editor tool over a browser window. The cookie `_identity-backend` is selected, and its value is displayed as `9614765fd7c3cf8263846cc0cd84b63829d0eb72f374ef4ba1be0a7e0cb74be9a%3A2%3A%7Bi%3A0%3Bs%3A17%3A%22_identity-backend%22%3B%3A1%3Bs%3A46%3A%22%5B1%2C%22U0cUMBYN0A2t26k_uq4S86cDyaeBzj%22%2C2592000%5D%22%3B%7D`. The browser window shows the Hartron website with a login button.

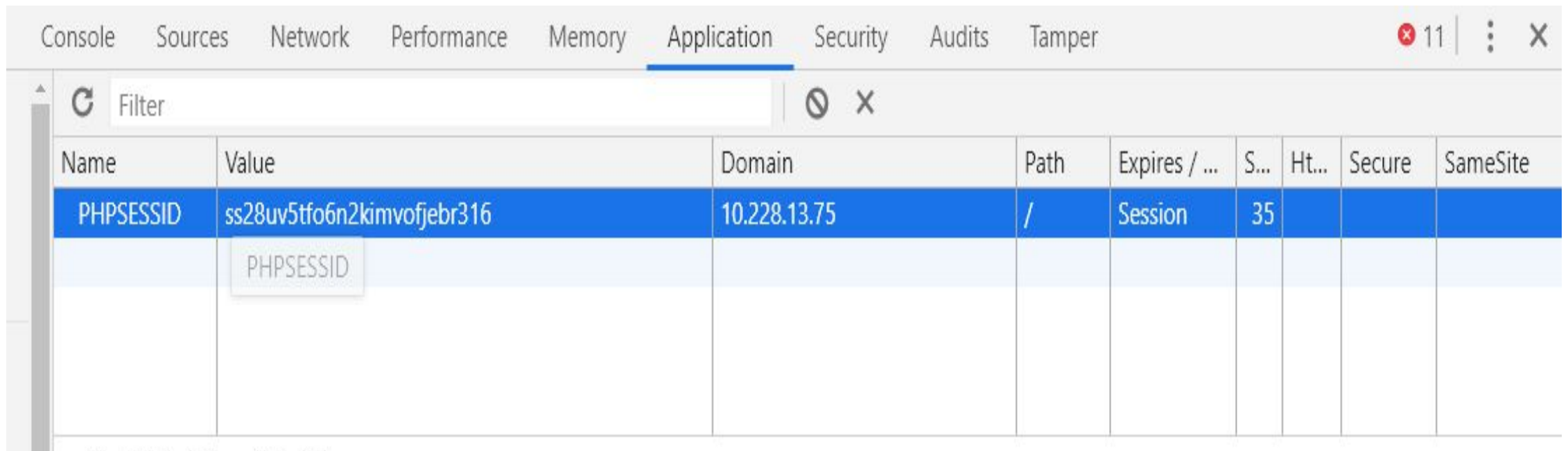
Name	Domain	Path	Expires	LastAccessed	Value	HttpOnly	SameSite
<code>_identity...</code>	<code>10.88.234.104</code>	<code>/admin/</code>	<code>Session</code>	<code>Mon, 13 Jan 2020 ...</code>	<code>9614765fd7c3cf8263846cc0cd84b63829d0eb72f374ef4ba1be0a7e0cb74be9a%3A2%3A%7Bi%3A0%3Bs%3A17%3A%22_identity-backend%22%3B%3A1%3Bs%3A46%3A%22%5B1%2C%22U0cUMBYN0A2t26k_uq4S86cDyaeBzj%22%2C2592000%5D%22%3B%7D</code>	<input type="checkbox"/>	<code>Unset</code>

REMEDIATION OF SESSION FIXATION

- Follow a secure session management life cycle which includes proper initialization, maintenance, authentication and termination of the session token.
- Application should generate different tokens for pre authentication and post authentication stages.
- To provide a unique, random and fresh session token.
- Consider regenerating a new session upon successful authentication or privilege level change.
- Use only the inbuilt session management mechanisms.
- Do not accept new, preset or invalid session identifiers either from the URL or from the request.

SESSION EXPIRATION

- Insufficient session expiration increases the exposure of other session-based attacks, as for the attacker to be able to reuse a valid session ID and hijack the associated session, it must still be active.
- Logout Button: Web applications must provide a visible and easily accessible logout (logoff, exit, or close session) button, so that the user can manually close the session at any time.



The screenshot shows the Chrome DevTools Application tab with the 'Application' pane open. The 'Cookies' section is selected, displaying a table of cookies. The first cookie is highlighted in blue. A tooltip is visible over the 'Value' cell of the first row.

Name	Value	Domain	Path	Expires / ...	S...	Ht...	Secure	SameSite
PHPSESSID	ss28uv5tfo6n2kimvofjebr316	10.228.13.75	/	Session	35			
	PHPSESSID							



AUTOMATIC SESSION EXPIRATION

- **Idle Timeout**

This timeout defines the amount of time a session will remain active in case there is no activity in the session, closing and invalidating the session upon the defined idle period for a given session ID.

- **Absolute Timeout**

This timeout defines the maximum amount of time a session can be active, closing and invalidating the session upon the defined absolute period since the given session was initially created by the web application

- **Renewal Timeout**

Alternatively, the web application can implement an additional renewal timeout after which the session ID is automatically renewed.

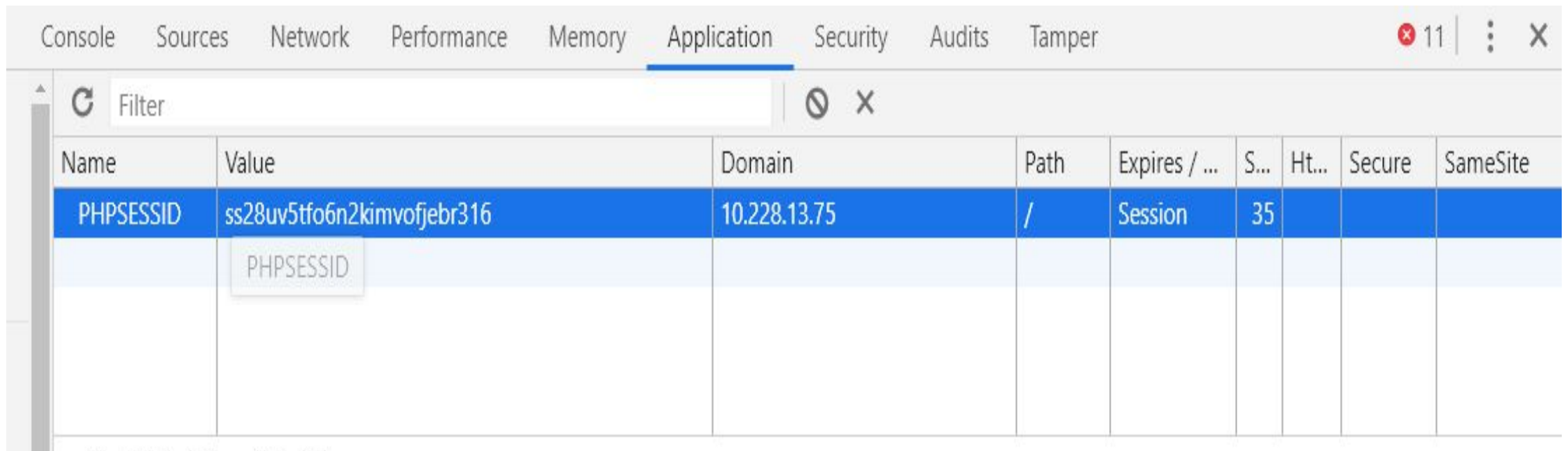


REMEDIATION OF SESSION EXPIRATION

- Implement automatic session expiration of 15 minutes.
- The session expiration timeout values must be set accordingly with the purpose and nature of the web application, and balance security and usability.
- It is mandatory for the web application to take active actions when the session expires, or the user actively logs out, by using the functions and methods offered by the session management mechanisms, such as `HttpSession.invalidate()` (J2EE), `Session.Abandon()` (ASP .NET) or `session_destroy()/unset()` (PHP).

SESSION EXPIRATION

- Insufficient session expiration increases the exposure of other session-based attacks, as for the attacker to be able to reuse a valid session ID and hijack the associated session, it must still be active.
- Logout Button: Web applications must provide a visible and easily accessible logout (logoff, exit, or close session) button, so that the user can manually close the session at any time.



The screenshot shows the Chrome DevTools Application tab with the 'Application' pane open. The 'Cookies' section is selected, displaying a table of cookies. The first row is highlighted in blue and contains the following data:

Name	Value	Domain	Path	Expires / ...	S...	Ht...	Secure	SameSite
PHPSESSID	ss28uv5tfo6n2kimvofjebr316	10.228.13.75	/	Session	35			

A tooltip is visible over the 'Value' cell of the first row, displaying the text 'PHPSESSID'.



AUTOMATIC SESSION EXPIRATION

- **Idle Timeout**

This timeout defines the amount of time a session will remain active in case there is no activity in the session, closing and invalidating the session upon the defined idle period for a given session ID.

- **Absolute Timeout**

This timeout defines the maximum amount of time a session can be active, closing and invalidating the session upon the defined absolute period since the given session was initially created by the web application

- **Renewal Timeout**

Alternatively, the web application can implement an additional renewal timeout after which the session ID is automatically renewed.



REMEDIATION OF SESSION EXPIRATION

- Implement automatic session expiration of 15 minutes.
- The session expiration timeout values must be set accordingly with the purpose and nature of the web application, and balance security and usability.
- It is mandatory for the web application to take active actions when the session expires, or the user actively logs out, by using the functions and methods offered by the session management mechanisms, such as `HttpSession.invalidate()` (J2EE), `Session.Abandon()` (ASP .NET) or `session_destroy()/unset()` (PHP).



URL & SAFE WEB BROWSING

Secure web browsing is a game of changing tactics. Just when you think you've made your computer as safe to use as possible, the landscape changes.

Always use HTTPS for banking transactions.

Builtwith.com, who.is, centralops.net

URL & SAFE WEB BROWSING

- Don't download free media.
- Don't store your payment information online.
- Don't over share personal information on social media accounts.
- Change passwords regularly.
- Keep your browser software up-to-date.
- Run Anti-Virus software.
- Scan downloaded files before executing.
- Watch out for phishing.
- Don't Reuse Passwords.
- Use HTTPS for banking transactions.
- Read Privacy Policies.
- Avoid Public or Free Wi-Fi.
- Disable Stored Passwords.

SECURING YOURSELF



1. Install OS/Software Updates



2. Run Anti-virus Software



3. Prevent Identity Theft



4. Turn on Personal Firewalls



5. Avoid Spyware/Adware



6. Protect Passwords



7. Back up Important Files

SECURING YOURSELF

- Awareness
 - What information you have
 - How important it is
 - How secure it is
- Assess
 - What could happen if lost or in the wrong hands
- Adequate
 - Precautions to protect it



SECURING YOURSELF

- Common Sense
- Awareness
- Regularly Update Patches
- Anti Virus, anti spyware...
- Be careful on P2P file sharing
- what you download
- Read the computer message(s)
- Don't blindly click next > next > next
- Be careful when you read email especially if it belongs to someone else
- Don't try to open every attachment
- Keep your password to yourself



THANK YOU

For any query, drop a mail at

[karanpreet\[at\]cdac\[dot\]in](mailto:karanpreet[at]cdac[dot]in)