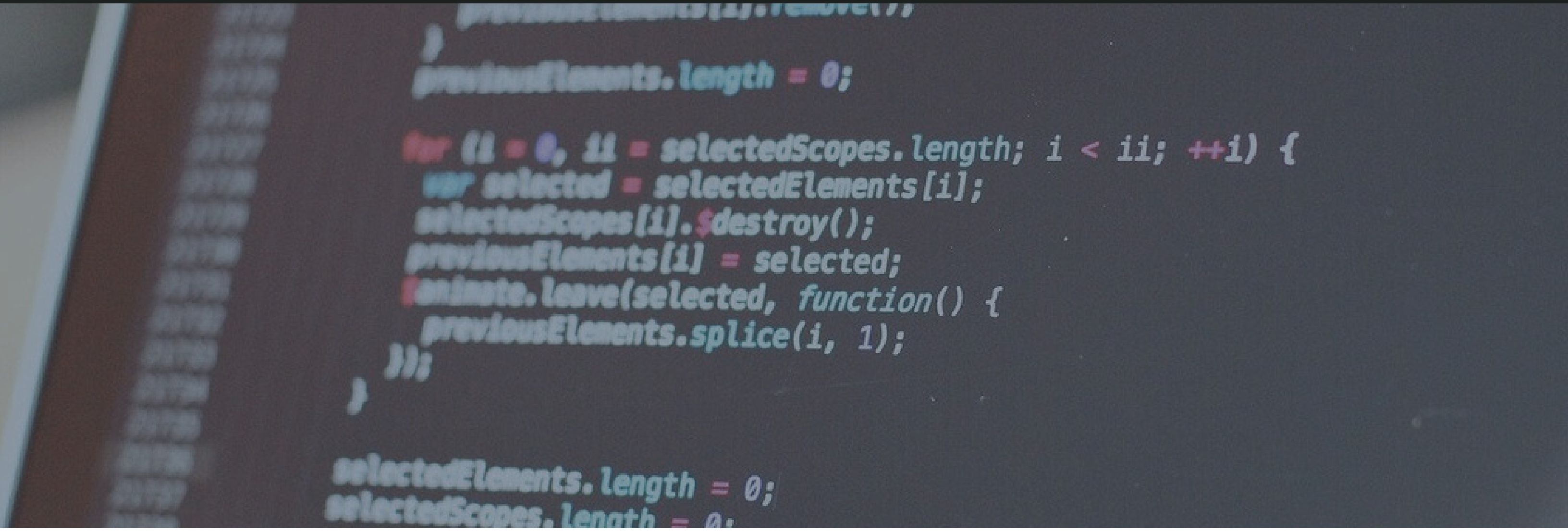
PROTEXITY



```
previousElements[i].remove();
}
previousElements.length = 0;

for (i = 0, ii = selectedScopes.length; i < ii; ++i) {
  var selected = selectedElements[i];
  selectedScopes[i].$destroy();
  previousElements[i] = selected;
  $animate.leave(selected, function() {
    previousElements.splice(i, 1);
  });
}

selectedElements.length = 0;
selectedScopes.length = 0;
```

PENETRATION TESTING

Penetration testing takes an adversarial approach to identifying vulnerabilities and demonstrating the impact those vulnerabilities could have on the organization if exploited by an attacker.

Protexity offers a full spectrum of penetration testing services to address an organization's specific needs. This spectrum covers cloud environments, physical office spaces, web applications and APIs, wireless networks, and internal / external networks.

CONTACT US:

☎ 844-474-6700

✉ SALES@PROTEXITY.COM

WWW.PROTEXITY.COM

EXTERNAL PENETRATION TESTING

External penetration testing is an offensive security assessment that focuses on evaluating the security of an organization's external-facing systems through simulated attacks. Its goal is to identify vulnerabilities in cloud environments and other elements of the network perimeter that could be exploited by attackers to gain unauthorized access, disrupt services, or compromise sensitive information.

INTERNAL PENETRATION TESTING

As it sounds, internal penetration testing is an offensive security assessment focused on identifying and exploiting vulnerabilities in an organization’s internal network. They are an excellent means to improving security posture as an internal network typically is not hardened like a network perimeter. Internal penetration tests are similar to external ones, but are usually more involved as there is a greater attack surface. For example, hosts will have more open ports and network traffic can be captured and analyzed for sensitive information such as user credentials.

CONTACT US:

☎ 844-474-6700

✉ SALES@PROTEXITY.COM

WWW.PROTEXITY.COM

WIRELESS PENETRATION TESTING

Wireless signals, in most cases, are not contained within a building and emanate beyond an organization’s walls. This introduces cyber risk as unauthorized access to the network becomes a real possibility. Wireless penetration testing helps identify vulnerabilities and misconfigurations in a wireless network that can lead to illegal access to a network and its data.

PHYSICAL PENETRATION TESTING

While cyber threats from a physical perspective are not at the same scale as their digital counterparts, they do exist. They can also lead to significant harm through business disruption, compliance violations, and reputational damage. Physical penetration testing helps identify vulnerabilities in physical access control systems, operational processes, policies and procedures, and more.

PROTEXITY

WEB APP & API PENETRATION TESTING

Web application penetration testing is a specialized form of security assessment that focuses on identifying vulnerabilities and weaknesses in web applications. Web applications can be only internally accessible or publicly accessible. The primary objective is to simulate real-world attacks on the target application(s) to proactively discover potential security risks that could be exploited by attackers. The end result being to gain assurance there is no path to unauthorized access, service disruption, or access to sensitive information.

KEY BENEFITS OF PENTESTING

- Proactively identify vulnerabilities
- Reduce your attack surface
- Mitigate business risk
- Know where your defenses stand
- Meet regulatory compliance requirements

CONTACT US:

☎ 844-474-6700

✉ SALES@PROTEXITY.COM

🌐 WWW.PROTEXITY.COM