

Hidden form fields

- Never use hidden form fields for sensitive data.
- Never use hidden form fields for sensitive data.

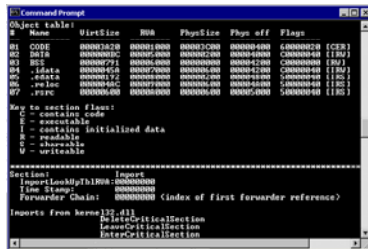
```
<form method="POST" action="login.asp">
  <p>User Name:<input type="text" name="username" size="20">|
  <p>Password:<input type="text" name="password" size="20">
  <input type="submit" value="Submit">
  <input type="reset" value="Reset">
  <input type="hidden" name="accountnumber" value="40-27-07:236743"></p>
</form>
```

- Never use hidden form fields for sensitive data.
- Never use hidden form fields for sensitive data.



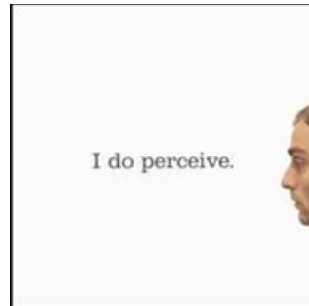
Validate third-party programs

- ISAPI DLLs can gain elevated privileges to the level of the built-in SYSTEM account.
- Inspect third party executables on your site.
- Use Microsoft's Binary File Dumper tool (dumpbin.exe).
- dumpbin /imports UntrustedISAPI.DLL | find "RevertToSelf"



End-to-end reliability

Lack of reliability
=
Perceived lack of
security



Phishing

- www.antiphishing.org

