TP01

Manipulation : Préparer les machines

1. Serveur PFSENSE

Vérification carte réseau:

| | PFSENSE - Paramètres | 8 |
|------------|---|---|
| 🧾 Général | Réseau | |
| Système | Adapter 1 Adapter 2 Adapter 3 Adapter 4 | |
| Affichage | Activer l'interface réseau | |
| Stockage | Mode d'accès réseau : NAT 🔹 | |
| 🕩 Son | <u>N</u> om : | ~ |
| 🗗 Réseau | Avancé | |
| an I | PFSENSE - Paramètres | 6 |
| 📃 Général | Réseau | |
| Système | Adapter <u>1</u> Adapter <u>2</u> Adapter <u>3</u> Adapter <u>4</u> | |
| Affichage | Activer l'interface réseau | |
| Stockage | Mode d'accès réseau : Réseau interne 🔹 | |
| 🕩 Son | Nom : lan-in | - |
| 📮 Réseau | ▶ A <u>v</u> ancé | |
| | PFSENSE - Paramètres | 8 |
| 🣃 Général | Réseau | |
| Système | Adapter 1 Adapter 2 Adapter 3 Adapter 4 | |
| Affichage | Activer l'interface réseau | |
| 😥 Stockage | Mode d'accès réseau : Réseau interne | |
| 🕩 Son | Nom : srv-in | * |
| 🕞 Réseau | ▶ A <u>v</u> ancé | |

Voici les cartes réseau dans le serveur pfsense. On peut voir que la carte em0 est bien configurée en NAT. La carte em1 est configurée en réseau interne lan-in et la carte em2 est elle aussi en interne srv-in.

| *** Welcome to | pfSense 2.4. | 4-RELEASE-p1 (amd64) on pfSense *** |
|----------------|--------------|-------------------------------------|
| WAN (wan) | -> em0 | -> |
| LAN_IN (lan) | -> em1 | -> v4: 192.168.50.254/24 |
| SRV_IN (opt1) | -> em2 | -> v4: 172.16.10.254/24 |

2. Serveur cible-mutillidae

Vérification carte réseau:

| | Serveur-cible- | mutillidae - Paramètres 🤤 |
|-----------|-----------------------------------|-----------------------------------|
| 📃 Général | Réseau | |
| Système | Adapter <u>1</u> Adapter <u>2</u> | Adapter <u>3</u> Adapter <u>4</u> |
| Affichage | ✓ Activer l'interface réseau | 1 |
| Stockage | Mode d'accès réseau : | Réseau interne 🔹 |
| 🕩 Son | <u>N</u> om : | srv-in |
| Réseau | ▶ A <u>v</u> ancé | |

Notre carte réseau a la bonne adresse IP. 172.16.10.5 Elle est donc bien dans le réseau srv-in.



3. Kali client

Vérification carte réseau:

| | Kali-2021 - Paramètres | 8 |
|-------------|---|---|
| 🣃 Général | Réseau | |
| Système | Adapter 1 Adapter 2 Adapter 3 Adapter 4 | |
| E Affichage | ✓ Activer l'interface réseau | |
| Stockage | Mode d'accès réseau : Réseau interne 🔹 | |
| 🕩 Son | <u>N</u> om : lan-in | • |
| 🗗 Réseau | Avancé | |

Clavier français:



Je n'ai pas la bonne adresse ip dans la machine kali, il faut donc ajouter une adresse ip et la configurer en manuel pour que la kali soit dans le réseau lan-in:



Pour ajouter un adresse ip en manuel kali:

Aller dans le menu Applications / Settings / NetworkConnections Puis cliquer sur le "+" pour éditer une nouvelle connexion.

| | Network Connections | _ = × |
|--------------------|---------------------|-------------|
| Name | | Last Used 🔫 |
| - Ethernet | | |
| Wired connection 1 | | 1 year ago |
| + - 🌣 | | |

Ethernet: Choisir son nom de connexion et choisir la bonne carte réseau.

| | | Editi | _ | | | |
|---------------|--------|------------------------|--------|-------|---------------|---------------|
| Connection na | me LA | N-IN | | | | |
| General | Ethern | et 802.1X Security | DCB | Proxy | IPv4 Settings | IPv6 Settings |
| | Dev | ice eth0 (08:00:27:CF: | 9B:43) | | | - |

IPV4 Settings: Mettre en manuel puis ajouter la bonne adresse ip et la bonne passerelle ainsi que le DNS.

| | | Editir | ng LAN-IN | | | | - 0 | × |
|-----------------|----------------|------------------|-----------|-----------|---------------|----|-------------|---|
| Connection name | LAN-IN | | | | | | | |
| General Eth | ernet 802 | 2.1X Security | DCB | Proxy | IPv4 Settings | IP | v6 Settings | |
| Method Manua | ıl | | | | | | • |] |
| Addresses | | | | | | | | |
| Address | | Netmask | | Gateway | | | Add | |
| 192.168.50.30 | | 24 | | 192.168.5 | 0.254 | | Delete | |
| | | | | | | | | |
| DNS servers | 192.168.50 |).254 | | | | | | |
| Search domains | 5 | | | | | | | |
| DHCP client ID | | | | | | | | |
| Require IPv4 | 4 addressing f | or this connecti | on to com | olete | | | | |
| | | | | | | | Routes |] |
| | | | | | Carro | | 15000 | |
| | | | | | Cance | et | ✓ Save | |

On peut donc apercevoir le réseau LAN-IN que je viens de créer.



Puis relancer la connexion:

```
(kali@kali)-[~]
$ sudo /etc/init.d/networking restart
Restarting networking (via systemctl): networking.service.
```

Et je vérifie l'adresse IP de ma carte réseau:

```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
group default qlen 1000
    link/ether 08:00:27:cf:9b:43 brd ff:ff:ff:ff:ff
    inet 192.168.50.30/24 brd 192.168.50.255 scope global noprefixroute eth0
    valid_lft forever preferred_lft forever
    inet6 fe80::ca3b:fdb1:c981:4a29/64 scope link noprefixroute
    valid_lft forever preferred_lft forever
```

Désormais toutes mes machines sont correctement configurées.

Ensuite la logique serait de se connecter directement sur le serveur mutillidae et de commencer le TP. Mais lorsque que l'on essaye, le navigateur nous affiche un message d'erreur du proxy qui nous dit qu'il a refusé la connexion au serveur.



Après cela on doit désactiver le proxy sur notre kali car :

Pour cela il suffit d'ouvrir son navigateur web pour ma part Mozilla, aller dans les paramètres "Général" puis dans "Network Settings" et cliquer sur "Settings...".

| \leftrightarrow \rightarrow G \textcircled{a} | లి Firefox | about:preferences#general | 습 | ۱۱۱۸ | | • |
|---|------------|--|---------------|-----------------|-----|---|
| | | Your browser is being managed by your organization. | ♀ Find in Pre | ferences | | |
| 🗱 Genera | | | | | | |
| ሰ Home | | Network Settings | | | | |
| Q Search | | Configure how Firefox connects to the internet. | Learn mor | S <u>e</u> ttin | ıgs | |

Puis cliquer sur "No proxy" afin de le désactiver:

| | Connection Settings | | | × |
|-----------------------|---|--------------|----|---|
| | | | | h |
| Configure Proxy | Access to the Internet | | | |
| 🔘 No proxy | | | | |
| Auto-detect p | roxy settings for this net <u>w</u> ork | | | |
| Use system pr | roxy settings | | | |
| <u>M</u> anual proxy | configuration | | | |
| HTTP Pro <u>x</u> y | | <u>P</u> ort | | |
| | Also use this proxy for FTP and HTTPS | | | |
| <u>H</u> TTPS Proxy | | | | |
| <u>F</u> TP Proxy | | | | |
| | | | | |
| SO <u>C</u> KS Host | | | | |
| (| SOC <u>K</u> S v4 ● SOCKS <u>v</u> 5 | | | |
| <u>A</u> utomatic pro | bxy configuration URL | | | |
| | | | | |
| <u>N</u> o proxy for | | | | |
| | | | | |
| | | | | |
| Example: .mozilla. | .org, .net.nz, 192.168.1.0/24 | | | |
| <u>H</u> elp | Canci | el | ОК | |
| | | | | |

Réessayer de se connecter au serveur mutillidae depuis son navigateur web avec le proxy désactivé:

| $\boldsymbol{\leftarrow} ightarrow$ $\boldsymbol{\Box}$ | 0 ① 172.16.10.5/mutillidae/ | ເ ☆ | II\ ⊡ II ≡ |
|--|--|---------------------------|--|
| • | OWASP Mutillidae II: Kee | p Calm an | d Pwn O |
| Version: | 2.6.67 Security Level: 0 (Hosed) Hints: En | abled (1 - Try easier | r) Not Logged |
| Home Login/Re | gister Toggle Hints Show Popup Hints Toggle Security E | nforce SSL Reset DB V | iew Log View Captı |
| OWASP 2017 | |] | |
| OWASP 2013 | Hints and Videos | | |
| OWASP 2010 | | TIP | : Click Hint and on each p |
| OWASP 2007 | | Ver | |
| Web Services | What Should I Do? | Video Tuto | rials |

Cela fonctionne correctement, notre contexte est alors bien configuré.

TP02 APPRENTISSAGE 1 : énumération des logins

Installation de l'extension Wsdler

| Wetcome to Burp Satte Community Edition. Use the options below to create or open a project. Image: Disclose of project are only supported on Burp Sulte Professional. Image: Disclose of project are only supported on Burp Sulte Professional. Image: Disclose of project are only supported on Burp Sulte Professional. Image: Disclose of project are only supported on Burp Sulte Professional. Image: Disclose of project are only supported on Burp Sulte Professional. Image: Disclose of project are only supported on Burp Sulte Professional. Image: Disclose on Burp Sulte Community Edition V20212.1 Image: Disclose on Burp Sulte Community Edition V20212.1 Image: Disclose on Burp Sulte Community Edition V2021.2.1 | | Burp Suite Community E | dition v2021.2.1 | _ C |
|--|--|---|--------------------------|--|
| New project on disk. Name: Price: Open existing project Open existing project Price: Pr | Welcome to Burp Suite Community Edition | n. Use the options below to create or o | pen a project. | 🛂 Burp Suit |
| Temporary project New project on disk Name: File: Choose file Open existing project Name File File: | Note: Disk-based projects are only suppor | ed on Burp Suite Professional. | | Community Editi |
| New project on disk Name: File: Choose file File: Pause Automated Tasks Cancel New Use "Burp defaults" et "StartBurp": Burp Suite Community Edition v2021.2.1 Select the configuration that you would like to load for this project. Use options saved with project Use options saved with project It use options saved with project End from configuration file File: Default to the above in future Disable extensions | Temporary project | | | |
| Choose File Open existing project Name File: Choose File File: Pause Automated Tasks Cancel New Uses "Burp defaults" et "StartBurp": Select the configuration that you would like to load for this project. Image: Subscript defaults Use options saved with project Image: Use options saved with project Image: Subscript defaults Image: Subscri | New project on disk Name | | | |
| Open existing project Name File File: File: Choose File Cance Next Uses "Burp defaults" et "StartBurp": Burp Suite Community Edition v2021.2.1 Select the configuration that you would like to load for this project. Select the configuration that you would like to load for this project. Select the configuration file Use options saved with project I use Burp defaults I use options saved with project File: Cload from configuration file File: Cload from configuration file File: Choose file | File: | | | Choose file |
| Orparitation grapher Ine | Open existing project | | - | -1. |
| File: Choose File Pause Automated Tasks Cancel Cancel New Uses "Burp defaults" et "StartBurp": Select the configuration that you would like to load for this project. Image: Select the configuration that you would like to load for this project. Image: Use Burp defaults Image: Use Burp defaults <td>Openezisting project</td> <td>Name</td> <td>F</td> <td>ile</td> | Openezisting project | Name | F | ile |
| File: Choose file Pause Automated Tasks Cancel Use "Burp defaults" et "StartBurp": Burp Suite Community Edition v2021.2.1 Select the configuration that you would like to load for this project. Image: Start Burp defaults Use Burp defaults Image: Start Burp defaults Image: Start Burp Suite Community Edition v2021.2.1 Image: Start Burp Suite Community Edition v2021.2.1 <td></td> <td></td> <td></td> <td></td> | | | | |
| File: Choose file ✓ Pause Automated Tasks Cancel Cancel Meet Uses "Burp defaults" et "StartBurp": | | | | |
| | | | | |
| Load from configuration file File File Choose file Ch | File: | use Automated Tasks | | Choose file. |
| Lead from configuration file Default to the above in future Disable extensions | | | | |
| Use "Burp defaults" et "StartBurp": Burp SuiteCommunityEdition v2021.2.1 - Select the configuration that you would like to load for this project. Select the configuration that you would like to load for this project. Use Burp defaults Use options saved with project Load from configuration file File File File Default to the above in future Disable extensions | | | | Cancel Next |
| Burp Suite Community Edition v2021.2.1 Select the configuration that you would like to load for this project. Image: Suite Community Edition v2021.2.1 Select the configuration that you would like to load for this project. Image: Suite Community Edition v2021.2.1 Select the configuration that you would like to load for this project. Image: Suite Community Edition v2021.2.1 Select the configuration that you would like to load for this project. Image: Suite Community Edition v2021.2.1 Community Edition v2021.2.1 Image: Suite Community Edition v2021.2.1 Community Edition v2021.2.1 Community Edition v2021.2.1 Image: Suite Community Edition v2021.2.1 Community Edition v2021.2.1 Image: Suite Community Edition v2021. | | | | |
| Select the configuration that you would like to load for this project. | Use "Burb defaults" et | "StartBurp": | | |
| Community Ed Comm | Use "Burp defaults" et | "StartBurp": Burp Suite Community E | dition v2021.2.1 | _ 1 |
| Use Burp defaults Use options saved with project Load from configuration file File File File Default to the above in future Disable extensions | Use "Burp defaults" et | "StartBurp": Burp Suite Community E | dition v2021.2.1 | – I A Duro Suit |
| Use options saved with project Load from configuration file File File File Choose file Default to the above in future Disable extensions | Use "Burp defaults" et | "StartBurp": Burp Suite Community E e to load for this project. | dition v2021.2.1 | Burp Sui |
| Load from configuration file File File File File: Choose file Default to the above in future Choose file | Select the configuration that you would lik | "StartBurp": Burp Suite Community E e to load for this project. | dition v2021.2.1 | Burp Sui Community Edit |
| Load from configuration file File File Choose file Default to the above in future Choose file | Select the configuration that you would lik Use Burp defaults Use options saved with project | "StartBurp": Burp Suite Community E e to load for this project. | dition v2021.2.1 | Burp Sui Community Edit |
| File: Choose file Default to the above in future Disable extensions | Select the configuration that you would lik Use Burp defaults Use options saved with project | "StartBurp": Burp Suite Community E e to load for this project. | dition v2021.2.1 | - Community Edit |
| File: Choose file Default to the above in future Disable extensions | Use "Burp defaults" et Select the configuration that you would lik Use Burp defaults Use options saved with project | "StartBurp": Burp Suite Community E e to load for this project. | dition v2021.2.1 File | S Burp Sui Community Edit |
| File: Choose file Default to the above in future Disable extensions | Use "Burp defaults" et Select the configuration that you would lik Ouse Burp defaults Use options saved with project Load from configuration file | "StartBurp": Burp Suite Community E e to load for this project. | dition v2021.2.1 | S Burp Suit Community Edit |
| File: Choose file Default to the above in future Disable extensions | Use "Burp defaults" et Select the configuration that you would lik Ouse Burp defaults Use options saved with project | "StartBurp": Burp Suite Community E e to load for this project. | dition v2021.2.1 File | - T Burp Suit Community Edit |
| Default to the above in future Disable extensions | Use "Burp defaults" et Select the configuration that you would lik Ouse Burp defaults Use options saved with project Load from configuration file | "StartBurp": Burp Suite Community E e to load for this project. | dition v2021.2.1 | - Community Edit |
| Default to the above in future Disable extensions | Use "Burp defaults" et Select the configuration that you would lik Ouse Burp defaults Use options saved with project Load from configuration file | "StartBurp": Burp Suite Community E e to load for this project. | dition v2021.2.1 File | - The second sec |
| Disable extensions | Select the configuration that you would lik Use Burp defaults Use options saved with project Load from configuration file File: | "StartBurp": Burp Suite Community E e to load for this project. | dition v2021.2.1 | - The second sec |
| | Use "Burp defaults" et Select the configuration that you would lik Use Burp defaults Use options saved with project Load from configuration file File: | "StartBurp": Burp Suite Community E e to load for this project. | dition v2021.2.1 | - r Description: Community Edit |
| | Select the configuration that you would lik Use Burp defaults Use options saved with project Use options file File: Default to the above in future Disable extensions | "StartBurp": Burp Suite Community E e to load for this project. | dition v2021.2.1 | - The second sec |

Et donc voici la page d'accueil de BurpSuite:

| 5 | | | | Burp Suite (| Community Edition v2 | 2021.2.1 - Temp | orary Project | | _ 0 X |
|-------------------|---------------|-----------------|--------|-------------------|----------------------|--|----------------------------------|---|-----------------|
| Burp Project | Intruder | Repeater | Window | Help | | | | | |
| Repeater | 5 | Sequencer | | Decoder | Comparer | Extender | Project options | User options | Wsdler |
| | Dashb | oard | | | Target | | Proxy | Intruder | |
| Tasks | | 🕀 News | can 💽 | New live task | (II) (D) (e' × * | Time to le | evel up? Catch more bugs with Bu | rrp Suite Pro Find out mo | re X |
| √ Filter Runn | ing Paus | ed Finish | ed | | | Issue activi | ty [Pro version only] | | ? 🖉 |
| 1. Live passive c | rawl from P | roxy (all traff | ic) | | 0 🔅 🗹 | \overline \overli \overline \overline \overline \overline \overline \overline \o | gh Medium Low Info | Certain Firm Te | entative |
| Add links. Add it | em itself, sa | me domain | and UR | 0 items added to | site map | | Issue type | Host | |
| Capturing: | | | | 0 responses proce | essed | Suspicious i | nput transformation (reflected) | http://insecure-bai | nk.com /url-sh |
| Capturing. | | | | 0 responses queu | ied. | SMTP head | erinjection | http://insecure-we | bsite.c /contac |
| L | | | | o responses que | | Serialized o | bject in HTTP message | http://insecure-bai | nk.com /blog |
| | | | | | | Cross-sites ML extern | al entity injection | https://vulnerable- | websit /produc |
| | | | | | | External ser | vice interaction (HTTP) | https://insecure-w | ebsite /produc |
| | | | | | | 9 Web cache | poisoning | http://insecure-bai | nk.com /contac |
| | | | | | | Server-side | template injection | http://insecure-bai | nk.com /user-h |
| | | | | | | OS commar | nd injection | https://unerable- https://insecure-w | ebsite /feedba |

Pour installer l'extension "Wsdler" il faut alors changer son réseau pour avoir Internet.

Puis créer un connexion NAT sur notre VM Kali afin de se connecter directement au réseau du lycée et avoir accès à Internet, nous allons donc sortir de notre contexte.

Pour créer notre connexion NAT aller dans les mêmes paramètres que lorsque l'on a créé le réseau LAN-IN. Mais il suffit de modifier IPV4 en Automatic. On va donc directement demander une adresse au serveur DHCP de notre réseau.

| | | | | Edit | ing NAT | | | - | | × |
|-----|------------|--------|-------------|-----------------------|------------|--------|---------------|------------|-----|---|
| Con | nection na | ame | NAT | | | | | | | |
| (| General | Etł | nernet | 802.1X Security | DCB | Proxy | IPv4 Settings | IPv6 Setti | ngs | |
| м | ethod 🛛 | Autom | natic (DHC | IP) | | | | | • | |
| A | dditionals | static | addresse | 5 | | | | | | |
| | Address | | | Netmask | | Gatewa | ау | Ado | I | |
| | | | | | | | | Dele | te | |
| | | | | | | | | | | |
| | Additia | nal D | NS corve | re | | | | | | |
| | Additio | | NJ SCIVE | | | | | | | |
| | Additiona | l sear | ch domair | าร | | | | | | |
| | | DH | CP client I | D | | | | | | |
| | Requi | re IPv | 4 address | ing for this connecti | on to comp | lete | | | | |
| | | | | | | | | Route | s | |
| | | | | | | | Cance | el 🗸 S | ave | |

Modifier aussi les paramètre de la VM en NAT

| | Kali-2021 - Paramètres | 8 |
|-----------|---|---|
| 🣃 Général | Réseau | |
| Système | Adapter 1 Adapter 2 Adapter 3 Adapter 4 | |
| Affichage | Activer l'interface réseau | |
| Stockage | Mode d'accès réseau : NAT 🔹 | |
| 🕩 Son | <u>N</u> om : | v |
| Réseau | Avancé | |

Puis sur Burp Suite aller dans "Extender", puis dans "BApp Store":

| Repeater | Sequencer | | Decoder | Comparer | Extender | |
|------------|------------|------|---------|----------|----------|--|
| Extensions | BApp Store | APIs | Options | | | |

Puis rechercher l'extension "Wsdler":

Elle est déjà installée mais par précaution je la réinstalle afin de la mettre à jour s' il y a des mises à jour.

BApp Store

| The BApp Store contains Burp extensions that have been written by users of Burp Suite, to extend Burp's capabilities. | | | | | | | |
|---|-----------|--------|------------|--------------|--------|---------|--|
| Name | Installed | Rating | Popularity | Last updated | Detail | Wedler | |
| Wsdler | 1 | **** | | 01 Nov 2016 | | vvsdter | |

Je clique donc sur "reinstall":

Wsdler

This extension takes a WSDL request, parses out t operations that are associated with the targeted v service, and generates SOAP requests that can the sent to the SOAP endpoints.

To use this extension, select a suitable item in Bu choose "Parse WSDL" from the context menu.

The extension builds upon the work done by Tom and his soap-ws project which is essentially the V parsing portion of Soap-UI without the UI.

Requires Java version 8

| Author: | Eric Gruber | | | | | | |
|-------------|------------------------------------|--|--|--|--|--|--|
| Version: | 2.0.12 | | | | | | |
| Source: | https://github.com/portswigger/wse | | | | | | |
| Updated: | 01 Nov 2016 | | | | | | |
| Rating: | <mark>አአአ</mark> አር Submit ra | | | | | | |
| Popularity: | | | | | | | |
| Reinstall | | | | | | | |

On vérifie qu'elle soit bien installée:

| Extensions | BApp Store | APIs | Options | | | | | | |
|--|--|------|---------|------|--|--|--|--|--|
| Burp Extensions | | | | | | | | | |
| Extensions let you customize Burp's behavior using your own or third-party code. | | | | | | | | | |
| | | | | | | | | | |
| Add | Loaded | Туре | | Name | | | | | |
| Remove | Image: A start of the start | Java | Wsdler | | | | | | |
| | | | | | | | | | |

Puis remodifier la connexion en LAN-IN.

Test d'une requête et d'une réponse sur un login inexistant

Toujours sur BurpSuite aller dans l'onglet proxy. Puis cliquer sur "Intercept is On" pour le mettre en Off.

| Dashboard Target | | Proxy | Intruder | Repeat |
|------------------------|--|-------|-----------------|--------|
| Intercept HTTP history | | y Web | Sockets history | Ор |
| | | | - | |
| Forward | | Drop | Intercept is a | off |
| | | | | |

Puis accéder à l'application Mutillidae en cliquant sur Open Browser.

| Proxy | Intruder | Repeater | Sequencer | Decoder | Con |
|-------|------------------|----------|-----------|--------------|--------------|
| / We | bSockets history | Options | | | |
| | | | | | |
|)rop | Intercept is | off | Action | Open Browser | $\mathbf{)}$ |

Puis aller dans OWASP 2017 > A2 > Username Enumeration > Lookup User

| | | ow/ | ASP Mutillidae II: |
|--------------|---------------------------------|----------------------------|---|
| | | Version: 2.6.67 | Security Level: 0 (Hosed) |
| | | Home Login/Register To | oggle Hints Show Popup Hints Toggle S |
| OWASP 2017 | A1 - Injection (SQL) | • | |
| OWASP 2013 | A1 - Injection (Other) | s and Videos | J |
| OWASP 2010 | A2 - Broken Authentication and | Authentication Bypass | TIP: Click Hint and Vide |
| OWASD 2007 | A2 Consitive Data Erroceuro | Priviliege Escalation | on each page |
| OWASP 2007 | | Username Enumeration | Login |
| Web Services | A4 - XML External Entities | | Lookup User (SOAP Web Service) |
| HTML 5 | A5 - Broken Access Control | • | User Account Management (REST |
| | A6 - Security Misconfiguration | • | Web Service) |
| Others | A7 - Cross Site Scripting (XSS) | N 📔 . | isting of vulnerabilities |

Ensuite remettre le proxy de BurpSuite en intercept on

| | Dashboard | Target | Proxy | Intruder | Repea |
|-----|--|-----------------------------------|--------------------------|-----------------|-------|
| | Intercept | HTTP histor | y Web | Sockets history | Ot |
| | Forward | | Drop | Intercept is | on |
| Cli | quer sur V | VSDL | | | |
| J |) NuSOA | P: ws-user-a | accoun × | + | |
| • | $\leftrightarrow \rightarrow \times$ | 🔺 Nots | ecure 17 | 2.16.1 | |
| v | S-USCI- View the <u>WS</u> on a operat details. | - ACCOUI | nt ce. Click wit's | | |
| | | <u>getUser</u> | | | |
| | 1 | <u>createUser</u> | | | |
| | | <u>updateUser</u> deletel iser | | | |
| | | ucicicosci | | | |

On est directement renvoyé sur le Burp dans l'onglet Raw.

| Burp P | Project | Intruder | Repeater | Window | Help | | | | |
|----------|------------|------------------------|----------------------|-------------|------------------|----------|---------------------------|------------------|--------------------|
| Dashbo | ard | Target | Proxy | Intruder | Rep | eater | Sequencer | Decoder | Compare |
| Intercep | pt | HTTP histor | ry Web | Sockets his | tory | Options | | | |
| 🖉 Requ | iest to ht | ttp://172.16. | 10.5:80 | | | | | | |
| For | ward | | Drop | Interce | pt is on | A | Action | Open Browser | |
| Pretty | Raw | \n Actio | ons 🗸 | | | | | | |
| 1 GET . | /mutil | llidae/we | bservice | s/soap/w | s-user- | account | .php? <mark>wsdl</mark> H | TTP/1.1 | |
| 2 Host | : 172 | .16.10.5 | | | | | | | |
| 3 Upgr | ade-Ir | nsecure-P | Requests: | 1 | | | | - Likita (Forda) | oc / ki mu |
| 4 User | - Agent | t: Mozill | a/5.0 (W | indows N | 10.0; .vml = | Win64; | x64) Apple | NebKit/53/.: | 36 (KHIMI |
| 6 Defe | rer k | -xt/ntmt, -++n·//17 | appiicai 72 16 10 | 5/mutill | idae/we | servic | es/soap/ws-i | .9,Image/av. | ti, image. Enbo |
| 7 Accel | nt - End | odina: a | zin. def | late | ruuc/wc | /SCI VIC | C3/300p/w34 | aser account | c . prip |
| 8 Acce | pt - Lar | nguage: e | n-US, en; | q=0.9 | | | | | |
| 9 Cook | ie: sł | nowhints= | 1; PHPSE | SSID=mml | gam16qn | 2uvllr | vqd8ng2a7 | | |
| 10 Conn | ection | n: close | | | | | | | |
| 11 | | | | | | | | | |
| 12 | | | | | | | | | |

Puis faire un clique droit dans l'onglet "Raw" et cliquer sur Parse WSDL:

Matthias Hautin

| Intercept is on Action Open Br | owser | |
|---|---------------------------------------|--------|
| | | |
| <pre>soap/ws-user-account.php?wsdl HTTP/1.3</pre> | Scan | |
| dows NT 10.0; Win64; x64) AppleWebKit, | Send to Intruder Ctrl-I | ne/88. |
| <pre>n/xhtml+xml, application/xml; q=0.9, ima</pre> | Send to Repeater Ctrl-R | ≮;q=0. |
| te | Send to Sequencer | |
| 0.9 ID=mmlgaml6gpp2uvllrvgd8pg2a7 | Send to Comparer | |
| 10-mmigumioqnp2dvittrvqdong2dv | Send to Decoder | |
| | Request in browser > | |
| | Parse WSDL | |
| | Engagement tools [Pro version only] > | |

Aller dans l'onglet Wsdler, je vérifie que j'ai bien getUser:

| | Burp Project | Intruder | Repeater | Window H | Help | | | | | | | | |
|---|----------------|----------|----------|----------|-----------|-----------|---------|----------|----------|---------------------|--------------|--------|-----|
| | Dashboard | Target | Proxy | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User options | Wsdler | |
| < | ws-user-accoun | it 🗙 | | | | | | | | | | | |
| | | | | | Operation | | | | | | | | Bin |
| | getUser | | | | | | | | WS- | user-accountBinding | | | |
| | createUser | | | | | | | | WS- | user-accountBinding | | | |
| | updateUser | | | | | | | | WS- | user-accountBinding | | | |
| | deleteUser | | | | | | | | WS- | user-accountBinding | | | |
| | | | | | | | | | | | | | |

Puis on peut voir la requête de getUser. Dans la balise username on peut apercevoir "gero et". En effet ce compte est en réalité un login qui n'existe pas dans la liste des logins valides des comptes déjà existants.

```
Request
 Pretty Raw \n Actions ∨
 1 POST /mutillidae/webservices/soap/ws-user-account.php HTTP/1.1
 2 Upgrade-Insecure-Requests: 1
 3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/5:
 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image,
 5 Referer: http://172.16.10.5/mutillidae/webservices/soap/ws-user-acc
 6 Accept-Encoding: gzip, deflate
 7 Accept-Language: en-US, en; q=0.9
 8 Cookie: showhints=1; PHPSESSID=t5clgqf86touojfi78dah81s4r
9 Connection: close
10 SOAPAction: urn:ws-user-account#getUser
11 Content-Type: text/xml;charset=UTF-8
12 Host: 172.16.10.5
13 Content-Length: 452
14
15 <soapenv:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instar</pre>
     <soapenv:Header/>
16
17
      <soapenv:Body>
         <urn:getUser soapenv:encodingStyle="http://schemas.xmlsoap.org</pre>
18
19
            <username xsi:type="xsd:string">gero et</username>
20
         </urn:getUser>
21
      </soapenv:Body>
22 </soapenv:Envelope>
```

Puis faire un clique droit ou "ctrl+R" sur la fenêtre et aller dans "Send to Repeater":

| | Scan | |] |
|----------------|-------------------|--------|-------|
| | Send to Intruder | Ctrl-I |] |
|)1/XMLSchema-i | Send to Repeater | Ctrl-R | 3.org |
| | Send to Sequencer | | |
| nemas.xmlsoap. | Send to Comparer | | |

Cette étape permet d'envoyer la requête dans l'onglet Repeater, cet onglet nous permet de modifier ou forger notre requête puis de la tester autant de fois que l'on souhaite avant de l'envoyer au serveur mutillidae.

Voici donc la requête:



Dans cet onglet il y a 2 parties:

- Request qui permet de voir et modifier notre requête
- **Response** qui permet de voir le flux traité après avoir envoyé la requête

On va donc envoyer la requête au serveur en cliquant sur "send":

```
Response
Pretty Raw Render \n Actions 🗸
 1 HTTP/1.1 200 OK
  Date: Sun, 27 Nov 2022 20:52:37 GMT
 3 Server: Apache/2.4.29 (Ubuntu)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
  Cache-Control: no-store, no-cache, must-revalidate
 5
 6 Pragma: no-cache
7 X-SOAP-Server: NuSOAP/0.9.5 (1.123)
 8 Vary: Accept-Encoding
 9 Content-Length: 559
10 Connection: close
11 Content-Type: text/xml; charset=ISO-8859-1
12
13 <?xml version="1.0" encoding="ISO-8859-1"?>
     <SOAP-ENV:Envelope SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
       <SOAP-ENV: Body>
         <nsl:getUserResponse xmlns:nsl="urn:ws-user-account">
           <return xsi:type="xsd:xml">
              <accounts message="User gero et does not exist}" />
            </return>
          </nsl:getUserResponse>
       </SOAP-ENV: Body>
     </SOAP-ENV:Envelope>
```

Le serveur nous dit qu'il n'existe pas d'user gero.

On peut aussi stocker la requête afin de la comparer à une autre en faisant un clique droit > Send to Comparer sur l'onglet de la réponse.

| e | ιc | 0.0 |)e | ≥ |
|---|----|-----|----|---|
| - | | | _ | |

| 1 |
|-------------------|
| Send to Sequencer |
| Send to Comparer |
| C |

Pour retrouver notre requête il suffit d'aller dans l'onglet "Comparer", notre première requête y est stockée.

| Dashboard | Target | Proxy | Intruder | Repeater | Sequencer | Decoder | Comparer | E |
|-------------------|---------------|---------------|---------------|-----------------|--------------------|--------------------|--------------------|------|
| Comparer | | | | | | | | |
| This function let | s you do a wo | rd- or byte-l | evel comparis | on between diff | erent data. You ca | in load, paste, oi | r send data here i | from |
| Select item 1: | | | | | | | | |
| | | | # | | | | | |
| 1 | | | | | | | 901 | |

A1.Q1 :

Commande a exécuter depuis l'onglet Proxy jusqu'à l'onglet Comparer. Aller dans

- BurpsSuite > Proxy/Intercept off >
 - Open Browser > 172.16.10.5/mutillidae > OWASP 2017/A2/Username Enumeration/Lookup User >
- BurpsSuite > Proxy/Intercept on >
 - Revenir sur le lien Lookup User et cliquer sur "WSDL" >
- BurpsSuite > Proxy/Intercept/clique droit/Parse WSDL > Wsdler/GetUser > clique droit/Send to Repeater > Repeater >
 - on peut modifier la requête si on le souhaite dans /Request
 - pour stocker le requête /clique droit /Send to Comparer
 - pour l'envoyer /Send on a la réponse dans /Response
- BurpsSuite > Comparer
 - pour comparer 2 requetes faire /Words

Test d'une requête et d'une réponse sur un login existant

Nous devons tout d'abord créer 2 utilisateurs avec des mdp sur mutillidae. Pour créer un utilisateur mutillidae:

| Please sign-in |
|--|
| Username |
| Password |
| Login |
| Dont have an account? Please register here |

Je créer donc 2 comptes :

1er

- username : utilisateur1
- Password : utilisateur1

2eme

- username : utilisateur2
- Password : utilisateur2

| Please choose your username, password and signature | | | | | | |
|---|-------------------------------|--------------------|--|--|--|--|
| | | | | | | |
| Username | utilisateur1 | | | | | |
| Password | ••••• | Password Generator | | | | |
| Confirm Password | ••••• | | | | | |
| | Created by Matthias <u>Ha</u> | utin | | | | |
| Signature | | 4 | | | | |
| | | | | | | |
| | | | | | | |

Create Account

Je fais donc la même chose pour le deuxième compte pour le créer.

On va donc tester comme dans l'étape précédente mais cette fois-ci avec l'un des logins que l'on vient de créer par exemple utilisateur1.

Je refais donc toute la manipulation.

Lorsque on arrive dans l'étape de Repeater on doit donc modifier la requête et mettre le user "utilisateur1" que l'on vient de créer à la place de "gero et".

Voici la modification:



Voici la Réponse:

| R | esponse | | | | | | | | |
|----|---|--|--|--|--|--|--|--|--|
| P | retty Raw Render \n Actions 🗸 | | | | | | | | |
| 1 | HTTP/1.1 200 OK | | | | | | | | |
| 2 | 2 Date: Sun, 27 Nov 2022 23:12:08 GMT | | | | | | | | |
| З | Server: Apache/2.4.29 (Ubuntu) | | | | | | | | |
| 4 | Expires: Thu, 19 Nov 1981 08:52:00 GMT | | | | | | | | |
| 5 | Cache-Control: no-store, no-cache, must-revalidate | | | | | | | | |
| 6 | Pragma: no-cache | | | | | | | | |
| 2 | X-SOAP-Server: NuSOAP/0.9.5 (1.123) | | | | | | | | |
| 8 | Vary: Accept-Encoding | | | | | | | | |
| 10 | Connection: close | | | | | | | | |
| 11 | Content-Type: text/xml: charset=ISO-8859-1 | | | | | | | | |
| 12 | boncene Typer text, xmc, endiset-100 0000 1 | | | | | | | | |
| LЗ | xml version="1.0" encoding="ISO-8859-1"? | | | | | | | | |
| | <soap-env:envelope soap-env:encodingstyle="http://schemas.x</th></tr><tr><th></th><th><SOAP-ENV: Body></th></tr><tr><th></th><th><nsl:getUserResponse xmlns:nsl=" urn:ws-user-account"=""></soap-env:envelope> | | | | | | | | |
| | <return xsi:type="xsd:xml"></return> | | | | | | | | |
| | <accounts message="Results for utilisateurl"></accounts> | | | | | | | | |
| | <account></account> | | | | | | | | |
| | <username></username> | | | | | | | | |
| | utilisateuri | | | | | | | | |
| | | | | | | | | | |
| | Created by Matthias Hautin | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

Burp trouve donc bien l'utilisateur1 et on a même la signature.

Envoyer la requête dans le Comparer: clique droit/ Send to Comparer Aller dans "Comparer" et eliquer our "Worde":

Aller dans "Comparer" et cliquer sur "Words":

Ceci va donc comparer notre ancienne requête avec "gero" et notre nouvelle requête avec "utilisateur1" et on va donc voir les différence comme par exemple l'heure d'envoi de notre requête au serveur ou encore la réponse:

| # | Length 🔿 | Data | | | | | |
|---|--|--|--|--|--|--|--|
| | 901 | HTTP/1.1 200 OKDate: Sun, 27 Nov 2022 20:52:37 GMTServer: Apache/2.4.29 (Ubuntu)Expires: Thu, 19 Nov 1981 08:52:00 (| | | | | |
| | 1008 | HTTP/1.1 200 OKDate: Sun, 27 Nov 2022 23:12:08 GMTServer: Apache/2.4.29 (Ubuntu)Expires: Thu, 19 Nov 1981 08:52:00 (| | | | | |
| 5 | Word compare of #1 and #3 (11 differences | a) × | | | | | |
| Length: 901 | • Text | Text O Hex | | | | | |
| http://LUOUS Date:Sun, 27Nov 2022 20 52 35 GMT Server: Apache/2.4.29 Ubuntu) Expres: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache X-SOAP-Server: NuSOAP/0.9.5 (1.123) Vary Accept-Encoding Content-Length: 555 Content-Length: 555 Content-Lippe: text/ml; charset=ISO-8859-1 xml version="1.0" encoding="ISO-8859-1"? <soap-env:en< th=""><th>nvelope SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encodi</th><th>AV 2022 29: 20 GMT 24.23 (Ubuntu) Nov 1981 06: 52.00 GMT no-store, no-cache, must-revalidate http://docs.com/ NuSOAPI0.9.5 (L123) koding Kodin</th></soap-env:en<> | nvelope SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encodi | AV 2022 29: 20 GMT 24.23 (Ubuntu) Nov 1981 06: 52.00 GMT no-store, no-cache, must-revalidate http://docs.com/ NuSOAPI0.9.5 (L123) koding Kodin | | | | | |
| | | | | | | | |
| Key: Modified Deleted Added | Modified Deleted Added | | | | | | |

Réponse première requête gero:

| Length: 901 O Text | |
|--|-------------------------|
| | lex |
| :return xsi:type="xsd:xml"> <accounts message="<mark>User gero et does not exist}"></accounts> </mark return> </td <td>50A</td> | 50A |
| Key: Modified Deleted Added | |
| Réponse deuxième requête utilisateur1: | |
| 3 (11 differences) | . . . × |
| Length: 1,008 | Hex |
| = "xsd:xml"> <accounts message="Results for utilisateur1"><account><username>utilisateur1</username><signature>Created by Matthias Hautin </signature></account><td><<mark>/</mark>returi</td></accounts> | < <mark>/</mark> returi |

On peut donc remarquer les différences.

Énumération des logins

Aller dans l'onglet Repeater de BurpSuite

Faire un clique droit sur l'onglet de la réponse correct avec utilisateur1 puis cliquer sur "Send to the Intruder" ou faire "Ctrl+l":

| Response | | | | | | | |
|--|-------------------|--------|-------|--|--|--|--|
| Pretty Raw Rend | ler \n Actions 🗸 | | | | | | |
| 1 HTTP/1.1 200 2 Date: Mon, 28 3 Server: Apach | ок Scan | | | | | | |
| 4 Expires: Thu, 5 Cache-Control | Send to Intruder | Ctrl-I | idate | | | | |
| 6 Pragma: no-ca | Send to Repeater | Ctrl-R | | | | | |

Se rendre dans l'onglet intruder/Positions puis cliquer sur "Clear §":

| Burp | Project | Intruder | Repeater | Window | Help |
|-----------|---------|----------|----------|----------|------|
| Dashboard | | Target | Proxy | Intruder | F |
| 1 × | 2 × | | | | |
| Target Po | | ositions | Payloads | Options | |
| | | | | | |

Payload Positions

Voilà notre requête que l'on vient d'envoyer.

Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads ar

```
Attack type: Sniper
 1 POST /mutillidae/webservices/soap/ws-user-account.php HTTP/1.1
 2 Upgrade-Insecure-Requests: 1
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Geo

 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image
 5 Referer: http://172.16.10.5/mutillidae/webservices/soap/ws-user-account.php
 6 Accept-Encoding: gzip, deflate
7 Accept-Language: en-US,en;q=0.9
 8 Cookie: showhints=§1§; PHPSESSID=§h98b9p9boou5jmn5s6mujh8i25§
 9 Connection: close
10 SOAPAction: urn:ws-user-account#getUser
11 Content-Type: text/xml;charset=UTF-8
12 Host: 172.16.10.5
13 Content-Length: 457
14
15 <soapenv:Envelope xmlns:xsi="§http://www.w3.org/2001/XMLSchema-instance§" xmlns:xsd="§htt
16
      <soapenv:Header/>
17
      <soapenv:Body>
         <urn:getUser soapenv:encodingStyle="§http://schemas.xmlsoap.org/soap/encoding/§">
18
             <username xsi:type="§xsd:string§">§utilisateurl§</username>
19
          </urn:getUser>
20
21
      </soapenv:Body>
22 </soapenv:Envelope>
```

Cliquer sur "Clear §":



Puis après avoir clear faire un double clique sur le login "utilisateur1", on peut voir apparaître la valeur en surligné jaune:



Puis cliquer sur "Add §"



On peut remarquer que utilisateur1 est en surligné vert et il est entouré de 2 "§":

```
.e="http://schemas.xmlsoap.org
;">§utilisateurl§</username>
```

Ensuite ouvrir un éditeur de texte par exemple Text editor, je l'ai appelé DicoMatthias. Y ajouter plusieurs login et le save dans Kali / Documents:



Puis aller dans l'onglet intruder/Payload:

| Dashbo | ard | Farget | Proxy | Intruder | |
|--------|-----------|--------|----------|----------|--|
| 1 × | 2 × | | _ | | |
| Target | Positions | | Payloads | Options | |

Puis Payload Options [Simple list] et y insérer notre liste:

Payload Options [Simple list]

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

| Paste | utilisateur2 | |
|---------------|-------------------|---|
| | matthias | |
| Load | Hugo | |
| Remove | paul | |
| | admin | 1 |
| Clear | Greg | |
| | Davy | |
| | louise | |
| | test | |
| | | |
| Add | Enter a new item | |
| Add from list | [Proversion only] | |

Après aller dans l'onglet intruder/Option:

| Burp | Project | Intruder | Repeater | Window | Help |
|-----------|---------|----------|----------|----------|------|
| Dashboard | | Target | Proxy | Intruder | F |
| 1 × | 2 × | | | | |
| Target | Po | sitions | Payloads | Options | |

Aller dans la rubrique Grep Extract, cliquer sur Add, puis saisir "Results for" ce qui correspond à une chaîne de caractère d'un login correct.

| ? | Grep - Extract | |
|---|--|--|
| Q | These settings can be us | ed to extract useful information from responses into the attack results table. |
| | Extract the followi | 5 Define extract |
| (| Add Edit Remove Duplicate Up | Define the location of the item to be extracted. Selecting the item in the realso modify the configuration manually to ensure it works effectively. Define start and end Start after expressiol: Results for Start at offset: 213 |
| | Clear Maximum capture leng | End at delimiter: End at fixed length: |
| ? | Grep - Payloads | Exclude HTTP headers 🔽 Update config based on selection below |

Puis cliquer sur "Start Attack":



23/11/22

Voici donc la liste d'énumération des logins:

| 5 | | | | Int | truder atta | ick2 | | _ [| × |
|-----------------|--------------|-------------|---------|-------|-------------|--------|--|---------|---|
| Attack Sa | ve Columns | | | | | | | | |
| Results | Target Posi | tions Paylo | ads Opt | ions | | | | | |
| Filter: Show | ingallitems | | | | | | | | ? |
| Request \land | Payloa | ad | Status | Error | Timeout | Length | Results for | Comment | |
| 0 | | 2 | 200 | | | 1008 | utilisateur1"> <account></account> | | |
| 1 | utilisateur2 | 2 | 200 | | | 1007 | utilisateur2"> <account></account> | | |
| 2 | matthias | 2 | 200 | | | 902 | | | |
| 3 | Hugo | 2 | 200 | | | 898 | | | |
| 4 | paul | 2 | 200 | | | 898 | | | |
| 5 | admin | 2 | 200 | | | 976 | admin"> <account><user< td=""><td></td><td></td></user<></account> | | |
| 6 | Greg | 2 | 200 | | | 898 | | | |
| 7 | Davy | 2 | 200 | | | 898 | | | |
| 8 | louise | 2 | 200 | | | 900 | | | |
| 9 | test | 2 | 200 | | | 898 | | | |

Force brute d'un mot de passe 1) Préparation de l'attaque

Une attaque de force Brut consiste à trouver un mot de passe d'un utilisateur existant à l'aide d'un dictionnaire de mots de passe que l'on teste en boucle. Nous allons créer nous même un dictionnaire, ne possèdent pas un dictionnaire important de mots de passe.

Aller sur Burp Suite mettre Intercep en mode "Intercept off", aller dans mutillidae avec Open Browser, mettre le level Security : 0

Puis aller dans OWASP 2017 > A2 > Authentication Bypass > Via Brute Force > Login:

| | | | 🤆 C | OWASP | Mutillida | e II: | Keep C |
|--------------|--|-----------------------|---------------|-----------------------|--------------------|-----------|--------------------|
| | | | Version: 2.6 | 6.67 Securi | ty Level: 0 (Hose | d) H | ints: Enabled (|
| | | ł | Iome Login/Re | egister 🛛 Toggle Hint | s Show Popup Hints | Toggle Se | curity Enforce SSL |
| OWASP 2017 | A1 - Injection (SQL) | | | | | | |
| OWASP 2013 | A1 - Injection (Other) | ts and Videos | | J | | | |
| OWASD 2010 | A2 - Broken Authentication and Session | Authentication Bypass | • | Via Brute Force | | ▶ L | ogin |
| 0 WASP 2010 | Management | Priviliege Escalation | • | Via Cookies | | | |
| OWASP 2007 | A3 - Sensitive Data Exposure | Username Enumeration | • | Via SQL Injection | 1 | ► I | |
| Web Services | A4 - XML External Entities | | Video II | utoriais | | | |

Page Login pour Brute Force:

| | | | ow 👾 ow | ASP Mutillidae | II: Keep Calm and | l Pwn On |
|--|------|------------------|---------------------|-----------------------------------|---|------------------------|
| | | | Version: 2.6.67 | Security Level: 0 (Hosed) | Hints: Enabled (1 - Try easier) | Not Logged In |
| | | | Home Login/Register | Toggle Hints Show Popup Hints Tog | ggle Security Enforce SSL Reset DB View I | Log View Captured Data |
| OWASP 2017 | | | | | Login | |
| OWASP 2013 | Back | Welp Me! | | | ¥ | |
| OWASP 2007 | | Uinte and Videoe |] | | | |
| Web Services | | Hints and videos | | | | |
| HTML 5 | | | | | Please sign-in | |
| Others 🕨 | | | | User | name [] |) |
| Documentation • | | | | Pass | word |) |
| Resources • | | | | | Login | |
| PayPal - The safer, easier way to pay online! | | | | Dont h | ave an account? Please register he | ere |

Retourner sur Burp Suite et mettre "Intercept On".

Cette partie consiste à créer une variable, sur mutillidae saisir:

Username : utilisateur2

Password : yugzey4566 (n'importe quel mot de passe erroné)

Sur Burp Suite on peut donc apercevoir la requête:



On retrouve le mot de passe que j'ai utilisé

2) Lancement de l'attaque

Faire un clique droit vers "Send to Intruder" comme déjà réalisé. Puis aller dans Intruder et y remarque un nouvel onglet "3 x":

| Burp | Project | Intruder | Repeater | Window He |
|-----------|---------|--------------|----------|-----------|
| Dashboard | | Target | Proxy | Intruder |
| 1 × | 2 × | (З × | | |
| Targe | t Po | sitions | Payloads | Options |

Puis l'onglet position et "Clear §" comme précédemment réalisé.

Puis double cliquer sur le password "yugzey4566" et faire "Add §" pour créer notre variable. username=utilisateur2&password=§yugzey4566§&l

23/11/22

Puis créer un nouveau dictionnaire avec différents mots de passe ainsi que le mot de passe correct de utilisateur2 = "utilisateur2":



Puis charger les mots de passes dans "Payload/Payload Options "comme précédemment effectué:

Payload Options [Simple list]

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

| Paste | admin | |
|---------------|--------------------|----|
| | test | |
| Load | 1234 | |
| Remove | pourquoipas | ι. |
| | utilisateur2 | ь |
| Clear | azerty | Ľ |
| | password | L |
| | adminpass | ι. |
| | | |
| | | |
| Add | Enter a new item | |
| Add from list | [Pro version only] | |

Et on lance l'attaque:

| Attack Sa | ve Columns | | | | | | | | | |
|---------------------------|---------------------|-----------|-------|---------|--------|---------|--|--|--|--|
| Results | Target Positions Pa | yloads Op | tions | | | | | | | |
| Filter: Showing all items | | | | | | | | | | |
| Request \land | Payload | Status | Error | Timeout | Length | Comment | | | | |
| 0 | | 200 | | | 55232 | | | | | |
| 1 | admin | 200 | | | 55232 | | | | | |
| 2 | test | 200 | | | 55232 | | | | | |
| 3 | 1234 | 200 | | | 55232 | | | | | |
| 4 | pourquoipas | 200 | | | 55232 | | | | | |
| 5 | utilisateur2 | 302 | | | 382 | | | | | |
| 6 | azerty | 200 | | | 55357 | | | | | |
| 7 | password | 200 | | | 55357 | | | | | |
| 8 | adminpass | 200 | | | 55357 | | | | | |

On a une réponse 302 ce qui signifie que le mot de passe "utilisateur2" correspond à la bonne authentification.

Bien évidemment qu' en conditions d'audit de sécurité nous utiliserons un dictionnaire beaucoup plus volumineux avec plus de mots de passe.

CHALLENGE 1 : énumération des logins en mode sécurisé

D1.Q1. Fermer puis relancer BurpSuite. Positionner le niveau de sécurité à 5 et relancer l'attaque en suivant les étapes "Test d'une requête et d'une réponse sur un login existant", "Énumération des logins". Montrez votre travail par des copies d'écran (avec votre nom) et des explications.

Tout d'abord créer un nouveau user dans Mozilla que je vais appeler:

username : Matthias Password : Matthias1234

Please choose your username, password and signature

| Username | Matthias |) | | |
|------------------|------------------------|--------------------|--|--|
| Password | ••••• | Password Generator | | |
| Confirm Password | ••••• |) | | |
| Signature | Create by Matthias Hay | tio | | |
| | Create Accoun | ıt | | |

Puis aller sur Burp Suite et aller dans Prox/Intercept, mettre "Intercept is off". Puis cliquer sur Open Browser:

| Burp | Project | Intruder | Repeater | Window | Help | | | | |
|-------|---------|-------------|----------|--------------|-----------|---------|----------|--------------|-----|
| Das | nboard | Target | Proxy | Intruder | Repe | ater Se | equencer | Decoder | Соп |
| Inter | rcept | HTTP histor | y Web | Sockets hist | ory O | ptions | | | |
| | | | | | | | | | |
| | Forward | | Drop | Intercep | ot is off | Actio | n (| Open Browser | |

Puis inserer le lien sur serveur mutillidae : *"172.16.10.5/mutillidae"* Mettre la sécurité au level 5 cliquer sur Toggle Security:

| ÷ | → | G | A Not secure | 172.16.10.5/mutillidae/index.php?popUpNotificatior |
|---|---|---|-----------------|--|
| | | | | OWASP Mutillidae II: K |
| | | ۷ | /ersion: 2.6.67 | 7 Security Level: 5 (Server-side Security) |
| | | | Н | lome Login/Register Show Popup Hints Toggle Security Dro |

Ensuite aller dans OWASP 2017 > A2 > Authentication Bypass > Via Brute Force > Login:

| | | | •¥ OV | VASP I | Mutillidae | e II: K | eep C |
|--------------|--|-----------------------|--------------------|------------------|-------------------|-----------------|-------------|
| | | | Version: 2.6.6 | 7 Security | / Level: 0 (Hosed | l) Hints: | Enabled (|
| | | | Home Login/Registe | er Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL |
| OWASP 2017 | A1 - Injection (SQL) | | | | | | |
| OWASP 2013 | A1 - Injection (Other) | ts and Videos | | | | | |
| OWASD 2010 | A2 - Broken Authentication and Session | Authentication Bypass | ► vi | ia Brute Force | | ▶ Login | |
| 0 WASP 2010 | Management | Priviliege Escalation | ► vi | ia Cookies | | | |
| OWASP 2007 | A3 - Sensitive Data Exposure | Username Enumeration | ▶ vi | ia SQL Injection | | • | |
| Web Services | A4 - XML External Entities | | Video Iuto | riais | | | |

Je remet "Intercept is on"

| Dashboard | Target | Proxy | Intruder | Repea | ater Sequ |
|-----------|-------------|-------|----------------|-------|-----------|
| Intercept | HTTP histor | y Web | Sockets histor | y O | ptions |
| | | | | | |
| Forward | | Drop | Intercept | is on | Action |

Comme prévu on arrive sur la page de login.

Dans cette page je dois m'identifier sans insérer un mauvais mot de passe afin de récupérer une requête que je vais pouvoir modifier.

Je vais donc tenter de me connecter avec:

username : Matthias Password : gfyzgf4157

Bien évidemment je sais que ce mot de passe n'est pas le bon mais on se met à la place de l'attaquant.

| | Login | | | |
|------|----------|----------------|--|--|
| Back | 🥞 Help N | Ne! | | |
| | | Please sign-in | | |
| | Username | Matthias | | |
| | Password | | | |
| | | Login | | |

Dont have an account? Please register here

Lorsque que je clique sur login une erreur qui dit que je ne peux pas envoyer la requête car il détecte un élément dangereux. Burp Suite est blacklisté.



D1.Q2. Les informations affichées par le comparateur sont-elles exploitables pour tenter une énumération?

Le navigateur nous dit qu'il détecte un élément dangereux. Qu'il ne peut pas autoriser cet élément qui est dans la liste noire. Donc nous savons que lorsque l'on met le niveau 5 de sécurité il y a donc plus de sécurité et un filtre qui bloque les attaques vers BurpSuite.

Par ailleurs, en inspectant la page du navigateur on trouve une fonction nommée onsubmit qui est sûrement liée au fait d'avoir le toggle security au level 5, l'erreur du navigateur provient de cela.

| R | 6 | Elements | Console | Sources | Network | Performance | Memory | Applica |
|---|---|----------------------------------|---------|---------|---------|-------------|--------|---------|
| | | <pre>><script></script></pre> | | | | | | |

Cependant, on peut aller plus loin en recherchant la fonction "onSubmitOfLoginForm" avec Ctrl+f dans notre inspection de la page.

```
... ple.main-table-frame tbody tr td t
onSubmitOfLoginForm
```

Désormais on en connait plus sur cette fonction, c'est donc du Js.

```
v<script type="text/javascript">
   <! - -
       var l loggedIn = false;
   var lAuthenticationAttemptResultFlag = -1;
   var lValidateInput = "FALSE"
       function onSubmitOfLoginForm(/*HTMLFormElement*/ theForm){
           try{
               if(lValidateInput == "TRUE"){
                   var lUnsafeCharacters = /[\ ~!@#$%^&*() - =+ []
   {}\\|;':",./<?]/;</pre>
                   if (theForm.username.value.length > 15 ||
                        theForm.password.value.length > 15){
                           alert('Username too long. We dont want to
   allow too many characters.\n\nSomeone might have enough room to
   enter a hack attempt.');
                            return false;
                   };// end if
                   if
   (theForm.username.value.search(lUnsafeCharacters) > -1 ||
   theForm.password.value.search(lUnsafeCharacters) > -1){
                           alert('Dangerous characters detected. We
   can\'t allow these. This all powerful blacklist will stop such
   attempts.\n\nMuch like padlocks, filtering cannot be
   defeated.\n\nBlacklisting is l33t like l33tspeak.');
                           return false;
                   };// end if
               };// end if(lValidateInput)
               return true;
           }catch(e){
               alert("Error: " + e.message);
           };// end catch
       };// end function onSubmitOfLoginForm(/*HTMLFormElement*/
   theForm)
   11-->
 </script>
```

D1.Q3. Dans tous les cas, tentez une énumération et indiquez ce qui se passe (copies d'écran...). Test level 1:

Je vais donc tenter de mettre le Toggle Security au niveau 1 et refaire le test entièrement afin de voir si on a toujours le message d'erreur.





On a toujours notre message d'erreur, et la fonction est toujours présente. Je descend donc encore d'un niveau.

Test level 0:

Encore une fois je vais donc mettre le Toggle Security au niveau 0 et refaire le test entièrement afin de voir si on a toujours le message d'erreur.

```
        Version: 2.6.67
        Security Level: 0 (Hosed)

        Home
        Login/Register
        Toggle Hints
        Show Popup Hints
        Togg
```

Par ailleurs, je rappelle mes identifiant de connexions choisi pour le test son:

username : Matthias

Password : gfyzgf4157 (mauvais mdp)

J'arrive à récupérer la requête dans le logiciel Burp Suite. On comprend donc que lorsque le niveau de sécurité est au plus faible le navigateur n'a plus le script en JS dans lequelle il y a la fonction "onSubmitOfLoginForm". Pour vérifier ceci j'inspecte la page et recherche la fonction. Que je ne trouve pas.

Requête BurpSuite:



Je peux donc continuer l'attaque:

Je clique droit sur la requête récupère et clique sur "Send to Intruder".

Je vais dans l'onglet Intruder et clique sur "Cleat §" afin de supprimer toutes les variables déjà créées.

Puis double clique sur mon faux password et Add §"

Voilà notre mot de passe est donc désormais en vert, c'est donc une variable:

username=Matthias&password=§gfyzgf4157§&login-php-submit-button=Login

Ensuite il faut créer notre propre dictionnaire de mot de passe. Avec le bon mot de passe dedans.



Puis on l'introduit dans le PayLoad ce qui va permettre de comparer tous les mot de passe. Et trouver le bon ou pas. En testant chacun des mots de passe requête par requête. Ce qui est donc facile à voir dans les logs du serveur mutillidae.

Payload Options [Simple list]

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

| Paste | test | |
|---------------|--------------|---|
| | Password | |
| Load | 1234567 | |
| Bomous | azertyuip | |
| Remove | Matthias1234 | |
| Clear | toto | |
| | lol | |
| | mdp | |
| | | |
| | | |
| | | _ |
| Add | | |
| | | - |
| Add from list | | ` |

Puis cliquer sur "Start Attack" pour lancer l'attaque.

Voici la réponse de l'attaque que je viens de lancer. On peut y apercevoir qu'au niveau du mot de passe correct le Status est "302", ce qui veut dire que le password est correct. On l'a donc trouvé.

| 5 | | | | Int | truder atta | ick1 | |
|-----------------|---------------|----------|----------|---------|-------------|--------|--|
| Attack Sa | ve Columns | | | | | | |
| Results | Target Po | ositions | Payloads | Options | | | |
| Filter: Show | ing all items | | | | | | |
| Request \land | Pay | load | Status | Error | Timeout | Length | |
| 0 | | | 200 | | | 55232 | |
| 1 | test | | 200 | | | 55232 | |
| 2 | Password | | 200 | | | 55232 | |
| 3 | 1234567 | | 200 | | | 55232 | |
| 4 | azertywip | | 200 | | | 55232 | |
| 5 🔇 | Matthias1234 | | 302 | | | 378 | |
| 6 | toto | | 200 | | | 55320 | |
| 7 | lol | | 200 | | | 55320 | |
| 8 | mdp | | 200 | | | 55320 | |

Lorsque l'on clique sur la requête qui a fonctionné on peut voir son descriptif.





On peut en conclure que la méthode d'attaque par Force Brute fonctionne correctement quand le niveau de sécurité du serveur n'est pas très élevé.

D1.Q4. Chercher dans le code source de la page ws-user-account.php (située dans /var/www/html/ mutillidae/webservices/soap/) le codage mis en place permettant d'obtenir un encodage sécurisé. Expliquer le rôle de l'instruction EncodeforHTML.

Aller dans la machine Mutillidae et chercher dans:

/var/www/html/mutillidae/webservices/soap/

ouvrir le fichier ws-account.php:

```
prof@prof:~$ cd /var/www/html/mutillidae/webservices/soap/
prof@prof:/var/www/html/mutillidae/webservices/soap$ ls
lib ws-hello-world.php ws-lookup-dns-record.php ws-user-account.php
prof@prof:/var/www/html/mutillidae/webservices/soap$ sudo nano ws-user-account.php
```

Pour trouver l'instruction plus facilement faire "Ctrl+W" et taper la recherche. Voici donc l'instruction EncodeforHTML:

| function doXMLEnco | deQueryResults(\$pUsername, \$pQueryResult, \$pEncodeOutput){ |
|---|---|
| \$lResults \$lUsername \$lSignatur | = " <accounts for="" message='\"Results' {\$pusername}\"="">"; e = ""; re = "";</accounts> |
| while(\$rou | u = \$pQueryResult->fetch_object()){ |
| \$p (\$row->username):\$1Usernam | EncodeOutput?\$lSignature = \$lUsername = \$Encoder->encodeForHTML ne = \$row->username;; |
| if (\$row->mysignature):\$lSign }/ | (isset(\$row->mysignature)){ \$pEncodeOutput?\$lSignature = \$Encoder->encodeForHTML ature = \$row->mysignature; 7 end if |
| \$1 \$1 if _ <signature>{\$1Signature} \$1</signature> | Results.= " <account>"; Results.= "<username>{\$1Username}</username>"; (isset(\$row->mysignature)){\$1Results.= ";}; Results.= "</account> "; |
| }// end wh | ile |

Cette partie de code permet de créer une signature encodée lors de la première authentification(register) puis récupérer cette signature encodée et la met dans un tableau.. Puis après lors d'une connexion il compare la signature créer dans la tableau avec celle de l'utilisateur qui veut se connecter donc la nouvelle demande de connexion. Si la signature est correcte alors la connexion est établie mais si celle-ci est mauvaise alors l'utilisateur voulant se connecter ne pourra pas.

APPRENTISSAGE 2 : vol de session Interception du cookie

L'objectif de cette partie est de trouver le login et le mot de passe de connexion d'un compte utilisateur en lui détournant les cookies d'authentification.

Pour commencer je vais me déconnecter de la mutillidae et arrêter la capture de trame du serveur proxy de BurpSuite.

Voilà comment arrêter la capture de trames, faire Proxy>Intercept>Intercept is off:

| Dashboard | | Target | Proxy |
|-----------------------|--------------------|------------------|-------|
| ntercept HTTP history | WebSockets history | Options | |
| | | | |
| Forward | Intercept is off | Action Open Brow | ISAL |
| Forward Drop | Intercept is on | | vser |

Puis je créer un compte totalement normal dans un nouveau navigateur.Que je note dans la description de ma VM.

| Please choose | your usernar | ne, password and signature |
|---|--------------|----------------------------|
| | | |
| Username | toto | |
| Password | toto1234 | Password Generator |
| Confirm Password | ••••• | |
| Signature | Bien joué!! | |
| | | li. |
| | | |
| | Create | Account |
| Note description VM: | | |
| Compte Mutillidae: | | |
| Username: toto Password:toto1234 | | |
| Username: Matthias Password: Matthias1 | 234 | |
| Username: utilisateu Password: utilisateur | r1 1 | |

A2.Q1 : Faites une copie d'écran qui montre ce niveau.

Puis mettre mutillidae en toggle security 0:



Retourner sur Burp Suite cliquer sur "Open Browser" et garder le "Intercept is off", on va réaliser une élévation des privilèges du compte que l'on vient de créer en se connectant au même moment.

Pour cela OWASP 2017> A2> Privilege Escalation > Login

| OWASP 2017 | A1 - Injection (SQL) | | |
|--------------|---|-----------------------|----------------------------|
| OWASP 2013 | A1 - Injection (Other) | s and Videos | J |
| OWASP 2010 | A2 - Broken Authentication and Session Management | Authentication Bypass | TIP: Click Hint and Videos |
| OWASP 2007 | A3 - Sensitive Data Exposure | Priviliege Escalation | Via Cookies |
| Web Services | A4 - XML External Entities | | Via CBC-bit Flipping |
| HTML 5 | A5 - Broken Access Control | | |

Puis entrer l'authentification du compte toto puis cliquer sur "Login":

| Please sign-in | | | |
|----------------|-------|--|--|
| Username | toto | | |
| Password | ••••• | | |
| | Login | | |

Dont have an account? Please register here

A2.Q2 : Faites une copie d'écran du résultat obtenu et indiquez comment vous voyez que vous êtes bien connecté avec votre utilisateur.

Ce message apparaît, on a donc bien plus de privilèges.



Je suis bien connecté en tant que toto.

On peut même voir la description de ma signature: "Bien joué!!"



Ensuite on va donc autorisé le proxy Burp à faire des capture de trames: Pour cela: "Intercept is on"



Puis actualiser la page afin de capter la requête: Pour cela:



ou "Ctrl + f5"

On sera donc automatiquement renvoyé sur la page Intercept du proxy BurpSuite. Voilà donc la requête récupéré:

| l | ntercept | HTTP history | WebSockets history | Options |
|-----------------------|---|---|---|--|
| | Request to l | http://172.16.10.5:8 | 0 Intercept is on | Action Open Browser |
| Р | retty Raw | \n Actions 🗸 | | |
| 1 2 3 4 5 | GET /muti Host: 172 Cache-Cor Upgrade-J User-Ager Chrome/88 Accept: | lllidae/index. 2.16.10.5 ntrol: max-age Insecure-Reque nt: Mozilla/5. 3.0.4324.150 S | php?popUpNotificat: =0 sts: 1 0 (Windows NT 10.0 afari/537.36 | ionCode=AU1 HTTP/1.1 : Win64; x64) AppleWebKit/537.36 (KHTML, like |
| 7 | text/html lication/ Referer: Accept-Er | .,application/ /signed-exchan http://172.16 ncoding: gzip, | xhtml+xml,applicat: ge;v=b3;q=0.9 .10.5/mutillidae/in deflate | lon/xml;q=0.9,image/avif,image/webp,image/apr ndex.php?page=login.php |
| 9 10 11 12 | Accept-La Cookie: s Connectio | anguage: en-US showhints=1; u on: close | ;,en;q=0.9 sername=toto; uid=: | L38; PHPSESSID=756gstipg8tvhgmoi3onrv3lfc |

A2.Q3 : Faites une copie d'écran pour montrer le cookie du nom de votre utilisateur. Quelle est sa valeur ?

Si on analyse mieux cette requête on peut donc voir différents cookies, on s'intéresse donc à 2 cookies en particulier: le nom de l'utilisateur "**username**=toto", le username id "**uid**=138"

Cookie: showhints=1; username=toto; uid=138; PHPSESSID=756gstipg8tvhgmoi3onrv3lfc Connection: close

Vol de la session

Dans cette partie on va tenter de voler la session admin grâce à l'uid de cookie récupéré dans la requête précédente

Pour débuter modifier la valeur de l'uid pas 1. Car on suppose que admin étant le premier utilisateur créé donc uid=1.

Saisir donc:



Puis cliquer sur "Forward":

On peut donc voir que l'on est connecté en tant qu' "admin".

| m and Pwn On | 8 | Status Update |
|------------------------------------|---|----------------|
| Logged In Admin: admin (g0t r00t?) | | Osci Addictica |

Nous arrivons donc à nous connecter avec le compte admin.

A2.Q4 : Répondez à toutes ces questions :

Pourquoi a-t-on changé d'utilisateur ?

On a changé d'utilisateur pour se mettre en admin afin de pouvoir avoir les privilèges du compte administrateur. Pour pouvoir avoir accès à toutes les données.

Pourquoi sommes-nous maintenant connectés en tant qu'administrateur ?

Nous sommes connectés en tant qu'admin car nous avons récupéré une requête qui contenait les cookies de connexion et nous les avons modifiés. Par déduction nous avons choisi le uid=1 qui était le user admin. Par contre si nous avions augmenté le toggle sécurité de mutillidae au niveau 1 ou 5, nous n'aurions pas pu nous connecter avec se uid.

Qu'elle est l'élément technique qui a permis ce changement, au niveau du serveur ?

L'élément technique qui a permis ce changement au niveau du serveur est que nous avons intercepté la trame envoyée vers le serveur depuis notre navigateur, puis l'avons modifiée afin de nous faire passer par l'utilisateur admin qui voulait se connecter.

S'agit-il d'une manipulation désirée par le serveur et légale ?

Cette manipulation n'est pas désirée par le serveur, elle n'est pas légale. C'est en quelque sorte une usurpation d'identité.

De plus, l'attaquant qui réalise cette attaque ne fait pas ça par hasard.

CHALLENGE 2 : Codage sécurisé et analyse du code source

D2.Q1. Fermer puis relancer BurpSuite. Positionner le niveau de sécurité à 5 et relancer l'attaque en suivant les étapes 1 et 2. La modification du cookie uid a t-elle une conséquence ?

Nous allons donc réessayer de faire une attaque de vol de session mais avec le toggle sécurité de mutillidae au niveau 5.

J'utiliserai le compte créé auparavant: username: toto password: toto1234

Je refait donc entièrement toute la manipulation:

Je vais sur Burpsuite désactiver le Interception des requêtes: "Intercept is off" Puis "Open Browser", je tape l'url du serveur mutillidae. Je mets le toggle sécurité au level 5. Puis OWASP 2017> A2> Privilege Escalation > Login

J'entre les identifiants de connexion du compte toto.

Un message d'erreur s'affiche:

Remarque: Il ressemble familièrement au message que nous avons déjà vu quand j'avais essayé de mettre le toggle sécurité au level 5 auparavant.



Nous n'arrivons donc pas à récupérer la requête car le navigateur nous bloque.

D2.Q2. Observez le code source de la page index.php (page d'accueil) et relever les différences avec le codage de niveau de sécurité 0 et 1.

```
level 0:
                                                                    //g///// 1000//NEC-1/00/01-1000122-7/ 00000/010
   <html>
    <head>...</head>
 v <body onload="onLoadOfBody(this);"> == $0
           ▶ ...
           <!-- Bubble hints code -->
  >>= ><script type="text/javascript">...</script>
           >_div style="border: lpx solid black;">...</div>
           > <script type="text/javascript">...</script>
                 <script type="text/javascript" src="javascript/jQuery/jquery.js"></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></scr
                 <script type="text/javascript" src="./javascript/jQuery/jquery.balloon.js">
                 </script>
                 <script src="javascript/jQuery/colorbox/jquery.colorbox-min.js"></script>
                 k rel="stylesheet" href="javascript/jQuery/colorbox/colorbox.css">
           ▶ <script>...</script>
                 <div id="cbox0verlay" style="display: none;"></div>
            <div id="colorbox" class style="display: none; padding-bottom: 42px; padding-right:</pre>
           42px; ">...</div>
          </body>
   </html>
level 1:
       <html>
         <head>...</head>
 ... ▼ <body onload="onLoadOfBody(this);"> == $0
                >...
               <!-- Bubble hints code -->
                ><script type="text/javascript">...</script>
           ><div style="border: lpx solid black;">...</div>
                > <script type="text/javascript">...</script>
                     <script type="text/javascript" src="javascript/jQuery/jquery.js"></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></scr
                     <script type="text/javascript" src="./javascript/jQuery/jquery.balloon.js">
                     </script>
                     <script src="javascript/jQuery/colorbox/jquery.colorbox-min.js"></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></script></scri
                      <link rel="stylesheet" href="javascript/jQuery/colorbox/colorbox.css">
                ▶ <script>...</script>
                     <link rel="stylesheet" type="text/css" href="styles/gritter/jquery.gritter.css">
                     <script type="text/javascript" src="javascript/gritter/jquery.gritter.min.js">
                      </script>
                ▶ <script>...</script>
                     <div id="cboxOverlay" style="display: none;"></div>
                <div id="colorbox" class style="display: none; padding-bottom: 42px; padding-right:</pre>
                42px; ">...</div>
               </body>
         </html>
```

On peut voir que de nouveau script ce sont ajouté comme par exemple "onSubmitOfLoginForm" et d'autres qui permettent une meilleur sécurité. **D2.Q3**. Expliquer les différences entre un cookie et une session. Conclure sur les bonnes pratiques de codage concernant le suivi des utilisateurs identifiés.

Tout d'abord les cookies et les sessions contiennent des informations sur l'utilisateur. Mais les différences sont que les cookies sont stockés côté client, navigateur web tandis que les sessions sont stockées côté serveur pour nous c'était mutillidae.

Les bonnes pratique en matières de codage concernant le suivi des utilisateurs sont:

- Il est préférable d'utiliser des valeurs uid générées de manières aléatoires et non prévisibles;
- Il faut qu'à chaque authentification avec succès l'id de session soit modifié;
- Et pour finir encoder les id de sessions.